Algebraic Integration of Retrenchment and Refinement

A thesis submitted to The University of Manchester for the degree of
Doctor of Philosophy
in the Faculty of Engineering and Physical Sciences

2005

Czeslaw Tadeusz Jeske

School of Computer Science

Contents

Abstract **6**

Declaration **7**

Copyright **8**

Acknowledgements **9**

Chapter 1
Introduction **11**

Chapter 2
Refinement by Simulation **18**
2.1 Notation 19
2.2 Simulation 20
2.2.1 The He, Hoare and Sanders model 20
2.2.2 Admitting partial operations 23
2.2.3 Operations with input and output 24
2.2.4 I/O-filtered refinements. 26
2.2.5 Related work 27
2.3 Transition System Framework 29
2.4 The Need to Liberalise Refinement 31
2.4.1 The number recycler 32

Chapter 3
Retrenchment **34**
3.1 From Refinement to Retrenchment 34
3.2 Primitive Retrenchment 35
3.3 Output Retrenchment 37
3.4 Definitions 38
3.5 Retrenchment in Action 39
3.6 Other Approaches to Liberalising Refinement 40

Chapter 4
Combining Retrenchments and Refinements **44**
4.1 Composing Retrenchments with Refinements 44
4.2 The Lifting Construction 49
4.3 The Lowering Construction 50
4.4 The Postjoin Construction 51
4.5 The Prejoin Construction 51

4.6 An Engineering Perspective 52
4.7 The Tower Pattern 53

Chapter 5
The Lifting Theorem **55**
5.1 The Lifting Theorem 55
5.2 Proof for Part (1) 56
5.2.1 The system *Univ* 57
5.2.2 The retrenchment from *Abs* to *Univ* 58
5.2.3 The refinement from *Univ* to *Conc* 60
5.2.4 The relations of the retrenchment from *Abs* to *Conc* 64
5.2.5 Properties of *Univ* 65
5.3 Proof for Part (2) 67
5.3.1 The system *Xtra*. 68
5.3.2 The refinement from *Univ* to *Xtra* 69
5.3.3 The inclusions 73
5.4 Proof for Part (3) 77
5.5 Idempotence 77
5.6 Inside *Univ* 79

Chapter 6
The Lowering Theorem **83**
6.1 The Lowering Theorem 83
6.2 Proof for Part (1) 84
6.2.1 The system *Univ* 85
6.2.2 The refinement from *Abs* to *Univ* 87
6.2.3 The retrenchment from *Univ* to *Conc* 89
6.2.4 The relations of the retrenchment from *Abs* to *Conc* 91
6.2.5 Properties of *Univ* 93
6.3 Proof for Part (2) 95
6.3.1 The system *Xtra*. 95
6.3.2 The refinement from *Xtra* to *Univ* 96
6.3.3 The inclusions 100
6.4 Proof for Part (3) 102
6.5 Idempotence 102
6.6 Inside *Univ* 105

Chapter 7
Completing the Square **107**
7.1 The Square and Its Components 107
7.2 Overture on *G* 108
7.3 Working in *C* 112
7.4 Encompassing I/O Components 116
7.5 The Class of Systems 121

Chapter 8
The Postjoin Theorem **122**
8.1 The Postjoin Theorem 122
8.2 Basic Definitions 123
8.3 Proof for Part (1) 126

8.3.1 The system *Univ* 127
8.3.2 The refinement from *Ret* to *Univ* 128
8.3.3 The retrenchment from *Ref* to *Univ* 131
8.3.4 The retrenchment from *Abs* to *Univ* 133
8.3.5 Properties of *Univ* 136
8.4 Proof for Part (2) 141
8.4.1 The system *Xtra*. 142
8.4.2 The refinement from *Univ* to *Xtra* 143
8.4.3 The inclusions 151
8.5 Proof for Part (3) 153
8.6 Lemmas 153
8.7 Inside *Univ* 154

Chapter 9
The Prejoin Theorem **159**
9.1 The Prejoin Theorem 159
9.2 Basic Definitions 160
9.3 Preconjointness 163
9.4 Proof for Part (1) 164
9.4.1 The system *Univ* 164
9.4.2 The refinement from *Univ* to *Ref* 166
9.4.3 The retrenchment from *Univ* to *Ret* 169
9.4.4 The retrenchment from *Univ* to *Conc* 170
9.4.5 Properties of *Univ* 174
9.5 Proof for Part (2) 177
9.5.1 The system *Xtra*. 177
9.5.2 The refinement from *Xtra* to *Univ* 178
9.5.3 The inclusions 183
9.6 Proof for Part (3) 184
9.7 Lemmas 184
9.8 Inside *Univ* 189

Chapter 10
Lifting the Mondex Purse **192**
10.1 The Mondex Purse Development 192
10.2 Refinement and Retrenchment in Z 194
10.3 The Retrenchment Step 195
10.4 Lifting and the Tower 201
10.5 Conclusion 204
10.6 Other Retrenchment Opportunities 205

Chapter 11
Conclusion **206**
11.1 Summary 206
11.2 Conclusions and Further Research 207

Appendix A
Postjoin Composition Proofs **210**
A.1 Composition Proofs 210
A.2 Lemmas 222

Appendix B
Prejoin Composition Proofs **238**
B.1 Composition Proofs 238
B.2 Lemmas 249

Bibliography **264**

Abstract

Refinement is one of the cornerstones in formal methods for the incremental development of specifications and the implementation of specifications to code. It is a correctness preserving transformation such that specifications related by refinement are guaranteed to share certain properties. Retrenchment is a liberalised form of refinement proposed as a mechanism that can capture the relationship between systems beyond the reach of the latter. Although with retrenchment we lose the guarantee refinement provides, we benefit by having a more flexible relation able to describe development steps not expressible under refinement.

One way to gain from the advantages that each technique has to offer is to combine retrenchment and refinement steps in specific ways, in order to provide mechanisms that enable the direct construction of new systems, out of systems (related by retrenchment and refinement) that already exist. For example, one configuration we present combines retrenchment and refinement in such a way that given a previously constructed refinement from specification to code, and a modification of the specification expressed as a retrenchment, we can directly generate a new version of the program incorporating the changes introduced via the retrenchment. The need to carry out a fresh refinement of the new specification is thus avoided.

In this thesis we present four different combinations of retrenchments and refinements and show how the systematic application of these combinations is encapsulated in a framework we call the Tower Pattern. We also describe the use of one of the combinations in work to extend the scope of the Mondex Purse development.

Declaration

No portion of the work referred to in this thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning.

Copyright

Copyright in text of this thesis rests with the Author. Copies (by any process) either in full, or of extracts, may be made **only** in accordance with instructions given by the Author and lodged in the John Rylands University Library of Manchester. Details may be obtained from the Librarian. This page must form part of any such copies made. Further copies (by any process) of copies made in accordance with such instructions may not be made without the permission (in writing) of the Author.

The ownership of any intellectual property rights which may be described in this thesis is vested in the University of Manchester, subject to any prior agreement to the contrary, and may not be made available for use by third parties without permission of the University, which will prescribe the terms and conditions of any such agreement.

Further information on the conditions under which disclosures and exploitation may take place is available from the head of the School of Computer Science.

Acknowledgements

My heartfelt gratitude to my supervisor Richard Banach for his guidance, encouragement and support as the work in this thesis took shape. My thanks also to the School of Computer Science, University of Manchester, who provided funding in the form of an Atlas Scholarship.

I thank all my family, friends and members of the retrenchment group for their support over the last few years. In particular, I am grateful to my mother and brother for their unfailing love and belief in me. I would also like to express my love and gratitude to my late father, Antoni, for all his love, and for laying the solid foundations for the road that has led me here. I miss you very much. To Teresa, I express my thanks for your love, encouragement, true friendship, and for being there during those difficult times. Without you this work would not have been completed.

To You who made this possible.

Chapter 1

Introduction

In today's world, computing devices are ubiquitous. They are indispensable in commerce, in industry, in science and engineering, in medicine, in defence. The failure of a system to operate properly can mean anything from a minor inconvenience to a major catastrophe. The power blackout which occurred in the north-eastern United States and Canada in August 2003, affected approximately 50 million people and resulted in an estimated financial loss of six billion U. S. dollars. A software bug in General Electric's Energy Management XA/21 system left operators unaware of a problem with the electricity supply. Had immediate action been taken, the widespread collapse of the power grid would most likely have been prevented [Pou04]. Therac-25, a computer controlled radiation therapy machine, resulted in the deaths of several cancer patients between June 1985 and January 1987. The fatalities were due to overdoses of radiation resulting from a race condition between concurrent tasks in the Therac-25 software [LT93].

The growing use of software in high consequence applications, demands development techniques that can ensure the production of more reliable, higher quality systems. The principal approach advocated to address these aims is the use of formal methods: the application of mathematical techniques to the specification, development and verification of software and hardware systems. A large array of formal specification languages have been proposed. All provide a mathematical notation which enables an unambiguous specification of desired behaviour to be given. Some are general purpose whereas others have been developed for specific application domains. One way to categorize specification languages is by whether they are property- or model-based (see e.g. [Bjø05]). The former can be used to define system behaviour indirectly by stating a set of properties the system

must satisfy. The latter define behaviour by constructing an explicit model of the system. When the model includes a state it is often described as a state-based specification. Such specifications also consist of a set of transitions which describe the permissible changes to the state. In this thesis we only consider model-oriented state-based specifications of sequential systems.

Refinement is one of the cornerstones in the formal methods armoury both for the construction of specifications and the implementation of specifications to code. A development proceeds stepwise, with each step resulting in a model which incorporates a greater level of detail and is a refinement of its precursor. Because refinement is a correctness preserving transformation, this guarantees that the behaviour of each model in a development is consistent with the one before. The end result is that properties are preserved along a development chain and thus for example, the behaviour defined in a specification will hold in the implemented code. Typical development steps involve either data or operation refinement. The former is concerned with replacing high-level data structures by more low-level ones, introducing implementable data types at some stage if the end result is to be at the level of code. The latter involves introducing or modifying algorithmic structure.

In recent times, refinement has been successfully applied in a number of industrial projects. One example is the Mondex Electronic Cash System [SCW98, SCW00], which is a smartcard based electronic purse. Its unique security architecture permits payments from person-to-person using a personal wallet device or telephone line, without the need for authorisation. Refinement was used to show that the security properties of the system captured in an easily comprehensible abstract model were preserved in a formal concrete model of the product. Another important example is the MÉTÉOR project [BBFM99, BDM00]. This used refinement to develop the distributed control system for automatic driverless trains on the new Météor line of the Paris metro, opened in October 1998. During testing of the control system, which consisted of over 80,000 lines of code, no bugs were discovered. A true testament to the power of the refinement mechanism. We also cite the Multos Operating System, a high-security multi-application operating system for smartcards [SC00, Ste01].

Such successes notwithstanding, there are many situations where refinement struggles or is unable to make a contribution. The most often cited examples involve the transformation of models using continuous and infinite types to ones using the finite and discrete types implementable on a computer. Let us consider a simple example, the refinement of a model using an unbounded buffer to one in which the buffer is bounded. To indicate the relative position of models in a development the terms abstract and concrete are often employed. Given two models, the one that occurs first in a development is commonly referred to as abstract, the other as concrete. Forward simulation, a standard method used to show that a concrete model refines an abstract one, includes demonstrating that whenever the concrete system makes a step, the abstract system must have a step that simulates it. For the boundary case, i.e. when the concrete buffer is full, whatever the concrete system does it cannot add another item to the buffer. Since the abstract system readily adds another item, the abstract system will not simulate the concrete, thus breaking the simulation rule. Our development step, which introduces implementation concerns regarding resource constraints, cannot be expressed as a refinement.

The inability of refinement to describe the transformation from continuous and/or infinite types to finite and/or discrete ones motivated Banach and Poppleton to propose a liberalisation of refinement, which they christened retrenchment [BP98]. Its aim is to capture those development steps beyond the reach of the refinement mechanism. Retrenchment achieves this by weakening the refinement simulation rules. With retrenchment, concrete steps are allowed do something different from their corresponding abstract counterparts. Thus returning to our example, the concrete system can refuse to add another item when the buffer is full and just signal an error, while the abstract buffer goes on and accepts a further item.

By modifying the simulation rules we lose the guarantee refinement offers to preserve correctness across a development step. But we benefit by having a more flexible mechanism able to bring in steps hitherto outside formal control. However, this flexibility brings with it responsibilities for a developer, who must ensure deviation from previously asserted behaviour is acceptable. As we shall see, retrenchment provides the means to explicitly specify which concrete steps simulate steps in the abstract model and which ones

approximate abstract behaviour and thus to detail precisely how a concrete model differs for its abstract counterpart.

Banach and Poppleton's intention was not to supplant refinement with retrenchment; rather the intention was for both to be used together in system development, and so, to gain from the advantages which each of the techniques has to offer. A particular approach that achieves this involves combining retrenchment and refinement steps in specific ways, in order to provide mechanisms that enable the direct construction of new systems with particular properties, out of the systems that already exist.

In this thesis we consider four different combinations of retrenchments and refinements: the *lifting*, *lowering*, *postjoin* and *prejoin* constructions shown in Figures 1.1 and 1.2.

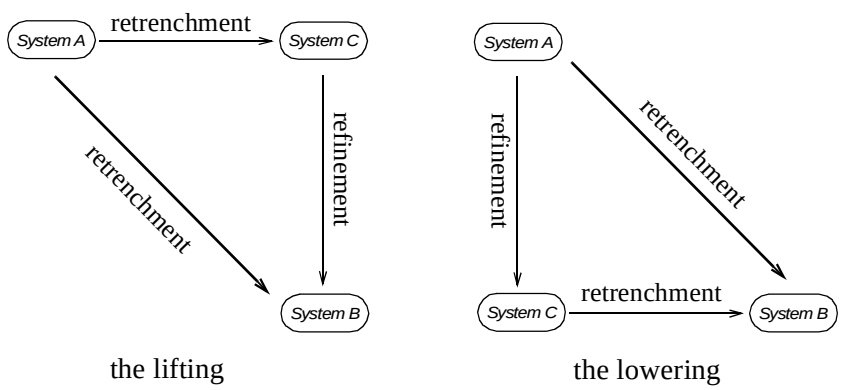


Figure 1.1: The Lifting and Lowering Constructions.

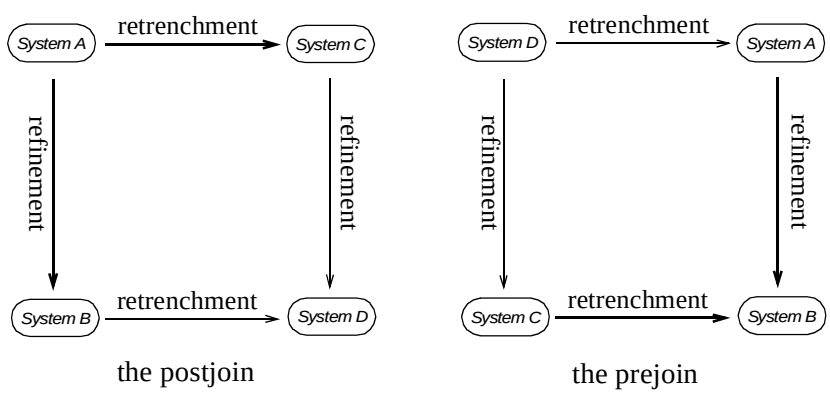


Figure 1.2: The Postjoin and Prejoin Constructions.

Each of these constructions can be used to obtain new systems with specific properties. For example, the lifting takes an existing retrenchment (the hypotenuse of the triangle) and builds a new system (*System C*) that expresses the changes introduced by the retrenchment in terms of the retrenched system (*System A*); we say we lift the constraints introduced by the retrenchment to the level of the retrenched system. An application of the lifting is the generation of a new specification (*System C*) from an original (*System A*) that incorporates the changes introduced by retrenchment during a development to some end product (*System B*).

In the case of the prejoin an existing retrenchment and refinement to the same system (the bottom and right sides of the square) are combined by forming a new retrenchment and refinement (the top and left sides of the square) from a new system (*System D*), that identifies corresponding steps in the original refined and retrenched systems (*System*s *A* and *C*). Given a previously constructed refinement from specification to code, an application of the prejoin is the generation of a new specification that incorporates the change from new to old program captured by the given retrenchment. We shall describe all four constructions in great detail in later chapters. We shall also show that the application of these constructions is encapsulated in a framework we call the *Tower Pattern*, which can be regarded as a systematic procedure for applying particular combinations of retrenchments and refinements.

The principal objective of the work presented is to establish that retrenchments and refinements can be combined in the specific ways we introduced above, giving new systems with particular properties. We achieve our goal by framing each combination of a retrenchment and a refinement as a theorem, which we then proceed to prove. We are successful in demonstrating that the configurations we have described can be constructed. We also underpin the value of our constructions by outlining how the lifting result has been used in work to extend the formal development of the Mondex Electronic Purse we mentioned earlier.

The results we obtain make a contribution to the development of retrenchment in a number of ways. First, they encourage its use by showing that retrenchment can be used in concert with refinement in system development: that the two techniques are not at odds with one another. Second, they open up new pathways for system development, enabling

the direct construction of new systems. Third, they make a significant first step to a complete algebraic theory of the integration of retrenchment and refinement.

The remainder of this thesis is organised as follows.

Chapter 2 introduces the theory of refinement by simulation. We outline the derivation of the particular form of simulation we use, which we call I/O-filtered refinement, and discuss related research. Next, we set up the transition system framework in which we present all our results. A brief summary of reasons for the need to liberalise refinement follows. We end with a simple running example: a desired development step that cannot be captured by the refinement mechanism.

Chapter 3 describes the retrenchment, in both primitive and output forms. We briefly justify the shape of the retrenchment rules. The development step example from the previous chapter is captured successfully using retrenchment. Last, we describe some other approaches to liberalising refinement.

Chapter 4 begins by looking at the composition of retrenchment and refinement steps. We show that such compositions can be defined as retrenchments. This is the first step in the theory of the integration of retrenchment and refinement. Next, we describe the *lifting*, *lowering*, *postjoin* and *prejoin* structures in more detail and explain how they can be used at a practical level. We conclude by introducing the *Tower Pattern*.

Chapter 5 presents our first construction uniting a retrenchment and a refinement, the *lifting*. We express the problem as a theorem and give a detailed proof. The new system created by the lifting is illustrated using our running example.

Chapter 6 details the *lowering* construction. Once again we cast the particular arrangement of a retrenchment and refinement that we want as a theorem. A full proof is given and the result discussed using the running example.

Chapter 7 is preparation for the more demanding material on the remaining postjoin and prejoin constructions.

Chapters 8 and 9 present the *postjoin* and *prejoin* respectively. The structure of these chapters follows that for the other constructions: we state the theorem, give a comprehensive proof and discuss the result using the running example.

Chapter 10 provides a sketch of how retrenchment has been used to broaden the scope of the Mondex Purse development. Following a summary of Mondex, both refinement and retrenchment are presented in Z, the notation used for the development. The use of retrenchment to remove the inexactitude present in the original development with respect to modelling transaction sequence numbers is described. We then show how the lifting construction, via the Tower Pattern schema, was used (in part) to generate a specification of the model constructed in the retrenchment step. The chapter ends with a brief summary of other modelling imprecisions or difficulties in Mondex that have been eliminated by using retrenchment.

Chapter 11 reviews the contribution made by the work in this thesis. Directions in which the research can be extended are also discussed.

Appendices A and B give the composition proofs for the post- and prejoin.

Chapter 2

Refinement by Simulation

Wirth described stepwise refinement as a process of program development in which a design is decomposed in successively greater detail until fully expressed in some implementation language [Wir71]. The use of the stepwise approach in a formal framework has its origins in the work of Hoare [Hoa71] and Dijkstra [Dij75]. Classic formalisations of stepwise refinement are the refinement calculi of Back [Bac80, Bac88, BvW98], Morgan [MR87, MGR93, Mor94] and Morris [Mor87, Mor89], and the simulation technique in methods like VDM (Vienna Development Method) [Jon90, FL98] and B [Abr96, Sch01a], and the Z notation [Spi92, BSC94, WD96]. The central point in each is that a refinement step guarantees that those properties which it preserves will hold in a new model if they hold in its precursor. Refinement calculi employ a calculational style of program development. A transformation law is applied at each step to produce a new model. The result is automatically a refinement of its predecessor (assuming any associated proof obligations can be discharged). The refinement methods use a posit-and-prove style of development. A developer writes down a new model and then uses rules to verify that it is a refinement of its predecessor. See [LW92] for a gentle introduction to refinement methods and calculi.

We use the simulation form of refinement in our work on the integration of the latter with retrenchment. This is a natural choice since the retrenchment technique arises from a modification of the refinement simulation rules. In this chapter we give a compressed account of the derivation of the standard simulation rules and then introduce the particular form of simulation, called I/O-filtered refinement, which we will use. We conclude with

some reasons why retrenchment is needed, and give a simple example which we shall later use to illustrate our results.

2.1 Notation

In this section we clarify some of the notation we use. Let V, W, X, Y, Z, A and B be sets where $A \subseteq X$ and $B \subseteq Y$.

The disjoint union of X and Y is

$$X \uplus Y = (X \times \{0\}) \cup (Y \times \{1\}).$$

For binary relations $R \subseteq X \times Y$, $S \subseteq Y \times Z$ and $T \subseteq V \times W$ we define the following.

A relation R is an injection if

$$(x, z) \in R \wedge (y, z) \in R \Rightarrow x = y.$$

The inverse of R is

$$R^{-1} = \{ (y, x) \mid (x, y) \in R \} .$$

The domain of R is

$$\mathrm{dom}(R) = \{ x \mid (\exists\, y \bullet (x, y) \in R) \} .$$

The range of R is

$$\mathrm{ran}(R) = \{ y \mid (\exists\, x \bullet (x, y) \in R) \} .$$

The sequential composition of R and S is

$$R ⨾ S = \{ (x, z) \mid (\exists\, y \bullet (x, y) \in R \wedge (y, z) \in S) \} .$$

The parallel composition of S and T is

$$S \parallel T = \{ ((y, v), (z, w)) \mid (y, z) \in S \wedge (v, w) \in T) \} .$$

The domain restriction of R to A is

$$A \lhd R = \{ (x, y) \mid (x, y) \in R \wedge x \in A \} .$$

The set of all finite sequences of objects from X is

$$\mathrm{seq}(X) = \{ x \mid x \in \mathbb{N} \rightarrowtail X \wedge (\exists\, n \bullet n \in \mathbb{N} \wedge \mathrm{dom}(R) = 1 \,..\, n) \} .$$

2.2 Simulation

2.2.1 The He, Hoare and Sanders model

Using a relational framework, He, Hoare and Sanders put forward the notion of simulation as a proof method for data refinement of state-based systems [HHS86, HHS87]. They considered the question of when one data type was the refinement of another. We summarize the salient points. A data type $\mathcal{X}$ is defined as the quadruple (X, xi, XOp, xf), where

- X is the space of values (or states) ;
- $xi \subseteq G \times X$ is an initialisation ;
- XOp is the family of operations $\{xo_i\}_{i \in I}$, indexed by $i \in I$, with $xo_i \subseteq X \times X$;
- $xf \subseteq X \times G$ is a finalisation .

The relations xi, $\{xo_i\}_{i \in I}$ and xf are all total.

A program $P(\mathcal{X}) \subseteq G \times G$, which uses data type $\mathcal{X}$, is a sequence of operations[1], represented by relations, starting with the initialisation xi, followed by a finite number of operations xo_i, and ending with the finalisation xf. For example,

$$P(\mathcal{X}) = xi \fatsemi xo_1 \fatsemi xo_3 \fatsemi xo_2 \fatsemi xf \,.$$

Two data types are said to be conformal if they share the same indexing set and their global spaces are equal. Let $\mathcal{A} = (A, ai, AOp, af)$ and $C = (C, ci, COp, cf)$, which we shall refer to as abstract and concrete respectively, be conformal data types. Then $\mathcal{A}$ is refined by C, denoted $\mathcal{A} \sqsubseteq C$, if and only if for all pairs of programs $P(\mathcal{A})$ and $P(C)$,

$$P(C) \subseteq P(\mathcal{A}) \,. \tag{2.1}$$

Figure 2.1 depicts the refinement relationship between $P(\mathcal{A})$ and $P(C)$. The definition of data refinement articulates the fundamental notion of substitutivity on which refinement is based. Quoting from [DB01, page 47],

1. This is a simplification of the material presented in [HHS86], but is sufficient for our purposes. The full theory is richer, providing a number of constructs for combining the primitive operations of the data type.

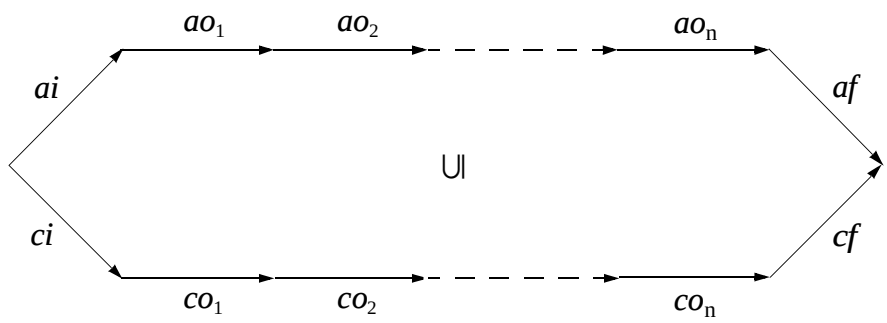


Figure 2.1: Data refinement

> **Principle of Substitutivity:** it is acceptable to replace one program by another, *provided* it is impossible for a user of the programs to observe that the substitution has taken place.

Since only pairs of global states are observable, (2.1) satisfies this principle.

Set inclusion of the relations corresponding to programs is a preorder, so it is reflexive and transitive. Thus, by transitivity, if $\mathcal{D}_1 \sqsubseteq \mathcal{D}_2 \sqsubseteq ... \sqsubseteq \mathcal{D}_n$, then $\mathcal{D}_1 \sqsubseteq \mathcal{D}_n$. This key property permits a specification to be developed stepwise, with the gradual introduction of detail. Adding detail usually involves the reduction of nondeterminism as design choices are resolved. Set inclusion thus only guarantees to preserve functional properties across a development step. Non-functional properties, such as security, are not preserved by refinement; see [Jac92, CSC05].

Establishing $\mathcal{A} \sqsubseteq C$ entails demonstrating that inclusion holds for all possible pairs of programs. This is clearly not feasible for all but the most simple cases. The approach used to obtain a practicable method is to define a relation between the state spaces of the abstract and concrete types, called a simulation or retrieve relation and marked τ in Figure 2.2. The problem is now reduced to showing that the paths around the three different shapes in the figure, the initial and final triangles and the square, weakly commute. Then by induction, for a finite sequence of operations, $P(C) \subseteq P(\mathcal{A})$ [dRE98, DB01]. One choice for weak commutativity of the square is to consider the two paths from top-left to

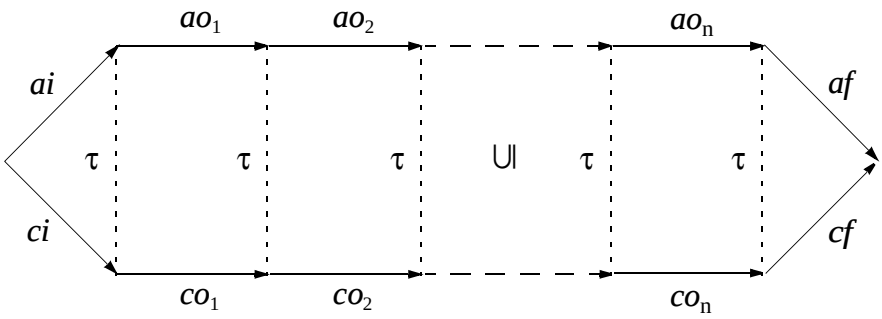


Figure 2.2: Data refinement using simulations

bottom-right, i.e. $\tau \fatsemi co_i$ and $ao_i \fatsemi t$. Together with appropriate choices for the initial and final triangles this gives the forward simulation rules.

If $\mathcal{A}$ and C share the same indexing set, and $r \subseteq A \times C$, then r is a **forward simulation** if

$$ci \subseteq ai \fatsemi r$$
$$r \fatsemi cf \subseteq af$$
$$r \fatsemi co_i \subseteq ao_i \fatsemi r\ , \quad \text{for each index } i.$$

Alternatively, we have the two paths from bottom-left to top-right. This results in the following backward simulation rules.

If $\mathcal{A}$ and C share the same indexing set, and $s \subseteq C \times A$, then s is a **backward simulation** if

$$ci \fatsemi s \subseteq ai$$
$$cf \subseteq s \fatsemi af$$
$$co_i \fatsemi s \subseteq s \fatsemi ao_i\ , \quad \text{for each index } i.$$

We will refer to each of the above as the HHS rules. We note that [HHS86] uses the terms downward and upward simulation for forward and backward simulation respectively.

Hoare, He and Sanders showed that as a method for proving data refinement, the forward and backward rules are sound and jointly complete. Thus the forward and backward simulation rules on their own are unable to prove correct certain valid refinements. For ex-

ample, refinements where the resolution of nondeterminism is postponed in the concrete program cannot be shown to be correct using the forward rules. For details see both [DB01] and [dRE98].

2.2.2 Admitting partial operations

The HHS rules require all operations to be total. Woodcock and Davies [WD96] show how partial operations can be accommodated. The approach involves *totalising* operations by defining behaviour for states not in the domain. To totalise a relation $xo \subseteq X \times X$, X is augmented to $X^{\perp}$ by adding the distinguished element $\perp$, which represents undefinedness. Elements in $(X^{\perp} - (\mathsf{dom}\, xo))$ are then linked to every element in $X^{\perp}$. The lifted totalised relation $\dot{xo}$ is therefore

$$\dot{xo} = xo \cup \{ (x, y) \in X^{\perp} \times X^{\perp} \mid x \notin \mathsf{dom}(xo) \} , \tag{2.2}$$

where $X^{\perp} = X \cup \{\perp\}$. The interpretation given to this form of totalisation is that anything may happen when an operation is applied to a value outside its original domain. This is known as the non-blocking or contract approach. An alternative is the blocking or behavioural approach, in which the application of an operation to values outside its domain is prohibited; see [BDW98] for a derivation of the simulation rules using the latter form. [DB01] also discusses both these approaches to totalisation.

It is not necessary to totalise the retrieve relation, but it must be extended so that $\perp$ retrieves to all elements, in order to preserve undefinedness. The resulting *lifted* relation $\overset{\circ}{\tau} \subseteq X^{\perp} \times Y^{\perp}$ is

$$\overset{\circ}{\tau} = \tau \cup (\{\perp\} \times Y^{\perp}) .$$

The totalised and lifted relations are now substituted into the HHS rules and after some manipulation we obtain rules expressed in terms of just partial operations and the unlifted retrieve relation. We reproduce the forward simulation rules below.

WD Forward Simulation Rules

Initialisation	$ci \subseteq ai \fatsemi r$
Finalisation	$r \fatsemi cf \subseteq af$
Applicability	$\mathrm{ran}(\mathrm{dom}(ao_i) \lhd r) \subseteq \mathrm{dom}(co_i)$, for each index i ,
Correctness	$\mathrm{dom}(ao_i) \lhd r \fatsemi co_i \subseteq ao_i \fatsemi r$, for each index i .

2.2.3 Operations with input and output

The operations in the WD rules have no I/O component themselves. The only input and output is to the program as a whole via before and after state pairs from G. Woodcock and Davies show how the rules can be extended to operations with their own input and output components. However, their treatment requires all abstract and concrete operations to have the same input space and similarly so for outputs, i.e. refinement of inputs and outputs from abstract to concrete operations is not permitted.

A more general derivation is given by Cooper, Stepney and Woodcock [CSW02], whose approach develops that in [WD96] to allow abstract operations to have input and output spaces that are different from those of the concrete operations. A program is a relation mapping sequences of inputs to sequences of outputs. Initialisation involves copying the sequence of ready-to-be-consumed inputs and an empty sequence of outputs to the local state. Each operation in the program then consumes the value at the head of the input sequence and appends the value it produces to the output sequence. Finalisation copies the output and now empty input sequences back to the global state.

In [CSW02] G is referred to as the global world. It is defined to consist of a global state space GS, a sequence of global inputs with elements from GI, and a sequence of global outputs with elements from GO. Hence,

$$G = GS \times (\mathrm{seq}\ GI \times \mathrm{seq}\ GO) .$$

The abstract and concrete worlds have a parallel structure.

$$A = AS \times (\mathrm{seq}\ AI \times \mathrm{seq}\ AO) ,$$
$$C = CS \times (\mathrm{seq}\ CI \times \mathrm{seq}\ CO) .$$

In addition to a retrieve relation, r, between abstract and concrete states, we also need an input retrieve relation i between abstract and concrete inputs, and output retrieve relation o between abstract and concrete outputs respectively, where

$$r \subseteq AS \times CS ,$$
$$i \subseteq AI \times CI ,$$
$$o \subseteq AO \times CO .$$

Henceforth we will refer to input retrieve relations as just input relations and similarly so for the output retrieve relations. We also need to define the relations between the global and abstract or concrete states, inputs and outputs as follows.

$$gcs \subseteq GS \times CS ,$$
$$gas \subseteq GS \times AS ,$$
$$gci \subseteq GI \times CI ,$$
$$gai \subseteq GI \times AI ,$$
$$gco \subseteq GO \times CO ,$$
$$gao \subseteq GO \times AO .$$

The abstract and concrete operations are defined as the relations α_i and γ_i, which map state-and-input to state-and-output. Thus

$$\alpha_i \subseteq (AS \times AI) \times (AS \times AO) ,$$
$$\gamma_i \subseteq (CS \times CI) \times (CS \times CO) .$$

The relations in the WD rules are now defined in terms of the relations we have given above. The definitions are then substituted into the WD rules to obtain the CSW rules. We refer the reader to the cited paper for the technical details. The CSW rules for forward simulation are given below.

CSW Forward Simulation Rules

Initialisation (*state*)	$cis \subseteq ais \fatsemi r$
Initialisation (*input*)	$gci \subseteq gai \fatsemi i$
Finalisation (*state*)	$r \fatsemi gcs^{-1} \subseteq gas^{-1}$
Finalisation (*output*)	$o \fatsemi gco^{-1} \subseteq gao^{-1}$

Applicability	$\mathsf{ran}(\mathsf{dom}(\alpha_i) \lhd (r \parallel i)) \subseteq \mathsf{dom}(\gamma_i)$, for each index i ,
Correctness	$(\mathsf{dom}(\alpha_i) \lhd (r \parallel i)) \fatsemi \gamma_i \subseteq \alpha_i \fatsemi (r \parallel o)$, for each index i .

The rules are in terms of the individual input and outputs of the operations and not in terms of sequences of inputs and outputs. The state initialisations *ais* and *cis* are defined to ignore their arguments, mapping all global states to a number of local initial states:

$$cis = GS \times \{ cs \in CS \mid \text{a constraint on } cs \} ,$$
$$ais = GS \times \{ as \in AS \mid \text{a constraint on } as \} .$$

Notice that there is now a state finalisation rule. This arises because a choice was made to preserve the last state as well as the sequence of accumulated outputs on finalisation.

The relation $(r \parallel i)$ is the parallel composition of its component relations. Recall that the operations α_i and γ_i map pairs of the form (*state*, *input*) to (*state*, *output*). Thus $(r \parallel i)$ is a composite retrieve relation associating corresponding abstract and concrete (*state*, *input*) pairs. Similarly $(r \parallel o)$ associates corresponding abstract and concrete (*state*, *output*) pairs.

2.2.4 I/O-filtered refinements

For each data type all operations in the CSW model have inputs and outputs with the same space respectively. As we shall see in the next chapter, this is not the case with the rules for retrenchment. To facilitate the integration of retrenchment with refinement, we therefore make a minor extension to the CSW model and allow each operation to have different input and output spaces.

Let operation α_i have input space AI_i and output space AO_i. *AI* and *AO* are then the disjoint union of the individual spaces as follows.

$$AI = \coprod_{\mathrm{i}} AI_\mathrm{i} ,$$

$$AO = \coprod_{\mathrm{i}} AO_\mathrm{i} .$$

CI, *CO*, *GI* and *GO* are defined in similar fashion. The input retrieve relation *i* now becomes the indexed family of relations,

$$i = (i_{\mathrm{i}} \subseteq AI_{\mathrm{i}} \times CI_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} .$$

Similarly,

$$gai = (gai_{\mathrm{i}} \subseteq GI_{\mathrm{i}} \times AI_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} ,$$
$$gao = (gao_{\mathrm{i}} \subseteq GI_{\mathrm{i}} \times AO_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} ,$$
$$o = (o_{\mathrm{i}} \subseteq AO_{\mathrm{i}} \times CO_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} ,$$
$$gci = (gci_{\mathrm{i}} \subseteq GI_{\mathrm{i}} \times CI_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} ,$$
$$gco = (gco_{\mathrm{i}} \subseteq GI_{\mathrm{i}} \times CO_{\mathrm{i}})_{\mathrm{i} \in \mathrm{I}} .$$

Finally, the operations become

$$\alpha_{\mathrm{i}} \subseteq (AS \times AI_{\mathrm{i}}) \times (AS \times AO_{\mathrm{i}}) ,$$
$$\gamma_{\mathrm{i}} \subseteq (CS \times CI_{\mathrm{i}}) \times (CS \times CO_{\mathrm{i}}) .$$

It is relatively easy to see that substituting these changes into the CSW rules results in separate input initialisation and output finalisation rules for each index i. The resulting forward simulation rules for I/O-filtered refinement are given below.

I/O-Filtered Refinement Forward Simulation Rules

Initialisation (*state*)	$cis \subseteq ais \fatsemi r$
Initialisation (*input*)	$gci_{\mathrm{i}} \subseteq gai_{\mathrm{i}} \fatsemi i_{\mathrm{i}}$, for each index i ,
Finalisation (*output*)	$o_{\mathrm{i}} \fatsemi gco_{\mathrm{i}}^{-1} \subseteq gao_{\mathrm{i}}^{-1}$, for each index i ,
Applicability	$\mathsf{ran}(\mathsf{dom}(\alpha_i) \lhd (r \parallel i_{\mathrm{i}})) \subseteq \mathsf{dom}(\gamma_i)$, for each index i ,
Correctness	$(\mathsf{dom}(\alpha_i) \lhd (r \parallel i_{\mathrm{i}})) \fatsemi \gamma_i \subseteq \alpha_i \fatsemi (r \parallel o_{\mathrm{i}})$, for each index i .

2.2.5 Related work

In an approach very similar to [CSW02], Derrick and Boiten also generalise the WD rules to permit I/O refinement [BD98, DB01]. In their model there is no explicit global state. The only components of the global world are the input and output sequences.

In the derivation of the WD rules, partial operations are made total through a process of lifted totalisation. A thorough investigation of this approach to totalisation is undertaken in the work of Deutsch, Henson and Reeves [DHR02, DHR03a, DHR03b, DH03a,

DH03b], for both operation refinement (the degenerate case of data refinement where the simulation relations are just identities) and data refinement by forward and backward simulation. The authors give a proof theoretic characterisation of refinement closely related to that of Spivey in [Spi92]. It is based on two properties expected in refinement. First, a refinement step may involve the reduction of nondeterminism, i.e. postconditions may not weaken. Second, a refinement step may involve an expansion of the domain of definition, i.e. preconditions may not strengthen. They take their proof theoretic definition as the fundamental characterisation. Deutsch and Henson show that for data refinement by forward simulation, totalisation of operations without lifting admits cases where preconditions can be strengthened in a refinement step. Therefore, given that lifting is necessary, must $\perp$ be mapped to all elements, giving non-strict lifting, as in (2.2), or can $\perp$ be mapped to just itself, giving strict lifting? Deutsch and Henson show that in fact these two choices are equivalent. Furthermore, in the case of the simulation relation it is necessary to use non-strict lifting, as was done by Woodcock and Davies, since strict lifting prevents the weakening of preconditions in certain situations.

In the monograph by de Roever and Engelhardt [dRE98], a theory for partial relations is developed in which the relations denoting operations are not made total and no special value is introduced to represent undefinedness. Refinement is still defined as relational inclusion. Forward and backward simulation rules for this partial correctness model are shown to be sound and jointly complete. De Roever and Engelhardt name the forward and backward simulations L- and L^{-1}-simulations. The names reflect the shapes of the paths around the squares we saw in Figure 2.2. There are in fact two other choices for paths around the square. The pair $t \fatsemi co_i \fatsemi t^{-1}$ and ao_i giving what the authors call U-simulation, and the pair co_i and $t^{-1} \fatsemi ao_i \fatsemi t$ giving U^{-1}-simulation. However, as de Roever and Engelhardt show, when the U- or U^{-1}-rule holds for two adjacent squares, the same rule does not necessarily hold for the resulting concatenated square, which blocks an inductive proof. This is not the case for forward and backward simulation.

In this partial correctness model the empty relation, which is interpreted as a nonterminating program, is a valid implementation of every other specification or program. To overcome this drawback, de Roever and Engelhardt extend their theory to a total correctness framework. They introduce the special value $\perp$ and model nontermination from some

state σ by mapping it to all states as well as $\perp$. The resulting model treats both definite and possible nontermination as the same, and termination now refines nontermination. They show L-simulation is sound and that under certain restrictions L- and L^{-1}-simulation are jointly complete in this total correctness framework.

The aim of the monograph is to compare several data refinement methods including Z, VDM and data refinement in Back's calculus with proof by simulation. To achieve this de Roever and Engelhardt represent operations in these methods as Hoare triples, $\{\pi_1\}\ S\ \{\pi_2\}$ [Hoa69]. Such a triple means that if precondition π_1 holds for some initial state σ, and if S terminates for initial state σ in final state σ', then π_2 holds for σ'. They also characterize L-, L^{-1}-, U and U^{-1}-simulation as single Hoare triples. Having set up this framework de Roever and Engelhardt are able to show that Z, VDM and data refinement in Back's refinement calculus are all applications of L-simulation.

A paper by Boiten and de Roever also describes theories of refinement by simulation, focusing on the differences that arise in modelling operations by partial and total relations and the introduction of the additional element $\perp$ to model nontermination and deadlock [BdR03].

In the simulation methods we have described above, there is a one-to-one mapping between abstract and concrete operations, with each abstract operation being refined by a corresponding concrete one. With their notion of non-atomic refinement Derrick and Boiten generalise this requirement for conformality and now allow one abstract operation to be refined by a sequence of concrete operations [DB99, DB01]. This permits a change in granularity as a specification is developed. Schellhorn's work on generalised forward simulation also breaks the requirement of atomicity [Sch01b]. Sequences of abstract steps are related to sequences of concrete steps in such a way that the retrieve relation is preserved by the two sequences.

2.3 Transition System Framework

We present all our results using a simple transition framework. We will need to consider relationships between an abstract system and a concrete one, which we will call *Abs* and *Conc* respectively. Each system will be described by a state space and a set of operation

names. Individual operations will be defined by a transition or step relation, and will have their own input and output spaces.

For *Abs* the state space will be denoted by U with typical element u. Ops_A will be the set of operation names with Op_A designating a typical operation. For each Op_A the input and output spaces will be I_{Op_A} and O_{Op_A} with i and o representing typical elements respectively. We will dispense with subscripts for i and o, since it will be clear from the context as to the Op_A to which they belong. A typical Op_A transition will be depicted by u -(i, Op_A, o)-› u', where u and u' are the before and after states, and i and o are the input and output values. The set of such steps will form the transition or step relation $stp_{Op_A}(u, i, u', o)$. We write $trm_{Op_A}(u, i)$ for the domain of stp_{Op_A}. $Init_A(u')$ will represent the initialisation operation and will set the state to some initial value u', ignoring the value of the initial global state.

The set up for the concrete system *Conc* parallels that for *Abs*. The state space will be W with typical element w. Inputs and outputs are $k \in \mathsf{K}$ and $q \in \mathsf{Q}$ respectively. The operation names are $Op_C \in \mathsf{Ops}_C$, and conformality requires $\mathsf{Ops}_A = \mathsf{Ops}_C$. For each Op_C the transition relation is $stp_{Op_C}(w, k, w', q)$, with typical transition w -(k, Op_C, q)-› w'. The domain is $trm_{Op_C}(w, k)$. The initialisation operation is $Init_C(w')$.

For each operation Op, we will denote the input and output spaces of the global world by H_{Op} and N_{Op} with typical elements h and n respectively. The relations mapping global inputs to abstract and concrete inputs will be $InitIn_{Op_A}(h, i)$ and $InitIn_{Op_C}(h, k)$. Relations mapping abstract and concrete outputs to the global world will be $FinOut_{Op_A}(o, n)$ and $FinOut_{Op_C}(q, n)$.

We will denote the retrieve relation between abstract and concrete states by $G(u, w)$. For each Op we denote the input and output relations between abstract and concrete inputs and outputs by $In_{Op}(i, k)$ and $Out_{Op}(o, q)$ respectively.

We will cast the forward simulation rules in the classical framework of first-order predicate logic and in this context refer to them as the refinement proof obligations (POs). Rewriting the rules for I/O-filtered refinement we obtain the following.

Input Initialisation PO (Inp Init PO)

$$InitIn_{Op_C}(h, k) \Rightarrow (\exists\, i \bullet InitIn_{Op_A}(h, i) \wedge In_{Op}(i, k)) \,. \tag{2.3}$$

State initialisation PO (Init PO)

$$Init_C(w') \Rightarrow (\exists\, u' \bullet Init_A(u') \wedge G(u', w')) \,. \tag{2.4}$$

Output Finalisation PO (Out Fin PO)

$$Out_{Op}(o, q) \wedge FinOut_{Op_C}(q, n) \Rightarrow FinOut_{Op_A}(o, n) \,. \tag{2.5}$$

Applicability PO (App PO)

$$G(u, w) \wedge In_{Op}(i, k) \wedge trm_{Op_A}(u, i) \Rightarrow trm_{Op_C}(w, k) \,. \tag{2.6}$$

Correctness PO (Corr PO)

$$\begin{aligned} &G(u, w) \wedge In_{Op}(i, k) \wedge trm_{Op_A}(u, i) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge G(u', w') \wedge Out_{Op}(o, q)) \,. \end{aligned} \tag{2.7}$$

2.4 The Need to Liberalise Refinement

Refinement guarantees that a concrete system always provides a possible behaviour of its abstract counterpart, thus ensuring the concrete system is observationally indistinguishable from the abstract. In practice, there are many situations where this property is too restrictive. For example, the real world is infinite and continuous whereas the world of the computer is finite and discrete. Transformation from one to the other ultimately necessitates that the concrete model will be an approximation of the abstract, no longer observationally indistinguishable. A refinement relation can often not be established between the two. For developments that begin with physical world models, the applicability of refinement in the migration to the digital, finite world is thus much reduced, forcing large parts of the process to take place outside formal control.

In other situations there may be a requirement not to obscure the functionality of an abstract model with low level implementational details, so as to make it more approachable and/or more amenable to formal analysis. Such postponement of detail may not always be possible under refinement. Alternatively, a customer may not agree to a change necessary to an abstract model in order that a refinement relation can be established to some (in certain aspects fixed) concrete model. The latter situation is one that actually arose during the Mondex Purse development, which we shall meet in the penultimate chapter.

To extend the benefits of a formal approach in all these situations, a more flexible relation is required, able to capture the degree to which a model satisfies the requirements of its precursor. Retrenchment, which we shall present in the next chapter, was designed specifically to fulfil this need.

Below we introduce a simple example, the Number Recycler. Its purpose is not to champion the case for retrenchment, but to provide a vehicle to illustrate the results we present in this thesis, hopefully without obfuscation. Nevertheless, it is characteristic of the kinds of situations retrenchment was designed to address, namely the approximation of abstract behaviour in a concrete model.

2.4.1 The number recycler

The Number Recycler has two operations. The first, *Add*, allows users to add a number to a bin. If the number is already in the bin, it is discarded. A message is generated to indicate whether the number has been added successfully. The second operation, *Rem*, allows an arbitrary number to be removed from the bin. The abstract model *Abs* for the recycler is given below.

$$\mathsf{U} = \mathbb{P}(\mathbb{N}),\ \mathsf{I}_{Add_A} = \mathbb{N},\ \mathsf{O}_{Add_A} = \{\mathsf{OK}, \mathsf{GOT}\},$$
$$\mathsf{I}_{Rem_A} = \varnothing,\ \mathsf{O}_{Rem_A} = \mathbb{N}. \tag{2.8}$$

$$u \text{ -}(i, Add_A, \mathsf{OK})\text{-}\!\rightarrow u \cup \{\, i \,\},\ \text{if } i \notin u\ ,$$
$$u \text{ -}(i, Add_A, \mathsf{GOT})\text{-}\!\rightarrow u,\ \text{if } i \in u\ . \tag{2.9}$$

$$u \uplus \{\, o \,\} \text{ -}(Rem_A, o)\text{-}\!\rightarrow u\ . \tag{2.10}$$

For the next stage of the development, we decide to address the reality that the capacity of the bin is finite. In fact, the bin can store no more than five numbers at once. We will need to generate a suitable message when the bin is full. To move closer towards an implementable data structure, we also decide to model the bin by an injective sequence. Our new specification is given below.

$$\mathsf{W} = \{w \in \mathsf{iseq}(\mathbb{N}) \mid \mathsf{len}(w) \leq 5\},\ \mathsf{K}_{Add_C} = \mathbb{N},\ \mathsf{Q}_{Add_C} = \{\mathsf{OK}, \mathsf{GOT}, \mathsf{FULL}\},$$
$$\mathsf{K}_{Rem_C} = \varnothing,\ \mathsf{Q}_{Rem_C} = \mathbb{N}\ . \tag{2.11}$$

$$w \text{-}(k, Add_C, \mathsf{OK})\text{-}\!\rightarrow w \frown \langle k \rangle, \text{ if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) \leq 4 ,$$
$$w \text{-}(k, Add_C, \mathsf{FULL})\text{-}\!\rightarrow w, \text{ if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) = 5 ,$$
$$w \text{-}(k, Add_C, \mathsf{GOT})\text{-}\!\rightarrow w, \text{ if } k \in \mathsf{ran}(w) . \tag{2.12}$$

$$\langle q \rangle \frown w \text{-}(Rem_A, q)\text{-}\!\rightarrow w . \tag{2.13}$$

It is immediately evident this model cannot be a refinement of *Abs*. When the bin is full there is no concrete step which maintains the same result as the abstract system, which will proceed to add another number to the bin[1]. We therefore cannot express this desired development step as a refinement. Refinement is unable to capture the transformation from infinite to finite data type. We will see in the next chapter how retrenchment effortlessly overcomes this problem.

1. We note that if we try to construct a suitable retrieve relation which will match concrete *Add* boundary steps with abstract steps which add a sixth number, we will run into difficulties when we come to consider the remove operation *Rem*.

Chapter 3

Retrenchment

The strong coupling between systems demanded by refinement means it is often unable to capture steps that occur in the development of many real-world applications. Retrenchment is a more liberal notion whose aim is bring into the formal fold those stages of development which hitherto have fallen beyond the reach of model-based refinement. The concept of retrenchment was introduced in [BP98]. A significant amount of work has taken place since, of which [BP01, BJ02, Ban03, BPJ04] give a good introduction to the topic. A review of the basic concepts and some of the issues explored to date can be found in the retrenchment tutorial [Ban][1].

The following sections introduce retrenchment presenting both primitive and output forms. We also return to the example in the previous chapter and show how retrenchment can successfully relate the systems involved in the desired development step. We conclude with a discussion of other approaches that can be found in the literature which also attempt to address the limitations of refinement.

3.1 From Refinement to Retrenchment

Retrenchment's genesis lies in Banach and Poppleton's unsuccessful attempts to apply refinement to a problem in radiotherapy dose calculation. This work further strengthened the impression that a more flexible and general mechanism was necessary in order to permit developers to relate the models that arise naturally in the engineering of systems with continuous variables. Examination of the limitations of refinement in both continuous

1. See also the retrenchment home page at http://www.cs.man.ac.uk/retrenchment

and discrete domains prompted Banach and Poppleton into considering how they could modify the refinement POs to permit the breaking of the refinement straitjacket in a controlled way. They took the forward simulation rules as a starting point, this being predominant in applications of refinement, and also the form used in the B-Method [Abr96, Sch01a] in which all the initial work on retrenchment was done. The result was a mechanism that used not only the retrieve relation G to link two systems, but had a further two relations per operation, the within and concedes relations, P_{Op} and C_{Op} respectively. P_{Op} occurs as a conjunct in the antecedents of both the termination and operation retrenchment POs, strengthening G in before-states, whereas C_{Op} appears as a disjunct in the consequent of the operation PO, weakening G in after-states. It is the introduction of the concession C_{Op} which most strongly sets retrenchment apart from other extensions to classical refinement that have been proposed in the literature.

3.2 Primitive Retrenchment

Using the transition system framework we introduced in Section 2.3, we now set out the basic form of retrenchment, that of primitive retrenchment. Once again we employ the two systems *Abs* and *Conc* to further progress. In retrenchment we relax the equality between abstract and concrete name spaces and allow the concrete system to include additional operations; thus $\mathsf{Ops}_{\mathrm{A}} \subseteq \mathsf{Ops}_{\mathrm{C}}$. Primitive retrenchment is defined by the three POs (3.1) to (3.3), which give its semantics.

State initialisation PO (Init PO)

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', w')) \;. \tag{3.1}$$

Termination PO (Term PO)

$$G(u, w) \wedge P_{Op}(i, k, u, w) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{C}}}(w, k) \;. \tag{3.2}$$

Operation PO (Op PO)

$$\begin{aligned} &G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_{\mathrm{C}}}(w, k, w', q) \;\Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge (\, G(u', w') \vee C_{Op}(u', w', o, q; i, k, u, w)\,)) \;. \end{aligned} \tag{3.3}$$

Corresponding abstract and concrete states are related by the familiar retrieve relation $G(u, w)$. In addition, for each $Op_{\mathrm{A}} \in \mathsf{Ops}_{\mathrm{A}}$, there is a within relation $P_{Op}(i, k, u, w)$ and

a concedes relation $C_{Op}(u', w', o, q; i, k, u, w)$. Note that (3.2) and (3.3) only hold for operations common to both systems.

The within relation is concerned with both before-states and input values and so enables a change in input signature as well as the movement of components between state and input spaces. This allows, for example, information which formed part of the state at one level, to be remodelled as input at the next. What is more, since the within relation strengthens the retrieve relation in before-states it can be used to restrict the relationship between adjoining levels of abstraction.

The concedes relation is mainly concerned with after-states and output values, but may also involve before-states and inputs for greater flexibility. The use of a semicolon in the syntax is intended to emphasise this view. Thus in the main the concedes relation allows a change of output signature and the interchange of output and state aspects. More importantly, it admits weakening of the retrieve relation in after-states by being a disjunct to it in the operation PO, and it is this aspect in particular which allows the expression of non-refinement like behaviour.

Naturally, justification for the shape of the retrenchment POs has at its heart that the mechanism furnishes the flexibility needed to relate the kinds of models we have already discussed. As noted, P_{Op} enables incompatible parts of abstract and concrete models to be excluded. C_{Op} enables incompatible parts to be included by providing a get out clause in the consequent of the operation PO. On top of this, the structure of (3.3) demands that for every concrete step for which both the retrieve and within relations hold, there must be a corresponding abstract step which either re-establishes the retrieve relation or satisfies the concedes relation. This shape forces us to speak about all concrete steps. The converse, where the abstract step appears in the antecedent and the concrete in the consequent, does not. Since an implementation is derived from the concrete system this provides for a more robust approach. More precisely, for every concrete step a decision has to be made as to how it is related to the abstract system. Specifically: is it unrelated because G and P_{Op} do not hold; related but establishes only C_{Op}; or related and re-establishes G?

Let us now consider the termination PO (3.2). As Banach argues in [Ban], the main focus of retrenchment should be on successful steps. In our relational model that means steps for which trm_{Op} holds. The conjunction $G \wedge P_{Op}$ defines which parts of the abstract and concrete systems are connected by retrenchment. Therefore, the simplest choice is for trm_{Op} to hold at both abstract and concrete levels whenever $G \wedge P_{Op}$ does[1], and this is the case in (3.2). We further observe that this also means the operation PO is only concerned with successful steps. More extensive arguments in support of the shape of the POs can be found in [BP98, BP01, Ban].

3.3 Output Retrenchment

For steps that re-establish the retrieve relation in PO (3.3), we are not required to say anything about the nature of the relationship between abstract and concrete outputs. If all we need is some means to document how the outputs are related we can use the concedes relation to do this because the disjunction in the antecedent is inclusive. However, at times this muddies the water a little because we do not have a clean partition between normally completing and conceding steps. In cases where this is an advantage, we can employ output retrenchment. This form of retrenchment has for each Op an additional output relation $O_{Op}(o, q; u', w', i, k, u, w)$ which is conjoined to G' to give a new Op PO as follows.

Operation PO (Op PO)

$$
\begin{aligned}
& G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_C}(w, k, w', q) \;\Rightarrow \\
& \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\
& \qquad (\,(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\,)) \,.
\end{aligned}
\tag{3.4}
$$

As before, the semicolon in O_{Op} separates the variables of principal concern from others that may occur when more intricate properties between outputs and other components need to be expressed. (3.4) retains the same basic shape as the primitive Op PO (3.3). Notice that when P_{Op}, O_{Op} and C_{Op} are trivial, the refinement POs (2.4), (2.6) and (2.7) fol-

1. In early work which set out retrenchment in the framework of the B-Method, e.g. [BP98, BP99, Pop01], the concrete trm_{Op} appears in the antecedent of the relevant PO and implies the abstract counterpart in the consequent. In light of insights gained from subsequent work on retrenchment, Banach now advocates the form of termination PO we use in this thesis. This later form in fact facilitates the combination of retrenchment with refinement.

low whenever the output retrenchment POs hold. It may well be the case that in many real developments, most abstract and concrete steps can be related by the retrenchment POs when P_{Op}, O_{Op} and C_{Op} are trivial. For such situations we are justified in regarding retrenchment as being "nearly a refinement".

We will use the output form of retrenchment in the structures combining retrenchment and refinement we present in this thesis. The fact that we have a predicate which says something about the nature of the outputs for normally completing cases simplifies some of the proofs we will discharge in later chapters.

3.4 Definitions

We will need the following concepts.

Definition 3.1. Let the abstract and concrete core predicates of the operation Op, $cor_{Op_A}(u, i)$ and $cor_{Op_C}(w, k)$ respectively, be given by

$$cor_{Op_A}(u, i) = (\exists\, w, k \bullet G(u, w) \wedge P_{Op}(i, k, u, w)) \,, \tag{3.5}$$

$$cor_{Op_C}(w, k) = (\exists\, u, i \bullet G(u, w) \wedge P_{Op}(i, k, u, w)) \,. \tag{3.6}$$

These core predicates identify those parts of the abstract and concrete state and input spaces for Op, for which PO (3.4) is non-trivial. A set of transitions of a system forming part of a retrenchment is said to be abstract (respectively concrete) core bound if and only if all the (before-state, input) pairs of the set satisfy the abstract (respectively concrete) core predicates. ■

Definition 3.2. Let u -(i, Op_A, o)-› u' be an abstract step and w -(k, Op_C, q)-› w' a concrete step. Then these steps are in simulation (or the abstract step simulates the concrete), if and only if we have

$$\begin{aligned} &G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_C}(w, k, w', q) \wedge stp_{Op_A}(u, i, u', o) \wedge \\ &(\,(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\,) \end{aligned} \tag{3.7}$$

An abstract (respectively concrete) step is simulable if and only if there is a concrete (respectively abstract) step such that (3.7) holds for the pair. ■

3.5 Retrenchment in Action

The development of the Number Recycler in Section 2.4.1 ran aground when we tried to capture a desired development step using refinement. Here we show how easily this step fits into the retrenchment framework. Noting that the model given by (2.11) to (2.13) does not say anything about what the operation *Rem* does when the bin is empty, we rectify this prior to defining the retrenchment. The natural approach to take is to generate an error message and leave the state unchanged. The resulting specification *Conc* is given below.

$$\mathsf{W} = \{w \in \mathsf{iseq}(\mathbb{N}) \mid \mathsf{len}(w) \leq 5\},\ \mathsf{K}_{Add_C} = \mathbb{N},\ \mathsf{Q}_{Add_C} = \{\mathsf{OK}, \mathsf{GOT}, \mathsf{FULL}\},$$
$$\mathsf{K}_{Rem_C} = \varnothing,\ \mathsf{Q}_{Rem_C} = \mathbb{N} \cup \{\mathsf{EMPTY}\}. \tag{3.8}$$

$$w \text{ -}(k, Add_C, \mathsf{OK})\text{-}\!\rightarrow w \frown \langle k \rangle,\ \text{if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) \leq 4\ ,$$
$$w \text{ -}(k, Add_C, \mathsf{FULL})\text{-}\!\rightarrow w,\ \text{if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) = 5\ ,$$
$$w \text{ -}(k, Add_C, \mathsf{GOT})\text{-}\!\rightarrow w,\ \text{if } k \in \mathsf{ran}(w)\ . \tag{3.9}$$

$$\langle\ \rangle \text{ -}(Rem_A, \mathsf{EMPTY})\text{-}\!\rightarrow \langle\ \rangle\ ,$$
$$\langle q \rangle \frown w \text{ -}(Rem_A, q)\text{-}\!\rightarrow w\ . \tag{3.10}$$

To establish a retrenchment we now define its component relations as follows.

$$H(u, w) \ = \ (u = \mathsf{ran}(w))\ ,$$
$$Q_{Add}(i, k, u, w) \ = \ (i = k)\ ,$$
$$N_{Add}(o, q, u', w'; i, k, u, w) \ = \ (o = q)\ ,$$
$$D_{Add}(u', w', o, q; i, k, u, w) \ =$$
$$(\ |u| = 5 \wedge i \notin u \wedge u' = u \cup \{\ i\ \} \wedge w' = w \wedge o = \mathsf{OK} \wedge p = \mathsf{FULL}\ )\ ,$$
$$Q_{Rem}(i, k, u, w) \ = \ (u = w \wedge |u| \neq 0)\ ,$$
$$N_{Rem}(o, q, u', w'; i, k, u, w) \ = \ (o = q)\ ,$$
$$D_{Rem}(u', w', o, q; i, k, u, w) \ = \ \mathit{false}\ . \tag{3.11}$$

Notice how concession D_{Add} allows *Conc* to exhibit different behaviour when the set is full. *Abs* adds another element but *Conc* performs a *skip*. So although the retrieve relation does not hold for the after-sates, D_{Add} does, and thus PO (3.4) is satisfied. For *Rem* the within clause Q_{Rem} excludes the ill-behaved cases from consideration. When $|u| = 0$, Q_{Rem} is false and so (3.4) holds trivially.

More convincing examples in support of retrenchment include [PB00], which looks at the specification of a program for dose calculation in radiotherapy, and in [PB02], which presents a control system case study. In contrast to these, [BP03] lies entirely in the discrete domain, and looks at a problem in telephony involving the construction of systems with interacting or conflicting requirements. Finally, we mention [BC04] which applies retrenchment to the process of fault injection and the subsequent generation of fault trees.

3.6 Other Approaches to Liberalising Refinement

Retrenchment is not the only proposal to address the limitations of refinement that can be found in the literature. Recently, Boiten and Derrick have put forward a method which they call refinement with approximations [BD05]. The approach involves replacing a specification S by a chain of specifications, written (S_n), whose limit is the replaced specification. Each S_n is an approximation to the limit S. n gives the position in the chain and is taken to be a parameter of the specification S_n. Using an example from the paper, an unbounded buffer $Buf_{¥}$ can be replaced by a sequence of bounded buffers (Buf_m), where m is the size of the buffer. The limit of (Buf_m) as $m \to \infty$ is $Buf_{¥}$.

The development process uses four different steps: *element-wise refinement* where a specification S is refined to a specification T in the normal way, or a chain (S_n) is refined to a chain (T_n) such that $S_n \sqsubseteq T_n$ for each n; *sequence introduction* where a specification S is replaced by a sequence of specifications (S_n) such that S is the limit of (S_n); *sequence replacement* where a sequence (S_n) with limit S is replaced by a sequence (T_n) with limit T such that $S \sqsubseteq T$; and *compromise* where a sequence (S_n) is replaced by one if its elements S_n. So for the buffer example, replacing $Buf_{¥}$ by (Buf_m) is sequence introduction, and replacing (Buf_m) by Buf_m for a fixed value of m is an example of a compromise step.

The closeness of a specification S_n to the ideal S is quantified by a suitable metric. Different metrics will be appropriate in different situations, e.g. when implementing real numbers the precision in the floating point representation is a possible measure. Two metrics proposed by Boiten and Derrick are one based on program length and one based on counting the number of inputs and outputs for which specifications differ. The program length metric, $d_l(S, T)$, is defined to be zero when S and T are interrefinable and 2^{-n} otherwise, where n is the minimum program length needed to distinguish data type S from T.

This metric works well for the buffer example. The limit of $d_l(Buf_m, Buf_¥)$ as $m \to \infty$ is zero.

An example for which d_l does not converge is the specification of a basic calculator with a simple memory function. Operation $Mem_¥$ stores input x in memory cell mem, where $x, mem \in \mathbb{N}$. We wish to replace $Mem_¥$ with (Mem_n) which sets mem to x if $x < n$. Whether we can tell the two apart now depends not on the length of the program but on the value of the input. To capture cases like this, Boiten and Derrick define the input/output metric, which we denote by $d_{i/o}$. Based on the forward simulation rules, it calculates a ratio of the number of inputs/outputs for which specification S_n correctly refines $S_¥$. To sidestep the problem of counting over an infinite domain Boiten and Derrick approximate $\mathbb{N}$ by 0 .. *maxint* for the purposes of the metric. Thus when $n > maxint$, Mem_n correctly refines $Mem_¥$. Applying $d_{i/o}$ to the calculator problem, the sequence (Mem_n) now converges to $Mem_¥$. The authors readily accept that the approach to accommodate infinite sets, to use their own words, is a fudge, and go on to suggest possible avenues to explore which may offer a better solution for a metric based on I/O. Indeed, the intention of the paper is to set out initial ideas on a possible way to tackle the restrictions that can occur with pure refinement. Further work is necessary to determine the efficacy of Boiten and Derrick's approach.

We observe that metrics by their nature only focus on particular properties of a system. They do not guarantee that in replacing a specification by elements of a chain, we do not end up introducing incorrect behaviour into a model of which a developer is unaware. In contrast, with retrenchment, we have to account for all behaviour in a concrete system. For every concrete step we need to decide whether or how it is related to the steps in the preceding model, and state this explicitly using the within and concedes clauses in order that we can discharge the attendant retrenchment POs.

Boiten and Derrick are not the first to exploit the observation that infinite domains often arise as limits of finite ones. In his thesis on a rigorous development method [Nei90], Neilson handles the transformation from infinite to finite resources by defining refinement over infinite domains as equivalent to the limit of refinement from infinite to finite ones.

In [Liu97] Shaoying Liu has also articulated the need for a formal framework to capture steps that are not refinements. He proposes a notion he calls Evolution. Let P be an operation with precondition *pre-P* and postcondition *post-P*. Operation Q is an evolution of operation P, written $P \sqsubset Q$, if the semantic equivalent of *pre-P* occurs as a component of *pre-Q*, and the semantic equivalent of *post-P* occurs as a component of *post-Q* (and neither *pre-Q* nor *post-Q* are false). Liu gives no insight as to the derivation of this definition. He shows that evolution is transitive, a necessary property for stepwise development, and since $P \sqsubseteq Q \Rightarrow P \sqsubset Q$, that it is a special case of refinement. Steps that are neither a refinement nor an evolution are classified as a modification. Liu thus admits all possible transformations into a development. However, as Banach observed in [Ban00], since S is equivalent to $(S \wedge T) \vee (S \wedge \neg T)$, the transformation from any P to any Q is an evolution, hence all models can be related by Liu's mechanism. The latter is also of course the case for retrenchment. Nevertheless, the advantage with retrenchment is that we must explicitly state the degree of the relationship between abstract and concrete operations by appropriate definition of the within and concedes predicates. Evolution offers no such device.

Another proposition is Realisation by Smith [Smi99, SF00], who gives as motivation arguments similar to those Banach and Poppleton gave for retrenchment [BP98]. The work is presented using the timed refinement calculus of Mahony and Hayes [Mah92, MH92], which was developed specifically for specifying embedded real-time systems. In this formalism a program is described by a specification statement of the form $\mathbf{x} : [A, E]$. This says that an implementation must achieve effect E under assumption A. $\mathbf{x}$ is a list of output variables, any other variables are inputs. A refinement step allows A to be weakened or E to be strengthened. This of course, is analogous to the refinement calculus of Morgan [Mor94].

Realisation extends the possible transformations by introducing three additional realisation rules. These allow the strengthening of A, not possible under refinement, and the modification of both inputs and outputs beyond what can be achieved using refinement, e.g. changes to model timing delays ignored in ideal abstract specifications. Each realisation also has a property transformation rule which allows the derivation of properties of the new specification from those of the old. This therefore offers advantages over Liu's

work which makes no mention of the changes that occur to properties in an evolution step. Retrenchment initially lacked a theory of how properties are transformed under its application, but this has now begun to be addressed [Ban03]. The realisation rules are shown to be complete if the specification is feasible and its assumption is satisfiable. Thus Smith stresses that the liberal nature of the rules imposes a responsibility on a developer to ensure that development steps result in “acceptable approximations”. Naturally, this onus is also applicable in retrenchment.

Chapter 4

Combining Retrenchments and Refinements

We begin by considering the composition of retrenchment and refinement steps. We then introduce the structures combining retrenchments and refinements we have investigated and outline how these structures can be utilised. The technical details for each of the constructions appear in later chapters.

4.1 Composing Retrenchments with Refinements

The first step to a complete theory of the integration of retrenchment and refinement is to investigate the composition of retrenchment and refinement steps. To compose a retrenchment and a refinement we must first decide on the nature of the resulting relationship. We define the composition of a retrenchment and a refinement to be a retrenchment. Given that retrenchment is the more general mechanism, this is realistically the only direction in which to proceed; the alternative, defining the composition as a refinement, involves trying to capture retrenchments inside refinements.

We will first consider the composition of a retrenchment step followed by a refinement step. To make further progress, in addition to the systems *Abs* and *Conc* we met in earlier chapters, we need an additional system *Btw* (for between) with variables v, j and p.

Proposition 4.1. Let there be a retrenchment from *Abs* to *Btw* given by retrieve relation $H(u, v)$ and for each *Op*, within relation $Q_{Op}(i, j, u, v)$, output relation $N_{Op}(o, p; u', v', i, j, u, v)$ and concedes relation $D_{Op}(u', v', o, p; i, j, u, v)$. Further, let there be a refinement

from *Btw* to *Conc* given by retrieve relation $K(v, w)$, and for each *Op*, input relation $R_{Op}(j, k)$ and output relation $V_{Op}(p, q)$. Then there is a retrenchment from *Abs* to *Conc* given by retrieve relation $G(u, w)$, and for each *Op*, within relation $P_{Op}(i, k, u, w)$, output relation $O_{Op}(o, q; u', w', i, k, u, w)$ and concedes relation $C_{Op}(u', w', o, q; i, k, u, w)$, which we define below.

Each of G, P_{Op}, O_{Op} and C_{Op} are defined in terms of the relations of the component retrenchment and refinement. For G, the sensible choice is to define it as the composition of H and K,

$$G(u, w) \;=\; H(u, v) \fatsemi K(v, w)\ . \tag{4.1}$$

Next, we consider P_{Op}. We note that there is no within relation for the refinement from *Btw* to *Conc* which we can compose with the within relation Q_{Op} of the retrenchment from *Abs* to *Btw*. The approach we adopt is to construct a suitable within relation, from the existing retrieve and input relations of the refinement. Let the new within relation be denoted by W_{Op}. Then

$$W_{Op}(j, k, v, w) \;=\; R_{Op}(j, k) \wedge K(v, w)\ . \tag{4.2}$$

Recalling the material from Chapter 2, W_{Op} is just the parallel composition of K and R_{Op}. Thus if we were working in the purely relational framework we used in the first part of Chapter 2, we would write $W_{Op} = K \parallel R_{Op}$. For P_{Op} we now have

$$P_{Op}(i, k, u, w) \;=\; Q_{Op}(i, j, u, v) \fatsemi W_{Op}(j, k, v, w)\ , \tag{4.3}$$

but we will always write such compositions in their expanded form,

$$P_{Op}(i, k, u, w) \;=\; Q_{Op}(i, j, u, v) \fatsemi (R_{Op}(j, k) \wedge K(v, w))\ , \tag{4.4}$$

and so avoid an additional level of definitions. As we shall see, (4.4) is not strong enough for our purposes and we in fact need $H(u, v)$ to hold whenever $Q_{Op}(i, j, u, v)$ holds. We shall comment on this further below. We therefore define P_{Op} as

$$P_{Op}(i, k, u, w) \;=\; (Q_{Op}(i, j, u, v) \wedge H(u, v)) \fatsemi (R_{Op}(j, k) \wedge K(v, w))\ . \tag{4.5}$$

Finally we define,

$$O_{Op}(o, q; u', w', i, k, u, w) \;=$$
$$N_{Op}(o, p; u', v', i, j, u, v) \fatsemi (V_{Op}(p, q) \wedge K(v', w') \wedge R_{Op}(j, k) \wedge K(v, w)) \;, \tag{4.6}$$

$$C_{Op}(u', w', o, q; i, k, u, w) =$$
$$D_{Op}(u', v', o, p; i, j, u, v) \fatsemi (K(v', w') \wedge V_{Op}(p, q) \wedge R_{Op}(j, k) \wedge K(v, w)) \;. \tag{4.7}$$

Given these definitions we can now prove Proposition 4.1.

Proof. To show that there is a retrenchment from *Abs* to *Conc* we must discharge the relevant Init, Op and Term POs. We take the Init PO first.

♦ We show

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', w')) \;. \tag{4.8}$$

Assume the antecedent $Init_{\mathrm{C}}(w')$. From the Init PO for the refinement from *Btw* to *Conc*,

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, v' \bullet Init_{\mathrm{B}}(v') \wedge K(v', w')), \tag{4.9}$$

we get $Init_{\mathrm{B}}(v')$ and $K(v', w')$ for chosen value v'. From the former and the Init PO for the retrenchment from *Abs* to *Btw*,

$$Init_{\mathrm{B}}(v') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge H(u', v')), \tag{4.10}$$

we get $Init_{\mathrm{A}}(u')$ and $H(u', v')$ for chosen value u'. So we have $Init_{\mathrm{A}}(u')$ and all we need is $G(u', w')$. This follows from the composition of K and H, by (4.1). We are done.

♦ Next we show the Term PO,

$$G(u, w) \wedge P_{Op}(i, k, u, w) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{C}}}(w, k) \;. \tag{4.11}$$

Assume the antecedents. From $P_{Op}(i, k, u, w)$, by (4.5), there are values, j and v say, such that $Q_{Op}(i, j, u, v)$, $H(u, v)$, $R_{Op}(j, k)$ and $K(v, w)$ hold. Then, from the Term PO for the retrenchment from *Abs* to *Btw*,

$$H(u, v) \wedge Q_{Op}(i, j, u, v) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{B}}}(v, j) \;, \tag{4.12}$$

we obtain $trm_{Op_A}(u, i)$, which we require, and $trm_{Op_B}(v, j)$. Notice that we needed to define P_{Op} in terms of both Q_{Op} and H, so as to ensure that they share a common u and thus that the antecedent of (4.12) holds. We can now use the App PO for the refinement from *Btw* to *Conc*,

$$K(v, w) \wedge R_{Op}(j, k) \wedge trm_{Op_B}(v, j) \;\Rightarrow\; trm_{Op_C}(w, k)\,, \tag{4.13}$$

to obtain the remaining conjunct $trm_{Op_C}(w, k)$. Thus (4.11) holds as required.

♦ Last we show the Op PO,

$$\begin{aligned} &G(u, w) \wedge P_{Op}(i, k, u, w) \wedge trm_{Op_B}(v, j) \wedge stp_{Op_C}(w, k, w', q) \;\Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\ &\qquad (\,(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\,))\,. \end{aligned} \tag{4.14}$$

Assume the antecedents. As we saw in the proof for PO (4.11), from $P_{Op}(i, k, u, w)$ we obtain $Q_{Op}(i, j, u, v)$, $H(u, v)$, $R_{Op}(j, k)$, $K(v, w)$ and $trm_{Op_B}(v, j)$. We can now use the refinement Corr PO

$$\begin{aligned} &K(v, w) \wedge R_{Op}(j, k) \wedge trm_{Op_B}(v, j) \wedge stp_{Op_C}(w, k, w', q) \;\Rightarrow \\ &\quad (\exists\, v', p \bullet stp_{Op_B}(v, j, v', p) \wedge K(v', w') \wedge V_{Op}(p, q))\,, \end{aligned} \tag{4.15}$$

to obtain $stp_{Op_B}(v, j, v', p)$, $K(v', w')$ and $V_{Op}(p, q)$ for values v' and p. We can now use the Op PO for the retrenchment from *Abs* to *Btw*,

$$\begin{aligned} &H(u, v) \wedge Q_{Op}(i, j, u, v) \wedge stp_{Op_B}(v, j, v', p) \;\Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\ &\qquad (\,(H(u', v') \wedge N_{Op}(o, p; u', v', i, j, u, v)) \vee D_{Op}(u', v', o, p; i, j, u, v)\,))\,, \end{aligned} \tag{4.16}$$

to assert values u' and o such that $stp_{Op_A}(u, i, u', o)$ and $(H(u', v') \wedge N_{Op}(o, p; u', v', i, j, u, v)) \vee D_{Op}(u', v', o, p; i, j, u, v)$ hold. So we now have the first conjunct, $stp_{Op_A}(u, i, u', o)$, of the consequent of (4.11). All we need is the second, $(G' \wedge O_{Op}) \vee C_{Op}$. We derive this from $(H' \wedge N_{Op}) \vee D_{Op}$ as follows. Assume $H' \wedge N_{Op}$. Then as $K(v', w')$ holds, we have $H(u', v') \fatsemi K(v', w')$ and thus $G(u', w')$, by (4.1). Furthermore, because K', V_{Op}, R_{Op} and K all hold, we have $N_{Op}(o, p; u', v', i, j, u, v) \fatsemi (V_{Op}(p, q) \wedge K(v', w') \wedge R_{Op}(j, k) \wedge K(v, w))$

and thus $O_{Op}(o, q; u', w', i, k, u, w)$, by (4.6). Now assume $D_{Op}(u', v', o, p; i, j, u, v)$. Then $D_{Op}(u', v', o, p; i, j, u, v) \fatsemi (K(v', w') \wedge V_{Op}(p, q) \wedge R_{Op}(j, k) \wedge K(v, w))$ gives $C_{Op}(u', w', o, q; i, k, u, w)$, by (4.7). Hence $(G' \wedge O_{Op}) \vee C_{Op}$ holds and we are done. ■

Proposition 4.2. Let there be a refinement from *Abs* to *Btw* given by retrieve relation $K(u, v)$, and for each *Op*, input relation $R_{Op}(i, j)$ and output relation $V_{Op}(o, p)$. Let there be a retrenchment from *Btw* to *Conc* given by retrieve relation $H(v, w)$ and for each *Op*, within relation $Q_{Op}(j, k, v, w)$, output relation $N_{Op}(p, q; v', w', j, k, v, w)$ and concedes relation $D_{Op}(v', w', p, q; j, k, v, w)$. Then there is a retrenchment from *Abs* to *Conc* given by retrieve relation $G(u, w)$ and for each *Op*, within relation $P_{Op}(i, k, u, w)$, output relation $O_{Op}(o, q; u', w', i, k, u, w)$ and concedes relation $C_{Op}(u', w', o, q; i, k, u, w)$, where

$$G(u, w) \;=\; K(u, v) \fatsemi H(v, w)\ , \tag{4.17}$$

$$P_{Op}(i, k, u, w) \;=\; (R_{Op}(i, j) \wedge K(u, v)) \fatsemi (Q_{Op}(j, k, v, w) \wedge H(v, w))\ , \tag{4.18}$$

$$\begin{aligned} &O_{Op}(o, q; u', w', i, k, u, w) \;= \\ &\quad (V_{Op}(o, p) \wedge K(u', v') \wedge R_{Op}(i, j) \wedge K(u, v)) \fatsemi N_{Op}(p, q; v', w', j, k, v, w)\ , \end{aligned} \tag{4.19}$$

$$\begin{aligned} &C_{Op}(u', w', o, q; i, k, u, w) = \\ &\quad (K(u', v') \wedge V_{Op}(o, p) \wedge R_{Op}(i, j) \wedge K(u, v)) \fatsemi D_{Op}(v', w', p, q; j, k, v, w)\ . \end{aligned} \tag{4.20}$$

Proof. Similar to Proposition 4.1. ■

Similar results for the composition of retrenchments and refinements in a partial correctness setting are reported in [BJP04], which also examines various forms of composition mechanisms for retrenchment. [BJ02] defines stronger forms of output retrenchment by imposing constraints on the component relations, and studies their composition and associativity.

We note the above definitions for the relations of the composite retrenchment are not the only ones possible. For example, in the postjoin and prejoin structures introduced later in this chapter, stronger forms for the output and concedes relations are used, securing the results we seek there.

4.2 The Lifting Construction

Suppose we have a retrenchment from a system *Abs* to a system *Conc*. The lifting construction takes the given retrenchment and decomposes it into a retrenchment followed by a refinement. The decomposition results in a new system *Univ*, which retrenches *Abs* and refines to *Conc*, as shown in Figure 4.1. In addition, *Univ* is required to be a system at the

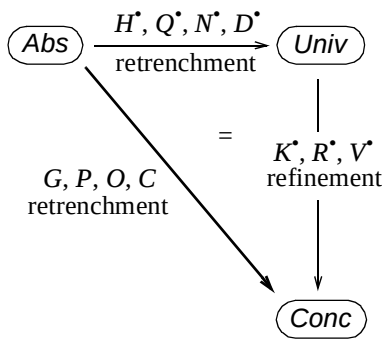


Figure 4.1: Decomposing a retrenchment into a retrenchment followed by a refinement.

level of abstraction of *Abs* but one which captures the constraints demanded by *Conc*. We say the construction lifts *Conc* to the level of *Abs*.

We obtain the desired level of abstraction for *Univ*, by ensuring that for any system *Xtra* which also decomposes the retrenchment from *Abs* to *Conc*, there is a refinement from *Univ* to *Xtra* (this thus being the universal property which characterizes *Univ*), see Figure 4.2. Hence *Univ* is the most abstract decomposition possible. As further evidence that *Univ* is at a high enough level of abstraction, we demonstrate that the *Abs* to *Univ* retrenchment is idempotent. By this we mean that applying the lifting construction to the *Abs* to *Univ* retrenchment itself, results in a system which is essentially *Univ*.

Univ and all the other systems *Xtra* which decompose the retrenchment belong to a class of systems, which describes the additional attributes that systems decomposing the retrenchment need in order to realize the desired construction. The class also defines what "abstraction" is in this technical context. We build *Univ* to be the most abstract in this class. In fact there may be a number of systems which are the most abstract in that they

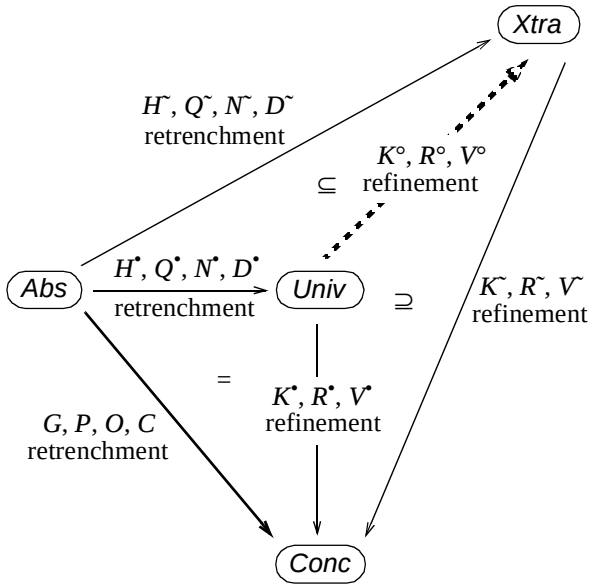


Figure 4.2: Lifting *Conc* to the level of *Abs*

refine onto all the other systems in the class of decompositions. These most abstract systems form an equivalence class, members of which are all interrefinable. *Univ* is then the most abstract in the class of systems decomposing the retrenchment, up to equivalence.

4.3 The Lowering Construction

This construction complements the lifting one by decomposing the retrenchment from *Abs* to *Conc* into a refinement from *Abs* to a system *Univ* and a retrenchment from *Univ* to *Conc*; see Figure 4.3. The objective this time is for *Univ* to be a the level of *Conc*. We say the construction lowers *Abs* to the level of *Conc*.

In the class of systems decomposing the retrenchment, we ensure *Univ* is the most concrete decomposition possible, up to equivalence, by requiring it to have the universal property that for all other systems *Xtra* in the class, there is a refinement from *Xtra* to the abstract core bound transitions of *Univ* (see Definition 3.1). Additional evidence that *Univ* is concrete enough is provided by demonstrating that the construction of *Univ* is idempotent: lowering the abstract core bound transitions of *Univ* again by repeating the construction yields nothing new.

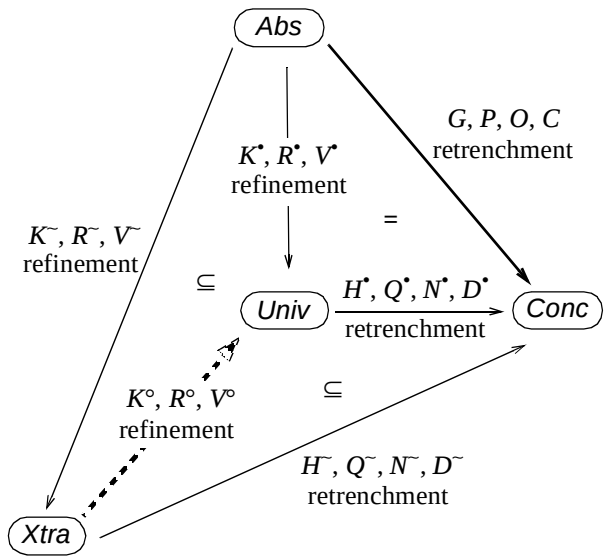


Figure 4.3: Lowering *Abs* to the level of *Conc*

4.4 The Postjoin Construction

Suppose we have a system *Abs* which is retrenched to a system *Ret*, and also refined to a system *Ref*. The postjoin construction produces a new system *Univ* such that *Univ* is simultaneously a retrenchment of *Ref* and a refinement of *Ret*. Additionally, the composition of the *Abs* to *Ret* retrenchment with the *Ret* to *Univ* refinement on the one hand, and the composition of the *Abs* to *Ref* refinement with the *Ref* to *Univ* retrenchment on the other, must both be equal and be a retrenchment from *Abs* to *Univ*. We further characterize *Univ* in a suitably universal manner, viz. that any other system *Xtra*, in the class of systems which achieve the same reconciliation, must be refinable from *Univ*. Thus, in the class, *Univ* is the most abstract possible completion of the square up to equivalence. See diagram (i), Figure 4.4.

4.5 The Prejoin Construction

The prejoin construction is the counterpart of the postjoin. Given a system *Conc* which is both a refinement of a system *Ret* and a retrenchment of a system *Ref*, the postjoin produces a system *Univ* which is both retrenchable to *Ret* and refinable to *Ref*, and for which the composition of the *Univ* to *Ret* retrenchment with the *Ret* to *Conc* refinement on the one hand, and the composition of the *Univ* to *Ref* refinement with the *Ref* to *Conc* re-

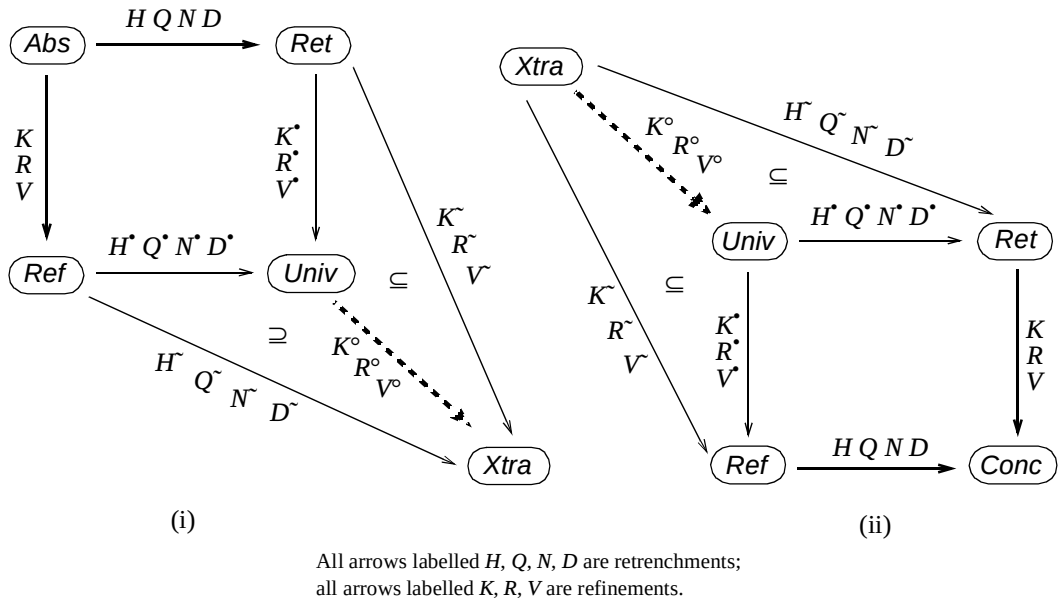


Figure 4.4: (i) the postjoin construction; (ii) the prejoin construction.

trenchment on the other, must both be equal and be a retrenchment from *Univ* to *Conc*. Additionally, *Univ* must be canonical in that for any other system *Xtra* in the class of systems which also complete the square, there is a refinement from *Xtra* to *Univ*. Thus *Univ* is the most concrete completion possible in the class up to equivalence. See diagram (ii), Figure 4.4.

4.6 An Engineering Perspective

The structures linking retrenchments and refinements described above are not merely mathematical curiosities: they also have practical benefits. First, they show that retrenchment and refinement are not incompatible techniques. They reassure practitioners that the two mechanisms can be used together, that the introduction of retrenchment into a development does not take the process down a route at odds with refinement. Second, these constructions provide mechanisms which can be used to generate new systems from given retrenchments and refinements.

Consider the lifting construction. It takes a retrenchment step and raises the concrete (retrenching) model to the level of its abstract precursor. The result is a new abstract model which is refinable back to the concrete one. Hence if the original abstract model is a spec-

ification, the lifting construction automatically generates a new specification which incorporates the retrenched constraints found in the concrete model. It is important to realize that the concrete model is not necessarily the immediate successor of the abstract specification. The single retrenchment step lifted by the construction could be the composition of several retrenchment and refinement steps. The reciprocal lowering construction on the other hand, allows us to lower the abstract model to the level of abstraction of the concrete one. It captures that part of the change in abstraction which can be expressed as a refinement alone. The result thus provides a different view of the abstract system, thereby enabling a developer to consider the problem from a different perspective, which is always a useful thing to do.

The postjoin also has a direct application. Referring back to Figure 4.4 (i), imagine that *Ref* is the end-product of a formal software development, refined from an original specification *Abs*. Sometime later, a new version of the software is proposed, and the original specification is altered to incorporate the changes. If we can relate the new specification to the initial one via a retrenchment, the new specification takes the place of *Ret* in the diagram. We can now avoid a complete reworking of the development, and use the postjoin to directly construct the new concrete version *Univ*.

The prejoin construction allows us to achieve something similar. Let the refinement from *Ret* to *Conc* in Figure 4.4 (ii) represent an existing development from abstract specification to code. Suppose now the code is changed to give a new program and the relationship between the two is a retrenchment from the new to the old, from *Ref* to *Conc* in the diagram. Then we can use the prejoin to automatically obtain *Univ*, an abstract representation of the new program.

4.7 The Tower Pattern

The scenarios in the previous section share a common theme which we educe in the methodological paradigm we call the *Tower Pattern*. When the above mechanisms are repeatedly applied to a stack of refinements, $M_0 \sqsubseteq M_1 \sqsubseteq M_2 \sqsubseteq \ldots \sqsubseteq M_n$, they result in the formation of the tower structure shown Figure 4.5, where the vertical relationships are refinements and the horizontal relationships are retrenchments. To build the tower we could start at the top, define the retrenchment M_0 to N_0, representing a change in specification

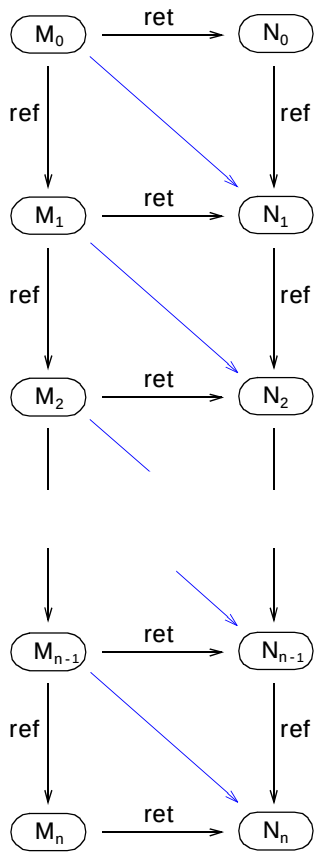


Figure 4.5: The Tower Pattern

for example, and then use the postjoin to successively construct the stack of refinements from N_0 to N_n, so pushing the change in requirements down through the stack. Alternatively, we could begin with the bottom retrenchment M_n to N_n, and first compose it with the refinement from M_{n-1} to M_n, to obtain the retrenchment M_{n-1} to N_n (the bottommost diagonal arrow). We then use the lifting construction to generate the refinement from N_{n-1} to N_n. We continue in similar fashion, building the tower upwards, relaying the change described by the bottom retrenchment to the topmost level. Of course there is also the option of working from the N-refinement stack and using the prejoin or lowering construction to create the M-stack instead.

Chapter 5

The Lifting Theorem

This chapter tackles the problem of decomposing a retrenchment from an abstract to a concrete system into a retrenchment followed by a refinement. We engineer a system *Univ* which is the most abstract up to equivalence within a class of systems achieving the same decomposition.

A previous attempt at the lifting construction [Ban00], has been shown to contain a bug by the author of this thesis. The material below is significantly different from this earlier work.

5.1 The Lifting Theorem

Theorem 5.1. Let there be a retrenchment from *Abs* to *Conc*, as shown in Figure 5.1. Then the following hold.

(1) There is a universal system *Univ* such that there is a retrenchment from *Abs* to *Univ* and a refinement from *Univ* to *Conc* whose composition is the given retrenchment, and which satisfies (U1) to (U7) below.

(2) Whenever there is a system *Xtra* and a retrenchment from *Abs* to *Xtra* and a refinement from *Xtra* to *Conc* whose composition is the given retrenchment, and which satisfies (X1) to (X7) below, then there is a refinement from *Univ* to *Xtra* such that the following inclusions hold. $H^{\sim} \Rightarrow H^{\bullet} ⨾ K^{\circ}$, $Q^{\sim}{}_{Op} \Rightarrow Q^{\bullet}{}_{Op} ⨾ (R^{\circ}{}_{Op} \wedge K^{\circ})$, $N^{\sim}{}_{Op} \Rightarrow N^{\bullet}{}_{Op} ⨾ (V^{\circ}{}_{Op} \wedge K^{\circ\prime} \wedge R^{\circ}{}_{Op} \wedge K^{\circ})$, $D^{\sim}{}_{Op} \Rightarrow D^{\bullet}{}_{Op} ⨾ (K^{\circ\prime} \wedge V^{\circ}{}_{Op} \wedge R^{\circ}{}_{Op} \wedge K^{\circ})$, $K^{\circ} ⨾ K^{\sim} \Rightarrow K^{\bullet}$, $R^{\circ}{}_{Op} ⨾ R^{\sim}{}_{Op} \Rightarrow R^{\bullet}{}_{Op}$ and $V^{\circ} ⨾ V^{\sim}{}_{Op} \Rightarrow V^{\bullet}{}_{Op}$ (see also (5.52) to (5.58)).

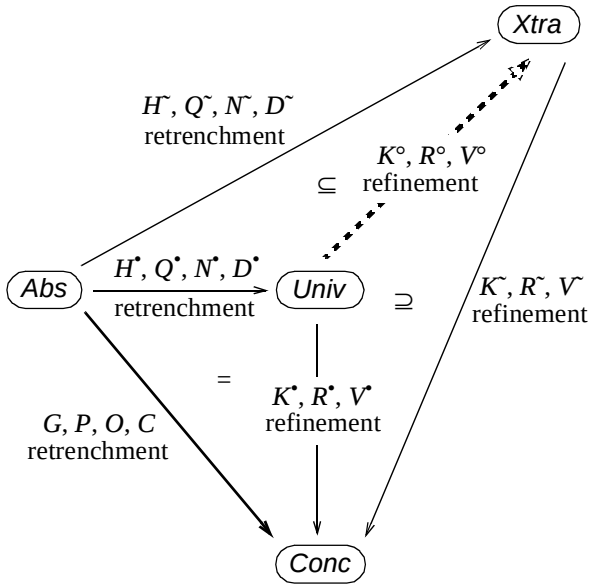


Figure 5.1: Lifting *Conc* to the level of *Abs*

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are mutually interrefinable.

In the following sections we prove each of the above parts.

5.2 Proof for Part (1)

We take the retrenchment from *Abs* to *Conc* and build a new, universal system, *Univ*, for which we then show there is *both* a retrenchment from *Abs* and a refinement to *Conc*. See Figure 5.1.

For *Abs* the operation names set is $Op_{\mathrm{A}} \in \mathsf{Ops}_{\mathrm{A}}$, state, input and output spaces are $u \in \mathsf{U}$, $i \in \mathsf{I}_{Op_{\mathrm{A}}}$, $o \in \mathsf{O}_{Op_{\mathrm{A}}}$, and initialisation and step predicates are $Init_{\mathrm{A}}$ and $stp_{Op_{\mathrm{A}}}$. Correspondingly, for *Conc* we have $Op_{\mathrm{C}} \in \mathsf{Ops}_{\mathrm{C}}$, $w \in \mathsf{W}$, $k \in \mathsf{K}_{Op_{\mathrm{C}}}$, $q \in \mathsf{Q}_{Op_{\mathrm{C}}}$, $Init_{\mathrm{C}}$ and $stp_{Op_{\mathrm{C}}}$. Here, $\mathsf{Ops}_{\mathrm{A}} \subseteq \mathsf{Ops}_{\mathrm{C}}$. Let the retrenchment from *Abs* to *Conc* have retrieve relation G, and for each Op, within relation P_{Op}, output relation O_{Op} and concedes relation C_{Op}.

5.2.1 The system *Univ*

The operation names set of *Univ* is Ops_U with elements Op_U. The state space is V with elements v. The inputs are $j \in \mathsf{J}$, and the outputs are $p \in \mathsf{P}$. These are all constructed from the systems *Abs* and *Conc* as follows. Firstly $\mathsf{Ops}_\mathrm{U} = \mathsf{Ops}_\mathrm{C} = \mathsf{Ops}_\mathrm{A} \cup (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$. So each Op_U is either an Op_A or an $Op_\mathrm{U} \in (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$. Next $\mathsf{V} = \mathsf{T} \times \mathsf{U} \times \mathsf{W}$, where $\mathsf{T} = \{0, 1\}$ and $t \in \mathsf{T}$ is a tag. For $Op_\mathrm{U} \in \mathsf{Ops}_\mathrm{A}$ the input and output spaces are $\mathsf{J}_{Op} = \mathsf{I}_{Op} \times \mathsf{K}_{Op}$ and $\mathsf{P}_{Op} = \mathsf{O}_{Op} \times \mathsf{Q}_{Op}$, while for $Op_\mathrm{U} \notin \mathsf{Ops}_\mathrm{A}$, $\mathsf{J}_{Op} = \mathsf{K}_{Op}$ and $\mathsf{P}_{Op} = \mathsf{Q}_{Op}$.

Let the initialization predicate $Init_\mathrm{U}(v')$ be defined as follows.

$$Init_\mathrm{U}(v') \;=\; (\; v' = (t', u', w') \wedge t' = 0 \wedge Init_\mathrm{A}(u') \wedge G(u', w') \;) \tag{5.1}$$

We now give the transitions of *Univ*. For $Op_\mathrm{U} \in \mathsf{Ops}_\mathrm{A}$ let the step relation be

$$\begin{aligned} &stp_{Op_\mathrm{U}}(v, j, v', p) \;=\; stp_{Op_\mathrm{U}}((t, u, w), (i, k), (t', u', w'), (o, q)) \;= \\ &\quad \big(\; t = t' = 0 \wedge G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_\mathrm{A}}(u, i, u', o) \wedge \\ &\quad (\; (G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w) \;) \;\big) \;. \end{aligned} \tag{5.2}$$

For $Op_\mathrm{U} \notin \mathsf{Ops}_\mathrm{A}$ let

$$stp_{Op_\mathrm{U}}(v, j, v', p) \;=\; stp_{Op_\mathrm{U}}((t, u, w), k, (t', u', w'), q) \;=\; stp_{Op_\mathrm{C}}(w, k, w', q) \;. \tag{5.3}$$

This completes the definition of *Univ*.

Given the above, observe that the following hold. For $Op_\mathrm{U} \in \mathsf{Ops}_\mathrm{A}$

$$\begin{aligned} &trm_{Op_\mathrm{U}}(v, j) \;=\; trm_{Op_\mathrm{U}}((t, u, w), (i, k)) \;= \\ &\quad (t = 0 \wedge G(u, w) \wedge P_{Op}(i, k, u, w) \wedge trm_{Op_\mathrm{A}}(u, i) \wedge \\ &\quad (\exists\, u', o, w', q \bullet stp_{Op_\mathrm{A}}(u, i, u', o) \wedge \\ &\qquad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)))) \;. \end{aligned} \tag{5.4}$$

For $Op_\mathrm{U} \notin \mathsf{Ops}_\mathrm{A}$

$$trm_{Op_\mathrm{U}}(v, j) \;=\; trm_{Op_\mathrm{U}}((t, u, w), k) \;=\; trm_{Op_\mathrm{C}}(w, k) \;. \tag{5.5}$$

5.2.2 The retrenchment from *Abs* to *Univ*

In this section we show that *Univ* is a retrenchment of *Abs*. To do this we first define the component relations of the retrenchment and then show that the retrenchment POs hold.

5.2.2.1 The component relations

The data for the retrenchment consists of the retrieve relation $H^{\bullet}$, and for each *Op*, the within relation $Q^{\bullet}_{Op}$, the output relation $N^{\bullet}_{Op}$, and the concedes relation $D^{\bullet}_{Op}$. These are defined as follows.

$$H^{\bullet}(u, v) \;=\; (v = (t, u, w) \wedge t = 0 \wedge G(u, w)) \tag{5.6}$$

$$Q^{\bullet}_{Op}(i, j, u, v) \;=\; (j = (i, k) \wedge v = (t, u, w) \wedge t = 0 \wedge P_{Op}(i, k, u, w)) \tag{5.7}$$

$$\begin{aligned} &N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \;= \\ &\quad (p = (o, q) \wedge v' = (t', u', w') \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\ &\quad O_{Op}(o, q; u', w', i, k, u, w)) \end{aligned} \tag{5.8}$$

$$\begin{aligned} &D^{\bullet}_{Op}(u', v', o, p; i, j, u, v) \;= \\ &\quad (v' = (t', u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\ &\quad C_{Op}(u', w', o, q; i, k, u, w)) \end{aligned} \tag{5.9}$$

5.2.2.2 The initialisation PO

We show

$$Init_{\mathrm{U}}(v') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge H^{\bullet}(u', v'))\ . \tag{5.10}$$

Proof. Assume the antecedent and let $v' = (t', u', w')$. Then by (5.1), $t' = 0$, $Init_{\mathrm{A}}(u')$ and $G(u', w')$ all hold. Hence, since $t' = 0$ and $G(u', w')$ holds, by (5.6), $H^{\bullet}(u', v')$ must also hold. Therefore the consequent holds for the value u'. ■

5.2.2.3 The termination PO

We show

$$H^{\bullet}(u, v) \wedge Q^{\bullet}_{Op}(i, j, u, v) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{U}}}(v, j)\ . \tag{5.11}$$

Proof. For this relationship Op_U only ranges over Ops_A. Choose values $v = (t, u, w)$ and $j = (i, k)$ for which the antecedents hold. From $H^\bullet(u, v)$, by (5.6), we get $G(u, w)$ and $t = 0$; from $Q^\bullet_{Op}(i, j, u, v)$, by (5.7), we get $P_{Op}(i, k, u, w)$. Therefore we can now use the Term PO for the retrenchment from *Abs* to *Conc*,

$$G(u, w) \wedge P_{Op}(i, k, u, w) \;\Rightarrow\; trm_{Op_A}(u, i) \wedge trm_{Op_C}(w, k)\ , \tag{5.12}$$

to derive $trm_{Op_A}(u, i)$, which we want, and $trm_{Op_C}(w, k)$ to boot. The latter guarantees that there are after values, w' and q say, such that $stp_{Op_C}(w, k, w', q)$ holds. We thus have the antecedents of the Op PO for the retrenchment from *Abs* to *Conc*,

$$\begin{aligned}
&G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_C}(w, k, w', q) \;\Rightarrow \\
&\quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\
&\qquad (\,(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\,))\ ,
\end{aligned} \tag{5.13}$$

from which we can derive enough to conclude, by (5.4), that $trm_{Op_U}(v, j)$ also holds. We are done. ■

5.2.2.4 The operation PO

We show

$$\begin{aligned}
&H^\bullet(u, v) \wedge Q^\bullet_{Op}(i, j, u, v) \wedge stp_{Op_U}(v, j, v', p) \;\Rightarrow \\
&\quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\
&\qquad (\,(H^\bullet(u', v') \wedge N^\bullet_{Op}(o, p; u', v', i, j, u, v)) \vee D^\bullet_{Op}(u', v', o, p; i, j, u, v)\,))\ .
\end{aligned} \tag{5.14}$$

Proof. For this relationship Op_U only ranges over Ops_A. Choose values $v = (t, u, w)$, $j = (i, k)$, $v' = (t', u', w')$, and $p = (o, q)$ for which the antecedents hold. From stp_{Op_U}, by (5.2), we get $stp_{Op_A}(u, i, u', o)$ and also $t = t' = 0$, and $G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)$ or $C_{Op}(u', w', o, q; i, k, u, w)$. Now assume $G' \wedge O_{Op}$ holds. Then, by (5.6) and (5.8), $H^\bullet(u', v') \wedge N^\bullet_{Op}(o, p; u', v', i, j, u, v)$ holds. Otherwise assume C_{Op} holds. Then, by (5.9), $D^\bullet_{Op}(u', v', o, p; i, j, u, v)$ holds. Therefore the consequent holds for the values u' and o.

■

5.2.3 The refinement from *Univ* to *Conc*

In this section we show that *Conc* is a refinement of *Univ*. To do this we first define the component relations of the refinement and then show that the refinement POs hold.

5.2.3.1 The component relations

The data for the refinement consists of the retrieve relation $K^{\bullet}$, and for each Op, the within relation $R^{\bullet}_{Op}$ and the nevertheless relation $V^{\bullet}_{Op}$. These are defined as follows.

$$K^{\bullet}(v, w) \;=\; (v = (t, u, w)) \;. \tag{5.15}$$

For $Op \in \mathsf{Ops}_{\mathrm{A}}$ we have

$$R^{\bullet}_{Op}(j, k) \;=\; (j = (i, k)) \;, \tag{5.16}$$

$$V^{\bullet}_{Op}(p, q) \;=\; (p = (o, q)) \;. \tag{5.17}$$

For $Op \notin \mathsf{Ops}_{\mathrm{A}}$

$$R^{\bullet}_{Op}(j, k) \;=\; (j = k) \;, \tag{5.18}$$

$$V^{\bullet}_{Op}(p, q) \;=\; (p = q) \;. \tag{5.19}$$

Relation (5.15) is a projection onto the third component. (5.16) and (5.17) are projections onto the second component. (5.18) and (5.19) are identities. These relations are therefore all total functions.

We also have the input initialisations and output finalisations. *Conc* is the only given system involved in the refinements, thus we use the input and output spaces of its operations to construct those of the global world. For $Op \in \mathsf{Ops}_{\mathrm{A}}$, $\mathsf{N}_{Op} = \mathsf{Q}_{Op}$ and let,

$$\mathsf{H}_{Op} \;=\; \{h \in \mathsf{K}_{Op} \mid \exists\, i, k, u, w \bullet k = h \wedge P_{Op}(i, k, u, w) \wedge G(u, w)\} \;, \tag{5.20}$$

$$InitIn_{Op_{\mathrm{C}}}(h, k) \;=\; (h = k) \;, \tag{5.21}$$

$$FinOut_{Op_{\mathrm{C}}}(q, n) \;=\; (q = n) \;, \tag{5.22}$$

$$InitIn_{Op_{\mathrm{U}}}(h, j) \;=\; (\exists\, i, k, u, w \bullet k = h \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge G(u, w)) \;, \tag{5.23}$$

$$FinOut_{Op_U}(p, n) = (p = (o, q) \wedge n = q) \ . \tag{5.24}$$

For $Op \notin \mathsf{Ops}_A$, $\mathsf{H}_{Op} = \mathsf{K}_{Op}$, $\mathsf{N}_{Op} = \mathsf{Q}_{Op}$ and let,

$$InitIn_{Op_C}(h, k) \ = \ (h = k) \ , \tag{5.25}$$

$$FinOut_{Op_C}(q, n) \ = \ (q = n) \ , \tag{5.26}$$

$$InitIn_{Op_U}(h, j) \ = \ (h = j) \ , \tag{5.27}$$

$$FinOut_{Op_U}(p, n) = (p = n) \ . \tag{5.28}$$

Note that all the above relations are total.

5.2.3.2 The input initialisation PO

We show

$$InitIn_{Op_C}(h, k) \ \Rightarrow \ (\exists\, j \bullet InitIn_{Op_U}(h, j) \wedge R^{\bullet}_{Op}(j, k)) \ . \tag{5.29}$$

Proof. As $Op_C \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op_C \in \mathsf{Ops}_A$. Assume $InitIn_{Op_C}(h, k)$. By (5.21), $h = k$. For this k, by (5.20), there are values, i, u and w say, for which $P_{Op}(i, k, u, w)$ and $G(u, w)$ hold. Let $j = (i, k)$ and $v = (t, u, w)$ with $t = 0$. Then $InitIn_{Op_U}(h, j)$ holds, by (5.23), and $R^{\bullet}_{Op}(j, k)$ holds, by (5.16). Done.

• Case $Op_C \notin \mathsf{Ops}_A$. Assume $InitIn_{Op_C}(h, k)$. By (5.25), $h = k$. Let $j = h$. Then, by (5.27), $InitIn_{Op_U}(h, j)$ holds, and, by (5.18), $R^{\bullet}_{Op}(j, k)$ holds. Done. ■

5.2.3.3 The initialisation PO

We show

$$Init_C(w') \ \Rightarrow \ (\exists\, v' \bullet Init_U(v') \wedge K^{\bullet}(v', w')) \ . \tag{5.30}$$

Proof. Assume the antecedent $Init_C(w')$. Since we have $Init_C(w')$, we can use the Init PO for the retrenchment from *Abs* to *Conc*,

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', w'))\ , \tag{5.31}$$

to get $Init_{\mathrm{A}}(u')$ and $G(u', w')$ for chosen value u'. Let $v' = (t', u', w')$ and $t' = 0$. Then $Init_{\mathrm{U}}(v')$ holds by (5.1) and $K^{\bullet}(v', w')$ holds by (5.15). Hence there is a value, the v' just derived, for which the consequent of (5.30) holds. ■

5.2.3.4 The applicability PO

We show

$$K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge trm_{Op_{\mathrm{U}}}(v, j) \;\Rightarrow\; trm_{Op_{\mathrm{C}}}(w, k)\ . \tag{5.32}$$

Proof. Since $\mathsf{Ops}_{\mathrm{U}}$ decomposes as $\mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, there are two cases to consider.

• Case $Op_{\mathrm{U}} \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents. $K^{\bullet}$ and (5.15) fix the third component of v to w, and let the first and second components be t and u respectively. $R^{\bullet}_{Op}$ and (5.16) fix the second component of j to k and let the first component be i. Thus $v = (t, u, w)$ and $j = (i, k)$. Then, from $trm_{Op_{\mathrm{U}}}(v, j)$, $G(u, w) \wedge P_{Op}(i, k, u, w)$ holds by (5.4). Hence, by (5.12), $trm_{Op_{\mathrm{C}}}(w, k)$ holds as required.

• Case $Op_{\mathrm{U}} \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents. $K^{\bullet}$ and (5.15) fix the third component of v to w and let the first and second components be t and u respectively. Thus $v = (t, u, w)$. $R^{\bullet}_{Op}$ and (5.18) fix $j = k$. Then, from $trm_{Op_{\mathrm{U}}}(v, j)$, $trm_{Op_{\mathrm{C}}}(w, k)$ holds by (5.5). ■

5.2.3.5 The correctness PO

We show

$$\begin{aligned} &K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge trm_{Op_{\mathrm{U}}}(v, j) \wedge stp_{Op_{\mathrm{C}}}(w, k, w', q) \;\Rightarrow \\ &\quad (\exists\, v', p \bullet stp_{Op_{\mathrm{U}}}(v, j, v', p) \wedge K^{\bullet}(v', w') \wedge V^{\bullet}_{Op}(p, q))\ . \end{aligned} \tag{5.33}$$

Proof. Since $\mathsf{Ops}_{\mathrm{U}}$ decomposes as $\mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, there are two cases to consider.

• Case $Op_U \in \mathsf{Ops}_A$. Assume the antecedents. $trm_{Op_U}(v, j)$ and (5.4) fix the first component t of v to 0, $K^\bullet$ and (5.15) fix the third component to w, and let the second component be u. $R^\bullet_{Op}$ and (5.16) fix the second component of j to k and let the first component be i. Thus $v = (0, u, w)$ and $j = (i, k)$. From $trm_{Op_U}(v, j)$, by (5.4), $G(u, w)$ and $P_{Op}(i, k, u, w)$ hold. G and P_{Op}, together with stp_{Op_C} make up the antecedent of the Op PO for the retrenchment from Abs to $Conc$, (5.13). Hence $stp_{Op_A}(u, i, u', o)$ and $(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)$ hold for chosen values u', o. Let $v' = (t', u', w')$, $t' = 0$ and $p = (o, q)$. Then $stp_{Op_U}(v, j, v', p)$ holds by (5.2); and $K^\bullet(v', w')$ and $V^\bullet_{Op}(p, q)$ hold by (5.15) and (5.17) respectively.

• Case $Op_U \notin \mathsf{Ops}_A$. Assume the antecedents. $K^\bullet$ and (5.15) fix the third component of v to w and let the first and second components be t and u. Thus $v = (t, u, w)$. $R^\bullet_{Op}$ and (5.18) fix $j = k$. We also have $stp_{Op_C}(w, k, w', q)$. So, let us pick any state in Abs, u' say, any value from T, t' say, and set $v' = (t', u', w')$. Furthermore, let $p = q$. Then $stp_{Op_U}(v, j, v', p)$ holds by (5.3); and $K^\bullet(v', w')$ and $V^\bullet_{Op}(p, q)$ hold by (5.15) and (5.19) respectively.

■

5.2.3.6 The output finalisation PO

We show

$$V^\bullet_{Op}(p, q) \wedge FinOut_{Op_C}(q, n) \;\Rightarrow\; FinOut_{Op_U}(p, n)\ . \tag{5.34}$$

Proof. Since Ops_C decomposes as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op_C \in \mathsf{Ops}_A$. Assume the antecedents. By (5.17), $V^\bullet_{Op}$ fixes the second component of p to q and let the first be o. Thus $p = (o, q)$. Next, by (5.22), $q = n$. Thus $FinOut_{Op_U}(p, n)$ holds, by (5.24).

• Case $Op_C \notin \mathsf{Ops}_A$. Assume the antecedents. By (5.19), $p = q$ and, by (5.26), $q = n$. Thus $FinOut_{Op_U}(p, n)$ holds, by (5.28). ■

5.2.4 The relations of the retrenchment from *Abs* to *Conc*

In this section we define the relations of the retrenchment from *Abs* to *Conc* in terms of the relations for the retrenchment from *Abs* to *Univ* and the refinement from *Univ* to *Conc*, and prove that these definitions do recover the relations of the *Abs* to *Conc* retrenchment. Let

$$G(u, w) \;=\; H^{\bullet}(u, v) ⨾ K^{\bullet}(v, w)\ , \tag{5.35}$$

$$P_{Op}(i, k, u, w) \;=\; Q^{\bullet}_{Op}(i, j, u, v) ⨾ (R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w))\ , \tag{5.36}$$

$$\begin{aligned} &O_{Op}(o, q; u', w', i, k, u, w) \;= \\ &\quad N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) ⨾ (V^{\bullet}_{Op}(p, q) \wedge K^{\bullet}(v', w') \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w)) \end{aligned} \tag{5.37}$$

$$\begin{aligned} &C_{Op}(u', w', o, q; i, k, u, w) = \\ &\quad D^{\bullet}_{Op}(u', v', o, p; i, j, u, v) ⨾ (K^{\bullet}(v', w') \wedge V^{\bullet}_{Op}(p, q) \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w)) \end{aligned} \tag{5.38}$$

In the above $Op \in \mathsf{Ops}_{\mathrm{A}}$.

We show (5.35) and (5.37); the others are similar.

Proof. Consider (5.35) first. We expand the RHS.

$H^{\bullet}(u, v) ⨾ K^{\bullet}(v, w)$

= [meaning of composition]

$(\exists\, v \bullet H^{\bullet}(u, v) \wedge K^{\bullet}(v, w))$

= [by (5.6) and (5.15)]

$(\exists\, v \bullet H^{\bullet}(u, v) \wedge K^{\bullet}(v, w) \wedge v = (0, u, w))$

= [one-point rule]

$H^{\bullet}(u, (0, u, w)) \wedge K^{\bullet}((0, u, w), w)$

= [by (5.15)]

$H^{\bullet}(u, (0, u, w))$

= [by (5.6)]

$G(u, w)$

Now consider (5.37). Again, we expand the RHS.

$N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) ⨾ (V^{\bullet}_{Op}(p, q) \wedge K^{\bullet}(v', w') \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w))$

= [meaning of composition]

$(\exists\, p, v', j, v \bullet N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \wedge V^{\bullet}_{Op}(p, q) \wedge K^{\bullet}(v', w') \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w))$

= [by (5.8), (5.15), (5.16) and (5.17)]

$(\exists\, p, v', j, v \bullet N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \wedge V^{\bullet}_{Op}(p, q) \wedge K^{\bullet}(v', w') \wedge R^{\bullet}_{Op}(j, k) \wedge$
$\quad K^{\bullet}(v, w) \wedge p = (o, q) \wedge v' = (0, u', w') \wedge j = (i, k) \wedge v = (0, u, w))$

= [one-point rule]

$N^{\bullet}_{Op}(o, (o, q); u', (0, u', w'), i, (i, k), u, (0, u, w)) \wedge V^{\bullet}_{Op}((o, q), q) \wedge K^{\bullet}((0, u', w'), w') \wedge$
$\quad R^{\bullet}_{Op}((i, k), k) \wedge K^{\bullet}((0, u, w), w)$

= [by (5.15), (5.16) and (5.17)]

$N^{\bullet}_{Op}(o, (o, q); u', (0, u', w'), i, (i, k), u, (0, u, w))$

= [by (5.8)]

$O_{Op}(o, q; u', w', i, k, u, w)$

Thus $G = H^{\bullet} ⨾ K^{\bullet}$ and $O_{Op} = N^{\bullet}_{Op} ⨾ (V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})$. ■

5.2.5 Properties of *Univ*

Below we state properties (U1) to (U7) of *Univ*.

$$\begin{aligned}&(H^{\bullet}(u, v) \vee Q^{\bullet}_{Op}(..., u, v) \vee N^{\bullet}_{Op}(..., u, v) \vee D^{\bullet}_{Op}(..., u, v) \vee \\ &\qquad N^{\bullet}_{Op}(o, p; u, v, ...) \vee D^{\bullet}_{Op}(u, v, ...)) \wedge K^{\bullet}(v, w) \wedge \\ &\quad H^{\bullet}(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, w) \Rightarrow v = \underline{v}\end{aligned} \tag{U1}$$

$$\begin{aligned}&(Q^{\bullet}_{Op}(i, j, ...) \vee N^{\bullet}_{Op}(..., i, j, ...) \vee D^{\bullet}_{Op}(...; i, j, ...)) \wedge R^{\bullet}_{Op}(j, k) \wedge \\ &\quad Q^{\bullet}_{Op}(i, \underline{j}, ...) \wedge R^{\bullet}_{Op}(\underline{j}, k) \Rightarrow j = \underline{j}\end{aligned} \tag{U2}$$

$$FinOut_{Op_U}(p, n) \Rightarrow (\exists\, q \bullet q = n \wedge V^{\bullet}_{Op}(p, q)) \tag{U3}$$

For $Op \in \mathsf{Ops}_A$

$$\begin{aligned}&InitIn_{Op_U}(h, j) \Rightarrow (\exists\, i, k, u, v, w \bullet k = h \wedge Q^{\bullet}_{Op}(i, j, u, v) \wedge \\ &\quad H^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w))\end{aligned} \tag{U4}$$

For $Op \notin \mathsf{Ops}_A$

$$K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge trm_{Op_C}(w, k) \Rightarrow trm_{Op_U}(v, j) \tag{U5}$$

$$K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v', w') \wedge V^{\bullet}_{Op}(p, q) \wedge stp_{Op_U}(v, j, v', p) \Rightarrow$$
$$stp_{Op_C}(w, k, w', q) \qquad \text{(U6)}$$

$$InitIn_{Op_U}(h, j) \Rightarrow (\exists\, k \bullet k = h \wedge R^{\bullet}_{Op}(j, k)) \qquad \text{(U7)}$$

In the above, $Q^{\bullet}_{Op}(..., u, v)$ is shorthand for $(\exists\, i, j \bullet Q^{\bullet}_{Op}(i, j, u, v))$, and similarly so for the other relations. We now show these properties hold.

♦ (U1): $(H^{\bullet}(u, v) \vee Q^{\bullet}_{Op}(..., u, v) \vee N^{\bullet}_{Op}(..., u, v) \vee D^{\bullet}_{Op}(..., u, v) \vee$
$N^{\bullet}_{Op}(o, p; u, v, ...) \vee D^{\bullet}_{Op}(u, v, ...)) \wedge$
$K^{\bullet}(v, w) \wedge H^{\bullet}(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, w) \Rightarrow v = \underline{v}$.

Proof. Assume the antecedents and let $v = (\underline{t}, \underline{u}, \underline{w})$ and $\underline{v} = (\underline{\underline{t}}, \underline{\underline{u}}, \underline{\underline{w}})$. Each one of (5.6) and $H^{\bullet}(u, v)$; (5.7) and $Q^{\bullet}_{Op}(..., u, v)$; (5.8) and $N^{\bullet}_{Op}(..., u, v)$ or $N^{\bullet}_{Op}(o, p; u, v, ...)$; and (5.9) and $D^{\bullet}_{Op}(..., u, v)$ or $D^{\bullet}_{Op}(u, v, ...)$ assert that $\underline{u} = u$ and $\underline{t} = 0$. Similarly, from $H^{\bullet}(u, \underline{v})$ we get $\underline{\underline{u}} = u$ and $\underline{\underline{t}} = 0$. Thus $\underline{\underline{u}} = \underline{u}$ and $\underline{\underline{t}} = \underline{t}$. In addition, by (5.15), $K^{\bullet}(v, w)$ asserts that $\underline{w} = w$, while $K^{\bullet}(\underline{v}, w)$ asserts that $\underline{\underline{w}} = w$. Thus $\underline{\underline{w}} = \underline{w}$. It therefore follows that $v = \underline{v}$. ■

♦ (U2): $(Q^{\bullet}_{Op}(i, j, ...) \vee N^{\bullet}_{Op}(..., i, j, ...) \vee D^{\bullet}_{Op}(...; i, j, ...)) \wedge$
$R^{\bullet}_{Op}(j, k) \wedge Q^{\bullet}_{Op}(i, \underline{j}, ...) \wedge R^{\bullet}_{Op}(\underline{j}, k) \Rightarrow j = \underline{j}$.

Proof. Similar to (U1). ■

♦ (U3): $FinOut_{Op_U}(p, n) \Rightarrow (\exists\, q \bullet q = n \wedge V^{\bullet}_{Op}(p, q))$

Proof. Since $Op \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume $FinOut_{Op_U}(p, n)$ with $p = (o, q)$. Now, by (5.17), $V^{\bullet}_{Op}(p, q)$ holds. Consequently, because (5.24) says $q = n$, we are done. ■

• Case $Op \notin \mathsf{Ops}_A$. Assume $FinOut_{Op_U}(p, n)$. By (5.28), $p = n$. Let $q = n$. Then, by (5.19), $V^{\bullet}_{Op}(p, q)$ holds, so we are done. ■

♦ (U4): $InitIn_{Op_U}(h, j) \Rightarrow$
$(\exists\, i, k, u, v, w \bullet k = h \wedge Q^{\bullet}_{Op}(i, j, u, v) \wedge H^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v, w))$

Proof. Assume $InitIn_{Op_U}(h, j)$. Using (5.21) we derive i, k, u and w for which $P_{Op}(i, k, u, w)$ and $G(u, w)$ hold, with $k = h$ and $j = (i, k)$. Let $v = (t, u, w)$ and $t = 0$. Then $Q^{\bullet}_{Op}(i, j, u, v)$ and $H^{\bullet}(u, v)$ hold, by (5.7) and (5.6) respectively. $R^{\bullet}_{Op}(j, k)$ and $K^{\bullet}(v, w)$ hold, by (5.16) and (5.15) respectively. We therefore have the consequent of (U4). Done. ■

♦ (U5): $K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge trm_{Op_C}(w, k) \Rightarrow trm_{Op_U}(v, j)$.

Proof. Assume the antecedents. $K^{\bullet}(v, w)$ and (5.15) fix the third component of v to w. Let the first and second be t and u. Thus $v = (t, u, w)$. $R^{\bullet}_{Op}(j, k)$ and (5.18) fix $j = k$. Therefore, since $trm_{Op_C}(w, k)$ holds, $trm_{Op_U}(v, j)$ holds by (5.5). ■

♦ (U6): $K^{\bullet}(v, w) \wedge R^{\bullet}_{Op}(j, k) \wedge K^{\bullet}(v', w') \wedge V^{\bullet}_{Op}(p, q) \wedge stp_{Op_U}(v, j, v', p) \Rightarrow$
$stp_{Op_C}(w, k, w', q)$

Proof. Assume the antecedents. By (5.15), $K^{\bullet}(v, w)$ fixes the third component of v to w, and let the first and second components be t and u. Thus $v = (t, u, w)$. Similarly from $K^{\bullet}(v', w')$ we get $v' = (t', u', w')$. Furthermore, $R^{\bullet}_{Op}(j, k)$ and (5.18) set $j = k$, and $V^{\bullet}_{Op}(p, q)$ and (5.19) set $p = q$. Thus $stp_{Op_C}(w, k, w', q)$ follows from stp_{Op_U}, by (5.3), as required.
■

♦ (U7): $InitIn_{Op_U}(h, j) \Rightarrow (\exists\, k \bullet k = h \wedge R^{\bullet}_{Op}(j, k))$

Proof. Assume $InitIn_{Op_U}(h, j)$. By (5.27), $h = j$. Let $k = h$. Then $j = k$, and thus, by (5.18), $R^{\bullet}_{Op}(j, k)$ holds. ■

This completes part (1) of the theorem.

5.3 Proof for Part (2)

The systems which decompose the retrenchment must belong to a class defined by (X1) to (X7) below, and the condition that the retrieve, input and output relations for the refinement to *Conc* are total functions. To prove part (2) we must show that for *any* system *Xtra* in the class, there is a refinement from *Univ* to *Xtra*. We structure the proof as follows. In Section 5.3.1 we detail the components of *Xtra* and state properties (X1) to (X7). In Section 5.3.2 we define the relations K°, R°_{Op}, V°_{Op} and then prove that they are the retrieve,

input and output relations of the desired refinement. Finally, in Section 5.3.3, we show that the inclusions stated in part (2) hold.

5.3.1 The system *Xtra*

The system *Xtra* has operation names set $Op_X \in \mathsf{Ops}_X$, with $\mathsf{Ops}_X = \mathsf{Ops}_U$. The state space is $v\tilde{} \in \mathsf{V}\tilde{}$. For each Op_X, the input space is $j\tilde{} \in \mathsf{J}\tilde{}_{Op_X}$ and output space is $p\tilde{} \in \mathsf{P}\tilde{}_{Op_X}$. We will denote the initialisation predicate by $Init_X$ and the step relation by stp_{Op_X}.

Let the retrenchment from *Abs* to *Xtra* be given by retrieve relation $H\tilde{}$, and for each Op, within relation $Q\tilde{}$, output relation $N\tilde{}$ and concedes relation $D\tilde{}$. Let the refinement from *Xtra* to *Conc* be given by retrieve relation $K\tilde{}$, and for each Op, the input relation $R\tilde{}_{Op}$, the output relation $V\tilde{}_{Op}$, the input initialisation $InitIn_{Op_X}$ and the output finalisation $FinOut_{Op_X}$. Let $InitIn_{Op_X}$ and $FinOut_{Op_X}$ be total and $K\tilde{}$, $R\tilde{}_{Op}$, $V\tilde{}_{Op}$ be total functions.

Let *Xtra* have properties (X1) to (X7) given below.

$$\begin{aligned}&(H\tilde{}(u, v\tilde{}) \vee Q\tilde{}_{Op}(..., u, v\tilde{}) \vee N\tilde{}_{Op}(..., u, v\tilde{}) \vee D\tilde{}_{Op}(..., u, v\tilde{}) \vee \\ &\qquad N\tilde{}_{Op}(o, p\tilde{}; u, v\tilde{}, ...) \vee D\tilde{}_{Op}(u, v\tilde{}, ...)) \wedge K\tilde{}(v\tilde{}, w) \wedge \\ &\quad H\tilde{}(u, \underline{v}\tilde{}) \wedge K\tilde{}(\underline{v}\tilde{}, w) \;\Rightarrow\; v\tilde{} = \underline{v}\tilde{}\end{aligned} \tag{X1}$$

$$\begin{aligned}&(Q\tilde{}_{Op}(i, j\tilde{}, ...) \vee N\tilde{}_{Op}(..., i, j\tilde{}, ...) \vee D\tilde{}_{Op}(...; i, j\tilde{}, ...)) \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge \\ &\quad Q\tilde{}_{Op}(i, \underline{j}\tilde{}, ...) \wedge R\tilde{}_{Op}(\underline{j}\tilde{}, k) \;\Rightarrow\; j\tilde{} = \underline{j}\tilde{}\end{aligned} \tag{X2}$$

$$FinOut_{Op_X}(p\tilde{}, n) \;\Rightarrow\; (\exists\, q \bullet q = n \wedge V\tilde{}_{Op}(p\tilde{}, q)) \tag{X3}$$

For $Op \in \mathsf{Ops}_A$

$$\begin{aligned}&InitIn_{Op_X}(h, j\tilde{}) \;\Rightarrow\; (\exists\, i, k, u, v\tilde{}, w \bullet k = h \wedge Q\tilde{}_{Op}(i, j\tilde{}, u, v\tilde{}) \wedge \\ &\quad H\tilde{}(u, v\tilde{}) \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge K\tilde{}_{Op}(v\tilde{}, w))\end{aligned} \tag{X4}$$

For $Op \notin \mathsf{Ops}_A$

$$K\tilde{}(v\tilde{}, w) \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge trm_{Op_C}(w, k) \;\Rightarrow\; trm_{Op_X}(v\tilde{}, j\tilde{}) \tag{X5}$$

$$\begin{aligned}&K\tilde{}(v\tilde{}, w) \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge K\tilde{}(v\tilde{}', w') \wedge V\tilde{}_{Op}(p\tilde{}, q) \wedge stp_{Op_X}(v\tilde{}, j\tilde{}, v\tilde{}', p\tilde{}) \;\Rightarrow \\ &\quad stp_{Op_C}(w, k, w', q)\end{aligned} \tag{X6}$$

$$InitIn_{Op_X}(h, j\tilde{}) \Rightarrow (\exists\, k \bullet k = h \wedge R\tilde{}_{Op}(j\tilde{}, k)) \qquad \text{(X7)}$$

Notice properties (U1) to (U7) are instances of (X1) to (X7) respectively when $V\tilde{} = V$, $J\tilde{} = J$ and $P\tilde{} = P$. In addition, $K^{\bullet}$, $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ are total functions, just like $K\tilde{}$, $R\tilde{}_{Op}$ and $V\tilde{}_{Op}$. Hence *Univ* and *Xtra* belong to the same class of systems which factorise the retrenchment from *Abs* to *Conc*.

5.3.2 The refinement from *Univ* to *Xtra*

To show *Xtra* is a refinement of *Univ* we first define the component relations and then show that the refinement POs hold.

5.3.2.1 The component relations

We define the retrieve relation $K°$, and for each *Op*, the input relation $R°_{Op}$ and output relation $V°_{Op}$ for the refinement from *Univ* to *Xtra*.

$$K°(v, v\tilde{}) = K°((t, u, w), v\tilde{}) = (\,(t = 0 \wedge G(u, w) \Rightarrow H\tilde{}(u, v\tilde{}))\, \wedge K\tilde{}(v\tilde{}, w)\,)\,. \qquad (5.39)$$

For $Op \in \mathrm{Ops}_A$

$$R°_{Op}(j, j\tilde{}) = R°_{Op}((i, k), j\tilde{}) = (\,(\forall\, u, w, v\tilde{} \bullet P_{Op}(i, k, u, w) \wedge H\tilde{}(u, v\tilde{}) \wedge K\tilde{}(v\tilde{}, w) \Rightarrow Q\tilde{}_{Op}(i, j\tilde{}, u, v\tilde{}))\, \wedge R\tilde{}_{Op}(j\tilde{}, k)\,)\,, \qquad (5.40)$$

$$V°_{Op}(p, p\tilde{}) = V°_{Op}((o, q), p\tilde{}) = V\tilde{}_{Op}(p\tilde{}, q)\,. \qquad (5.41)$$

For $Op \notin \mathrm{Ops}_A$

$$R°_{Op}(j, j\tilde{}) = (\,j = k \wedge R\tilde{}_{Op}(j\tilde{}, k)\,)\,, \qquad (5.42)$$

$$V°_{Op}(p, p\tilde{}) = (\,p = q \wedge V\tilde{}_{Op}(p\tilde{}, q)\,)\,. \qquad (5.43)$$

5.3.2.2 The input initialisation PO

We show

$$InitIn_{Op_X}(h, j\tilde{}) \Rightarrow (\exists\, j \bullet InitIn_{Op_U}(h, j) \wedge R°_{Op}(j, j\tilde{}))\,. \qquad (5.44)$$

Proof. Since Ops_X decomposes as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op_X \in \mathsf{Ops}_A$. Assume $InitIn_{Op_X}(h, \tilde{j})$. By (X4), we derive i, k, u, $\tilde{v}$ and w, such that $\tilde{Q}_{Op}(i, \tilde{j}, u, \tilde{v})$, $\tilde{H}(u, \tilde{v})$, $\tilde{R}_{Op}(\tilde{j}, k)$ and $\tilde{K}_{Op}(\tilde{v}, w)$ hold, with $k = h$. Then, $\tilde{Q}_{Op}(i, \tilde{j}, u, \tilde{v}) ⨟ (\tilde{R}_{Op}(\tilde{j}, k) \wedge \tilde{K}_{Op}(\tilde{v}, w))$ gives $P_{Op}(i, k, u, w)$ and $\tilde{H}(u, \tilde{v}) ⨟ \tilde{K}_{Op}(\tilde{v}, w)$ gives $G(u, w)$. Let $j = (i, k)$. Hence $InitIn_{Op_U}(h, j)$ holds, by (5.23).

It remains to show $R^\circ_{Op}(j, \tilde{j})$. We take the two conjuncts of (5.40) in turn. To establish the first conjunct assume $P_{Op}(i, k, \underline{u}, \underline{w}) \wedge \tilde{H}(\underline{u}, \underline{\tilde{v}}) \wedge \tilde{K}(\underline{\tilde{v}}, \underline{w})$. We require $\tilde{Q}_{Op}(i, \tilde{j}, \underline{u}, \underline{\tilde{v}})$. Now, $P_{Op}(i, k, \underline{u}, \underline{w}) = \tilde{Q}_{Op}(i, \underline{\tilde{j}}, \underline{u}, \underline{\tilde{v}}) ⨟ (\tilde{R}_{Op}(\underline{\tilde{j}}, k) \wedge \tilde{K}(\underline{\tilde{v}}, \underline{w}))$. Accordingly, we pick witnesses $\underline{\tilde{j}}$ and $\underline{\tilde{v}}$ for which $\tilde{Q}_{Op}(i, \underline{\tilde{j}}, \underline{u}, \underline{\tilde{v}})$, $\tilde{R}_{Op}(\underline{\tilde{j}}, k)$ and $\tilde{K}(\underline{\tilde{v}}, \underline{w})$ hold. Then, by (X1), $\underline{\tilde{v}} = \underline{\tilde{v}}$, and, by (X2), $\underline{\tilde{j}} = \tilde{j}$. Thus $\tilde{Q}_{Op}(i, \underline{\tilde{j}}, \underline{u}, \underline{\tilde{v}}) = \tilde{Q}_{Op}(i, \tilde{j}, \underline{u}, \underline{\tilde{v}})$, as required. The second conjunct is immediate because we have $\tilde{R}_{Op}(\tilde{j}, k)$. We are done.

• Case $Op_X \notin \mathsf{Ops}_A$. Assume $InitIn_{Op_X}(h, \tilde{j})$. By (X7), we derive k such that $\tilde{R}_{Op}(\tilde{j}, k)$ holds, with $k = h$. Let $j = h$. Then $InitIn_{Op_U}(h, j)$ and $R^\circ_{Op}(j, \tilde{j})$ are true, by (5.27) and (5.42) respectively. ■

5.3.2.3 The initialisation PO

We show

$$Init_X(\tilde{v}') \Rightarrow (\exists\, v' \bullet Init_U(v') \wedge K^\circ(v', \tilde{v}')) \,. \tag{5.45}$$

Proof. Assume $Init_X(\tilde{v}')$. Since we have $Init_X(\tilde{v}')$, the Init PO for the retrenchment from *Abs* to *Xtra*,

$$Init_X(\tilde{v}') \Rightarrow (\exists\, u' \bullet Init_A(u') \wedge \tilde{H}(u', \tilde{v}')) \,, \tag{5.46}$$

gives $Init_A(u')$ and $\tilde{H}(u', \tilde{v}')$. Now $\tilde{K}$ is total. Therefore, there is a state, say w', for which $\tilde{K}(\tilde{v}', w')$ holds. But then, by the composition $\tilde{H}'; \tilde{K}'$ it follows that $G(u', w')$ must also hold. Let $v' = (t', u', w')$ and $t' = 0$. Then $Init_U(v')$ holds by (5.1). Finally, since both $(t' = 0 \wedge G(u', w') \Rightarrow \tilde{H}(u', \tilde{v}'))$ and $\tilde{K}(\tilde{v}', w')$ hold, $K^\circ(v', \tilde{v}')$ holds by (5.39). ■

5.3.2.4 The applicability PO

We show

$$K^\circ(v, \tilde{v}) \wedge R^\circ_{Op}(j, \tilde{j}) \wedge trm_{Op_U}(v, j) \;\Rightarrow\; trm_{Op_X}(\tilde{v}, \tilde{j}) \,. \tag{5.47}$$

Proof. Since Ops_U decomposes as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op_U \in \mathsf{Ops}_A$. Assume the antecedents with $v = (t, u, w)$ and $j = (i, k)$. From $trm_{Op_U}(v, j)$, by (5.4), we have $t = 0$, $G(u, w)$, $P_{Op}(i, k, u, w)$ and $trm_{Op_A}(u, i)$. Now, $K^\circ(v, \tilde{v})$, $t = 0$ and $G(u, w)$ give $\tilde{H}(u, \tilde{v})$ and $\tilde{K}(\tilde{v}, w)$, by (5.39). Also, $R^\circ_{Op}(j, \tilde{j})$, $P_{Op}(i, k, u, w)$, $\tilde{H}(u, \tilde{v})$ and $\tilde{K}(\tilde{v}, w)$ give $\tilde{Q}_{Op}(i, \tilde{j}, u, \tilde{v})$ and $\tilde{R}_{Op}(\tilde{j}, k)$, by (5.40). We now have all the antecedents of the Term PO for the retrenchment from *Abs* to *Xtra*,

$$\tilde{H}(u, \tilde{v}) \wedge \tilde{Q}_{Op}(i, \tilde{j}, u, \tilde{v}) \;\Rightarrow\; trm_{Op_X}(\tilde{v}, \tilde{j}) \,. \tag{5.48}$$

Therefore $trm_{Op_X}(\tilde{v}, \tilde{j})$ holds as required.

• Case $Op_U \notin \mathsf{Ops}_A$. Assume the antecedents with $v = (t, u, w)$ and $j = k$. From $K^\circ(v, \tilde{v})$, by (5.39), we get $\tilde{K}(\tilde{v}, w)$; from $R^\circ_{Op}(j, \tilde{j})$, by (5.42), we get $\tilde{R}_{Op}(\tilde{j}, k)$; and from $trm_{Op_U}(v, j)$, by (5.5), we get $trm_{Op_C}(w, k)$. Therefore we have all the antecedents of (X5). Hence $trm_{Op_X}(\tilde{v}, \tilde{j})$ holds as required. ■

5.3.2.5 The correctness PO

We show

$$\begin{aligned} &K^\circ(v, \tilde{v}) \wedge R^\circ_{Op}(j, \tilde{j}) \wedge trm_{Op_U}(v, j) \wedge stp_{Op_X}(\tilde{v}, \tilde{j}, \tilde{v}', \tilde{p}) \;\Rightarrow \\ &\quad (\exists\, v', p \bullet stp_{Op_U}(v, j, v', p) \wedge K^\circ(v', \tilde{v}') \wedge V^\circ_{Op}(p, \tilde{p})) \,. \end{aligned} \tag{5.49}$$

Proof. Since Ops_U and Ops_X decompose as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume the antecedents and let $v = (t, u, w)$ and $j = (i, k)$. First we shall derive $stp_{Op_U}(v, j, v', p)$. We proceed as follows. From $trm_{Op_U}(v, j)$ we get $t = 0$, $G(u, w)$ and $P_{Op}(i, k, u, w)$ by (5.4). Thus, because we have $t = 0$, $G(u, w)$ and $K^\circ(v, \tilde{v})$, we get

$H\tilde{}(u, v\tilde{})$ and $K\tilde{}(v\tilde{}, w)$ by (5.39). At this point we have $R°_{Op}(j, j\tilde{})$, $P_{Op}(i, k, u, w)$, $H\tilde{}(u, v\tilde{})$ and $K\tilde{}(v\tilde{}, w)$. Hence we get $Q\tilde{}_{Op}(i, j\tilde{}, u, v\tilde{})$ and $R\tilde{}_{Op}(j\tilde{}, k)$, by (5.40). Now, $H\tilde{}(u, v\tilde{})$, $Q\tilde{}_{Op}(i, j\tilde{}, u, v\tilde{})$ and $stp_{Op_X}(v\tilde{}, j\tilde{}, v\tilde{}', p\tilde{})$ make up the antecedent of the Op PO for the retrenchment from *Abs* to *Xtra*,

$$
\begin{aligned}
& H\tilde{}(u, v\tilde{}) \wedge Q\tilde{}_{Op}(i, j\tilde{}, u, v\tilde{}) \wedge stp_{Op_X}(v\tilde{}, j\tilde{}, v\tilde{}', p\tilde{}) \;\Rightarrow \\
& \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\
& \qquad (\,(H\tilde{}(u', v\tilde{}') \wedge N\tilde{}_{Op}(o, p\tilde{}; u', v\tilde{}', i, j\tilde{}, u, v\tilde{})) \vee \\
& \qquad D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{})\,)) \,. \qquad (5.50)
\end{aligned}
$$

Therefore for chosen values, u' and o, $stp_{Op_A}(u, i, u', o)$ and $(H\tilde{}(u', v\tilde{}') \wedge N\tilde{}_{Op}(o, p\tilde{}; u', v\tilde{}', i, j\tilde{}, u, v\tilde{})) \vee D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{})$ hold. Now because $K\tilde{}$ and $V\tilde{}_{Op}$ are total, given that we have $v\tilde{}'$ and $p\tilde{}$, there must be values w' and q say, such that $K\tilde{}(v\tilde{}', w')$ and $V\tilde{}_{Op}(p\tilde{}, q)$ hold. Let $v' = (t', u', w')$, $t' = 0$ and $p = (o, q)$.

If we examine (5.2) we see that we have all the necessary pieces except for $(G' \wedge O_{Op}) \vee C_{Op}$. We can derive this from $(H\tilde{}(u', v\tilde{}') \wedge N\tilde{}_{Op}(o, p\tilde{}; u', v\tilde{}', i, j\tilde{}, u, v\tilde{})) \vee D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{})$. Suppose $H\tilde{}(u', v\tilde{}') \wedge N\tilde{}_{Op}(o, p\tilde{}; u', v\tilde{}', i, j\tilde{}, u, v\tilde{})$ holds. Then $H\tilde{}(u', v\tilde{}') ⨾ K\tilde{}(v\tilde{}', w')$ gives $G(u', w')$, and $N\tilde{}_{Op}(o, p\tilde{}; u', v\tilde{}', i, j\tilde{}, u, v\tilde{}) ⨾ (V\tilde{}_{Op}(p\tilde{}, q) \wedge K\tilde{}(v\tilde{}', w') \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge K\tilde{}(v\tilde{}, w))$ gives $O_{Op}(o, q; u', w', i, k, u, w)$. On the other hand suppose $D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{})$ holds. Then $D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{}) ⨾ (K\tilde{}(v\tilde{}', w') \wedge V\tilde{}_{Op}(p\tilde{}, q) \wedge R\tilde{}_{Op}(j\tilde{}, k) \wedge K\tilde{}(v\tilde{}, w))$ gives $C_{Op}(u', w', o, q; i, k, u, w)$. Thus $(G' \wedge O_{Op}) \vee C_{Op}$ holds and therefore so does $stp_{Op_U}(v, j, v', p)$. The reader may have noticed we could obtain $stp_{Op_U}(v, j, v', p)$ directly from $trm_{Op_U}(v, j)$. Unfortunately, we then do not have enough information to establish $K°'$, which we do next.

We already have $K\tilde{}(v\tilde{}', w')$, so all we need to establish is the first conjunct of (5.39). Thus assume the antecedent $G(u', w')$; t' is already 0. We need to derive $H\tilde{}(u', v\tilde{}')$. From $G(u', w')$, by composition, there must be some value, $\underline{v}\tilde{}'$ say, such that $H\tilde{}(u', \underline{v}\tilde{}')$ and $K\tilde{}(\underline{v}\tilde{}', w')$ hold. But $H\tilde{}(u', v\tilde{}') \vee D\tilde{}_{Op}(u', v\tilde{}', o, p\tilde{}; i, j\tilde{}, u, v\tilde{})$ and $K\tilde{}(v\tilde{}', w')$ hold. Hence by (X1), $\underline{v}\tilde{}' = v\tilde{}'$. So because $H\tilde{}(u', \underline{v}\tilde{}')$ holds, $H\tilde{}(u', v\tilde{}')$ holds as required. The final piece, $V°_{Op}(p, p\tilde{})$, is easy to show. We have $V\tilde{}_{Op}(p\tilde{}, q)$, thus $V°_{Op}$ holds by (5.41). This completes the proof for this case.

• Case $Op \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents and let $v = (t, u, w)$ and $j = k$. From $K^{\circ}(v, \tilde{v})$, by (5.39), we get $\tilde{K}(\tilde{v}, w)$; and from $R^{\circ}_{Op}(j, \tilde{j})$, by (5.42), we get $\tilde{R}_{Op}(\tilde{j}, k)$. Now, because $\tilde{K}$ and $\tilde{V}_{Op}$ are total, there must be values, w' and q say, such that $\tilde{K}(\tilde{v}', w')$ and $\tilde{V}_{Op}(\tilde{p}, q)$ hold. Hence by (X6), $stp_{Op_{\mathrm{C}}}(w, k, w', q)$ holds. Let $v' = (t', u', w')$, $t' = 1$ and $p = q$. Then by (5.3) $stp_{Op_{\mathrm{U}}}(v, j, v', p)$ holds.

It remains to show $K^{\circ}(v', \tilde{v}')$ and $V^{\circ}_{Op}(p, \tilde{p})$. Take $K^{\circ}(v', \tilde{v}')$. Since $t' = 1$, the first conjunct of (5.39) is true. We also have $\tilde{K}(\tilde{v}', w')$. Thus the second conjunct is also true. Therefore $K^{\circ}(v', \tilde{v}')$ holds. Finally, since $p = q$ and we have $\tilde{V}_{Op}(\tilde{p}, q)$, then $V^{\circ}_{Op}(p, \tilde{p})$ holds by (5.43). ■

5.3.2.6 The output finalisation PO

We show

$$V^{\circ}_{Op}(p, \tilde{p}) \wedge FinOut_{Op_{\mathrm{X}}}(\tilde{p}, n) \;\Rightarrow\; FinOut_{Op_{\mathrm{U}}}(p, n)\ . \tag{5.51}$$

Proof. Since $\mathsf{Ops}_{\mathrm{X}}$ decomposes as $\mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, there are two cases to consider.

• Case $Op_{\mathrm{X}} \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents and let $p = (o, q)$. From $V^{\circ}_{Op}(p, \tilde{p})$, by (5.41), we get $\tilde{V}_{Op}(\tilde{p}, q)$. From $FinOut_{Op_{\mathrm{X}}}(\tilde{p}, n)$, by (X3), we get $\tilde{V}_{Op}(\tilde{p}, \underline{q})$, with $\underline{q} = n$. Hence, as $\tilde{V}_{Op}$ is a function, $q = \underline{q}$. Therefore, $FinOut_{Op_{\mathrm{U}}}(p, n)$ holds, by (5.24).

• Case $Op_{\mathrm{X}} \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents. From $V^{\circ}_{Op}(p, \tilde{p})$, by (5.43), we get $\tilde{V}_{Op}(\tilde{p}, q)$, with $p = q$. From $FinOut_{Op_{\mathrm{X}}}(\tilde{p}, n)$, by (X3), we get $\tilde{V}_{Op}(\tilde{p}, \underline{q})$, with $\underline{q} = n$. Hence, as $\tilde{V}_{Op}$ is a function, $q = \underline{q}$. Therefore, $FinOut_{Op_{\mathrm{U}}}(p, n)$ holds, by (5.28). ■

5.3.3 The inclusions

Below we list the inclusions of part (2) of the theorem in detail.

$$\tilde{H}(u, \tilde{v}) \Rightarrow H^{\bullet}(u, v) \fatsemi K^{\circ}(v, \tilde{v}) \tag{5.52}$$

$$\tilde{Q}_{Op}(i, \tilde{j}, u, \tilde{v}) \Rightarrow Q^{\bullet}_{Op}(i, j, u, v) \fatsemi (R^{\circ}_{Op}(j, \tilde{j}) \wedge K^{\circ}(v, \tilde{v})) \tag{5.53}$$

$$N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim}) \Rightarrow$$
$$N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \fatsemi (V^{\circ}_{Op}(p, p^{\sim}) \wedge K^{\circ}(v', v^{\sim\prime}) \wedge R^{\circ}_{Op}(j, j^{\sim}) \wedge K^{\circ}(v, v^{\sim})) \tag{5.54}$$

$$D^{\sim}_{Op}(u', v^{\sim\prime}, o, p^{\sim}; i, j^{\sim}, u, v^{\sim}) \Rightarrow$$
$$D^{\bullet}_{Op}(u', v'; o, p, i, j, u, v) \fatsemi (K^{\circ}(v', v^{\sim\prime}) \wedge V^{\circ}_{Op}(p, p^{\sim}) \wedge R^{\circ}_{Op}(j, j^{\sim}) \wedge K^{\circ}(v, v^{\sim})) \tag{5.55}$$

$$K^{\circ}(v, v^{\sim}) \fatsemi K^{\sim}(v^{\sim}, w) \Rightarrow K^{\bullet}(v, w) \tag{5.56}$$

$$R^{\circ}_{Op}(j, j^{\sim}) \fatsemi R^{\sim}_{Op}(j^{\sim}, k) \Rightarrow R^{\bullet}_{Op}(j, k) \tag{5.57}$$

$$V^{\circ}(p, p^{\sim}) \fatsemi V^{\sim}_{Op}(p^{\sim}, q) \Rightarrow V^{\bullet}_{Op}(p, q)\ . \tag{5.58}$$

We now show these inclusions hold.

♦ (5.52): $H^{\sim}(u, v^{\sim}) \Rightarrow H^{\bullet}(u, v) \fatsemi K^{\circ}(v, v^{\sim})$.

Proof. Assume the antecedent $H^{\sim}(u, v^{\sim})$. Since $K^{\sim}$ is total there must be a state, w say, such that $K^{\sim}(v^{\sim}, w)$ holds. Therefore from the composition $H^{\sim}(u, v^{\sim}) \fatsemi K^{\sim}(v^{\sim}, w)$, we know $G(u, w)$ also holds. Let $v = (t, u, w)$ and $t = 0$. Then $H^{\bullet}(u, v)$ holds by (5.6). Furthermore, because both $(t = 0 \wedge G(u, w))$ and $H^{\sim}(u, v^{\sim})$ hold, $K^{\circ}(v, v^{\sim})$ holds by (5.39). Thus $H^{\sim}(u, v^{\sim})$ does indeed imply $H^{\bullet}(u, v) \fatsemi K^{\circ}(v, v^{\sim})$. ■

♦ (5.53): $Q^{\sim}_{Op}(i, j^{\sim}, u, v^{\sim}) \Rightarrow Q^{\bullet}_{Op}(i, j, u, v) \fatsemi (R^{\circ}_{Op}(j, j^{\sim}) \wedge K^{\circ}(v, v^{\sim}))$.

Proof. Assume the antecedent $Q^{\sim}_{Op}(i, j^{\sim}, u, v^{\sim})$. Now, both $K^{\sim}$ and $R^{\sim}_{Op}$ are total, so there must be values, w and k say, such that $K^{\sim}(v^{\sim}, w)$ and $R^{\sim}_{Op}(j^{\sim}, k)$ hold. Therefore, from the composition $Q^{\sim}_{Op}(i, j^{\sim}, u, v^{\sim}) \fatsemi (R^{\sim}_{Op}(j^{\sim}, k) \wedge K^{\sim}(v^{\sim}, w))$, we know that $P_{Op}(i, k, u, w)$ also holds. Let $v = (t, u, w)$, $t = 0$ and $j = (i, k)$. Then $Q^{\bullet}_{Op}(i, j, u, v)$ holds by (5.7).

It remains to show $R^{\circ}_{Op}(j, j^{\sim})$ and $K^{\circ}(v, v^{\sim})$. We take R°_{Op} first. The second conjunct of (5.40) is true because we have $R^{\sim}_{Op}(j^{\sim}, k)$. To prove the first conjunct assume $P_{Op}(i, k, \underline{u}, \underline{w})$, $H^{\sim}(\underline{u}, \underline{v}^{\sim})$ and $K^{\sim}(\underline{v}^{\sim}, \underline{w})$. We need to derive $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{v}^{\sim})$. From $P_{Op}(i, k, \underline{u}, \underline{w})$ we know that $Q^{\sim}_{Op}(i, \underline{j}^{\sim}, \underline{u}, \underline{v}^{\sim}) \fatsemi (R^{\sim}_{Op}(\underline{j}^{\sim}, k) \wedge K^{\sim}(\underline{v}^{\sim}, \underline{w}))$ holds. But we also have $Q^{\sim}_{Op}(i, j^{\sim}, u, v^{\sim})$ and $R^{\sim}_{Op}(j^{\sim}, k)$. Therefore, by (X2), $\underline{j}^{\sim} = j^{\sim}$. Hence $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{v}^{\sim})$ holds. This, to-

gether with $K^{\sim}(\underline{\underline{v}}^{\sim}, \underline{w})$, $H^{\sim}(\underline{u}, \underline{v}^{\sim})$ and $K^{\sim}(\underline{v}^{\sim}, \underline{w})$ means that we can use (X1) to infer $\underline{\underline{v}}^{\sim} = \underline{v}^{\sim}$. Hence $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{v}^{\sim})$ holds as required.

We turn to $K^{\circ}(v, v^{\sim})$. The second conjunct of (5.39) is true because we have $K^{\sim}(v^{\sim}, w)$. To prove the first conjunct assume $G(u, w)$; t is already 0. We need to derive $H^{\sim}(u, v^{\sim})$. From $G(u, w)$ we know that $H^{\sim}(u, \underline{v}^{\sim}) \fatsemi K^{\sim}(\underline{v}^{\sim}, w)$ holds. But we also have $Q^{\sim}_{Op}(i, j^{\sim}, u, v^{\sim})$ and $K^{\sim}(v^{\sim}, w)$. Therefore, by (X1), $\underline{v}^{\sim} = v^{\sim}$. Hence $H^{\sim}(u, v^{\sim})$ holds as required. ■

♦ (5.54): $N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim}) \Rightarrow$

$$N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \fatsemi (V^{\circ}_{Op}(p, p^{\sim}) \wedge K^{\circ}(v', v^{\sim\prime}) \wedge R^{\circ}_{Op}(j, j^{\sim}) \wedge K^{\circ}(v, v^{\sim})) .$$

Proof. Assume the antecedent $N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim})$. Now, $K^{\sim}$, $R^{\sim}_{Op}$ and $V^{\sim}_{Op}$ are total, so there must be values, q, w', k and w say, such that $V^{\sim}_{Op}(p^{\sim}, q)$, $K^{\sim}(v^{\sim\prime}, w')$, $R^{\sim}_{Op}(j^{\sim}, k)$ and $K^{\sim}(v^{\sim}, w)$ hold. Therefore, from the composition $N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim}) \fatsemi (V^{\sim}_{Op}(p^{\sim}, q) \wedge K^{\sim}(v^{\sim\prime}, w') \wedge R^{\sim}_{Op}(j^{\sim}, k) \wedge K^{\sim}(v^{\sim}, w))$, we know that $O_{Op}(o, q; u', w', i, k, u, w)$ also holds. Let $v = (t, u, w)$, $j = (i, k)$, $v' = (t', u', w')$, $p = (o, q)$ and $t' = t = 0$. Then $N^{\bullet}_{Op}(o, p; u', v', i, j, u, v)$ holds by (5.8).

It remains to show $V^{\circ}_{Op}(p, p^{\sim})$, $K^{\circ}(v', v^{\sim\prime})$, $R^{\circ}_{Op}(j, j^{\sim})$ and $K^{\circ}(v, v^{\sim})$. Take $V^{\circ}_{Op}(p, p^{\sim})$. By (5.41) this holds because we have $V^{\sim}_{Op}(p^{\sim}, q)$.

For $K^{\circ}(v', v^{\sim\prime})$ we proceed as follows. The second conjunct of (5.39) is true because we have $K^{\sim}(v^{\sim\prime}, w')$. To prove the first conjunct assume $G(u', w')$; t' is already 0. We need to derive $H^{\sim}(u', v^{\sim\prime})$. From $G(u', w')$ we know that $H^{\sim}(u', \underline{\underline{v}}^{\sim\prime}) \fatsemi K^{\sim}(\underline{\underline{v}}^{\sim\prime}, w')$ holds. But we also have $N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim})$ and $K^{\sim}(v^{\sim\prime}, w')$. Therefore, by (X1), $\underline{\underline{v}}^{\sim\prime} = v^{\sim\prime}$. Hence $H^{\sim}(u', v^{\sim\prime})$ holds as required.

Next take $R^{\circ}_{Op}(j, j^{\sim})$. The second conjunct of (5.40) is true because we have $R^{\sim}_{Op}(j^{\sim}, k)$. To prove the first conjunct assume $P_{Op}(i, k, \underline{u}, \underline{w})$, $H^{\sim}(\underline{u}, \underline{v}^{\sim})$ and $K^{\sim}(\underline{v}^{\sim}, \underline{w})$. We need to derive $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{v}^{\sim})$. From $P_{Op}(i, k, \underline{u}, \underline{w})$ we know that $Q^{\sim}_{Op}(i, \underline{i}^{\sim}, \underline{u}, \underline{\underline{v}}^{\sim}) \fatsemi (R^{\sim}_{Op}(\underline{i}^{\sim}, k) \wedge K^{\sim}(\underline{\underline{v}}^{\sim}, \underline{w}))$ holds. But we also have $N^{\sim}_{Op}(o, p^{\sim}; u', v^{\sim\prime}, i, j^{\sim}, u, v^{\sim})$ and $R^{\sim}_{Op}(j^{\sim}, k)$. Therefore, by (X2), $\underline{i}^{\sim} = j^{\sim}$. Hence $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{\underline{v}}^{\sim})$ holds. This, together with $K^{\sim}(\underline{\underline{v}}^{\sim}, \underline{w})$, $H^{\sim}(\underline{u}, \underline{v}^{\sim})$ and $K^{\sim}(\underline{v}^{\sim}, \underline{w})$ means that we can use (X1) to infer $\underline{\underline{v}}^{\sim} = \underline{v}^{\sim}$. Hence $Q^{\sim}_{Op}(i, j^{\sim}, \underline{u}, \underline{v}^{\sim})$ holds as required.

Finally we show $K^{\circ}(v, \tilde{v})$. The second conjunct of (5.39) is true because we have $K^{\sim}(\tilde{v}, w)$. To prove the first conjunct assume $G(u, w)$; t is already 0. We need to derive $H^{\sim}(u, \tilde{v})$. From $G(u, w)$ we know that $H^{\sim}(u, \underline{\underline{\tilde{v}}})\fatsemi K^{\sim}(\underline{\underline{\tilde{v}}}, w)$ holds. But we also have $N^{\sim}_{Op}(o, \tilde{p}; u', \tilde{v}', i, \tilde{j}, u, \tilde{v})$ and $K^{\sim}(\tilde{v}, w)$. Therefore, by (X1), $\underline{\underline{\tilde{v}}} = \tilde{v}$. Hence $H^{\sim}(u, \tilde{v})$ holds as required.

Thus $N^{\sim}_{Op}(o, \tilde{p}; u', \tilde{v}', i, \tilde{j}, u, \tilde{v})$ does indeed imply $N^{\bullet}_{Op}(o, p; u', v', i, j, u, v)\fatsemi(V^{\circ}_{Op}(p, \tilde{p}) \wedge K^{\circ}(v', \tilde{v}') \wedge R^{\circ}_{Op}(j, \tilde{j}) \wedge K^{\circ}(v, \tilde{v}))$. ■

♦ (5.55): $D^{\sim}_{Op}(u', \tilde{v}', o, \tilde{p}; i, \tilde{j}, u, \tilde{v}) \Rightarrow$
$D^{\bullet}_{Op}(u', v'; o, p, i, j, u, v)\fatsemi(K^{\circ}(v', \tilde{v}') \wedge V^{\circ}_{Op}(p, \tilde{p}) \wedge R^{\circ}_{Op}(j, \tilde{j}) \wedge K^{\circ}(v, \tilde{v}))$.

Proof. Similar to (5.54). ■

♦ (5.56): $K^{\circ}(v, \tilde{v})\fatsemi K^{\sim}(\tilde{v}, w) \Rightarrow K^{\bullet}(v, w)$.

Proof. Assume the antecedents and let $v = (\underline{t}, \underline{u}, \underline{w})$. Then from $K^{\circ}(v, \tilde{v})$, by (5.56), $K^{\sim}(\tilde{v}, \underline{w})$ holds. But $K^{\sim}(\tilde{v}, w)$ also holds. Hence, as $K^{\sim}$ is a function, $\underline{w} = w$. Thus $v = (\underline{t}, \underline{u}, w)$. Therefore, by (5.15), $K^{\bullet}(v, w)$ holds as required. ■

♦ (5.57): $R^{\circ}_{Op}(j, \tilde{j})\fatsemi R^{\sim}_{Op}(\tilde{j}, k) \Rightarrow R^{\bullet}_{Op}(j, k)$.

Proof. Since $Op \in \mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents and let $j = (\underline{i}, \underline{k})$. Then from $R^{\circ}_{Op}(j, \tilde{j})$, by (5.40), $R^{\sim}_{Op}(\tilde{j}, \underline{k})$ holds. But $R^{\sim}_{Op}(\tilde{j}, k)$ also holds. Hence, as $R^{\sim}_{Op}$ is a function, $\underline{k} = k$. Thus $j = (\underline{i}, k)$. Therefore, by (5.16), $R^{\bullet}_{Op}(j, k)$ holds as required.

• Case $Op \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents. Then from $R^{\circ}_{Op}(j, \tilde{j})$, by (5.42), $R^{\sim}_{Op}(\tilde{j}, \underline{k})$ holds, with $j = \underline{k}$. But $R^{\sim}_{Op}(\tilde{j}, k)$ also holds. Hence, as $R^{\sim}_{Op}$ is a function, $\underline{k} = k$. Thus, as $j = \underline{k}$, then $j = k$. Therefore, by (5.18), $R^{\bullet}_{Op}(j, k)$ holds as required. ■

♦ (5.58): $V^{\circ}(p, \tilde{p})\fatsemi V^{\sim}_{Op}(\tilde{p}, q) \Rightarrow V^{\bullet}_{Op}(p, q)$.

Proof. Similar to (5.57). ■

5.4 Proof for Part (3)

Part (3) of the theorem follows readily by observing that for a system *Univ** having the same properties as *Univ*, there will be a refinement from *Univ* to *Univ** and a refinement from *Univ** to *Univ*. ☺ ■

This completes the proof of Theorem 5.1.

5.5 Idempotence

We claim *Univ* is at the level of abstraction of *Abs*. Additional evidence to support this assertion can be obtained by demonstrating that the application of the lifting construction to the *Abs* to *Univ* retrenchment (see Figure 5.2), yields a system *UUniv*, which essentially

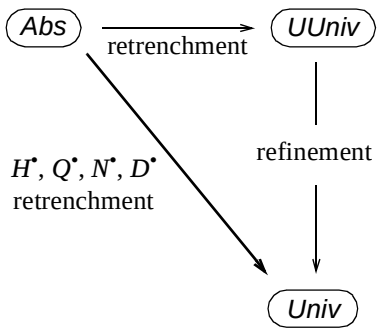


Figure 5.2: Applying the lifting construction to the *Abs* to *Univ* retrenchment.

is like *Univ* in character. The transitions of *UUniv* are given by

$$
\begin{aligned}
& stp_{Op_{\mathrm{UU}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \\
& = [(5.3) \text{ rewritten for } H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet} \text{ retrenchment}] \\
& \Big(\underline{v} = (\underline{t}, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v}' = (\underline{t}', u', v') \wedge \underline{p} = (o, p) \wedge \underline{t} = \underline{t}' = 0 \wedge \\
& \quad H^{\bullet}(u, v) \wedge Q^{\bullet}_{Op}(i, j, u, v) \wedge stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge \\
& \quad ((H^{\bullet}(u', v') \wedge N^{\bullet}_{Op}(o, p; u', v', i, j, u, v)) \vee D^{\bullet}_{Op}(u', v', o, p; i, j, u, v)) \Big) . \qquad (5.59)
\end{aligned}
$$

From this we get

$stp_{Op_{UU}}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$

= [expanding]

$$\begin{aligned}
&\Big(\underline{v} = (\underline{t}, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v}' = (\underline{t}', u', v') \wedge \underline{p} = (o, p) \wedge \underline{t} = \underline{t}' = 0 \wedge \\
&\quad v = (t, u, w) \wedge t = 0 \wedge G(u, w) \wedge \\
&\quad j = (i, k) \wedge v = (t, u, w) \wedge t = 0 \wedge P_{Op}(i, k, u, w) \wedge \\
&\quad stp_{Op_A}(u, i, u', o) \wedge \\
&\quad \big((v' = (t', u', w') \wedge t' = 0 \wedge G(u', w') \wedge \\
&\qquad p = (o, q) \wedge v' = (t', u', w') \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\
&\qquad O_{Op}(o, q; u', w', i, k, u, w)) \vee \\
&\qquad\quad (v' = (t', u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\
&\qquad\quad C_{Op}(u', w', o, q; i, k, u, w)) \big) \Big)
\end{aligned}$$

= [$a \wedge a \Leftrightarrow a$]

$$\begin{aligned}
&\Big(\underline{v} = (\underline{t}, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v}' = (\underline{t}', u', v') \wedge \underline{p} = (o, p) \wedge \underline{t} = \underline{t}' = 0 \wedge \\
&\quad v = (t, u, w) \wedge t = 0 \wedge G(u, w) \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge \\
&\quad \big((v' = (t', u', w') \wedge G(u', w') \wedge \\
&\qquad\quad p = (o, q) \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee \\
&\qquad (v' = (t', u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\
&\qquad\quad C_{Op}(u', w', o, q; i, k, u, w)) \big) \Big)
\end{aligned}$$

= [$(a \wedge b) \vee (a \wedge c) \Leftrightarrow a \wedge (a \vee c)$]

$$\begin{aligned}
&\Big(\underline{v} = (\underline{t}, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v}' = (\underline{t}', u', v') \wedge \underline{p} = (o, p) \wedge \underline{t} = \underline{t}' = 0 \wedge \\
&\quad v = (t, u, w) \wedge t = 0 \wedge G(u, w) \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge \\
&\quad v' = (t', u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (t, u, w) \wedge t = t' = 0 \wedge \\
&\quad \big((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w) \big) \Big)
\end{aligned}$$

= [rearranging, $a \wedge a \Leftrightarrow a$, $\underline{t} = t$, $\underline{t}' = t'$]

$$\begin{aligned}
&\Big(\underline{v} = (t, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v} = (t', u', w') \wedge \underline{p} = (o, p) \wedge \\
&\quad v = (t, u, w) \wedge j = (i, k) \wedge v' = (t', u', w') \wedge p = (o, q) \wedge \\
&\quad t = t' = 0 \wedge G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge \\
&\quad \big((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w) \big) \Big)
\end{aligned}$$

= [(5.3)]

$$\begin{aligned}
&\Big(\underline{v} = (t, u, v) \wedge \underline{j} = (i, j) \wedge \underline{v} = (t', u', w') \wedge \underline{p} = (o, p) \wedge \\
&\quad v = (t, u, w) \wedge j = (i, k) \wedge v' = (t', u', w') \wedge p = (o, q) \wedge \\
&\quad stp_{Op_U}(v, j, v', p) \Big)
\end{aligned}$$

= [substituting]

$$\big(\underline{v} = (t, u, (t, u, w)) \wedge \underline{i} = (i, (i, k)) \wedge \underline{v}' = (t', u', (t', u', w')) \wedge \underline{p} = (o, (o, q)) \wedge$$
$$stp_{Op_{\mathrm{U}}}((t, u, w), (i, k), (t', u', w'), (o, q)) \big) .$$

So we see that repeating the construction leads to a system whose data is that of *Univ* but with redundant duplications. Such a system is obviously interrefinable with *Univ* and hence equivalent to *Univ* for all our purposes.

5.6 Inside *Univ*

In Chapter 10 we will see retrenchment and the lifting construction applied to extend the Mondex Purse development. For now, we return to the Number Recycler and use it to illustrate the structure of *Univ*. Recall the abstract system *Abs* models a bin as a set to which we can add numbers using the operation *Add*. If a user tries to add a number already in the bin, it is thrown away and the system outputs the message GOT. The operation *Rem* allows an arbitrary number to be removed from the bin. We specify *Abs* below.

$$\mathsf{U} = \mathbb{P}(\mathbb{N}),\ \mathsf{I}_{Add_{\mathrm{A}}} = \mathbb{N},\ \mathsf{O}_{Add_{\mathrm{A}}} = \{\mathsf{OK}, \mathsf{GOT}\},$$
$$\mathsf{I}_{Rem_{\mathrm{A}}} = \varnothing,\ \mathsf{O}_{Rem_{\mathrm{A}}} = \mathbb{N}. \tag{5.60}$$

$$u \text{ -}(i, Add_{\mathrm{A}}, \mathsf{OK})\text{-}\!\rightarrow u \cup \{ i \},\ \text{ if } i \notin u ,$$
$$u \text{ -}(i, Add_{\mathrm{A}}, \mathsf{GOT})\text{-}\!\rightarrow u,\ \text{ if } i \in u . \tag{5.61}$$

$$u \uplus \{ o \} \text{ -}(Rem_{\mathrm{A}}, o)\text{-}\!\rightarrow u . \tag{5.62}$$

The concrete system *Conc* models the bin as a sequence of maximum length five. It outputs error messages when the bin is either empty or full, as shown below.

$$\mathsf{W} = \{w \in \mathsf{iseq}(\mathbb{N}) \mid \mathsf{len}(w) \leq 5\},\ \mathsf{K}_{Add_{\mathrm{C}}} = \mathbb{N},\ \mathsf{Q}_{Add_{\mathrm{C}}} = \{\mathsf{OK}, \mathsf{GOT}, \mathsf{FULL}\},$$
$$\mathsf{K}_{Rem_{\mathrm{C}}} = \varnothing,\ \mathsf{Q}_{Rem_{\mathrm{C}}} = \mathbb{N} \cup \{\mathsf{EMPTY}\} . \tag{5.63}$$

$$w \text{ -}(k, Add_{\mathrm{C}}, \mathsf{OK})\text{-}\!\rightarrow w \frown \langle k \rangle,\ \text{ if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) \leq 4 ,$$
$$w \text{ -}(k, Add_{\mathrm{C}}, \mathsf{FULL})\text{-}\!\rightarrow w,\ \text{ if } k \notin \mathsf{ran}(w) \wedge \mathsf{len}(w) = 5 ,$$
$$w \text{ -}(k, Add_{\mathrm{C}}, \mathsf{GOT})\text{-}\!\rightarrow w,\ \text{ if } k \in \mathsf{ran}(w) . \tag{5.64}$$

$$\langle\ \rangle \text{ -}(Rem_{\mathrm{A}}, \mathsf{EMPTY})\text{-}\!\rightarrow \langle\ \rangle ,$$
$$\langle q \rangle \frown w \text{ -}(Rem_{\mathrm{A}}, q)\text{-}\!\rightarrow w . \tag{5.65}$$

Lastly, we define the component relations of the retrenchment as follows.

$$
\begin{aligned}
&G(u, w) \;=\; (u = \mathsf{ran}(w)) \,, \\
&P_{Add}(i, k, u, w) \;=\; (i = k) \,, \\
&O_{Add}(o, q, u', w'; i, k, u, w) \;=\; (o = q) \,, \\
&N_{Add}(u', w', o, q; i, k, u, w) \;= \\
&\qquad (\,|u| = 5 \wedge i \notin u \wedge u' = u \cup \{\, i \,\} \wedge w' = w \wedge o = \mathsf{OK} \wedge p = \mathsf{FULL}\,) \,, \\
&P_{Rem}(i, k, u, w) \;=\; (u = w \wedge |u| \neq 0) \,, \\
&O_{Rem}(o, q, u', w'; i, k, u, w) \;=\; (o = q) \,, \\
&C_{Add}(u', w', o, q; i, k, u, w) \;=\; \mathit{false} \,.
\end{aligned}
\tag{5.66}
$$

The states of *Univ* are triples (t, u, w) such that t is a tag with value either 0 or 1, u is a set of natural numbers and w is a sequence of natural numbers, e.g. $(0, \{3, 41\}, \langle 8, 50, 51\rangle\}$. The tag is used to differentiate between operations in both Ops_A and Ops_C, for which $t = 0$, and those that occur only in Ops_C, for which $t = 1$. We add that for retrenchments where $\mathsf{Ops}_C = \mathsf{Ops}_A$, the tag becomes redundant and can be omitted entirely, resulting in a slightly simpler version of the lifting construction. Returning to u and w, notice that the sequence w is not necessarily a serialisation of the set u. However, by (5.2), this must be the case for states of non-boundary transitions. For Add_U and Rem_U typical non-boundary steps are

$$(0, \{1, 2\}, \langle 2, 1\rangle) \text{-}((3, 3), Add_U, (\mathsf{OK}, \mathsf{OK}))\text{-}\!\rightarrow (0, \{1, 2, 3\}, \langle 3, 2, 1\rangle)$$

and

$$(0, \{1, 2, 3\}, \langle 1, 2, 3\rangle) \text{-}(Rem_U, (3, 3))\text{-}\!\rightarrow (0, \{1, 2\}, \langle 1, 2\rangle) \,.$$

Observe that the concrete before and after components of both transitions do not have to constitute an Add_C or Rem_C step respectively, since *Univ* is the subset of only abstract transitions for which $G \wedge P_{Op} \wedge ((G' \wedge O_{Op}) \vee C_{Op})$ holds. It thus contains abstract transitions piggybacked by corresponding concrete state and I/O data, and it is in this way that the constraints imposed in the retrenchment to *Conc* are expressed at the abstract level.

Turning to boundary cases a typical Add_U step is

$$(0, \{1 \,..\, 5\}, \langle 1 \,..\, 5\rangle) \text{-}((8, 8), Add_U, (\mathsf{OK}, \mathsf{FULL}))\text{-}\!\rightarrow (0, \{1 \,..\, 5, 8\}, \langle 1 \,..\, 5\rangle) \,.$$

This brings together abstract and concrete steps with different behaviour, related by the concedes clause of the retrenchment. When we come to consider Rem_{U}, we find there is no step which describes the removal of a number from an empty bin. For such cases P_{Rem} does not hold, so denying the possibility of a *Univ* step. The concrete step $(\langle\,\rangle)$ -(Rem_{C}, EMPTY)-› $(\langle\,\rangle)$ falls outside the scope of the retrenchment from *Abs* to *Conc*, and therefore outside the scope of the lifting construction too.

The systems involved in the decomposition belong to a class which articulates conditions members must satisfy in order that we obtain the required lifting. We briefly look at the properties defining the class. The condition that the relations for the refinement to *Conc* are functions ensures inclusions (5.56) to (5.58) can be established, and expresses that the lifting must preserve the distinction between different concrete data values. The requirement that these relations are total, prevents the lifting from introducing data values which do not correspond to anything in the concrete system, and ensures the refinement from *Univ* to *Xtra* and the remaining inclusions can be established. Since we are interested in lifting *Conc* we consider these restrictions to be reasonable. Properties (X1) and (X2) are a little harder to appreciate from their definition, but their presence can be traced to the need to ensure all of *Conc* that is related to *Abs* is lifted. If this is not the case, although $G \wedge P_{Op}$ and thus $trm_{Op_{\mathrm{C}}}$ may hold, we are unable to guarantee points $v\tilde{}$ and $j\tilde{}$ for which $H\tilde{} \wedge Q\tilde{}_{Op}$ holds and hence the existence of a corresponding $trm_{Op_{\mathrm{X}}}$. Properties (X3) and (X4) require $FinOut_{Op_{\mathrm{X}}}$ and $InitIn_{Op_{\mathrm{X}}}$ to be faithful to the *Univ* counterparts. Finally, operations only in $\mathrm{Ops}_{\mathrm{C}}$ are not part of the retrenchment and (X5) to (X7) say we just replicate such operations in any lifted system, thus making certain that the POs for the refinement to *Conc* will go through.

Chapter 6

The Lowering Theorem

This chapter tackles the problem of decomposing a retrenchment from an abstract to a concrete system into a refinement followed by a retrenchment. We engineer a system *Univ* such that its abstract core bound transitions are the most concrete up to equivalence in the class of systems achieving the same decomposition.

[JB02] investigated the lowering construction in a partial correctness setting. This chapter tackles the problem in a total correctness framework. A substantial reworking of the earlier material was required.

6.1 The Lowering Theorem

Theorem 6.1. Let there be a retrenchment from *Abs* to *Conc*, as shown in Figure 6.1.

Then the following hold.

(1) There is a universal system *Univ* such that there is a refinement from *Abs* to *Univ* and a retrenchment from *Univ* to *Conc* whose composition is the given retrenchment, and which satisfies (U1) to (U6) below.

(2) Whenever there is a system *Xtra* and a refinement from *Abs* to *Xtra* and a retrenchment from *Xtra* to *Conc* whose composition is the given retrenchment, and which satisfies (X1) to (X6) below, then there is a refinement from *Xtra* to the abstract core bound transitions of *Univ* such that the following inclusions hold. $H^{\sim} \Rightarrow K^{\circ} ⨾ H^{\bullet}$, $Q^{\sim}{}_{Op} \Rightarrow (R^{\circ}{}_{Op} \wedge K^{\circ}) ⨾ Q^{\bullet}{}_{Op}$, $N^{\sim}{}_{Op} \Rightarrow (V^{\circ}{}_{Op} \wedge K^{\circ\prime} \wedge R^{\circ}{}_{Op} \wedge K^{\circ}) ⨾ N^{\bullet}{}_{Op}$, $D^{\sim}{}_{Op} \Rightarrow (K^{\circ\prime} \wedge V^{\circ}{}_{Op}$

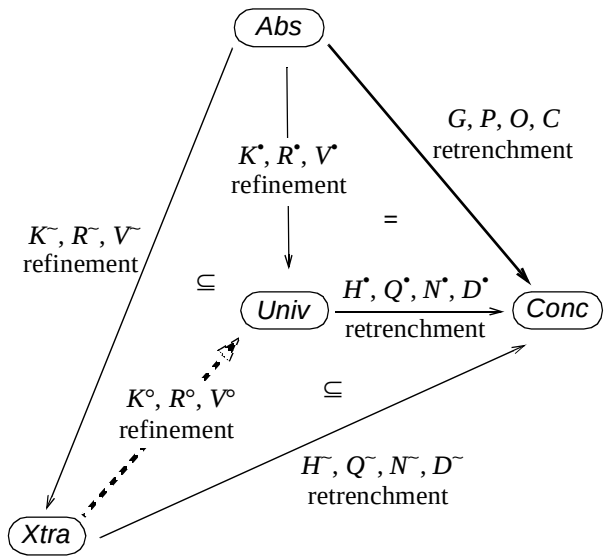


Figure 6.1: Lowering *Abs* to the level of *Conc*

$\wedge\ R^{\circ}{}_{Op} \wedge K^{\circ})\fatsemi D^{\bullet}{}_{Op},\ K^{\breve{}}\fatsemi K^{\circ} \Rightarrow K^{\bullet},\ R^{\breve{}}{}_{Op}\fatsemi R^{\circ}{}_{Op} \Rightarrow R^{\bullet}{}_{Op}$ and $V^{\breve{}}\fatsemi V^{\circ}{}_{Op} \Rightarrow V^{\bullet}{}_{Op}$ (see also (6.39) to (6.45)).

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are mutually interrefinable.

6.2 Proof for Part (1)

We take the retrenchment from *Abs* to *Conc* and build a new, universal system, *Univ*, for which we then show there is *both* a refinement from *Abs* and a retrenchment to *Conc*. See Figure 6.1.

For *Abs* the operation names set is $Op_{\mathrm{A}} \in \mathsf{Ops}_{\mathrm{A}}$, state, input and output spaces are $u \in \mathsf{U}$, $i \in \mathsf{I}_{Op_{\mathrm{A}}}$, $o \in \mathsf{O}_{Op_{\mathrm{A}}}$, and initialisation and step predicates are $Init_{\mathrm{A}}$ and $stp_{Op_{\mathrm{A}}}$. Correspondingly, for *Conc* we have $Op_{\mathrm{C}} \in \mathsf{Ops}_{\mathrm{C}}$, $w \in \mathsf{W}$, $k \in \mathsf{K}_{Op_{\mathrm{C}}}$, $q \in \mathsf{Q}_{Op_{\mathrm{C}}}$, $Init_{\mathrm{C}}$ and $stp_{Op_{\mathrm{C}}}$. Here, $\mathsf{Ops}_{\mathrm{A}} \subseteq \mathsf{Ops}_{\mathrm{C}}$. Let the retrenchment from *Abs* to *Conc* have retrieve relation G, and for each Op, within relation P_{Op}, output relation O_{Op} and concedes relation C_{Op}.

6.2.1 The system *Univ*

We construct *Univ* out of the elements of *Abs* and *Conc*. The operation names set of *Univ* is $\mathsf{Ops}_{\mathrm{U}}$ with elements Op_{U} and $\mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{A}}$. The state space is $\mathsf{V} = \mathsf{U} \times \mathsf{W}$ with elements $v = (u, w)$. The input and output spaces are $\mathsf{J}_{Op} = \mathsf{I}_{Op} \times \mathsf{K}_{Op}$ and $\mathsf{P}_{Op} = \mathsf{O}_{Op} \times \mathsf{Q}_{Op}$, with typical elements $j = (i, k)$ and $p = (o, q)$ respectively.

Let the initialization predicate $Init_{\mathrm{U}}(v')$ be defined as follows.

$$Init_{\mathrm{U}}(v') \;=\; (\; v' = (u', w') \wedge Init_{\mathrm{A}}(u') \wedge Init_{\mathrm{C}}(w') \wedge G(u', w') \;) \tag{6.1}$$

Let the transition (or step) relation for *Univ* be

$$\begin{aligned}
&stp_{Op_{\mathrm{U}}}(v, j, v', p) \;=\; stp_{Op_{\mathrm{U}}}((u, w), (i, k), (u', w'), (o, q)) \;= \\
&\quad \big(\; trm_{Op_{\mathrm{A}}}(u, i) \wedge \neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \;\Rightarrow\; stp_{Op_{\mathrm{A}}}(u, i, u', o) \;\big) && \text{(a)} \\
&\wedge \\
&\quad \big(\; trm_{Op_{\mathrm{A}}}(u, i) \wedge (G(u, w) \wedge P_{Op}(i, k, u, w)) \;\Rightarrow \\
&\qquad stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge stp_{Op_{\mathrm{C}}}(w, k, w', q) \wedge \\
&\qquad (\; (G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w) \;) \;\big) \;. \\
& && \text{(b)}
\end{aligned} \tag{6.2}$$

This completes the definition of *Univ*.

Given the above, the following holds.

$$\begin{aligned}
&trm_{Op_{\mathrm{U}}}(v, j) \;=\; trm_{Op_{\mathrm{U}}}((u, w), (i, k)) \;= \\
&\quad \neg\, trm_{Op_{\mathrm{A}}}(u, i) \vee && \text{(a)} \\
&\quad \neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \vee && \text{(b)} \\
&\quad \big(G(u, w) \wedge P_{Op}(i, k, u, w) \wedge \\
&\qquad (\exists\, u', o, w', q \bullet stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge stp_{Op_{\mathrm{C}}}(w, k, w', q) \wedge \\
&\qquad\quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w))\big) && \text{(c)}
\end{aligned} \tag{6.3}$$

Proof.

$trm_{Op_U}(v, j)$

= [definition of trm_{Op}]

$(\exists\, v', p \bullet stp_{Op_U}(v, j, v', p))$

= [by (6.2), and using obvious abbreviations]

$(\exists\, v', p \bullet (trm_{Op_A} \wedge \neg GP_{Op} \Rightarrow stp_{Op_A}) \wedge$
$\quad (trm_{Op_A} \wedge GP_{Op} \Rightarrow stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op}))$

= [$(t \wedge a \Rightarrow c) \wedge (t \wedge b \Rightarrow c) \Leftrightarrow (t \Rightarrow (a \Rightarrow c) \wedge (b \Rightarrow c)$]

$(\exists\, v', p \bullet trm_{Op_A} \Rightarrow (\neg GP_{Op} \Rightarrow stp_{Op_A}) \wedge (GP_{Op} \Rightarrow stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op}))$

= [$(\neg a \Rightarrow b) \wedge (a \Rightarrow c) \Leftrightarrow (\neg a \wedge b) \vee (a \wedge c) \vee (b \wedge c)$, $(\neg a \wedge b) \vee (a \wedge c) \vee (b \wedge c) \Leftrightarrow (\neg a \wedge b) \vee (a \wedge c)$]

$(\exists\, v', p \bullet trm_{Op_A} \Rightarrow (\neg GP_{Op} \wedge stp_{Op_A}) \vee (GP_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op}))$

= [$a \Rightarrow b \Leftrightarrow \neg a \vee b$]

$(\exists\, v', p \bullet \neg\, trm_{Op_A} \vee (\neg GP_{Op} \wedge stp_{Op_A}) \vee (GP_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op}))$

= [$(\exists \ldots \bullet a \vee b \vee c) \Leftrightarrow (\exists \ldots \bullet a) \vee (\exists \ldots \bullet b) \vee (\exists \ldots \bullet c)$]

$(\exists\, v', p \bullet \neg\, trm_{Op_A}) \vee (\exists\, v', p \bullet \neg GP_{Op} \wedge stp_{Op_A}) \vee$
$\quad (\exists\, v', p \bullet GP_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op})$

= [expanding]

$(\exists\, v', p \bullet \neg\, trm_{Op_A}(u, i)) \vee (\exists\, v', p \bullet \neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \wedge stp_{Op_A}(u, i, u', o)) \vee$
$\quad (\exists\, v', p \bullet G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$
$\quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)))$

= [simplifying and using $v = (u, w)$, $j = (i, k)$]

$\neg\, trm_{Op_A}(u, i) \vee (\neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \wedge (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o))) \vee$
$\quad (G(u, w) \wedge P_{Op}(i, k, u, w) \wedge (\exists\, u', o, w', q \bullet stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$
$\quad\quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w))))$

= [$(\exists\, u', o \bullet stp_{Op_A}(u, i, u', o)) \Leftrightarrow trm_{Op_A}(u, i)$]

$\neg\, trm_{Op_A}(u, i) \vee (\neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \wedge trm_{Op_A}(u, i)) \vee$
$\quad (G(u, w) \wedge P_{Op}(i, k, u, w) \wedge (\exists\, u', o, w', q \bullet stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$
$\quad\quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w))))$

= [$\neg t \vee (a \wedge t) \;\Leftrightarrow\; \neg t \vee a$]

$\neg\, trm_{Op_A}(u, i) \vee \neg(G(u, w) \wedge P_{Op}(i, k, u, w)) \vee$
$\quad (G(u, w) \wedge P_{Op}(i, k, u, w) \wedge (\exists\, u', o, w', q \bullet stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$
$\quad\quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w))))$ ■

6.2.2 The refinement from *Abs* to *Univ*

In this section we show that *Univ* is a refinement of *Abs*. To do this we first define the component relations of the refinement and then show that the refinement POs hold.

6.2.2.1 The component relations

The data for the refinement consists of the retrieve relation $K^{\bullet}$, and for each Op, the input relation $R^{\bullet}_{Op}$ and the output relation $V^{\bullet}_{Op}$. These are defined as follows.

$$K^{\bullet}(u, v) \;=\; (v = (u, w)) \;. \tag{6.4}$$

$$R^{\bullet}_{Op}(i, j) \;=\; (j = (i, k)) \;, \tag{6.5}$$

$$V^{\bullet}_{Op}(o, p) \;=\; (p = (o, q)) \;. \tag{6.6}$$

Notice that (6.4) to (6.6) are both injective (see Section 2.1) and surjective.

We also have the input initialisation and output finalisation relations. *Abs* is the only given system involved in the refinements, thus we use the input and output spaces of its operations to construct those of the global world. Thus for each Op let $\mathsf{N}_{Op} = \mathsf{Q}_{Op}$ and

$$\mathsf{H}_{Op} \;=\; \{h \in \mathsf{I}_{Op} \mid \exists\, i, k, u, w \bullet i = h \wedge P_{Op}(i, k, u, w) \wedge G(u, w)\} \;, \tag{6.7}$$

$$InitIn_{Op_{\mathrm{A}}}(h, i) \;=\; (\, h = i \,) \;, \tag{6.8}$$

$$FinOut_{Op_{\mathrm{A}}}(o, n) \;=\; (\, o = n \,) \;, \tag{6.9}$$

$$InitIn_{Op_{\mathrm{U}}}(h, j) \;=\; (\exists\, i, k, u, w \bullet i = h \wedge\; j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge G(u, w)) \;, \tag{6.10}$$

$$FinOut_{Op_{\mathrm{U}}}(p, n) \;=\; (\, p = (o, q) \wedge n = o \,) \;. \tag{6.11}$$

Observe that (6.8) to (6.11) are all total relations.

6.2.2.2 The input initialisation PO

We show

$$InitIn_{Op_{\mathrm{U}}}(h, j) \;\Rightarrow\; (\exists\, i \bullet InitIn_{Op_{\mathrm{A}}}(h, i) \wedge R^{\bullet}_{Op}(i, j)) \;. \tag{6.12}$$

Proof. Assume $InitIn_{Op_U}(h, j)$ and let $j = (i, k)$. By (6.10) $h = i$. Then, $InitIn_{Op_A}(h, i)$ holds, by (6.8), and $R^{\bullet}_{Op}(i, j)$ holds, by (6.5). We are done. ■

6.2.2.3 The initialisation PO

We show

$$Init_U(v') \Rightarrow (\exists\, u' \bullet Init_A(u') \wedge K^{\bullet}(u', v')) \,. \tag{6.13}$$

Proof. Assume $Init_U(v')$, with $v' = (u', w')$. By (6.1), $Init_A(u')$ is true. By (6.4), $K^{\bullet}(u', v')$ is true. Hence the consequent of the PO holds. ■

6.2.2.4 The applicability PO

We show

$$K^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(i, j) \wedge trm_{Op_A}(u, i) \Rightarrow trm_{Op_U}(v, j) \,. \tag{6.14}$$

Proof. Assume the antecedents. By (6.4), $K^{\bullet}(u, v)$ fixes the first component of v to u and let the second component be w. Thus $v = (u, w)$. Similarly $R^{\bullet}_{Op}(i, j)$ gives $j = (i, k)$. There are now two possibilities. Either $G(u, w) \wedge P_{Op}(i, k, u, w)$ holds, or it does not.

• Case $\neg(G(u, w) \wedge P_{Op}(i, k, u, w))$. $trm_{Op_U}(v, j)$ holds by (6.3b).

• Case $G(u, w) \wedge P_{Op}(i, k, u, w)$. From the termination PO for the retrenchment from *Abs* to *Conc*,

$$G(u, w) \wedge P_{Op}(i, k, u, w) \Rightarrow trm_{Op_A}(u, i) \wedge trm_{Op_C}(w, k) \,, \tag{6.15}$$

we get $trm_{Op_C}(w, k)$. The latter guarantees values, pick u' and o, such that $stp_{Op_C}(w, k, w', q)$ holds. We now have the antecedents of the Op PO for the retrenchment from *Abs* to *Conc*,

$$\begin{aligned} & G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow \\ & \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\ & \qquad (\,(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\,)) \,. \end{aligned} \tag{6.16}$$

Hence we can derive u' and o, for which stp_{Op_A} and $(G' \wedge O_{Op}) \vee C_{Op}$ hold. We now have enough to conclude, by (6.3c), that $trm_{Op_U}(v, j)$ holds. ■

6.2.2.5 The correctness PO

We show

$$K^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(i, j) \wedge trm_{Op_A}(u, i) \wedge stp_{Op_U}(v, j, v', p) \Rightarrow$$
$$(\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge K^{\bullet}(u', v') \wedge V^{\bullet}_{Op}(o, p)) \,. \tag{6.17}$$

Proof. Assume the antecedents. By the same process as for PO (6.16), we have $v = (u, w)$ and $j = (i, k)$. Let $v' = (u', w')$ and $p = (o, q)$. Now, either $G(u, w) \wedge P_{Op}(i, k, u, w)$ holds, or it does not. Then, since we have $trm_{Op_A}(u, i)$, $stp_{Op_A}(u, i, u', o)$ holds, either by (6.2a) or (6.2b). Finally, $K^{\bullet}(u', v')$ and $V^{\bullet}_{Op}(o, p)$ hold, by (6.4) and (6.6) respectively. ■

6.2.2.6 The output finalisation PO

We show

$$V^{\bullet}_{Op}(o, p) \wedge FinOut_{Op_U}(p, n) \Rightarrow FinOut_{Op_A}(o, n) \,. \tag{6.18}$$

Proof. Assume the antecedents. By (6.6), $V^{\bullet}_{Op}$ sets the first component of p to o and let the second component be q. Ergo $p = (o, q)$. Then, by (6.11), $FinOut_{Op_U}(p, n)$ sets $n = o$. Hence, by (6.9), $FinOut_{Op_A}(o, n)$ holds, as required. ■

6.2.3 The retrenchment from *Univ* to *Conc*

In this section we show that *Conc* is a retrenchment of *Univ*. To do this we first define the component relations of the retrenchment and then show that the retrenchment POs hold.

6.2.3.1 The component relations

The data for the retrenchment consists of the retrieve relation $H^{\bullet}$, and for each Op, the within relation $Q^{\bullet}_{Op}$, the output relation $N^{\bullet}_{Op}$, and the concedes relation $D^{\bullet}_{Op}$. These are defined as follows.

$$H^{\bullet}(v, w) = (v = (u, w) \wedge G(u, w)) \tag{6.19}$$

$$Q^{\bullet}_{Op}(j, k, v, w) \;=\; (j = (i, k) \wedge v = (u, w) \wedge P_{Op}(i, k, u, w)) \tag{6.20}$$

$$N^{\bullet}_{Op}(p, q; v', w', j, k, v, w) \;=$$
$$(p = (o, q) \wedge v' = (u', w') \wedge j = (i, k) \wedge v = (u, w) \wedge O_{Op}(o, q; u', w', i, k, u, w)) \tag{6.21}$$

$$D^{\bullet}_{Op}(v', w', p, q; j, k, v, w) \;=$$
$$(v' = (u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (u, w) \wedge C_{Op}(u', w', o, q; i, k, u, w)) \tag{6.22}$$

6.2.3.2 The initialisation PO

We show

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, v' \bullet Init_{\mathrm{U}}(v') \wedge H^{\bullet}(v', w'))\ . \tag{6.23}$$

Proof. Assume $Init_{\mathrm{C}}(w')$. From this, using the Init PO for the retrenchment from *Abs* to *Conc*,

$$Init_{\mathrm{C}}(w') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', w'))\ , \tag{6.24}$$

we derive u' for which $Init_{\mathrm{A}}(u')$ and $G(u', w')$ are true. Let $v' = (u', w')$. Then, by (6.1), $Init_{\mathrm{U}}(v')$ holds, and what is more, by (6.19), $H^{\bullet}(v', w')$ holds too. We are done. ■

6.2.3.3 The termination PO

We show

$$H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w) \;\Rightarrow\; trm_{Op_{\mathrm{U}}}(v, j) \wedge trm_{Op_{\mathrm{C}}}(w, k) \tag{6.25}$$

Proof. Assume the antecedents. From $H^{\bullet}(v, w)$, by (6.19), the second component of v must be w and let the first component be u. Hence $v = (u, w)$. We also get $G(u, w)$. Similarly, from $Q^{\bullet}_{Op}(j, k, v, w)$, by (6.20), we get $j = (i, k)$ and $P_{Op}(i, k, u, w)$. We now have the antecedents of PO (6.15). Thus we can conclude $trm_{Op_{\mathrm{C}}}(w, k)$, which we want, holds. What is more, $stp_{Op_{\mathrm{C}}}(w, k, w', q)$, for values which we fix to w' and q, must also hold. We now have the antecedents of PO (6.16). Hence $stp_{Op_{\mathrm{A}}}(u, i, u', o)$ and $(G(u', w') \wedge O_{Op}(o,$

$q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)$ are true. Therefore, $trm_{Op_U}(v, j)$ holds, by (6.3c). We are done. ■

6.2.3.4 The operation PO

We show

$$H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow$$
$$(\exists\, v', p \bullet stp_{Op_U}(v, j, v', p) \wedge$$
$$(\,(H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)) \vee D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)\,))\,. \tag{6.26}$$

Proof. Assume the antecedents. From $H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w)$, by the same process as for PO (6.25), we obtain $G(u, w) \wedge P_{Op}(i, k, u, w)$, with $v = (u, w)$ and $j = (i, k)$. We now have the antecedents of PO (6.16). Hence, there are values, u' and o say, such that $stp_{Op_A}(u, i, u', o)$ and thus $trm_{Op_A}(u, i)$, and also $(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)$ are true. Let $v' = (u', w')$ and $p = (o, q)$. Then $stp_{Op_U}(v, j, v', p)$ holds.

It remains to show $(H^{\bullet\prime} \wedge N^{\bullet}_{Op}) \vee D^{\bullet}_{Op}$. This follows from $(G' \wedge O_{Op}) \vee C_{Op}$. Suppose $(G' \wedge O_{Op})$ holds. Then $H^{\bullet}(v', w')$ holds, by (6.19), and $N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)$ holds, by (6.21). Otherwise we have C_{Op}, in which case $D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)$ holds, by (6.22). We are done. ■

6.2.4 The relations of the retrenchment from *Abs* to *Conc*

In this section we define the relations of the retrenchment from *Abs* to *Conc* in terms of the relations for the refinement from *Abs* to *Univ* and the retrenchment from *Univ* to *Conc*, and prove that these definitions do recover the relations of the *Abs* to *Conc* retrenchment. Let

$$G(u, w) \;=\; K^{\bullet}(u, v) \fatsemi H^{\bullet}(v, w)\,, \tag{6.27}$$

$$P_{Op}(i, k, u, w) \;=\; (R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v)) \fatsemi Q^{\bullet}_{Op}(j, k, v, w)\,, \tag{6.28}$$

$$O_{Op}(o, q; u', w', i, k, u, w) =$$
$$(V^{\bullet}_{Op}(o, p) \wedge K^{\bullet}(u', v') \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v)) ⨾ N^{\bullet}_{Op}(p, q; v', w', j, k, v, w) \quad (6.29)$$

$$C_{Op}(u', w', o, q; i, k, u, w) =$$
$$(K^{\bullet}(u', v') \wedge V^{\bullet}_{Op}(o, p) \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v)) ⨾ D^{\bullet}_{Op}(v', w', p, q; j, k, v, w) \quad (6.30)$$

We show (6.27) and (6.29); the others are similar.

Proof. Consider (6.27) first. We expand the RHS.

$K^{\bullet}(u, v) ⨾ H^{\bullet}(v, w)$

= [meaning of composition]

$(\exists\, v \bullet K^{\bullet}(u, v) \wedge H^{\bullet}(v, w))$

= [by (6.4) and (6.19)]

$(\exists\, v \bullet K^{\bullet}(u, v) \wedge H^{\bullet}(v, w) \wedge v = (u, w))$

= [one-point rule]

$K^{\bullet}(u, (u, w)) \wedge H^{\bullet}((u, w), w)$

= [by (6.4)]

$H^{\bullet}((u, w), w)$

= [by (6.19)]

$G(u, w)$

Now consider (6.29). Again, we expand the RHS.

$(V^{\bullet}_{Op}(o, p) \wedge K^{\bullet}(u', v') \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v)) ⨾ N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)$

= [meaning of composition]

$(\exists\, p, v', j, v \bullet V^{\bullet}_{Op}(o, p) \wedge K^{\bullet}(u', v') \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v) \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w))$

= [by (6.4), (6.5), (6.6) and (6.21)]

$(\exists\, p, v', j, v \bullet V^{\bullet}_{Op}(o, p) \wedge K^{\bullet}(u', v') \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v) \wedge$
$\quad N^{\bullet}_{Op}(p, q; v', w', j, k, v, w) \wedge p = (o, q) \wedge v' = (u', w') \wedge j = (i, k) \wedge v = (u, w))$

= [one-point rule]

$V^{\bullet}_{Op}(o, (o, q)) \wedge K^{\bullet}(u', (u', w')) \wedge R^{\bullet}_{Op}(i, (i, k)) \wedge K^{\bullet}(u, (u, w)) \wedge$
$\quad N^{\bullet}_{Op}((o, q), q; (u', w'), w', (i, k), k, (u, w), w)$

= [by (6.4), (6.5) and (6.6)]

$N^{\bullet}_{Op}((o, q), q; (u', w'), w', (i, k), k, (u, w), w)$

$= [\text{by (6.21)}]$

$O_{Op}(o, q; u', w', i, k, u, w)$

Thus $G = K^{\bullet} ⨾ H^{\bullet}$ and $O_{Op} = (V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet}) ⨾ N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)$. ■

6.2.5 Properties of *Univ*

$$K^{\bullet}(u, v) \wedge (H^{\bullet}(v, w) \vee Q^{\bullet}_{Op}(..., v, w) \vee N^{\bullet}_{Op}(..., v, w) \vee D^{\bullet}_{Op}(..., v, w) \vee N^{\bullet}_{Op}(...; v, w, ...) \vee D^{\bullet}_{Op}(v, w, ...)) \wedge K^{\bullet}(u, \underline{v}) \wedge H^{\bullet}(\underline{v}, w) \Rightarrow v = \underline{v} \tag{U1}$$

$$R^{\bullet}_{Op}(i, j) \wedge (Q^{\bullet}_{Op}(j, k, ...) \vee N^{\bullet}_{Op}(..., j, k, ...) \vee D^{\bullet}_{Op}(...; j, k, ...)) \wedge R^{\bullet}_{Op}(i, \underline{j}) \wedge Q^{\bullet}_{Op}(\underline{j}, k, ...) \Rightarrow j = \underline{j} \tag{U2}$$

$$R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge H^{\bullet}(v, w) \Rightarrow (\exists\, h \bullet h = i \wedge InitIn_{Op_U}(h, j)) \tag{U3}$$

$$Init_A(u') \wedge K^{\bullet}(u', v') \wedge H^{\bullet}(v', w') \wedge Init_C(w') \Rightarrow Init_U(v') \tag{U4}$$

$$stp_{Op_A}(u, i, u', o) \wedge K^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u', v') \wedge V^{\bullet}_{Op}(o, p) \wedge H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge ((H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)) \vee D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow stp_{Op_U}(v, j, v', p) \tag{U5}$$

$$V^{\bullet}_{Op}(o, p) \wedge n = o \Rightarrow FinOut_{Op_U}(p, n) \tag{U6}$$

♦ (U1):

$$K^{\bullet}(u, v) \wedge (H^{\bullet}(v, w) \vee Q^{\bullet}_{Op}(..., v, w) \vee N^{\bullet}_{Op}(..., v, w) \vee D^{\bullet}_{Op}(..., v, w) \vee N^{\bullet}_{Op}(...; v, w, ...) \vee D^{\bullet}_{Op}(v, w, ...)) \wedge K^{\bullet}(u, \underline{v}) \wedge H^{\bullet}(\underline{v}, w) \Rightarrow v = \underline{v}$$

Proof. Assume the antecedents and let $v = (\underline{\underline{u}}, \underline{\underline{w}})$ and $\underline{v} = (\underline{u}, \underline{w})$. By (6.4), from $K^{\bullet}(u, v)$ we have $\underline{\underline{u}} = u$, and from $K^{\bullet}(u, \underline{v})$ we have $\underline{u} = u$. Therefore, $\underline{\underline{u}} = \underline{u}$. Similarly, each one

of (6.19) and $H^{\bullet}(v, w)$; (6.20) and $Q^{\bullet}_{Op}(..., v, w)$; (6.21) and $N^{\bullet}_{Op}(..., v, w)$ or $N^{\bullet}_{Op}(...; v, w, ...)$; (6.22) and $D^{\bullet}_{Op}(..., v, w)$ or $D^{\bullet}_{Op}(v, w, ...)$ assert that $\underline{\underline{w}} = w$. Lastly, $H^{\bullet}(\underline{v}, w)$ asserts $\underline{w} = w$. Thus $\underline{\underline{w}} = \underline{w}$, and so $v = \underline{v}$. ■

♦ (U2).

Proof. Similar to (U1). ■

♦ (U3): $R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u, v) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge H^{\bullet}(v, w) \Rightarrow$
$(\exists\, h \bullet h = i \wedge InitIn_{Op_{\mathrm{U}}}(h, j))$

Proof. Assume the antecedents. From $R^{\bullet}_{Op}(i, j)$, $K^{\bullet}(u, v)$ and $Q^{\bullet}_{Op}(j, k, v, w)$, by (6.5), (6.4) and (6.20), $j = (i, k)$ and $v = (u, w)$. From $Q^{\bullet}_{Op}(j, k, v, w)$ we also get $P_{Op}(i, k, u, w)$; and $H^{\bullet}(v, w)$, by (6.19), gives $G(u, w)$. Then, by (6.10), $InitIn_{Op_{\mathrm{U}}}(h, j)$ holds, with $h = i$. We are done. ■

♦ (U4): $Init_{\mathrm{A}}(u') \wedge K^{\bullet}(u', v') \wedge H^{\bullet}(v', w') \wedge Init_{\mathrm{C}}(w') \Rightarrow Init_{\mathrm{U}}(v')$

Proof. Assume the antecedents. From $K^{\bullet}(u', v')$, by (6.4), and $H^{\bullet}(v', w')$, by (6.19), we have $v' = (u', w')$ and $G(u', w')$. Thus, since we have $Init_{\mathrm{A}}(u')$ and $Init_{\mathrm{C}}(w')$, (6.1) says $Init_{\mathrm{U}}(v')$ holds, as required. ■

♦ (U5):

$$
\begin{aligned}
&stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge K^{\bullet}(u, v) \wedge R^{\bullet}_{Op}(i, j) \wedge K^{\bullet}(u', v') \wedge V^{\bullet}_{Op}(o, p) \wedge \\
&H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge \\
&((H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)) \vee D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)) \wedge \\
&stp_{Op_{\mathrm{C}}}(w, k, w', q) \Rightarrow stp_{Op_{\mathrm{U}}}(v, j, v', p)
\end{aligned}
$$

Proof. Assume the antecedents. Let $v = (\underline{u}, \underline{w})$. From $K^{\bullet}(u, v)$, by (6.4), we have $u = \underline{u}$. From $H^{\bullet}(v, w)$, by (6.19), we have $w = \underline{w}$. Hence $v = (u, w)$. Using the same method, we also obtain from the other antecedents $j = (i, k)$, $v' = (u', w')$ and $p = (o, q)$. Next, $H^{\bullet}(v, w)$ and (6.19) give $G(u, w)$, $Q^{\bullet}_{Op}(j, k, v, w)$ and (6.20) give $P_{Op}(i, k, u, w)$, $H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p,$

q; v', w', j, k, v, w) and (6.19) and (6.20) give $G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)$, $D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)$ and (6.22) give $C_{Op}(u', w', o, q; i, k, u, w)$. In addition, because $stp_{Op_A}(u, i, u', o)$ is true then so is $trm_{Op_A}(u, i)$. Thus, altogether we have $trm_{Op_A}(u, i) \wedge G(u, w) \wedge P_{Op}(i, k, u, w)$, $stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q)$ and $(G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)$. Hence $stp_{Op_U}(v, j, v', p)$ holds, by (6.2b). We are done. ■

♦ (U6): $V^{\bullet}_{Op}(o, p) \wedge n = o \Rightarrow FinOut_{Op_U}(p, n)$

Proof. Assume the antecedents. By (6.6), $V^{\bullet}_{Op}$ sets the first component of p to o and let the second component be q. Therefore $p = (o, q)$, and since $n = o$, we have $FinOut_{Op_U}(p, n)$, by (6.11). Done. ■

This completes part (1) of the theorem.

6.3 Proof for Part (2)

The systems which decompose the retrenchment must belong to a class defined by (X1) to (X6), and the condition that the retrieve, input and output relations for the refinement to *Conc* are injective and surjective. To prove part (2) we must show that for *any* system *Xtra* in the class, there is a refinement from *Xtra* to *Univ*. We structure the proof as follows. In Section 6.3.1 we detail the components of *Xtra* and state properties (X1) to (X6). In Section 6.3.2 we define the relations K°, R°_{Op}, V°_{Op} and then prove that they are the retrieve, input and output relations of the desired refinement. Finally, in Section 6.3.3, we show that the inclusions stated in part (2) hold.

6.3.1 The system *Xtra*

The system *Xtra* has operation names set $Op_X \in \mathsf{Ops}_X$, with $\mathsf{Ops}_X = \mathsf{Ops}_U$. The state space is $v^{\sim} \in \mathsf{V}^{\sim}$. For each Op_X, the input space is $j^{\sim} \in \mathsf{J}^{\sim}_{Op_X}$ and output space is $p^{\sim} \in \mathsf{P}^{\sim}_{Op_X}$. We will denote the initialisation predicate by $Init_X$ and the step relation by stp_{Op_X}.

Let the refinement from *Abs* to *Xtra* be given by retrieve relation $K^{\sim}$, and for each *Op*, the input relation $R^{\sim}_{Op}$ and output relation $V^{\sim}_{Op}$, the input initialisation $InitIn_{Op_X}$ and the output finalisation $FinOut_{Op_X}$. Let the retrenchment from *Xtra* to *Conc* be given by retrieve

relation $H^{\sim}$, and for each Op, within relation $Q^{\sim}$, output relation $N^{\sim}$ and concedes relation $D^{\sim}$. Let the relations $K^{\sim}$, $R^{\sim}$ and $V^{\sim}$ be injective and surjective, and $InitIn_{Op_X}$ and $FinOut_{Op_X}$ be total.

Let *Xtra* have properties (X1) to (X6) given below.

$$K^{\sim}(u, v^{\sim}) \wedge (H^{\sim}(v^{\sim}, w) \vee Q^{\sim}_{Op}(..., v^{\sim}, w) \vee N^{\sim}_{Op}(..., v^{\sim}, w) \vee D^{\sim}_{Op}(..., v^{\sim}, w) \vee N^{\sim}_{Op}(...; v^{\sim}, w, ...) \vee D^{\sim}_{Op}(v^{\sim}, w, ...)) \wedge K^{\sim}(u, \underline{v}^{\sim}) \wedge H^{\sim}(\underline{v}^{\sim}, w) \Rightarrow v^{\sim} = \underline{v}^{\sim} \quad \text{(X1)}$$

$$R^{\sim}_{Op}(i, j^{\sim}) \wedge (Q^{\sim}_{Op}(j^{\sim}, k, ...) \vee N^{\sim}_{Op}(..., j^{\sim}, k, ...) \vee D^{\sim}_{Op}(...; j^{\sim}, k, ...)) \wedge R^{\sim}_{Op}(i, \underline{j}^{\sim}) \wedge Q^{\sim}_{Op}(\underline{j}^{\sim}, k, ...) \Rightarrow j^{\sim} = \underline{j}^{\sim} \quad \text{(X2)}$$

$$R^{\sim}_{Op}(i, j^{\sim}) \wedge K^{\sim}(u, v^{\sim}) \wedge Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w) \wedge H^{\sim}(v^{\sim}, w) \Rightarrow (\exists\, h \bullet h = i \wedge InitIn_{Op_X}(h, j^{\sim})) \quad \text{(X3)}$$

$$Init_A(u') \wedge K^{\sim}(u, v^{\sim}) \wedge H^{\sim}(v^{\sim}, w) \wedge Init_C(w') \Rightarrow Init_X(v^{\sim\prime}) \quad \text{(X4)}$$

$$stp_{Op_A}(u, i, u', o) \wedge K^{\sim}(u, v^{\sim}) \wedge R^{\sim}_{Op}(i, j^{\sim}) \wedge K^{\sim}(u', v^{\sim\prime}) \wedge V^{\sim}_{Op}(o, p^{\sim}) \wedge H^{\sim}(v^{\sim}, w) \wedge Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w) \wedge ((H^{\sim}(v^{\sim\prime}, w') \wedge N^{\sim}_{Op}(p^{\sim}, q; v^{\sim\prime}, w', j^{\sim}, k, v^{\sim}, w)) \vee D^{\sim}_{Op}(v^{\sim\prime}, w', p^{\sim}, q; j^{\sim}, k, v^{\sim}, w)) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow stp_{Op_X}(v^{\sim}, j^{\sim}, v^{\sim\prime}, p^{\sim}) \quad \text{(X5)}$$

$$V^{\sim}_{Op}(o, p^{\sim}) \wedge n = o \Rightarrow FinOut_{Op_X}(p^{\sim}, n) \quad \text{(X6)}$$

Notice properties (U1) to (U6) are instances of (X1) to (X6) respectively when $\mathsf{V}^{\sim} = \mathsf{V}$, $\mathsf{J}^{\sim} = \mathsf{J}$ and $\mathsf{P}^{\sim} = \mathsf{P}$. In addition, $K^{\bullet}$, $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ are both injective and surjective, just like $K^{\sim}$, $R^{\sim}_{Op}$ and $V^{\sim}_{Op}$. Hence *Univ* and *Xtra* belong to the same class of systems which factorise the retrenchment from *Abs* to *Conc*.

6.3.2 The refinement from *Xtra* to *Univ*

To show that the abstract core bound transitions of *Univ* refine *Xtra*, we first define the component relations and then show that the refinement POs hold.

6.3.2.1 The component relations

We define the retrieve relation K°, and for each Op, the input relation R°_{Op} and output relation V°_{Op} for the refinement from $Xtra$ to $Univ$.

$$K^\circ(v\tilde{}, v) \;=\; K^\circ(v\tilde{}, (u, w)) \;=\; (\,(G(u, w) \Rightarrow H\tilde{}(v\tilde{}, w)) \wedge K\tilde{}(u, v\tilde{})\,)\,, \tag{6.31}$$

$$\begin{aligned} R^\circ_{Op}(j\tilde{}, j) \;&=\; R^\circ_{Op}(j\tilde{}, (i, k)) \;= \\ &(\,(\forall\, u, w, v\tilde{} \bullet P_{Op}(i, k, u, w) \wedge K\tilde{}(u, v\tilde{}) \wedge H\tilde{}(v\tilde{}, w) \Rightarrow Q\tilde{}_{Op}(j\tilde{}, k, v\tilde{}, w)) \wedge \\ &R\tilde{}_{Op}(i, j\tilde{})\,)\,, \end{aligned} \tag{6.32}$$

$$V^\circ_{Op}(p\tilde{}, p) \;=\; V^\circ_{Op}(p\tilde{}, (o, q)) \;=\; V\tilde{}_{Op}(o, p\tilde{})\,. \tag{6.33}$$

6.3.2.2 The input initialisation PO

We show

$$InitIn_{Op_U}(h, j) \;\Rightarrow\; (\exists\, j\tilde{} \bullet InitIn_{Op_X}(h, j\tilde{}) \wedge R^\circ_{Op}(j\tilde{}, j))\,. \tag{6.34}$$

Proof. Assume $InitIn_{Op_U}(h, j)$ and let $j = (i, k)$. By (6.10) there are values, u and w say, for which $P_{Op}(i, k, u, w) \wedge G(u, w)$ holds, with $h = i$. Then, since $P_{Op}(i, k, u, w) = (R\tilde{}_{Op}(i, j\tilde{}) \wedge K\tilde{}(u, v\tilde{}))\fatsemi Q\tilde{}_{Op}(j\tilde{}, k, v\tilde{}, w)$, we pick $j\tilde{}$ and $v\tilde{}$, for which $R\tilde{}_{Op}(i, j\tilde{})$, $K\tilde{}(u, v\tilde{})$ and $Q\tilde{}_{Op}(j\tilde{}, k, v\tilde{}, w)$ hold. Next, $G(u, w) = K\tilde{}(u, v\tilde{})\fatsemi H\tilde{}(v\tilde{}, w)$, so we pick $\bar{v}\tilde{}$, for which $K\tilde{}(u, \bar{v}\tilde{})$ and $H\tilde{}(\bar{v}\tilde{}, w)$ hold. We have $K\tilde{}(u, v\tilde{})$, $Q\tilde{}_{Op}(j\tilde{}, k, v\tilde{}, w)$, $K\tilde{}(u, \bar{v}\tilde{})$ and $H\tilde{}(\bar{v}\tilde{}, w)$. Thus, by (X1), $v\tilde{} = \bar{v}\tilde{}$, which means $H\tilde{}(v\tilde{}, w)$ must hold too. Hence, by (X3), $InitIn_{Op_X}(h, j\tilde{})$ holds.

It remains to show $R^\circ_{Op}(j\tilde{}, j)$. We thus confirm both conjuncts of (6.32). The second conjunct is immediate because we have $R\tilde{}_{Op}(i, j\tilde{})$. Consider the first conjunct. Assume $P_{Op}(i, k, \underline{u}, \underline{w}) \wedge K\tilde{}(\underline{u}, \underline{v}\tilde{}) \wedge H\tilde{}(\underline{v}\tilde{}, \underline{w})$. We want $Q\tilde{}_{Op}(j\tilde{}, k, \underline{v}\tilde{}, \underline{w})$. From $P_{Op}(i, k, \underline{u}, \underline{w})$, by composition, we have $\underline{i}\tilde{}$ and $\underline{\underline{v}}\tilde{}$, for which $R\tilde{}_{Op}(i, \underline{i}\tilde{})$, $K\tilde{}(\underline{u}, \underline{\underline{v}}\tilde{})$ and $Q\tilde{}_{Op}(\underline{i}\tilde{}, k, \underline{\underline{v}}\tilde{}, \underline{w})$ hold. Now, $R\tilde{}_{Op}(i, j\tilde{})$, $Q\tilde{}_{Op}(j\tilde{}, k, v\tilde{}, w)$, $R\tilde{}_{Op}(i, \underline{i}\tilde{})$, $Q\tilde{}_{Op}(\underline{i}\tilde{}, k, \underline{\underline{v}}\tilde{}, \underline{w})$ and (X2) give $\underline{i}\tilde{} = j\tilde{}$. Similarly, $K\tilde{}(\underline{u}, \underline{\underline{v}}\tilde{})$, $Q\tilde{}_{Op}(\underline{i}\tilde{}, k, \underline{\underline{v}}\tilde{}, \underline{w})$, $K\tilde{}(\underline{u}, \underline{v}\tilde{})$, $H\tilde{}(\underline{v}\tilde{}, \underline{w})$ and (X1) give $\underline{\underline{v}}\tilde{} = \underline{v}\tilde{}$. Thus, since $Q\tilde{}_{Op}(\underline{i}\tilde{}, k, \underline{\underline{v}}\tilde{}, \underline{w})$ holds, then so does $Q\tilde{}_{Op}(j\tilde{}, k, \underline{v}\tilde{}, \underline{w})$. We are done. ■

6.3.2.3 The initialisation PO

We show

$$Init_{\mathrm{U}}(v') \;\Rightarrow\; (\exists\, \tilde{v}' \bullet Init_{\mathrm{X}}(\tilde{v}') \wedge K^{\circ}(\tilde{v}', v')) \,. \tag{6.35}$$

Proof. Assume the antecedent with $v' = (u', w')$. From $Init_{\mathrm{U}}(v')$, by (6.1), we thus have $Init_{\mathrm{A}}(u')$, $Init_{\mathrm{C}}(w')$ and $G(u', w')$. From the latter, it follows that $\tilde{K}(u, \tilde{v}) \fatsemi \tilde{H}(\tilde{v}, w)$ must be true. So, picking $\tilde{v}$, we have $\tilde{K}(u, \tilde{v})$ and $\tilde{H}(\tilde{v}, w)$. We now have enough to be able to use (X4) to obtain $Init_{\mathrm{X}}(\tilde{v}')$, which we want. All we need now is $K^{\circ}(\tilde{v}', v')$. Therefore by (6.31), we need $G(u, w) \Rightarrow \tilde{H}(\tilde{v}, w)$ and $\tilde{K}(u, \tilde{v})$. Both of these hold. Done. ■

6.3.2.4 The applicability PO

We show

$$K^{\circ}(\tilde{v}, v) \wedge R^{\circ}_{Op}(\tilde{j}, j) \wedge trm_{Op_{\mathrm{X}}}(\tilde{v}, \tilde{j}) \;\Rightarrow\; trm_{Op_{\mathrm{U}}}(v, j) \,. \tag{6.36}$$

Proof. Assume the antecedents and let $v = (u, w)$ and $j = (i, k)$. Suppose that for these values $trm_{Op_{\mathrm{A}}}(u, i)$ is false. Then $trm_{Op_{\mathrm{U}}}(v, j)$ holds by (6.3a). Alternatively, suppose $trm_{Op_{\mathrm{A}}}(u, i)$ is true. Then we have two further possibilities. Either $G(u, w) \wedge P_{Op}(i, k, u, w)$ holds, or it does not. The proofs for these two cases mirror those given for PO (6.14) and establish either (6.3b) or (6.3c). Hence $trm_{Op_{\mathrm{U}}}(v, j)$ holds, as required. ■

6.3.2.5 The correctness PO

We show

$$\begin{aligned} &K^{\circ}(\tilde{v}, v) \wedge R^{\circ}_{Op}(\tilde{j}, j) \wedge trm_{Op_{\mathrm{X}}}(\tilde{v}, \tilde{j}) \wedge stp_{Op_{\mathrm{U}}}(v, j, v', p) \;\Rightarrow \\ &\quad (\exists\, \tilde{v}', \tilde{p} \bullet stp_{Op_{\mathrm{X}}}(\tilde{v}, \tilde{j}, \tilde{v}', \tilde{p}) \wedge K^{\circ}(\tilde{v}', v') \wedge V^{\circ}_{Op}(\tilde{p}, p)) \end{aligned} \tag{6.37}$$

for *Univ* steps which are abstract core bound.

Proof. Assume the antecedents and let $v = (u, w)$, $j = (i, k)$, $v' = (u', w')$ and $p = (o, q)$. We are only interested in steps in $stp_{Op_{\mathrm{U}}}(v, j, v', p)$ which are abstract core bound. Hence, by Definition 3.1, there must be values, $\underline{w}$ and $\underline{k}$ say, such that $H^{\bullet}(v, \underline{w}) \wedge Q^{\bullet}_{Op}(j, \underline{k}, v, \underline{w})$

holds. Then, by (6.19), we have $\underline{w} = w$ and $G(u, w)$; by (6.20), we have $\underline{k} = k$ and $P_{Op}(i, k, u, w)$. Now, since $G(u, w) \wedge P_{Op}(i, k, u, w)$ holds, by PO (6.15), so must $trm_{Op_A}(u, i)$.

Next, from $K^{\circ}(\tilde{v}, v)$ and $G(u, w)$, we get $K^{\sim}(u, \tilde{v})$ and $H^{\sim}(\tilde{v}, w)$, by (6.31). Then, from $R^{\circ}_{Op}(\tilde{j}, j)$ and $P_{Op}(i, k, u, w)$, $K^{\sim}(u, \tilde{v})$ and $H^{\sim}(\tilde{v}, w)$, we get $Q^{\sim}_{Op}(\tilde{j}, k, \tilde{v}, w)$ and $R^{\sim}_{Op}(i, \tilde{j})$, by (6.32). We have $stp_{Op_U}(v, j, v', p)$, $trm_{Op_A}(u, i)$, $G(u, w)$ and $P_{Op}(i, k, u, w)$. Therefore, (6.2b) says $stp_{Op_A}(u, i, u', o)$, $stp_{Op_C}(w, k, w', q)$, $((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w))$ are all also true. We now proceed by assuming each disjunct of $(G' \wedge O_{Op}) \vee C_{Op}$ in turn.

First suppose $(G' \wedge O_{Op})$ holds. Then G' says $K^{\sim}(u', \tilde{v}')\fatsemi H^{\sim}(\tilde{v}', w')$ is true. So we have $\underline{\tilde{v}}'$ say, for which $K^{\sim}(u', \underline{\tilde{v}}')$ and $H^{\sim}(\underline{\tilde{v}}', w')$ are true. Similarly O_{Op} implies $(V^{\sim}_{Op}(o, \tilde{p}) \wedge K^{\sim}(u', \tilde{v}') \wedge R^{\sim}_{Op}(i, \tilde{j}) \wedge K^{\sim}(u, \tilde{v}))\fatsemi N^{\sim}_{Op}(\tilde{p}, q; \tilde{v}', w', \tilde{j}, k, \tilde{v}, w)$. So we have $\underline{\tilde{p}}$, $\underline{\tilde{v}}'$, $\underline{\tilde{j}}$ and $\underline{\tilde{v}}$ say, for which $V^{\sim}_{Op}(o, \underline{\tilde{p}})$, $K^{\sim}(u', \underline{\tilde{v}}')$, $R^{\sim}_{Op}(i, \underline{\tilde{j}})$, $K^{\sim}(u, \underline{\tilde{v}})$ and $N^{\sim}_{Op}(\underline{\tilde{p}}, q; \underline{\tilde{v}}', w', \underline{\tilde{j}}, k, \underline{\tilde{v}}, w)$ are true. Then, using (X1), first with $K^{\sim}(u', \underline{\tilde{v}}')$ and $H^{\sim}(\underline{\tilde{v}}', w')$, we get $\underline{\tilde{v}}' = \underline{\tilde{v}}'$; second with $K^{\sim}(u, \tilde{v})$ and $H^{\sim}(\tilde{v}, w)$, we get $\underline{\tilde{v}} = \tilde{v}$. Similarly, using (X2) with $R^{\sim}_{Op}(i, \tilde{j})$ and $Q^{\sim}_{Op}(\tilde{j}, k, \tilde{v}, w)$, we get $\underline{\tilde{j}} = \tilde{j}$. Therefore, altogether we have $stp_{Op_A}(u, i, u', o)$, $K^{\sim}(u, \tilde{v})$, $R^{\sim}_{Op}(i, \tilde{j})$, $K^{\sim}(u', \underline{\tilde{v}}')$, $V^{\sim}_{Op}(o, \underline{\tilde{p}})$, $H^{\sim}(\tilde{v}, w)$, $Q^{\sim}_{Op}(\tilde{j}, k, \tilde{v}, w)$, $H^{\sim}(\underline{\tilde{v}}', w') \wedge N^{\sim}_{Op}(\underline{\tilde{p}}, q; \underline{\tilde{v}}', w', \tilde{j}, k, \tilde{v}, w)$ and $stp_{Op_C}(w, k, w', q)$. Thus $stp_{Op_X}(\tilde{v}, \tilde{j}, \underline{\tilde{v}}', \underline{\tilde{p}})$ holds by (X5).

Second suppose C_{Op} holds. Then $(K^{\sim}(u', \tilde{v}') \wedge V^{\sim}_{Op}(o, \tilde{p}) \wedge R^{\sim}_{Op}(i, \tilde{j}) \wedge K^{\sim}(u, \tilde{v}))\fatsemi D^{\sim}_{Op}(\tilde{v}', w', \tilde{p}, q; \tilde{j}, k, \tilde{v}, w)$ is true. We now use similar steps to those in the previous paragraph, and for this case we end up with $stp_{Op_A}(u, i, u', o)$, $K^{\sim}(u, \tilde{v})$, $R^{\sim}_{Op}(i, \tilde{j})$, $K^{\sim}(u', \underline{\tilde{v}}')$, $V^{\sim}_{Op}(o, \underline{\tilde{p}})$, $H^{\sim}(\tilde{v}, w)$, $Q^{\sim}_{Op}(\tilde{j}, k, \tilde{v}, w)$, $D^{\sim}_{Op}(\underline{\tilde{v}}', w', \underline{\tilde{p}}, q; \tilde{j}, k, \tilde{v}, w)$ and $stp_{Op_C}(w, k, w', q)$. Thus $stp_{Op_X}(\tilde{v}, \tilde{j}, \underline{\tilde{v}}', \underline{\tilde{p}})$ holds by (X5) once again.

So we have $\underline{\tilde{v}}'$ and $\underline{\tilde{p}}$ and $stp_{Op_X}(\tilde{v}, \tilde{j}, \underline{\tilde{v}}', \underline{\tilde{p}})$. It remains to show $K^{\circ}(\underline{\tilde{v}}', v')$ and $V^{\circ}_{Op}(\underline{\tilde{p}}, p)$. Take V°_{Op}. This holds by (6.33) because we have $V^{\sim}_{Op}(o, \underline{\tilde{p}})$. To show $K^{\circ}(\underline{\tilde{v}}', v')$ we need to establish both conjuncts of (6.31). The second conjunct holds because we have $K^{\sim}(u', \underline{\tilde{v}}')$. To show the first assume $G(u', w')$. We require $H^{\sim}(\underline{\tilde{v}}', w')$. We already have this for the case $(G' \wedge O_{Op})$. For the case when C_{Op} holds we argue thus. As $G(u', w') = K^{\sim}(u', \tilde{v}')\fatsemi H^{\sim}(\tilde{v}', w')$, we can choose a value, $\bar{v}^{\sim\prime}$ say, for which $K^{\sim}(u', \bar{v}^{\sim\prime})$ and $H^{\sim}(\bar{v}^{\sim\prime},$

w') hold. Now, $K^{\sim}(u', \underline{\underline{v}}^{\sim\prime})$ and $D^{\sim}_{Op}(\underline{\underline{v}}^{\sim\prime}, w', ...)$ also hold. Therefore, by (X1), $\underline{\underline{v}}^{\sim\prime} = \bar{v}^{\sim\prime}$. Consequently, since $H^{\sim}(\bar{v}^{\sim\prime}, w')$ is true, then so is $H^{\sim}(\underline{\underline{v}}^{\sim\prime}, w')$. We are done.

6.3.2.6 The output finalisation PO

We show

$$V^{\circ}_{Op}(p^{\sim}, p) \wedge FinOut_{Op_U}(p, n) \;\Rightarrow\; FinOut_{Op_X}(p^{\sim}, n)\ . \tag{6.38}$$

Proof. Assume the antecedents and let $p = (o, q)$. From $V^{\circ}_{Op}(p^{\sim}, p)$, by (6.33), $V^{\sim}_{Op}(o, p^{\sim})$ is true. From $FinOut_{Op_U}(p, n)$, by (6.11), $n = o$. Therefore, by (X6), $FinOut_{Op_X}(p^{\sim}, n)$ holds, as required. ■

6.3.3 The inclusions

Below we list the inclusions of part (2) of the theorem in detail.

$$H^{\sim}(v^{\sim}, w) \Rightarrow K^{\circ}(v^{\sim}, v) \fatsemi H^{\bullet}(v, w) \tag{6.39}$$

$$Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w) \Rightarrow (R^{\circ}_{Op}(j^{\sim}, j) \wedge K^{\circ}(v^{\sim}, v)) \fatsemi Q^{\bullet}_{Op}(j, k, v, w) \tag{6.40}$$

$$\begin{aligned} &N^{\sim}_{Op}(p^{\sim}, q; v^{\sim\prime}, w', j^{\sim}, k, v^{\sim}, w) \Rightarrow \\ &\quad (V^{\circ}_{Op}(p^{\sim}, p) \wedge K^{\circ}(v^{\sim\prime}, v') \wedge R^{\circ}_{Op}(j^{\sim}, j) \wedge K^{\circ}(v^{\sim}, v)) \fatsemi N^{\bullet}_{Op}(p, q; v', w', j, k, v, w) \end{aligned} \tag{6.41}$$

$$\begin{aligned} &D^{\sim}_{Op}(v^{\sim\prime}, w', p^{\sim}, q; j^{\sim}, k, v^{\sim}, w) \Rightarrow \\ &\quad (K^{\circ}(v^{\sim\prime}, v') \wedge V^{\circ}_{Op}(p^{\sim}, p) \wedge R^{\circ}_{Op}(j^{\sim}, j) \wedge K^{\circ}(v^{\sim}, v)) \fatsemi D^{\bullet}_{Op}(v', w'; p, q, j, k, v, w) \end{aligned} \tag{6.42}$$

$$K^{\sim}(u, v^{\sim}) \fatsemi K^{\circ}(v^{\sim}, v) \Rightarrow K^{\bullet}(u, v) \tag{6.43}$$

$$R^{\sim}_{Op}(i, j^{\sim}) \fatsemi R^{\circ}_{Op}(j^{\sim}, j) \Rightarrow R^{\bullet}_{Op}(i, j) \tag{6.44}$$

$$V^{\sim}_{Op}(o, p^{\sim}) \fatsemi V^{\circ}(p^{\sim}, p) \Rightarrow V^{\bullet}_{Op}(o, p)\ . \tag{6.45}$$

We now show these inclusions hold.

♦ (6.39): $H^{\sim}(v^{\sim}, w) \Rightarrow K^{\circ}(v^{\sim}, v) \fatsemi H^{\bullet}(v, w)$.

Proof. Assume the antecedent $H^{\sim}(v^{\sim}, w)$. Since $K^{\sim}$ is surjective there must be a state, u say, such that $K^{\sim}(u, v^{\sim})$ holds. Then from $K^{\sim}(u, v^{\sim})\fatsemi H^{\sim}(v^{\sim}, w)$ we get $G(u, w)$. Let $v = (u, w)$. Then first, $K^{\circ}(v^{\sim}, v)$ holds, by (6.31); second, $H^{\bullet}(v, w)$ holds, by (6.19). Done. ■

♦ (6.40): $Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w) \Rightarrow (R^{\circ}_{Op}(j^{\sim}, j) \wedge K^{\circ}(v^{\sim}, v))\fatsemi Q^{\bullet}_{Op}(j, k, v, w)$.

Proof. Assume the antecedent $Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w)$. Since $K^{\sim}$ and $R^{\sim}_{Op}$ are surjective there must be values, i and u say, such that $R^{\sim}_{Op}(i, j^{\sim})$ and $K^{\sim}(u, v^{\sim})$ hold. Then from $(R^{\sim}_{Op}(i, j^{\sim}) \wedge K^{\sim}(u, v^{\sim}))\fatsemi Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w)$ we get $P_{Op}(i, k, u, w)$. Let $j = (i, k)$ and $v = (u, w)$. Then $Q^{\bullet}_{Op}(j, k, v, w)$ holds, by (6.20).

It remains to show $R^{\circ}_{Op}(j^{\sim}, j)$ and $K^{\circ}(v^{\sim}, v)$. Take $R^{\circ}_{Op}(j^{\sim}, j)$ first. We establish both conjuncts of (6.32). The second conjunct is immediate because we have $R^{\sim}_{Op}(i, j^{\sim})$. To show the first conjunct assume $P_{Op}(i, k, \underline{u}, \underline{w}) \wedge K^{\sim}(\underline{u}, \underline{v}^{\sim}) \wedge H^{\sim}(\underline{v}^{\sim}, \underline{w})$. We require $Q^{\sim}_{Op}(j^{\sim}, k, \underline{v}^{\sim}, \underline{w})$. Now $P_{Op}(i, k, \underline{u}, \underline{w})$ implies $(R^{\sim}_{Op}(i, \underline{j}^{\sim}) \wedge K^{\sim}(\underline{u}, \underline{\underline{v}}^{\sim}))\fatsemi Q^{\sim}_{Op}(\underline{j}^{\sim}, k, \underline{\underline{v}}^{\sim}, \underline{w})$. Thus, fixing witnesses, we have $R^{\sim}_{Op}(i, \underline{j}^{\sim})$, $K^{\sim}(\underline{u}, \underline{\underline{v}}^{\sim})$ and $Q^{\sim}_{Op}(\underline{j}^{\sim}, k, \underline{\underline{v}}^{\sim}, \underline{w})$. Then, $R^{\sim}_{Op}(i, j^{\sim})$, $Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w)$, $R^{\sim}_{Op}(i, \underline{j}^{\sim})$ and $Q^{\sim}_{Op}(\underline{j}^{\sim}, k, \underline{\underline{v}}^{\sim}, \underline{w})$ give, by (X2), $j^{\sim} = \underline{j}^{\sim}$. Similarly, $K^{\sim}(\underline{u}, \underline{v}^{\sim})$, $H^{\sim}(\underline{v}^{\sim}, \underline{w})$, $K^{\sim}(\underline{u}, \underline{\underline{v}}^{\sim})$, $Q^{\sim}_{Op}(\underline{j}^{\sim}, k, \underline{\underline{v}}^{\sim}, \underline{w})$ and (X1) give $\underline{v}^{\sim} = \underline{\underline{v}}^{\sim}$. Hence, $Q^{\sim}_{Op}(\underline{j}^{\sim}, k, \underline{\underline{v}}^{\sim}, \underline{w})$ furnishes $Q^{\sim}_{Op}(j^{\sim}, k, \underline{v}^{\sim}, \underline{w})$.

To show $K^{\circ}(v^{\sim}, v)$ we need to establish both conjuncts of (6.31). The second conjunct is true because we have $K^{\sim}(u, v^{\sim})$. To show the first conjunct assume $G(u, w)$. We require $H^{\sim}(v^{\sim}, w)$. Now $G(u, w)$ implies $K^{\sim}(u, \underline{\underline{v}}^{\sim})\fatsemi H^{\sim}(\underline{\underline{v}}^{\sim}, w)$. Thus, fixing witnesses, we have $K^{\sim}(u, \underline{\underline{v}}^{\sim})$ and $H^{\sim}(\underline{\underline{v}}^{\sim}, w)$. Then, because we also have $K^{\sim}(u, v^{\sim})$ and $Q^{\sim}_{Op}(j^{\sim}, k, v^{\sim}, w)$, by (X1), $v^{\sim} = \underline{\underline{v}}^{\sim}$. Hence, from $H^{\sim}(\underline{\underline{v}}^{\sim}, w)$, we get $H^{\sim}(v^{\sim}, w)$, as required. We are done. ■

♦ (6.41) and (6.42).

Proof. Similar to (6.40). ■

♦ (6.43): $K^{\sim}(u, v^{\sim})\fatsemi K^{\circ}(v^{\sim}, v) \Rightarrow K^{\bullet}(u, v)$.

Proof. Assume the antecedent. Thus, fixing the witness we have $K^{\sim}(u, v^{\sim})$ and $K^{\circ}(v^{\sim}, v)$. Let $v = (\underline{u}, \underline{w})$. Then from K°, by (6.31), $K^{\sim}(\underline{u}, v^{\sim})$ holds. But $K^{\sim}$ is injective. Thus $u = \underline{u}$ and therefore $v = (u, \underline{w})$. Hence, $K^{\bullet}(u, v)$ holds by (6.4). ■

♦ (6.44) and (6.45).

Proof. Similar to (6.43). ■

6.4 Proof for Part (3)

Part (3) of the theorem follows readily by observing that for a system *Univ** having the same properties as *Univ*, there will be a refinement from *Univ* to *Univ** and a refinement from *Univ** to *Univ*. ☺ ■

This completes the proof of Theorem 6.1.

6.5 Idempotence

One of the aims of the lowering construction is for the abstract core bound transitions of *Univ* to be at the level of abstraction of *Conc*. We therefore constructed *Univ* so that for all other systems *Xtra* achieving the same decomposition, there was a refinement from *Xtra* to the abstract core bound transitions of *Univ*. But can we be sure the level of abstraction is low enough? As further indication that we are at the desired level, we show that applying the lowering construction to *Univ* results in a system *UUniv* whose abstract core bound transitions are those of *Univ*.

For the abstract core bound transitions $cbt_{Op_U}(v, j, v', p)$ of *Univ*, we saw in Section 6.3.2.5 that $G(u, w) \wedge P_{Op}(i, k, u, w) \wedge trm_{Op_A}(u, i)$ holds. Therefore,

$$
\begin{aligned}
& cbt_{Op_U}(v, j, v', p) \\
& = \\
& v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge \\
& G(u, w) \wedge P_{Op}(i, k, u, w) \wedge trm_{Op_A}(u, i) \wedge stp_{Op_U}(v, j, v', p) \\
& = \text{[by (6.2), and using obvious abbreviations]} \\
& trm_{Op_A} \wedge GP_{Op} \wedge \big(\big(trm_{Op_A} \wedge \neg GP_{Op} \Rightarrow stp_{Op_A} \big) \wedge \\
& \quad \big(trm_{Op_A} \wedge GP_{Op} \Rightarrow stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op} \big) \big) \\
& = [\ a \wedge (a \wedge b \Rightarrow c) \Leftrightarrow a \wedge (b \Rightarrow c)\ ] \\
& trm_{Op_A} \wedge GP_{Op} \wedge \big(\big(\neg GP_{Op} \Rightarrow stp_{Op_A} \big) \wedge \big(GP_{Op} \Rightarrow stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op} \big) \big) \\
& = [\ (a \wedge \neg a \Rightarrow b) \Leftrightarrow a, \quad a \wedge (a \Rightarrow b) \Leftrightarrow a \wedge b\ ] \\
& trm_{Op_A} \wedge \big(\big(GP_{Op} \big) \wedge \big(GP_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op} \big) \big)
\end{aligned}
$$

$= [\ a \wedge a \Leftrightarrow a,\quad trm_{Op_A} \wedge stp_{Op_A} \Leftrightarrow stp_{Op_A}]$

$GP_{Op} \wedge stp_{Op_A} \wedge stp_{Op_C} \wedge G'OC_{Op}$

$= [\text{ expanding}]$

$$G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$$
$$(\ (G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)\ ) \qquad (6.46)$$

Analogously, the abstract core bound transitions of *UUniv* will be

$$cbt_{Op_{UU}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) =$$
$$\mathbf{(}\ \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$$
$$H^{\bullet}(v, w) \wedge Q^{\bullet}_{Op}(j, k, v, w) \wedge stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$$
$$(\ (H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)) \vee D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)\ )\ \mathbf{)}\ . \qquad (6.47)$$

Expanding this gives

$$cbt_{Op_{UU}}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$$
$$=$$
$$\mathbf{(}\ \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$$
$$v = (u, w) \wedge G(v, w) \wedge$$
$$v = (u, w) \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge$$
$$stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$$
$$(\ (H^{\bullet}(v', w') \wedge N^{\bullet}_{Op}(p, q; v', w', j, k, v, w)) \vee D^{\bullet}_{Op}(v', w', p, q; j, k, v, w)\ )\ \mathbf{)}$$

$= [\text{ expanding }]$

$$\mathbf{(}\ \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$$
$$v = (u, w) \wedge G(u, w) \wedge$$
$$v = (u, w) \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge$$
$$stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$$
$$(\ (v' = (u', w') \wedge G(u', w') \wedge$$
$$p = (o, q) \wedge j = (i, k) \wedge v = (u, w) \wedge O_{Op}(o, q; u', w', i, k, u, w)\ ) \vee$$
$$(\ v' = (u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (u, w) \wedge C_{Op}(u', w', o, q; i, k, u, w)\ )\ )\ \mathbf{)}$$

$= [\ (a \wedge b) \vee (a \wedge c) \Leftrightarrow a \wedge (b \vee c)\ ]$

$$\mathbf{(}\ \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$$
$$v = (u, w) \wedge G(u, w) \wedge$$

$v = (u, w) \wedge j = (i, k) \wedge P_{Op}(i, k, u, w) \wedge$

$stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$

$v' = (u', w') \wedge p = (o, q) \wedge j = (i, k) \wedge v = (u, w) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \;\mathbf{)}$

= [a ∧ a ⇔ a, rearranging]

$\mathbf{(}\; \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$

$v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge$

$G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \;\mathbf{)}$

= [by (6.15), $G \wedge P \Rightarrow trm_{Op_A}$, hence $G \wedge P \;\Leftrightarrow G \wedge P \wedge trm_{Op_A}$]

$\mathbf{(}\; \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$

$v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge$

$G(u, w) \wedge P_{Op}(i, k, u, w) \wedge trm_{Op_A}(u, i) \wedge stp_{Op_U}(v, j, v', p) \wedge stp_{Op_C}(w, k, w', q) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \;\mathbf{)}$

= [by (6.46), since $G \wedge P_{Op} \wedge trm_{Op_A} \wedge stp_{Op_U} = cbt_{Op_U}$]

$\mathbf{(}\; \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$

$v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge$

$G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \wedge$

$stp_{Op_C}(w, k, w', q) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \;\mathbf{)}$

= [a ∧ a ⇔ a]

$\mathbf{(}\; \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$

$v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge$

$G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(w, k, w', q) \wedge$

$((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \;\mathbf{)}$

= [(6.46)]

$\mathbf{(}\; \underline{v} = (v, w) \wedge \underline{j} = (j, k) \wedge \underline{v}' = (v', w') \wedge \underline{p} = (p, q) \wedge$

$v = (u, w) \wedge j = (i, k) \wedge v' = (u', w') \wedge p = (o, q) \wedge$

$cbt_{Op_U}(v, j, v', p) \;\mathbf{)}$

= [substituting]

$\mathbf{(}\; \underline{v} = ((u, w), w) \wedge \underline{j} = ((i, k), k) \wedge \underline{v}' = ((u', w'), w') \wedge \underline{p} = ((o, q), q) \wedge$

$cbt_{Op_U}((u, w), (i, k), (u', w'), (o, q)) \;\mathbf{)}$

So we see that repeating the construction leads to a system whose data is that of *Univ* but with redundant duplications. Such a system is obviously interrefinable with *Univ* and hence equivalent to *Univ* for all our purposes.

6.6 Inside *Univ*

To close this chapter we use the Number Recycler example as described in Section 5.6 to exhibit the structure of *Univ*. The states of *Univ* are pairs (u, w) such that u is a set of natural numbers and w is a sequence of natural numbers, e.g. $(\{3, 41\}, \langle 8, 50, 51\rangle\}$. Note once again that w is not necessarily a serialisation of u.

From the retrenchment PO (6.15), we know $G \wedge P_{Op}$ and thus $trm_{Op_A} \wedge trm_{Op_C}$ hold for those parts of *Abs* and *Conc* related by retrenchment. We keep this in mind as we examine the transitions of *Univ*. By (6.2), the transitions separate into three groups. The first consists of transitions for which trm_{Op_A} does not hold and therefore cannot be concerned with the *Abs* to *Conc* retrenchment. The second group consists of *Abs* transitions for which $\neg(G \wedge P_{Op})$. Such *Abs* transitions, and therefore this group of *Univ* transitions, also fall outside the scope of the retrenchment. The function of these two groups is to provide transitions for those parts of *Abs*, *Xtra* and *Univ*, not related to *Conc* by retrenchment, so that the relevant refinement POs can be satisfied.

What remains is the third group which contains *Univ* transitions for which $G \wedge P_{Op}$ holds. We saw in Section 6.5 that these are the abstract core bound transitions of *Univ*. Hence the abstract core bound transitions are the part of *Univ* concerned with the retrenchment from *Abs* to *Conc*. The abstract core bound transitions combine *Abs* and *Conc* steps that are in simulation. We can think of the lowering construction as tagging simulable *Abs* steps with corresponding *Conc* steps. Examples of abstract core bound steps for non-boundary cases for Add_U and Rem_U are

$$(\{1, 2\}, \langle 2, 1\rangle) \text{ -}((3, 3), Add_U, (\mathsf{OK}, \mathsf{OK}))\text{-}\rightarrow (\{1, 2, 3\}, \langle 2, 1, 3\rangle)$$

and

$$(\{1, 2, 3\}, \langle 3, 1, 2\rangle) \text{ -}(Rem_U, (3, 3))\text{-}\rightarrow (\{1, 2\}, \langle 1, 2\rangle) ,$$

and we see they pair steps related by the retrenchment.

For boundary cases a typical Add_{U} step is

$$(\{1 .. 5\}, \langle 1 .. 5\rangle) \text{ -((8, 8), } Add_{\mathrm{U}}\text{, (OK, FULL))-›} (\{1 .. 5, 8\}, \langle 1 .. 5\rangle) .$$

For Rem_{U} we find the situation is the same as in the lifting construction. There is no step which describes the removal of a number from an empty bin: P_{Rem} does not hold, consequently there can be no abstract core bound *Univ* step.

As was the position for the abstract lifting in Chapter 5, the systems which decompose the retrenchment belong to a class. The properties which define the class in this case are analogues of ones we saw in the previous chapter, except (X4) and (X5). (X5) restricts the systems to ones which ***at least*** lower the same *Abs* steps *Conc* does, and is consistent with finding a concrete representation of those *Abs* steps simulated in *Conc*. (X4) is the counterpart for initial values.

Chapter 7

Completing the Square

It was relatively straightforward to get the triangles in the lifting and lowering theorems to commute. This turns out not to be the case for the squares in the post- and prejoins. This time we have to work a lot harder to obtain commutativity. Consequently the material which presents the technical details of the constructions is considerably more complicated. The purpose behind this chapter is therefore to provide the reader with some insight into the function of some of the components used in the construction of the squares. We only discuss the postjoin construction. By symmetry the prejoin is similar.

7.1 The Square and Its Components

Recall from Chapter 4 that an objective of the postjoin construction is to obtain a system *Univ* which is a refinement of *Ret* and a retrenchment of *Ref*, such that the square commutes. Thus when the given retrenchment is composed with the new refinement on the one hand, and the given refinement is composed with the new retrenchment on the other, they are equal as retrenchments from *Abs* to *Univ*. We recap this in Figure 7.1.

Let the state space of *Abs* be U with $u \in \mathsf{U}$, the inputs be $i \in \mathsf{I}$ and the outputs $o \in \mathsf{O}$. For *Ret* we have $v \in \mathsf{V}$, $j \in \mathsf{J}$, $p \in \mathsf{P}$; for *Ref* $w \in \mathsf{W}$, $k \in \mathsf{K}$, $q \in \mathsf{Q}$; and for *Univ* $t \in \mathsf{T}$, $h \in \mathsf{H}$, $s \in \mathsf{S}$.

Let H, Q, N and D be the retrieve, within, output and concedes relations for the retrenchment from *Abs* to *Ret*. Similarly, let $H^\bullet$, $Q^\bullet$, $N^\bullet$ and $D^\bullet$ be the relations for the retrenchment from *Ref* to *Univ*. The data for the refinement from *Abs* to *Ref* has retrieve relation K, input retrieve relation R and output retrieve relation V. Likewise, let $K^\bullet$, $R^\bullet$ and $V^\bullet$ be

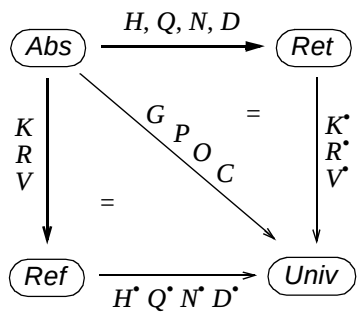


Figure 7.1: Completing the square in a prejoin.

the relations for the refinement from *Ret* to *Univ*. Finally, let G, P, O and C be the retrieve, within, output and concedes relations for the retrenchment from *Abs* to *Univ*. These are all shown in Figure 7.1. We start by discussing systems with no I/O components and focus just on the retrieve relation G.

7.2 Overture on *G*

We define G in terms of the other retrieve relations, and if the square is to commute then

$$G(u, t) \;=\; H(u, \underline{v}) \fatsemi K^{\bullet}(\underline{v}, t) \;=\; K(u, \underline{w}) \fatsemi H^{\bullet}(\underline{w}, t)\ , \tag{7.1}$$

which we write as $G(u, t) = H \fatsemi K^{\bullet}(u, t) = K \fatsemi H^{\bullet}(u, t)$ for short.

Consider Figure 7.2, where the spaces U, V and W consist only of the states shown. It should be evident that for the square to commute, whatever point w_0 is joined to in *Univ*, let us call it t_0, then both v_1 and v_2 must also be joined to the same point. We can picture a similar situation arising when two points w_1 and w_2 in *Ref* share a common point v_0 in *Ret*. To cover such cases we define the individual points in *Univ* to be ordered pairs of equivalence classes as follows.

$$\mathsf{T} = \mathsf{V}/{\sim_{\mathrm{V}}} \times \mathsf{W}/{\sim_{\mathrm{W}}}, \tag{7.2}$$

where

$$\sim_{\mathrm{V}} = ((K^{\mathrm{T}} \fatsemi H)^{\mathrm{T}} \fatsemi (K^{\mathrm{T}} \fatsemi H))^{*}\ , \tag{7.3}$$

$$\sim_{\mathrm{W}} = ((H^{\mathrm{T}} \fatsemi K)^{\mathrm{T}} \fatsemi (H^{\mathrm{T}} \fatsemi K))^{*}\ , \tag{7.4}$$

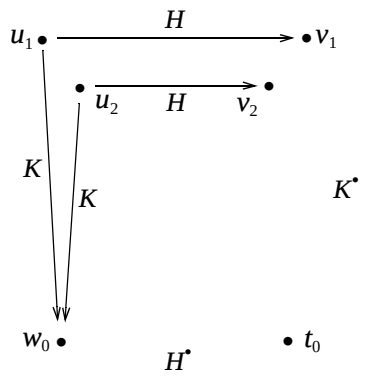


Figure 7.2

with $[v] \in \mathsf{V}/{\sim_V}$ and $[w] \in \mathsf{W}/{\sim_W}$. So for Figure 7.2 we have $[v_1] = [v_2] = \{v_1, v_2\}$, $[w_0] = \{w_0\}$, and $t_0 = ([v_1], [w_0])$. We now define

$$K^\bullet(\underline{v}, ([v], [w])) \;=\; \underline{v} \in [v]\,, \tag{7.5}$$

$$H^\bullet(\underline{w}, ([v], [w])) \;=\; \underline{w} \in [w]\,, \tag{7.6}$$

and so $H \fatsemi K^\bullet = K \fatsemi H^\bullet$, as shown in Figure 7.3,.

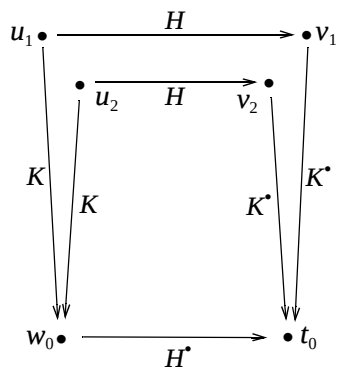


Figure 7.3

The equivalence classes capture more general arrangements, and in fact each $[v]$ is a set of states from *Ret*, which are connected (directly or indirectly) to a common state in *Ref* (via *Abs*); and similarly so for $[w]$. For instance, the setup in Figure 7.4 results in the classes $[v_1] = \{v_1, v_2, v_3, v_4\}$, $[w_1] = \{w_1, w_2\}$ and $[w_3] = \{w_3\}$. Here $\mathsf{T} = \{([v_1],[w_1]), ([v_1],[w_3])\}$. (Note that T pairs every $[v]$ with every $[w]$. This simplifies the definition of

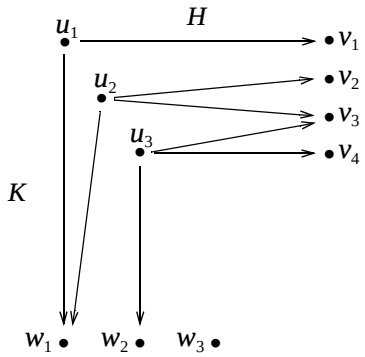


Figure 7.4

operations $Op_U \notin \mathsf{Ops}_A$. These only occur in *Ret* and not in *Ref*, and consequently only affect the first component of any ([v], [w]).)

Unfortunately, what we have so far is not enough to achieve commutativity. Consider Figure 7.5, where t_0 = ([v_0], [w_0]). Here, $K^\bullet(v_0, t_0)$ cannot hold, otherwise $H \fatsemi K^\bullet(u_1, t_0)$

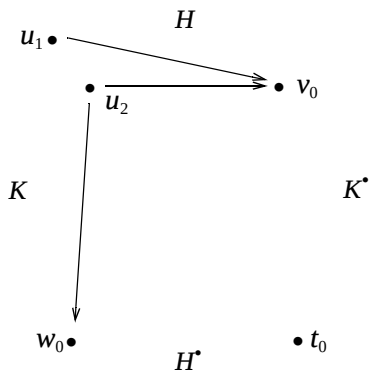


Figure 7.5

will hold, even though $K \fatsemi H^\bullet(u_1, t_0)$ cannot. To exclude such cases we change $K^\bullet$ to

$$K^\bullet(\underline{v}, ([v], [w])) \;=\; \underline{v} \in [v] \wedge HK([v], [w]) \;, \tag{7.7}$$

where

$$HK([v], [w]) \;=\; (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}))) \;. \tag{7.8}$$

We hasten to add that this is not the only possible approach, but it is just not feasible to discuss the pros and cons of each here. The intention is to give the reader an insight into the components that form the definitions he or she will encounter in subsequent chapters.

We must also change $H^\bullet$ otherwise $K \fatsemi H^\bullet(u_2, t_0)$ would be true whilst $H \fatsemi K^\bullet(u_2, t_0)$ would not. Hence

$$H^\bullet(\underline{w}, ([v], [w])) \;=\; \underline{w} \in [w] \wedge HK([v], [w]) \;. \tag{7.9}$$

To rule out with the situation pictured in Figure 7.6, we introduce a further modification.

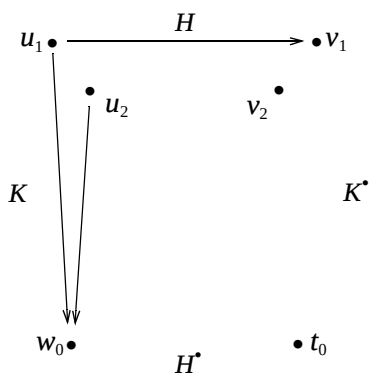


Figure 7.6

Let

$$H^\bullet(\underline{w}, ([v], [w])) \;=\; \underline{w} \in [w] \wedge HK([v], [w]) \wedge KH(\underline{w}, [v]) \;, \tag{7.10}$$

$$K^\bullet(\underline{v}, ([v], [w])) \;=\; \underline{v} \in [v] \wedge HK([v], [w]) \;, \tag{7.11}$$

where

$$KH(\underline{w}, [v]) \;=\; (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \;. \tag{7.12}$$

Thus (7.10) prevents $H^\bullet(w_0, t_0)$ from holding because we have $K(u_2, w_0)$, but no v to which H connects u_2, which means it is not possible for $H \fatsemi K^\bullet(u_2, t_0)$ to hold. Therefore we do not want $K \fatsemi H^\bullet(u_2, t_0)$. Notice we must also prevent $K^\bullet(v_1, t_0)$ from holding, otherwise $H \fatsemi K^\bullet(u_1, t_0)$ will hold, which compels $K \fatsemi H^\bullet(u_1, t_0)$ to hold, but this requires $H^\bullet(w_0, t_0)$,

which we have just said must not hold. To disallow $K^{\bullet}(v_1, t_0)$, we also add $KH(\underline{w}, [v])$ to the definition of $HK([v], [w])$ as follows.

$$HK([v], [w]) \;=\; (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow \\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))) \;. \tag{7.13}$$

There is one more constraint that we impose on $H^{\bullet}$. Consider the situation depicted in Figure 7.7.

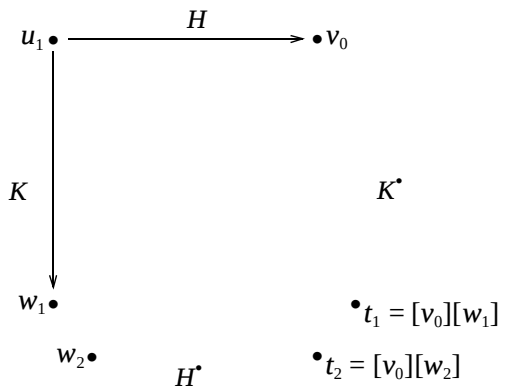


Figure 7.7

If we examine (7.10), we see that $H^{\bullet}(w_2, t_2)$ holds. However, there is no need for $H^{\bullet}$ to hold here, since there is no path from u_1 to w_2, and thus no possibility of $K \fatsemi H^{\bullet}(u_1, t_2)$ holding. We therefore prevent $H^{\bullet}$ holding, by adding the conjunct $(\exists\, u \bullet K(u, \underline{w}))$ to its definition as follows.

$$H^{\bullet}(\underline{w}, ([v], [w])) \;=\; \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge HK([v], [w]) \wedge KH(\underline{w}, [v]) \;. \tag{7.14}$$

Using definitions (7.11) to (7.14), we now have $G = H \fatsemi K^{\bullet} = K \fatsemi H^{\bullet}$.

7.3 Working in *C*

Thus far we have not taken into account other relations that involve the state. A retrenchment also has concedes relations, which can hold for pairs of after states for which the retrieve relation does not. The concedes relation for the retrenchment from *Abs* to *Univ* is $C_{Op}(u', t', o, s; i, h, u, t)$. We are only interested in the after states in this section, therefore

we hide the other components and write $C_{Op}(u', t', ...)$ as shorthand for $(\exists\, o, s, i, h, u, t \bullet C_{Op}(u', t', o, s; i, h, u, t))$, and similarly so for other relations. We define C_{Op} in terms of the concedes relations of the other retrenchments and the retrieve relations of the refinements as follows.

$$C_{Op}(u', t', ...) = D_{Op}(u', \underline{v}', ...) \fatsemi K^{\bullet}(\underline{v}', t') = K(u', \underline{w}') \fatsemi D^{\bullet}{}_{Op}(\underline{w}', t', ...)\ . \tag{7.15}$$

This has the same structure as (7.1), with D_{Op} and $D^{\bullet}{}_{Op}$, replacing H and $H^{\bullet}$ respectively. It is therefore not difficult to appreciate that in order for (7.15) to hold, we will need to take steps similar to those we saw above for G.

We start with the following observation. Take the case shown in Figure 7.8. By (7.3) and

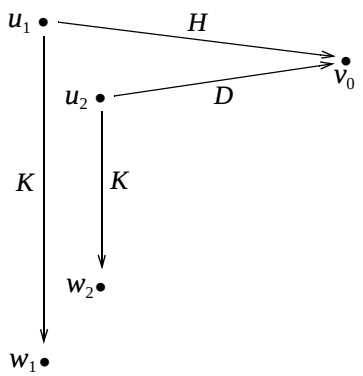


Figure 7.8

(7.4), the equivalence classes are the singletons $[v_0]$, $[w_1]$ and $[w_2]$, so $\mathsf{T} = \{([v_0], [w_1]), ([v_0], [w_2])\}$. Consider linking the state v_0 to the state $([v_0], [w_1]) = t_0$ in *Univ*. As shown in Figure 7.9, since $H \fatsemi K^{\bullet}(u_1, t_0)$ and $D \fatsemi K^{\bullet}(u_2, t_0)$ hold, both w_1 and w_2 will need to be joined to t_0, otherwise the square will not commute: G and/or C_{Op} will not hold. Consequently $D^{\bullet}{}_{Op}(w_2, t_0, ...)$ must be true. We are therefore going to need to define $D^{\bullet}{}_{Op}$ in such a way that we can link w_2 with $([v_0], [w_1])$, even though $w_2 \notin [w_1]$. This suggests that in fact w_1 and w_2 should both be in the same equivalence class, and this is the ap-

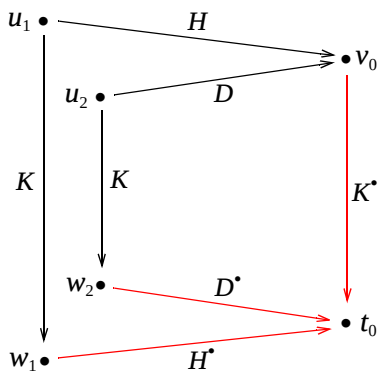


Figure 7.9

proach we adopt. We note there is a similar problem if we choose $([v_0], [w_2])$ for t_0, but this time with $H^\bullet$. We therefore redefine the equivalence relations to

$$\sim_V = ((K^T ⨾ HD)^T ⨾ (K^T ⨾ HD))^* , \tag{7.16}$$

$$\sim_W = ((HD^T ⨾ K)^T ⨾ (HD^T ⨾ K))^* , \tag{7.17}$$

where

$$HD(u, v) = H(u, v) \vee D_{Op}(u, v, ...) . \tag{7.18}$$

For the example, these equivalences give the class $[w_1] = \{w_1, w_2\}$, as required.

When defining $K^\bullet$ we must now concern ourselves with D_{Op} as well as H. We already know that to exclude cases like the one shown in Figure 7.5, where for u_1 we have $H(u_1, v_0)$ but no K, we need HK to hold. But exactly the same problems can arise with $D_{Op}(u', v', ...)$. So we need to strengthen $K^\bullet$ to

$$K^\bullet(\underline{v}, ([v], [w])) \;=\; \underline{v} \in [v] \wedge HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) . \tag{7.19}$$

Hence, $H^\bullet$ must change to

$$\begin{aligned} H^\bullet(\underline{w}, ([v], [w])) \;=\; & \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge \\ & HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) . \end{aligned} \tag{7.20}$$

To obtain $D^{\bullet}_{Op}$ we apply the same reasoning we used to derive $H^{\bullet}$. We find that

$$D^{\bullet}_{Op}(\underline{w}', ([v'], [w']), ...) \;=\; \underline{w}' \in [w'] \wedge (\exists\, u' \bullet K(u', \underline{w}')) \wedge KD_{Op}(\underline{w}', [v']) \wedge \\ HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \;, \tag{7.21}$$

where

$$DK_{Op}([v], [w]) \;=\; (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge D_{Op}(u, \underline{v}, ...) \Rightarrow \\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KD_{Op}(\underline{w}, [v]))) \;, \tag{7.22}$$

$$KD_{Op}(\underline{w}, [v]) \;=\; (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge D_{Op}(u, \underline{v}, ...))) \;. \tag{7.23}$$

With these definitions (7.1) and (7.15) both hold. We will treat the remaining components of C_{Op}, including the before states, in the next section.

An alternative approach to the problem in Figure 7.9, would be to simply exclude it. However, the arrangement arises from the perfectly reasonable retrenchment from *Abs* to *Ret* shown in Figure 7.10, which we do not want to rule out. The bold arrows in the figure

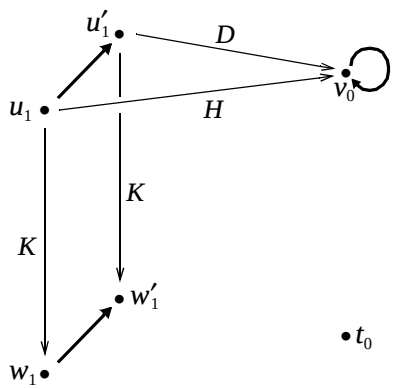


Figure 7.10

depict transitions. The transition $u_1 \mapsto u'_1$ is retrenched by $v_0 \mapsto v_0$, a skip, and refined by the step $w_1 \mapsto w'_1$. This is exactly the same setup as in the previous figure, only the states are labelled differently. Turining to *Univ* we ask what its transitions look like. In this example, the classes are $[v_0] = \{v_0\}$, $[w_1] = \{w_1, w'_1\}$ and there is only one *Univ* state t_0 =

$([v_0], [w_1])$. So the only possibility is $t_0 \mapsto t_0$. In this transition we in effect pair the corresponding steps $v_0 \mapsto v_0$ and $w_1 \mapsto w'_1$. We can think of the equivalence classes in $t_0 \mapsto t_0$ as together forming a container for the related *Ret* and *Ref* steps. We reinforce this view with another example.

Consider Figure 7.11. By (7.16) and (7.17), we have the singletons $[v_1]$ and $[v'_1]$, and the

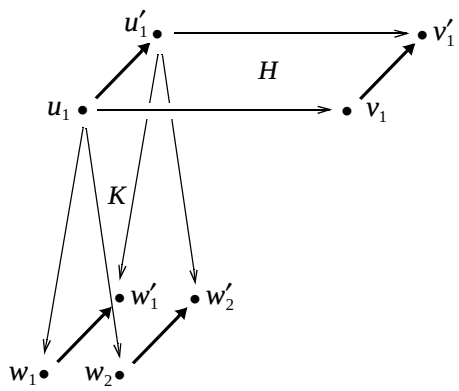


Figure 7.11

doubletons $[w_1] = \{w_1, w_2\}$ and $[w'_1] = \{w'_1, w'_2\}$. Hence, there are four *Univ* states $([v_1], [w_1])$, $([v_1], [w'_1])$, $([v'_1], [w_1])$ and $([v'_1], [w'_1])$. The definition for *Univ* transitions, which we omit here, identifies the corresponding transition as $([v_1], [w_1]) \mapsto ([v'_1], [w'_1])$. Again we can picure this as being a container for $v_1 \mapsto v'_1$, $w_1 \mapsto w'_1$ and $w_2 \mapsto w'_2$. Keep this interpretation in mind when studying the transition definitions in later chapters.

7.4 Encompassing I/O Components

In this section we extend our discussion to cover input and output. Consider the within relation P_{Op}, which we define as

$$
\begin{aligned}
& P_{Op}(i, h, u, t) \\
&= (Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \fatsemi (R^{\bullet}{}_{Op}(\underline{j}, h) \wedge K^{\bullet}(\underline{v}, t)) \\
&= (R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \fatsemi (Q^{\bullet}{}_{Op}(\underline{k}, h, \underline{w}, t) \wedge H^{\bullet}(\underline{w}, t)) \qquad (7.24)
\end{aligned}
$$

and abbreviate to $P_{Op}(i, h, u, t) = QH⨾R^{\bullet}K^{\bullet}(i, h, u, t) = RK⨾Q^{\bullet}H^{\bullet}(i, h, u, t)$.

Let us focus on the state components first. From what we saw earlier, for cases like the one shown in Figure 7.12, we perhaps expect to further constrain $K^{\bullet}$ with the conjunct

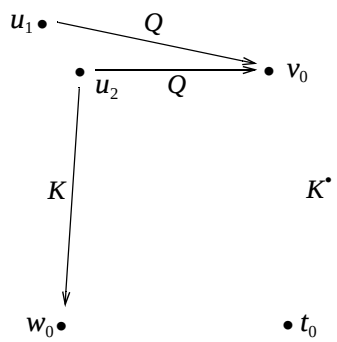


Figure 7.12

QK_{Op} where

$$QK_{Op}([v], [w]) \;=\; (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge Q_{Op}(..., u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KQ_{Op}(\underline{w}, [v]))) \tag{7.25}$$

and

$$KQ_{Op}(\underline{w}, [v]) \;=\; (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge Q_{Op}(..., u, \underline{v}))) \;. \tag{7.26}$$

However, let us examine $(Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))⨾(R^{\bullet}{}_{Op}(\underline{j}, h) \wedge K^{\bullet}(\underline{v}, t))$. This can only hold when $Q_{Op}(i, \underline{j}, u, \underline{v})$ and $H(u, \underline{v})$ hold for some $\underline{j}$ and $\underline{v}$. Thus any $Q_{Op}(i, \underline{j}, u, \underline{v})$ without a matching $H(u, \underline{v})$ is immediately excluded, and when $H(u, \underline{v})$ does hold, it must satisfy $K^{\bullet}(\underline{v}, t)$. Hence cases like Figure 7.12 are already covered and we need not make any further changes to the definition for $K^{\bullet}$. For similar reasons we do not need to include $Q_{Op}(..., u, \underline{v})$ when determining the equivalence classes on state: H is sufficient.

This leaves the inputs. They produce the same problems we saw with states in the previous sections and thus we handle them in a similar manner. We define the inputs in *Univ* to be pairs of equivalence classes. For each *Op* we have

$$\mathsf{H}_{Op} = \mathsf{J}/{\sim_J} \times \mathsf{K}/{\sim_K}, \tag{7.27}$$

where

$$\sim_J = ((R_{Op}^T ⨾ QQ_{Op})^T ⨾ (R_{Op}^T ⨾ QQ_{Op}))^* , \tag{7.28}$$

$$\sim_K = ((QQ_{Op}^T ⨾ R_{Op})^T ⨾ (QQ_{Op}^T ⨾ R_{Op}))^* , \tag{7.29}$$

$$QQ_{Op}(i, j) = (\exists\, u, v \bullet Q_{Op}(i, j, u, v)) \tag{7.30}$$

with $[j] \in \mathsf{J}/{\sim_J}$ and $[k] \in \mathsf{K}/{\sim_K}$.

We also introduce analogues to *HK* and *KH*. Let

$$\begin{aligned} &QR_{Op}([j], [k]) = \\ &\quad (\forall\, \underline{j}, i, u, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^\bullet(\underline{v}, ([v], [w])) \Rightarrow \\ &\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))) , \end{aligned} \tag{7.31}$$

$$\begin{aligned} &RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \;=\; (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\ &\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))) . \end{aligned} \tag{7.32}$$

Then

$$R^\bullet_{Op}(\underline{j}, ([j], [k])) \;=\; \underline{j} \in [j] \wedge QR_{Op}([j], [k]) , \tag{7.33}$$

$$\begin{aligned} &Q^\bullet_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \;= \\ &\quad \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge \\ &\quad RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \end{aligned} \tag{7.34}$$

Consider Figure 7.13 (i), where $h_0 = (j_0, k_0)$. QR_{Op} prevents $R^\bullet_{Op}(j_0, h_0)$ and thus $QH ⨾ R^\bullet K^\bullet(i_1, h_0, u_1, t_0)$, since there is no $R_{Op}(i_1, k_0)$ and thus no possibility of $RK ⨾ Q^\bullet H^\bullet(i_1, h_0, u_1, t_0)$. It also bars $Q^\bullet_{Op}(k_0, h_0, w_0, t_0)$ since now $QH ⨾ R^\bullet K^\bullet(i_2, h_0, u_2, t_0)$ cannot hold and thus $RK ⨾ Q^\bullet H^\bullet(i_2, h_0, u_2, t_0)$ must not.

Notice the additional antecedents *H* and $K^\bullet$ in QR_{Op} when compared to *HK*. These express the fact that we only need to exclude problematic Q_{Op}s which are candidates for composition with respect to state, i.e. ones for which *H* and $K^\bullet$ hold.

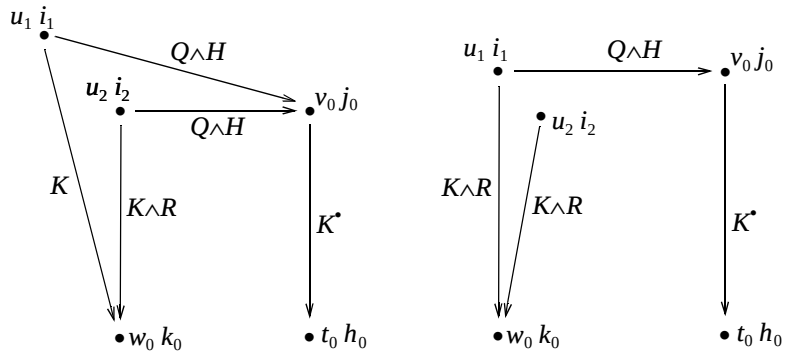


Figure 7.13

In Figure 7.13 (ii) RQ_{Op} prevents $Q^\bullet_{Op}(k_0, h_0, w_0, t_0)$. This cannot hold, otherwise we have $RK⨾Q^\bullet H^\bullet(i_2, h_0, u_2, t_0)$ but no possibility of $QH⨾R^\bullet K^\bullet(i_2, h_0, u_2, t_0)$. We must also include RQ_{Op} in the definition of QR_{Op} in order to preclude $R^\bullet_{Op}(j_0, h_0)$. This cannot hold, otherwise we have $QH⨾R^\bullet K^\bullet(i_1, h_0, u_1, t_0)$, which in turn demands $RK⨾Q^\bullet H^\bullet(i_1, h_0, u_1, t_0)$, but this requires $Q^\bullet_{Op}(k_0, h_0, w_0, t_0)$, and this we have already ruled out.

We tackle O_{Op} in exactly the same way and therefore omit the details here. Let us now return to C_{Op} and consider the components we ignored in the previous section. We define

$$\begin{aligned}
&C_{Op}(u', t', o, s; i, h, u, t)\\
&= (D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))⨾\\
&\quad (K^\bullet(\underline{v}', t') \wedge V^\bullet_{Op}(\underline{p}, o) \wedge R^\bullet_{Op}(\underline{j}, h) \wedge K^\bullet(\underline{v}, t))\\
&= (K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}))⨾\\
&\quad (D^\bullet_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q^\bullet_{Op}(\underline{k}, h, \underline{w}, t) \wedge H^\bullet(\underline{w}, t))
\end{aligned} \tag{7.35}$$

We construct the outputs of *Univ* in the expected manner. For each *Op*

$$\mathsf{S}_{Op} = \mathsf{P}/{\sim_{\mathrm{P}}} \times \mathsf{Q}/{\sim_{\mathrm{Q}}}, \tag{7.36}$$

where

$$\sim_{\mathrm{P}} = ((V^{\mathrm{T}}_{Op}⨾ND_{Op})^{\mathrm{T}}⨾(V^{\mathrm{T}}_{Op}⨾ND_{Op}))^* , \tag{7.37}$$

$$\sim_{\mathrm{Q}} = ((ND^{\mathrm{T}}_{Op}⨾V_{Op})^{\mathrm{T}}⨾(ND^{\mathrm{T}}_{Op}⨾V_{Op}))^* , \tag{7.38}$$

$$ND_{Op}(o, p) = N_{Op}(o, p; ...) \vee D_{Op}(..., o, p; ...) \tag{7.39}$$

with $[p] \in \mathsf{P}/\sim_{\mathrm{P}}$ and $[q] \in \mathsf{Q}/\sim_{\mathrm{Q}}$.

For the same reasons we articulated for P_{Op}, we do not need to take any further steps to treat problematic cases involving the before states or inputs. The relations involving outputs follow the now familiar pattern and for $V^{\bullet}_{Op}$ we get

$$V^{\bullet}_{Op}(\underline{p}, ([p], [q])) = \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) , \tag{7.40}$$

where NV_{Op} and DV_{Op} are analogues of QR_{Op}. NV_{Op} excludes rogue instances of $N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})$ and DV_{Op} does the same with $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. We miss out the definitions which can be found in the next chapter. We covered after states and thus $K^{\bullet\prime}$ in the previous section, so only $D^{\bullet}_{Op}$ remains. Its definition is

$$\begin{aligned} &D^{\bullet}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) = \\ &\quad \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \\ &\quad (\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge \\ &\quad VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\ &\quad HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \end{aligned} \tag{7.41}$$

Based on what we saw for $Q^{\bullet}_{Op}$, we find the terms we expect: $VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$, $NV_{Op}([p], [q])$ and $DV_{Op}([p], [q])$. We also have $HK([v'], [w'])$ and $DK_{Op}([v'], [w'])$. These are needed to deal with after states. We saw this in the previous section, where we derived a definition for $D^{\bullet}_{Op}$, (7.21), for after states only. This also had the term $KD_{Op}(\underline{w}', [v'])$ which does not occur in (7.41). However, this missing term follows from $(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}))$ and $VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$, by Lemma A.13.

With the above definitions $C_{Op} = (D_{Op} \wedge Q_{Op} \wedge H)\fatsemi(K^{\bullet\prime} \wedge V^{\bullet}_{Op} \wedge R^{\bullet}_{Op} \wedge K^{\bullet}) = (K' \wedge V_{Op} \wedge R_{Op} \wedge K)\fatsemi(D^{\bullet}_{Op} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet})$.

Although at first sight the definitions for $K^{\bullet}$, $R^{\bullet}_{Op}$, $V^{\bullet}_{Op}$, $H^{\bullet}$, $Q^{\bullet}_{Op}$, $N^{\bullet}_{Op}$ and $D^{\bullet}_{Op}$ may appear somewhat complicated, we have seen that they all share a common structure and that their components have readily identifiable roles.

7.5 The Class of Systems

It follows from what we have seen, that for both the pre- and postjoins, any system *Xtra* which completes the square, will be subject to the kinds of constraints we described above. This reality gives rise in each case to a number of properties which must hold for the class of systems completing the square. For the postjoin, *Univ* is then constructed to be the most abstract in its class up to interrefinability equivalence, while for the prejoin, *Univ* is constructed so as to be the most concrete.

Chapter 8

The Postjoin Theorem

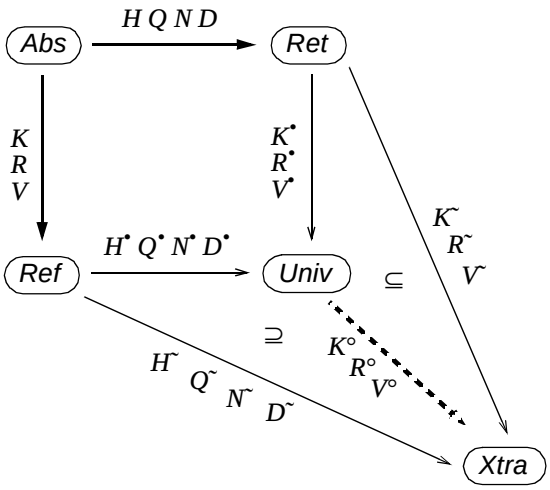
Given a system *Abs* which is retrenched to a system *Ret*, and also refined to a system *Ref*, the postjoin completes the square by constructing a system *Univ* with the following properties. First, *Univ* is both a retrenchment of *Ref* and a refinement of *Ret*. Second, the composition of the *Abs* to *Ret* retrenchment with the *Ret* to *Univ* refinement on the one hand, and the composition of the *Abs* to *Ref* refinement with the *Ref* to *Univ* retrenchment on the other, are both equal as a retrenchment from *Abs* to *Univ*. Third, in the class of systems achieving a similar completion, *Univ* is the most abstract up to equivalence. We make these ideas precise in the theorem below.

8.1 The Postjoin Theorem

Theorem 8.1. Let there be a retrenchment from *Abs* to *Ret*, and a refinement from *Abs* to *Ref*, as shown in Figure 8.1. Then the following hold.

(1) There is a universal system *Univ* such that there is a retrenchment from *Ref* to *Univ* and a refinement from *Ret* to *Univ* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Abs* to *Univ*, and which satisfies (U1) to (U12) below.

(2) Whenever there is a system *Xtra* and a retrenchment from *Ref* to *Xtra* and a refinement from *Ret* to *Xtra* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Abs* to *Xtra*, and which satisfies (X1) to (X12) below, then there is a refinement from *Univ* to *Xtra* such that $H^{\bullet} ⨾ K^{\circ} \Rightarrow H^{\sim}$, $(Q^{\bullet} \wedge H^{\bullet}) ⨾ (R^{\circ} \wedge K^{\circ}) \Rightarrow (Q^{\sim} \wedge H^{\sim})$, $(D^{\bullet} \wedge Q^{\bullet} \wedge H^{\bullet}) ⨾ (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \Rightarrow (D^{\sim} \wedge Q^{\sim} \wedge H^{\sim})$,



All arrows labelled H, Q, N, D are retrenchments;
all arrows labelled K, R, V are refinements.

Figure 8.1: The relationship between systems in a postjoin.

$(N^\bullet \wedge H^{\bullet\prime} \wedge Q^\bullet \wedge H^\bullet) \fatsemi (V^\circ \wedge K^{\circ\prime} \wedge R^\circ \wedge K^\circ) \Rightarrow (N^\sim \wedge H^{\sim\prime} \wedge Q^\sim \wedge H^\sim)$, and such that $K^\bullet \fatsemi K^\circ \Rightarrow K^\sim$, $R^\bullet \fatsemi R^\circ \Rightarrow R^\sim$, $V^\bullet \fatsemi V^\circ \Rightarrow V^\sim$ (see also (8.81) to (8.87)).

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are mutually interrefinable.

8.2 Basic Definitions

For *Abs* the operation names set is $Op_{\mathrm{A}} \in \mathsf{Ops}_{\mathrm{A}}$, state, input and output spaces are $u \in \mathsf{U}$, $i \in \mathsf{I}_{Op_{\mathrm{A}}}$, $o \in \mathsf{O}_{Op_{\mathrm{A}}}$, and initialisation and step predicates are $Init_{\mathrm{A}}$ and $stp_{Op_{\mathrm{A}}}$. Correspondingly, for *Ret* we have $Op_{\mathrm{T}} \in \mathsf{Ops}_{\mathrm{T}}$, $v \in \mathsf{V}$, $j \in \mathsf{J}_{Op_{\mathrm{T}}}$, $p \in \mathsf{P}_{Op_{\mathrm{T}}}$, $Init_{\mathrm{T}}$ and $stp_{Op_{\mathrm{T}}}$, and for *Ref*, $Op_{\mathrm{F}} \in \mathsf{Ops}_{\mathrm{F}}$, $w \in \mathsf{W}$, $k \in \mathsf{K}_{Op_{\mathrm{F}}}$, $q \in \mathsf{Q}_{Op_{\mathrm{F}}}$, $Init_{\mathrm{F}}$ and $stp_{Op_{\mathrm{F}}}$. Here, $\mathsf{Ops}_{\mathrm{A}} = \mathsf{Ops}_{\mathrm{F}} \subseteq \mathsf{Ops}_{\mathrm{T}}$.

Let the refinement from *Abs* to *Ref* have retrieve relation K, and for each Op, input relation R_{Op} and output relation V_{Op}. Let the retrenchment from *Abs* to *Ret* have retrieve relation H, and for each Op, within relation Q_{Op}, output relation N_{Op} and concedes relation D_{Op}.

In the remainder of this section we define the various elements we will use in the construction of *Univ* and the associated retrenchment and refinement. Let,

$$HD(u, v) = H(u, v) \vee \bigvee_{Op} (\exists\, \underline{\underline{o}}, \underline{\underline{p}}, \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}} \bullet D_{Op}(u, v, \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})) \,, \tag{8.1}$$

$$QQ_{Op}(i, j) = (\exists\, \underline{\underline{u}}, \underline{\underline{v}} \bullet Q_{Op}(i, j, \underline{\underline{u}}, \underline{\underline{v}})) \,, \tag{8.2}$$

$$ND_{Op}(o, p) = \\ (\exists\, \underline{\underline{u}}', \underline{\underline{v}}', \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}} \bullet N_{Op}(o, p; \underline{\underline{u}}', \underline{\underline{v}}', \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}) \vee D_{Op}(\underline{\underline{u}}', \underline{\underline{v}}', o, p; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})) \,. \tag{8.3}$$

Given these, we now introduce the following equivalence relations.

$$\sim_{\mathrm{V}} = ((K^{\mathrm{T}} ⨾ HD)^{\mathrm{T}} ⨾ (K^{\mathrm{T}} ⨾ HD))^* \,, \tag{8.4}$$

$$\sim_{\mathrm{W}} = ((HD^{\mathrm{T}} ⨾ K)^{\mathrm{T}} ⨾ (HD^{\mathrm{T}} ⨾ K))^* \,, \tag{8.5}$$

$$\sim_{\mathrm{J}_{Op}} = ((R_{Op}^{\mathrm{T}} ⨾ QQ_{Op})^{\mathrm{T}} ⨾ (R_{Op}^{\mathrm{T}} ⨾ QQ_{Op}))^* \,, \tag{8.6}$$

$$\sim_{\mathrm{K}_{Op}} = ((QQ_{Op}^{\mathrm{T}} ⨾ R_{Op})^{\mathrm{T}} ⨾ (QQ_{Op}^{\mathrm{T}} ⨾ R_{Op}))^* \,, \tag{8.7}$$

$$\sim_{\mathrm{P}_{Op}} = ((V_{Op}^{\mathrm{T}} ⨾ ND_{Op})^{\mathrm{T}} ⨾ (V_{Op}^{\mathrm{T}} ⨾ ND_{Op}))^* \,, \tag{8.8}$$

$$\sim_{\mathrm{Q}_{Op}} = ((ND_{Op}^{\mathrm{T}} ⨾ V_{Op})^{\mathrm{T}} ⨾ (ND_{Op}^{\mathrm{T}} ⨾ V_{Op}))^* \,. \tag{8.9}$$

Let $[v] \in \mathsf{V}/{\sim_{\mathrm{V}}}$, $[w] \in \mathsf{W}/{\sim_{\mathrm{W}}}$, $[j] \in \mathsf{J}_{Op}/{\sim_{\mathrm{J}_{Op}}}$, $[k] \in \mathsf{K}_{Op}/{\sim_{\mathrm{K}_{Op}}}$, $[p] \in \mathsf{P}_{Op}/{\sim_{\mathrm{P}_{Op}}}$ and $[q] \in \mathsf{Q}_{Op}/{\sim_{\mathrm{Q}_{Op}}}$. Then,

$$KH(\underline{w}, [v]) \;=\; (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \,, \tag{8.10}$$

$$HK([v], [w]) \;=\; (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow \\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))) \,, \tag{8.11}$$

$$KD_{Op}(\underline{w}, [v]) \;=\; (\forall\, u \bullet K(u, \underline{w}) \Rightarrow \\ (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge (\exists\, \underline{\underline{o}}, \underline{\underline{p}}, \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}} \bullet D_{Op}(u, \underline{v}, \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})))) \,, \tag{8.12}$$

$$DK_{Op}([v], [w]) \;= \\ (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge (\exists\, \underline{\underline{o}}, \underline{\underline{p}}, \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}} \bullet D_{Op}(u, \underline{v}, \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})) \Rightarrow \\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KD_{Op}(\underline{w}, [v]))) \,, \tag{8.13}$$

$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \;=\; (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\ (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))) \,, \tag{8.14}$$

$$
\begin{aligned}
&QR_{Op}([j], [k]) = \\
&\quad (\forall\, \underline{j}, i, u, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))) ,
\end{aligned}
\tag{8.15}
$$

$$
\begin{aligned}
&\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) = \\
&\quad \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge \\
&\quad RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) ,
\end{aligned}
\tag{8.16}
$$

$$
\begin{aligned}
&VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) = \\
&\quad (\forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\
&\qquad (\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\qquad N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))) ,
\end{aligned}
\tag{8.17}
$$

$$
\begin{aligned}
&NV_{Op}([p], [q]) = \\
&\quad (\forall\, \underline{p}, o, u', \underline{v}', i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet \\
&\quad \underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge \\
&\quad K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow \\
&\qquad (\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge \\
&\qquad K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]))) ,
\end{aligned}
\tag{8.18}
$$

$$
\begin{aligned}
&VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) = \\
&\quad (\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\
&\qquad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\qquad D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))) ,
\end{aligned}
\tag{8.19}
$$

$$
\begin{aligned}
&DV_{Op}([p], [q]) = \\
&\quad (\forall\, \underline{p}, u', \underline{v}', o, i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet \\
&\quad \underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge \\
&\quad K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow \\
&\qquad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge \\
&\qquad V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))) ,
\end{aligned}
\tag{8.20}
$$

$$T_{Op}([j], [k]) \;=$$
$$(\forall\, \underline{j}, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}) \Rightarrow$$
$$trm_{Op_{\mathrm{U}}}(([v], [w]), ([j], [k]))\;) \;, \tag{8.21}$$

$$T_{Op}(\underline{j}, h) \;=$$
$$(\forall\, \underline{v}, v, w \bullet \underline{j} = h \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}) \Rightarrow$$
$$trm_{Op_{\mathrm{U}}}(([v], [w]), h)\;) \;. \tag{8.22}$$

Finally, let

$$K^{\bullet}(\underline{v}, ([v], [w])) \;=\; \underline{v} \in [v] \wedge HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \;, \tag{8.23}$$

$$H^{\bullet}(\underline{w}, ([v], [w])) \;=\; \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge$$
$$HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \;, \tag{8.24}$$

$$R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \;=\; \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \;, \tag{8.25}$$

$$Q^{\bullet}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \;=$$
$$\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge T_{Op}([j], [k]) \;, \tag{8.26}$$

$$V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \;=\; \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \;, \tag{8.27}$$

$$N^{\bullet}_{Op}(\underline{q}, ([p], [q]); \underline{w}', ([v'], [w']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \;=$$
$$\underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$(\exists\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$$
$$VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \;, \tag{8.28}$$

$$D^{\bullet}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \;=$$
$$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$$
$$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$$
$$HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \;. \tag{8.29}$$

8.3 Proof for Part (1)

We take the retrenchment from *Abs* to *Ret* and the refinement from *Abs* to *Ref*, and build a new, universal system *Univ*, to which we then show there is *both* a retrenchment from *Ref* and a refinement from *Ret*; see Figure 8.1.

8.3.1 The system *Univ*

The operation names set of *Univ* is Ops_U with elements Op_U. State, input and output spaces are $t \in \mathsf{T}$, $h \in \mathsf{H}_{Op_\mathrm{U}}$, $s \in \mathsf{S}_{Op_\mathrm{U}}$. Initialisation and step predicates are $Init_\mathrm{U}$ and stp_{Op_U}. These are all constructed from the systems *Ret* and *Ref* as follows. Firstly $\mathsf{Ops}_\mathrm{U} = \mathsf{Ops}_\mathrm{T} = \mathsf{Ops}_\mathrm{A} \cup (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$. So each Op_U is either an Op_A or an $Op_\mathrm{U} \in (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$. Next $\mathsf{T} = \mathsf{V}/{\sim_\mathrm{V}} \times \mathsf{W}/{\sim_\mathrm{W}}$. For $Op_\mathrm{U} \in \mathsf{Ops}_\mathrm{A}$ the input and output spaces are $\mathsf{H}_{Op} = \mathsf{J}_{Op}/{\sim_{\mathrm{J}_{Op}}} \times \mathsf{K}_{Op}/{\sim_{\mathrm{K}_{Op}}}$ and $\mathsf{S}_{Op} = \mathsf{P}_{Op}/{\sim_{\mathrm{P}_{Op}}} \times \mathsf{Q}_{Op}/{\sim_{\mathrm{Q}_{Op}}}$, whereas for $Op_\mathrm{U} \notin \mathsf{Ops}_\mathrm{A}$, $\mathsf{H}_{Op} = \mathsf{J}_{Op}$ and $\mathsf{S}_{Op} = \mathsf{P}_{Op}$.

Let the initialization predicate $Init_\mathrm{U}(t')$ be defined as follows.

$$\begin{aligned} &Init_\mathrm{U}(t') \;=\; Init_\mathrm{U}(([v'], [w'])) = \\ &\quad (\exists\, \underline{v}' \bullet Init_\mathrm{T}(\underline{v}') \wedge K^\bullet(\underline{v}', ([v'], [w']))) \;\wedge\; (\exists\, \underline{w}' \bullet Init_\mathrm{F}(\underline{w}') \wedge H^\bullet(\underline{w}', ([v'], [w']))) \end{aligned} \tag{8.30}$$

We now give the transitions of *Univ*. The operation names set Ops_U decomposes as $\mathsf{Ops}_\mathrm{U} = \mathsf{Ops}_\mathrm{A} \cup (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$. There are therefore two possibilities. For $Op_\mathrm{U} \in \mathsf{Ops}_\mathrm{A}$ let

$$\begin{aligned} &stp_{Op_\mathrm{U}}(t, h, t', s) \;=\; stp_{Op_\mathrm{U}}(([v], [w]), ([j], [k]), ([v'], [w']), ([p], [q])) \;= \\ &\quad \mathbf{(}\, \forall\, \underline{v}, \underline{j} \bullet \underline{v} \in [v] \wedge \underline{j} \in [j] \Rightarrow (\exists\, \underline{v}', \underline{p} \bullet stp_{Op_\mathrm{T}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \\ &\qquad K^\bullet(\underline{v}', ([v'], [w'])) \wedge V^\bullet_{Op}(\underline{p}, ([p], [q]))) \,\mathbf{)} \qquad \text{(a)} \\ &\quad \wedge \\ &\quad \mathbf{(}\, \forall\, \underline{w}, \underline{k} \bullet H^\bullet(\underline{w}, ([v], [w])) \wedge \overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \Rightarrow \\ &\qquad (\exists\, \underline{w}', \underline{q} \bullet stp_{Op_\mathrm{F}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \mathbf{(}\, (H^\bullet(\underline{w}', ([v'], [w'])) \wedge \\ &\qquad\quad N^\bullet_{Op}(\underline{q}, ([p], [q]); \underline{w}', ([v'], [w']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))) \vee \\ &\qquad\quad D^\bullet_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))\,\mathbf{)}\,\mathbf{)}\,\mathbf{)}\,. \qquad \text{(b)} \end{aligned} \tag{8.31}$$

For $Op_\mathrm{U} \in (\mathsf{Ops}_\mathrm{U} - \mathsf{Ops}_\mathrm{A})$, i.e. $Op_\mathrm{U} \notin \mathsf{Ops}_\mathrm{A}$, let the step relation be

$$\begin{aligned} &stp_{Op_\mathrm{U}}(t, h, t', s) \;=\; stp_{Op_\mathrm{U}}(([v], [w]), h, ([v'], [w']), s) \;= \\ &\quad \mathbf{(}\, \forall\, \underline{v}, \underline{j} \bullet \underline{v} \in [v] \wedge \underline{j} = h \;\Rightarrow \\ &\qquad (\,\exists\, \underline{v}', \underline{p} \bullet stp_{Op_\mathrm{T}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K^\bullet(\underline{v}', ([v'], [w'])) \wedge \underline{p} = s\,)\,\mathbf{)}\,. \end{aligned} \tag{8.32}$$

This completes the definition of *Univ*.

Given the above, observe that the following hold. For $Op_A \in \mathsf{Ops}_A$,

$$trm_{Op_U}(([v], [w]), ([j], [k])) \Rightarrow$$
$$(\ (\ \forall\ \underline{v}, \underline{j} \bullet \underline{v} \in [v] \wedge \underline{j} \in [j] \Rightarrow trm_{Op_T}(\underline{v}, \underline{j})\ ) \wedge$$
$$(\ \forall\ \underline{w}, \underline{k} \bullet H^{\bullet}(\underline{w}, ([v], [w])) \wedge \overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \Rightarrow trm_{Op_F}(\underline{w}, \underline{k})\ )\ ) . \tag{8.33}$$

For $Op_U \notin \mathsf{Ops}_A$,

$$trm_{Op_U}(([v], [w]), h) \Rightarrow$$
$$(\ \forall\ \underline{v}, \underline{j} \bullet \underline{v} \in [v] \wedge \underline{j} = h \Rightarrow trm_{Op_T}(\underline{v}, \underline{j})\ ) . \tag{8.34}$$

8.3.2 The refinement from *Ret* to *Univ*

We show that *Univ* refines *Ret*. We do this by first specifying the component relations for the refinement and then showing that the refinement POs hold.

8.3.2.1 The component relations

The data for the refinement consists of the retrieve relation $K^{\bullet}(\underline{v}, t)$, and for each *Op*, the input relation $R^{\bullet}_{Op}(\underline{j}, h)$ and the output relation $V^{\bullet}_{Op}(\underline{p}, s)$. $K^{\bullet}$ is given by (8.23). For $Op \in \mathsf{Ops}_A$, $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ are given by (8.25) and (8.27) respectively. For $Op \notin \mathsf{Ops}_A$ let

$$R^{\bullet}_{Op}(\underline{j}, h) = (\ \underline{j} = h \wedge T_{Op}(\underline{j}, h)\ ) , \tag{8.35}$$

$$V^{\bullet}_{Op}(\underline{p}, s) = (\ \underline{p} = s\ ) . \tag{8.36}$$

We also have the input initialisations and output finalisations. For *Ret* let the input initialisation be $InitIn_{Op_T}$ and output finalisation be $FinOut_{Op_T}$. Similarly, for *Univ* we have $InitIn_{Op_U}$ and $FinOut_{Op_U}$. Since *Ret* is the given system refined to both *Univ* and *Xtra*, we use the input and output spaces of its operations to define those of the global world. For $Op \in \mathsf{Ops}_A$, let $\mathsf{N}_{Op} = \mathsf{P}_{Op}$ and

$$\mathsf{L}_{Op} = \{l \in \mathsf{J}_{Op} \mid \exists\ j, k \bullet j = l \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k])\} . \tag{8.37}$$

Then,

$$InitIn_{Op_T}(l, \underline{j}) \;=\; (\, l \sim \underline{j} \,) \;, \tag{8.38}$$

$$FinOut_{Op_T}(\underline{p}, n) \;=\; (\, \underline{p} \sim n \,) \;, \tag{8.39}$$

$$InitIn_{Op_U}(l, h) \;=\; (\, h = ([j], [k]) \wedge l \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \,) \;, \tag{8.40}$$

$$FinOut_{Op_U}(s, n) \;=\; (\, s = ([p], [q]) \wedge n \in [p] \,) \;. \tag{8.41}$$

For $Op \notin \mathsf{Ops}_A$, let $\mathsf{N}_{Op} = \mathsf{P}_{Op}$ and

$$\mathsf{L}_{Op} \;=\; \{ l \in \mathsf{J}_{Op} \mid \exists\, j, h \bullet j = l \wedge h = j \wedge T_{Op}(j, h) \} \;. \tag{8.42}$$

Then,

$$InitIn_{Op_T}(l, \underline{j}) \;=\; (\, l = \underline{j} \,) \;, \tag{8.43}$$

$$FinOut_{Op_T}(\underline{p}, n) \;=\; (\, \underline{p} = n \,) \;, \tag{8.44}$$

$$InitIn_{Op_U}(l, h) \;=\; (\, l = h \wedge T_{Op}(l, h) \,) \;, \tag{8.45}$$

$$FinOut_{Op_U}(s, n) \;=\; (\, s = n \,) \;. \tag{8.46}$$

Observe that (8.38) to (8.41) and (8.43) to (8.46) are all total relations. This is easy to see, even for (8.40) and (8.45), which, by (8.37) and (8.42) respectively, have for every l a suitable h.

8.3.2.2 The input initialisation PO

We show

$$InitIn_{Op_U}(l, h) \;\Rightarrow\; (\exists\, \underline{j} \bullet InitIn_{Op_T}(l, \underline{j}) \wedge R^{\bullet}_{Op}(\underline{j}, h)) \;. \tag{8.47}$$

Proof. As $Op \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume the antecedent with $h = ([j], [k])$. By (8.40) we therefore have, $l \in [j]$, $QR_{Op}([j], [k])$ and $T_{Op}([j], [k])$. Let $\underline{j} = l$. Then $InitIn_{Op_T}(l, \underline{j})$ and $R^{\bullet}_{Op}(\underline{j}, h)$ hold, by (8.38) and (8.25) respectively. We are done.

• Case $Op \notin \mathsf{Ops}_A$. Assume the antecedent. By (8.45) we therefore have $l = h$ and $T_{Op}(l, h)$. Let $\underline{j} = l$. Then $InitIn_{Op_T}(l, \underline{j})$ and $R^{\bullet}_{Op}(\underline{j}, h)$ hold, by (8.43) and (8.35) respectively. ■

8.3.2.3 The initialisation PO

We show

$$Init_U(t') \Rightarrow (\exists\, \underline{v}' \bullet Init_T(\underline{v}') \wedge K^{\bullet}(\underline{v}', t')) \,. \tag{8.48}$$

Proof. Assume $Init_U(t')$ with $t' = ([v'], [w'])$. Then by (8.30) the consequent is immediate.

■

8.3.2.4 The applicability PO

We show

$$K^{\bullet}(\underline{v}, t) \wedge R^{\bullet}_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \Rightarrow trm_{Op_U}(t, h) \,. \tag{8.49}$$

Proof. Since Ops_T decomposes as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op_T \in \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$ and $h = ([j], [k])$. $R^{\bullet}_{Op}$ and (8.25) give $\underline{j} \in [j]$ and $T_{Op}([j], [k])$. From these, $K^{\bullet}(\underline{v}, t)$ and $trm_{Op_T}(\underline{v}, \underline{j})$, the required $trm_{Op_U}(t, h)$ follows by (8.21).

• Case $Op_T \notin \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$. $R^{\bullet}_{Op}$ and (8.35) give $\underline{j} = h$ and $T_{Op}(\underline{j}, h)$. From these, $K^{\bullet}(\underline{v}, t)$ and $trm_{Op_T}(\underline{v}, \underline{j})$, the required $trm_{Op_U}(t, h)$ follows by (8.22). ■

8.3.2.5 The correctness PO

We show

$$\begin{aligned} &K^{\bullet}(\underline{v}, t) \wedge R^{\bullet}_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge stp_{Op_U}(t, h, t', s) \Rightarrow \\ &\qquad (\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K^{\bullet}(\underline{v}', t') \wedge V^{\bullet}_{Op}(\underline{p}, s)) \,. \end{aligned} \tag{8.50}$$

Proof. As $Op \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$. Then $K^\bullet$ and (8.23) give $\underline{v} \in [v]$; $R^\bullet_{Op}$ and (8.25) give $\underline{j} \in [j]$. The consequent now follows from (a).

• Case $Op \notin \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$. Then $K^\bullet$ and (8.23) give $\underline{v} \in [v]$; $R^\bullet_{Op}$ and (8.35) give $\underline{j} = h$. Hence from $stp_{Op_U}(t, h, t', s)$, by (8.32), there are values, $\underline{v}'$ and $\underline{p}$ say, such that $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^\bullet(\underline{v}', t')$ and $\underline{p} = s$ hold. Then from the latter, by (8.36), $V^\bullet_{Op}(\underline{p}, s)$ holds too, and we are done. ■

8.3.2.6 The output finalisation PO

We show

$$V^\bullet_{Op}(\underline{p}, s) \wedge FinOut_{Op_U}(s, n) \Rightarrow FinOut_{Op_T}(\underline{p}, n) . \tag{8.51}$$

Proof. As $Op \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume the antecedents with $s = ([p], [q])$. From $V^\bullet_{Op}(\underline{p}, s)$, by (8.27), $\underline{p} \in [p]$. From $FinOut_{Op_U}(s, n)$, by (8.41), $n \in [p]$. Therefore, $\underline{p} \sim n$, from which $FinOut_{Op_T}(\underline{p}, n)$ follows, by (8.39).

• Case $Op \notin \mathsf{Ops}_A$. Assume the antecedents. From $V^\bullet_{Op}(\underline{p}, s)$, by (8.36), $\underline{p} = s$. From $FinOut_{Op_U}(s, n)$, by (8.46), $s = n$. Therefore, $\underline{p} = n$, from which $FinOut_{Op_T}(\underline{p}, n)$ follows, by (8.44). ■

8.3.3 The retrenchment from *Ref* to *Univ*

We show *Univ* retrenches *Ref*. We do this by first specifying the component relations of the retrenchment and then showing that the retrenchment POs hold.

8.3.3.1 The component relations

The data for the retrenchment consists of the retrieve relation $H^\bullet$, and for each Op, the within relation $Q^\bullet_{Op}$, the output relation $N^\bullet_{Op}$ and the concedes relation $D^\bullet_{Op}$. These are given by (8.24), (8.26), (8.28) and (8.29) respectively.

8.3.3.2 The initialisation PO

We show

$$Init_{\mathrm{U}}(t') \;\Rightarrow\; (\exists\, \underline{w}' \bullet Init_{\mathrm{F}}(\underline{w}') \wedge H^{\bullet}(\underline{w}', t')) \;. \tag{8.52}$$

Proof. Assume $Init_{\mathrm{U}}(t')$ with $t' = ([v'], [w'])$. Then by (8.30) the consequent is immediate.

■

8.3.3.3 The termination PO

We show

$$H^{\bullet}(\underline{w}, t) \wedge Q^{\bullet}{}_{Op}(\underline{k}, h, \underline{w}, t) \;\Rightarrow\; trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}) \wedge trm_{Op_{\mathrm{U}}}(t, h) \tag{8.53}$$

Proof. For this relationship Op only ranges over $\mathsf{Ops}_{\mathrm{A}}$. Choose values $t = ([v], [w])$ and $h = ([j], [k])$ for which the antecedents hold. From $Q^{\bullet}{}_{Op}$, by (8.26) and (8.16), we derive values i and u such that $R_{Op}(i, \underline{k})$ and $K(u, \underline{w})$ hold. We also get $RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$. Thus, by (8.14), we can derive values $\underline{j}$ and $\underline{v}$ for which $Q_{Op}(i, \underline{j}, u, \underline{v})$ and $H(u, \underline{v})$ hold, with $\underline{j} \in [j]$ and $\underline{v} \in [v]$. Hence, from the Term PO for the retrenchment from *Abs* to *Ret*,

$$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}) \tag{8.54}$$

we get $trm_{Op_{\mathrm{A}}}(u, i)$. Therefore, since we also have $K(u, \underline{w})$ and $R_{Op}(i, \underline{k})$, we can use the App PO for the refinement from *Abs* to *Ref*,

$$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge trm_{Op_{\mathrm{A}}}(u, i) \;\Rightarrow\; trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}) \tag{8.55}$$

to obtain $trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k})$, which is the first conjunct of the antecedent of (8.53). We derive the second conjunct as follows. From $H^{\bullet}(\underline{w}, t)$ and $\underline{v} \in [v]$, by (8.24) and (8.23), we get $K^{\bullet}(\underline{v}, t)$. From $Q^{\bullet}{}_{Op}(\underline{k}, h, \underline{w}, t)$, by (8.26), we get $T_{Op}([j], [k])$. From (8.54) we also have $trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j})$, with $\underline{j} \in [j]$. Thus, by (8.21), $trm_{Op_{\mathrm{U}}}(t, h)$ holds.

8.3.3.4 The operation PO

We show

$$H^{\bullet}(\underline{w}, t) \wedge Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', s) \;\Rightarrow$$
$$(\exists\, \underline{w}', \underline{q} \bullet stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge$$
$$(\,(H^{\bullet}(\underline{w}', t') \wedge N^{\bullet}_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t)) \vee D^{\bullet}_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)\,)\,)\,. \tag{8.56}$$

Proof. For this relationship Op_{U} only ranges over $\mathsf{Ops}_{\mathrm{A}}$. Choose values $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$ for which the antecedent holds. Then, by (8.26), $\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ holds. Hence, the consequent follows by (8.31b).

■

8.3.4 The retrenchment from *Abs* to *Univ*

The next step is to show that the composition of the *Abs* to *Ret* retrenchment with the *Ret* to *Univ* refinement on the one hand, and the *Abs* to *Ref* refinement with the *Ref* to *Univ* retrenchment on the other, yield the *same* retrenchment from *Abs* to *Univ*. To do this we define the relations of the *Abs* to *Univ* retrenchment in terms of the *Abs* to *Ret* and *Ret* to *Univ* relations, and also in terms of the *Abs* to *Ref* and *Ref* to *Univ* ones. We then show that two definitions are equal. Finally, we demonstrate that the retrenchment POs hold.

8.3.4.1 The component relations

Let the retrieve, within, output and concedes relations of the retrenchment from *Abs* to *Univ* be given by G, P_{Op}, O_{Op} and C_{Op} respectively. Then Figure 8.1 commutes in the following sense. Firstly,

$$G(u, ([v], [w])) \;=\; H(u, \underline{v}) ⨾ K^{\bullet}(\underline{v}, ([v], [w])) \;=\; K(u, \underline{w}) ⨾ H^{\bullet}(\underline{w}, ([v], [w]))\,. \tag{8.57}$$

We write this for short as

$$G = H ⨾ K^{\bullet} = K ⨾ H^{\bullet}\,.$$

Secondly,

$$P_{Op}(i, ([j], [k]), u, ([v], [w]))$$
$$= \mathbf{(}Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)} ⨾ \mathbf{(}R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\mathbf{)}$$
$$= \mathbf{(}R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})\mathbf{)} ⨾ \mathbf{(}Q^{\bullet}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))\mathbf{)}\,, \tag{8.58}$$

or more briefly

$$P_{Op} = (Q_{Op} \wedge H)\fatsemi(R^{\bullet}{}_{Op} \wedge K^{\bullet}) = (R_{Op} \wedge K)\fatsemi(Q^{\bullet}{}_{Op} \wedge H^{\bullet}) \ .$$

Thirdly,

$$\begin{aligned}
&O_{Op}(o, ([p], [q]); u', ([v'], [w']), i, ([j], [k]), u, ([v], [w]))\\
&= \mathbf{(}N_{Op}(o, \underline{p}, u', \underline{v}'; i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\fatsemi\\
&\quad \mathbf{(}V^{\bullet}{}_{Op}(\underline{p}, ([p], [q])) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\mathbf{)}\\
&= \mathbf{(}V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})\mathbf{)}\fatsemi\\
&\quad \mathbf{(}N^{\bullet}{}_{Op}(\underline{q}, ([p], [q]); \underline{w}', ([v'], [w']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge\\
&\qquad H^{\bullet}(\underline{w}', ([v'], [w'])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))\mathbf{)}\ ,
\end{aligned} \tag{8.59}$$

or

$$\begin{aligned}
O_{Op} &= (N_{Op} \wedge H' \wedge Q_{Op} \wedge H)\fatsemi(V^{\bullet}{}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}{}_{Op} \wedge K^{\bullet})\\
&= (V_{Op} \wedge K' \wedge R_{Op} \wedge K)\fatsemi(N^{\bullet}{}_{Op} \wedge H^{\bullet\prime} \wedge Q^{\bullet}{}_{Op} \wedge H^{\bullet}) \ .
\end{aligned}$$

Lastly,

$$\begin{aligned}
&C_{Op}(u', ([v'], [w']), o, ([p], [q]); i, ([j], [k]), u, ([v], [w]))\\
&= \mathbf{(}D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\fatsemi\\
&\quad \mathbf{(}K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}{}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\mathbf{)}\\
&= \mathbf{(}K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})\mathbf{)}\fatsemi\\
&\quad \mathbf{(}D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge\\
&\qquad Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))\mathbf{)}\ ,
\end{aligned} \tag{8.60}$$

or

$$\begin{aligned}
C_{Op} &= (D_{Op} \wedge Q_{Op} \wedge H)\fatsemi(K^{\bullet\prime} \wedge V^{\bullet}{}_{Op} \wedge R^{\bullet}{}_{Op} \wedge K^{\bullet})\\
&= (K' \wedge V_{Op} \wedge R_{Op} \wedge K)\fatsemi(D^{\bullet}{}_{Op} \wedge Q^{\bullet}{}_{Op} \wedge H^{\bullet}) \ .
\end{aligned}$$

In the above $Op \in \mathsf{Ops}_{\mathrm{A}}$. The proofs showing that the above compositions hold are given in Appendix A.

8.3.4.2 The initialisation PO

We show

$$Init_{\mathrm{U}}(t') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', t')) \;. \tag{8.61}$$

Proof. Assume $Init_{\mathrm{U}}(t')$ with $t' = ([v'], [w'])$. By (8.30) there is a value, $\underline{v}'$ say, for which $Init_{\mathrm{T}}(\underline{v}')$ and $K^{\bullet}(\underline{v}', t')$ hold. Hence, from the Init PO for the retrenchment from *Abs* to *Ret*,

$$Init_{\mathrm{T}}(\underline{v}') \;\Rightarrow\; (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge H(u', \underline{v}')) \;, \tag{8.62}$$

$Init_{\mathrm{A}}(u')$ and $H(u', \underline{v}')$ hold for chosen u'. We now have $H(u', \underline{v}')$ and $K^{\bullet}(\underline{v}', t')$. These compose to give $G(u', t')$, by (8.57). Thus there is a u' for which (8.61) holds. ■

8.3.4.3 The termination PO

We show

$$G(u, t) \wedge P_{Op}(i, h, u, t) \;\Rightarrow\; trm_{Op_{\mathrm{A}}}(u, i) \wedge trm_{Op_{\mathrm{U}}}(t, h) \;. \tag{8.63}$$

Proof. Assume the antecedents with $t = ([v], [w])$ and $h = ([j], [k])$. Now $P_{Op}(i, ([j], [k]), u, ([v], [w])) = (Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\fatsemi(R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])))$, by (8.58), with, by (8.23) and (8.25), $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Therefore, from $H \wedge Q_{Op}$, by (8.54), we have the first conjunct, $trm_{Op_{\mathrm{A}}}(u, i)$, of the desired antecedent. We derive the other thus. (8.54) also gives $trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j})$. In addition, from $R^{\bullet}_{Op}$, by (8.25), we have $T_{Op}([j], [k])$. Then, because $\underline{j} \in [j]$ and $K^{\bullet}(\underline{v}, ([v], [w])$ holds, (8.21) gives $trm_{Op_{\mathrm{U}}}(t, h)$. We are done.

■

8.3.4.4 The operation PO

We show

$$\begin{aligned} &G(u, t) \wedge P_{Op}(i, h, u, t) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', s) \;\Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge \\ &\qquad ((G(u', t') \wedge O_{Op}(o, s; u', t', i, h, u, t)) \vee C_{Op}(u', t', o, s; i, h, u, t))) \;. \end{aligned} \tag{8.64}$$

Proof. Here Op_U only ranges over Ops_A. Assume the antecedents with $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$. Now $P_{Op}(i, ([j], [k]), u, ([v], [w])) = (Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\fatsemi(R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])))$, by (8.58), with, by (8.23) and (8.25), $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Hence, as $stp_{Op_U}(t, h, t', s)$ implies $trm_{Op_U}(t, h)$, $trm_{Op_T}(\underline{v}, \underline{j})$ holds by (8.33). We now have enough to use (8.50), to obtain $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\bullet}(\underline{v}', t')$ and $V^{\bullet}_{Op}(\underline{p}, s)$, for chosen values $\underline{v}'$ and $\underline{p}$.

Next, $H(u, \underline{v})$, $Q_{Op}(i, \underline{j}, u, \underline{v})$ and $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$ make up the antecedent of the Op PO for the retrenchment from *Abs* to *Ret*,

$$\begin{aligned} & H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow \\ & \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge \\ & \quad\quad (H(u', \underline{v}') \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) . \end{aligned} \tag{8.65}$$

Therefore we can chose values, we pick u' and o, such that $stp_{Op_A}(u, i, u', o)$ and $(H' \wedge N_{Op}) \vee D_{Op}$ hold. So we now have the first conjunct of the consequent of (8.64). All we need is the second, $(G' \wedge O_{Op}) \vee C_{Op}$. We derive this from $(H' \wedge N_{Op}) \vee D_{Op}$ as follows. Assume $H' \wedge N_{Op}$. Then as $K^{\bullet}(\underline{v}', t')$ holds, we have $H(u', \underline{v}')\fatsemi K^{\bullet}(\underline{v}', t')$ and thus $G(u', t')$, by (8.57). Furthermore, because H, Q_{Op}, $K^{\bullet\prime}$, $V^{\bullet}_{Op}$, $R^{\bullet}_{Op}$ and $K^{\bullet}$ all hold, we have $(N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\fatsemi(V^{\bullet}_{Op}(\underline{p}, s) \wedge K^{\bullet}(\underline{v}', t') \wedge R^{\bullet}_{Op}(\underline{j}, h) \wedge K^{\bullet}(\underline{v}, t))$ and thus $O_{Op}(o, s; u', t', i, h, u, t)$, by (8.59). Now assume $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. Then $(D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\fatsemi(K^{\bullet}(\underline{v}', t') \wedge V^{\bullet}_{Op}(\underline{p}, s) \wedge R^{\bullet}_{Op}(\underline{j}, h) \wedge K^{\bullet}(\underline{v}, t))$ gives $C_{Op}(u', t', o, s; i, h, u, t)$, by (8.60). Hence $(G' \wedge O_{Op}) \vee C_{Op}$ holds and we are done. ■

8.3.5 Properties of *Univ*

We state properties (U1) to (U12) of *Univ*.

$$K^{\bullet}(v', t') \wedge K^{\bullet}(\underline{v}', t') \Rightarrow v' \sim \underline{v}' \tag{U1}$$

$$V^{\bullet}_{Op}(p, s) \wedge V^{\bullet}_{Op}(\underline{p}, s) \Rightarrow p \sim \underline{p} \tag{U2}$$

$$\begin{aligned} & (N^{\bullet}_{Op}(q, s; w', t', ...) \vee D^{\bullet}_{Op}(w', t', q, s; ...)) \wedge \\ & \quad (N^{\bullet}_{Op}(\underline{q}, s; \underline{w}', t', ...) \vee D^{\bullet}_{Op}(\underline{w}', t', \underline{q}, s; ...)) \Rightarrow q \sim \underline{q} \wedge w' \sim \underline{w}' \end{aligned} \tag{U3}$$

$$K^{\bullet}(v', t') \wedge \underline{v}' \in [v'] \Rightarrow K^{\bullet}(\underline{v}', t') \tag{U4}$$

$$R^{\bullet}_{Op}(j, h) \wedge \underline{j} \in [j] \Rightarrow R^{\bullet}_{Op}(\underline{j}, h) \tag{U5}$$

$$V^{\bullet}_{Op}(p, s) \wedge \underline{p} \in [p] \Rightarrow V^{\bullet}_{Op}(\underline{p}, s) \tag{U6}$$

$$K^{\bullet}(v', t') \Rightarrow (H^{\bullet}(w', t') \Leftrightarrow H^{\bullet}(w', ([v'], [w']))) \tag{U7}$$

$$\begin{aligned} & R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow \\ & \quad \mathbf{(} \forall\, k, w \bullet Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t) \Leftrightarrow \\ & \qquad Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w])) \mathbf{)} \end{aligned} \tag{U8}$$

$$\begin{aligned} & V^{\bullet}_{Op}(p, s) \wedge K^{\bullet}(v', t') \wedge R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow \\ & \quad \mathbf{(} \forall\, q, w', k, w \bullet N^{\bullet}_{Op}(q, s; w', t', k, h, w, t) \wedge H^{\bullet}(w', t') \wedge \\ & \qquad Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t) \Leftrightarrow \\ & \qquad\quad N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w])) \wedge \\ & \qquad\quad H^{\bullet}(w', ([v'], [w'])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w])) \mathbf{)} \end{aligned} \tag{U9}$$

$$\begin{aligned} & K^{\bullet}(v', t') \wedge V^{\bullet}_{Op}(p, s) \wedge R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow \\ & \quad \mathbf{(} \forall\, w', q, k, w \bullet D^{\bullet}_{Op}(w', t', q, s; k, h, w, t) \wedge Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t) \Leftrightarrow \\ & \qquad D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w])) \wedge \\ & \qquad Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w])) \mathbf{)} \end{aligned} \tag{U10}$$

$$K^{\bullet}(v', t') \Rightarrow (\exists\, w' \bullet K^{\bullet}(v', ([v'], [w']))) \tag{U11}$$

$$V^{\bullet}_{Op}(p, s\tilde{}) \Rightarrow (\exists\, q \bullet V^{\bullet}_{Op}(p, ([p], [q]))) \tag{U12}$$

Note, (U3), (U5), (U6), (U8), (U9), (U10) and (U12) only hold for $Op \in \mathsf{Ops}_A$.

In the following we show that the above properties are true.

♦ (U1): $K^{\bullet}(v', t') \wedge K^{\bullet}(\underline{v}', t') \Rightarrow v' \sim \underline{v}'$.

Proof. Assume the antecedent and let $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then by (8.23) $v' \in [\underline{\underline{v}}']$ and $\underline{v}' \in [\underline{\underline{v}}']$. Hence $v' \sim \underline{v}'$. ■

♦ (U2) and (U3).

Proof. Similar to (U1). ■

♦ (U4): $K^{\bullet}(v', t') \wedge \underline{v}' \in [v'] \Rightarrow K^{\bullet}(\underline{v}', t')$.

Proof. Suppose $K^{\bullet}(v', t')$ and $\underline{v}' \in [v']$ hold with $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then (8.23) asserts $v' \in [\underline{\underline{v}}']$, $HK([\underline{\underline{v}}'], [\underline{\underline{w}}'])$ and $DK_{Op}([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. But $\underline{v}' \in [v']$, so $\underline{v}' \in [\underline{\underline{v}}']$. Hence $K^{\bullet}(\underline{v}', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$ holds, by (8.23), and we are done. ■

♦ (U5) and (U6).

Proof. Similar to (U4). ■

♦ (U7): $K^{\bullet}(v', t') \Rightarrow (H^{\bullet}(w', t') \Leftrightarrow H^{\bullet}(w', ([v'], [w']))$.

Proof. First we assume $K^{\bullet}(v', t')$ and $H^{\bullet}(w', t')$, and prove $H^{\bullet}(w', ([v'], [w']))$. Let $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then from $H^{\bullet}(w', t')$ and (8.24) we have $w' \in [\underline{\underline{w}}']$, $(\exists\, u \bullet K(u, w'))$, $KH(w', [\underline{\underline{v}}'])$, $HK([\underline{\underline{v}}'], [\underline{\underline{w}}'])$ and $DK_{Op}([\underline{\underline{v}}'], [\underline{\underline{w}}'])$; and from $K^{\bullet}(v', t')$ and (8.23), we have $v' \in [\underline{\underline{v}}']$. Thus $w' \sim \underline{\underline{w}}'$ and $v' \sim \underline{\underline{v}}'$. Hence $KH(w', [v'])$, $HK([v'], [w'])$ and $DK_{Op}([v'], [w'])$ are also true. We now have enough to obtain $H^{\bullet}(w', ([v'], [w']))$ by (8.24).

Now we assume $K^{\bullet}(v', t')$ and $H^{\bullet}(w', ([v'], [w']))$, and prove $H^{\bullet}(w', t')$. Let $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. From $K^{\bullet}(v', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$, by (8.23), $v' \in [\underline{\underline{v}}']$, and $HK([\underline{\underline{v}}'], [\underline{\underline{w}}'])$ holds. Thus $v' \sim \underline{\underline{v}}'$ and so $HK([v'], [\underline{\underline{w}}'])$ holds too. From $H^{\bullet}(w', ([v'], [w']))$, by (8.24), $K(u', w')$ holds for chosen value u'. Then as $K(u', w') ⨾ H^{\bullet}(w', ([v'], [w']))$ holds, by (8.57), there must be a value, $\underline{v}'$ say, for which $H(u', \underline{v}') ⨾ K^{\bullet}(\underline{v}', ([v'], [w']))$ holds, with, by (8.23), $\underline{v}' \in [v']$. We also have $H(u', \underline{v}')$ and $HK([v'], [\underline{\underline{w}}'])$. So, by (8.11), there must be a value, $\underline{w}'$ say, such that $K(u', \underline{w}')$ holds, with $\underline{w}' \in [\underline{\underline{w}}']$. Thus $\underline{w}' \sim \underline{\underline{w}}'$. Now notice we have $K(u', w')$, $K(u', \underline{w}')$ and $H(u', \underline{v}')$. So by (8.5) $w' \sim \underline{w}'$. But as $\underline{w}' \sim \underline{\underline{w}}'$, $w' \sim \underline{\underline{w}}'$. Finally recall that $v' \sim \underline{\underline{v}}'$. Therefore because $H^{\bullet}(w', ([v'], [w']))$ holds, $H^{\bullet}(w', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$ also holds and we are done. ■

♦ (U8):

$R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow$

$\quad (\forall\, k, w \bullet Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t) \Leftrightarrow$

$\quad\quad Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w]))\ )$.

Proof. First we assume $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $Q^{\bullet}_{Op}(k, h, w, t)$ and $H^{\bullet}(w, t)$, and prove $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$.

Let $h = ([\underline{j}], [\underline{\underline{k}}])$ and $t = ([\underline{v}], [\underline{\underline{w}}])$. From the assumed $Q^{\bullet}_{Op}$, (8.26) and (8.16) we have $k \sim \underline{\underline{k}}$ and $w \sim \underline{\underline{w}}$. Furthermore $R^{\bullet}_{Op}$, $K^{\bullet}$, (8.25) and (8.23) give $j \sim \underline{j}$ and $v \sim \underline{\underline{v}}$. Hence, since $Q^{\bullet}_{Op}(k, ([\underline{j}], [\underline{\underline{k}}]), w, ([\underline{v}], [\underline{\underline{w}}]))$ and $H^{\bullet}(w, ([\underline{v}], [\underline{\underline{w}}]))$ hold, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$ follow from the established equivalences.

Now we assume $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$, and prove $Q^{\bullet}_{Op}(k, h, w, t)$ and $H^{\bullet}(w, t)$. We proceed as follows. Let $h = ([\underline{j}], [\underline{\underline{k}}])$ and $t = ([\underline{v}], [\underline{\underline{w}}])$. By (8.26) and (8.16), the given $Q^{\bullet}_{Op}$ lets us assert values i and u, such that $R_{Op}(i, k)$ and $K(u, w)$ are true. Then as $(R_{Op}(i, k) \wedge K(u, w)) ⨾ (Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w])))$ holds, by (8.58), there must be values, $\underline{j}$ and $\underline{v}$ say, such that $(Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) ⨾ (R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])))$ holds. Hence, by (8.25) and (8.23), $\underline{j} \in [j]$ and $\underline{v} \in [v]$.

Now take $R^{\bullet}_{Op}(j, ([\underline{j}], [\underline{\underline{k}}]))$. By (8.25) we get $j \sim \underline{j}$ and $QR_{Op}([\underline{j}], [\underline{\underline{k}}])$, from which $QR_{Op}([j], [\underline{\underline{k}}])$ follows. Since we also have $\underline{j} \in [j]$, $Q_{Op}(i, \underline{j}, u, \underline{v})$, $H(u, \underline{v})$ and $K^{\bullet}(\underline{v}, ([v], [w]))$, by (8.15), we derive $\underline{k}$ for which $R_{Op}(i, \underline{k})$ holds, with $\underline{k} \sim \underline{\underline{k}}$. Now, $R_{Op}(i, k)$, $R_{Op}(i, \underline{k})$ and $Q_{Op}(i, \underline{j}, u, \underline{v})$ all hold. So by (8.7), $k \sim \underline{k}$, and as $\underline{k} \sim \underline{\underline{k}}$, then $k \sim \underline{\underline{k}}$.

Similarly, $K^{\bullet}(v, ([\underline{v}], [\underline{\underline{w}}]))$ and (8.23) gives $v \sim \underline{\underline{v}}$ and $HK([v], [\underline{\underline{w}}])$. So we can use (8.11) to derive value $\underline{w}$, with $\underline{w} \sim \underline{\underline{w}}$, for which $K(u, \underline{w})$ holds. Then using (8.5) and $\underline{w} \sim \underline{\underline{w}}$, we get $w \sim \underline{\underline{w}}$.

So altogether we have $j \sim \underline{j}$, $k \sim \underline{\underline{k}}$, $v \sim \underline{\underline{v}}$ and $w \sim \underline{\underline{w}}$. Hence, because $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$ hold, $Q^{\bullet}_{Op}(k, ([\underline{j}], [\underline{\underline{k}}]), w, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$ and $H^{\bullet}(w, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$ must also hold, as required. ■

♦ (U9):

$V^{\bullet}_{Op}(p, s) \wedge K^{\bullet}(v', t') \wedge R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow$

$\quad (\forall\, q, w', k, w \bullet N^{\bullet}_{Op}(q, s; w', t', k, h, w, t) \wedge H^{\bullet}(w', t') \wedge$

$$Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t) \Leftrightarrow$$
$$N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w])) \wedge$$
$$H^{\bullet}(w', ([v'], [w'])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w]))\ \mathbf{)}\ .$$

Proof. First we assume $V^{\bullet}_{Op}(p, s)$, $K^{\bullet}(v', t')$, $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $N^{\bullet}_{Op}(q, s; w', t', k, h, w, t)$, $H^{\bullet}(w', t')$, $Q^{\bullet}_{Op}(k, h, w, t)$ and $H^{\bullet}(w, t)$, and prove $N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w]))$, $H^{\bullet}(w', ([v'], [w']))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$.

Let $s = ([\underline{p}], [\underline{q}])$, $t' = ([\underline{v}'], [\underline{w}'])$, $h = ([\underline{j}], [\underline{k}])$ and $t = ([\underline{v}], [\underline{w}])$. From the assumed $N^{\bullet}_{Op}$ and (8.28) we have $q \sim \underline{q}$, $w' \sim \underline{w}'$, $k \sim \underline{k}$ and $w \sim \underline{w}$. Furthermore $K^{\bullet\prime}$, $V^{\bullet}_{Op}$, $R^{\bullet}_{Op}$, $K^{\bullet}$, (8.23), (8.25) and (8.27) give $v' \sim \underline{v}'$, $p \sim \underline{p}$, $j \sim \underline{j}$ and $v \sim \underline{v}$. Hence, since $N^{\bullet}_{Op}(q, ([\underline{p}], [\underline{q}]); w', ([\underline{v}'], [\underline{w}']), k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{w}]))$, $H^{\bullet}(w', ([\underline{v}'], [\underline{w}']))$, $Q^{\bullet}_{Op}(k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{w}]))$ and $H^{\bullet}(w, ([\underline{v}], [\underline{w}]))$ hold, $N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w]))$, $H^{\bullet}(w', ([v'], [w']))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$ follow from the established equivalences.

Now we assume $V^{\bullet}_{Op}(p, s)$, $K^{\bullet}(v', t')$, $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w]))$, $H^{\bullet}(w', ([v'], [w']))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$, and prove $N^{\bullet}_{Op}(q, s; w', t', k, h, w, t)$, $H^{\bullet}(w', t')$, $Q^{\bullet}_{Op}(k, h, w, t)$ and $H^{\bullet}(w, t)$. We proceed as follows. Let $s = ([\underline{p}], [\underline{q}])$, $t' = ([\underline{v}'], [\underline{w}'])$, $h = ([\underline{j}], [\underline{k}])$ and $t = ([\underline{v}], [\underline{w}])$. By (8.28), the given $N^{\bullet}_{Op}$ lets us assert values o, u', i and u, such that $V_{Op}(o, q)$, $K(u', w')$, $R_{Op}(i, k)$ and $K(u, w)$ are true. Then as $(V_{Op}(o, q) \wedge K(u', w') \wedge R_{Op}(i, k) \wedge K(u, w)) \fatsemi (N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w', ([v'], [w'])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w])))$ holds, by (8.59), there must be values, $\underline{p}$, $\underline{v}'$, $\underline{j}$ and $\underline{v}$ say, such that $(N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \fatsemi (V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])))$ holds. Hence, by (8.23), (8.25) and (8.27), $\underline{p} \in [p]$, $\underline{v}' \in [v']$, $\underline{j} \in [j]$ and $\underline{v} \in [v]$.

Now take $V^{\bullet}_{Op}(p, ([\underline{p}], [\underline{q}]))$. By (8.27) we get $p \sim \underline{p}$ and $NV_{Op}([\underline{p}], [\underline{q}])$, from which $NV_{Op}([p], [\underline{q}])$ follows. Since we also have $\underline{p} \in [p]$, $N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})$, $H(u', \underline{v}')$, $Q_{Op}(i, \underline{j}, u, \underline{v})$, $H(u, \underline{v})$, $K^{\bullet}(\underline{v}', ([v'], [w']))$, $R^{\bullet}_{Op}(\underline{j}, ([j], [k]))$ and $K^{\bullet}(\underline{v}, ([v], [w]))$, by (8.18), we derive $\underline{q}$ for which $V_{Op}(o, \underline{q})$ holds, with $\underline{q} \sim \underline{q}$. Now, $V_{Op}(o, q)$, $V_{Op}(o, \underline{q})$ and $N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})$ all hold. So by (8.9), $q \sim \underline{q}$, and as $\underline{q} \sim \underline{q}$, then $q \sim \underline{q}$.

Next take $K^{\bullet}(v', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$. From this, by (8.23), we get $v' \sim \underline{\underline{v}}'$ and also $HK([\underline{\underline{v}}'], [\underline{\underline{w}}'])$, from which $HK([v'], [\underline{\underline{w}}'])$ follows. Therefore by (8.11), $H(u', \underline{v}')$, $\underline{v}' \in [v']$ and $HK([v'], [\underline{\underline{w}}'])$ give $K(u', \underline{w}')$ with $\underline{w}' \sim \underline{\underline{w}}'$, for chosen value $\underline{w}'$. So we have $K(u', w')$, $K(u', \underline{w}')$ and $H(u', \underline{v}')$. Hence by (8.5) $w' \sim \underline{w}'$. But as $\underline{w}' \sim \underline{\underline{w}}'$ then $w' \sim \underline{\underline{w}}'$.

Similarly, $R^{\bullet}_{Op}(j, ([\underline{\underline{j}}], [\underline{\underline{k}}]))$ and (8.25) gives $j \sim \underline{\underline{j}}$ and $QR_{Op}([j], [\underline{\underline{k}}])$. This, together with $\underline{\underline{j}} \in [j]$, $Q_{Op}(i, \underline{\underline{j}}, u, \underline{v})$, $H(u, \underline{v})$ and $K^{\bullet}(\underline{v}, ([v], [w]))$ then give $R_{Op}(i, \underline{k})$ with $\underline{k} \sim \underline{\underline{k}}$, by (8.15). Therefore because $R_{Op}(i, k)$, $R_{Op}(i, \underline{k})$ and $Q_{Op}(i, \underline{\underline{j}}, u, \underline{v})$ hold, from (8.7) and $\underline{k} \sim \underline{\underline{k}}$, we get $k \sim \underline{\underline{k}}$.

Last, $K^{\bullet}(v, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$ and (8.23) gives $v \sim \underline{\underline{v}}$ and $HK([v], [\underline{\underline{w}}])$. So we can use (8.11) to derive value $\underline{w}$, with $\underline{w} \sim \underline{\underline{w}}$, for which $K(u, \underline{w})$ holds. Then using (8.5) and $\underline{w} \sim \underline{\underline{w}}$, we get $w \sim \underline{\underline{w}}$.

So altogether we have $p \sim \underline{\underline{p}}$, $q \sim \underline{\underline{q}}$, $v' \sim \underline{\underline{v}}'$, $w' \sim \underline{\underline{w}}'$, $j \sim \underline{\underline{j}}$, $k \sim \underline{\underline{k}}$, $v \sim \underline{\underline{v}}$ and $w \sim \underline{\underline{w}}$. Hence, because $N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w]))$, $H^{\bullet}(w', ([v'], [w']))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $H^{\bullet}(w, ([v], [w]))$ hold, $N^{\bullet}_{Op}(q, ([\underline{\underline{p}}], [\underline{\underline{q}}]); w', ([\underline{\underline{v}}'], [\underline{\underline{w}}']), k, ([\underline{\underline{j}}], [\underline{\underline{k}}]), w, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$, $H^{\bullet}(w', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$, $Q^{\bullet}_{Op}(k, ([\underline{\underline{j}}], [\underline{\underline{k}}]), w, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$ and $H^{\bullet}(w, ([\underline{\underline{v}}], [\underline{\underline{w}}]))$ must also hold, as required. ■

♦ (U10).

Proof. Similar to (U9). ■

♦ (U11): $K^{\bullet}(v', t') \Rightarrow (\exists\, w' \bullet K^{\bullet}(v', ([v'], [w'])))$.

Proof. Assume $K^{\bullet}(v', t')$ with $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then by (8.23) $v' \sim \underline{\underline{v}}'$, which means $K^{\bullet}(v', ([v'], [\underline{\underline{w}}']))$ holds and therefore so does the consequent of (U11). ■

♦ (U12).

Proof. Similar to (U11). ■

8.4 Proof for Part (2)

The systems which complete the square must belong to a class defined by the list of properties (X1) to (X12). To prove the second part of Theorem 8.1 we show that for *any* sys-

tem *Xtra* in the class, there is a refinement from *Univ* to *Xtra*. We proceed as follows. In Section 8.4.1 we define the elements of *Xtra* and list properties (X1) to (X12). In Section 8.4.2 we specify the component relations of the refinement and show that the relevant POs hold. Finally, in Section 8.4.3, we prove the inclusions stated in part (2).

8.4.1 The system *Xtra*

The operation names set of *Xtra* is Ops_X with elements Op_X and $\mathsf{Ops}_X = \mathsf{Ops}_U$. State, input and output spaces are $t\tilde{} \in \mathsf{T}\tilde{}$, $h\tilde{} \in \mathsf{H}\tilde{}_{Op_X}$, $s\tilde{} \in \mathsf{S}\tilde{}_{Op_X}$. Initialisation and step predicates are $Init_X$ and stp_{Op_X}.

Let the retrenchment from *Ref* to *Xtra* be given by the retrieve relation $H\tilde{}$, and for each *Op*, the within relation $Q\tilde{}$, output relation $N\tilde{}$, and concedes relation $D\tilde{}$. Let the refinement from *Ret* to *Xtra* be given by retrieve relation $K\tilde{}$, and for each *Op*, the input relation $R\tilde{}_{Op}$, the output relation $V\tilde{}_{Op}$, the input initialisation $InitIn_{Op_X}$ and the output finalisation $FinOut_{Op_X}$. Let $InitIn_{Op_X}$ and $FinOut_{Op_X}$ be total.

Finally, let *Xtra* have properties (X1) to (X12) below.

$$K\tilde{}(v', t\tilde{}') \wedge K\tilde{}(\underline{v}', t\tilde{}') \Rightarrow v' \sim \underline{v}' \tag{X1}$$

$$V\tilde{}_{Op}(p, s\tilde{}) \wedge V\tilde{}_{Op}(\underline{p}, s\tilde{}) \Rightarrow p \sim \underline{p} \tag{X2}$$

$$\begin{aligned}&(N\tilde{}_{Op}(q, s\tilde{}; w', t\tilde{}', ...) \vee D\tilde{}_{Op}(w', t\tilde{}', q, s\tilde{}; ...)) \wedge \\ &\quad (N\tilde{}_{Op}(\underline{q}, s\tilde{}; \underline{w}', t\tilde{}', ...) \vee D\tilde{}_{Op}(\underline{w}', t\tilde{}', \underline{q}, s\tilde{}; ...)) \Rightarrow q \sim \underline{q} \wedge w' \sim \underline{w}'\end{aligned} \tag{X3}$$

$$K\tilde{}(v', t\tilde{}') \wedge \underline{v}' \in [v'] \Rightarrow K\tilde{}(\underline{v}', t\tilde{}') \tag{X4}$$

$$R\tilde{}_{Op}(j, h\tilde{}) \wedge \underline{j} \in [j] \Rightarrow R\tilde{}_{Op}(\underline{j}, h\tilde{}) \tag{X5}$$

$$V\tilde{}_{Op}(p, s\tilde{}) \wedge \underline{p} \in [p] \Rightarrow V\tilde{}_{Op}(\underline{p}, s\tilde{}) \tag{X6}$$

$$K\tilde{}(v', t\tilde{}') \Rightarrow (H\tilde{}(w', t\tilde{}') \Leftrightarrow H^{\bullet}(w', ([v'], [w']))) \tag{X7}$$

$$\begin{aligned}&R\tilde{}_{Op}(j, h\tilde{}) \wedge K\tilde{}(v, t\tilde{}) \Rightarrow \\ &\quad \mathbf{(} \forall\, k, w \bullet Q\tilde{}_{Op}(k, h\tilde{}, w, t\tilde{}) \wedge H\tilde{}(w, t\tilde{}) \Leftrightarrow \\ &\qquad Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w]))\ \mathbf{)}\end{aligned} \tag{X8}$$

$$V^{\sim}_{Op}(p, s^{\sim}) \wedge K^{\sim}(v', t^{\sim\prime}) \wedge R^{\sim}_{Op}(j, h^{\sim}) \wedge K^{\sim}(v, t^{\sim}) \Rightarrow$$
$$\mathbf{(}\ \forall\ q, w', k, w \bullet N^{\sim}_{Op}(q, s^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w', t^{\sim\prime}) \wedge$$
$$Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w, t^{\sim}) \Leftrightarrow$$
$$N^{\bullet}_{Op}(q, ([p], [q]); w', ([v'], [w']), k, ([j], [k]), w, ([v], [w])) \wedge$$
$$H^{\bullet}(w', ([v'], [w'])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w]))\ \mathbf{)} \tag{X9}$$

$$K^{\sim}(v', t^{\sim\prime}) \wedge V^{\sim}_{Op}(p, s^{\sim}) \wedge R^{\sim}_{Op}(j, h^{\sim}) \wedge K^{\sim}(v, t^{\sim}) \Rightarrow$$
$$\mathbf{(}\ \forall\ w', q, k, w \bullet D^{\sim}_{Op}(w', t^{\sim\prime}, q, s^{\sim}; k, h^{\sim}, w, t^{\sim}) \wedge Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w, t^{\sim}) \Leftrightarrow$$
$$D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w])) \wedge$$
$$Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge H^{\bullet}(w, ([v], [w]))\ \mathbf{)} \tag{X10}$$

$$K^{\sim}(v', t^{\sim\prime}) \Rightarrow (\exists\ w' \bullet K^{\bullet}(v', ([v'], [w']))) \tag{X11}$$

$$V^{\sim}_{Op}(p, s^{\sim}) \Rightarrow (\exists\ q \bullet V^{\bullet}_{Op}(p, ([p], [q]))) \tag{X12}$$

Notice properties (U1) to (U12) are instances of (X1) to (X12) respectively when $\mathsf{T}^{\sim} = \mathsf{T}$, $\mathsf{H}^{\sim} = \mathsf{H}$ and $\mathsf{S}^{\sim} = \mathsf{S}$. Hence *Univ* is a member of the class defined by properties (X1) to (X12).

8.4.2 The refinement from *Univ* to *Xtra*

To show that *Xtra* refines *Univ*, we first define the relations for this refinement and then show that the appropriate POs hold.

8.4.2.1 The component relations

We define the retrieve relation K°, and for each *Op*, the retrieve relation R°_{Op} and output relation V°_{Op} for the refinement from *Univ* to *Xtra*.

$$K^{\circ}(t, t^{\sim}) = K^{\circ}(([v], [w]), t^{\sim}) =$$
$$\mathbf{(}\ \forall\ \underline{v} \bullet \underline{v} \in [v] \Rightarrow K^{\sim}(\underline{v}, t^{\sim})\ \mathbf{)} \wedge \mathbf{(}\ \forall\ \underline{w} \bullet H^{\bullet}(\underline{w}, ([v], [w])) \Rightarrow H^{\sim}(\underline{w}, t^{\sim})\ \mathbf{)} \tag{8.66}$$

For $Op \in \mathsf{Ops}_{\mathrm{A}}$

$$R^{\circ}_{Op}(h, h^{\sim}) = R^{\circ}_{Op}(([j], [k]), h^{\sim}) =$$
$$\mathbf{(}\ \forall\ \underline{j} \bullet \underline{j} \in [j] \Rightarrow R^{\sim}_{Op}(\underline{j}, h^{\sim})\ \mathbf{)} \wedge$$

$$\begin{aligned}
&\mathbf{(}\ \forall\ \underline{k}, \underline{w}, t, \tilde{t} \bullet \overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, t) \wedge H^{\bullet}(\underline{w}, t) \wedge K^{\circ}(t, \tilde{t}) \Rightarrow \\
&\quad Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, \tilde{t}) \wedge H^{\sim}(\underline{w}, \tilde{t})\ \mathbf{)}\ , \qquad (8.67)
\end{aligned}$$

$$\begin{aligned}
&V^{\circ}_{Op}(s, s^{\sim}) \ = \ V^{\circ}_{Op}(([p], [q]), s^{\sim}) \ = \\
&\quad \mathbf{(}\ \forall\ \underline{p} \bullet \underline{p} \in [p] \Rightarrow V^{\sim}_{Op}(\underline{p}, s^{\sim})\ \mathbf{)} \wedge \\
&\quad \mathbf{(}\ \forall\ \underline{q}, \underline{w}', t', \underline{k}, h, \underline{w}, t, \tilde{t}', h^{\sim}, \tilde{t} \bullet \\
&\qquad N^{\bullet}_{Op}(\underline{q}, ([p], [q]); \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H^{\bullet}(\underline{w}', t') \wedge Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t) \wedge H^{\bullet}(\underline{w}, t) \wedge \\
&\qquad K^{\circ}(t', \tilde{t}') \wedge R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, \tilde{t}) \Rightarrow \\
&\qquad\quad N^{\sim}_{Op}(\underline{q}, s^{\sim}; \underline{w}', \tilde{t}', \underline{k}, h^{\sim}, \underline{w}, \tilde{t}) \wedge H^{\sim}(\underline{w}', \tilde{t}') \wedge Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, \tilde{t}) \wedge H^{\sim}(\underline{w}, \tilde{t})\ \mathbf{)} \wedge \\
&\quad \mathbf{(}\ \forall\ \underline{w}', t', \underline{q}, \underline{k}, h, \underline{w}, t, \tilde{t}', h^{\sim}, \tilde{t} \bullet \\
&\qquad D^{\bullet}_{Op}(\underline{w}', t', \underline{q}, ([p], [q]); \underline{k}, h, \underline{w}, t) \wedge Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t) \wedge H^{\bullet}(\underline{w}, t) \wedge \\
&\qquad K^{\circ}(t', \tilde{t}') \wedge R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, \tilde{t}) \Rightarrow \\
&\qquad\quad D^{\sim}_{Op}(\underline{w}', \tilde{t}', \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, \tilde{t}) \wedge Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, \tilde{t}) \wedge H^{\sim}(\underline{w}, \tilde{t})\ \mathbf{)}\ . \qquad (8.68)
\end{aligned}$$

For $Op \notin \mathsf{Ops}_{\mathrm{A}}$

$$R^{\circ}_{Op}(h, h^{\sim}) \ = \ (\exists\ j \bullet h = j \wedge R^{\sim}_{Op}(j, h^{\sim}))\ , \qquad (8.69)$$

$$V^{\circ}_{Op}(s, s^{\sim}) \ = \ (\exists\ p \bullet s = p \wedge V^{\sim}_{Op}(p, s^{\sim}))\ . \qquad (8.70)$$

8.4.2.2 The input initialisation PO

We show

$$InitIn_{Op_{\mathrm{X}}}(l, h^{\sim}) \ \Rightarrow\ (\exists\ h \bullet InitIn_{Op_{\mathrm{U}}}(l, h) \wedge R^{\circ}_{Op}(h, h^{\sim}))\ . \qquad (8.71)$$

Proof. As $Op \in \mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedent $InitIn_{Op_{\mathrm{X}}}(l, h^{\sim})$. Then, from the Input Initialisation PO for the refinement from *Ret* to *Xtra*,

$$InitIn_{Op_{\mathrm{X}}}(l, h^{\sim}) \ \Rightarrow\ (\exists\ \underline{j} \bullet InitIn_{Op_{\mathrm{T}}}(l, \underline{j}) \wedge R^{\sim}_{Op}(\underline{j}, h^{\sim})) \qquad (8.72)$$

we derive $\underline{j}$ such that $InitIn_{Op_{\mathrm{T}}}(l, \underline{j})$ and $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ hold. Now, from the former, by (8.38), $l \sim \underline{j}$. Next, because $l \in \mathsf{L}_{Op}$, by (8.37), there are values, j and k say, such that $j = l$ and $QR_{Op}([j], [k]) \wedge T_{Op}([j], [k])$. Let $h = ([j], [k])$. Then, by (8.40), as $l \in [j]$, $InitIn_{Op_{\mathrm{U}}}(l, h)$ holds.

It remains to show $R^{\circ}_{Op}(h, h^{\sim})$. This we do by establishing each conjunct of (8.67). Take the first conjunct and assume $\underline{j} \in [j]$. We require $R^{\sim}_{Op}(\underline{j}, h^{\sim})$. Now, from above, $l \sim \underline{j}$ and $j = l$. Hence, $j \sim \underline{j}$, and therefore $\underline{j} \in [\underline{j}]$. Thus $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ follows from (X5) because we have $R^{\sim}_{Op}(\underline{j}, h^{\sim})$.

To show the second conjunct assume $\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, \underline{t})$, $H^{\bullet}(\underline{w}, \underline{t})$ and $K^{\circ}(\underline{t}, \underline{t}^{\sim})$, with $\underline{t} = ([\underline{v}], [\underline{\underline{w}}])$. We require $Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, \underline{t}^{\sim}) \wedge H^{\sim}(\underline{w}, \underline{t}^{\sim})$. We work as follows. Given $\overline{Q}_{Op}$ and T_{Op}, by (8.26), $Q^{\bullet}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([\underline{v}], [\underline{\underline{w}}]))$ holds. Furthermore, $j \sim \underline{j}$ and, by (8.16), $\underline{k} \sim k$ and $\underline{w} \sim \underline{\underline{w}}$, which gives $Q^{\bullet}_{Op}(\underline{k}, ([j], [\underline{k}]), \underline{w}, ([\underline{v}], [\underline{w}]))$ and $H^{\bullet}(\underline{w}, ([\underline{v}], [\underline{w}]))$. Also, since we have $K^{\circ}(([\underline{v}], [\underline{\underline{w}}]), \underline{t}^{\sim})$ and $\underline{v} \in [\underline{v}]$, then $K^{\sim}(\underline{v}, \underline{t}^{\sim})$ holds by (8.66). Hence, by (X8), $Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, \underline{t}^{\sim}) \wedge H^{\sim}(\underline{w}, \underline{t}^{\sim})$ holds as required.

• Case $Op \notin \mathsf{Ops}_{\mathrm{A}}$. Assume $InitIn_{Op_{\mathrm{X}}}(l, h^{\sim})$. Then, by (8.72), we derive $\underline{j}$ for which $InitIn_{Op_{\mathrm{T}}}(l, \underline{j})$ and $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ hold. Hence, by (8.43), $l = \underline{j}$. Furthermore, as $l \in \mathsf{L}_{Op}$, by (8.42), there is a value, h say, such that $\underline{j} = h \wedge T_{Op}(\underline{j}, h)$. Hence, by (8.45), $InitIn_{Op_{\mathrm{U}}}(\underline{j}, h)$ and thus $InitIn_{Op_{\mathrm{U}}}(l, h)$ holds. It remains to show $R^{\circ}_{Op}(h, h^{\sim})$. This follows easily from (8.69), because we have $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ with $h = \underline{j}$. Done. ■

8.4.2.3 The initialisation PO

We show

$$Init_{\mathrm{X}}(t^{\sim\prime}) \;\Rightarrow\; (\exists\, t' \bullet Init_{\mathrm{U}}(t') \wedge K^{\circ}(t', t^{\sim\prime})) \;. \tag{8.73}$$

Assume the antecedent $Init_{\mathrm{X}}(t^{\sim\prime})$. Now, we know there is a refinement from *Ret* to *Xtra* and the retrenchment from *Ref* to *Xtra* for which the Init POs are

$$Init_{\mathrm{X}}(t^{\sim\prime}) \;\Rightarrow\; (\exists\, v' \bullet Init_{\mathrm{T}}(v') \wedge K^{\sim}(v', t^{\sim\prime})) \tag{8.74}$$

and

$$Init_{\mathrm{X}}(t^{\sim\prime}) \;\Rightarrow\; (\exists\, w' \bullet Init_{\mathrm{F}}(w') \wedge H^{\sim}(w', t^{\sim\prime})) \tag{8.75}$$

respectively. Accordingly, for the initial $t^{\sim\prime}$, we have v' for which $Init_{\mathrm{T}}(v')$ and w' for which $Init_{\mathrm{F}}(w')$ are true. Furthermore, $K^{\sim}(v', t^{\sim\prime})$ and $H^{\sim}(w', t^{\sim\prime})$ hold, from which, by (X7),

$H^{\bullet}(w', ([v'], [w'])$ holds. From this we can derive $K^{\bullet}(v', ([v'], [w']))$ by using (8.23) and (8.24). Let $t' = ([v'], [w'])$. Then, by (8.30), $Init_{\mathrm{U}}(t')$ is true.

It remains to show $K°$, defined by (8.66), holds for this value of t'. To establish the first conjunct of (8.66), suppose $\underline{v}' \in [v']$. Then because $K\tilde{}(v', t\tilde{}')$ holds, (X4) asserts $K\tilde{}(\underline{v}', t\tilde{}')$ holds, as required. To establish the second conjunct, assume $H^{\bullet}(\underline{w}', ([v'], [w']))$. Then, by (8.24), $\underline{w}' \sim w'$. This means $H^{\bullet}(\underline{w}', ([v'], [\underline{w}']))$ holds, and as we have $K\tilde{}(v', t\tilde{}')$, by (X7), $H\tilde{}(\underline{w}', t\tilde{}')$ holds, as required. We are done. ■

8.4.2.4 The applicability PO

$$K°(t, t\tilde{}) \wedge R°_{Op}(h, h\tilde{}) \wedge trm_{Op_{\mathrm{U}}}(t, h) \;\Rightarrow\; trm_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{}) \,. \tag{8.76}$$

Proof. $Op_{\mathrm{U}} \in \mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, so there are two cases to consider.

• Case $Op_{\mathrm{U}} \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents with $t = ([v], [w])$ and $h = ([j], [k])$. As $v \in [v]$, $K°(t, t\tilde{})$ gives $K\tilde{}(v, t\tilde{})$ by (8.66). Similarly $R°_{Op}(h, h\tilde{})$ gives $R\tilde{}_{Op}(j, h\tilde{})$ by (8.67). Last, $trm_{Op_{\mathrm{U}}}(t, h)$ gives $trm_{Op_{\mathrm{T}}}(v, j)$ by (8.33). Now, $K\tilde{}$, $R\tilde{}_{Op}$ and $trm_{Op_{\mathrm{T}}}$ are the antecedents of the App PO for the refinement from *Ret* to *Xtra*,

$$K\tilde{}(v, t\tilde{}) \wedge R\tilde{}_{Op}(j, h\tilde{}) \wedge trm_{Op_{\mathrm{T}}}(v, j) \;\Rightarrow\; trm_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{}) \,. \tag{8.77}$$

Thus $trm_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{})$ holds as required.

• Case $Op_{\mathrm{U}} \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents with $t = ([v], [w])$. As $v \in [v]$, $K°(t, t\tilde{})$ gives $K\tilde{}(v, t\tilde{})$ by (8.66). From $R°_{Op}(h, h\tilde{})$, by (8.69), we get $R\tilde{}_{Op}(j, h\tilde{})$, with $j = h$. From $v \in [v]$, $j = h$ and $trm_{Op_{\mathrm{U}}}(t, h)$, by (8.34), we get $trm_{Op_{\mathrm{T}}}(v, j)$. Hence, by (8.77), $trm_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{})$ holds, as required. ■

8.4.2.5 The correctness PO

$$\begin{aligned} &K°(t, t\tilde{}) \wedge R°_{Op}(h, h\tilde{}) \wedge trm_{Op_{\mathrm{U}}}(t, h) \wedge stp_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{}, t\tilde{}', s\tilde{}) \;\Rightarrow \\ &\qquad (\exists\, t', s \bullet stp_{Op_{\mathrm{U}}}(t, h, t', s) \wedge K°(t', t\tilde{}') \wedge V°_{Op}(s, s\tilde{})) \end{aligned} \tag{8.78}$$

Proof. Again, $Op \in \mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, so there are two cases to consider.

8.4.2.5.1 Case $Op_X \in \mathsf{Ops}_A$.

Assume the antecedents with $t = ([v], [w])$ and $h = ([j], [k])$. Then, since $v \in [v]$ and $j \in [j]$, by Lemma 8.2, $K^{\sim}(v, t^{\sim})$ and $R^{\sim}_{Op}(j, h^{\sim})$ hold, and furthermore there are values, which we fix as v' and p, for which $stp_{Op_T}(v, j, v', p)$, $K^{\sim}(v', t^{\sim\prime})$ and $V^{\sim}_{Op}(p, s^{\sim})$ hold.

At this point, we will split the proof into two parts. First we will establish that there are t' and s for which $stp_{Op_U}(t, h, t', s)$, the first conjunct of the consequent of (8.78), holds. Second, we will show that for such t' and s, the remainder of the consequent holds.

To show $stp_{Op_U}(t, h, t', s)$, we need to establish both conjuncts of (8.31). Consider (b). For all values $\underline{k}$ and $\underline{w}$ for which the antecedent holds, Lemma 8.3 asserts we have values $\underline{w}'$ and $\underline{q}$ for which $(H^{\sim\prime} \wedge N^{\sim}_{Op})$ or $D^{\sim}_{Op}$ holds. Thus we have three possibilities: (i) there are no values for which the antecedent of (b) holds; (ii) for all values for which the antecedent holds, $H^{\sim\prime} \wedge N^{\sim}_{Op}$ always holds; and (iii) there is at least one pair of values for which the antecedent holds for which $D^{\sim}_{Op}$ holds. We take each case in turn.

- Case (i). (b) holds trivially. It remains to show (a). Its antecedent holds for values v and j, for which we already have $stp_{Op_T}(v, j, v', p)$, $K^{\sim}(v', t^{\sim\prime})$ and $V^{\sim}_{Op}(p, s^{\sim})$. From $K^{\sim\prime}$, by (X11), we know there is a value, $\underline{w}'$ say, such that $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds. Similarly, from $V^{\sim}_{Op}$, by (X12), we get $V^{\bullet}_{Op}(p, ([p], [\underline{q}]))$ for chosen value $\underline{q}$. Let $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Then the consequent of (a) holds.

  Having fixed t' and s, we need to show (a) holds for any other choice of antecedent. So suppose $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Then by Lemma 8.2 there are values, we pick $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ hold. Since we now have both $K^{\sim}(v', t^{\sim\prime})$ and $K^{\sim}(\underline{v}', t^{\sim\prime})$, by (X1), $v' \sim \underline{v}'$ and thus $\underline{v}' \in [v']$. Therefore, because $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds, by (8.23), $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ and therefore $K^{\bullet}(\underline{v}', t')$ holds. Likewise, from $V^{\sim}_{Op}(p, s^{\sim})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$, by (X2) and (8.27) we establish $V^{\bullet}_{Op}(\underline{p}, s)$. Done.

- Case (ii). Let the antecedent of (b) hold for $H^{\bullet}(\underline{w}, t)$ and $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$. Then by Lemma 8.3, we obtain $\underline{w}'$ and $\underline{q}$ such that $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $H^{\sim}(\underline{w}', t^{\sim\prime}) \wedge N^{\sim}_{Op}(\underline{q}, s^{\sim}; \underline{w}', t^{\sim\prime}, \underline{k}, h^{\sim}, \underline{w}, t^{\sim})$ hold ($D^{\sim}_{Op}$ is false for this case). Furthermore, because we have $R^{\circ}_{Op}(h, h^{\sim})$ and $K^{\circ}(t, t^{\sim})$, we have $H^{\sim}(\underline{w}, t^{\sim})$ and $Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, t^{\sim})$, by (8.67). We know, $V^{\sim}_{Op}(p, s^{\sim})$, $K^{\sim}(v', t^{\sim\prime})$, $R^{\sim}_{Op}(j, h^{\sim})$ and $K^{\sim}(v, t^{\sim})$ hold. Hence we can derive $N^{\bullet}_{Op}(\underline{q}, ([p],$

$[\underline{q}]$); $\underline{w}'$, ($[v']$, $[\underline{w}']$), $\underline{k}$, ($[j]$, $[\underline{k}]$), $\underline{w}$, ($[v]$, $[\underline{w}]$)) and $H^{\bullet}(\underline{w}', ([v'], [\underline{w}']))$ via (X9). What is more, because $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$ holds with $h = ([j], [k])$ and $t = ([v], [w])$, by (8.16), $\underline{k} \sim k$ and $\underline{w} \sim w$. Thus $N^{\bullet}_{Op}(\underline{q}, ([p], [\underline{q}]); \underline{w}', ([v'], [\underline{w}']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ holds. Let $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Then the consequent of (b) holds.

Having now fixed t' and s, it is necessary to show (b) for any other choice of antecedent. Thus, assume $H^{\bullet}(\underline{\underline{w}}, t)$ and $\overline{Q}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$. Then by Lemma 8.3, we obtain $\underline{\underline{w}}'$ and $\underline{\underline{q}}$ such that $stp_{Op_F}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}})$ and $H^{\sim}(\underline{\underline{w}}', t^{\sim\prime}) \wedge N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ hold (again $D^{\sim}_{Op}$ is false). Furthermore, because we have $R^{\circ}_{Op}(h, h^{\sim})$ and $K^{\circ}(t, t^{\sim})$, we have $H^{\sim}(\underline{\underline{w}}, t^{\sim})$ and $Q^{\sim}_{Op}(\underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$, by (8.67). We know $V^{\sim}_{Op}(p, s^{\sim})$, $K^{\sim}(v', t^{\sim\prime})$, $R^{\sim}_{Op}(j, h^{\sim})$ and $K^{\sim}(v, t^{\sim})$ hold. Hence we derive $N^{\bullet}_{Op}(\underline{\underline{q}}, ([p], [\underline{\underline{q}}]); \underline{\underline{w}}', ([v'], [\underline{\underline{w}}']), \underline{\underline{k}}, ([j], [\underline{\underline{k}}]), \underline{\underline{w}}, ([v], [\underline{\underline{w}}]))$ and $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$, via (X9). Now $N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ and $N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ imply $\underline{\underline{q}} \sim \underline{q}$ and $\underline{\underline{w}}' \sim \underline{w}'$ by (X3). What is more, because $\overline{Q}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$ holds with $t = ([v], [w])$ and $h = ([j], [k])$, by (8.16), $\underline{\underline{k}} \sim k$ and $\underline{\underline{w}} \sim w$. Thus $N^{\bullet}_{Op}(\underline{\underline{q}}, ([p], [\underline{\underline{q}}]); \underline{\underline{w}}', ([v'], [\underline{\underline{w}}']), \underline{\underline{k}}, ([j], [k]), \underline{\underline{w}}, ([v], [w]))$ and $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$ hold. Hence (b) is always true for our choice of t' and s.

We now show (a) for t' and s. Assume the antecedent of (a) for $\underline{v} \in [v]$ and $\underline{j} \in [j]$. By Lemma 8.2, we obtain $\underline{v}'$ and $\underline{p}$ such that $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ hold. Now $K^{\sim}(v', t^{\sim\prime})$ and $K^{\sim}(\underline{v}', t^{\sim\prime})$ imply $v' \sim \underline{v}'$, by (X1). So, since $H^{\bullet}(\underline{w}', t')$ holds, by (8.24) and (8.23), $K^{\bullet}(\underline{v}', t')$ holds as well. Similarly, $V^{\sim}_{Op}(p, s^{\sim})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ imply $p \sim \underline{p}$, by (X2). Thus, since $N^{\bullet}_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t)$ holds, by (8.28) and (8.27), $V^{\bullet}_{Op}(\underline{p}, s)$ does too. We are done.

• Case (iii). Let $H^{\bullet}(\underline{w}, t)$ and $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$ be the choice of antecedent in (b) for which, by Lemma 8.3, $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $D^{\sim}_{Op}(\underline{w}', t^{\sim\prime}, \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, t^{\sim})$ hold, with chosen values $\underline{w}'$ and $\underline{q}$. From $H^{\bullet}$ and $\overline{Q}_{Op}$ because we have $R^{\circ}_{Op}(h, h^{\sim})$ and $K^{\circ}(t, t^{\sim})$, by (8.67), we also have $H^{\sim}(\underline{w}, t^{\sim})$ and $Q^{\sim}_{Op}(\underline{k}, h^{\sim}, \underline{w}, t^{\sim})$. Now, $K^{\sim}(v', t^{\sim\prime})$, $V^{\sim}_{Op}(p, s^{\sim})$, $R^{\sim}_{Op}(j, h^{\sim})$ and $K^{\sim}(v, t^{\sim})$ all hold. Thus $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [\underline{k}]), \underline{w}, ([v], [\underline{w}]))$ follows from (X10). Note, because we have $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$ with $t = ([v], [w])$ and $h = ([j], [k])$, by (8.16), $\underline{k} \sim k$ and $\underline{w} \sim w$. Hence $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ is also true. Let $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Then the consequent of (b) holds for our choice of antecedent.

We now show that for this t' and s, (b) holds for any other choice of antecedent. So assume $H^{\bullet}(\underline{\underline{w}}, t)$ and $\overline{Q}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$. Then, by Lemma 8.3, we have $\underline{\underline{w}}'$ and $\underline{\underline{q}}$ such that $stp_{Op_F}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}})$ and $(H^{\sim}(\underline{\underline{w}}', t^{\sim\prime}) \wedge N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})) \vee D^{\sim}_{Op}(\underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{q}}, s^{\sim}; \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ hold. And, as we have $R^{\circ}_{Op}(h, h^{\sim})$ and $K^{\circ}(t, t^{\sim})$, by (8.67), $H^{\sim}(\underline{\underline{w}}, t^{\sim})$ and $Q^{\sim}_{Op}(\underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ hold.

First we assume $H^{\sim}(\underline{\underline{w}}', t^{\sim\prime}) \wedge N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$. Then, by (X9), we have $N^{\bullet}_{Op}(\underline{\underline{q}}, ([p], [\underline{q}]); \underline{\underline{w}}', ([v'], [\underline{w}']), \underline{\underline{k}}, ([j], [\underline{k}]), \underline{\underline{w}}, ([v], [\underline{w}])) \wedge H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{w}'])$. Now, by (X3), $N^{\sim}_{Op}(\underline{\underline{q}}, s^{\sim}; \underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ and $D^{\sim}_{Op}(\underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{q}}, s^{\sim}; \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$ imply $\underline{\underline{w}}' \sim \underline{w}'$ and $\underline{\underline{q}} \sim \underline{q}$. Also, because $\overline{Q}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$ holds with $t = ([v], [w])$ and $h = ([j], [k])$, by (8.16), $\underline{\underline{k}} \sim k$ and $\underline{\underline{w}} \sim w$. Thus $N^{\bullet}_{Op}(\underline{\underline{q}}, ([p], [\underline{q}]); \underline{\underline{w}}', ([v'], [\underline{w}']), \underline{\underline{k}}, ([j], [k]), \underline{\underline{w}}, ([v], [w])) \wedge H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{w}'])$ holds and therefore so does the consequent of (b).

On the other hand assume $D^{\sim}_{Op}(\underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{q}}, s^{\sim}; \underline{\underline{k}}, h^{\sim}, \underline{\underline{w}}, t^{\sim})$. Then, by (X10), we have $D^{\bullet}_{Op}(\underline{\underline{w}}', ([v'], [\underline{w}']), \underline{\underline{q}}, ([p], [\underline{q}]); \underline{\underline{k}}, ([j], [\underline{k}]), \underline{\underline{w}}, ([v], [\underline{w}]))$. By (X3), from $D^{\sim}_{Op}(\underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{q}}, s^{\sim}; ...)$ and $D^{\sim}_{Op}(\underline{\underline{w}}', t^{\sim\prime}, \underline{\underline{q}}, s^{\sim}; ...)$ we obtain $\underline{\underline{w}}' \sim \underline{w}'$ and $\underline{\underline{q}} \sim \underline{q}$; and we already have $\underline{\underline{k}} \sim k$ and $\underline{\underline{w}} \sim w$. Hence $D^{\bullet}_{Op}(\underline{\underline{w}}', ([v'], [\underline{w}']), \underline{\underline{q}}, ([p], [\underline{q}]); \underline{\underline{k}}, ([j], [k]), \underline{\underline{w}}, ([v], [w]))$ and the consequent of (b) hold as required.

We now show (a) for $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Assume $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Then, by Lemma 8.2, we have $\underline{v}'$ and $\underline{p}$ for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ hold. Next, $K^{\sim}(v', t^{\sim\prime})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and (X1) assert $v' \sim \underline{v}'$; $V^{\sim}_{Op}(p, s^{\sim})$, $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ and (X2) assert $p \sim \underline{p}$. From above we know $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ is true. Hence (8.29) gives $HK([v'], [\underline{w}'])$ and $DK_{Op}([v'], [\underline{w}'])$. Therefore, as $v' \sim \underline{v}'$, $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ holds by (8.23). (8.29) also gives $NV_{Op}([p], [\underline{q}])$ and $DV_{Op}([p], [\underline{q}])$, so, since $p \sim \underline{p}$, $V^{\bullet}_{Op}(\underline{p}, ([p], [\underline{q}]))$ follows by (8.27). Ergo (a) holds for t' and s. This completes the first part of the proof.

For part two we need to confirm $K^{\circ}(t', t^{\sim\prime})$ and $V^{\circ}_{Op}(s, s^{\sim})$ for $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. To show $K^{\circ\prime}$ we prove both conjuncts of (8.66). Take the first conjunct and assume $\underline{v}' \in [v']$. Then, because $K^{\sim}(v', t^{\sim\prime})$ is true, (X4) gives $K^{\sim}(\underline{v}', t^{\sim\prime})$, as required. Now for the second conjunct. Assume $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{w}']))$. By (8.24), $\underline{\underline{w}}' \in [\underline{w}']$, which means we also have $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$. From this, by (X7), $H^{\sim}(\underline{\underline{w}}', t^{\sim\prime})$ holds, as required.

We turn to V°_{Op}, defined by (8.68). To prove the first conjunct assume $\underline{p} \in [p]$. Then because $V^{\sim}_{Op}(p, s^{\sim})$ is true, (X6) gives $V^{\sim}_{Op}(\underline{p}, s^{\sim})$, as required.

Take the second conjunct. Assume $N^{\bullet}_{Op}(\underline{q}, ([p], [\underline{q}]); \underline{\underline{w}}', \underline{t}', \underline{k}, \underline{h}, \underline{\underline{w}}, \underline{t}), H^{\bullet}(\underline{\underline{w}}', \underline{t}'), Q^{\bullet}_{Op}(\underline{k}, \underline{h}, \underline{\underline{w}}, \underline{t}), H^{\bullet}(\underline{\underline{w}}, \underline{t}), K^{\circ}(\underline{t}', \underline{t}^{\sim\prime}), R^{\circ}_{Op}(\underline{h}, \underline{h}^{\sim})$ and $K^{\circ}(\underline{t}, \underline{t}^{\sim})$, with $\underline{t}' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$, $\underline{h} = ([\underline{j}], [\underline{k}])$, $\underline{t} = ([\underline{\underline{v}}], [\underline{\underline{w}}])$ and $([p], [\underline{q}]) = s = ([p], [\underline{q}])$; the second components are fixed by (8.28) and equivalence. Now, $\underline{\underline{v}}' \in [\underline{\underline{v}}']$ plus $K^{\circ}(\underline{t}', \underline{t}^{\sim\prime})$, by (8.66), give $K^{\sim}(\underline{\underline{v}}', \underline{t}^{\sim\prime})$; $\underline{j} \in [\underline{j}]$ plus $R^{\circ}_{Op}(\underline{h}, \underline{h}^{\sim})$, by (8.67), give $R^{\sim}_{Op}(\underline{j}, \underline{h}^{\sim})$; and $\underline{\underline{v}} \in [\underline{\underline{v}}]$ plus $K^{\circ}(\underline{t}, \underline{t}^{\sim})$, by (8.66), give $K^{\sim}(\underline{\underline{v}}, \underline{t}^{\sim})$. Then because we have $V^{\sim}_{Op}(p, s^{\sim})$, by (X9), we get $N^{\sim}_{Op}(\underline{q}, s^{\sim}; \underline{\underline{w}}', \underline{t}^{\sim\prime}, \underline{k}, \underline{h}^{\sim}, \underline{\underline{w}}, \underline{t}^{\sim}) \wedge H^{\sim}(\underline{\underline{w}}', \underline{t}^{\sim\prime}) \wedge Q^{\sim}_{Op}(\underline{k}, \underline{h}^{\sim}, \underline{\underline{w}}, \underline{t}^{\sim}) \wedge H^{\sim}(\underline{\underline{w}}, \underline{t}^{\sim})$, as required.

The third conjunct is similar. We are done.

8.4.2.5.2 Case $Op_X \notin \mathsf{Ops}_A$.

Assume the antecedents with $t = ([v], [w])$ and let $j = h$. Since $v \in [v]$, by Lemma 8.4, there are values, which we fix as v' and p, such that $stp_{Op_T}(v, j, v', p)$, $K^{\sim}(v', t^{\sim\prime})$ and $V^{\sim}_{Op}(p, s^{\sim})$ hold. From $K^{\sim}(v', t^{\sim\prime})$, by (X11), we know there is a value, $\underline{w}'$ say, such that $K^{\bullet}(v', ([v'], [\underline{w}']))$ is true. Let $t' = ([v'], [\underline{w}'])$ and $s = p$. We now show that for these values of t' and s, stp_{Op_U}, defined by (8.32), holds. Suppose the antecedent of (8.32) is true for $\underline{v} \in [v]$ and $\underline{j} = h$. Then using Lemma 8.4 again, we have values $\underline{v}'$ and $\underline{p}$ such that $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$ hold. Hence, both $K^{\sim}(v', t^{\sim\prime})$ and $K^{\sim}(\underline{v}', t^{\sim\prime})$ are true. Thus, by (X1), $v' \sim \underline{v}'$. Therefore, because $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds, by (8.23), $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ must too. We also have $V^{\sim}_{Op}(p, s^{\sim})$ and $V^{\sim}_{Op}(\underline{p}, s^{\sim})$. Thus, by (X2), $\underline{p} = p$ (because the equivalence class is a singleton), and therefore $\underline{p} = s$. Hence the consequent of (8.32) holds as required.

Finally we show that $K^{\circ}(t', t^{\sim\prime})$ and $V^{\circ}_{Op}(s, s^{\sim})$ hold. The proof for $K^{\circ}(t', t^{\sim\prime})$ is identical to case $Op \in \mathsf{Ops}_A$. Take $V^{\circ}_{Op}(s, s^{\sim})$, defined by (8.70). This clearly holds because we have both $V^{\sim}_{Op}(p, s^{\sim})$ and $s = p$. Done. ■

8.4.2.6 The output finalisation PO

We show

$$V^{\circ}_{Op}(s, s^{\sim}) \wedge FinOut_{Op_X}(s^{\sim}, n) \;\Rightarrow\; FinOut_{Op_U}(s, n)\ . \tag{8.79}$$

Proof. As $Op \in \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider.

• Case $Op \in \mathsf{Ops}_A$. Assume the antecedents with $s = ([p], [q])$. Then, as $p \in [p]$, by (8.68), $V^{\sim}_{Op}(p, s^{\sim})$ holds. Hence, from the Output Finalisation PO for the refinement from *Ret* to *Xtra*,

$$V^{\sim}_{Op}(p, s^{\sim}) \wedge FinOut_{Op_X}(s^{\sim}, n) \;\Rightarrow\; FinOut_{Op_T}(p, n) \tag{8.80}$$

we obtain $FinOut_{Op_T}(p, n)$. Therefore, by (8.39), $p \sim n$. Hence, $n \in [p]$, and consequently, by (8.41), $FinOut_{Op_U}(s, n)$ holds as required.

• Case $Op \notin \mathsf{Ops}_A$. Assume the antecedents. By (8.70), we therefore have $s = p$ and $V^{\sim}_{Op}(p, s^{\sim})$. Hence, by (8.80), we have $FinOut_{Op_T}(p, n)$. From the latter, by (8.44), $p = n$. Thus $s = n$, and so, by (8.46), $FinOut_{Op_U}(s, n)$ holds as required. ■

This completes part (2) of the theorem.

8.4.3 The inclusions

Below we list the inclusions of part (2) of the theorem.

$$K^{\bullet}(\underline{v}, t) ⨾ K^{\circ}(t, t^{\sim}) \Rightarrow K^{\sim}(v, t^{\sim}) \tag{8.81}$$

$$R^{\bullet}_{Op}(\underline{i}, h) ⨾ R^{\circ}_{Op}(h, h^{\sim}) \Rightarrow R^{\sim}_{Op}(\underline{i}, h^{\sim}) \tag{8.82}$$

$$V^{\bullet}_{Op}(\underline{p}, s) ⨾ V^{\circ}_{Op}(s, s^{\sim}) \Rightarrow V^{\sim}_{Op}(\underline{p}, s^{\sim}) \tag{8.83}$$

$$H^{\bullet}(w, t) ⨾ K^{\circ}(t, t^{\sim}) \Rightarrow H^{\sim}(w, t^{\sim}) \tag{8.84}$$

The remaining inclusions only apply to $Op \in \mathsf{Ops}_A$.

$$\begin{aligned}&(Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t)) ⨾ (R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, t^{\sim})) \Rightarrow \\ &\quad (Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w, t^{\sim}))\end{aligned} \tag{8.85}$$

$$\begin{aligned}&(N^{\bullet}_{Op}(q, s; w', t', k, h, w, t) \wedge H^{\bullet}(w', t') \wedge Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t)) ⨾ \\ &\quad (V^{\circ}_{Op}(s, s^{\sim}) \wedge K^{\circ}(t', t^{\sim\prime}) \wedge R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, t^{\sim})) \Rightarrow \\ &\qquad N^{\sim}_{Op}(q, s^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w', t^{\sim\prime}) \wedge Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge\end{aligned}$$

$$H^{\sim}(w, t^{\sim})$$

(8.86)

$$(D^{\bullet}_{Op}(w', t', q, s; k, h, w, t) \wedge Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t)) \fatsemi (K^{\circ}(t', t^{\sim\prime}) \wedge V^{\circ}_{Op}(s, s^{\sim}) \wedge R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, t^{\sim})) \Rightarrow (D^{\sim}_{Op}(w', t^{\sim\prime}, q, s^{\sim}; k, h^{\sim}, w, t^{\sim}) \wedge Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w, t^{\sim})) \quad (8.87)$$

We now show these inclusions hold.

♦ (8.81): $K^{\bullet}(\underline{v}, t) \fatsemi K^{\circ}(t, t^{\sim}) \Rightarrow K^{\sim}(v, t^{\sim})$.

Proof. Assume the antecedents and let $t = ([v], [w])$. Then from $K^{\bullet}(\underline{v}, ([v], [w]))$, by (8.23), $\underline{v} \in [v]$, and thus from $K^{\circ}(([v], [w]), t^{\sim})$, by (8.66), $K^{\sim}(\underline{v}, t^{\sim})$ follows, as required. ■

♦ (8.82): $R^{\bullet}_{Op}(\underline{j}, h) \fatsemi R^{\circ}_{Op}(h, h^{\sim}) \Rightarrow R^{\sim}_{Op}(\underline{j}, h^{\sim})$.

Proof. $Op \in \mathsf{Ops}_{\mathrm{A}} \cup (\mathsf{Ops}_{\mathrm{U}} - \mathsf{Ops}_{\mathrm{A}})$, so there are two cases to consider.

• Case $Op \in \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents and let $h = ([j], [k])$. Then from $R^{\bullet}_{Op}(\underline{j}, ([j], [k]))$, by (8.25), $\underline{j} \in [j]$, and thus from $R^{\circ}_{Op}(([j], [k]), h^{\sim})$, by (8.67), $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ follows.

• Case $Op \notin \mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents. From $R^{\bullet}_{Op}$, by (8.35), $\underline{j} = h$, and therefore from $R^{\circ}_{Op}(h, h^{\sim})$, by (8.69), $R^{\sim}_{Op}(\underline{j}, h^{\sim})$ follows. ■

♦ (8.83).

Proof. Similar to (8.82). ■

♦ (8.84): $H^{\bullet}(w, t) \fatsemi K^{\circ}(t, t^{\sim}) \Rightarrow H^{\sim}(w, t^{\sim})$.

Proof. The consequent follows immediately from the antecedents by (8.66). ■

♦ (8.85): $(Q^{\bullet}_{Op}(k, h, w, t) \wedge H^{\bullet}(w, t)) \fatsemi (R^{\circ}_{Op}(h, h^{\sim}) \wedge K^{\circ}(t, t^{\sim})) \Rightarrow (Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge H^{\sim}(w, t^{\sim}))$.

Proof. Assume the antecedents. As $Q^{\bullet}_{Op}(k, h, w, t)$ gives $\overline{Q}_{Op}(k, h, w, t)$ by (8.26), the consequent follows from the antecedent, by (8.67). ■

♦ (8.86) and (8.87).

Proof. Similar to (8.84). ■

8.5 Proof for Part (3)

Part (3) follows readily by observing that for a system *Univ** having the same properties as *Univ*, there will be a refinement from *Univ* to *Univ** and a refinement from *Univ** to *Univ*. ☺ ■

This completes the proof of Theorem 8.1.

8.6 Lemmas

Lemma 8.2. Suppose $K^{\circ}(t, \tilde{t})$, $R^{\circ}_{Op}(h, \tilde{h})$, $trm_{Op_U}(t, h)$ and $stp_{Op_X}(\tilde{t}, \tilde{h}, \tilde{t}', \tilde{s})$ hold with $t = ([v], [w])$ and $h = ([j], [k])$. Furthermore suppose $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Then $\tilde{K}(\underline{v}, \tilde{t})$ and $\tilde{R}_{Op}(\underline{j}, \tilde{h})$ hold, and moreover there are values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $\tilde{K}(\underline{v}', \tilde{t}')$ and $\tilde{V}_{Op}(\underline{p}, \tilde{s})$ hold.

Proof. From $K^{\circ}(t, \tilde{t})$ and $\underline{v} \in [v]$ we get $\tilde{K}(\underline{v}, \tilde{t})$, by (8.66); from $R^{\circ}_{Op}(h, \tilde{h})$ and $\underline{j} \in [j]$ we get $\tilde{R}_{Op}(\underline{j}, \tilde{h})$, by (8.67); and from $trm_{Op_U}(t, h)$, $\underline{v} \in [v]$ and $\underline{j} \in [j]$ we get $trm_{Op_T}(\underline{v}, \underline{j})$ by (8.33). $\tilde{K}$, $\tilde{R}_{Op}$, trm_{Op_T} and stp_{Op_X} are the antecedents of the Op PO for the refinement from *Ret* to *Xtra*,

$$\begin{aligned} &\tilde{K}(\underline{v}, \tilde{t}) \wedge \tilde{R}_{Op}(\underline{j}, \tilde{h}) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge stp_{Op_X}(\tilde{t}, \tilde{h}, \tilde{t}', \tilde{s}) \Rightarrow \\ &\quad (\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \tilde{K}(\underline{v}', \tilde{t}') \wedge \tilde{V}_{Op}(\underline{p}, \tilde{s}))\ . \end{aligned} \tag{8.88}$$

Thus we can pick values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $\tilde{K}(\underline{v}', \tilde{t}')$ and $\tilde{V}_{Op}(\underline{p}, \tilde{s})$ hold. Done. ■

Lemma 8.3. Suppose $K^{\circ}(t, \tilde{t})$, $R^{\circ}_{Op}(h, \tilde{h})$ and $stp_{Op_X}(\tilde{t}, \tilde{h}, \tilde{t}', \tilde{s})$ hold with $t = ([v], [w])$ and $h = ([j], [k])$. Furthermore suppose $H^{\bullet}(\underline{w}, t)$ and $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$ hold. Then there are

values, which we fix as $\underline{w}'$ and $\underline{q}$, for which $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $(H^{\sim}(\underline{w}', t^{\sim\prime}) \wedge N^{\sim}{}_{Op}(\underline{q}, s^{\sim}; \underline{w}', t^{\sim\prime}, \underline{k}, h^{\sim}, \underline{w}, t^{\sim})) \vee D^{\sim}{}_{Op}(\underline{w}', t^{\sim\prime}, \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, t^{\sim})$ hold.

Proof. From $R^{\circ}{}_{Op}(h, h^{\sim})$, $H^{\bullet}(\underline{w}, t)$, $\overline{Q}_{Op}(\underline{k}, h, \underline{w}, t)$ and $K^{\circ}(t, t^{\sim})$ we get $H^{\sim}(\underline{w}, t^{\sim})$ and $Q^{\sim}{}_{Op}(\underline{k}, h^{\sim}, \underline{w}, t^{\sim})$, by (8.67). $H^{\sim}$, $Q^{\sim}{}_{Op}$ and stp_{Op_X} are the antecedents of the Op PO for the retrenchment from *Ref* to *Xtra*,

$$\begin{aligned} & H^{\sim}(w, t^{\sim}) \wedge Q^{\sim}{}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, s^{\sim}) \Rightarrow \\ & \quad (\exists\, \underline{w}', \underline{q} \bullet stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \\ & \qquad ((H^{\sim}(\underline{w}', t^{\sim\prime}) \wedge N^{\sim}{}_{Op}(\underline{q}, s^{\sim}; \underline{w}', t^{\sim\prime}, \underline{k}, h^{\sim}, \underline{w}, t^{\sim})) \vee D^{\sim}{}_{Op}(\underline{w}', t^{\sim\prime}, \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, t^{\sim}))) . \end{aligned} \tag{8.89}$$

Thus we can pick values, which we fix as $\underline{w}'$ and $\underline{q}$, for which $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $(H^{\sim}(\underline{w}', t^{\sim\prime}) \wedge N^{\sim}{}_{Op}(\underline{q}, s^{\sim}; \underline{w}', t^{\sim\prime}, \underline{k}, h^{\sim}, \underline{w}, t^{\sim})) \vee D^{\sim}{}_{Op}(\underline{w}', t^{\sim\prime}, \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, t^{\sim})$ hold. ■

Lemma 8.4. Suppose $K^{\circ}(t, t^{\sim})$, $R^{\circ}{}_{Op}(h, h^{\sim})$, $trm_{Op_U}(t, h)$ and $stp_{Op_X}(t^{\sim}, h^{\sim}, t^{\sim\prime}, s^{\sim})$ hold with $t = ([v], [w])$. Furthermore suppose $\underline{v} \in [v]$ and let $\underline{j} = h$. Then there are values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}{}_{Op}(\underline{p}, s^{\sim})$ hold.

Proof. From $K^{\circ}(t, t^{\sim})$ and $\underline{v} \in [v]$ we get $K^{\sim}(\underline{v}, t^{\sim})$, by (8.66); from $R^{\circ}{}_{Op}(h, h^{\sim})$ we get $R^{\sim}{}_{Op}(\underline{j}, h^{\sim})$, by (8.69). Then from $\underline{v} \in [v]$ and $\underline{j} = h$, we get $trm_{Op_T}(\underline{v}, \underline{j})$, by (8.34). $K^{\sim}$, $R^{\sim}{}_{Op}$, trm_{Op_T} and stp_{Op_X} are the antecedents of PO (8.88), so we can pick values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K^{\sim}(\underline{v}', t^{\sim\prime})$ and $V^{\sim}{}_{Op}(\underline{p}, s^{\sim})$ hold. ■

8.7 Inside *Univ*

Let us again go back to the Number Recycler and the *Add* operation, and see what we get for *Univ*. As in Chapter 5, *Abs* specifies an unbounded bin modelled by a set. We reproduce the parts of *Abs* germane to our discussion.

$$\mathsf{U} = \mathbb{P}(\mathbb{N}),\ \mathsf{I}_{Add_A} = \mathbb{N},\ \mathsf{O}_{Add_A} = \{\mathsf{OK}, \mathsf{GOT}\} . \tag{8.90}$$

$$\begin{aligned} & u \text{ -}(i, Add_A, \mathsf{OK})\text{-}\!\!> u \cup \{\, i \,\}, \text{ if } i \notin u , \\ & u \text{ -}(i, Add_A, \mathsf{GOT})\text{-}\!\!> u, \text{ if } i \in u . \end{aligned} \tag{8.91}$$

For the retrenchment to *Ret* we introduce a limit on the size of the bin. We restrict the capacity to five and add a message to indicate when the bin is full. We still use a set for the bin. The specification for *Ret* is therefore

$$\mathsf{V} = \{v \in \mathbb{P}(\mathbb{N}) \mid |v| \leq 5\},\ \mathsf{J}_{Add_C} = \mathbb{N},\ \mathsf{P}_{Add_C} = \{\mathsf{OK}, \mathsf{GOT}, \mathsf{FULL}\}\ . \tag{8.92}$$

$$\begin{aligned} &v \text{ -}(j, Add_C, \mathsf{OK})\text{-}\!\rightarrow v \cup \{\, j \,\},\ \text{ if } j \notin v \wedge |\, v \,| \leq 4\ , \\ &v \text{ -}(j, Add_C, \mathsf{FULL})\text{-}\!\rightarrow v,\ \text{ if } j \notin v \wedge |\, v \,| = 5\ , \\ &v \text{ -}(j, Add_C, \mathsf{GOT})\text{-}\!\rightarrow v,\ \text{ if } j \in v\ . \end{aligned} \tag{8.93}$$

The data for the retrenchment is as follows.

$$\begin{aligned} &H(u, v) = (u = v)\ , \\ &Q_{Add}(i, j, u, v) \ = \ (i = j)\ , \\ &N_{Add}(o, p, u', v'; i, j, u, v) \ = \ (o = p)\ , \\ &D_{Add}(u', v', o, p; i, j, u, v) \ = \\ &\qquad (\ |u| = 5 \wedge i \notin u \wedge u' = u \cup \{\, i \,\} \wedge v' = u \wedge o = \mathsf{OK} \wedge p = \mathsf{FULL}\ )\ . \end{aligned} \tag{8.94}$$

The refinement from *Abs* to *Ret* replaces the set by a sequence. Like the set, the sequence is boundless. So we have

$$\mathsf{W} = \mathsf{iseq}(\mathbb{N}),\ \mathsf{K}_{Add_F} = \mathbb{N},\ \mathsf{Q}_{Add_F} = \{\mathsf{OK}, \mathsf{GOT}\}\ . \tag{8.95}$$

$$\begin{aligned} &w \text{ -}(k, Add_F, \mathsf{OK})\text{-}\!\rightarrow w \frown \langle\, k \,\rangle,\ \text{ if } k \notin \mathsf{ran}(w)\ , \\ &w \text{ -}(k, Add_F, \mathsf{GOT})\text{-}\!\rightarrow w,\ \text{ if } k \in \mathsf{ran}(w)\ . \end{aligned} \tag{8.96}$$

Last we define the relations for the refinement.

$$\begin{aligned} &K(u, w) = (u = \mathsf{ran}(w))\ , \\ &R_{Add}(i, k) \ = \ (i = k)\ , \\ &V_{Add}(o, q) \ = \ (o = q)\ . \end{aligned} \tag{8.97}$$

Having specified all the relations, we can look at how the spaces of *Ref* and *Ret* are partitioned by (8.4) to (8.9). We start with W, the state space of *Ref*. This is divided up as follows. Sequences of length four or less occur in the same class if they have the same range, i.e. if they are serialisations of the same set. For example, for $\{1, 2\}$ we have $K^{\mathrm{T}} \fatsemi HD(\langle 1, 2\rangle, \{1, 2\})$ and $K^{\mathrm{T}} \fatsemi HD(\langle 2, 1\rangle, \{1, 2\})$. This results in the class $[w] = \{\langle 1, 2\rangle, \langle 2,$

1⟩}. Sequences of length five and six fall in the same class when the range of the first five elements is equal, e.g. [w] = {⟨1 .. 5⟩, ⟨1 .. 5, 6⟩, ⟨1 .. 5, 7⟩, ..., ⟨5 .. 1⟩, ⟨5 .. 1, 6⟩, ⟨5 .. 1, 7⟩, ..., ⟨2, 1, 3, 4, 5⟩, ⟨2, 1, 3, 4, 5, 6⟩, ...}. Figure 8.2 shows why ⟨1 .. 5⟩ and ⟨1 .. 5, 6⟩ are in

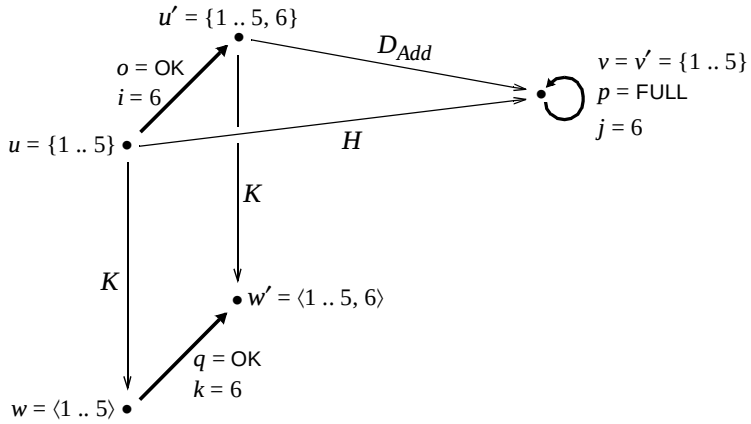


Figure 8.2

the same class: both are linked to {1 .. 5}. Notice D_{Add} is shown joining just the after states, because, by (8.1) and (8.5), only these components are involved in the definition of the class. Lastly, each sequence of length seven or more forms its own singleton class, e.g. [w] = {⟨11, 22, 88, 1, 2000, 3, 318⟩}. This is because H (and D_{Add} for before states) does not hold for sets of cardinality greater than 5. The situation for V, the state space of *Ret*, is much simpler. Each set just forms its own singleton, e.g. [v] = {{1 .. 5}} or [v] = {{16, 77, 1001}}.

(8.6) and (8.7) partition the input spaces J_{Add_T} and K_{Add_F} into singletons with elements from ℕ, e.g. [j] = {48} and [k] = {1}. For the output spaces, we note N_{Add} links o = GOT with p = GOT and o = OK with p = OK, whereas D_{Add} links o = OK with p = FULL. Therefore, by (8.8), P_{Add_F} is partitioned into the singleton [GOT] and the doubleton [OK] = {OK, FULL}. From Q_{Add_F}, by (8.9), we get the two singletons [OK] and [GOT].

Let us now consider the transitions of *Univ* for $Op \in \mathsf{Ops}_A$. These are given by (8.31), which looks pretty complicated. Fortunately, the definition is easily tamed by picturing

a *Univ* step as being a container which brings together corresponding *Ret* and *Ref* steps. Suppose (8.31) holds for the step $([v], [w])$ -(($[j]$, $[k]$), Op_{U}, ($[p]$, $[q]$))-› $([v'], [w'])$. Then, by (8.31a), $\underline{w}$ -($\underline{k}$, Op_{F}, $\underline{q}$)-› $\underline{w}'$, will be contained in the *Univ* step if $H^{\bullet} \wedge \overline{Q}_{Op} \wedge ((H^{\bullet\prime} \wedge N^{\bullet}{}_{Op}) \vee D^{\bullet}{}_{Op}))$ holds. Similarly, by (8.31b), so will $\underline{v}$ -($\underline{j}$, Op_{T}, $\underline{p}$)-› $\underline{v}'$, if $\underline{v} \in [v] \wedge \underline{j} \in [j] \wedge K^{\bullet\prime} \wedge V^{\bullet}{}_{Op}$ holds. Notice, since $v \in [v]$ and $j \in [j]$, each *Univ* step must incorporate at least one *Ret* step. Further, if (8.31b) holds trivially, *Univ* may contain no *Ref* steps. We refer to such *Univ* steps as junk. However, when we restrict attention to that part of *Univ* which is a retrenchment of *Abs*, $G \wedge P_{Op}$ must hold, which implies, by (8.58), $Q^{\bullet}{}_{Op} \wedge H^{\bullet}$ holds as well. Hence, the part of *Univ* which is a retrenchment of *Abs* will bring together at least one *Ret* and one *Ref* transition.

A simple example is shown in Figure 8.3, in which I/O has been suppressed. The *Ret* and

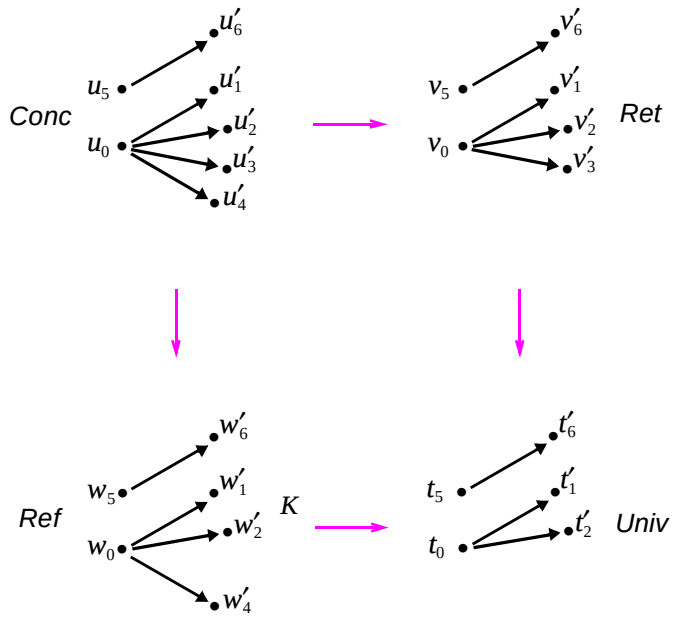


Figure 8.3

Ref transitions satisfy (8.31). Transitions with matching subscripts are related in that one retrenches or refines the other. Thus $w_0 \mapsto w'_4$ refines $u_0 \mapsto u'_4$ and $v_5 \mapsto v'_6$ retrenches u_5

$\mapsto u'_6$. Each *Univ* step is an amalgam of *Ret* and *Ref* steps which match it on subscripts. Hence, $t_0 \mapsto t'_2$ is a combination of the steps $v_0 \mapsto v'_2$ and $w_0 \mapsto w'_2$.

Univ is the most abstract completion in the class. Therefore any other member of the class completing the square will be refinable from *Univ*. As refinement is concerned with reduction in nondeterminism, this therefore precludes solutions like the *Univ* in Figure 8.3 but with, for instance, the transition $t_0 \mapsto t'_2$ omitted (the old *Univ* still completes the square so must be refinable from the one with the omitted transition).

Returning to our running example, the Add_U step which brings together the two boundary transitions shown in Figure 8.2 is

$$([\{1 .. 5\}], [\langle 1 .. 5\rangle])\ \text{-}(([6], [6]), Add_U, ([\mathsf{FULL}], [\mathsf{OK}]))\text{-}\rightarrow\ ([\{1 .. 5\}], [\langle 1 .. 5, 6\rangle])\ .$$

Of course, $\langle 1 .. 5\rangle$ -(6, Add_F, OK)-› $\langle 1 .. 5, 6\rangle$ is not the only Add_F step which corresponds to $\{1 .. 5\}$ -(6, Add_T, FULL)-› $\{1 .. 5\}$. All Add_F steps whose before state $\underline{w}$ is a serialisation of $\{1 .. 5\}$ and after state is $\underline{w} \wedge \langle 6\rangle$, will also be part of the Add_U step, e.g. $\langle 4, 2, 1, 5, 3\rangle$ -(6, Add_F, OK)-› $\langle 4, 2, 1, 5, 3, 6\rangle$.

We see a similar situation for non-boundary steps, e.g.

$$([\{1, 2\}], [\langle 2, 1\rangle])\ \text{-}(([2], [2]), Add_U, ([\mathsf{GOT}], [\mathsf{GOT}]))\text{-}\rightarrow\ ([\{1, 2\}], [\langle 2, 1\rangle])\ .$$

This brings together the corresponding steps $\{1, 2\}$ -(2, Add_T, GOT)-› $\{1, 2\}$, $\langle 1, 2\rangle$ -(2, Add_F, GOT)-› $\langle 1, 2\rangle$ and $\langle 2, 1\rangle$ -(2, Add_F, GOT)-› $\langle 2, 1\rangle$.

We conclude with the following remark. A point sometimes made is that surely a solution for *Univ* is just the system *Ret*. Why this is not so is clearly shown in Figure 8.3. Putting *Ret* in place of *Univ* means $v_0 \mapsto v'_3$ will not have a suitable step in *Ref* which it can retrench.

Chapter 9

The Prejoin Theorem

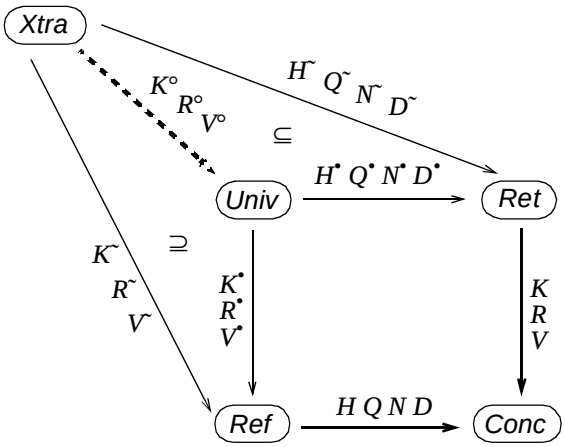
Given a system *Conc* that is both a refinement of a system *Ret* and a retrenchment of a system *Ref*, such that the refinement and retrenchment are preconjoint (see below), the prejoin completes the square by constructing a system *Univ* with the following properties. First, from *Univ* there is both a retrenchment to *Ret* and a refinement to *Ref*. Second, the composition of the *Univ* to *Ret* retrenchment with the *Ret* to *Conc* refinement on the one hand, and the composition of the *Univ* to *Ref* refinement with the *Ref* to *Conc* retrenchment on the other, are both equal as a retrenchment from *Univ* to *Conc*. Third, in the class of systems achieving a similar completion, *Univ* is the most concrete up to equivalence. We make these ideas precise in the theorem below.

9.1 The Prejoin Theorem

Theorem 9.1. Let there be a retrenchment from *Ref* to *Conc*, and a refinement from *Ret* to *Conc*, as shown in Figure 9.1. If the retrenchment and refinement are *preconjoint*, the following hold.

(1) There is a universal system *Univ* for which there is a retrenchment from *Univ* to *Ret* and a refinement from *Univ* to *Ref* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Univ* to *Conc*, and which satisfies (U1) to (U7) below.

(2) Whenever there is a system *Xtra* and a retrenchment from *Xtra* to *Ret* and a refinement from *Xtra* to *Ref* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Xtra* to *Conc*, and which satisfies (X1)



All arrows labelled H, Q, N, D are retrenchments;
all arrows labelled K, R, V are refinements.

Figure 9.1: The relationship between systems in a prejoin.

to (X7) below, then there is a refinement from *Xtra* to *Univ* such that $K^{\circ} \fatsemi H^{\bullet} \Rightarrow H^{\sim}$, $(R^{\circ} \wedge K^{\circ}) \fatsemi (Q^{\bullet} \wedge H^{\bullet}) \Rightarrow (Q^{\sim} \wedge H^{\sim})$, $(V^{\circ} \wedge K^{\circ\prime} \wedge R^{\circ} \wedge K^{\circ}) \fatsemi (N^{\bullet} \wedge H^{\bullet\prime} \wedge Q^{\bullet} \wedge H^{\bullet}) \Rightarrow (N^{\sim} \wedge H^{\sim\prime} \wedge Q^{\sim} \wedge H^{\sim})$, $(K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \fatsemi (D^{\bullet} \wedge Q^{\bullet} \wedge H^{\bullet}) \Rightarrow (D^{\sim} \wedge Q^{\sim} \wedge H^{\sim})$, and such that $K^{\circ} \fatsemi K^{\bullet} \Rightarrow K^{\sim}$, $R^{\circ} \fatsemi R^{\bullet} \Rightarrow R^{\sim}$, $V^{\circ} \fatsemi V^{\bullet} \Rightarrow V^{\sim}$ (see also (9.74) to (9.80)).

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are mutually interrefinable.

9.2 Basic Definitions

For *Ret* the operation names set is $Op_{\mathrm{T}} \in \mathsf{Ops}_{\mathrm{T}}$, state, input and output spaces are $v \in \mathsf{V}$, $j \in \mathsf{J}_{Op_{\mathrm{T}}}$, $p \in \mathsf{P}_{Op_{\mathrm{T}}}$, and initialisation and step predicates are $Init_{\mathrm{T}}$ and $stp_{Op_{\mathrm{T}}}$. Correspondingly, for *Ref* we have $Op_{\mathrm{F}} \in \mathsf{Ops}_{\mathrm{F}}$, $w \in \mathsf{W}$, $k \in \mathsf{K}_{Op_{\mathrm{F}}}$, $q \in \mathsf{Q}_{Op_{\mathrm{F}}}$, $Init_{\mathrm{F}}$ and $stp_{Op_{\mathrm{F}}}$, and for *Conc*, $Op_{\mathrm{C}} \in \mathsf{Ops}_{\mathrm{C}}$, $t \in \mathsf{T}$, $h \in \mathsf{H}_{Op_{\mathrm{C}}}$, $s \in \mathsf{S}_{Op_{\mathrm{C}}}$, $Init_{\mathrm{C}}$ and $stp_{Op_{\mathrm{C}}}$. Here, $\mathsf{Ops}_{\mathrm{F}} \subseteq \mathsf{Ops}_{\mathrm{C}} = \mathsf{Ops}_{\mathrm{T}}$.

Let the refinement from *Ret* to *Conc* have retrieve relation K, and for each Op, input relation R_{Op} and output relation V_{Op}. Let the retrenchment from *Ref* to *Conc* have retrieve relation H, and for each Op, within relation Q_{Op}, output relation N_{Op} and concedes relation D_{Op}.

In the remainder of this section we define the various elements we use in the construction of *Univ* and the associated retrenchment and refinement. Let,

$$HD(w, t) = H(w, t) \vee \bigvee_{Op} (\exists\, \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(w, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \,, \tag{9.1}$$

$$QQ_{Op}(k, h) = (\exists\, \underline{w}, \underline{t} \bullet Q_{Op}(k, h, \underline{w}, \underline{t})) \,, \tag{9.2}$$

$$ND_{Op}(q, s) = \\ (\exists\, \underline{w}', \underline{t}', \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet N_{Op}(q, s; \underline{w}', \underline{t}', \underline{k}, \underline{h}, \underline{w}, \underline{t}) \vee D_{Op}(\underline{w}', \underline{t}', q, s; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \,. \tag{9.3}$$

Using the above, we specify the following equivalence relations.

$$\sim_{\mathrm{V}} = ((K \fatsemi HD^{\mathrm{T}}) \fatsemi (K \fatsemi HD^{\mathrm{T}})^{\mathrm{T}})^{*} \,, \tag{9.4}$$

$$\sim_{\mathrm{W}} = ((HD \fatsemi K^{\mathrm{T}}) \fatsemi (HD \fatsemi K^{\mathrm{T}})^{\mathrm{T}})^{*} \,, \tag{9.5}$$

$$\sim_{\mathrm{J}_{Op}} = ((R_{Op} \fatsemi QQ_{Op}^{\mathrm{T}}) \fatsemi (R_{Op} \fatsemi QQ_{Op}^{\mathrm{T}})^{\mathrm{T}})^{*} \,, \tag{9.6}$$

$$\sim_{\mathrm{K}_{Op}} = ((QQ_{Op} \fatsemi R_{Op}^{\mathrm{T}}) \fatsemi (QQ_{Op} \fatsemi R_{Op}^{\mathrm{T}})^{\mathrm{T}})^{*} \,, \tag{9.7}$$

$$\sim_{\mathrm{P}_{Op}} = ((V_{Op} \fatsemi ND_{Op}^{\mathrm{T}}) \fatsemi (V_{Op} \fatsemi ND_{Op}^{\mathrm{T}})^{\mathrm{T}}{}_{p})^{*} \,, \tag{9.8}$$

$$\sim_{\mathrm{Q}_{Op}} = ((ND_{Op} \fatsemi V_{Op}^{\mathrm{T}}) \fatsemi (ND_{Op} \fatsemi V_{Op}^{\mathrm{T}})^{\mathrm{T}})^{*} \,. \tag{9.9}$$

Let $[v] \in \mathsf{V}/\sim_{\mathrm{V}}$, $[w] \in \mathsf{W}/\sim_{\mathrm{W}}$, $[j] \in \mathsf{J}_{Op}/\sim_{\mathrm{J}_{Op}}$, $[k] \in \mathsf{K}_{Op}/\sim_{\mathrm{K}_{Op}}$, $[p] \in \mathsf{P}_{Op}/\sim_{\mathrm{P}_{Op}}$ and $[q] \in \mathsf{Q}_{Op}/\sim_{\mathrm{Q}_{Op}}$. Then,

$$KH(\underline{v}, [w]) \;=\; (\forall\, t \bullet K(\underline{v}, t) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))) \,, \tag{9.10}$$

$$HK([v], [w]) \;=\; (\forall\, \underline{w}, t \bullet \underline{w} \in [w] \wedge H(\underline{w}, t) \Rightarrow \\ (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w]))) \,, \tag{9.11}$$

$$KD_{Op}(\underline{v}, [w]) \;=\; (\forall\, t \bullet K(\underline{v}, t) \Rightarrow \\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge (\exists\, \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(\underline{w}, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})))) \,, \tag{9.12}$$

$$DK_{Op}([v], [w]) \;= \\ (\forall\, \underline{w}, t \bullet \underline{w} \in [w] \wedge (\exists\, \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(\underline{w}, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \Rightarrow \\ (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KD_{Op}(\underline{v}, [w]))) \,, \tag{9.13}$$

$$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) =$$
$$trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))\,, \tag{9.14}$$

$$QR_{Op}([j], [k]) =$$
$$(\forall\, \underline{k}, h, \underline{w}, t, v, w \bullet \underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))\,, \tag{9.15}$$

$$VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) =$$
$$trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))\,, \tag{9.16}$$

$$NV_{Op}([p], [q]) =$$
$$(\forall\, \underline{q}, s, \underline{w}', t', \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$
$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$
$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])))\,, \tag{9.17}$$

$$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) =$$
$$trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))\,, \tag{9.18}$$

$$DV_{Op}([p], [q]) =$$
$$(\forall\, \underline{q}, \underline{w}', t', s, \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$
$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))\,, \tag{9.19}$$

$$T_{Op}([k]) =$$
$$(\forall\, w \bullet trm_{Op_F}(w, k) \Rightarrow$$
$$(\forall\, \underline{w}, \underline{k} \bullet \underline{w} \in [w] \wedge \underline{k} \in [k] \Rightarrow trm_{Op_F}(\underline{w}, \underline{k}))\,)\,. \tag{9.20}$$

Finally, let

$$K^{\bullet}(([v], [w]), \underline{w}) = \underline{w} \in [w] \wedge HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \,, \tag{9.21}$$

$$H^{\bullet}(([v], [w]), \underline{v}) = \underline{v} \in [v] \wedge (\exists\, t \bullet K(\underline{v}, t)) \wedge KH(\underline{v}, [w]) \wedge$$
$$HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \,, \tag{9.22}$$

$$R^{\bullet}_{Op}(([j], [k]), \underline{k}) = \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \,, \tag{9.23}$$

$$Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) =$$
$$\underline{j} \in [j] \wedge \underline{v} \in [v] \wedge (\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge$$
$$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \,, \tag{9.24}$$

$$V^{\bullet}_{Op}(([p], [q]), \underline{q}) = \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \,, \tag{9.25}$$

$$N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) =$$
$$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$(\exists\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge$$
$$VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \,, \tag{9.26}$$

$$D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) =$$
$$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$(\exists\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge$$
$$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$$
$$HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \,. \tag{9.27}$$

9.3 Preconjointness

A retrenchment from *Ref* to *Conc* and refinement from *Ret* to *Conc*, are said to be *preconjoint* when they satisfy the following. Note that in (9.28) to (9.31), all the ingredients are built out of the given retrenchment and refinement.

$$Init_{\mathrm{F}}(\underline{w}') \Rightarrow (\exists\, v', w' \bullet K^{\bullet}(([v'], [w']), \underline{w}')) \,, \tag{9.28}$$

$$K^{\bullet}(([v], [w]), \underline{w}) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \Rightarrow$$
$$(\exists\, v', w', p, q \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}_{Op}(([p], [q]), \underline{q})) \,, \tag{9.29}$$

$$Init_{\mathrm{T}}(\underline{v}') \Rightarrow (\exists\, v', w' \bullet H^{\bullet}(([v'], [w']), \underline{v}')) \,, \tag{9.30}$$

$$H^{\bullet}(([v], [w]), \underline{v}) \wedge Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge stp_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow$$
$$(\exists\, v', w', p, q \bullet (H^{\bullet}(([v'], [w']), \underline{v}') \wedge$$
$$N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v})) \vee$$
$$D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}))\ . \qquad (9.31)$$

9.4 Proof for Part (1)

We take the retrenchment from *Ref* to *Conc* and the refinement from *Ret* to *Conc*, and build a new, universal system *Univ*, from which we then show there is *both* a retrenchment to *Ret* and a refinement to *Ref*; see Figure 9.1.

9.4.1 The system *Univ*

The operation names set of *Univ* is $\mathsf{Ops}_{\mathrm{U}}$ with elements Op_{U}. State, input and output spaces are $u \in \mathsf{U}$, $i \in \mathsf{I}_{Op_{\mathrm{U}}}$, $o \in \mathsf{O}_{Op_{\mathrm{U}}}$. Initialisation and step predicates are $Init_{\mathrm{U}}$ and $stp_{Op_{\mathrm{U}}}$. These are all constructed from the systems *Ret* and *Ref* as follows. $\mathsf{U} = \mathsf{V}/{\sim_{\mathrm{V}}} \times \mathsf{W}/{\sim_{\mathrm{W}}}$ and $\mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{F}}$. For each Op_{U}, $\mathsf{I}_{Op} = \mathsf{J}_{Op}/{\sim_{\mathrm{J}_{Op}}} \times \mathsf{K}_{Op}/{\sim_{\mathrm{K}_{Op}}}$ and $\mathsf{O}_{Op} = \mathsf{P}_{Op}/{\sim_{\mathrm{P}_{Op}}} \times \mathsf{Q}_{Op}/{\sim_{\mathrm{Q}_{Op}}}$.

Let the initialization predicate be

$$Init_{\mathrm{U}}(u') \;=\; Init_{\mathrm{U}}(([v'], [w'])) =$$
$$(\exists\, \underline{w}' \bullet Init_{\mathrm{F}}(\underline{w}') \wedge K^{\bullet}(([v'], [w']), \underline{w}')) \qquad \text{(a)}$$
$$\vee$$
$$(\exists\, \underline{v}' \bullet Init_{\mathrm{T}}(\underline{v}') \wedge H^{\bullet}(([v'], [w']), \underline{v}'))\ . \qquad \text{(b)}$$
$$(9.32)$$

Let the transitions of *Univ* be

$$stp_{Op_{\mathrm{U}}}(u, i, u', o) \;=\; stp_{Op_{\mathrm{U}}}(([v], [w]), ([j], [k]), ([v'], [w']), ([p], [q])) \;=$$
$$\mathbf{(}\,\exists\, \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^{\bullet}(([v], [w]), \underline{w}) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge$$
$$stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}_{Op}(([p], [q]), \underline{q})\,\mathbf{)} \qquad \text{(a)}$$
$$\vee$$

$$
\begin{aligned}
&\mathbf{(}\ \exists\ \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^{\bullet}(([v], [w]), \underline{v}) \wedge Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
&\quad stp_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge (\ (H^{\bullet}(([v'], [w']), \underline{v}') \wedge \\
&\qquad N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v})) \vee \\
&\quad D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})\ )\ \mathbf{)}\ . \qquad \text{(b)}
\end{aligned}
\tag{9.33}
$$

This completes the definition of *Univ*.

Given the above, the following holds.

$$
\begin{aligned}
&trm_{Op_{\mathrm{U}}}(u, i) \ = \\
&\quad \mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k})\ \mathbf{)} \qquad \text{(a)} \\
&\quad \vee \\
&\quad \mathbf{(}\ \exists\ \underline{v}, \underline{j} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j})\ \mathbf{)} \qquad \text{(b)}
\end{aligned}
\tag{9.34}
$$

Proof. First we show the RHS follows from $trm_{Op_{\mathrm{U}}}(u, i)$.

$$
\begin{aligned}
&trm_{Op_{\mathrm{U}}}(u, i) \\
&\Rightarrow [\text{definition of } trm_{Op}] \\
&(\ \exists\ u', o \bullet stp_{Op_{\mathrm{U}}}(u, i, u', o)\ ) \\
&\Rightarrow [(9.33)] \\
&(\ \exists\ u', o \bullet \\
&\quad \mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \\
&\qquad K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q})\ \mathbf{)} \\
&\quad \vee \\
&\quad \mathbf{(}\ \exists\ \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \\
&\qquad (\ (H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})\ )\ \mathbf{)}\ \mathbf{)} \\
&\Rightarrow [stp_{Op} \Leftrightarrow stp_{Op} \wedge trm_{Op}] \\
&(\ \exists\ u', o \bullet \\
&\quad \mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}) \wedge \\
&\qquad K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q})\ \mathbf{)} \\
&\quad \vee \\
&\quad \mathbf{(}\ \exists\ \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}) \wedge \\
&\qquad (\ (H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})\ )\ \mathbf{)}\ \mathbf{)}
\end{aligned}
$$

$\Rightarrow$ [$(\exists ... K^{\bullet} \wedge R^{\bullet} \wedge stp \wedge trm \wedge K^{\bullet\prime} \wedge V^{\bullet}) \Leftrightarrow (\exists ... K^{\bullet} \wedge R^{\bullet} \wedge stp \wedge trm \wedge K^{\bullet\prime} \wedge V^{\bullet}) \wedge (\exists ... K^{\bullet} \wedge R^{\bullet} \wedge trm)$,

and similarly so for the other disjunct]

$$
\begin{array}{l}
(\exists\, u', o \bullet \\
\quad \mathbf{(} (\exists\, \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge trm_{Op_F}(\underline{w}, \underline{k}) \wedge \\
\qquad K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q})) \wedge (\exists\, \underline{w}, \underline{k} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_F}(\underline{w}, \underline{k})) \mathbf{)} \\
\quad \vee \\
\quad \mathbf{(} (\exists\, \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \\
\qquad (\, (H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})\,)) \wedge \\
\qquad (\exists\, \underline{w}, \underline{k} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge trm_{Op_T}(\underline{v}, \underline{j})) \mathbf{)}\,) \\
\Rightarrow \\
(\exists\, u', o \bullet \\
\quad \mathbf{(} \exists\, \underline{w}, \underline{k} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_F}(\underline{w}, \underline{k}) \mathbf{)} \\
\quad \vee \\
\quad \mathbf{(} \exists\, \underline{w}, \underline{k} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \mathbf{)}\,)
\end{array}
$$

$\Rightarrow$ [expression independent of u' and o]

$$
\begin{array}{l}
\mathbf{(} \exists\, \underline{w}, \underline{k} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_F}(\underline{w}, \underline{k}) \mathbf{)} \\
\vee \\
\mathbf{(} \exists\, \underline{w}, \underline{k} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \mathbf{)}\, .
\end{array}
$$

Now we show that the LHS, $trm_{Op_U}(u, i)$, follows from disjunct (9.34a). $trm_{Op_F}(\underline{w}, \underline{k})$ implies there exist $\underline{w}'$ and $\underline{q}$ such that $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ holds. Then, by (9.29), we have values u' and o such that $K^{\bullet}(u', \underline{w}')$ and $V^{\bullet}_{Op}(o, \underline{q})$ hold. Hence, by (9.33a), $stp_{Op_U}(u, i, u', o)$ holds from which we have $trm_{Op_U}(u, i)$ as required. The proof starting with disjunct (9.34b) is similar. ■

9.4.2 The refinement from *Univ* to *Ref*

We show *Ref* refines *Univ*. We do this by first specifying the component relations for the refinement and then showing that the refinement POs hold.

9.4.2.1 The component relations

The data for the refinement consists of the retrieve relation $K^{\bullet}(u, \underline{w})$, and for each Op, the input relation $R^{\bullet}_{Op}(i, \underline{k})$ and the output relation $V^{\bullet}_{Op}(o, \underline{q})$. $K^{\bullet}$, $R^{\bullet}_{Op}$ and $V^{\bullet}_{Op}$ are given by (9.21), (9.23) and (9.25) respectively.

We also have the input initialisations and output finalisations. For *Ref* let the input initialisation be $InitIn_{Op_F}$ and output finalisation be $FinOut_{Op_F}$. Similarly, for *Univ* we have $InitIn_{Op_U}$ and $FinOut_{Op_U}$. Since *Ref* is the given system which refines both *Univ* and *Xtra*, we use the input and output spaces of its operations to define those of the global world. Let $\mathsf{N}_{Op} = \mathsf{O}_{Op}$ and

$$\mathsf{L}_{Op} = \{l \in \mathsf{K}_{Op} \mid \exists\, j, k \bullet k = l \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k])\} \ . \tag{9.35}$$

Then,

$$InitIn_{Op_F}(l, \underline{k}) = (\, l \sim \underline{k}\,) \ , \tag{9.36}$$

$$FinOut_{Op_F}(\underline{q}, n) = (\, \underline{q} \sim n\,) \ , \tag{9.37}$$

$$InitIn_{Op_U}(l, i) = (\, i = ([j], [k]) \wedge l \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k])\,) \ , \tag{9.38}$$

$$FinOut_{Op_U}(o, n) = (\, o = ([p], [q]) \wedge n \in [q]\,) \ . \tag{9.39}$$

Observe that (9.36) to (9.39) are all total relations. This is easy to see, even for (9.38), which, by (9.35), has for every l a suitable i.

9.4.2.2 The input initialisation PO

We show

$$InitIn_{Op_F}(l, \underline{k}) \Rightarrow (\exists\, i \bullet InitIn_{Op_U}(l, i) \wedge R^{\bullet}_{Op}(i, \underline{k})) \ . \tag{9.40}$$

Proof. Assume $InitIn_{Op_F}(l, \underline{k})$. Then, by (9.36), $l \sim \underline{k}$, and as $l \in \mathsf{L}_{Op}$, by (9.35), we have inputs, j and k say, such that $QR_{Op}([j], [k])$ and $T_{Op}([k])$, with $k = l$. Let $i = ([j], [k])$. Then, as $k \sim \underline{k}$, $InitIn_{Op_U}(l, i)$ and $R^{\bullet}_{Op}(i, \underline{k})$ hold, by (9.38) and (9.23) respectively. ■

9.4.2.3 The initialisation PO

We show

$$Init_{\mathrm{F}}(\underline{w}') \Rightarrow (\exists\, u' \bullet Init_{\mathrm{U}}(u') \wedge K^{\bullet}(u', \underline{w}')) \,. \tag{9.41}$$

Proof. Let $\underline{w}'$ be an initial value. By (9.28) we have values, v' and w' say, for which $K^{\bullet}(([v'], [w']), \underline{w}')$ holds. Let $u' = ([v'], [w'])$. Then, since $Init_{\mathrm{F}}(\underline{w}')$ holds, $Init_{\mathrm{U}}(u')$ holds by (9.32). Thus the consequent of (9.41) holds as required. ■

9.4.2.4 The applicability PO

We show

$$K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_{\mathrm{U}}}(u, i) \;\Rightarrow\; trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}) \,. \tag{9.42}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From $K^{\bullet}$, by (9.21), $\underline{w} \in [w]$. From $R^{\bullet}_{Op}$, by (9.23), $\underline{k} \in [k]$ and $T_{Op}([k])$. From $trm_{Op_{\mathrm{U}}}(u, i)$, either (i), disjunct (9.34a), or (ii), disjunct (9.34b) holds. We consider each case in turn.

• Case (i). From (9.34a) we have $trm_{Op_{\mathrm{F}}}(\underline{\underline{w}}, \underline{\underline{k}})$, with $\underline{\underline{w}} \in [w]$ and $\underline{\underline{k}} \in [k]$. Hence, $\underline{\underline{w}} \sim w \sim \underline{w}$ and $\underline{\underline{k}} \sim k \sim \underline{k}$. Thus $T_{Op}([\underline{\underline{k}}])$ holds and therefore, by (9.20), $trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k})$ holds as required.

• Case (ii). From (9.34b) we have $H^{\bullet}(u, \underline{\underline{v}}) \wedge Q^{\bullet}_{Op}(i, \underline{\underline{j}}, u, \underline{\underline{v}})$ and $trm_{Op_{\mathrm{T}}}(\underline{\underline{v}}, \underline{\underline{j}})$, with $\underline{\underline{v}} \in [v]$ and $\underline{\underline{j}} \in [j]$. From $Q^{\bullet}_{Op}$, by (9.24), we know $RQ_{Op}(\underline{\underline{j}}, \underline{\underline{v}}, [k], [w])$ holds and furthermore, we can derive t and h such that $R_{Op}(\underline{\underline{j}}, h)$ and $K(\underline{\underline{v}}, t)$ hold. Therefore, by (9.14), we obtain values, $\underline{\underline{k}}$ and $\underline{\underline{w}}$ say, such that $\underline{\underline{k}} \in [k]$, $\underline{\underline{w}} \in [w]$, $H(\underline{\underline{w}}, t)$ and $Q_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$. We can now use the termination PO for the retrenchment from *Ref* to *Conc*,

$$H(\underline{\underline{w}}, t) \wedge Q_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t) \;\Rightarrow\; trm_{Op_{\mathrm{F}}}(\underline{\underline{w}}, \underline{\underline{k}}) \wedge trm_{Op_{\mathrm{C}}}(t, h) \tag{9.43}$$

to derive $trm_{Op_{\mathrm{F}}}(\underline{\underline{w}}, \underline{\underline{k}})$. Finally, we argue as for case (i) to obtain $trm_{Op_{\mathrm{F}}}(\underline{w}, \underline{k})$. ■

9.4.2.5 The correctness PO

We show

$$K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge trm_{Op_{\mathrm{U}}}(u, i) \wedge stp_{Op_{\mathrm{F}}}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \Rightarrow$$
$$(\exists\, u', o \bullet stp_{Op_{\mathrm{U}}}(u, i, u', o) \wedge K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q})) \ . \qquad (9.44)$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From (9.29) we know there are values, which we fix as v', w', p and q, such that $K^{\bullet}(([v'], [w']), \underline{w}')$ and $V^{\bullet}_{Op}(([p], [q]), \underline{q})$ both hold. Let $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then, by (9.33a), $stp_{Op_{\mathrm{U}}}(u, i, u', o)$ holds. Hence the consequent of (9.44) holds and we are done. ■

9.4.2.6 The output finalisation PO

We show

$$V^{\bullet}_{Op}(o, \underline{q}) \wedge FinOut_{Op_{\mathrm{F}}}(\underline{q}, n) \ \Rightarrow\ FinOut_{Op_{\mathrm{U}}}(o, n) \ . \qquad (9.45)$$

Proof. Assume the antecedents with $o = ([p], [q])$. From $V^{\bullet}_{Op}(o, \underline{q})$, by (9.25), $\underline{q} \in [q]$. From $FinOut_{Op_{\mathrm{F}}}(\underline{q}, n)$, by (9.37), $\underline{q} \sim n$. Therefore, $n \in [q]$, from which $FinOut_{Op_{\mathrm{U}}}(o, n)$ follows, by (9.39).

9.4.3 The retrenchment from *Univ* to *Ret*

We show *Ret* retrenches *Univ*. We do this by first specifying the component relations of the retrenchment and then showing that the retrenchment POs hold.

9.4.3.1 The component relations

The data for the retrenchment consists of the retrieve relation $H^{\bullet}$, and for each Op, the within relation $Q^{\bullet}_{Op}$, the output relation $N^{\bullet}_{Op}$ and the concedes relation $D^{\bullet}_{Op}$. These are given by (9.22), (9.24), (9.26) and (9.27) respectively.

9.4.3.2 The initialisation PO

We show

$$Init_{\mathrm{T}}(\underline{v}') \Rightarrow (\exists\, u' \bullet Init_{\mathrm{U}}(u') \wedge H^{\bullet}(u', \underline{v}')) \ . \qquad (9.46)$$

Proof. Assume the antecedent. By (9.30) we have values, v' and w' say, for which $H^{\bullet}(([v'], [w']), \underline{v}')$ holds. Let $u' = ([v'], [w'])$. Then, since $Init_{\mathrm{T}}(\underline{v}')$ holds, $Init_{\mathrm{U}}(u')$ holds by (9.32). Hence the consequent of (9.46) holds as required. ■

9.4.3.3 The termination PO

We show

$$H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \;\Rightarrow\; trm_{Op_{\mathrm{U}}}(u, i) \wedge trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}) \tag{9.47}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From $Q^{\bullet}_{Op}$, by (9.24) and (9.14), $trm_{Op_{\mathrm{T}}}(\underline{v}, \underline{j})$ holds. What is more, given the latter, $trm_{Op_{\mathrm{U}}}(u, i)$ follows by (9.34b) . We are done. ■

9.4.3.4 The operation PO

We show

$$\begin{aligned} & H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_{\mathrm{T}}}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow \\ & \quad (\exists\, u', o \bullet stp_{Op_{\mathrm{U}}}(u, i, u', o) \wedge \\ & \qquad ((H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) \,. \end{aligned} \tag{9.48}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From (9.31) we know there are values, which we fix as v', w', p and q, such that $(H^{\bullet}(([v'], [w']), \underline{v}') \wedge N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v})) \vee D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds. Let $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then (9.33b) and thus $stp_{Op_{\mathrm{U}}}(u, i, u', o)$ holds. Hence (9.48) holds. Done. ■

9.4.4 The retrenchment from *Univ* to *Conc*

The next step is to show that the composition of the *Univ* to *Ret* retrenchment with the *Ret* to *Conc* refinement on the one hand, and the *Univ* to *Ref* refinement with the *Ref* to *Conc* retrenchment on the other, yield the *same* retrenchment from *Univ* to *Conc*. To do this we define the relations of the *Univ* to *Conc* retrenchment in terms of the *Univ* to *Ret* and *Ret* to *Conc* relations, and also in terms of the *Univ* to *Ref* and *Ref* to *Conc* ones. We then

show that two definitions are equal. Finally, we demonstrate that the retrenchment POs hold.

9.4.4.1 The component relations

Let the retrieve, within, output and concedes relations of the retrenchment from *Univ* to *Conc* be given by G, P_{Op}, O_{Op} and C_{Op} respectively. Then Figure 9.1 commutes in the following sense. Firstly,

$$G(([v], [w]), t) \;=\; H^{\bullet}(([v], [w]), \underline{v})\fatsemi K(\underline{v}, t) \;=\; K^{\bullet}(([v], [w]), \underline{w})\fatsemi H(\underline{w}, t)\ . \tag{9.49}$$

We write this for short as

$$G = H^{\bullet}\fatsemi K = K^{\bullet}\fatsemi H\ .$$

Secondly,

$$\begin{aligned}
&P_{Op}(([j], [k]), h, ([v], [w]), t)\\
&= \mathbf{(}Q^{\bullet}{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v})\mathbf{)}\fatsemi\mathbf{(}R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)}\\
&= \mathbf{(}R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})\mathbf{)}\fatsemi\mathbf{(}Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\mathbf{)}\ ,
\end{aligned} \tag{9.50}$$

or more briefly

$$P_{Op} = (Q^{\bullet}{}_{Op} \wedge H^{\bullet})\fatsemi(R_{Op} \wedge K) = (R^{\bullet}{}_{Op} \wedge K^{\bullet})\fatsemi(Q_{Op} \wedge H)\ .$$

Thirdly,

$$\begin{aligned}
&O_{Op}(([p], [q]), s; ([v'], [w']), t', ([j], [k]), h, ([v], [w]), t)\\
&= \mathbf{(}N^{\bullet}{}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v'}, ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge\\
&\quad H^{\bullet}(([v'], [w']), \underline{v'}) \wedge Q^{\bullet}{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v})\mathbf{)}\fatsemi\\
&\quad \mathbf{(}V_{Op}(\underline{p}, s) \wedge K(\underline{v'}, t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)}\\
&= \mathbf{(}V^{\bullet}{}_{Op}(([p], [q]), \underline{q}) \wedge K^{\bullet}(([v'], [w']), \underline{w'}) \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})\mathbf{)}\fatsemi\\
&\quad (N_{Op}(\underline{q}, s; \underline{w'}, t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w'}, t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))
\end{aligned} \tag{9.51}$$

or

$$O_{Op} = (N^{\bullet}_{Op} \wedge H^{\bullet\prime} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet}) ⨾ (V_{Op} \wedge K' \wedge R_{Op} \wedge K)$$
$$= (V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet}) ⨾ (N_{Op} \wedge H' \wedge Q_{Op} \wedge H) \ .$$

Lastly,

$$\begin{aligned}
& C_{Op}(([v'], [w']), t', ([p], [q]), s; ([j], [k]), h, ([v], [w]), t) \\
= \ & (D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
& \quad Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v})) ⨾ \\
& (K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \\
= \ & (K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}_{Op}(([p], [q]), \underline{q}) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})) ⨾ \\
& (D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \ ,
\end{aligned} \tag{9.52}$$

or

$$C_{Op} = (D^{\bullet}_{Op} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet}) ⨾ (K' \wedge V_{Op} \wedge R_{Op} \wedge K)$$
$$= (K^{\bullet\prime} \wedge V^{\bullet}_{Op} \wedge R^{\bullet}_{Op} \wedge K^{\bullet}) ⨾ (D_{Op} \wedge Q_{Op} \wedge H) \ .$$

The proofs showing that the above compositions hold are given in Appendix B.

9.4.4.2 The initialisation PO

We show

$$Init_{\mathrm{C}}(t') \Rightarrow (\exists\, u' \bullet Init_{\mathrm{U}}(u') \wedge G(u', t')) \ , \tag{9.53}$$

Proof. Assume $Init_{\mathrm{C}}(t')$. Then the Init PO for the refinement from *Ret* to *Conc*,

$$Init_{\mathrm{C}}(t') \ \Rightarrow \ (\exists\, \underline{v}' \bullet Init_{\mathrm{T}}(\underline{v}') \wedge K(\underline{v}', t')) \ , \tag{9.54}$$

implies the existence of a state, let it be $\underline{v}'$, such that $Init_{\mathrm{T}}(\underline{v}')$ and $K(\underline{v}', t')$ are true. From $Init_{\mathrm{T}}(\underline{v}')$ we can assert, by (9.46), u' for which $Init_{\mathrm{U}}(u')$ and $H^{\bullet}(u', \underline{v}')$ hold. All we need now is $G(u', t')$, and this follows from $H^{\bullet}(u', \underline{v}') ⨾ K(\underline{v}', t')$. Done. ■

9.4.4.3 The termination PO

We show

$$G(u, t) \wedge P_{Op}(i, h, u, t) \;\Rightarrow\; trm_{Op_U}(u, i) \wedge trm_{Op_C}(t, h)\ , \tag{9.55}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. Now $P_{Op}(i, h, u, t) = (Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v}))\fatsemi(R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$, by (9.50). Thus we have $Q^{\bullet}_{Op}$, $H^{\bullet}$, R_{Op} and K for values which we fix as $\underline{j}$ and $\underline{v}$. From $Q^{\bullet}_{Op}$ and $H^{\bullet}$, by PO (9.47), we get $trm_{Op_U}(u, i)$, and also $trm_{Op_T}(\underline{v}, \underline{j})$, from which, by the App PO for the refinement from *Ret* to *Conc*,

$$K(\underline{v}, t) \wedge R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \;\Rightarrow\; trm_{Op_C}(t, h)\ . \tag{9.56}$$

we get $trm_{Op_C}(t, h)$. We are done. ■

9.4.4.4 The operation PO

We show

$$\begin{aligned} &G(u, t) \wedge P_{Op}(i, h, u, t) \wedge stp_{Op_C}(t, h, t', s) \Rightarrow \\ &\quad (\exists\, u', o \bullet stp_{Op_U}(u, i, u', o) \wedge \\ &\qquad ((G(u', t') \wedge O_{Op}(o, s; u', t', i, h, u, t)) \vee C_{Op}(u', t', o, s; i, h, u, t)))\ . \end{aligned} \tag{9.57}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. Now $P_{Op}(i, h, u, t) = (Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v}))\fatsemi(R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$, by (9.50). Thus we have $Q^{\bullet}_{Op}$, $H^{\bullet}$, R_{Op} and K for values which we fix as $\underline{j}$ and $\underline{v}$. From $Q^{\bullet}_{Op}$ and $H^{\bullet}$, by PO (9.47), $trm_{Op_T}(\underline{v}, \underline{j})$ holds. Thus we have the antecedents of the Op PO for the refinement from *Ret* to *Conc*,

$$\begin{aligned} &K(\underline{v}, t) \wedge R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge stp_{Op_C}(t, h, t', s) \;\Rightarrow \\ &\qquad (\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s))\ . \end{aligned} \tag{9.58}$$

Hence we have values, $\underline{v}'$ and $\underline{p}$ say, such that $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K(\underline{v}', t')$ and $V_{Op}(\underline{p}, s)$ hold. So stp_{Op_T}, $H^{\bullet}$ and $Q^{\bullet}_{Op}$ are true. These are the antecedents of PO (9.48). Therefore we have values, u' and o say, such that $stp_{Op_U}(u, i, u', o)$, which we require, and $(H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ hold.

It remains to show $(G' \wedge O_{Op}) \vee C_{Op}$. This follows from $(H^{\bullet\prime} \wedge N^{\bullet}_{Op}) \vee D^{\bullet}_{Op}$. Assume $H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})$. Then $H^{\bullet}(u', \underline{v}')\fatsemi K(\underline{v}', t')$ gives $G(u', t')$, by (9.49), and $(N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u', \underline{v}') \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v}))\fatsemi(V_{Op}(\underline{p}, s) \wedge K(\underline{v}',$

$t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$ gives $O_{Op}(o, s; u', t', i, h, u, t)$, by (9.51). Alternatively assume $D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. Then $(D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v}))\fatsemi(K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$ gives $C_{Op}(u', t', o, s; i, h, u, t)$, by (9.52). Hence $(G' \wedge O_{Op}) \vee C_{Op}$ holds and we are done. ■

9.4.5 Properties of *Univ*

We state properties (U1) to (U7) of *Univ*.

$$K^{\bullet}(u', w') \wedge \underline{w}' \in [w'] \Rightarrow K^{\bullet}(u', \underline{w}') \tag{U1}$$

$$R^{\bullet}_{Op}(i, k) \wedge \underline{k} \in [k] \Rightarrow R^{\bullet}_{Op}(i, \underline{k}) \tag{U2}$$

$$V^{\bullet}_{Op}(o, q) \wedge \underline{q} \in [q] \Rightarrow V^{\bullet}_{Op}(o, \underline{q}) \tag{U3}$$

$$K^{\bullet}(u', w') \Rightarrow (H^{\bullet}(u', v') \Leftrightarrow H^{\bullet}(([v'], [w']), v')) \tag{U4}$$

$$\begin{aligned} & R^{\bullet}_{Op}(i, k) \wedge K^{\bullet}(u, w) \Rightarrow \\ & \quad \mathbf{(} \forall j, v \bullet Q^{\bullet}_{Op}(i, j, u, v) \wedge H^{\bullet}(u, v) \Leftrightarrow \\ & \qquad Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{U5}$$

$$\begin{aligned} & V^{\bullet}_{Op}(o, q) \wedge K^{\bullet}(u', w') \wedge R^{\bullet}_{Op}(i, k) \wedge K^{\bullet}(u, w) \Rightarrow \\ & \quad \mathbf{(} \forall p, v', j, v \bullet N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \wedge H^{\bullet}(u', v') \wedge \\ & \qquad Q^{\bullet}_{Op}(i, j, u, v) \wedge H^{\bullet}(u, v) \Leftrightarrow \\ & \qquad\quad N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v) \wedge \\ & \qquad\quad H^{\bullet}(([v'], [w']), v') \wedge Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{U6}$$

$$\begin{aligned} & K^{\bullet}(u', w') \wedge V^{\bullet}_{Op}(o, q) \wedge R^{\bullet}_{Op}(i, k) \wedge K^{\bullet}(u, w) \Rightarrow \\ & \quad \mathbf{(} \forall v', p, j, v \bullet D^{\bullet}_{Op}(u', v', o, p; i, j, u, v) \wedge Q^{\bullet}_{Op}(i, j, u, v) \wedge H^{\bullet}(u, v) \Leftrightarrow \\ & \qquad D^{\bullet}_{Op}(([v'], [w']), v', ([p], [q]), p; ([j], [k]), j, ([v], [w]), v) \wedge \\ & \qquad Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{U7}$$

In the following we show that the above properties are true.

♦ (U1): $K^{\bullet}(u', w') \wedge \underline{w}' \in [w'] \Rightarrow K^{\bullet}(u', \underline{w}')$

Proof. Assume the antecedents with $u' = ([\underline{\underline{v'}}], [\underline{\underline{w'}}])$. From $K^{\bullet}(u', w')$, by (9.21), $w' \sim \underline{\underline{w'}}$. From $\underline{w'} \in [w']$, $\underline{w'} \sim w'$. Hence $\underline{w'} \sim \underline{\underline{w'}}$. Therefore because $K^{\bullet}(u', w')$ holds, then so does $K^{\bullet}(u', \underline{w'})$. ■

♦ (U2) and (U3).

Proof. Similar to (U1). ■

♦ (U4): $K^{\bullet}(u', w') \Rightarrow (H^{\bullet}(u', v') \Leftrightarrow H^{\bullet}(([v'], [w']), v'))$

Proof. First we assume $K^{\bullet}(u', w')$ and $H^{\bullet}(u', v')$, and prove $H^{\bullet}(([v'], [w']), v')$. Let $u' = ([\underline{\underline{v'}}], [\underline{\underline{w'}}])$. From $K^{\bullet}(u', w')$, by (9.21), $w' \sim \underline{\underline{w'}}$. From $H^{\bullet}(u', v')$, by (9.22), $v' \sim \underline{\underline{v'}}$. Therefore because $H^{\bullet}(([\underline{\underline{v'}}], [\underline{\underline{w'}}]), v')$ holds, then so does $H^{\bullet}(([v'], [w']), v')$.

Now we assume $K^{\bullet}(u', w')$ and $H^{\bullet}(([v'], [w']), v')$, and prove $H^{\bullet}(u', v')$. Let $u' = ([\underline{\underline{v'}}], [\underline{\underline{w'}}])$. From $K^{\bullet}(u', w')$, by (9.21), we have $w' \sim \underline{\underline{w'}}$ and $HK([\underline{\underline{v'}}], [\underline{\underline{w'}}])$. Therefore $HK([\underline{\underline{v'}}], [w'])$ holds. From $H^{\bullet}(([v'], [w']), v')$, by (9.22), we can derive t', for which $K(v', t')$ is true. Then as $H^{\bullet}(([v'], [w']), v') ⨾ K(v', t')$ holds, by (9.49), there must be a value, $\underline{w'}$ say, for which $K^{\bullet}(([v'], [w']), \underline{w'}) ⨾ H(\underline{w'}, t')$ holds, with, by (9.21), $\underline{w'} \in [w']$. As a result, we have $HK([\underline{\underline{v'}}], [w'])$, $H(\underline{w'}, t')$ and $\underline{w'} \in [w']$. So, by (9.11), there must be a value, $\underline{v'}$ say, such that $K(\underline{v'}, t')$ holds, with $\underline{v'} \in [\underline{\underline{v'}}]$. Hence, $K(v', t')$, $K(\underline{v'}, t')$ and $H(\underline{w'}, t')$ all hold. Therefore, by (9.4), $v' \sim \underline{v'}$. But $\underline{v'} \sim \underline{\underline{v'}}$. So $v' \sim \underline{\underline{v'}}$, and earlier we showed $w' \sim \underline{\underline{w'}}$. Therefore because $H^{\bullet}(([v'], [w']), v')$ holds, $H^{\bullet}(([\underline{\underline{v'}}], [\underline{\underline{w'}}]), v')$ holds, as required. ■

♦ (U5).

Proof. Similar to (U4) and (U6). ■

♦ (U6):

$$
\begin{aligned}
& V^{\bullet}_{Op}(o, q) \wedge K^{\bullet}(u', w') \wedge R^{\bullet}_{Op}(i, k) \wedge K^{\bullet}(u, w) \Rightarrow \\
& \quad \big(\forall\, p, v', j, v \bullet N^{\bullet}_{Op}(o, p; u', v', i, j, u, v) \wedge H^{\bullet}(u', v') \wedge Q^{\bullet}_{Op}(i, j, u, v) \wedge H^{\bullet}(u, v) \Leftrightarrow \\
& \qquad N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v) \wedge \\
& \qquad H^{\bullet}(([v'], [w']), v') \wedge Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \big)
\end{aligned}
$$

Proof. First we assume $V^{\bullet}_{Op}(o, q)$, $K^{\bullet}(u', w')$, $R^{\bullet}_{Op}(i, k)$, $K^{\bullet}(u, w)$, $N^{\bullet}_{Op}(o, p; u', v', i, j, u, v)$, $H^{\bullet}(u', v')$, $Q^{\bullet}_{Op}(i, j, u, v)$ and $H^{\bullet}(u, v)$, and prove $N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v)$, $H^{\bullet}(([v'], [w']), v')$, $Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v)$ and $H^{\bullet}(([v], [w]), v)$.

Let $o = ([\underline{p}], [\underline{q}])$, $u' = ([\underline{v}'], [\underline{w}'])$, $i = ([\underline{j}], [\underline{k}])$ and $u = ([\underline{v}], [\underline{w}])$. From the assumed $N^{\bullet}_{Op}$ and (9.26) we have $p \sim \underline{p}$, $v' \sim \underline{v}'$, $j \sim \underline{j}$ and $v \sim \underline{v}$. Furthermore $V^{\bullet}_{Op}$, $K^{\bullet\prime}$, $R^{\bullet}_{Op}$, $K^{\bullet}$, (9.21), (9.23) and (9.25) give $w' \sim \underline{w}'$, $q \sim \underline{q}$, $k \sim \underline{k}$ and $w \sim \underline{w}$. Hence, since $N^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), p; ([\underline{v}'], [\underline{w}']), v', ([\underline{j}], [\underline{k}]), j, ([\underline{v}], [\underline{w}]), v)$, $H^{\bullet}(([\underline{v}'], [\underline{w}']), v')$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), j, ([\underline{v}], [\underline{w}]), v)$ and $H^{\bullet}(([\underline{v}], [\underline{w}]), v)$ hold, $N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v)$, $H^{\bullet}(([v'], [w']), v')$, $Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v)$ and $H^{\bullet}(([v], [w]), v)$ follow from the established equivalences.

Now we assume $V^{\bullet}_{Op}(o, q)$, $K^{\bullet}(u', w')$, $R^{\bullet}_{Op}(i, k)$, $K^{\bullet}(u, w)$, $N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v)$, $H^{\bullet}(([v'], [w']), v')$, $Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v)$ and $H^{\bullet}(([v], [w]), v)$, and prove $N^{\bullet}_{Op}(o, p; u', v', i, j, u, v)$, $H^{\bullet}(u', v')$, $Q^{\bullet}_{Op}(i, j, u, v)$ and $H^{\bullet}(u, v)$.

We proceed as follows. Let $o = ([\underline{p}], [\underline{q}])$, $u' = ([\underline{v}'], [\underline{w}'])$, $i = ([\underline{j}], [\underline{k}])$ and $u = ([\underline{v}], [\underline{w}])$. By (9.26), the given $N^{\bullet}_{Op}$ lets us assert values s, t', h and t, such that $V_{Op}(p, s)$, $K(v', t')$, $R_{Op}(j, h)$ and $K(v, t)$ are true. Then as $(N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v'], [w']), v') \wedge Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v))$;$(V_{Op}(p, s) \wedge K(v', t') \wedge R_{Op}(j, h) \wedge K(v, t))$ holds, by (9.51), there must be values, $\underline{q}$, $\underline{w}'$, $\underline{k}$ and $\underline{w}$ say, such that $(V^{\bullet}_{Op}(([p], [q]), \underline{q}) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}))$;$(N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$ holds. Hence, by (9.21), (9.23) and (9.25), $\underline{q} \in [q]$, $\underline{w}' \in [w']$, $\underline{k} \in [k]$ and $\underline{w} \in [w]$.

Now take $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), q)$. By (9.25) we get $q \sim \underline{q}$ and $NV_{Op}([\underline{p}], [\underline{q}])$, from which $NV_{Op}([\underline{p}], [q])$ follows. Since we also have $\underline{q} \in [q]$, $N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t)$, $H(\underline{w}', t')$, $Q_{Op}(\underline{k}, h, \underline{w}, t)$, $H(\underline{w}, t)$, $K^{\bullet}(([v'], [w']), \underline{w}')$, $R^{\bullet}_{Op}(([j], [k]), \underline{k})$ and $K^{\bullet}(([v], [w]), \underline{w})$, by (9.17), we derive $\underline{p}$ for which $V_{Op}(\underline{p}, s)$ holds, with $\underline{p} \sim \underline{p}$. Now, $V_{Op}(p, s)$, $V_{Op}(\underline{p}, s)$ and $N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t)$ all hold. So by (9.8), $p \sim \underline{p}$, and as $\underline{p} \sim \underline{p}$, then $p \sim \underline{p}$.

Next take $K^{\bullet}(([\underline{v}'], [\underline{w}']), w')$. From this, by (9.21), we get $w' \sim \underline{w}'$ and also $HK([\underline{v}'], [\underline{w}'])$, from which $HK([\underline{v}'], [w'])$ follows. Therefore by (9.11), $H(\underline{w}', t')$, $\underline{w}' \in [w']$ and $HK([\underline{v}'], [w'])$ give $K(\underline{v}', t')$ with $\underline{v}' \sim \underline{v}'$, for chosen value $\underline{v}'$. So we have $K(v', t')$, $K(\underline{v}', t')$ and $H(\underline{w}', t')$. Hence by (9.4) $v' \sim \underline{v}'$. But as $\underline{v}' \sim \underline{v}'$ then $v' \sim \underline{v}'$.

Similarly, $R^{\bullet}_{Op}(([\underline{j}], [\underline{\underline{k}}]), k)$ and (9.23) gives $k \sim \underline{\underline{k}}$ and thus $QR_{Op}([\underline{j}], [k])$. This, together with $\underline{k} \in [k]$, $Q_{Op}(\underline{k}, h, \underline{w}, t)$, $H(\underline{w}, t)$ and $K^{\bullet}(([v], [w]), \underline{w})$ then give $R_{Op}(\underline{j}, h)$ with $\underline{j} \sim \underline{j}$, by (9.15). Therefore, because $R_{Op}(j, h)$, $R_{Op}(\underline{j}, h)$ and $Q_{Op}(\underline{k}, h, \underline{w}, t)$ hold, from (9.6), we get $j \sim \underline{j}$, and as $\underline{j} \sim \underline{j}$, then $j \sim \underline{j}$.

Last, $K^{\bullet}(([\underline{v}], [\underline{\underline{w}}]), w)$ and (9.21) gives $w \sim \underline{\underline{w}}$ and thus $HK([\underline{v}], [w])$. Therefore, by (9.11), $H(\underline{w}, t)$, $\underline{w} \in [w]$ and $HK([\underline{v}], [w])$ give $K(\underline{v}, t)$ with $\underline{v} \sim \underline{v}$, for chosen value $\underline{v}$. So we have $K(v, t)$, $K(\underline{v}, t)$ and $H(\underline{w}, t)$. Hence, by (9.4), $v \sim \underline{v}$. But $\underline{v} \sim \underline{\underline{v}}$, so $v \sim \underline{\underline{v}}$.

So altogether we have $p \sim \underline{\underline{p}}$, $q \sim \underline{\underline{q}}$, $v' \sim \underline{\underline{v}}'$, $w' \sim \underline{\underline{w}}'$, $j \sim \underline{j}$, $k \sim \underline{\underline{k}}$, $v \sim \underline{\underline{v}}$ and $w \sim \underline{\underline{w}}$. Hence, because $N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v)$, $H^{\bullet}(([v'], [w']), v')$, $Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v)$ and $H^{\bullet}(([v], [w]), v)$ hold, then $N^{\bullet}_{Op}(([\underline{\underline{p}}], [\underline{\underline{q}}]), p; ([\underline{\underline{v}}'], [\underline{\underline{w}}']), v', ([\underline{j}], [\underline{\underline{k}}]), j, ([\underline{\underline{v}}], [\underline{\underline{w}}]), v)$, $H^{\bullet}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), v')$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{\underline{k}}]), j, ([\underline{\underline{v}}], [\underline{\underline{w}}]), v)$ and $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), v)$ must also hold, as required. ■

♦ (U7).

Proof. Similar to (U6). ■

9.5 Proof for Part (2)

The systems which complete the square must belong to a class defined by the list of properties (X1) to (X7) below. To prove the second part of Theorem 9.1 we show that for *any* system *Xtra* in the class, there is a refinement from *Xtra* to *Univ*. We proceed as follows. In Section 9.5.1 we define the elements of *Xtra* and list properties (X1) to (X7). In Section 9.5.2 we specify the component relations of the refinement and show that the relevant POs hold. Finally, in Section 9.5.3, we prove the inclusions stated in part (2).

9.5.1 The system *Xtra*

The operation names set of *Xtra* is $\mathsf{Ops}_{\mathrm{X}}$ with elements Op_{X} and $\mathsf{Ops}_{\mathrm{X}} = \mathsf{Ops}_{\mathrm{U}}$. State, input and output spaces are $u\tilde{} \in \mathsf{U}\tilde{}$, $i\tilde{} \in \mathsf{I}\tilde{}_{Op_{\mathrm{X}}}$, $o\tilde{} \in \mathsf{O}\tilde{}_{Op_{\mathrm{X}}}$. Initialisation and step predicates are $Init_{\mathrm{X}}$ and $stp_{Op_{\mathrm{X}}}$.

Let the retrenchment from *Xtra* to *Ret* have the retrieve relation $H\tilde{}$, and for each *Op*, the within relation $Q\tilde{}_{Op}$, output relation $N\tilde{}_{Op}$, and concedes relation $D\tilde{}_{Op}$. Let the refine-

ment from *Xtra* to *Ref* have retrieve relation $K\tilde{}$, and for each *Op*, the input relation $R\tilde{}_{Op}$, the output relation $V\tilde{}_{Op}$, the input initialisation $InitIn_{Op_X}$ and the output finalisation $FinOut_{Op_X}$. Let $InitIn_{Op_X}$ and $FinOut_{Op_X}$ be total.

Finally, let properties (X1) to (X7) below, hold for *Xtra*.

$$K\tilde{}(u\tilde{}', w') \wedge \underline{w}' \in [w'] \Rightarrow K\tilde{}(u\tilde{}', \underline{w}') \tag{X1}$$

$$R\tilde{}_{Op}(i\tilde{}, k) \wedge \underline{k} \in [k] \Rightarrow R\tilde{}_{Op}(i\tilde{}, \underline{k}) \tag{X2}$$

$$V\tilde{}_{Op}(o\tilde{}, q) \wedge \underline{q} \in [q] \Rightarrow V\tilde{}_{Op}(o\tilde{}, \underline{q}) \tag{X3}$$

$$K\tilde{}(u\tilde{}', w') \Rightarrow (H\tilde{}(u\tilde{}', v') \Leftrightarrow H^{\bullet}(([v'], [w']), v')) \tag{X4}$$

$$\begin{aligned} & R\tilde{}_{Op}(i\tilde{}, k) \wedge K\tilde{}(u\tilde{}, w) \Rightarrow \\ & \quad \mathbf{(} \forall j, v \bullet Q\tilde{}_{Op}(i\tilde{}, j, u\tilde{}, v) \wedge H\tilde{}(u\tilde{}, v) \Leftrightarrow \\ & \qquad Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{X5}$$

$$\begin{aligned} & V\tilde{}_{Op}(o\tilde{}, q) \wedge K\tilde{}(u\tilde{}', w') \wedge R\tilde{}_{Op}(i\tilde{}, k) \wedge K\tilde{}(u\tilde{}, w) \Rightarrow \\ & \quad \mathbf{(} \forall p, v', j, v \bullet N\tilde{}_{Op}(o\tilde{}, p; u\tilde{}', v', i\tilde{}, j, u\tilde{}, v) \wedge H\tilde{}(u\tilde{}', v') \wedge \\ & \qquad Q\tilde{}_{Op}(i\tilde{}, j, u\tilde{}, v) \wedge H\tilde{}(u\tilde{}, v) \Leftrightarrow \\ & \qquad\quad N^{\bullet}_{Op}(([p], [q]), p; ([v'], [w']), v', ([j], [k]), j, ([v], [w]), v) \wedge \\ & \qquad\quad H^{\bullet}(([v'], [w']), v') \wedge Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{X6}$$

$$\begin{aligned} & K\tilde{}(u\tilde{}', w') \wedge V\tilde{}_{Op}(o\tilde{}, q) \wedge R\tilde{}_{Op}(i\tilde{}, k) \wedge K\tilde{}(u\tilde{}, w) \Rightarrow \\ & \quad \mathbf{(} \forall v', p, j, v \bullet D\tilde{}_{Op}(u\tilde{}', v', o\tilde{}, p; i\tilde{}, j, u\tilde{}, v) \wedge Q\tilde{}_{Op}(i\tilde{}, j, u\tilde{}, v) \wedge H\tilde{}(u\tilde{}, v) \Leftrightarrow \\ & \qquad D^{\bullet}_{Op}(([v'], [w']), v', ([p], [q]), p; ([j], [k]), j, ([v], [w]), v) \wedge \\ & \qquad Q^{\bullet}_{Op}(([j], [k]), j, ([v], [w]), v) \wedge H^{\bullet}(([v], [w]), v) \mathbf{)} \end{aligned} \tag{X7}$$

Notice properties (U1) to (U7) are instances of (X1) to (X7) respectively, when $\mathsf{U}\tilde{} = \mathsf{U}$, $\mathsf{I}\tilde{} = \mathsf{I}$ and $\mathsf{O}\tilde{} = \mathsf{O}$. Hence *Univ* is a member of the class defined by properties (X1) to (X7).

9.5.2 The refinement from *Xtra* to *Univ*

To show that *Univ* refines *Xtra*, we first define the relations for this refinement and then show that the appropriate POs hold.

9.5.2.1 The component relations

We define the retrieve relation K°, and for each Op, the input relation R°_{Op} and output relation V°_{Op} for the refinement from *Xtra* to *Univ*.

$$
\begin{aligned}
&K^\circ(\tilde{u}, u) \;=\; K^\circ(\tilde{u}, ([v], [w])) \;= \\
&\quad HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \wedge \\
&\quad (\forall\, \underline{w} \bullet \underline{w} \in [w] \Rightarrow \tilde{K}(\tilde{u}, \underline{w}))\ \wedge\ (\forall\, \underline{v} \bullet H^\bullet(([v], [w]), \underline{v}) \Rightarrow \tilde{H}(\tilde{u}, \underline{v}))
\end{aligned}
\tag{9.59}
$$

$$
\begin{aligned}
&R^\circ_{Op}(\tilde{i}, i) \;=\; R^\circ_{Op}(\tilde{i}, ([j], [k])) \;= \\
&\quad QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \\
&\quad (\forall\, \underline{k} \bullet \underline{k} \in [k] \Rightarrow \tilde{R}_{Op}(\tilde{i}, \underline{k}))\ \wedge \\
&\quad (\forall\, \underline{j}, u, \underline{v}, \tilde{u} \bullet Q^\bullet_{Op}(([j], [k]), \underline{j}, u, \underline{v}) \wedge H^\bullet(u, \underline{v}) \wedge K^\circ(\tilde{u}, u) \Rightarrow \\
&\qquad \tilde{Q}_{Op}(\tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \tilde{H}(\tilde{u}, \underline{v}))\,,
\end{aligned}
\tag{9.60}
$$

$$
\begin{aligned}
&V^\circ_{Op}(\tilde{o}, o) \;=\; V^\circ_{Op}(\tilde{o}, ([p], [q])) \;= \\
&\quad NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad (\forall\, \underline{q} \bullet \underline{q} \in [q] \Rightarrow \tilde{V}_{Op}(\tilde{o}, \underline{q}))\ \wedge \\
&\quad (\forall\, \underline{p}, u', \underline{v}', i, \underline{j}, u, \underline{v}, \tilde{u}', \tilde{i}, \tilde{u} \bullet \\
&\qquad N^\bullet_{Op}(([p], [q]), \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H^\bullet(u', \underline{v}') \wedge Q^\bullet_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^\bullet(u, \underline{v}) \wedge \\
&\qquad K^\circ(\tilde{u}', u') \wedge R^\circ_{Op}(\tilde{i}, i) \wedge K^\circ(\tilde{u}, u) \Rightarrow \\
&\qquad\quad \tilde{N}_{Op}(\tilde{o}, \underline{p}; \tilde{u}', \underline{v}', \tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \tilde{H}(\tilde{u}', \underline{v}') \wedge \tilde{Q}_{Op}(\tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \tilde{H}(\tilde{u}, \underline{v}))\ \wedge \\
&\quad (\forall\, u', \underline{v}', \underline{p}, i, \underline{j}, u, \underline{v}, \tilde{u}', \tilde{i}, \tilde{u} \bullet \\
&\qquad D^\bullet_{Op}(u', \underline{v}', ([p], [q]), \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q^\bullet_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^\bullet(u, \underline{v}) \wedge \\
&\qquad K^\circ(\tilde{u}', u') \wedge R^\circ_{Op}(\tilde{i}, i) \wedge K^\circ(\tilde{u}, u) \Rightarrow \\
&\qquad\quad \tilde{D}_{Op}(\tilde{u}', \underline{v}', \tilde{o}, \underline{p}; \tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \tilde{Q}_{Op}(\tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \tilde{H}(\tilde{u}, \underline{v}))\,.
\end{aligned}
\tag{9.61}
$$

9.5.2.2 The input initialisation PO

We show

$$
InitIn_{Op_U}(l, i) \;\Rightarrow\; (\exists\, \tilde{i} \bullet InitIn_{Op_X}(l, \tilde{i}) \wedge R^\circ_{Op}(\tilde{i}, i))\,. \tag{9.62}
$$

Proof. Assume $InitIn_{Op_U}(l, i)$ with $i = ([j], [k])$. Then, by (9.38), $l \in [k]$, $QR_{Op}([j], [k])$ and $T_{Op}([k])$ all hold. So, since $l \sim k$, by (9.36), $InitIn_{Op_F}(l, k)$ holds. Thus, from the Input Initialisation PO for the refinement from *Xtra* to *Ref*,

$$InitIn_{Op_F}(l, k) \Rightarrow (\exists\, i\tilde{} \bullet InitIn_{Op_X}(l, i\tilde{}) \wedge R\tilde{}_{Op}(i\tilde{}, k)) \tag{9.63}$$

we derive $i\tilde{}$ such that $InitIn_{Op_X}(l, i\tilde{})$, the first predicate we seek, and $R\tilde{}_{Op}(i\tilde{}, k)$ hold.

It remains to show $R°_{Op}(i\tilde{}, i)$. This we do by establishing each conjunct of (9.60). The first conjunct holds because we have both $QR_{Op}([j], [k])$ and $T_{Op}([k])$. Take the second conjunct and assume $\underline{k} \in [k]$. We require $R\tilde{}_{Op}(i\tilde{}, \underline{k})$. This follows from (X2) because we have $R\tilde{}_{Op}(i\tilde{}, k)$.

To show the third conjunct assume $Q^{\bullet}_{Op}(([j], [k]), \underline{j}, \underline{u}, \underline{v})$, $H^{\bullet}(\underline{u}, \underline{v})$ and $K°(\underline{u}\tilde{}, \underline{u})$, with $\underline{u} = ([\underline{v}], [\underline{w}])$. We require $Q\tilde{}_{Op}(i\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$ and $H\tilde{}(\underline{u}\tilde{}, \underline{v})$. We work as follows. From $Q^{\bullet}_{Op}$, by (9.24), $\underline{j} \sim j$ and $\underline{v} \sim \underline{v}$. So $([j], [k]) = ([\underline{j}], [k])$ and $([\underline{v}], [\underline{w}]) = ([\underline{v}], [\underline{w}])$. From $K°(\underline{u}\tilde{}, ([\underline{v}], [\underline{w}]))$, as $\underline{w} \in [\underline{w}]$, by (9.59), $K\tilde{}(\underline{u}\tilde{}, \underline{w})$ holds. Hence, since we have $R\tilde{}_{Op}(i\tilde{}, k)$, $K\tilde{}(\underline{u}\tilde{}, \underline{w})$, $Q^{\bullet}_{Op}(([\underline{j}], [k]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ and $H^{\bullet}(([\underline{v}], [\underline{w}]), \underline{v})$, using (X5) we obtain $Q\tilde{}_{Op}(i\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$ and $H\tilde{}(\underline{u}\tilde{}, \underline{v})$, as required. This completes the proof. ■

9.5.2.3 The initialisation PO

We show

$$Init_U(u') \Rightarrow (\exists\, u\tilde{}' \bullet Init_X(u\tilde{}') \wedge K°(u\tilde{}', u')) \,. \tag{9.64}$$

Proof. Assume the antecedent with $u' = ([v'], [w'])$. Since we have $Init_U(u')$, either (9.32a) or (9.32b) must hold. We take each case in turn.

- Case (i). (9.32a) holds, so we have value $\underline{w}'$ say, for which $Init_F(\underline{w}')$ and $K^{\bullet}(u', \underline{w}')$ are true. Therefore, because $Init_F(\underline{w}')$ holds, we can use the Init PO for the refinement from *Xtra* to *Ref*,

$$Init_F(\underline{w}') \Rightarrow (\exists\, u\tilde{}' \bullet Init_X(u\tilde{}') \wedge K\tilde{}(u\tilde{}', \underline{w}')) \,, \tag{9.65}$$

  to obtain $Init_X(u\tilde{}')$, which we want, and also $K\tilde{}(u\tilde{}', \underline{w}')$, for value $u\tilde{}'$. It remains to show $K°(u\tilde{}', u')$. This holds by Lemma 9.2, because we have both $K^{\bullet}(u', \underline{w}')$ and $K\tilde{}(u\tilde{}', \underline{w}')$.

• Case (ii). (9.32b) holds, so we have value $\underline{v}'$ say, for which $Init_{\mathrm{T}}(\underline{v}')$ and $H^{\bullet}(u', \underline{v}')$ is true. Therefore, because $Init_{\mathrm{T}}(\underline{v}')$ holds, we can use the Init PO for the retrenchment from *Xtra* to *Ret*,

$$Init_{\mathrm{T}}(\underline{v}') \Rightarrow (\exists\, \tilde{u}' \bullet Init_{\mathrm{X}}(\tilde{u}') \wedge H^{\sim}(\tilde{u}', \underline{v}')) \,, \tag{9.66}$$

to obtain $Init_{\mathrm{X}}(\tilde{u}')$, which we want, and $H^{\sim}(\tilde{u}', \underline{v}')$, for value $\tilde{u}'$. It remains to show $K^{\circ}(\tilde{u}', u')$. This holds by Lemma 9.3, because we have both $H^{\bullet}(u', \underline{v}')$ and $H^{\sim}(\tilde{u}', \underline{v}')$.

■

9.5.2.4 The applicability PO

$$K^{\circ}(\tilde{u}, u) \wedge R^{\circ}{}_{Op}(\tilde{i}, i) \wedge trm_{Op_{\mathrm{X}}}(\tilde{u}, \tilde{i}) \;\Rightarrow\; trm_{Op_{\mathrm{U}}}(u, i) \,. \tag{9.67}$$

Proof. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. Since $w \in [w]$, from K°, by (9.59), $K^{\sim}(\tilde{u}, w)$ holds. Similarly, by (9.60), $R^{\circ}{}_{Op}$ gives $R^{\sim}{}_{Op}(\tilde{i}, k)$. Hence, from the applicability PO for the refinement from *Xtra* to *Ref*,

$$K^{\sim}(\tilde{u}, w) \wedge R^{\sim}{}_{Op}(\tilde{i}, k) \wedge trm_{Op_{\mathrm{X}}}(\tilde{u}, \tilde{i}) \;\Rightarrow\; trm_{Op_{\mathrm{F}}}(w, k) \,, \tag{9.68}$$

we know $trm_{Op_{\mathrm{F}}}(w, k)$ holds. From K° we also get $HK([v], [w])$ and $\bigwedge_{Op} DK_{Op}([v], [w])$, therefore, by (9.21), we know $K^{\bullet}(u, w)$ holds. From $R^{\circ}{}_{Op}$ we also get $QR_{Op}([j], [k])$ and $T_{Op}([k])$, therefore, by (9.23), $R^{\bullet}{}_{Op}(i, k)$ holds. Hence, (9.34a), and thus $trm_{Op_{\mathrm{U}}}(u, i)$ holds as required. ■

9.5.2.5 The correctness PO

We show

$$\begin{aligned} &K^{\circ}(\tilde{u}, u) \wedge R^{\circ}{}_{Op}(\tilde{i}, i) \wedge trm_{Op_{\mathrm{X}}}(\tilde{u}, \tilde{i}) \wedge stp_{Op_{\mathrm{U}}}(u, i, u', o) \Rightarrow \\ &\qquad (\exists\, \tilde{u}', \tilde{o} \bullet stp_{Op_{\mathrm{X}}}(\tilde{u}, \tilde{i}, \tilde{u}', \tilde{o}) \wedge K^{\circ}(\tilde{u}', u') \wedge V^{\circ}{}_{Op}(\tilde{o}, o)) \,. \end{aligned} \tag{9.69}$$

Proof. Assume the antecedents with $u = ([v], [w])$, $i = ([j], [k])$, $u' = ([v'], [w'])$ and $o = ([p], [q])$. Since we have $stp_{Op_{\mathrm{U}}}$, either (9.33a) or (9.33b) must hold. We take each case in turn.

• Case (i). (9.33a) holds, so we have values $\underline{w}$, $\underline{k}$, $\underline{w}'$ and $\underline{q}$, say, for which $K^{\bullet}(u, \underline{w})$, $R^{\bullet}_{Op}(i, \underline{k})$, $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$, $K^{\bullet}(u', \underline{w}')$ and $V^{\bullet}_{Op}(o, \underline{q})$ are true, with, by (9.21), $\underline{w} \in [w]$ and, by (9.22), $\underline{k} \in [k]$. Then from K°, by (9.59), we get $K^{\sim}(u^{\sim}, \underline{w})$, and from R°_{Op}, by (9.60), we get $R^{\sim}_{Op}(i^{\sim}, \underline{k})$. We can now use the correctness PO for the refinement from *Xtra* to *Ref*,

$$K^{\sim}(u^{\sim}, \underline{w}) \wedge R^{\sim}_{Op}(i^{\sim}, \underline{k}) \wedge trm_{Op_X}(u^{\sim}, i^{\sim}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \Rightarrow$$
$$(\exists\, u^{\sim\prime}, o^{\sim} \bullet stp_{Op_X}(u^{\sim}, i^{\sim}, u^{\sim\prime}, o^{\sim}) \wedge K^{\sim}(u^{\sim\prime}, \underline{w}') \wedge V^{\sim}_{Op}(o^{\sim}, \underline{q}))\ , \tag{9.70}$$

to obtain $stp_{Op_X}(u^{\sim}, i^{\sim}, u^{\sim\prime}, o^{\sim})$, which we want, and also $K^{\sim}(u^{\sim\prime}, \underline{w}')$ and $V^{\sim}_{Op}(o^{\sim}, \underline{q})$, for values $u^{\sim\prime}$ and $o^{\sim}$. It remains to show $K^{\circ}(u^{\sim\prime}, u')$ and $V^{\circ}_{Op}(o^{\sim}, o)$. These hold by Lemma 9.2 and Lemma 9.5 respectively, because we have both $K^{\bullet}(u', \underline{w}')$ and $K^{\sim}(u^{\sim\prime}, \underline{w}')$, and $V^{\bullet}_{Op}(o, \underline{q})$ and $V^{\sim}_{Op}(o^{\sim}, \underline{q})$.

• Case (ii). (9.33b) holds, so we have values $\underline{v}$, $\underline{j}$, $\underline{v}'$ and $\underline{p}$, say, for which $H^{\bullet}(u, \underline{v})$, $Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v})$, $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $(H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ are true. Then from $H^{\bullet}$, $Q^{\bullet}_{Op}$, K° and R°_{Op}, by (9.60), we get $H^{\sim}(u^{\sim}, \underline{v})$, $Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$. We can now use the Op PO for the retrenchment from *Xtra* to *Ret*,

$$H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow$$
$$(\exists\, u^{\sim\prime}, o^{\sim} \bullet stp_{Op_X}(u^{\sim}, i^{\sim}, u^{\sim\prime}, o^{\sim}) \wedge$$
$$((H^{\sim}(u^{\sim\prime}, \underline{v}') \wedge N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v})) \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v}))\ )\ , \tag{9.71}$$

to obtain $stp_{Op_X}(u^{\sim}, i^{\sim}, u^{\sim\prime}, o^{\sim})$, which we want, and $(H^{\sim\prime} \wedge N^{\sim}_{Op}) \vee D^{\sim}_{Op}$ to boot, for values $u^{\sim\prime}$ and $o^{\sim}$. Then, because we also have $(H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ and $H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$, by Lemma 9.4 and Lemma 9.6, $K^{\circ}(u^{\sim\prime}, u')$ and $V^{\circ}_{Op}(o^{\sim}, o)$ hold. We are done. ■

9.5.2.6 The output finalisation PO

We show

$$V^{\circ}_{Op}(o^{\sim}, o) \wedge FinOut_{Op_U}(o, n) \ \Rightarrow\ FinOut_{Op_X}(o^{\sim}, n)\ . \tag{9.72}$$

Proof. Assume the antecedents with $o = ([p], [q])$. From V°_{Op}, by (9.61), because $q \in [q]$, we get $V^{\sim}_{Op}(o^{\sim}, q)$. From $FinOut_{Op_U}(o, n)$, by (9.39), $n \in [q]$, so, by (9.37), $FinOut_{Op_F}(q, n)$ holds. Hence, we can use the output finalisation PO for the refinement from *Xtra* to *Ref*,

$$V^{\sim}_{Op}(o^{\sim}, q) \wedge FinOut_{Op_F}(q, n) \;\Rightarrow\; FinOut_{Op_X}(o^{\sim}, n) \tag{9.73}$$

to obtain $FinOut_{Op_X}(o^{\sim}, n)$. We are done. ■

This completes part (2) of the theorem.

9.5.3 The inclusions

Below we list the inclusions of part (2) of the theorem.

$$K^{\circ}(u^{\sim}, u) ⨾ K^{\bullet}(u, \underline{w}) \;\Rightarrow\; K^{\sim}(u^{\sim}, \underline{w}) \tag{9.74}$$

$$R^{\circ}_{Op}(i^{\sim}, i) ⨾ R^{\bullet}_{Op}(i, \underline{k}) \;\Rightarrow\; R^{\sim}_{Op}(i^{\sim}, \underline{k}) \tag{9.75}$$

$$V^{\circ}_{Op}(o^{\sim}, o) ⨾ V^{\bullet}_{Op}(o, \underline{q}) \;\Rightarrow\; V^{\sim}_{Op}(o^{\sim}, \underline{q}) \tag{9.76}$$

$$K^{\circ}(u^{\sim}, u) ⨾ H^{\bullet}(u, \underline{v}) \;\Rightarrow\; H^{\sim}(u^{\sim}, \underline{v}) \tag{9.77}$$

$$\begin{aligned}&(R^{\circ}_{Op}(i^{\sim}, i) \wedge K^{\circ}(u^{\sim}, u)) ⨾ (Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v})) \;\Rightarrow \\ &\quad (Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim}, \underline{v}))\end{aligned} \tag{9.78}$$

$$\begin{aligned}&(V^{\circ}_{Op}(o^{\sim}, o) \wedge K^{\circ}(u^{\sim\prime}, u') \wedge R^{\circ}_{Op}(i^{\sim}, i) \wedge K^{\circ}(u^{\sim}, u)) ⨾ \\ &\quad (N^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u', \underline{v}') \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v})) \;\Rightarrow \\ &\qquad N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim\prime}, \underline{v}') \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim}, \underline{v})\end{aligned} \tag{9.79}$$

$$\begin{aligned}&(K^{\circ}(u^{\sim\prime}, u') \wedge V^{\circ}_{Op}(o^{\sim}, o) \wedge R^{\circ}_{Op}(i^{\sim}, i) \wedge K^{\circ}(u^{\sim}, u)) ⨾ \\ &\quad (D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge H^{\bullet}(u, \underline{v})) \;\Rightarrow \\ &\qquad D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim}, \underline{v})\end{aligned} \tag{9.80}$$

We now show these inclusions hold.

♦ (9.74): $K^{\circ}(u^{\sim}, u) ⨾ K^{\bullet}(u, \underline{w}) \;\Rightarrow\; K^{\sim}(u^{\sim}, \underline{w})$.

Proof. Assume the antecedents and let $u = ([v], [w])$. Then from $K^{\bullet}(([v], [w]), \underline{w})$, by (9.21), $\underline{w} \in [w]$, and thus from $K^{\circ}(u^{\sim}, ([v], [w]))$, by (9.59), $K^{\sim}(u^{\sim}, \underline{w})$ follows, as required.

■

♦ (9.75) and (9.76).

Proof. Similar to (9.74). ■

♦ (9.77): $K^{\circ}(u^{\sim}, u) ⨾ H^{\bullet}(u, \underline{v}) \Rightarrow H^{\sim}(u^{\sim}, \underline{v})$.

Proof. The consequent follows immediately from the antecedents by (9.59).

■

♦ (9.78) to (9.80).

Proof. Similar to (9.77). ■

9.6 Proof for Part (3)

Part (3) follows readily by observing that for a system *Univ** having the same properties as *Univ*, there will be a refinement from *Univ* to *Univ** and a refinement from *Univ** to *Univ*. ☺ ■

This completes the proof of Theorem 9.1.

9.7 Lemmas

Lemma 9.2. Suppose $K^{\bullet}(u', \underline{w}')$ and $K^{\sim}(u^{\sim\prime}, \underline{w}')$ hold. Then $K^{\circ}(u^{\sim\prime}, u')$ holds.

Proof. Let $u' = ([v'], [w'])$. Then, from $K^{\bullet}(u', \underline{w}')$, by (9.21), $\underline{w}' \in [w']$. To show $K^{\circ\prime}$ we now establish each of the three conjuncts of (9.59) in turn.

• *1st conjunct.* $HK([v'], [w'])$ and $\bigwedge_{Op} DK_{Op}([v'], [w'])$ follow from $K^{\bullet}(u', \underline{w}')$, by (9.21).

• *2nd conjunct.* Assume $\underline{\underline{w}}' \in [w']$. We require $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$. We have $\underline{w}' \sim w' \sim \underline{\underline{w}}'$. So $\underline{\underline{w}}' \in [\underline{w}']$, and since $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds, (X1) gives $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$. Done.

• *3rd conjunct.* Assume $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$. We require $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$. From $H^{\bullet\prime}$, by (9.22), $v' \sim \underline{\underline{v}}'$, and we have $w' \sim \underline{w}'$. Thus $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$ holds. Hence, as we have $K^{\sim}(u^{\sim\prime}, \underline{w}')$, (X4) gives $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$, as required. ■

Lemma 9.3. Suppose $H^{\bullet}(u', \underline{v}')$ and $H^{\sim}(u^{\sim\prime}, \underline{v}')$ hold. Then $K^{\circ}(u^{\sim\prime}, u')$ holds.

Proof. Let $u' = ([v'], [w'])$. To show $K^{\circ\prime}$ we now establish each of the three conjuncts of (9.59).

• *1st conjunct.* $HK([v'], [w'])$ and $\bigwedge_{Op} DK_{Op}([v'], [w'])$ follow from $H^{\bullet\prime}$, by (9.22).

• *2nd conjunct.* Assume $\underline{\underline{w}}' \in [w']$. We require $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$. By Lemma 9.7, $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds with $\underline{w}' \in [w']$. Hence, $\underline{\underline{w}}' \sim w' \sim \underline{w}'$. Therefore, $\underline{\underline{w}}' \in [\underline{w}']$, and so, by (X1), $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ holds, as required.

• *3rd conjunct.* Assume $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$. We require $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$. From $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$, by (9.22), $\underline{\underline{v}}' \sim v'$. Next, by Lemma 9.7, $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds with $\underline{w}' \in [w']$. Hence, as $\underline{\underline{v}}' \sim v'$ and $\underline{w}' \sim w'$, $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$ holds. Thus, by (X4), $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$ holds. Done. ■

Lemma 9.4. Suppose $(H^{\bullet}(u', \underline{v}') \wedge N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v})) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ and $(H^{\sim}(u^{\sim\prime}, \underline{v}') \wedge N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v})) \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$ hold, along with $H^{\sim}(u^{\sim}, \underline{v})$ and $Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$. Then $K^{\circ}(u^{\sim\prime}, u')$ holds.

Proof. Let $o = ([p], [q])$ and $u' = ([v'], [w'])$. To show $K^{\circ\prime}$ we establish each of the three conjuncts of (9.59).

• *1st conjunct.* $HK([v'], [w'])$ and $\bigwedge_{Op} DK_{Op}([v'], [w'])$ follows from both $H^{\bullet\prime}$, by (9.22), and $D^{\bullet}_{Op}$, by (9.27).

• *2nd conjunct.* Assume $\underline{\underline{w}}' \in [w']$. We require $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$. By Lemma 9.7, $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds with $\underline{w}' \in [w']$. Hence, $\underline{\underline{w}}' \sim w' \sim \underline{w}'$. Therefore, $\underline{\underline{w}}' \in [\underline{w}']$, and so, by (X1), $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ holds, as required.

• *3rd conjunct.* Assume $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$. We require $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$. From $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$, by (9.22), $\underline{\underline{v}}' \sim v'$. Next, by Lemma 9.7, $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds with $\underline{w}' \in [w']$. Hence, as $\underline{\underline{v}}' \sim v'$ and $\underline{w}' \sim w'$, $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$ holds. Thus, by (X4), $H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}')$ holds, as required. ■

Lemma 9.5. Suppose $V^{\bullet}_{Op}(o, \underline{q})$ and $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ hold. Then $V^{\circ}_{Op}(o^{\sim}, o)$ holds.

Proof. Let $o = ([p], [q])$. Then, from $V^{\bullet}_{Op}(o, \underline{q})$, by (9.25), $\underline{q} \in [q]$. To show V°_{Op} we now establish each of the four conjuncts of (9.61) in turn.

• *1st conjunct.* $NV_{Op}([p], [q])$ and $DV_{Op}([p], [q])$ follow from $V^{\bullet}_{Op}(o, \underline{q})$, by (9.25).

• *2nd conjunct.* Assume $\underline{q} \in [q]$. We require $V^{\sim}_{Op}(o^{\sim}, \underline{q})$. We have $\underline{q} \sim q \sim \underline{q}$. So $\underline{q} \in [\underline{q}]$, and since $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ holds, (X3) gives $V^{\sim}_{Op}(o^{\sim}, \underline{q})$. Done.

• *3rd conjunct.* Assume $N^{\bullet}_{Op}(([p], [q]), \underline{p}; \underline{u}', \underline{v}', \underline{i}, \underline{j}, \underline{u}, \underline{v}) \wedge H^{\bullet}(\underline{u}', \underline{v}') \wedge Q^{\bullet}_{Op}(\underline{i}, \underline{j}, \underline{u}, \underline{v}) \wedge H^{\bullet}(\underline{u}, \underline{v}) \wedge K^{\circ}(\underline{u}^{\sim\prime}, \underline{u}') \wedge R^{\circ}_{Op}(\underline{i}^{\sim}, \underline{i}) \wedge K^{\circ}(\underline{u}^{\sim}, \underline{u})$. We require $N^{\sim}_{Op}(o^{\sim}, \underline{p}; \underline{u}^{\sim\prime}, \underline{v}', \underline{i}^{\sim}, \underline{j}, \underline{u}^{\sim}, \underline{v}) \wedge H^{\sim}(\underline{u}^{\sim\prime}, \underline{v}') \wedge Q^{\sim}_{Op}(\underline{i}^{\sim}, \underline{j}, \underline{u}^{\sim}, \underline{v}) \wedge H^{\sim}(\underline{u}^{\sim}, \underline{v})$. We proceed as follows. From $N^{\bullet}_{Op}(([p], [q]), \underline{p}; \underline{u}', \underline{v}', \underline{i}, \underline{j}, \underline{u}, \underline{v})$, by (9.26), the first component of $\underline{u}'$ is $[\underline{v}']$, and let the second be $[\underline{\underline{w}}']$. Thus $\underline{u}' = ([\underline{v}'], [\underline{\underline{w}}'])$. Similarly, we obtain $\underline{i} = ([\underline{j}], [\underline{\underline{k}}])$, $\underline{u} = ([\underline{v}], [\underline{\underline{w}}])$ and $o = ([p], [q]) = ([\underline{p}], [\underline{q}])$; recall $\underline{q} \sim q$.

Next, $K^{\circ}(\underline{u}^{\sim\prime}, \underline{u}')$ and $\underline{\underline{w}} \in [\underline{\underline{w}}']$, by (9.59), give $K^{\sim}(\underline{u}^{\sim\prime}, \underline{\underline{w}}')$. Likewise, $R^{\circ}_{Op}(\underline{i}^{\sim}, \underline{i})$, by (9.60), gives $R^{\sim}_{Op}(\underline{i}^{\sim}, \underline{k})$; $K^{\circ}(\underline{u}^{\sim}, \underline{u})$, by (9.59), gives $K^{\sim}(\underline{u}^{\sim}, \underline{\underline{w}})$. Notice that we also have $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ and $N^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{v}'], [\underline{\underline{w}}']), \underline{v}', ([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{v}], [\underline{\underline{w}}]), \underline{v}) \wedge H^{\bullet}(([\underline{v}'], [\underline{\underline{w}}']), \underline{v}') \wedge Q^{\bullet}_{Op}(([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{v}], [\underline{\underline{w}}]), \underline{v}) \wedge H^{\bullet}(([\underline{v}], [\underline{\underline{w}}]), \underline{v})$. So, (X6) gives $N^{\sim}_{Op}(o^{\sim}, \underline{p}; \underline{u}^{\sim\prime}, \underline{v}', \underline{i}^{\sim}, \underline{j}, \underline{u}^{\sim}, \underline{v}) \wedge H^{\sim}(\underline{u}^{\sim\prime}, \underline{v}') \wedge Q^{\sim}_{Op}(\underline{i}^{\sim}, \underline{j}, \underline{u}^{\sim}, \underline{v}) \wedge H^{\sim}(\underline{u}^{\sim}, \underline{v})$, as required.

• *4th conjunct.* Similar to that for the 3rd. ■

Lemma 9.6. Suppose $N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ and $(N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim\prime}, \underline{v}')) \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$ hold, along with $H^{\sim}(u^{\sim}, \underline{v})$ and $Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$. Then $V^{\circ}_{Op}(o^{\sim}, o)$ holds.

Proof. Let $o = ([p], [q])$ and $u' = ([v'], [w'])$. To show V°_{Op} we establish each of the four conjuncts of (9.61).

• *1st conjunct.* $NV_{Op}([p], [q])$ and $DV_{Op}([p], [q])$ follow from both $N^{\bullet}_{Op}$, by (9.26), and $D^{\bullet}_{Op}$, by (9.27).

• *2nd conjunct*. Assume $\underline{\underline{q}} \in [q]$. We require $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$. By Lemma 9.8, $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ holds, with $\underline{q} \in [q]$. Hence, $\underline{\underline{q}} \sim q \sim \underline{q}$. Therefore, $\underline{\underline{q}} \in [\underline{q}]$, and so, by (X3), $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$ holds, as required.

• *3rd conjunct*. Assume $N^{\bullet}_{Op}(([p], [q]), \underline{\underline{p}}; \underline{\underline{u}}', \underline{\underline{v}}', \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}) \wedge H^{\bullet}(\underline{\underline{u}}', \underline{\underline{v}}') \wedge Q^{\bullet}_{Op}(\underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}) \wedge H^{\bullet}(\underline{\underline{u}}, \underline{\underline{v}}) \wedge K^{\circ}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{u}}') \wedge R^{\circ}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{i}}) \wedge K^{\circ}(\underline{\underline{u}}^{\sim}, \underline{\underline{u}})$. We require $N^{\sim}_{Op}(o^{\sim}, \underline{\underline{p}}; \underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge H^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}') \wedge Q^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$. We proceed as follows.

First, by Lemma 9.8, $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$ holds, with $\underline{\underline{q}} \in [q]$. Next, from $N^{\bullet}_{Op}(([p], [q]), \underline{\underline{p}}; \underline{\underline{u}}', \underline{\underline{v}}', \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})$, by (9.26), the first component of $\underline{\underline{u}}'$ is $[\underline{\underline{v}}']$, and let the second be $[\underline{\underline{w}}']$. Thus $\underline{\underline{u}}' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Similarly, we obtain $\underline{\underline{i}} = ([\underline{\underline{j}}], [\underline{\underline{k}}])$, $\underline{\underline{u}} = ([\underline{\underline{v}}], [\underline{\underline{w}}])$ and $o = ([p], [q]) = ([\underline{\underline{p}}], [\underline{\underline{q}}])$; recall $\underline{\underline{q}} \sim q$. Last, $K^{\circ}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{u}}')$ and $\underline{\underline{w}} \in [\underline{\underline{w}}']$, by (9.59), give $K^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{w}}')$. Likewise, $R^{\circ}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{i}})$, by (9.60), gives $R^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$; $K^{\circ}(\underline{\underline{u}}^{\sim}, \underline{\underline{u}})$, by (9.59), gives $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$.

Hence, because we also have $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$ and $N^{\bullet}_{Op}(([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{\underline{j}}], [\underline{\underline{k}}]), \underline{\underline{j}}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}}) \wedge H^{\bullet}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}') \wedge Q^{\bullet}_{Op}(([\underline{\underline{j}}], [\underline{\underline{k}}]), \underline{\underline{j}}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}}) \wedge H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, by (X6), $N^{\sim}_{Op}(o^{\sim}, \underline{\underline{p}}; \underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge H^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}') \wedge Q^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$ holds and we are done.

• *4th conjunct*. Similar to the 3rd conjunct. ■

Lemma 9.7. Suppose $H^{\bullet}(u', \underline{v}')$ and $H^{\sim}(u^{\sim\prime}, \underline{v}')$ hold, with $u' = ([v'], [w'])$. Then $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds, with $\underline{w}' \in [w']$.

Proof. From $H^{\bullet}(u', \underline{v}')$, by (9.22), $KH(\underline{v}', [w'])$ holds and we can derive t' for which $K(\underline{v}', t')$ holds. It thus follows, by (9.10), that we have a value, $\underline{w}'$ say, such that $H(\underline{w}', t')$ holds, with $\underline{w}' \in [w']$. Then because $H^{\sim}(u^{\sim\prime}, \underline{v}') ⨾ K(\underline{v}', t')$ is true, by (9.49), we have $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}') ⨾ H(\underline{\underline{w}}', t')$. Accordingly, we can pick witness $\underline{\underline{w}}'$ for which $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ and $H(\underline{\underline{w}}', t')$ hold. Therefore, $H(\underline{\underline{w}}', t')$, $H(\underline{w}', t')$ and $K(\underline{v}', t')$ are all true. Thus, by (9.5), $\underline{\underline{w}}' \sim \underline{w}'$. So we have $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ and $\underline{w}' \in [\underline{\underline{w}}']$. Hence, by (X1), $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds, with $\underline{w}' \in [w']$. ■

Lemma 9.8. Suppose $N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ and $(H^{\sim}(u^{\sim\prime}, \underline{v}') \wedge N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v})) \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$ hold, along with $H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$, and let $o = ([\underline{p}], [q])$ and $u' = ([\underline{v}'], [w'])$. Then $K^{\sim}(u^{\sim\prime}, \underline{w}')$ and $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ hold, with $\underline{w}' \in [w']$ and $\underline{q} \in [q]$.

Proof. We have $N^{\bullet}_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. So first assume $N^{\bullet}_{Op}$. Then by (9.26), $VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])$ holds and we can derive s, t', h and t for which $V_{Op}(\underline{p}, s)$, $K(\underline{v}', t')$, $R_{Op}(\underline{j}, h)$ and $K(\underline{v}, t)$ hold. It thus follows, by (9.16), that we have a value, $\underline{q}$ say, such that $N_{Op}(\underline{q}, s; ...)$ holds, with $\underline{q} \in [q]$; and a value, $\underline{w}'$ say, such that $H(\underline{w}', t')$ holds, with $\underline{w}' \in [w']$.

On the other hand, assume $D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. Then by (9.27), $VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])$ holds, and we can derive t', s, h and t for which $K(\underline{v}', t')$, $V_{Op}(\underline{p}, s)$, $R_{Op}(\underline{j}, h)$ and $K(\underline{v}, t)$ hold. It thus follows, by (9.18), that we have a values, $\underline{w}'$ and $\underline{q}$ say, such that $D_{Op}(\underline{w}', t', \underline{q}, s; ...)$ holds, with $\underline{w}' \in [w']$ and $\underline{q} \in [q]$. Hence, from $N^{\bullet}_{Op} \vee D^{\bullet}_{Op}$ we have $(N_{Op}(\underline{q}, s; ...) \wedge H(\underline{w}', t')) \vee D_{Op}(\underline{w}', t', \underline{q}, s; ...)$, with $\underline{q} \in [q]$, $\underline{w}' \in [w']$ and also $V_{Op}(\underline{p}, s)$, $K(\underline{v}', t')$, $R_{Op}(\underline{j}, h)$ and $K(\underline{v}, t)$.

Now, $(N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim\prime}, \underline{v}')) \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$ is also true, together with $H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$. So, first assume $N^{\sim}_{Op} \wedge H^{\sim\prime}$. Then, because $(N^{\sim}_{Op}(o^{\sim}, \underline{p}; u^{\sim\prime}, \underline{v}', i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim\prime}, \underline{v}') \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim\prime}, \underline{v}'))$⨟$(V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$ is true, by (9.51), we have $(V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}}) \wedge K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}') \wedge R^{\sim}_{Op}(i^{\sim}, \underline{\underline{k}}) \wedge K^{\sim}(u^{\sim}, \underline{\underline{w}}))$⨟$(N_{Op}(\underline{\underline{q}}, s; \underline{\underline{w}}', t', \underline{\underline{k}}, h, \underline{\underline{w}}, t) \wedge H(\underline{\underline{w}}', t') \wedge Q_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t) \wedge H(\underline{\underline{w}}, t))$. Accordingly, we can pick witnesses $\underline{\underline{q}}$ and $\underline{\underline{w}}'$ for which $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$, $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$, $N_{Op}(\underline{\underline{q}}, s; ...)$ and $H(\underline{\underline{w}}', t')$ hold.

Therefore, $N_{Op}(\underline{\underline{q}}, s; ...)$, $N_{Op}(\underline{q}, s; ...) \vee D_{Op}(..., \underline{q}, s; ...)$ and $V_{Op}(\underline{p}, s)$ are all true. Thus, by (9.9), $\underline{\underline{q}} \sim \underline{q}$. So we have $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$ and $\underline{q} \in [\underline{\underline{q}}]$. Therefore by (X3), $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ holds, with $\underline{q} \in [q]$, as required.

Additionally, $H(\underline{\underline{w}}', t')$, $H(\underline{w}', t') \vee D_{Op}(\underline{w}', t', ...)$ and $K(\underline{v}', t')$ are all true. Thus, by (9.5), $\underline{\underline{w}}' \sim \underline{w}'$. So we have $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ and $\underline{w}' \in [\underline{\underline{w}}']$. Therefore by (X1), $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds, with $\underline{w}' \in [w']$, as required.

Alternatively, assume $D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$. Then, because $(D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge H^{\sim}(u^{\sim}, \underline{v}))$⨟$(K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$ is true, by (9.52), we have $(K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}') \wedge V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}}) \wedge R^{\sim}_{Op}(i^{\sim}, \underline{\underline{k}}) \wedge K^{\sim}(u^{\sim}, \underline{\underline{w}}))$⨟$(D_{Op}(\underline{\underline{w}}', t', \underline{\underline{q}}, s; \underline{\underline{k}}, h, \underline{\underline{w}}, t) \wedge Q_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t) \wedge H(\underline{\underline{w}}, t))$. Accordingly, we can pick witnesses $\underline{\underline{w}}'$ and $\underline{\underline{q}}$ for which $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$, $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$, $D_{Op}(\underline{\underline{w}}', t', \underline{\underline{q}}, s; ...)$ hold.

Therefore, $D_{Op}(..., \underline{q}, s; ...)$, $N_{Op}(\underline{q}, s; ...) \vee D_{Op}(..., \underline{q}, s; ...)$ and $V_{Op}(\underline{p}, s)$ hold; and so do $D_{Op}(\underline{\underline{w}}', t', ...)$, $H(\underline{w}', t') \vee D_{Op}(\underline{w}', t', ...)$ and $K(\underline{v}', t')$. We now argue as for $(\tilde{N}_{Op} \wedge \tilde{H}') \vee \tilde{D}_{Op}$ to derive $\tilde{V}_{Op}(\tilde{o}, \underline{q})$ and $\tilde{K}(\tilde{u}', \underline{w}')$ once again. Done. ■

9.8 Inside *Univ*

To end this chapter we return to the *Add* operation of the Number Recycler and consider the structure of *Univ*. We have already described the systems *Ref* and *Ret* in the previous chapter, and *Conc* was covered in Chapter 5. Both *Ref* and *Conc* represent the number bin by a sequence, while *Ret* uses a set. Further, recall that the retrenchment from *Ref* to *Conc* introduces a bound on the sequence, while the refinement from *Ret* to *Conc* replaces sets with sequences. We reproduce the relevant part of *Conc* below, to keep notation consistent.

$$\mathsf{T} = \{t \in \mathsf{iseq}(\mathbb{N}) \mid \mathsf{len}(t) \leq 5\},\ \mathsf{H}_{Add_C} = \mathbb{N},\ \mathsf{S}_{Add_C} = \{\mathsf{OK}, \mathsf{GOT}, \mathsf{FULL}\}. \tag{9.81}$$

$$\begin{aligned}
&t \text{ -}(h, Add_C, \mathsf{OK})\text{-}\rightarrow t \frown \langle h \rangle, \text{ if } h \notin \mathsf{ran}(t) \wedge \mathsf{len}(t) \leq 4\ ,\\
&t \text{ -}(h, Add_C, \mathsf{FULL})\text{-}\rightarrow t, \text{ if } h \notin \mathsf{ran}(t) \wedge \mathsf{len}(t) = 5\ ,\\
&t \text{ -}(h, Add_C, \mathsf{GOT})\text{-}\rightarrow t, \text{ if } h \in \mathsf{ran}(t)\ .
\end{aligned} \tag{9.82}$$

We now give the data for the retrenchment from *Ref* to *Conc*.

$$\begin{aligned}
&H(w, t) = (w = t)\ ,\\
&Q_{Add}(k, h, w, t) \ = \ (k = h)\ ,\\
&N_{Add}(q, s, w', t'; k, h, w, t) \ = \ (q = s)\ ,\\
&D_{Add}(w', t', q, s; k, h, w, t) \ =\\
&\qquad (\mathsf{len}(w) = 5 \wedge k \notin \mathsf{ran}(w) \wedge w' = w \frown \langle k \rangle \wedge t' = w \wedge q = s)\ .
\end{aligned} \tag{9.83}$$

For the refinement from *Ret* to *Conc* we have

$$\begin{aligned}
&K(v, t) = (v = \mathsf{ran}(t))\ ,\\
&R_{Add}(j, h) \ = \ (j = h)\ ,\\
&V_{Add}(p, s) \ = \ (p = s)\ .
\end{aligned} \tag{9.84}$$

The equivalence relations partition the spaces of *Ret* and *Ref* in exactly the same way as we saw for the postjoin. We can thus move on to discuss the transitions for *Univ*. We find

that *Univ* groups together corresponding *Ret* and *Ref* transitions. For non-boundary cases, we have steps like

$$([\{1, 2\}], [\langle 1, 2\rangle])\ \text{-}(([3], [3]), Add_{\mathrm{U}}, ([\mathsf{OK}], [\mathsf{OK}]))\text{-}\rightarrow\ ([\{1, 2, 3\}], [\langle 1, 2, 3\rangle])\ .$$

This satisfies (9.33) and through the equivalence classes brings together the related steps $\langle 1,2\rangle$ -(3, Add_{F}, OK)-› $\langle 1,2,3\rangle$, $\langle 2,1\rangle$ -(3, Add_{F}, OK)-› $\langle 2,1,3\rangle$ and $\{1,2\}$ -(3, Add_{T}, OK)-› $\{1,2,3\}$.

An example of a boundary step is

$$([\{1 .. 5\}], [\langle 1 .. 5\rangle])\ \text{-}(([6], [6]), Add_{\mathrm{U}}, ([\mathsf{FULL}], [\mathsf{OK}]))\text{-}\rightarrow\ ([\{1 .. 5\}], [\langle 1 .. 6\rangle])\ ,$$

which also satisfies (9.33). This time the *Univ* step bundles together $\langle 1 .. 5\rangle$ -(6, Add_{F}, OK)-› $\langle 1 .. 6\rangle$, all the other similar *Ref* steps where the before state w is a serialisation of $\{1 .. 5\}$ and the after state is $w \wedge \langle 6\rangle$, and the *Ret* step $\{1 .. 5\}$ -(6, Add_{T}, FULL)-› $\{1 .. 5\}$. Notice that $[\langle 1 .. 5\rangle] = [\langle 1 .. 6\rangle]$.

In general, since $a \vee b \equiv a \vee (a \wedge b) \vee b$, (9.33) states that a *Univ* transition consists of a group of corresponding *Ret* and *Ref* transitions (as in the above cases), one or more *Ret* transitions only, or one or more *Ref* transitions only. This is illustrated by the case shown in Figure 9.2. In the figure I/O has been suppressed, and the *Ret* and *Ref* transitions shown satisfy (9.33a) and (9.33b) respectively. Transitions with matching subscripts are related in that one retrenches or refines the other. Thus $w_5 \mapsto w'_5$ refines $u_5 \mapsto u'_5$ and $v_0 \mapsto v'_3$ retrenches $u_0 \mapsto u'_3$. Each *Univ* step is an amalgam of *Ret* and/or *Ref* steps which match it on subscripts. Hence, $u_0 \mapsto u'_2$ is a combination of the steps $v_0 \mapsto v'_2$ and $w_0 \mapsto w'_2$, $u_0 \mapsto u'_3$ contains just the step $v_0 \mapsto v'_2$ and $u_0 \mapsto u'_4$ contains just $w_0 \mapsto w'_4$.

Going back to Add_{F}, the transition $w_5 \mapsto w'_6$ represents any step which adds a number to a sequence of length six or more, e.g. $\langle 1 .. 9, 15\rangle$ -(21, Add_{F}, OK)-› $\langle 1 .. 9, 15, 21\rangle$. This of course has no match in the bounded system *Ret* (or *Conc* for that matter). Notice that there are no such comparable steps for *Ret*. As $Q^{\bullet}_{Op} \wedge H^{\bullet}$ implies $Q_{Op} \wedge H$, which in turn implies $trm_{Op_{\mathrm{F}}}$, for every *Ret* step in *Univ*, its $trm_{Op_{\mathrm{T}}}$ must have a corresponding $trm_{Op_{\mathrm{F}}}$. So at most we have are transitions like $v_0 \mapsto v'_3$; where v_0 corresponds with w_0. We refer

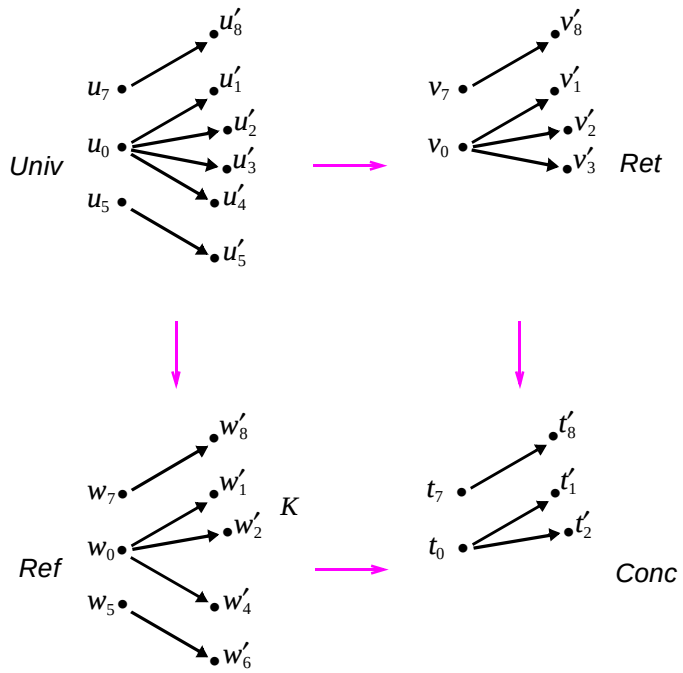


Figure 9.2

to *Univ* steps for which either only (9.33a) or (9.33b) holds as junk, since they fall outside the scope of the retrenchment from *Univ* to *Conc*.

We also require *Univ* to be the most concrete completion of the square. By this we mean that any other system which also completes the square must be refinable to *Univ*. As refinement is concerned with reduction in nondeterminism, this therefore precludes solutions like the *Univ* in Figure 9.2 but with, for instance, the additional transition $u_0 \mapsto u'_9$ (the old *Univ* still completes the square so must be refinable to the one with the extra transition). Finally, notice that *Ref* is not a solution for *Univ*, as is sometimes suggested. As can be seen from the example in Figure 9.2, putting *Ref* in place of *Univ* results in $v_0 \mapsto v'_3$ no longer having a suitable step which it can refine.

Chapter 10

Lifting the Mondex Purse

This chapter outlines how the lifting construction has been applied in [BPJS05a] to extend the scope of the Mondex Purse Development [SCW98, SCW00]. The precise details are considerable and beyond the scope of this thesis. A review of work on Mondex and retrenchment can also be found in [BJPS]. The material in this chapter is closely based on [BPJS05a]. A knowledge of Z, the notation used for the Mondex development, is assumed.

10.1 The Mondex Purse Development

The Mondex Purse is a system of electronic purses hosted on Smartcards that provides an alternative to the use of physical money. The system was developed by the NatWest Development Team in the 1990s, and was followed by a pilot in Swindon, U.K. Mondex is obviously an extremely security-critical application. To increase confidence in the product, in particular that there were no errors in design or implementation with security implications, formal techniques were employed. An abstract model capturing required security properties, and a concrete model closely reflecting the actual purse design were developed, and a nontrivial refinement was manually shown to hold between the two. The Mondex product was the first ever to earn an ITSEC rating of E6 [DTI91], equal to the present day Common Criteria EAL 7 certification.

The abstract model, *Abstract*, describes a world of purses which exchange monetary value via atomic transactions. It also expresses security properties that must be preserved by the world. These necessitate the total amount of money in the entire system is maintained and

transfers only occur between authentic purses. An important feature of the model is that it is straightforward to understand, allowing the client to see that required properties have been captured. In the concrete model, *Concrete*, transactions occur via a three-step protocol and the communication medium is insecure and lossy. Purses must log unsuccessful transactions locally (for later uploading), and there are no global properties: each purse is on its own.

The introduction of non-atomic transactions in the concrete model results in certain non-determinism being resolved earlier in the abstract model than in the concrete. We mentioned in Chapter 2, that the backward simulation rules are needed to establish a refinement between such models. However, as explained in [SCW98], to discharge the backward rules in this case, information embedded in the global properties is needed, and this information cannot be included in the concrete model, since there, the purses exist in isolation. To overcome this hurdle, an additional model *Between* was introduced, which included the global information. A backward refinement could now be established from *Abstract* to *Between*, and the more usual forward refinement holds from *Between* to *Concrete*. Since the security properties expressed in the abstract model are functional, and refinement is transitive, the security properties are preserved in the concrete model. The three models in the development are shown in the left column of Figure 10.1.

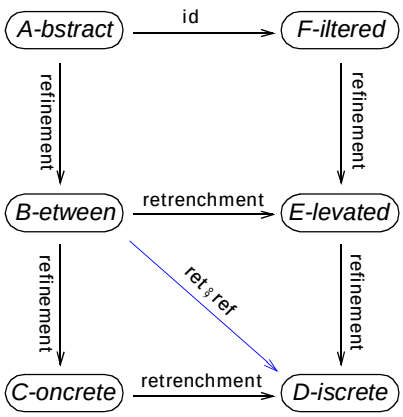


Figure 10.1: The Tower Pattern applied to the Mondex Purse

The success of Mondex is an important accomplishment and shows that formal techniques can make a contribution in real, industrial-scale developments. Nevertheless, in order for a refinement to be established, a number of issues were deemed to be outside the scope of the project or were handled in a rather unnatural way. One of these issues concerns the transaction protocol. To differentiate between separate transactions, each is stamped with a sequence number. In *Concrete* these numbers are modelled as naturals whereas in reality they are bounded. A more accurate representation of the purse design should reflect the nature of the transaction sequence numbers. By using retrenchment we can capture the transformation from infinite to finite sequence number and thus narrow the gap between the most concrete model and the real purse and so increase the veracity of the Mondex development.

[BPJS05a] addresses the sequence number disparity. A suitable retrenchment is constructed from *Concrete* to a new model *Discrete*, as depicted in Figure 10.1, in which the transaction number is restricted. *Discrete* is then lifted by the construction in Chapter 5 to give a new model *Elevated*, which is at the level of *Between*. It turns out that for the operation considered in the paper, *Elevated* is a backward refinement of *Abstract*. Thus *Filtered*, the top level model on the right side of the tower, which is to be at the level of *Abstract*, is obtained by simply relabelling the latter. In the sequel we will usually refer to the models by just the first letter of their name; thus *Between* is the B model.

10.2 Refinement and Retrenchment in Z

For completeness we first recall the forward refinement rules in Z, after which we give the rules for (forward) retrenchment in what is for the latter a less familiar setting. We will not need to concern ourselves with the backward refinement rules.

We give the refinement rules in the context of a forward simulation from model B to C. Let model B be given by the ADT $(B, BInit, \{BOp, BI_{Op}, BO_{Op} \mid Op \in \mathsf{Ops}\})$, and let model C be given by the ADT $(C, CInit, \{COp, CI_{Op}, CO_{Op} \mid Op \in \mathsf{Ops}\})$. So schemas B, C give the abstract and concrete state spaces, and the corresponding per-operation I/O spaces are given by schemas BI_{Op}, BO_{Op} and CI_{Op}, CO_{Op}. We assume a retrieve relation $R_{BC} : [B ; C]$ between the two state spaces, and for each operation Op, input and output

mapping relations $RI_{BC,Op} : [BI_{Op} ; BO_{Op}]$ and $RO_{BC,Op} : [CI_{Op} ; CO_{Op}]$. The initialisation, applicability and correctness POs for forward refinement in Z are as follows[1].

$$\forall\ C' \bullet CInit \Rightarrow \exists\ B' \bullet BInit \wedge R'_{BC} \tag{10.1}$$

$$\forall\ B; BI_{Op}; C; CI_{Op} \bullet R_{BC} \wedge RI_{BC,Op} \wedge \mathsf{pre}\ BOp \Rightarrow \mathsf{pre}\ COp \tag{10.2}$$

$$\begin{aligned}&\forall\ B; BI_{Op}; C; CI_{Op}; C'; CO_{Op} \bullet R_{BC} \wedge RI_{BC,Op} \wedge \mathsf{pre}\ BOp \wedge COp \Rightarrow \\ &\quad \exists\ B'; BO_{Op} \bullet BOp \wedge R'_{BC} \wedge RO_{BC,Op}\end{aligned} \tag{10.3}$$

We now turn to the retrenchment from model C to D. Let model D be given by the ADT $(D, DInit, \{DOp, DI_{Op}, DO_{Op} \mid Op \in \mathsf{Ops}\})$. Let the retrieve relation be $R_{CD} : [C ; D]$. For each operation, the within, output and concedes relations are $W_{CD,Op} : [CI_{Op} ; C ; DI_{Op} ; D]$ and $O_{CD,Op}; C_{CD,Op} : [CI_{Op} ; C ; C' ; CO_{Op} ; DI_{Op} ; D ; D' ; DO_{Op}]$. The initialisation and operation PO for (forward) retrenchment in Z are shown below[2].

$$\forall\ D' \bullet DInit \Rightarrow \exists\ C' \bullet CInit \wedge R'_{CD} \tag{10.4}$$

$$\begin{aligned}&\forall\ C; CI_{Op}; D; DI_{Op}; D'; DO_{Op} \bullet R_{CD} \wedge W_{CD,Op} \wedge DOp \Rightarrow \\ &\quad \exists\ C'; CO_{Op} \bullet COp \wedge ((R'_{CD} \wedge O_{CD,Op}) \vee C_{CD,Op})\end{aligned} \tag{10.5}$$

10.3 The Retrenchment Step

The state of a concrete purse *CConPurse* consists of various components including $CnextSeqNo : \mathbb{N}$ which stores the transaction sequence number. Several operations can increase *CnextSeqNo*. The treatment in [BPJS05a] considered only ***CIncreasePurse-Okay***, shown below, which for simplicity was taken as being representative.

```
┌─ CIncreasePurseOkay ──────────────────────────────
│ ΔCConPurse
│ Cm?, Cm! : CMESSAGE
├──────────────────────────
│ ΞCConPurseIncrease
│ CnextSeqNo' ≥ CnextSeqNo
│ Cm! = ⊥
└───────────────────────────────────────────────────
```

1. B and C operations have identical inputs and outputs so input initialisation and output finalisation POs can be omitted.

2. Since all operations in the Mondex development and those we define are total, the termination PO is trivially true and so can be omitted.

where

$$CConPurseIncrease == CConPurse \setminus (CnextSeqNo)$$

CConPurseIncrease hides *CnextSeqNo*, so Ξ*CConPurseIncrease* stipulates that *CIncreasePurseOkay* does not change any of the other purse state components. The operation outputs the value $\perp$, which need not concern us here (but does not represent undefinedness as it did in Chapter 2).

We want to modify the C model to obtain a more faithful representation of the physical purse in which the transaction sequence number is bounded This is the job of the D model[1]. We define *DnextSeqNo* to take values from 0..*BIGNUM*, where *BIGNUM* represents the implemented limit. For the actual operation, the choice made was to disturb the original behaviour as little as possble. Thus the purse just skips once the maximum sequence number is reached and produces the output message *DpurseBlocked Dname*, where *Dname* is the name of the purse involved. No new purse states are introduced. *DIncreasePurseOkay* is detailed below.

$$\begin{array}{|l}
\hline
\textit{DIncreasePurseOkay} \\
\Delta DConPurse \\
Dm?, Dm! : DMESSAGE \\
\hline
\Xi DConPurseIncrease \\
(DnextSeqNo < BIGNUM \Rightarrow \\
\quad DnextSeqNo' \geq DnextSeqNo \wedge Dm! = \perp) \\
(DnextSeqNo = BIGNUM \Rightarrow \\
\qquad DnextSeqNo' = DnextSeqNo \wedge Dm! = DpurseBlocked\ Dname) \\
\hline
\end{array}$$

In the above schema *DConPurseIncrease* ‘is as’[2] *CConPurseIncrease*. The transformation from the C to D operation can be captured by a retrenchment with the following data.

1. We follow [BPJS05a]. As stated therein, we employ a convention of pre-capitalizing only the names of types. This is extended by prefixing a single letter *A*, *B*, etc. to a name as required, to denote the model in question. Thus *CThing* is a schema or other type in the C model, whereas *Dthing* is a variable, usually a schema component, in the D model.

2. We write *DSchema* ‘is as’ *CSchema* to indicate that the text of *DSchema* can be obtained from that of *CSchema* by replacing all *Cthing*s by *Dthing*s.

R_{CD}

$CConPurse; DConPurse$
$CDConPurseIncreaseEquality$

$CnextSeqNo = DnextSeqNo$

$W_{CD,IncreasePurseOkay}$

$CConPurse; DConPurse$
$Cm? : CMESSAGE$
$Dm? : DMESSAGE$

$O_{CD,IncreasePureseOkay}$

$Cm! : CMESSAGE$
$Dm! : DMESSAGE$

$Cm! = Dm!$

$C_{CD,IncreasePurseOkay}$

$CConPurse'; DConPurse'$
$CDConPurseIncreaseEquality'$
$Cm! : CMESSAGE$
$Dm! : DMESSAGE$

$CnextSeqNo' \geq DnextSeqNo'$
$Cm! = \bot$
$Dm! = DpurseBlocked\ Dname$

CDConPurseIncreaseEquality is shorthand for equalities between corresponding variables in *CConPurseIncrease* and *DConPurseIncrease*.

Having dealt with a single purse, we use promotion (a Z specification structuring mechanism, see e.g. [DB01] or [WD96]) to create the D world of purses *DConWorld*. This mirrors the formation of the C world of purses in the Mondex development. Thus *DConWorld*, which we give below, 'is as' *CConWorld* (which we do not quote since it is easily derivable from its D counterpart; we adopt this practice in general).

$$
\begin{array}{l}
\textit{DConWorld} \\
\hline
DconAuthPurse : NAME \rightarrowtail\!\!\!\!\!\rightarrow DConPurse \\
Dether : \mathbb{P}\ DMESSAGE \\
Darchive : \mathbb{P}\ DLogbook \\
\hline
\forall\ n : \mathrm{dom}\ DconAuthPurse \bullet (DconAuthPurse\ n).Dname = n \\
\forall\ nld : Darchive \bullet first\ nld \in \mathrm{dom}\ DconAuthPurse \\
\hline
\end{array}
$$

$$
\begin{array}{l}
\Phi DOp \\
\hline
\Delta DConWorld; \Delta DConPurse \\
Dm?, Dm! : DMESSAGE \\
Dname? : NAME \\
\hline
Dm? \in Dether \\
Dname? \in \mathrm{dom}\ DconAuthPurse \\
\theta DConPurse = DconAuthPurse\ Dname? \\
DconAuthPurse' = DconAuthPurse \oplus \{Dname? \mapsto \theta DConPurse'\} \\
Darchive' = Darchive \\
Dether' \subseteq Dether \cup \{Dm!\} \\
\hline
\end{array}
$$

$$
DIncrease == DIgnore \vee (\exists\ \Delta DConPurse \bullet \Phi DOp \wedge DIncreasePurseOkay)
$$

The (global) state of *DConWorld* consists of the index function *DconAuthPurse* of purses, as well as *Dether*, a collection of all messages sent so far, and *Darchive*, a secure store of transaction logs downloaded from purses. To complete the promotion we also need the promotion or framing schema ΦDOp which 'is as' ΦCOp. Finally we can define *DIncrease* which 'is as' *CIncrease* and promotes the individual purse operation *DIncreasePurseOkay*. The disjunct *DIgnore* (which 'is as' *CIgnore*) is a do-nothing operation which again need not concern us[1].

We can now turn to the promotion of the retrenchment between the single purse states to one between the C and D worlds. The promotion of a refinement would involve the definition of a global retrieve relation between the two worlds in question, such that for every purse the (local) retrieve relation R_{CD} holds. The case for retrenchment offers additional possibilities since a particular purse in the D world, may either re-establish R_{CD} or establish $C_{CD,IncreasePurseOkay}$ on completion of a *DIncreasePurseOkay* step. If we insist that the global retrieve relation holds only if R_{CD} holds for all purses (as for the refinement case), we have what is called strong promotion. An alternative, is to define

1. As we have remarked, all operations are total and this is achieved here by the disjunction with *DIgnore*.

the global retrieve relation to be true so long as there is at least one purse for which R_{CD} is true. This is weak promotion. A more intricate approach involves keeping track of which purses are still retrieving and which have conceded. This latter form, called precise promotion, is the approach we adopt here. More details on all these forms of promotion can be found in [BPJ04]. To keep track, we will use a world-level variable, the set *Dgood*, to maintain the names of purses that are still retrieving.

For precise promotion to function properly, since retrenchment does not prohibit R_{CD} and $C_{CD,IncreasePurseOkay}$ from both being true simultaneously, we need the following separability axiom (which must hold for each pair of corresponding abstract and concrete operations).

$$DEstRet^{PP}_{DOp} \wedge DEstCon^{PP}_{DOp} \Leftrightarrow \text{false} \tag{10.6}$$

where

$$DEstRet^{PP}_{DOp} \;==\; D; DI_{Op}; D'; DO_{Op} \mid DOp \wedge$$
$$(\exists\, C; CI_{Op}; C'; CO_{Op} \bullet R_{CD} \wedge W_{CD,Op} \wedge COp \wedge (R'_{CD} \wedge O_{CD,Op}))$$

$$DEstCon^{PP}_{DOp} \;==\; D; DI_{Op}; D'; DO_{Op} \mid DOp \wedge$$
$$(\exists\, C; CI_{Op}; C'; CO_{Op} \bullet R_{CD} \wedge W_{CD,Op} \wedge COp \wedge C_{CD,Op})$$

$$DNotEstRet^{PP}_{DOp} \;==\; D; DI_{Op}; D'; DO_{Op} \mid DOp \wedge$$
$$\neg(\exists\, C; CI_{Op}; C'; CO_{Op} \bullet R_{CD} \wedge W_{CD,Op} \wedge COp \wedge (R'_{CD} \wedge O_{CD,Op}))$$

When (10.6) holds, we can determine from a concrete step alone whether it re-establishes the local retrieve relation or whether it concedes. This allows the concrete promotion to accurately maintain *Dgood*. With the above framework in place, we can now write down the schema for the promoted world $DConWorld^{PP}$.

$$\begin{array}{|l}
\hline
\textit{DConWorld}^{PP} \\
\textit{DConWorld} \\
\textit{Dgood} : \mathbb{P}\, \textit{NAME} \\
\hline
\textit{Dgood} \subseteq \mathsf{dom}\ \textit{DconAuthPurse} \\
\hline
\end{array}$$

The associated framing schema ΦDOp^{PP} only differs form ΦDOp in the replacement of

DConWorld by $DConWorld^{PP}$ so we do not reproduce it here. Finally, we define the promoted operation, $DIncrease^{PP}$ as follows.

$$
\begin{aligned}
DIncrease^{PP} == DIgnore \lor \big(\exists\, \Delta DConPurse \bullet \Phi DOp^{PP} \land DIncreasePurseOkay \land \\
(DEstRet^{PP}_{DIncrease} \Rightarrow Dgood' = Dgood) \land \\
(DNotEstRet^{PP}_{DIncrease} \Rightarrow Dgood' = Dgood \setminus \{Dname?\}) \big)
\end{aligned}
$$

All that remains is to define the relations for the precisely promoted retrenchment. We give these below[1].

R^{PP}_{CD}

$CConWorld; DConWorld^{PP}$

$\mathsf{dom}\ CconAuthPurse = \mathsf{dom}\ DconAuthPurse$
$\forall\ Dnm : Dgood \bullet$
$\quad (CconAuthPurse\ Dnm).CnextSeqNo = (DconAuthPurse\ Dnm).DnextSeqNo \land$
$\quad$ “ $CDnamedConPurseIncreaseEquality\ Dnm$ ”
$Dgood \lhd Carchive = Dgood \lhd Darchive$
$(Dgood \times Dgood) \lhd Cether = (Dgood \times Dgood) \lhd Dether$

$W^{PP}_{CD,Increase}$

$CConWorld; DConWorld^{PP}$
$Cm? : CMESSAGE$
$Dm? : DMESSAGE$
$Cname?, Dname? : NAME$

$Cname? = Dname?$
$Cname? \in Dgood$

$O^{PP}_{CD,Increase}$

$\Delta DConWorld^{PP}$
$Cm! : CMESSAGE$
$Dm! : DMESSAGE$
$Dname? : NAME$

$Dgood' = Dgood$
$Cm! = Dm!$

1. A simplification made in arriving at the promoted relations is that all messages in the ether are tagged with the names of the credit and debit purses involved in a transaction, as the first two fields of the message. Although this is not the case in reality, the required information can be derived from the message contents.

$$
\begin{array}{l}
C^{PP}_{CD,Increase} \\
\hline
CConWorld'; DConWorld^{PP} \\
CDConPurseIncreaseEquality' \\
Cm! : CMESSAGE \\
Dm! : DMESSAGE \\
Dname? : NAME \\
\hline
Dgood' = Dgood - \{Dname?\} \\
\text{“}\ CDnamedConPurseIncreaseEquality\ Dnm\ \text{”} \\
(CconAuthPurse'\ Cname?).CnextSeqNo \geq \\
\qquad (DconAuthPurse'\ Dname?).DnextSeqNo \\
Cm! = \bot \\
Dm! = DpurseBlocked\ Dname? \\
Dgood' \lhd Carchive' = Dgood \lhd Darchive' \\
(Dgood' \times Dgood') \lhd Cether' = (Dgood' \times Dgood') \lhd Dether'
\end{array}
$$

In the above, **“** *CDnamedConPurseIncreaseEquality Dnm* **”** stipulates that the components of *DConPurseIncrease* and its C counterpart for the named purse are equal. This completes the retrenchment from the C to D world.

10.4 Lifting and the Tower

We now have the bottom of the tower in Figure 10.1. In this section we show how to obtain models E and F, which together with D form the right column of the tower. The first stage involves using the lifting construction to get *EIncrease* by lifting $DIncrease^{PP}$ to the level of *BIncrease*, which is given by

$$BIncrease == BIgnore \vee (\exists\ \Delta BConPurse \bullet \Phi BOp \wedge BIncreasePurseOkay)\ .$$

BIncreasePurseOkay ‘is as’ *CIncreasePurseOkay* and the rest looks to be what we expect, but recall that the B world contains additional global properties that are not present in the C (and D) worlds. In the B model, promotion is to a *BetweenWorld* and not to *BConWorld*. The *BetweenWorld* imposes additional properties on *BConWorld*, in the form of constraints on the ether, that allow the backward refinement from A to B to be established. In outline, the B world has the following structure.

ΦBOp

$\Delta BetweenWorld; \Delta BConPurse$
$Bm?, Bm! : DMESSAGE$
$Bname? : NAME$

$Bm? \in Bether$
$Bname? \in \mathrm{dom}\ BconAuthPurse$
$\theta BConPurse = BconAuthPurse\ Bname?$
$BconAuthPurse' = BconAuthPurse \oplus \{Bname? \mapsto \theta BConPurse'\}$
$Barchive' = Barchive$
$Bether' = Bether \cup \{Bm!\}$

$BetweenWorld$

$BAuxWorld$

---

constraints on the ether

$BAuxWorld$

$BConWorld$
auxiliary variables

---

definitions of auxiliary variables

where $BConWorld$ 'is as' $DConWorld$. The auxiliary variables do not put any additional constraints on the state, they are introduced purely to make some of the proofs in the Mondex development easier to discharge. The constraints in $BetweenWorld$ have no bearing on the lifting of $DIncrease^{PP}$ so we will not dwell on them further.

To apply the lifting we need a retrenchment from B to D. By Proposition 4.2, page 48, we know that we can compose the forward refinement from B to C and the retrenchment from C to D to obtain the required retrenchment. For the B to C refinement, R_{BC} is

R_{BC}

$BetweenWorld$
$CConWorld$

$CconAuthPurse = BconAuthPurse$
$Cether \subseteq Bether$
$Carchive = Barchive$

and the inputs and outputs in B and C are identical. For the C to D retrenchment the component relations have already been defined. Let the retrenchment from B to D have retrieve relation R_{BD}, within relation $W_{BD,Increase}$, output relation $O_{BD,Increase}$ and concedes relation $C_{BD,Increase}$. We find that R_{BD} 'is as' R_{CD}, and similarly so for the other relations.

We could now use (5.2), which gives the transitions of *Univ* in Chapter 5, to obtain *EIncrease*. However, we will first make a simplification. The retrenchment from C to D, and hence the one from B to D, does not introduce additional operations. We can therefore simplify *Univ* by dropping the tag *t* from the state space, because this is only required for cases where a retrenchment introduces new operations. The transitions for *Univ* in the simpler case are

$$\begin{aligned} & stp_{Op_U}(v, j, v', p) \;=\; stp_{Op_U}((u, w), (i, k), (u', w'), (o, q)) \;= \\ & \quad \big(G(u, w) \wedge P_{Op}(i, k, u, w) \wedge stp_{Op_A}(u, i, u', o) \wedge \\ & \quad ((G(u', w') \wedge O_{Op}(o, q; u', w', i, k, u, w)) \vee C_{Op}(u', w', o, q; i, k, u, w)) \big) \;. \end{aligned} \tag{10.7}$$

Rewriting (10.7) as a Z schema in the current context we obtain

protoEIncrease

$BIncrease; \Delta DConWorld^{PP}$
$Dm?, Dm! : DMESSAGE$

$R_{BD} \wedge W_{BD,Increase} \wedge ((R'_{BD} \wedge O_{BD,Increase}) \vee C_{BD,Increase})$

in which *BIncrease* contributes the steps of the B model. By Theorem 5.1, $DIncrease^{PP}$ refines *protoEIncrease*. We could proceed to expand *protoEIncrease* to see precisely what we have, and simplify to obtain the final *EIncrease* model. But instead, the following observation will enable us to employ a labour saving simplification. As discussed in Section 5.6, (10.7) describes the subset of *BIncrease* transitions for which $R_{BD} \wedge W_{BD} \wedge ((R'_{BD} \wedge O_{BD}) \vee C_{BD})$ holds. A quick examination soon reveals that the transitions in *protoEIncrease* are (ignoring other state components as they do not change)

$(BnextSeqNo, DnextSeqNo)\text{-}(protoEIncrease, (\perp, \perp))\text{-}\!\rightarrow(BnextSeqNo', DnextSeqNo')$

where $BnextSeqNo < BIGNUM \wedge BnextSeqNo \leq BnextSeqNo' \leq BIGNUM$

and

$(BIGNUM, BIGNUM)\text{-}(protoEIncrease, (\perp, DpurseBlocked\ Dname))\text{-}\!\rightarrow(BIGNUM, BIGNUM)$,

and each of these transitions has a corresponding transition in D. Hence $DIncrease^{PP}$ is interrefinable with *protoEIncrease* and therefore by Theorem 5.1 we can replace *protoEIncrease* with

EIncrease which 'is as' $DIncrease^{PP}$,

giving our final E model. So $DIncrease^{PP}$ was at the right level of abstraction after all, and this can be attributed to the minimal change in the construction of D.

In general, to obtain the F model, we would need to carry out a further lifting. However, recall that in this case the refinement from A to B is a backward simulation, and we have not considered such refinements in any of the constructions we have presented in this thesis. Fortunately, for the increase operation, this turns out not to be a problem. In the Mondex development the *Increase* operation in the B and C models is required to refine *AIgnore* (a do-nothing operation). Remember that *Abstract* has no sequence numbers, and the only change we have introduced by the retrenchment is the skipping behaviour of the E purse. This is therefore simulated by the do-nothing behaviour of the A operation. Thus *EIncrease* is a (backward) refinement of *AIgnore*. Hence, we can simply relabel the A model to obtain F[1].

10.5 Conclusion

We have seen how retrenchment can be integrated with an existing refinement-based development, and how for Mondex, retrenchment permitted the construction of a more accurate concrete model of the actual purse design. Once the retrenchment step had been completed, we proceeded to lift the resulting D model to the level of the initial abstract specification, building the tower in Figure 10.1 from the bottom up. The objective of this exercise was to obtain the specification refined by the D model. For the operation we considered we were able to exploit a property of the lifting construction to obtain model E. Finally, we observed that E was in fact a refinement of A, allowing us to complete the tower. In general, the final lifted model will not be a facsimile of the initial specification, in which case, since retrenchment is not a correctness preserving transformation, the

1. If we widen our scope beyond just the *Increase* operation, this is no longer true, since our final E model does not contain any global properties and, as we have already noted, this information is necessary to establish a backward refinement.

ability to generate a refinable initial specification, which can be examined, increases confidence in the appropriateness of the retrenchment steps undertaken to arrive at a final concrete system (D in this case).

10.6 Other Retrenchment Opportunities

The transaction sequence number is only one of several areas of the Mondex development where we can incorporate retrenchment in order to increase the fidelity of the final concrete model. These other retrenchment opportunities involve the purse log, log clear codes and a balance enquiry operation. We summarise these briefly.

• *purse log* Each purse has a local log to record unsuccessful transactions which in reality is bounded and small, but in the Mondex development is modelled as an unbounded store.

• *log clear* A purse needs to be assured that data in its log is in an off-card archive before deleting it from memory. A message containing a clear code instructs the purse to clear the log. In the concrete model, the purse log contents are assumed to be in total injective correspondence with the clear codes, a simplification necessary to enable proofs to be successfully discharged. In reality a cryptographic hash function is used, which is not injective.

• *balance enquiry* Each purse has a balance enquiry operation. If this is invoked at a particular point in the middle of a B model value transfer, a discrepancy can occur between the model A and B balances due to differences in where nondeterminism is resolved in the two models. This is handled in the Mondex development in a somewhat unnatural manner.

The two issues concerning the purse log are discussed in [BPJS05b, BPJS05c]. These papers also employ the Tower Pattern, using the lifting construction to build from the bottom up. [BPJS05d] describes how retrenchment helped in establishing a genuine forward refinement for Mondex.

Chapter 11

Conclusion

11.1 Summary

We have described stepwise refinement and the use of forward and backward simulation as a method for proving its correctness. We have also briefly looked at the limitations of refinement and why a more expressive development relation is needed. We introduced retrenchment, a liberalisation of refinement that addresses the restrictions encountered with the latter. We saw how the retrenchment POs are obtained by modifying the refinement forward simulation rules.

The contribution made by the work in this thesis is detailed in Chapters 4 to 8. There we joined retrenchment and refinement steps in structures which furnished new canonical systems possessing particular properties. One end goal of this activity is a complete algebraic theory of the integration of retrenchment and refinement. The first stage to this objective must be the composition of retrenchment and refinement steps. This we studied in Chapter 4 where we showed that both a retrenchment followed by a refinement and the converse compose to give a retrenchment.

We have looked in detail at four combinations of retrenchments and refinements and suggested ways in which they can be utilised at a practical level. Chapter 5 reported the first such combination: the lifting construction. This takes a retrenchment from an abstract to a concrete system and decomposes it into a retrenchment followed by a refinement to give a new system at the level of abstraction of the abstract one. The lifting offers a mechanism by which concrete structure introduced by one or more retrenchment steps can be raised all the way up to the abstract most level.

The reciprocal lowering construction in Chapter 6 decomposes a retrenchment from an abstract to a concrete system into a refinement followed by a retrenchment and gives a system at the level of the concrete one. It can be understood as a mechanism which generates a system that identifies abstract and concrete transitions related by a retrenchment. This offers a useful perspective on retrenchments introduced in the course of a development.

Chapter 8 presented the postjoin. Given a refinement from A to B and a retrenchment from A to C, the postjoin reconciles the retrenchment and refinement by constructing a new canonical system that is both a refinement of C and a retrenchment of B. It can be used to incorporate a change to the top level model A, expressed as a retrenchment to C, into the existing refinement B of the top model.

The last construction, the prejoin, was the subject of Chapter 9. This takes a refinement from A to C and a retrenchment from B to C (that are preconjoint) and engineers a new canonical system from which there is a retrenchment to A and a refinement to B. If the retrenchment from B to C captures a change to C expressed as B, the prejoin can be used to incorporate the change to the bottom level model C into the top level model A which C refines.

Chapter 10 gave an account of how the lifting construction and the Tower Pattern have been employed in work on extending the Mondex Purse. We built a new model which took account of the finite nature of transaction sequence numbers and related this via retrenchment to the original development's concrete model. Using the lifting theorem we then showed that there was a refinement from the original development's abstract specification to our newly constructed model. The operation we modified in constructing the new model was therefore correct with respect to the original specification.

11.2 Conclusions and Further Research

We have answered the question as to whether refinements and retrenchments can be combined in the four configurations we have considered in this thesis affirmatively. The results we have obtained demonstrate that retrenchment and refinement can work smoothly together, and therefore that the inclusion of retrenchment in a development will not shut

out refinement. This is important because it increases confidence in the relatively new technique of retrenchment, helping to promote its value in the formal methods community and encouraging its adoption by system developers. Moreover, the configurations we have considered provide a toolbox of mechanisms that permit the direct generation of new systems from previously constructed ones. The application of one of these configurations, the lifting, in the extension of the Mondex Purse development clearly indicates the kinds of benefits that the tools have to offer. Given the entirely formal nature of the mechanisms, they should be of particular interest to developers of high consequence software systems.

The application of our results in extensions to the Mondex Purse has led to the identification of the Tower Pattern as a structure that encapsulates how retrenchment steps may be incorporated into a refinement based development strategy. The configurations of retrenchments and refinements we have studied, enable the construction of the tower in several ways, starting from the top or the bottom and working from the left or from the right, with the process being essentially transparent to the particular requirements issues dealt with by the component retrenchments.

The postjoin and prejoin results we have obtained are certainly not straightforward; in fact they are somewhat involved and opaque to the non-specialist. These constructions are really a first attempt so see if the desired configurations were at all feasible. We wanted to discover what needed to be done to bring together retrenchments and refinements of as general a kind as possible, rather than to look for a particularly elegant but restricted result. However, given the complexity of the solutions, the pre- and postjoin need to be reexamined to see if there is a more easily accessible formulation of the desired integrations. One possible avenue is the expression of the theory in terms of the simulation relation for retrenchments and refinements. These are relations between abstract and concrete variables for which all the predicates involved in the principal PO hold. Thus for retrenchment it is one for which (3.7) is true. Another avenue, is a reformulation in terms of a double category of retrenchment/refinement two-cells. We could also consider whether by imposing conditions on the nature of the retrenchments and refinements we integrate, we can obtain simpler solutions that still admit enough cases as to make them worthwhile.

The algebraic theory of the integration of retrenchment and refinement we have developed thus far, only considers the forward simulation form of refinement. An obvious direction in which to extend present work is therefore to incorporate backward refinement in the various integrations. However, before this can be done, we need to investigate the appropriate shape of the POs for backward retrenchment.

We have claimed that the constructions in this thesis will prove useful in system development. Of course such claims can only be backed up by the application of our results. To make this a viable proposition, especially in the case of industrial scale developments, we need to mechanise the constructions we have developed. This will permit the automatic generation of the new systems that our constructions produce. What is more, recall that the theorems permit the replacement of the system generated by a more convenient one which is interrefinable with it. We exploited this very property in the Mondex Purse extension in the previous chapter. Such replacement can also benefit from mechanisation. A toolkit for retrenchment, named FROG, is currently under development. The intention is for the theorems we have presented to be automated in FROG when the tool is mature enough.

Appendix A

Postjoin Composition Proofs

A.1 Composition Proofs

In Section 8.3.4.1 we defined the retrieve, within, output and concedes relations, G, P_{Op}, O_{Op} and C_{Op} respectively, for the retrenchment from *Abs* to *Univ*. In this section we show that the two compositions given for each relation, which correspond to the two paths around the square from *Abs* to *Univ* in Figure 8.1, are equal. To simplify the proofs, we assume that Ops_A only has one operation.

♦ (8.57): $G = H \fatsemi K^{\bullet} = K \fatsemi H^{\bullet}$.

Proof. We expand each part in turn. Take $H \fatsemi K^{\bullet}$ first.

$H(u, \underline{v}) \fatsemi K^{\bullet}(\underline{v}, ([v], [w]))$

= [definition of composition]

$(\exists\, \underline{v} \bullet H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\,)$

= [definition of $K^{\bullet}$ (8.23)]

$(\exists\, \underline{v} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])\,)$

= [Lemma A.1]

$(\exists\, \underline{v} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\quad (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))\,)$

= [rewriting in prenex normal form]

$(\exists\, \underline{v}, \underline{w} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))$ **)**

= [rearranging]

($\exists\, \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge K(u, \underline{w}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$KH(\underline{w}, [v])$ **)** .

Now for $K ⨾ H^{\bullet}$.

$K(u, \underline{w}) ⨾ H^{\bullet}(\underline{w}, ([v], [w]))$

= [definition of composition]

($\exists\, \underline{w} \bullet K(u, \underline{w}) \wedge H^{\bullet}(\underline{w}, ([v], [w])$ **)**

= [definition of $H^{\bullet}$ (8.24)]

($\exists\, \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge$

$DK_{Op}([v], [w])$ **)**

= [$K(u, \underline{w}) \wedge (\exists\, u \bullet K(u, \underline{w})) \Leftrightarrow K(u, \underline{w})$]

($\exists\, \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [Lemma A.2]

($\exists\, \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$(\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$ **)**

= [rewriting in prenex normal form]

($\exists\, \underline{w}, \underline{v} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{v} \in [v] \wedge H(u, \underline{v})$ **)**

= [rearranging]

($\exists\, \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge K(u, \underline{w}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$

$\wedge\, KH(\underline{w}, [v])$**)**

Hence $K^{\bullet} ⨾ H = H^{\bullet} ⨾ K$. ■

♦ (8.58): $P_{Op} = (Q_{Op} \wedge H) ⨾ (R^{\bullet}{}_{Op} \wedge K^{\bullet}) = (R_{Op} \wedge K) ⨾ (Q^{\bullet}{}_{Op} \wedge H^{\bullet})$.

Proof. We expand each part in turn. Take $(H \wedge Q_{Op}) ⨾ (K^{\bullet} \wedge R^{\bullet}{}_{Op})$ first.

$$(H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) ⨾ (K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])))$$

= [definition of composition]

$$(\exists\, \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k]))\ )$$

= [definition of $R^{\bullet}{}_{Op}$ (8.25)]

$$(\exists\, \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k])$$
$$\wedge\, T_{Op}([j], [k])\ )$$

= [Lemma A.3]

$$(\exists\, \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge$$
$$\wedge\, T_{Op}([j], [k]) \wedge$$
$$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\ )$$

= [rewriting in prenex normal form]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge$$
$$\wedge\, T_{Op}([j], [k]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])\ )$$

= [definition of $K^{\bullet}$ (8.23)]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$
$$\underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v])\ )$$

= [Lemma A.4]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$
$$\underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])\ )$$

= [rearranging]

$$(\exists\, \underline{j}, \underline{k}, \underline{v}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{k} \in [k] \wedge \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge$$
$$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge QR_{Op}([j], [k]) \wedge$$
$$T_{Op}([j], [k]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])\ )$$

Next, we expand $(K \wedge R_{Op}) ⨾ (H^{\bullet} \wedge Q^{\bullet}{}_{Op})$.

$$\mathbf{(}K(u, \underline{w}) \wedge R_{Op}(i, \underline{k})\mathbf{)}\fatsemi\mathbf{(}H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w]))\mathbf{)}$$

= [definition of composition]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w]))\ \mathbf{)}$$

= [definition of $Q^{\bullet}$ (8.26)]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge$$
$$T_{Op}([j], [k])\ \mathbf{)}$$

= [definition of $\overline{Q}$ (8.16)]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$(\exists\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k])\ \mathbf{)}$$

= [$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge (\exists\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \Leftrightarrow K(u, \underline{w}) \wedge R_{Op}(i, \underline{k})$]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k])\ \mathbf{)}$$

= [Lemma A.5]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

= [rewriting in prenex normal form]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\ \mathbf{)}$$

= [definition of $H^{\bullet}$ (8.24)]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge \underline{w} \in [w] \wedge (\exists\ u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge$$
$$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$$
$$QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\ \mathbf{)}$$

= [$K(u, \underline{w}) \wedge (\exists\ u \bullet K(u, \underline{w})) \Leftrightarrow K(u, \underline{w})$]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge$$
$$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$$

$QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$ **)**

[rearranging, a ∧ a ⇔ a]

($\exists\, \underline{j}, \underline{k}, \underline{v}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{k} \in [k] \wedge \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge QR_{Op}([j], [k]) \wedge$

$T_{Op}([j], [k]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

Hence $(H \wedge Q_{Op})\fatsemi(K^{\bullet} \wedge R^{\bullet}_{Op}) = (K \wedge R_{Op})\fatsemi(H^{\bullet} \wedge Q^{\bullet}_{Op})$. ■

♦ (8.59): $O_{Op} = (N_{Op} \wedge H' \wedge Q_{Op} \wedge H)\fatsemi(V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})$

$= (V_{Op} \wedge K' \wedge R_{Op} \wedge K)\fatsemi(N^{\bullet}_{Op} \wedge H^{\bullet\prime} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet})$.

Proof. We expand each part in turn. Take $(N \wedge H' \wedge Q \wedge H)\fatsemi(V^{\bullet} \wedge K^{\bullet\prime} \wedge R^{\bullet} \wedge K^{\bullet})$ first.

($N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$ **)**⨾

($V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [definition of composition]

($\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [definition of $V^{\bullet}_{Op}$ (8.27)]

($\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$

$R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [Lemma A.9]

($\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$

$R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$

$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])$ **)**)

= [rewriting in prenex normal form]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$
$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])\ )$$

= [Lemma A.12]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$
$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge KH(\underline{w}', [v'])\ )$$

= [Lemma A.10]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$
$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge$$
$$KH(\underline{w}', [v']) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])\ )$$

= [Lemma A.4]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$
$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge$$
$$KH(\underline{w}', [v']) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])\ )$$

= [definition of $K^{\bullet}$, $K^{\bullet\prime}$ (8.23) and $R^{\bullet}$ (8.25)]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \underline{v}' \in [v'] \wedge HK([v'], [w']) \wedge$$
$$DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge$$
$$DK_{Op}([v], [w]) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$
$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge$$

$KH(\underline{w}', [v']) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

= [rearranging]

($\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge HK([v], [w]) \wedge$

$DK_{Op}([v], [w]) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge KH(\underline{w}', [v']) \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

Now for $(V_{Op} \wedge K' \wedge R_{Op} \wedge K) ⨾ (N^{\bullet}{}_{Op} \wedge H^{\bullet\prime} \wedge Q^{\bullet}{}_{Op} \wedge H^{\bullet})$.

($V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})$**)**⨾

($N^{\bullet}{}_{Op}(\underline{q}, ([p], [q]); \underline{w}', ([v'], [w']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}', ([v'], [w'])) \wedge$

$Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))$**)**

= [definition of composition]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$N^{\bullet}{}_{Op}(\underline{q}, ([p], [q]); \underline{w}', ([v'], [w']), \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}', ([v'], [w'])) \wedge$

$Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))$**)**

= [definition of $H^{\bullet}$, $H^{\bullet\prime}$ (8.24), $Q^{\bullet}$ (8.26) and $N^{\bullet}$ (8.28)]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$

$VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$\underline{w}' \in [w'] \wedge (\exists\, u' \bullet K(u', \underline{w}')) \wedge KH(\underline{w}', [v']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [definition of $\overline{Q}$ (8.16)]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$

$VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$\underline{w}' \in [w'] \wedge (\exists\, u' \bullet K(u', \underline{w}')) \wedge KH(\underline{w}', [v']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= $[V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge (\exists\, V \wedge K' \wedge R \wedge K) \wedge (\exists\, K') \wedge (\exists\, R \wedge K) \wedge (\exists\, K) \Leftrightarrow$

$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})$]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge \underline{w}' \in [w'] \wedge KH(\underline{w}', [v']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [Lemma A.11]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge \underline{w}' \in [w'] \wedge KH(\underline{w}', [v']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\,)$ **)**

= [rewriting in prenex normal form]

($\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{q} \in [q] \wedge$

$\underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge$

$NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \underline{w}' \in [w'] \wedge KH(\underline{w}', [v']) \wedge HK([v'], [w']) \wedge$

$DK_{Op}([v'], [w']) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge$

$T_{Op}([j], [k]) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge$

$Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$ **)**

[rearranging, a ∧ a ⇔ a]

($\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \wedge$

$KH(\underline{w}', [v']) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

Hence $(N \wedge H' \wedge Q \wedge H) ⨾ (V^{\bullet} \wedge K^{\bullet\prime} \wedge R^{\bullet} \wedge K^{\bullet}) = (V \wedge K' \wedge R \wedge K) ⨾ (N^{\bullet} \wedge H^{\bullet\prime} \wedge Q^{\bullet} \wedge H^{\bullet})$. ■

♦ (8.60): $C_{Op} = (D_{Op} \wedge Q_{Op} \wedge H) ⨾ (K^{\bullet\prime} \wedge V^{\bullet}_{Op} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})$
$= (K' \wedge V_{Op} \wedge R_{Op} \wedge K) ⨾ (D^{\bullet}_{Op} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet})$.

Proof. We expand each side in turn. Take $(D_{Op} \wedge Q_{Op} \wedge H) ⨾ (K^{\bullet\prime} \wedge V^{\bullet}_{Op} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})$ first.

($D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$ **)** ⨾

($K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [definition of composition]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$

$V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [definition of $V^{\bullet}_{Op}$ (8.12)]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$

$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ **)**

= [Lemma A.6]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$

$\underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$**)**)

= [rewriting in prenex normal form]

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$$

= [Lemma A.7]

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$$

= [Lemma A.4]

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v]))$$

= [definition of $K^{\bullet}$, $K^{\bullet\prime}$ (8.23) and $R^{\bullet}$ (8.25)]

$$\mathbf{(} \exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge \underline{v}' \in [v'] \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{p} \in [p] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v]) \mathbf{)}$$

= [rearranging]

$$\mathbf{(} \exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge HK([v], [w]) \wedge$

$DK_{Op}([v], [w]) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$KH(\underline{w}, [v])$ **)**

Now for $(K' \wedge V_{Op} \wedge R_{Op} \wedge K) ⨾ (D^{\bullet}{}_{Op} \wedge Q^{\bullet}{}_{Op} \wedge H^{\bullet})$.

($K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})$**)**⨾

($D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge$

$Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))$**)**

= [definition of composition]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge$

$Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge H^{\bullet}(\underline{w}, ([v], [w]))$**)**

= [definition of $D^{\bullet}$ (8.29), $Q^{\bullet}$ (8.26) and $H^{\bullet}$ (8.24)]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\overline{Q}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [definition of $\overline{Q}$ (8.16)]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= $[K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge (\exists\, u', o, i, u \bullet K' \wedge V \wedge R \wedge K) \wedge (\exists\, i, u \bullet R \wedge K) \wedge (\exists\, u \bullet K) \Leftrightarrow$

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})\ ]$

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [Lemma A.8]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\ )$ **)**

= [rewriting in prenex normal form]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w}' \in [w'] \wedge$

$\underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge$

$\underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$ **)**

= [rearranging, a $\wedge$ a $\Leftrightarrow$ a]

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([j], [k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v]))$$

Hence $(H \wedge Q \wedge D)\fatsemi(K^{\bullet\prime} \wedge V^{\bullet} \wedge R^{\bullet} \wedge K^{\bullet}) = (K' \wedge V \wedge R \wedge K)\fatsemi(H^{\bullet} \wedge Q^{\bullet} \wedge D^{\bullet})$. ■

A.2 Lemmas

Lemma A.1.

$$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge HK([v], [w]) \;\Rightarrow\; (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))$$

Proof.

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge HK([v], [w])$

$=$ [definition of HK (8.11)]

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge$

$\quad (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v])))$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge$

$\quad (\underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))) \wedge$

$\quad (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v])))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge (\underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v])))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))$ ■

Lemma A.2. $K(u, \underline{w}) \wedge KH(\underline{w}, [v]) \;\Rightarrow\; (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$

Proof.

$K(u, \underline{w}) \wedge KH(\underline{w}, [v])$

$=$ [definition of KH (8.10)]

$K(u, \underline{w}) \wedge (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$K(u, \underline{w}) \wedge (K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \wedge$

$\quad (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$K(u, \underline{w}) \wedge (K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$ ■

Lemma A.3.

$$\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge QR_{Op}([j], [k]) \Rightarrow$$
$$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$$

Proof.

$\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge QR_{Op}([j], [k])$

$=$ [definition of QR (8.15)]

$\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

$\quad (\forall\, \underline{j}, i, u, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$

$\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])))$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

$\quad (\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$

$\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))) \wedge$

$\quad (\forall\, \underline{j}, i, u, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$

$\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

$\quad (\underline{j} \in [j] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$ ■

Lemma A.4. $R_{Op}(i, \underline{k}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \Rightarrow KH(\underline{w}, [v])$

Proof.

$R_{Op}(i, \underline{k}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$

$=$ [definition of RQ (8.14)]

$R_{Op}(i, \underline{k}) \wedge (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))$

$=$ [$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \Leftrightarrow$

$\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \wedge (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$]

$R_{Op}(i, \underline{k}) \wedge (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \wedge$

$\quad\quad (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$)

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$R_{Op}(i, \underline{k}) \wedge (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \wedge$

$\quad (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$R_{Op}(i, \underline{k}) \wedge (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$R_{Op}(i, \underline{k}) \wedge (\forall\, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \wedge$

$\quad (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$R_{Op}(i, \underline{k}) \wedge (\ \forall\ u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ )$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \ \Leftrightarrow\ a \wedge (b \Rightarrow c)$]

$R_{Op}(i, \underline{k}) \wedge (\ \forall\ u \bullet K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ )$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$(\ \forall\ u \bullet K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ )$

$\Rightarrow$ [(8.10)]

$KH(\underline{v}, [w])$ ■

Lemma A.5.

$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \Rightarrow$
$\quad (\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))$

Proof.

$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$

$=$ [definition of RQ (8.14)]

$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$
$\quad (\forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$
$\qquad (\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$
$\quad (R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})))\ \wedge$
$\quad (\forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$
$\qquad (\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$
$\quad (R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$ ■

Lemma A.6.

$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge DV_{Op}([p], [q]) \Rightarrow$$
$$\mathbf{(}\ \exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])\ \mathbf{)}$$

Proof.

$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge DV_{Op}([p], [q])$$

= [definition of *DV* (8.20)]

$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$\mathbf{(}\ \forall\ \underline{p}, u', \underline{v}', o, i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet$$
$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))\ \mathbf{)}$$

= [meaning of ∀, a ∧ a ⇔ a]

$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$\mathbf{(}\ \underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))\ \mathbf{)} \wedge$$
$$\mathbf{(}\ \forall\ \underline{p}, u', \underline{v}', o, i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet$$
$$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$ **)**

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

($\underline{p} \in [p] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$

$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$ **)**

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$ **)** ■

Lemma A.7.

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \Rightarrow RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$

Proof.

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$

= [definition of *VD* (8.19)]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$

$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$**)**)

= [**(**$\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D \wedge Q \wedge H$**)** $\Leftrightarrow$

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D \wedge Q \wedge H$**)** $\wedge$ **(**$\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q \wedge H$**)**]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$

($\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

(**(**$\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})$**)** $\wedge$

$$\mathbf{(}\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\ )\ \mathbf{)}$$

$=$ [meaning of $\forall$, $(a \Rightarrow (b \wedge c)) \Leftrightarrow ((a \Rightarrow b) \wedge (a \Rightarrow c))$]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$\mathbf{(}\ \forall\, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$\mathbf{(}\ \forall\, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \;\Leftrightarrow\; a \wedge (b \Rightarrow c)$]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge \mathbf{(}\ \forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$(\ \forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \mathbf{(}\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\ )$$

$\Rightarrow$ [(8.14)]

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$ ■

Lemma A.8.

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))$$

Proof.

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$$

= [definition of *VD* (8.19)]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

= [meaning of ∀, a ∧ a ⇔ a]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$
$$\mathbf{(}\ K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$\mathbf{(}\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\ \mathbf{)}$$ ■

Lemma A.9.

$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge NV_{Op}([p], [q]) \Rightarrow$$
$$\mathbf{(}\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])\ \mathbf{)}$$

Proof.

$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge NV_{Op}([p], [q])$$

= [definition of *NV* (8.18)]

$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$\mathbf{(}\ \forall\ \underline{p}, o, u', \underline{v}', i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet$$
$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]))\ \mathbf{)}$$

= [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$\mathbf{(}\ \underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]))\ \mathbf{)} \wedge$$
$$\mathbf{(}\ \forall\ \underline{p}, o, u', \underline{v}', i, \underline{j}, u, \underline{v}, v', w', j, k, v, w \bullet$$
$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$

$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$\mathbf{(}\ \underline{p} \in [p] \wedge N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]))\ \mathbf{)}$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$\mathbf{(}\ \exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge V_{Op}(o, \underline{q}) \wedge$$
$$K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])\ \mathbf{)} \qquad \blacksquare$$

Lemma A.10.

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \Rightarrow RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$$

Proof.

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])$$

= [definition of *VN* (8.17)]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$
$$(\ (\forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})))\ )$$

= [$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N \wedge H' \wedge Q \wedge H) \Leftrightarrow$
$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N \wedge H' \wedge Q \wedge H) \wedge (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q \wedge H)$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$
$$\mathbf{(}\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\ \mathbf{(}\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\ \wedge$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )\ )$$

$=$ [meaning of $\forall$, $(a \Rightarrow (b \wedge c)) \Leftrightarrow ((a \Rightarrow b) \wedge (a \Rightarrow c))$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$

$$(\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )\ \wedge$$

$$(\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$

$$(\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$

$$(\ \forall\, i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )\ \wedge$$

$$(\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge$$

$$(\ \forall\, i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \ \Leftrightarrow\ a \wedge (b \Rightarrow c)$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge (\ \forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$(\ \forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$\Rightarrow$ [(8.14)]

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$ ■

Lemma A.11.

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))$$

Proof.

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])$$

$=$ [definition of *VN* (8.17)]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ \forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$
$$\mathbf{(}\ V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$\mathbf{(}\ V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$\mathbf{(}\ \exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\ \mathbf{)} \qquad \blacksquare$$

Lemma A.12.

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v]) \Rightarrow KH(\underline{w}', [v'])$$

Proof.

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VN_{Op}(\underline{q}, \underline{w}', \underline{k}, \underline{w}, [p], [v'], [j], [v])$$

$=$ [definition of VN (8.17)]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$(\ (\forall\ o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ )$$

$=$ [$\mathbf{(}\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N \wedge H' \wedge Q \wedge H\mathbf{)} \Leftrightarrow$

$\mathbf{(}\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N \wedge H' \wedge Q \wedge H\mathbf{)} \wedge \mathbf{(}\exists\ \underline{v}' \bullet \underline{v}' \in [v'] \wedge H'\mathbf{)}$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$\mathbf{(}\ \forall\ o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\ \mathbf{(}\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})\mathbf{)}\ \wedge$$

$$\mathbf{(}\exists\ \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}')\mathbf{)}\ )\ \mathbf{)}$$

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$\mathbf{(}\ \forall\ o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$N_{Op}(o, \underline{p}; u', \underline{v}', i, \underline{j}, u, \underline{v}) \wedge H(u', \underline{v}') \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\ o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\qquad (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ )$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, u' \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\qquad (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ ) \wedge$

$\quad (\forall\, o, u', i, u \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\qquad (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ )$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, u' \bullet V_{Op}(o, \underline{q}) \wedge K(u', \underline{w}') \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\qquad (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ )$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $(a \wedge (a \wedge b \Rightarrow c)) \Leftrightarrow (a \wedge (b \Rightarrow c))$]

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, u' \bullet K(u', \underline{w}') \Rightarrow (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ )$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$(\forall\, u' \bullet K(u', \underline{w}') \Rightarrow (\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge H(u', \underline{v}'))\ )$

$\Rightarrow$ [(8.10)]

$KH(\underline{w}', [v'])$ ■

Lemma A.13.

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \Rightarrow KD_{Op}(\underline{w}', [v'])$$

Proof.

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$

$=$ [definition of *VD* (8.19)]

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$$((\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))))$$

$= [\, (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D \wedge Q \wedge H) \Leftrightarrow$

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D \wedge Q \wedge H) \wedge$

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D) \,]$

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$((\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v})) \wedge$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))))$$

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge H(u, \underline{v}))) \wedge$$
$$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})))$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$
$$(\forall\, u' \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) \wedge$$
$$(\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$\mathbf{(}\ \forall\, u' \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $(a \wedge (a \wedge b \Rightarrow c)) \Leftrightarrow (a \wedge (b \Rightarrow c))$]

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$\mathbf{(}\ \forall\, u' \bullet K(u', \underline{w}') \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$(\ \forall\, u' \bullet K(u', \underline{w}') \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ )$$

$\Rightarrow$ [$\mathbf{(}\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D\mathbf{)} \Leftrightarrow$

$\mathbf{(}\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D\mathbf{)} \wedge \mathbf{(}\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge (\exists\, o, p, i, j, u, v \bullet D)\mathbf{)}$]

$$(\ \forall\, u' \bullet K(u', \underline{w}') \Rightarrow$$

$$(\exists\, \underline{v}' \bullet \underline{v}' \in [v'] \wedge (\exists\, o, p, i, j, u, v \bullet D_{Op}(u', \underline{v}', o, p; i, j, u, v)))\ )$$

$\Rightarrow$ [(8.12)]

$$KD_{Op}(\underline{w}', [v']) \qquad \blacksquare$$

Appendix B

Prejoin Composition Proofs

B.1 Composition Proofs

In Section 9.4.4.1 we defined the retrieve, within, output and concedes relations, G, P_{Op}, O_{Op} and C_{Op} respectively, for the retrenchment from *Univ* to *Conc*. In this section we show that the two compositions given for each relation, which correspond to the two paths around the square from *Univ* to *Conc* in Figure 9.1, are equal. To simplify the proofs, we assume that $\mathsf{Ops}_{\mathrm{C}}$ only has one operation.

♦ (9.49): $G = H^{\bullet} ⨾ K = K^{\bullet} ⨾ H$.

Proof. We expand each part in turn. Take $H^{\bullet} ⨾ K$ first.

$H^{\bullet}(([v], [w]), \underline{v}) ⨾ K(\underline{v}, t)$

= [definition of composition]

$\mathbf{(} \exists\, \underline{v} \bullet H^{\bullet}(([v], [w]), \underline{v}) \wedge K(\underline{v}, t) \mathbf{)}$

= [definition of $H^{\bullet}$ (9.22)]

$\mathbf{(} \exists\, \underline{v} \bullet \underline{v} \in [v] \wedge (\exists\, t \bullet K(\underline{v}, t)) \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge K(\underline{v}, t) \mathbf{)}$

= [$K(\underline{v}, t) \wedge (\exists\, t \bullet K(\underline{v}, t)) \Leftrightarrow K(\underline{v}, t)$]

$\mathbf{(} \exists\, \underline{v} \bullet \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge K(\underline{v}, t) \mathbf{)}$

= [Lemma B.1]

$\mathbf{(} \exists\, \underline{v} \bullet \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge K(\underline{v}, t) \wedge$

$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t)) \mathbf{)}$

= [rewriting in prenex normal form, rearranging]

$$(\exists\, \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge K(\underline{v}, t) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w]))$$

Now for $K^{\bullet} ⨾ H$.

$$K^{\bullet}(([v], [w]), \underline{w}) ⨾ H(\underline{w}, t)$$

= [definition of composition]

$$(\exists\, \underline{w} \bullet K^{\bullet}(([v], [w]), \underline{w}) \wedge H(\underline{w}, t))$$

= [definition of $K^{\bullet}$ (9.21)]

$$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge H(\underline{w}, t))$$

= [Lemma B.5]

$$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge H(\underline{w}, t) \wedge (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w]))$$

= [rewriting in prenex normal form, rearranging]

$$(\exists\, \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge K(\underline{v}, t) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w]))\ .$$

Hence $H^{\bullet} ⨾ K = K^{\bullet} ⨾ H$. ■

♦ (9.50): $P_{Op} = (Q^{\bullet}{}_{Op} \wedge H^{\bullet}) ⨾ (R_{Op} \wedge K) = (R^{\bullet}{}_{Op} \wedge K^{\bullet}) ⨾ (Q_{Op} \wedge H)$.

Proof. We expand each part in turn. Take $(Q^{\bullet}{}_{Op} \wedge H^{\bullet}) ⨾ (R_{Op} \wedge K)$ first.

$$(Q^{\bullet}{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v})) ⨾ (R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$$

= [definition of composition]

$$(\exists\, \underline{v}, \underline{j} \bullet Q^{\bullet}{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v}) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$$

= [definition of $Q^{\bullet}$ (9.24)]

$$(\exists\, \underline{v}, \underline{j} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge (\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge H^{\bullet}(([v], [w]), \underline{v}) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$$

= [$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge (\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \Leftrightarrow R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$]

$$(\exists\, \underline{v}, \underline{j} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$
$$H^{\bullet}(([v], [w]), \underline{v}) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\,)$$

= [Lemma B.2]

$$(\exists\, \underline{v}, \underline{j} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$
$$H^{\bullet}(([v], [w]), \underline{v}) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$
$$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\,)$$

= [rewriting in prenex normal form]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$
$$H^{\bullet}(([v], [w]), \underline{v}) \wedge$$
$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$$

= [definition of $H^{\bullet}$ (9.22)]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$
$$\underline{v} \in [v] \wedge (\exists\, t \bullet K(\underline{v}, t)) \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$
$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$$

= [$K(\underline{v}, t) \wedge (\exists\, t \bullet K(\underline{v}, t)) \Leftrightarrow K(\underline{v}, t)$]

$$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$
$$\underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$
$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$$

= [rearranging, a $\wedge$ a $\Leftrightarrow$ a]

$$(\exists\, \underline{k}, \underline{w}, \underline{j}, \underline{v} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge QR_{Op}([j], [k]) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge$$
$$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w])\,)$$

Now for $(R^{\bullet}_{Op} \wedge K^{\bullet})\fatsemi(Q_{Op} \wedge H)$.

$$(R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}))\fatsemi(Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$$

= [definition of composition]

$$(\exists\, \underline{w}, \underline{k} \bullet R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$$

= [definition of $R^{\bullet}$ (9.23)]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ \mathbf{)}$$

= [Lemma B.6]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k} \bullet \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))\ \mathbf{)}$$

= [rewriting in prenex normal form]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$

$$K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$

$$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])\ \mathbf{)}$$

= [definition of $K^{\bullet}$ (9.21)]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$

$$\underline{w} \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$

$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$

$$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])\ \mathbf{)}$$

= [Lemma B.8]

$$\mathbf{(}\ \exists\ \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$$

$$\underline{w} \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$$

$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$

$$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge KH(\underline{v}, [w])\ \mathbf{)}$$

= [rearranging]

$$\mathbf{(}\ \exists\ \underline{k}, \underline{w}, \underline{j}, \underline{v} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge QR_{Op}([j], [k]) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge$$

$$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w])\ \mathbf{)}$$

Hence $(Q^{\bullet}_{Op} \wedge H^{\bullet})\fatsemi(R_{Op} \wedge K) = (R^{\bullet}_{Op} \wedge K^{\bullet})\fatsemi(Q_{Op} \wedge H)$. ■

♦ (9.51): $O_{Op} = (N^{\bullet}_{Op} \wedge H^{\bullet\prime} \wedge Q^{\bullet}_{Op} \wedge H^{\bullet})\fatsemi(V_{Op} \wedge K' \wedge R_{Op} \wedge K)$

$= (V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})\fatsemi(N_{Op} \wedge H' \wedge Q_{Op} \wedge H)$.

Proof. We expand each part in turn. Take $(N^{\bullet} \wedge H^{\bullet\prime} \wedge Q^{\bullet} \wedge H^{\bullet})\fatsemi(V \wedge K' \wedge R \wedge K)$ first.

$$\begin{aligned}
&\mathbf{(}N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
&\quad H^{\bullet}(([v'], [w']), \underline{v}') \wedge Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v})\mathbf{)}\fatsemi \\
&\qquad \mathbf{(}V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \\
&= \text{[definition of composition]} \\
&\mathbf{(}\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet N^{\bullet}_{Op}(([p], [q]), \underline{p}; ([v'], [w']), \underline{v}', ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
&\quad H^{\bullet}(([v'], [w']), \underline{v}') \wedge Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^{\bullet}(([v], [w]), \underline{v}) \wedge \\
&\quad V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ \mathbf{)} \\
&= \text{[definition of } N^{\bullet} \text{ (9.26), } Q^{\bullet} \text{ (9.24) and } H^{\bullet\prime}, H^{\bullet} \text{ (9.22)]} \\
&\mathbf{(}\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad \mathbf{(}\exists\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \wedge \\
&\quad VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad \underline{v}' \in [v'] \wedge \mathbf{(}\exists\, t' \bullet K(\underline{v}', t')\mathbf{)} \wedge KH(\underline{v}', [w']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \\
&\quad \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \mathbf{(}\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge \\
&\quad QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge \mathbf{(}\exists\, t \bullet K(\underline{v}, t)\mathbf{)} \wedge KH(\underline{v}, [w]) \wedge \\
&\quad HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ \mathbf{)} \\
&= [\ V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge (\exists\, V \wedge K' \wedge R \wedge K) \wedge (\exists\, K') \wedge (\exists\, R \wedge K) \wedge (\exists\, K) \Leftrightarrow \\
&\qquad V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ ] \\
&\mathbf{(}\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad \underline{v}' \in [v'] \wedge KH(\underline{v}', [w']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge \\
&\quad HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ \mathbf{)}
\end{aligned}$$

= [Lemma B.3]

$$\begin{aligned}
&\mathbf{(}\ \exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad \underline{v}' \in [v'] \wedge KH(\underline{v}', [w']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge \\
&\quad HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \\
&\quad (\ \exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \\
&\qquad N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ )\ \mathbf{)}
\end{aligned}$$

= [rewriting in prenex normal form]

$$\begin{aligned}
&\mathbf{(}\ \exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v}, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad \underline{v}' \in [v'] \wedge KH(\underline{v}', [w']) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge \\
&\quad HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \\
&\quad \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge \\
&\quad Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ )
\end{aligned}$$

= [rearranging, a ∧ a ⇔ a]

$$\begin{aligned}
&\mathbf{(}\ \exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{p} \in [p] \wedge \\
&\quad \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge \\
&\quad Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \\
&\quad NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge \\
&\quad HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge KH(\underline{v}', [w']) \wedge QR_{Op}([j], [k]) \wedge \\
&\quad RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w])\ \mathbf{)}
\end{aligned}$$

Now for $(V^{\bullet}_{Op} \wedge K^{\bullet\prime} \wedge R^{\bullet}_{Op} \wedge K^{\bullet})\fatsemi(N_{Op} \wedge H' \wedge Q_{Op} \wedge H)$.

$$\begin{aligned}
&\mathbf{(}V^{\bullet}_{Op}(([p], [q]), \underline{q}) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})\mathbf{)}\fatsemi \\
&\quad \mathbf{(}N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\mathbf{)}
\end{aligned}$$

= [definition of composition]

$$\mathbf{(}\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet V^{\bullet}_{Op}(([p], [q]), \underline{q}) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge$$
$$K^{\bullet}(([v], [w]), \underline{w}) \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ \mathbf{)}$$

= [definition of $V^{\bullet}$ (9.25)]

$$\mathbf{(}\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge$$
$$R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge$$
$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ \mathbf{)}$$

= [Lemma B.7]

$$\mathbf{(}\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge$$
$$R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge$$
$$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$\mathbf{(}\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$
$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])\mathbf{)}\ \mathbf{)}$$

= [rewriting in prenex normal form]

$$(\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge$$
$$K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])\ )$$

= [Lemma B.12]

$$(\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge$$
$$K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge KH(\underline{v}', [w'])\ )$$

= [Lemma B.10]

$$(\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$$

$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge$

$K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge KH(\underline{v}', [w']) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))$

= [Lemma B.9]

$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge$

$K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge KH(\underline{v}', [w']) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge$

$KH(\underline{v}, [w]))$

= [definition of $K^{\bullet}$, $K^{\bullet\prime}$ (9.21) and $R^{\bullet}$ (9.23)]

$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$\underline{w}' \in [w'] \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge$

$T_{Op}([k]) \wedge w \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$\underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge$

$K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge KH(\underline{v}', [w']) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge$

$KH(\underline{v}, [w]))$

= [rearranging]

$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w}, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{p} \in [p] \wedge$

$\underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

$NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge KH(\underline{v}', [w']) \wedge QR_{Op}([j], [k]) \wedge$

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge KH(\underline{v}, [w]))$

Hence $(N^\bullet \wedge H^{\bullet\prime} \wedge Q^\bullet \wedge H^\bullet) ⨾ (V \wedge K' \wedge R \wedge K) = (V^\bullet \wedge K^{\bullet\prime} \wedge R^\bullet \wedge K^\bullet) ⨾ (N \wedge H' \wedge Q \wedge H)$. ■

♦ (9.52): $C_{Op} = (D^\bullet{}_{Op} \wedge Q^\bullet{}_{Op} \wedge H^\bullet) ⨾ (K' \wedge V_{Op} \wedge R_{Op} \wedge K)$
$= (K^{\bullet\prime} \wedge V^\bullet{}_{Op} \wedge R^\bullet{}_{Op} \wedge K^\bullet) ⨾ (D_{Op} \wedge Q_{Op} \wedge H)$.

Proof. We expand each part in turn. Take $(D^\bullet{}_{Op} \wedge Q^\bullet{}_{Op} \wedge H^\bullet) ⨾ (K' \wedge V_{Op} \wedge R_{Op} \wedge K)$ first.

$$\begin{aligned}
&\mathbf{(}D^\bullet{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
&\quad Q^\bullet{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^\bullet(([v], [w]), \underline{v})\mathbf{)} ⨾ \\
&\quad \mathbf{(}K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \\
&= \text{[definition of composition]} \\
&\mathbf{(}\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet D^\bullet{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\
&\quad Q^\bullet{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge H^\bullet(([v], [w]), \underline{v}) \wedge \\
&\quad K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \\
&= \text{[definition of } D^\bullet \text{ (9.27), } Q^\bullet \text{ (9.24) and } H^\bullet \text{ (9.22)]} \\
&\mathbf{(}\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad \mathbf{(}\exists\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \wedge \\
&\quad VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \\
&\quad \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \mathbf{(}\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \wedge \\
&\quad RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \\
&\quad \underline{v} \in [v] \wedge \mathbf{(}\exists\, t \bullet K(\underline{v}, t)\mathbf{)} \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \\
&\quad K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ \mathbf{)} \\
&= [K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge (\exists\, t', s, h, t \bullet K' \wedge V \wedge R \wedge K) \wedge (\exists\, h, t \bullet R \wedge K) \wedge (\exists\, t \bullet K) \Leftrightarrow \\
&\quad K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\ ] \\
&\mathbf{(}\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
&\quad VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \\
&\quad HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge \\
&\quad QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge
\end{aligned}$$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$ **)**

= [Lemma B.4]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge$

$QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$ **)**

= [rewriting in prenex normal form]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge$

$QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)$ **)**

= [rearranging, a ∧ a ⇔ a]

($\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{v}' \in [v'] \wedge$

$\underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

$QR_{Op}([j], [k]) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$KH(\underline{v}, [w])\,)$

Now for $(K^{\bullet\prime} \wedge V^{\bullet} \wedge R^{\bullet} \wedge K^{\bullet})\fatsemi(D_{Op} \wedge Q_{Op} \wedge H)$.

($K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}{}_{Op}(([p], [q]), \underline{q}) \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})$**)**$\fatsemi$

$(D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$

= [definition of composition]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}_{Op}(([p], [q]), \underline{q}) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge$

$K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$

= [definition of $V^{\bullet}$ (9.25)]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,)$

= [Lemma B.8]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge$

$R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))\,)$

= [rewriting in prenex normal form]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])\,)$

= [Lemma B.11]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])\,)$

= [Lemma B.9]

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet K^{\bullet}(([v'], [w']), \underline{w}') \wedge \underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge$

$DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge KH(\underline{v}, [w])\ )$

= [definition of $K^{\bullet}$, $K^{\bullet\prime}$ (9.21) and $R^{\bullet}$ (9.23)]

$(\ \exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{w}' \in [w'] \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$\underline{q} \in [q] \wedge NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge \underline{k} \in [k] \wedge QR_{Op}([j], [k]) \wedge T_{Op}([k]) \wedge$

$\underline{w} \in [w] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge KH(\underline{v}, [w])\ )$

= [rearranging]

$(\ \exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \underline{v}' \in [v'] \wedge$

$\underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$NV_{Op}([p], [q]) \wedge DV_{Op}([p], [q]) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

$QR_{Op}([j], [k]) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge T_{Op}([k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$KH(\underline{v}, [w])\ )$

Hence $(D^{\bullet} \wedge Q^{\bullet} \wedge H^{\bullet}) \fatsemi (K' \wedge V \wedge R \wedge K) = (K^{\bullet\prime} \wedge V^{\bullet} \wedge R^{\bullet} \wedge K^{\bullet}) \fatsemi (D \wedge Q \wedge H)$. ■

This completes the proofs for the compositions.

B.2 Lemmas

Lemma B.1. $K(\underline{v}, t) \wedge KH(\underline{v}, [w]) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))$

Proof.

$K(\underline{v}, t) \wedge KH(\underline{v}, [w])$

= [definition of KH (9.10)]

$K(\underline{v}, t) \wedge (\forall\ t \bullet K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t)))$

= [meaning of ∀, a ∧ a ⇔ a]

$K(\underline{v}, t) \wedge (K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))) \wedge$

$(\forall\ t \bullet K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t)))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$K(\underline{v}, t) \wedge (K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t)))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))$ ■

Lemma B.2.

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \Rightarrow$
$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$

Proof.

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$

= [definition of *RQ* (9.14)]

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$(\ \forall\ h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )$

= [meaning of ∀, a ∧ a ⇔ a]

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$(R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))) \wedge$

$(\forall\ h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$(R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))$

$\Rightarrow$ [$((a \wedge b) \wedge (a \Rightarrow c)) \Rightarrow c$]

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$ ■

Lemma B.3.

$$V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$$

Proof.

$$V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])$$

= [definition of *VN* (9.16)]

$$V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$
$$\mathbf{(}\ \forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

= [meaning of ∀, a ∧ a ⇔ a]

$$V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$
$$\mathbf{(}\ \forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)} \wedge$$
$$\mathbf{(}\ V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

⇒ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$
$$\mathbf{(}\ V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

⇒ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$\mathbf{(}\ \exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\ \mathbf{)} \qquad \blacksquare$$

Lemma B.4.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \Rightarrow$$

$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$$

Proof.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])$$

= [definition of *VD* (9.18)]

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

= [meaning of ∀, a ∧ a ⇔ a]

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

⇒ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$$

$$\mathbf{(}\ K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$(\exists\, \underline{w'}, \underline{q}, \underline{k}, \underline{w} \bullet \underline{w'} \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\,) \qquad \blacksquare$$

Lemma B.5.

$$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge HK([v], [w]) \;\Rightarrow\; (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w]))$$

Proof.

$$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge HK([v], [w])$$

$=$ [definition of HK (9.11)]

$$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge$$
$$(\forall\, \underline{w}, t \bullet \underline{w} \in [w] \wedge H(\underline{w}, t) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w])))$$

$=$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge$$
$$(\underline{w} \in [w] \wedge H(\underline{w}, t) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w]))) \wedge$$
$$(\forall\, \underline{w}, t \bullet \underline{w} \in [w] \wedge H(\underline{w}, t) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w])))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge (\underline{w} \in [w] \wedge H(\underline{w}, t) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w])))$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$(\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KH(\underline{v}, [w])) \qquad \blacksquare$$

Lemma B.6.

$$\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge QR_{Op}([j], [k]) \Rightarrow$$
$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))$$

Proof.

$$\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge QR_{Op}([j], [k])$$

$=$ [definition of QR (9.15)]

$$\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$(\forall\ \underline{k}, h, \underline{w}, t, v, w \bullet \underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))$$

= [meaning of ∀, a ∧ a ⇔ a]

$$\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$(\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))) \wedge$$
$$(\forall\ \underline{k}, h, \underline{w}, t, v, w \bullet \underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))$$

⇒ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$(\underline{k} \in [k] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))$$

⇒ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))$$ ■

Lemma B.7.

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge NV_{Op}([p], [q]) \Rightarrow$$
$$(\exists\ \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$
$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]))$$

Proof.

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge NV_{Op}([p], [q])$$

= [definition of *NV* (9.17)]

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$(\forall\ \underline{q}, s, \underline{w}', t', \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$
$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$

$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]))$$

= [meaning of ∀, a ∧ a ⇔ a]

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$(\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$

$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]))) \wedge$$

$$(\forall\, \underline{q}, s, \underline{w}', t', \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$

$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$

$$(\underline{q} \in [q] \wedge N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$

$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge$$

$$K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]))$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$(\exists\, \underline{p}, \underline{v}', \underline{j}, \underline{v} \bullet \underline{p} \in [p] \wedge \underline{v}' \in [v'] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge$$

$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])) \qquad \blacksquare$$

Lemma B.8.

$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge DV_{Op}([p], [q]) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))$$

Proof.

$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge DV_{Op}([p], [q])$$

= [definition of *DV* (9.19)]

$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$(\forall\, \underline{q}, \underline{w}', t', s, \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$
$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))$$

= [meaning of ∀, a ∧ a ⇔ a]

$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$$
$$(\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))) \wedge$$
$$(\forall\, \underline{q}, \underline{w}', t', s, \underline{k}, h, \underline{w}, t, v', w', j, k, v, w \bullet$$
$$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$$
$$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

$(\underline{q} \in [q] \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t) \wedge$

$K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))$ ■

Lemma B.9. $R_{Op}(\underline{j}, h) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \Rightarrow KH(\underline{v}, [w])$

Proof.

$R_{Op}(\underline{j}, h) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$

= [definition of RQ (9.14)]

$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))$)

= [$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \Leftrightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \wedge (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))$]

$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$(\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$((\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \wedge$

$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))$))

= [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$(\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \wedge$

$$\mathbf{(}\ \forall\ h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \mathbf{(}\ \forall\ h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \mathbf{(}\ \forall\ t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\ h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \mathbf{(}\ \forall\ t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \Leftrightarrow a \wedge (b \Rightarrow c)$]

$$R_{Op}(\underline{j}, h) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \mathbf{(}\ \forall\ t \bullet K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$\mathbf{(}\ \forall\ t \bullet K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ \mathbf{)}$$

$\Rightarrow$ [(9.10)]

$$KH(\underline{v}, [w])$$ ■

Lemma B.10.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \Rightarrow RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$$

Proof.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])$$

$=$ [definition of *VN* (9.16)]

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$(\ \forall\ s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$\mathbf{(}\exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$

$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\mathbf{)}\ )$$

$=$ [$\mathbf{(}\exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N \wedge H' \wedge Q \wedge H\mathbf{)} \Leftrightarrow$

$\mathbf{(}\exists\ \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N \wedge H' \wedge Q \wedge H\mathbf{)} \wedge$

$\mathbf{(}\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q \wedge H\mathbf{)}$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\,(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$\quad\quad\quad N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \wedge$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )\ )$

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$\quad\quad\quad N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ ) \wedge$

$\quad (\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ ) \wedge$

$\quad (\forall\, t', s, h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ )$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \;\Leftrightarrow\; a \wedge (b \Rightarrow c)$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\,)$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\,)$

$\Rightarrow$ [(9.14)]

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$ ■

Lemma B.11.

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \Rightarrow RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$

Proof.

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])$

$=$ [definition of *VD* (9.18)]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\qquad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$\qquad\quad D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\,)$

$=$ [$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge D \wedge Q \wedge H) \Leftrightarrow$

$\quad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge D \wedge Q \wedge H) \wedge (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q \wedge H)$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$\quad (\forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\qquad (\,(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$\qquad\quad D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \wedge$

$\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\,)\,)$

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$

$$\begin{aligned}
&\mathbf{(}\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge \\
&\qquad\qquad D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)} \wedge \\
&\mathbf{(}\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}
\end{aligned}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$\begin{aligned}
&K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \\
&\quad \mathbf{(}\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}
\end{aligned}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$\begin{aligned}
&K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \\
&\quad \mathbf{(}\ \forall\, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)} \wedge \\
&\quad \mathbf{(}\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}
\end{aligned}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\begin{aligned}
&K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \\
&\quad \mathbf{(}\ \forall\, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}
\end{aligned}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \ \Leftrightarrow\ a \wedge (b \Rightarrow c)$]

$$\begin{aligned}
&K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge \\
&\quad \mathbf{(}\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\qquad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t))\ \mathbf{)}
\end{aligned}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$\begin{aligned}
&trm_{Op_T}(\underline{v}, \underline{j}) \wedge (\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow \\
&\quad \mathbf{(}\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)\mathbf{)}\ )
\end{aligned}$$

$\Rightarrow$ [(9.14)]

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$ ■

Lemma B.12.

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w]) \Rightarrow KH(\underline{v}', [w'])$$

Proof.

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VN_{Op}(\underline{p}, \underline{v}', \underline{j}, \underline{v}, [q], [w'], [k], [w])$$

= [definition of *VN* (9.16)]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$
$$(\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)))$$

= [$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N \wedge H' \wedge Q \wedge H) \Leftrightarrow$
$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge N \wedge H' \wedge Q \wedge H) \wedge (\exists\, \underline{w}' \bullet \underline{w}' \in [w'] \wedge H')$]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$
$$(\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$((\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \wedge$$
$$(\exists\, \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t')))$$

= [meaning of $\forall$, $a \Rightarrow (b \wedge c) \Leftrightarrow (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$
$$(\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{q}, \underline{w}', \underline{k}, \underline{w} \bullet \underline{q} \in [q] \wedge \underline{w}' \in [w'] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$N_{Op}(\underline{q}, s; \underline{w}', t', \underline{k}, h, \underline{w}, t) \wedge H(\underline{w}', t') \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge H(\underline{w}, t)) \wedge$$
$$(\forall\, s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$
$$(\exists\, \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge c$]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ t' \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\ s, t', h, t \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ t' \bullet V_{Op}(\underline{p}, s) \wedge K(\underline{v}', t') \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

$$(\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, a $\wedge$ a $\Leftrightarrow$ a, $a \wedge (a \wedge b \Rightarrow c) \Leftrightarrow a \wedge (b \Rightarrow c)$]

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge trm_{Op_T}(\underline{v}, \underline{j}) \wedge$$

$$\mathbf{(}\ \forall\ t' \bullet K(\underline{v}', t') \Rightarrow (\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$\mathbf{(}\ \forall\ t' \bullet K(\underline{v}', t') \Rightarrow (\exists\ \underline{w}' \bullet \underline{w}' \in [w'] \wedge H(\underline{w}', t'))\ \mathbf{)}$$

$\Rightarrow$ [(9.10)]

$$KH(\underline{v}', [w']) \qquad \blacksquare$$

Bibliography

[Abr96] J.-R. Abrial. *The B-Book: Assigning Programs to Meanings*. Cambridge University Press, 1996.

[Bac80] R. J. R. Back. Correctness Preserving Program Refinement: Proof Theory and Applications. Technical Report 131, Mathematical Centre, Amsterdam, 1980.

[Bac88] R. J. R. Back. A Calculus of Refinements for Program Derivations. *Acta Informatica*, 25:593-624, 1988.

[Ban] R. Banach. Retrenchment: an overview. (no date). [online: http://www.cs.man.ac.uk/retrenchment/Retrenchment.TUTORIAL.pdf] (retrieved 1 Jun 2005).

[Ban00] R. Banach. Maximally Abstract Retrenchments. In *Proceedings IEEE ICFEM2000*, pages 133-142, IEEE Computer Society Press, 2000.

[Ban03] R. Banach. Retrenchment and System Properties, 2003. Submitted. [online: http://www.cs.man.ac.uk/~banach/some.pubs/Retrench.Props.pdf] (retrieved 1 Jun 2005).

[BBFM99] P. Behm, P. Benoit, A. Faivre and J.-M. Meynadier. MÉTÉOR: A successful application of B in a large project. In J. M. Wing, J. Woodcock and J. Davies (eds.), *Proceedings of FM'99: World Congress on Formal Methods, Lecture Notes in Computer Science*, 1709:369-387, Springer, 1999.

[BC04] R. Banach and R. Cross. Safety Requirements and Fault Trees using Retrenchment. In M. Heisel, P. Liggesmeyer and S. Wittmann (eds.), *Proceedings SAFECOMP'04, Lecture Notes in Computer Science*, 3219:210-223, Springer, 2004.

[BD98] E. Boiten and J. Derrick. IO-refinement in Z. In A. Evans, D. Duke and T. Clark (eds.), *Third BCS-FACS Northern Formal Methods Workshop*, Springer-Verlag, September 1998.

[BD05] E. Boiten and J. Derrick. Formal Program Development with Approximations. In H. Treharne, S. King, M. Henson and S. Schneider (eds.), *ZB 2005, Lecture Notes in Computer Science*, 3455:375-393. Springer, April 2005.

[BDGK00] J. P. Bowen, S. Dunne, A. Galloway and S. King (eds.), *Proceedings ZB2000: Formal Specification and Development in Z and B, Lecture Notes in Computer Science*, volume 1878, Springer, 2000.

[BDM00] P. Behm, P. Desforges and Meynadier J-M. Météor: An industrial success in formal development. In Bowen et al. [BDGK00], pages 374-393.

[BdR03] E. Boiten and W.-P. de Roever. Getting to the Bottom of Relational Refinement: Relations and Correctness, Partial and Total. In R. Berghammer and B. Moller (eds.), *7th International Seminar on Relational Methods in Computer Science (RelMiCS 7)*, pages 82-88. University of Kiel, May 2003.

[BDW98] C. Bolton, J. Davies and J. Woodcock. On the refinement and simulation of data types and processes. In K. Araki, A. Galloway and K. Taguchi (eds.), *Proceedings of IFM '99*, Springer, 1999.

[BJ02] R. Banach and C. Jeske. Output Retrenchments, Defaults, Stronger Compositions, Feature Engineering. 2002. Submitted. [online: http://www.cs.man.ac.uk/~banach/some.pubs/Retrench.Composition.pdf]

[Bjø05] D. Bjørner. *Software Engineering 1: Abstraction and Modelling.* Springer-Verlag, 2005.

[BJP04] R. Banach, C. Jeske and M. Poppleton. Composition Mechanisms for Retrenchment. 2004. [online: http://www.cs.man.ac.uk/~banach/some.pubs/Retrench.Composition.pdf]

[BJPS] R. Banach, C. Jeske, M. Poppleton and S. Stepney. Retrenchment and Mondex. (no date). [online: http://www.cs.man.ac.uk/retrenchment/Retrenchment.MONDEX.pdf] (retrieved 1 Jun 2005).

[BP98] R. Banach and M. Poppleton. Retrenchment: An Engineering Variation on Refinement. In Bert (ed.), *Proceedings B'98*, *Lecture Notes in Computer Science*, 1393:129-147, Springer, 1998. See also UMCS Technical Report, UMCS-99-3-2, [online: http://www.cs.man.ac.uk/cstechrep].

[BP99] R. Banach and M. R. Poppleton. Sharp Retrenchment, Modulated Refinement and Punctured Simulation. *Formal Aspects of Computing*, 11:498-540, 1999.

[BP01] R. Banach and M. Poppleton. Some Engineering and Theoretical Underpinnings of Retrenchment, 2001. Submitted. [online: http://www.cs.man.ac.uk/~banach/some.pubs/Retrench.Some.Underpin.pdf]

[BP03] R. Banach and M. Poppleton. Retrenching partial requirements into system definitions: a simple feature interaction case study. *Requirements Engineering Journal*, 8(4): 266-288, 2003.

[BPJ04] R. Banach, M. Poppleton and C. Jeske. Retrenchment and Promotion in Z, 2004. Unpublished.

[BPJS05a] R. Banach, M. Poppleton, C. Jeske and S. Stepney. Retrenching the Purse: Finite Sequence Numbers and the Tower Pattern. In J. Fitzgerald, I. Hayes and A. Tarlecki (eds.) *Proceedings FM'05, Lecture Notes in Computer Science*, 3582:382-398, Springer, 2005.

[BPJS05b] R. Banach, M. Poppleton, C. Jeske and S. Stepney. Retrenching the Purse: Finite Exception Logs, and Validating the Small. 2005. Submitted.

[BPJS05c] R. Banach, M. Poppleton, C. Jeske and S. Stepney. Retrenching the Purse: Hashing Injective CLEAR Codes, and Security Properties. 2005. Submitted.

[BPJS05d] R. Banach, M. Poppleton, C. Jeske and S. Stepney. Retrenching the Purse: The Balance Enquiry Quandary, and Generalised and (1,1) Forward Refinements. 2005. Submitted.

[BSC94] R. Barden, S. Stepney and D. Cooper. *Z in Practice. BCS Practitioners Series*. Prentice Hall, 1994.

[BvW98] R. J. R. Back and J. von Wright. *Refinement Calculus: A Systematic Introduction.* Springer, 1998.

[CSC05] J. A. Clark, S. Stepney and H. Chivers. Breaking the Model: finalisation and a taxonomy of security attacks. *REFINE 2005 workshop. Electronic Notes in Theoretical Computer Science*, Elsevier, 2005.

[CSW02] D. Cooper, S. Stepney and J. Woodcock. Derivation of Z Refinement Proof Rules. *Technical Report YCS-2002-347*, University of York, December 2002.

[DB99] J. Derrick and E. Boiten. Non-atomic refinement in Z. In J. M. Wing, J. C. P. Woodcock and J. Davies (eds.), *FM'99 World Congress on Formal Methods in the Development of Computing Systems, Lecture Notes in Computer Science*, 1708:1477-1496, Springer-Verlag, 1999.

[DB01] J. Derrick and E. Boiten. *Refinement in Z and Object-Z. FACIT*. Springer, 2001.

[DH03a] M. Deutsch and M. C. Henson. An analysis of forward simulation data refinement. In D. Bert, J. Bowen, S. King and M. Waldén (eds.), *ZB2003: Formal Specification and Development in Z and B, Lecture Notes in Computer Science*, 2651:148-167, Springer-Verlag, 2003.

[DH03b] M. Deutsch and M. C. Henson. An Analysis of Backward Simulation Data-Refinement for Partial Relation Semantics. In *10th Asia-Pacific Software Engineering Conference (APSEC 2003)*, pages 38 - 48, IEEE Computer Society Press, December 2003.

[DHR02] M. Deutsch, M. C. Henson and S. Reeves. Results in Formal Stepwise Design in Z. In *9th Asia-Pacific Software Engineering Conference (APSEC 2002)*, pages 33 - 42, IEEE Computer Society Press, December 2002.

[DHR03a] M. Deutsch, M. C. Henson, and S. Reeves. An analysis of total correctness refinement models for partial relation semantics I. *Logic Journal of the IGPL*, 11(3):287-317, 2003.

[DHR03b] M. Deutsch, M. C. Henson, and S. Reeves. An analysis of total correctness refinement models for partial relation semantics II. *Logic Journal of the IGPL*, 11(3):319-352, 2003.

[Dij75] E. W. Dijkstra. Guarded commands, nondeterminacy and formal derivation of programs. *Communications of the ACM*, 18:453-457, 1975.

[Dij76] E. W. Dijkstra. *A Discipline of Programming.* Prentice-Hall, 1976.

[dRE98] W.-P. de Roever and K. Engelhardt. *Data Refinement: Model-Oriented Proof Methods and their Comparison.* Cambridge University Press, 1998.

[DTI91] Department of Trade and Industry. *Information Technology Security Evaluation Criteria*. 1991. [online: http://www.cesg.gov.uk/site/iacs/itsec/media/formal-docs/Itsec.pdf]

[FL98] J. Fitzgerald and P. G. Larsen. *Modelling Systems: Practical Tools and Techniques for Software Development.* Cambridge University Press, 1998.

[HHS86] He Jifeng, C. A. R. Hoare and J. W. Sanders. Data Refinement Refined. In Robinet and Wilhelm (eds.), *Proceedings ESOP'86: European Symposium on Programming, Lecture Notes in Computer Science*, 213:187-196, Springer, 1986.

[HHS87] C. A. R. Hoare, He Jifeng and J. W. Sanders. Prespecification in Data Refinement. *Information Processing Letters*, 25(2):71-76, May 1987.

[Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576-585, October 1969.

[Hoa71] C. A. R. Hoare. Proof of a program: FIND. *Communications of the ACM*, 14:39-45, January 1971.

[Jac92] J. Jacob. Basic theorems about security. *Journal of Computer Security*, 1(4):385-411, 1992.

[JB02] C. Jeske and R. Banach. Minimally and Maximally Abstract Retrenchments. In *Proceedings of IFM'02, Lecture Notes in Computer Science*, 2335:380-399, Springer, 2002.

[Jon90] C. B. Jones. *Systematic Software Development Using VDM (2nd edition)*. Prentice-Hall, 1990.

[Liu97] S. Liu. Evolution: A More Practical Approach than Refinement for Software Development. In *Proceedings ICECCS-97*, pages 142-151, IEEE, 1997.

[LT93] N. Leveson and C. S. Turner. An Investigation of the Therac-25 Accidents. *IEEE Computer*, 26(7):18-41, July 1993.

[LW92] H. J. Litteck and P. J. L. Wallis. Refinement Methods and Refinement Calculi. *Software Engineering Journal*, **7**:(3):219-229, 1992.

[Mah92] B. Mahony. *The Specification and Refinement of Timed Processes.* Ph.D. thesis, Department of Computer Science, Queensland University, 1992.

[MGR93] C. C. Morgan, P. H. B. Gardiner and K. A. Robinson. *On the Refinement Calculus.* Springer-Verlag, 1993.

[MH92] B. Mahony and I. Hayes. A case-study in timed refinement: A mine pump. *IEEE Transactions on Software Engineering*, 18(9):817-826, 1992.

[Mor87] J. M. Morris A Theoretical Basis for Stepwise Refinement and the Programming Calculus. *Science of Computer Programming*, 9:287-306, 1987.

[Mor89] J. M. Morris. Laws of Data Refinement. *Acta Informatica*, 26:287-308, 1989.

[Mor94] C. C. Morgan. *Programming from Specifications (2nd edition)*. Prentice-Hall, 1994.

[MR87] C. C. Morgan and K. A. Robinson. Specification statements and refinement. *IBM Journal of Research and Development*, 31(5):546-555, September 1987.

[Nei90] D. S. Neilson. *From Z to C: Illustration of a Rigorous Development Method*. D.Phil. thesis, Oxford University Computing Laboratory, Technical Monograph PRG-101, 1990.

[PB00] M. Poppleton and R. Banach. Retrenchment: Extending Refinement for Continuous and Control Systems. In D. Sinclair and P. Gibson (eds.), *Proceedings IWFM'00, Electronic Workshop in Computer Science Series*, Springer, 2000.

[PB02] M. Poppleton and R. Banach. Controlling Control Systems: An Application of Evolving Retrenchment. In D. Bert, J. P. Bowen, M. C. Henson and K. Robinson (eds.), *Proceedings of ZB2002: Formal Specification and Development in Z and B, Lecture Notes in Computer Science*, 2272:42-61, Springer-Verlag, 2002.

[Pop01] M. R. Poppleton. *Formal Methods for Continuous Systems: Liberalising Refinement in B*. Ph.D. thesis, Department of Computer Science, University of Manchester, 2001.

[Pou04] K. Poulson. Software Bug Contributed to Blackout. *SecurityFocus 2004*. [online: http://www.securityfocus.com/news/8016] (retrieved 16 May 2004).

[SC00] S. Stepney and D. Cooper. Formal methods for industrial products. In Bowen et al. [BDGK00], pages 374-393.

[Sch01a] S. Schneider. *The b-method: an introduction*. Palgrave, 2001.

[Sch01b] G. Schellhorn. Verification of ASM refinements using generalized forward simulation. *Journal of Universal Computer Science*, 7(11):952-979, 2001.

[SCW98] S. Stepney, D. Cooper and J. Woodcock. More Powerful Z Data Refinement: pushing the state of the art in industrial refinement. In J. P. Bowen, A. Fett and M. G. Hinchey (eds.), *Proceedings ZUM'98, Lecture Notes in Computer Science*, 1493:284-307, Springer, 1998.

[SCW00] S. Stepney, D. Cooper and J. Woodcock. *AN ELECTRONIC PURSE Specification, Refinement, and Proof*. Technical Report PRG-126, Oxford University Computing Laboratory, 2000.

[SF00] G. Smith and C. Fidge Incremental Development of Real-Time Requirements: The Light Control Case Study. *Journal of Universal Computer Science*, 6(7):704-730, 2000.

[Smi99] G. Smith. Stepwise Development from Ideal Specifications. Technical Report 99-35, Software Verification Centre, School of Information Technology, University of Queensland, Brisbane, Australia. November 1999.

[Spi92] J. M. Spivey. *The Z Notation: A Reference Manual (2nd edition)*. Prentice-Hall, 1992.

[Ste01] S. Stepney. New horizons in formal methods. *The Computer Bulletin*, pages 24-26, 2001.

[WD96] J. Woodcock and J. Davies. *Using Z: Specification, Refinement, and Proof*. Prentice-Hall, 1996.

[Wir71] N. Wirth. Program Development by Stepwise Refinement. *Communications of the ACM*, 14:(4):221-227, April 1971.