Retrenchment and Refinement Interworking: the Tower Theorems

R. Banach, C. Jeske
School of Computer Science, Manchester University, Manchester, M13 9PL, U.K.
banach@cs.man.ac.uk , cjeske@cs.man.ac.uk

Abstract. Retrenchment is a flexible model evolution formalism that compensates for the limitations imposed by specific formulations of refinement. Its refinement-like proof obligations feature additional predicates for accommodating design data describing the model change. The best results are obtained when refinement and retrenchment cooperate, the paradigmatic scheme for this being the commuting square or *Tower*, in which 'horizontal retrenchment rungs' commute with 'vertical refinement columns' to navigate through a much more extensive design space than permitted by refinement alone. In practice, the navigation is accomplished via 'square completion' constructions, and a full suite of square completion theorems is presented and proved.
Keywords. Retrenchment, Refinement, Composition, Square Completion, Tower Pattern.

1 Introduction

As a design and development technique, model based refinement (see eg. [de Roever and Engelhardt (1998)] for a survey) has proved its worth on many occasions. Despite the broad reluctance among mainstream developers to embrace as mathematical an approach to development as refinement proposes, a number of well known industrial scale developments have demonstrated the enhanced dependability that accrues from using a technique enjoying such a level of rigour. See for instance [Stepney, Cooper et al. (1998, 2000)], for the public presentation of the Mondex formal development in Z, and [Jones and Woodcock (2008)] for its more recent reappraisal in the context of the Verification Grand Challenge [Jones et al. (2006), Woodcock (2006), Woodcock and Banach (2007)]. See for instance [Behm et al. (1999), Behm et al. (2000)], for the use of the B-Method in the development of MÉTÉOR, and its subsequent further development in projects like Roissy-VAL [Badeau and Amelot (2005)]. In niche areas, where the benefits of the aforementioned dependability has been appreciated, these techniques continue to be applied, though, often, little appears in the public domain due to reasons of commercial confidentiality.[1]

As a design and development technique, (a given, specific, incarnation of) model based refinement can sometimes fall short of what is desired, as regards treating specific requirements issues in the most faithful way possible. Retrenchment was introduced as a means for addressing such awkward requirements issues, with the aim of allowing them to be treated in a formal manner, whilst at the same time not interfering with the benefits of a perhaps over-idealised refinement development. In [Banach,

1. For instance, the proceedings of FM 2005 (LNCS **3582**) contain a collection of short papers documenting the Industry Day, whereas the proceedings of FM 2011 (LNCS **6664**) do not have any Industry Day papers, the day having been confined to oral presentations only.

Poppleton et al. (2007)] there is a comprehensive and broadly based overview of retrenchment. In that paper, background and context are extensively discussed, some key issues that arise with retrenchment are described, and some case studies are explored.[2] Moving on from that starting point, the present paper is concerned with a key technical topic, the interworking of retrenchment and refinement.

The issue is the following. Retrenchment, as conventionally presented, is extremely permissive (deliberately so). So using it as *sole* formal technique in a development process can let through a whole host of design deviations that might be considered undesirable, and that could derail the development process. This possibility can in turn demand considerable self-discipline, and intensive investment in validation, to ensure that the development stays on track. However, using retrenchment in a controlled way in concert with refinement considerably alleviates this situation, as a good deal of what would otherwise be validation burden, can be delegated to the guarantees that (some particular notion committed to, of) model based refinement offers, especially when backed up via an appropriate tool.

How then to arrange for such fruitful cooperation between the two notions? The paradigm investigated in this paper, is to see retrenchment and refinement as orthogonal directions in a development landscape which enjoys a higher 'dimensionality' than one in which refinement is seen as being the only possible means of progress. Thus, one can visualise refinement as proceeding 'downwards' from abstract to concrete (this being the only possible means of progress in a conventional formal development world), and can visualise retrenchment as proceeding 'horizontally', bridging between refinement strands that would remain isolated from one another without the use of retrenchment. This architecture is given solidity by demanding that diverse paths through this two dimensional landscape between the same two system models should be related in a composable and understandable way. And this in turn can be realised if we establish a sufficient store of 'square completion' constructions, each of which fills in a missing piece in an incomplete square of horizontal retrenchments and vertical refinements. One thing that this achieves is to allow us to interchange suitable retrenchment/refinement pairs, and thus by repeated application, to morph one path between the two system models into a different one. Going further, the automatic construction of systems afforded by such square completion constructions, widens the scope for 'system building by theorem', from the pure refinement paradigm,[3] to a wider gamut of requirements issues that include ones that become formally addressable only by means of retrenchment. This is the aim of the present paper.

The rest of the paper is as follows. In Section 2 we give a broad informal overview of retrenchment and describe some of the case studies and scenarios in which it has been employed. In Section 3 we change from an informal to a technically rigorous orientation, recalling the basics of retrenchment, and give a fairly general purpose formulation of refinement for interworking with it. The refinement notion is one that can be instantiated to capture a range of existing refinement formulations in the literature.[4] Section 4 covers the compositions of retrenchments and refinements that we need in the sequel. Section 5 outlines the main results of the rest of the paper, summarising the theorems, and indicating their use in the Tower Pattern [Banach et al.

---

2. See [Retrenchment Homepage] for the latest developments.
3. This is exemplified at the time of writing by toolsets such as Rodin [Rodin] (and others), each designed for the formal development of systems via (some specific notion of) refinement.

(2005)] — it can be used for convenient overview. The remaining sections focus on the technical details of the specific theorems, one by one. Section 6 covers the Lifting Theorem. Section 7 covers the Lowering Theorem. Section 8 covers the Postjoin Theorem. Section 9 covers the Prejoin Theorem. Adhering to a rather categorical paradigm, all of these results are proved up to notions of equivalence, which amount to inter-simulability, inter-retrenchability, or inter-refinability, as appropriate, and as described in detail in each relevant theorem. This gives a precise definition of the way that each of the results obtained is characterised, beyond the details of the explicit construction given. This in turn is good for replacing the explicit construction by something equally useful but more appealing from a system requirements point of view. Readers less concerned with the technical details can skip over the proofs in these four sections. Section 10 discusses associativity, general tower constructions and system engineering, sketching how the above technical material might be applied. Section 11 concludes.

This paper readdresses results and constructions investigated in depth originally in [Jeske (2005)]. The results in [Jeske (2005)] took a particular stance on how the constructions should be approached, and strove for the greatest degree of generality possible from that perspective. While this aim appeared at the outset to be innocuous enough, it led, in the end, to some ferociously complicated results — results whose overwhelming technical convolutedness certainly proved to be an impediment to their widespread application. The aim of the present paper is to revisit these issues, employing the wisdom of hindsight, and to give counterparts which are much more approachable and thus more readily applied. Although a comparison of the present work with [Jeske (2005)] shows extensive detailed technical differences, the debt this paper owes to [Jeske (2005)] for illuminating the consequences of the earlier approach cannot be overstated.

Assumption 1.1 We work in a set theoretic and relational framework, in which relations are manipulated using logical operations on the predicates that define their bodies. To avoid a proliferation of pathological cases, we assume henceforth, that any set or relation mentioned in the hypotheses of a construction or theorem is nonempty, so that, for example, a mentioned putative choice of some element from it can actually be made.

Notation 1.2 We write X^{T} for the transpose of a relation X, (i.e. xXx' iff $x'X^{\mathrm{T}}x$). We write $Z \lhd X$ for the domain restriction of a relation X, i.e. $Z \lhd X \equiv X \cap ((Z \cap \mathrm{dom}(X)) \times \mathrm{rng}(X))$.

2 Retrenchment, an Overview

What we now refer to as model based refinement had its origins in the work of Wirth, Dijkstra and Hoare, in papers such as [Wirth (1971), Dijkstra (1972), Hoare (1972)].

4. In a further paper [Banach (2009)], a number of specific real world refinement formulations are examined in order to infer the most appropriate way to design retrenchment notions, and the insights of the present paper are used to reinforce the conclusions drawn. In turn, the formulation of refinement used here is designed to be capable of realising various specific notions examined in [Banach (2009)]. Thus, although the present paper is technically self-contained, there is strong conceptual cross-fertilisation between the present paper, [Banach (2009)], and [Banach, Poppleton et al. (2007)].

In those days, the message was straightforward enough, in that refinement was a process whereby a piece of abstract program could be replaced by a piece of more concrete program without changing observable behaviour. If, for some set of sufficient conditions, it could be *proved* that observations were unchanged, those conditions could be adopted as a general purpose working method for establishing refinement.

As with any technique which gets fixed *a priori*, but that deals with problems expressible in a 'general purpose programming-like notation', as one tackles problem instances of increasing size, complexity eventually rears its head and becomes an issue to contend with. In the case of notions of refinement, there is not only complexity of problem descriptions in the sense of some formal complexity measure or other, as one would normally understand such a concept, but there is also complexity of a less precisely defined kind, having its roots in various 'management level' concerns that have an impact when one tackles the development of applications in the real world.

Thus, applying some particular flavour of model based refinement to a real application 'out of the box' may become infeasible, not only because the problem instance becomes too big according to some objective formal measure, but also sooner than that, because modeling at the level needed to properly take all relevant requirements concerns into account increases model (and development) complexity to a level unacceptable from a mangement perspective (for instance, because the resulting model is not perspicuous enough, or for other reasons emerging from the wider problem context, or the real world system construction context).

Retrenchment, treated in detail below, (see [Banach, Poppleton et al. (2007), Banach et al. (2008), Banach and Jeske (2010)], and other work available from [Retrenchment Homepage]), was introduced in order to address the issues mentioned in the previous paragraph. The idea was to introduce a notion that would accommodate departures from the exigencies of formal refinement, yet would be capable of smooth interworking with refinement when circumstances allowed. Speaking rather informally, if we say that the core idea of model based refinement is captured in a 'forward simulation' proof obligation of the form:

$$G \wedge stp_{Op_{\mathrm{C}}} \;\Rightarrow\; (\exists\, stp_{Op_{\mathrm{A}}} \wedge G') \tag{2.1}$$

where G is a retrieve, or gluing relation, the prime decoration refers to after-states, and $stp_{Op_{\mathrm{C}}}$ and $stp_{Op_{\mathrm{A}}}$ are concrete and abstract steps of the operation Op, then the form adopted for the corresponding proof obligation of retrenchment is of the form:

$$G \wedge P_{Op} \wedge stp_{Op_{\mathrm{C}}} \;\Rightarrow\; (\exists\, stp_{Op_{\mathrm{A}}} \wedge ((G' \wedge O_{Op}) \vee C_{Op})) \tag{2.2}$$

In (2.2), P_{Op} is the within, or provided relation, tightening the scope of the proof obligation. Similarly we have the output relation O_{Op}, allowing strengthening of the claim made by the PO. Crucially though, there is also C_{Op}, the concedes relation, which allows arbitrary departures from refinement-like behaviour, which is the essential characteristic of retrenchment. The broad similarity between the shapes of (2.1) and (2.2) leads us to conjecture that a mathematically rigorous integration of refinement and retrenchment ought to be possible, and this, in fact, is the main topic of this paper.

Of course, being construed in a similar way to model based refinement (i.e. as a more or less fixed scheme for relating system models and for generating proof obligations regarding such relationships), retrenchment ultimately suffers from similar complexity challenges to those already described. Nevertheless, in being a weaker notion than refinement (in the sense of offering weaker guarantees than refinement typically does), it is hoped that the point at which the complexity issues alluded to start to defeat development strategies that employ retrenchment alongside refinement in suitable combinations, lies considerably further out, bringing considerably more real world developments feasibly into the formal fold.

Giving precise meaning to the phrase 'suitable combinations' is the main technical contribution of this paper, and we discuss this extensively below. For now, we describe how these techniques have been used fruitfully in some applications to date.

The most visible use of the technology proposed here has been in the treatment of a number of requirements issues in the Mondex formal development. The Mondex Purse is a smartcard based electronic purse, whose security architecture permits payments from person-to-person using a wallet device or telephone line, without the need for separate authorisation. The Mondex project was one of the earliest formal development exercises in which refinement played a central role [Stepney et al. (2000), Stepney et al. (1998)]. In seeking to keep the refinement tractable, a number of requirements issues were purposely simplified and then treated informally outside of the formal development. Subsequently, these were revisited using retrenchment to integrate a more formal treatement with the existing idealised development.

One such issue was the boundedness of Mondex sequence numbers. For the usual security reasons, Mondex transactions need to have unique sequence numbers. For simplicity, these were modeled as natural numbers in [Stepney et al. (2000)], though obviously, in practice, they are bounded. The discrepancy between idealised and realistic sequence numbers, and its consequences, was treated in a retrenchment in [Banach et al. (2005)].

Another such issue was the boundedness of Mondex error logs. For predictable reasons connected with transaction recovery, Mondex purses need to log various kinds of failed transaction. For simplicity, these logs were modeled as unbounded sets in [Stepney et al. (2000)], though obviously, in practice, they are bounded. For implementation reasons, the size of the log is rather small, which imposes a collection of requirement issues quite different from those connected with the finiteness of the sequence number bound. These issues were treated in a retrenchment in [Banach et al. (2006a)].

Yet another issue was connected with the properties of a hash function used during Mondex transaction recovery. For simplicity (and more importantly, to make the security proof go through at all), this hash function was modeled as an injective function, though obviously, in practice, any real hash function is going to be many-one. This opens up interesting security repercussions, which were treated in a retrenchment in [Banach et al. (2006b)].

Finally, for subtle reasons connected with the use of backward refinement in the Mondex development, an operation as simple as a purse balance enquiry could not be modeled in the original development. The whole issue was revisited, and a satisfactory resolution developed using retrenchment in [Banach, Jeske et al. (2007)]. (This later led to an abstract development of protocol refinement in general in [Banach and Schellhorn (2010)].)

All of the above were treated using the precursor of the theory of this paper, namely using the theory in [Jeske (2005)]. Given that the theorems of [Jeske (2005)] differ from those here in detail, it is worth asking how these earlier Mondex retrenchments might be affected if redone using the present theory. The good news is that they are not affected at all, this being due to the extreme simplicity of the relevant refinements in [Stepney et al. (2000)] through which the retrenchments of interest were being pulled; these refinements in fact being injections on the state space — the theorems of [Jeske (2005)] do not differ in their effects from those developed here when applied to such simple refinements. Therefore, these earlier case studies act just as well as confirmations of the utility of the present theory, as they did as confirmations of the former theory.

Looking further afield, beyond the applications just described, in [Jeffords et al. (2009)], the authors adapt the basic retrenchment idea, and by adjoining a suitable collection of additional conditions (policed by corresponding proof obligations within the tool), they are able to formally introduce faulty behaviours into their system model, which depart from and subsequently rejoin (a refinement of) nominal abstract behaviour. Beyond that, in [Banach (2011)], an extension of the Event-B formalism to include retrenchment development steps (precisely along the lines of the theory expounded in the present paper) is introduced. Some of the ramifications of this are being explored in [Project Advance]. Looking further afield still, in [Banach et al. (2012)], the greater flexibility of retrenchment proves extremely useful in accommodating variable discrepancies between abstract continuous model behaviour, and concrete discretized model behaviour, in situations where these cannot be statically bounded. Again, cooperation between refinement and retrenchment aspects is policed using the theoretical ideas of this paper. Many further applications of a similar kind are forseen.

3 Transition Systems, Retrenchment and Refinement

In this section we give our basic definitions and notations. At any single moment, we will typically be dealing with a pair of systems in a development activity, the first, in some sense, more 'abstract' than the second, which is more 'concrete'. We model systems as transition systems which are organised as follows. Focusing on the abstract system Abs, it has a set of operation names $\mathsf{Ops}_{\mathrm{A}}$, with typical element Op_{A}. An operation Op_{A} works on the abstract state space U having typical element u (the before-state), and on an input space $\mathsf{I}_{Op_{\mathrm{A}}}$ with typical element i. Op_{A} will produce an after-state typically written u' and once more in U, and an output o drawn from an output space $\mathsf{O}_{Op_{\mathrm{A}}}$. Initial states satisfy the predicate $Init_{\mathrm{A}}(u')$ (allowing initial states to be viewed as results of an initialisation operation if need be).

Individual steps of Op_{A} are written u -(i, Op_{A}, o)-› u'. Their totality constitutes the step relation $stp_{Op_{\mathrm{A}}}(u, i, u', o)$ of Op_{A}. Aggregating over all of $\mathsf{Ops}_{\mathrm{A}}$, we obtain the complete transition relation for the Abs system, $stp_{\mathrm{A}} = \bigcup_{Op_{\mathrm{A}} \in \mathsf{Ops}_{\mathrm{A}}} stp_{Op_{\mathrm{A}}}$, where the union is necessarily disjoint since the relevant Op_{A} name is part of every execution step.

Later, we will have several systems in play simultaneously, so we use similar notational conventions for them. We set out our generic notions using a pair of concrete systems which we name $\mathsf{Conc}_{\mathrm{T}}$ and $\mathsf{Conc}_{\mathrm{F}}$. For $\mathsf{Conc}_{\mathrm{T}}$, the operation names are $Op_{\mathrm{C}} \in \mathsf{Ops}_{\mathrm{C}}$. States are $v \in \mathsf{V}$, inputs $j \in \mathsf{J}_{Op_{\mathrm{C}}}$, outputs $p \in \mathsf{P}_{Op_{\mathrm{C}}}$. Initial states satisfy $Init_C(v')$. Transitions are v -(j, Op_C, p)-› v', elements of the complete step relation $stp_{Op_C}(v, j, v', p)$. For Conc_F, let us say the operation names are also $Op_C \in \mathsf{Ops}_C$, but the variables are $w \in \mathsf{W}$, inputs $k \in \mathsf{K}_{Op_C}$, outputs $q \in \mathsf{Q}_{Op_C}$, the rest being predictable.

3.1 Retrenchment

Given the above context, a retrenchment from Abs to Conc_T is defined by three facts. Firstly, $\mathsf{Ops}_A \cap \mathsf{Ops}_C = \mathsf{Ops}_{AC} \neq \varnothing$, i.e. the abstract and concrete operation name sets have some elements in common. Secondly, we have a collection of relations as follows: there is a retrieve relation $G(u, v)$ between abstract and concrete state spaces; and there is a family of within, output, and concedes relations for each common operation name $Op \in \mathsf{Ops}_{AC}$: $P_{Op}(i, j, u, v)$, $O_{Op}(o, p; u', v', i, j, u, v)$, $C_{Op}(u', v', o, p; i, j, u, v)$ respectively.[5] These relations are over the variables shown, i.e. the within relations involve the inputs and before-states, while the output and concedes relations involve predominantly the outputs and after-states, though inputs and before-states can also feature if required (the semicolon cosmetically separating these additional possibilities). The relations are collectively referred to as the retrenchment data, and for brevity, we refer to the retrenchment as G,P,O,C. Note that we suppress the 'A' and 'C' subscripts on Op in these relations since they concern both levels of abstraction equally.

Thirdly, a collection of properties (the proof obligations or POs) must hold. The initial states must satisfy:

$$Init_C(v') \;\Rightarrow\; (\exists\, u' \bullet Init_A(u') \wedge G(u', v')) \tag{3.1}$$

and for every corresponding operation pair Op_A and Op_C, the abstract and concrete step relations must satisfy the operation PO:

$$\begin{aligned} & G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_C}(v, j, v', p) \;\Rightarrow \\ & \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee \\ & \qquad C_{Op}(u', v', o, p; i, j, u, v))) \end{aligned} \tag{3.2}$$

For an $Op \in \mathsf{Ops}_{AC}$, an important counterfoil to the operation PO is the operation's simulation relation. This holds for an abstract step u -(i, Op_A, o)-› u' and a corresponding concrete step v -(j, Op_C, p)-› v', the two steps being *in simulation*, iff:

$$\begin{aligned} & G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_C}(v, j, v', p) \wedge stp_{Op_A}(u, i, u', o) \wedge \\ & ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee C_{Op}(u', v', o, p; i, j, u, v)) \end{aligned} \tag{3.3}$$

holds.

A retrenchment (with retrenchment data as above) is a biretrenchment iff, along with (3.1) and (3.2), we also have:

$$Init_A(u') \;\Rightarrow\; (\exists\, v' \bullet Init_C(v') \wedge G(u', v')) \tag{3.4}$$

5. This confirms that the 'A' and 'C' and (later) similar subscripts on operation names are meta level tags, suppressed when it is convenient to do so and it does not cause confusion. Usually, $\mathsf{Ops}_A \subseteq \mathsf{Ops}_C$ is assumed; we will be more general here. Also, nothing prevents arbitrary correspondences between (otherwise unrelated) names in Ops_A and Ops_C being set up via suitable mappings. Though it would just add clutter theoretically here, such a thing is highly desirable in the context of an industrial strength tool, to add flexibility.

$$G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_A}(u, i, u', o) \Rightarrow \\ \quad (\exists\, v', p \bullet stp_{Op_C}(v, j, v', p) \wedge ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee \\ \quad\quad C_{Op}(u', v', o, p; i, j, u, v))) \tag{3.5}$$

Thus in a biretrenchment we can exchange the roles of abstract and concrete systems with impunity using the same data.

Going further, if we only have (3.4) and (3.5) (and not (3.1) and (3.2)), then we call such a setup a converse retrenchment (i.e. a converse retrenchment is characterised by having the signatures of the constituent relations the opposite way round to what we would normally expect).

Finally, suppose that we simply have some relations defined on two transition systems and appropriately indexed by operation names as above, which have the signatures required to qualify as retrenchment data, but we cannot (or choose not to try to) establish (3.1) and (3.2). Then the relations $G(u, v)$ and:

$$G(u, v) \wedge P_{Op}(i, j, u, v) \wedge \\ ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee C_{Op}(u', v', o, p; i, j, u, v)) \tag{3.6}$$

(the latter from u, i, u', o, to v, j, v', p, with $Op \in \mathsf{Ops}_{AC}$), constitute a pseudoretrenchment. In a pseudoretrenchment we evidently have the simulation relations (3.3) without the abstract and concrete transitions.

3.2 Refinement

Now, given two systems Abs and Conc_F, we set up refinement as a relationship between the operations with identical names. In this paper we assume that for a refinement, the abstract and concrete operations name sets are identical.[6] The refinement data will consist of a retrieve relation $G(u, w)$, and a family of input and output relations for each common $Op \in \mathsf{Ops}$: $In_{Op}(i, k)$ and $Out_{Op}(o, q)$. These latter relations are over the variables shown, i.e. just the I/O variables. For brevity, we refer to the refinement as G,In,Out.

The POs are, for initialisation:

$$Init_C(w') \Rightarrow (\exists\, u' \bullet Init_A(u') \wedge G(u', w')) \tag{3.7}$$

and for the operations:

$$G(u, w) \wedge In_{Op}(i, k) \wedge stp_{Op_C}(w, k, w', q) \Rightarrow \\ \quad (\exists\, u', o \bullet stp_{Op_A}(u, i, u', o) \wedge G(u', w') \wedge Out_{Op}(o, q)) \tag{3.8}$$

In addition to (3.7) and (3.8), many notions of refinement feature additional criteria, typically expressed via subsets of the before- and input spaces, that control the detailed semantics of operations. Often they have names such as: domain conditions, preconditions, guards, etc. To mimic these generically, we let each common operation $Op \in \mathsf{Ops}$ have an associated applicability set: APP_{Op_A} for Op_A and APP_{Op_C} for Op_C. The typical conditions such sets have to satisfy are either:

$$\mathrm{APP}_{Op_A}(u, i) \wedge G(u, w) \wedge In_{Op}(i, k) \Rightarrow \mathrm{APP}_{Op_C}(w, k) \tag{3.9}$$

6. We could of course opt for greater generality on this point, along the lines of footnote 5.

or:

$$\mathrm{APP}_{Op_\mathrm{A}}(u, i) \Leftarrow G(u, w) \wedge In_{Op}(i, k) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k) \tag{3.10}$$

(since some theories insist on weakening, and others on strengthening such applicability criteria). As a shorthand below, we refer to both (3.9) and (3.10) using:

$$\mathrm{APP}_{Op_\mathrm{A}}(u, i) \wedge G(u, w) \wedge In_{Op}(i, k) \Lleftarrow\!\!\Rrightarrow G(u, w) \wedge In_{Op}(i, k) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k) \tag{3.11}$$

In (3.11) the symbol $\Lleftarrow\!\!\Rrightarrow$ represents the two separate cases in (3.9) and (3.10). Thus (3.7), (3.8) and (3.11) represent three species of refinement theory. The first has (3.7) and (3.8) alone. The second has (3.7), (3.8) and (3.9). The third has (3.7), (3.8) and (3.10).

The simulation relation corresponding to these notions of refinement is:

$$\begin{aligned}&G(u, w) \wedge In_{Op}(i, k) \wedge [\mathrm{APP}_{Op_\mathrm{A}}(u, i) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k)] \wedge \\ &stp_{Op_\mathrm{C}}(w, k, w', q) \wedge stp_{Op_\mathrm{A}}(u, i, u', o) \wedge G(u', w') \wedge Out_{Op}(o, q)\end{aligned} \tag{3.12}$$

and again we say that the two steps are *in simulation*. In (3.12), the term $[\mathrm{APP}_{Op_\mathrm{A}}(u, i) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k)]$ is bracketed to indicate that it is not relevant for the simple formulation of refinement.

As for retrenchment, if in addition to (3.7) and (3.8) we also have:

$$Init_\mathrm{A}(u') \Rightarrow (\exists\, w' \bullet Init_\mathrm{C}(w') \wedge G(u', w')) \tag{3.13}$$

$$\begin{aligned}&G(u, w) \wedge In_{Op}(i, k) \wedge stp_{Op_\mathrm{A}}(u, i, u', o) \Rightarrow \\ &\quad (\exists\, w', q \bullet stp_{Op_\mathrm{C}}(w, k, w', q) \wedge G(u', w') \wedge Out_{Op}(o, q))\end{aligned} \tag{3.14}$$

then the refinement is a birefinement. If we are dealing with a notion of refinement requiring the use of APP sets, then in the corresponding notion of birefinement we also insist on:

$$\mathrm{APP}_{Op_\mathrm{A}}(u, i) \wedge G(u, w) \wedge In_{Op}(i, k) \Leftrightarrow G(u, w) \wedge In_{Op}(i, k) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k) \tag{3.15}$$

Going further, if we only have (3.13), (3.14), and the converse of (3.11) if appropriate (and not (3.7), (3.8), and (3.11) if appropriate), then we call such a setup a converse refinement.

Finally, suppose that we have three relations defined on two transition systems and appropriately indexed by operation names, which have the signatures required to qualify as refinement data, but we cannot (or choose not to try to) establish (3.7), (3.8) (and (3.11) if appropriate). Then the relations $G(u, w)$ and:

$$\begin{aligned}&G(u, w) \wedge In_{Op}(i, k) \wedge [\mathrm{APP}_{Op_\mathrm{A}}(u, i) \wedge \mathrm{APP}_{Op_\mathrm{C}}(w, k)] \wedge \\ &G(u', w') \wedge Out_{Op}(o, q)\end{aligned} \tag{3.16}$$

(the latter from u, i, u', o, to w, k, w', q, with $Op \in \mathsf{Ops}$), are referred to as a pseudorefinement. As for a pseudoretrenchment, a pseudorefinement omits the transitions from the simulation relation.

4 Compositions

Below we will make much use of compositions of relationships between systems. The relationships are retrenchments, refinements, their converses, their pseudo- analogues, and so on. Various notions of composition involving the basic retrenchment and refinement concepts are thoroughly studied in [Banach et al. (2008)], so we just review the relevant results here. It turns out that these notions of composition are all based on various compositions of relations, so they readily extend to the converse and pseudo- variants. We principally need vertical composition of retrenchments (and refinements), and disjunctive fusion composition.

4.1 Vertical Composition

Suppose we have a system Sys_0, which is retrenched to a system Sys_1, and that Sys_1 is further retrenched to a system Sys_2. Assuming that the granularity of the individual transitions in these models does not change, Sys_0 and Sys_2 are related by a vertical composition. Subscripting the retrenchment data for the two original retrenchments '1', and '2' respectively, and subscripting the retrenchment data for the composition '(1,2)', we find:

$$G_{(1,2)} \equiv G_1 \mathbin{⨾} G_2 \tag{4.1}$$

$$P_{Op,(1,2)} \equiv (G_1 \wedge P_{Op,1}) \mathbin{⨾} (G_2 \wedge P_{Op,2}) \tag{4.2}$$

$$O_{Op,(1,2)} \equiv O_{Op,1} \mathbin{⨾} O_{Op,2} \tag{4.3}$$

$$C_{Op,(1,2)} \equiv (G'_1 \wedge O_{Op,1} \mathbin{⨾} C_{Op,2}) \vee (C_{Op,1} \mathbin{⨾} G'_2 \wedge O_{Op,2}) \vee (C_{Op,1} \mathbin{⨾} C_{Op,2}) \tag{4.4}$$

In (4.1)-(4.4) the forward relational composition $⨾$ is via the relevant variables of the intermediate system. Thus the composed retrieve relation is straightforwardly the composition of the two retrieves; likewise for the composed output relation. The composed within relation is the composition of the two withins, but strengthened by the composed retrieve. Lastly the composed concession has the most complex form: either the after-state retrieve and output relations for the first retrenchment, composed with the concession for the second holds; or the converse holds; or the composition of the two concessions holds. Since much will depend on this composition, we next give a precise statement. It also explains what was signified by 'we find' just before (4.1) — it referred to a soundness result, since the proof of Proposition 4.1 requires that the hypothesised retrenchment data do in fact satisfy the POs (3.1)-(3.2).

Proposition 4.1 Let Sys_0 (with variables u_0, i_0, o_0) be retrenched to Sys_1 (with variables u_1, i_1, o_1) using G_1, $\{P_{Op,1}, O_{Op,1}, C_{Op,1} \mid Op \in \mathsf{Ops}_{01}\}$, and Sys_1 be retrenched to Sys_2 (with variables u_2, i_2, o_2) using G_2, $\{P_{Op,2}, O_{Op,2}, C_{Op,2} \mid Op \in \mathsf{Ops}_{12}\}$. Then Sys_0 is retrenched to Sys_2 using retrieve, within, and concedes relations $G_{(1,2)}$, $\{P_{Op,(1,2)}, O_{Op,(1,2)}, C_{Op,(1,2)} \mid Op \in \mathsf{Ops}_{01} \cap \mathsf{Ops}_{12}\}$, where:[7]

$$G_{(1,2)}(u_0, u_2) \equiv (\exists\, u_1 \bullet G_1(u_0, u_1) \wedge G_2(u_1, u_2)) \tag{4.5}$$

$$\begin{aligned} &P_{Op,(1,2)}(i_0, i_2, u_0, u_2) \equiv (\exists\, u_1, i_1 \bullet \\ &\qquad G_1(u_0, u_1) \wedge G_2(u_1, u_2) \wedge P_{Op,1}(i_0, i_1, u_0, u_1) \wedge P_{Op,2}(i_1, i_2, u_1, u_2)) \end{aligned} \tag{4.6}$$

$$\begin{aligned} &O_{Op,(1,2)}(o_0, o_2; u'_0, u'_2, i_0, i_2, u_0, u_2) \equiv (\exists\, u'_1, o_1, u_1, i_1 \bullet \\ &\qquad O_{Op,1}(o_0, o_1; u'_0, u'_1, i_0, i_1, u_0, u_1) \wedge O_{Op,2}(o_1, o_2; u'_1, u'_2, i_1, i_2, u_1, u_2)) \end{aligned} \tag{4.7}$$

7. In (4.8), and below, we use braces to delimit large disjunctions (especially those which are not at top level), delimiting individual large disjuncts using square brackets.

$$
\begin{aligned}
&C_{Op,(1,2)}(u'_0, u'_2, o_0, o_2; i_0, i_2, u_0, u_2) \equiv (\exists\, u'_1, o_1, u_1, i_1 \bullet \\
&\quad \{[G_1(u'_0, u'_1) \wedge O_{Op,1}(o_0, o_1; u'_0, u'_1, i_0, i_1, u_0, u_1) \wedge \\
&\qquad C_{Op,2}(u'_1, u'_2, o_1, o_2; i_1, i_2, u_1, u_2)] \vee \\
&\quad [C_{Op,1}(u'_0, u'_1, o_0, o_1; i_0, i_1, u_0, u_1) \wedge \\
&\qquad G_2(u'_1, u'_2) \wedge O_{Op,2}(o_1, o_2; u'_1, u'_2, i_1, i_2, u_1, u_2)] \vee \\
&\quad [C_{Op,1}(u'_0, u'_1, o_0, o_1; i_0, i_1, u_0, u_1) \wedge \\
&\qquad C_{Op,2}(u'_1, u'_2, o_1, o_2; i_1, i_2, u_1, u_2)]\}) \qquad (4.8)
\end{aligned}
$$

The above deals with the composition of two retrenchments. The composition of a retrenchment (first) with a refinement (second) follows by defaulting the data for the second retrenchment. In more detail: the retrieve relation (4.5) remains unchanged; (4.6) has $P_{Op,2}$ replaced by $In_{Op,2}$, which is the relevant input relation; (4.7) has $O_{Op,2}$ replaced by $Out_{Op,2} \wedge G'_2 \wedge In_{Op,2} \wedge G_2$, which is the relevant output relation strengthened by the retrieve relation (in both the after- and before- values) and the input relation (all this in order to match with all of the '1' variables of $O_{Op,1}$); (4.8) has $C_{Op,2}$ set to false and $O_{Op,2}$ replaced as just described. We can summarise the result as:

$$G_{(1,2)} \equiv G_1 \mathbin{⨾} G_2 \qquad (4.9)$$

$$P_{Op,(1,2)} \equiv (G_1 \wedge P_{Op,1}) \mathbin{⨾} (G_2 \wedge In_{Op,2}) \qquad (4.10)$$

$$O_{Op,(1,2)} \equiv O_{Op,1} \mathbin{⨾} (Out_{Op,2} \wedge G'_2 \wedge In_{Op,2} \wedge G_2) \qquad (4.11)$$

$$C_{Op,(1,2)} \equiv C_{Op,1} \mathbin{⨾} (Out_{Op,2} \wedge G'_2 \wedge In_{Op,2} \wedge G_2) \qquad (4.12)$$

Note that the result is a retrenchment; so there is no APP_{Op} data to worry about — the APP_{Op} from the refinement (if applicable) is simply discarded. Moreover, if we have a refinement (first) composed with a retrenchment (second), then we simply interchange the roles of the two in the preceding.

If we have two refinements, the reasoning is relatively familiar. It is easy to prove that the following data yields a sound composed refinement:

$$G_{(1,2)} \equiv G_1 \mathbin{⨾} G_2 \qquad (4.13)$$

$$In_{Op,(1,2)} \equiv In_{Op,1} \mathbin{⨾} In_{Op,2} \qquad (4.14)$$

$$Out_{Op,(1,2)} \equiv Out_{Op,1} \mathbin{⨾} Out_{Op,2} \qquad (4.15)$$

From these it is also easy to show that for any relevant 'APP_{Op}' criteria, either two instances of (3.9) or two instances of (3.10), compose in a sound way.

4.2 Disjunctive Fusion Composition

The fact that retrenchment is phrased via a PO whose top level structure is an implication, together with the fact that $A \Rightarrow B$ and $C \Rightarrow D$ implies $A \vee C \Rightarrow B \vee D$, yields a strategy for composing different retrenchments about the same pair of abstract and concrete systems: disjunctive fusion composition. (Since one could replace '$\vee$' by '$\wedge$' in the preceding, there also is an alternative, conjunctive variant. This will play a much smaller role below than the disjunctive case — we allude to it in a couple of places, as needed.)

If the retrenchment data for the first retrenchment are subscripted '1' and for the second '2', we will subscript the composed data '$(1\vee2)$'. In outline, the retrenchment data for disjunctive fusion composition is as follows:

$$G_{(1\vee 2)} \;\equiv\; G_1 \vee G_2 \tag{4.16}$$

$$P_{Op,(1\vee 2)} \;\equiv\; (G_1 \vee P_{Op,2}) \wedge (P_{Op,1} \vee G_2) \wedge (P_{Op,1} \vee P_{Op,2}) \tag{4.17}$$

$$O_{Op,(1\vee 2)} \;\equiv\; (G'_1 \vee O_{Op,2}) \wedge (O_{Op,1} \vee G'_2) \wedge (O_{Op,1} \vee O_{Op,2}) \tag{4.18}$$

$$C_{Op,(1\vee 2)} \;\equiv\; C_{Op,1} \vee C_{Op,2} \tag{4.19}$$

In more detail, the basic soundness result is as follows.

Proposition 4.2 Let Abs be retrenched to Conc using G_1, $\{P_{Op,1}, O_{Op,1}, C_{Op,1} \mid Op \in \mathsf{Ops}_{\mathrm{AC}}\}$ (with the usual variables). Let Abs also be retrenched to Conc using G_2, $\{P_{Op,2}, O_{Op,2}, C_{Op,2} \mid Op \in \mathsf{Ops}_{\mathrm{AC}}\}$ (with the usual variables). Then Abs is retrenched to Conc also via $G_{(1\vee 2)}$ and $\{P_{Op,(1\vee 2)}, O_{Op,(1\vee 2)}, C_{Op,(1\vee 2)} \mid Op \in \mathsf{Ops}_{\mathrm{A}}\}$ where:

$$G_{(1\vee 2)}(u, v) \;\equiv\; G_1(u, v) \vee G_2(u, v) \tag{4.20}$$

$$\begin{aligned} &P_{Op,(1\vee 2)}(i, j, u, v) \;\equiv \\ &\quad (G_1(u, v) \vee P_{Op,2}(i, j, u, v)) \wedge \\ &\quad (P_{Op,1}(i, j, u, v) \vee G_2(u, v)) \wedge \\ &\quad (P_{Op,1}(i, j, u, v) \vee P_{Op,2}(i, j, u, v)) \end{aligned} \tag{4.21}$$

$$\begin{aligned} &O_{Op,(1\vee 2)}(o, p; u', v', i, j, u, v) \;\equiv \\ &\quad (G_1(u', v') \vee O_{Op,2}(o, p; u', v', i, j, u, v)) \wedge \\ &\quad (O_{Op,1}(o, p; u', v', i, j, u, v) \vee G_2(u', v')) \wedge \\ &\quad (O_{Op,1}(o, p; u', v', i, j, u, v) \vee O_{Op,2}(o, p; u', v', i, j, u, v)) \end{aligned} \tag{4.22}$$

$$\begin{aligned} &C_{Op,(1\vee 2)}(u', v', o, p; i, j, u, v) \;\equiv \\ &\quad C_{Op,1}(u', v', o, p; i, j, u, v) \vee C_{Op,2}(u', v', o, p; i, j, u, v) \end{aligned} \tag{4.23}$$

5 Square Completions

In this section we outline the main results of the ensuing four sections in a schematic fashion, for easier digestability of the details to follow.

The main idea is 'square completion'. Consider the left hand side of Fig. 1. It consists of two triangles. Focus on the upper one. The two filled boxes are two given systems and the solid arrow is a retrenchment between them (with given retrenchment data). The hollow box is another system, its hollow nature illustrating that it is to be constructed from the given data. The *Lifting Theorem* (Section 6) shows that the to-be-constructed system can indeed be constructed from the given data in a generic way, and that moreover, it can be connected to the given systems via the dashed arrows, the horizontal one being a retrenchment and the vertical one being a refinement (with the retrenchment and refinement data for these again being constructed from the given data in a generic way). Not only this, but the constructed retrenchment and refinement compose via (4.9)-(4.12) to yield an equivalent of the original (solid) retrenchment. Furthermore the construction is unique up to inter-refinability. The latter point is important since the generically constructed system (in this and subsequent theorems) is frequently unnatural-looking from an application perspective. So the opportunity to replace it with something that is theoretically equivalent but more intuitively appealing application-wise is highly desirable from a system engineering vantage point. See Section 10 for more extensive discussion of this point.

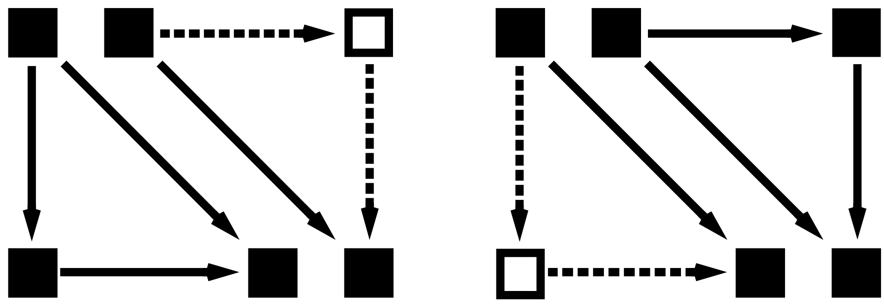


Fig. 1. Illustrating the lifting and lowering constructions. Vertical arrows are refinements while horizontal and diagonal arrows are retrenchments.

Consider now the lower triangle of the left hand side of Fig. 1. It shows a vertical refinement followed by a horizontal retrenchment. The composition of these (via the dual of (4.9)-(4.12)) yields a retrenchment, the hypotenuse of the lower triangle. We may suppose that this retrenchment is the starting point of the construction we have just discussed in the upper triangle. Therefore the Lifting Theorem enables us to complete the 'L shape' in the lower triangle to a square. Doing this, permits the interchange of the order of a refinement and retrenchment in a composition, in such a way that the result of the two compositions, either way round, yields the same retrenchment (i.e. the diagonal). The fact that the construction only needs the diagonal as input data, means that many of the details of the specific refinement and retrenchment are not relevant to the carrying out of the interchange.

Consider now the right hand side of Fig. 1. It also consists of two triangles. Focus on the lower one. The two filled boxes are two given systems and the solid arrow is a retrenchment between them (with given retrenchment data). The hollow box is another system, its hollow nature illustrating that it is to be constructed from the given data. The *Lowering Theorem* (Section 7) shows that the to-be-constructed system can indeed be constructed from the given data in a generic way, and that moreover, it can be connected to the given systems via the dashed arrows, the horizontal one being a retrenchment and the vertical one being a refinement (with the retrenchment and refinement data for these again being constructed from the given data in a generic way). Again, the constructed refinement and retrenchment compose via the dual of (4.9)-(4.12) to yield an equivalent of the original (solid) retrenchment. As previously, the construction is unique up to inter-refinability, this being useful for the reasons previously stated. The upper triangle of the right hand side of Fig. 1 plays the same role as its counterpart, the lower triangle of the left hand side of Fig. 1. It therefore shows that we have another square completion, and shows that the order of a refinement and retrenchment in a composition may be interchanged, but this time proceeding in the other direction, and again yielding the same retrenchment.

All this covers the first two major results of the paper. For the remaining results, consider Fig. 2. On the left is a square, part solid and part dashed. As previously, the

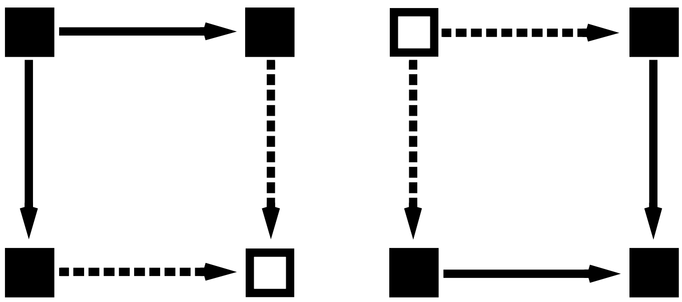


Fig. 2. Illustrating the postjoin and prejoin constructions. Vertical arrows are refinements while horizontal arrows are retrenchments.

horizontal arrows are retrenchments and the vertical arrows are refinements, with the dashed parts to be constructed out of the (given) solid parts. The *Postjoin Theorem* (Section 8) shows that there is a generic construction which allows this to be done in such a way that the composition of the given retrenchment with the constructed refinement, combines with the composition of the given refinement with the constructed retrenchment (via disjunctive fusion composition), to yield a retrenchment (the top left to bottom right diagonal, not shown) from the top left system to the bottom right (constructed) system. The construction of the dashed system in the bottom right corner is again unique, but up to a weaker notion (inter-simulability this time, in the sense defined in Section 3), which subsumes inter-refinability. (Thus using inter-refinability to police the replacement of the generically constructed system by one closer to application concerns, remains acceptable.) Obviously we have another square completion.

The square on the right of Fig. 2 is the dual of this construction. It shows that if we are given a (vertical) refinement and (horizontal) retrenchment converging to the same system, then we can complete the square generically to create a system, together with a suitable refinement and retrenchment, such that the dual properties of the postjoin construction hold. Thus we again have a retrenchment from top left to bottom right given by a fusion composition of the two routes round the square, and the universality of the basic construction is again characterised by inter-simulability, again strengthening under suitable circumstances to inter-refinability.

6 The Lifting Theorem

In this section we consider the Lifting Theorem in detail. The relevant part of Fig. 1 is elaborated in Fig. 3. The given systems are *Abs* and *Conc*, with the usual retrenchment between them. The constructed system is *Univ*, and the universal nature of its relationship with *Abs* and *Conc* is expressed by saying that whenever there is a system *Xtra*, enjoying similar properties to *Univ*, then *Xtra* is more abstract than *Univ*, i.e. there is a refinement from *Xtra* to *Univ*.

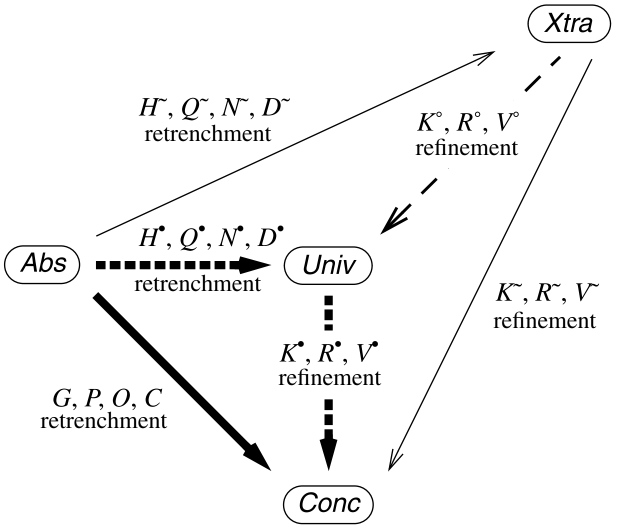


Fig. 3. The lifting construction in detail.

Theorem 6.1 Let *Abs* (with variables u, i, o) and *Conc* (with variables v, j, p) be two systems, and let there be a retrenchment from *Abs* to *Conc* with retrenchment data G, $\{P_{Op}, O_{Op}, C_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{AC}}\}$ where $\mathsf{Ops}_{\mathrm{AC}}$ is the set of common names of related operations of *Abs* and *Conc*. Then we have the following.

(1) There is a system *Univ* (with variables t, h, n), with operation name set $\mathsf{Ops}_{\mathrm{U}}$, where $\mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{C}}$, such that:

(i) there is a retrenchment from *Abs* to *Univ* (with retrenchment data $H^{\bullet}(u, t)$, $\{Q^{\bullet}_{Op}, N^{\bullet}_{Op}, D^{\bullet}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{AU}}\}$ say);

(ii) there is a refinement from *Univ* to *Conc* (with refinement data $K^{\bullet}(t, v)$, $\{R^{\bullet}_{Op}, V^{\bullet}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say), which is a birefinement;

(iii) the composition (in the sense of (4.9)-(4.12)) of the retrenchment $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ and refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ yields the retrenchment $G, G \wedge P, O, C$;

(iv) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Univ* are given by:

$$\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \equiv (\exists\, v, j \bullet K^{\bullet}(t, v) \wedge R^{\bullet}_{Op}(h, j) \wedge \mathrm{APP}_{Op_{\mathrm{C}}}(v, j)) \qquad (6.1)$$

(2) Whenever there is a system *Xtra* (with variables $t^{\sim}$, $h^{\sim}$, $n^{\sim}$), with operation name set Ops_X where $\mathsf{Ops}_X = \mathsf{Ops}_C$, with a retrenchment from *Abs* to *Xtra* given by $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$, with a refinement from *Xtra* to *Conc* given by $K^{\sim}$,$R^{\sim}$,$V^{\sim}$, where the composition of $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ and $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ yields G,$G \wedge P$,O,C, then:

   (i) there is a refinement from *Xtra* to *Univ* (with refinement data $K^{\circ}(t^{\sim}, t)$, $\{R^{\circ}_{Op}, V^{\circ}_{Op} \mid Op \in \mathsf{Ops}_U\}$ say);

   (ii) $H^{\sim} ⨾ K^{\circ} \Leftarrow H^{\bullet}$ and $(H^{\sim} \wedge Q^{\sim}) ⨾ (K^{\circ} \wedge R^{\circ}) \Leftarrow (H^{\bullet} \wedge Q^{\bullet})$ and $N^{\sim} ⨾ (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \Leftarrow N^{\bullet}$ and $D^{\sim} ⨾ (K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \Leftarrow D^{\bullet}$;

   (iii) $K^{\circ} ⨾ K^{\bullet} = K^{\sim}$ and $R^{\circ} ⨾ R^{\bullet} = R^{\sim}$ and $V^{\circ} ⨾ V^{\bullet} = V^{\sim}$.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-refinable.

Proof. For (1), we start by completing the details of *Univ*, and of the retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ and refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$. Assuming the usual conventions for *Abs* and *Conc*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V}$. There are two cases for the input and output spaces of *Univ*. If $Op \in \mathsf{Ops}_{AU}$ (in other words $Op \in \mathsf{Ops}_{AC}$), then we have $h \in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op}$. However if $Op \in \mathsf{Ops}_{U \setminus AU}$ (in other words $Op \in \mathsf{Ops}_C - \mathsf{Ops}_{AC} = \mathsf{Ops}_{C \setminus AC}$), then $h \in \mathsf{H}_{Op} = \mathsf{J}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{P}_{Op}$.

Initialisation in *Univ* is given by:

$$Init_U(t') \equiv (t' = (u', v') \wedge Init_A(u') \wedge Init_C(v') \wedge G(u', v')) \tag{6.2}$$

The operations of *Univ* are given by:

$$\begin{aligned}
&stp_{Op_U}(t, h, t', n) \equiv \\
&\quad (t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge \\
&\quad \{[G(u, v) \wedge P_{Op}(i, j, u, v) \wedge stp_{Op_A}(u, i, u', o) \wedge stp_{Op_C}(v, j, v', p) \wedge \\
&\qquad ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee C_{Op}(u', v', o, p; i, j, u, v))] \vee \\
&\quad [\neg(G(u, v) \wedge P_{Op}(i, j, u, v)) \wedge stp_{Op_C}(v, j, v', p)]\}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{AU} \\
&\quad (t' = (u', v') \wedge n = p \wedge h = j \wedge t = (u, v) \wedge stp_{Op_C}(v, j, v', p)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{U \setminus AU}
\end{aligned} \tag{6.3}$$

The retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is given by the data:[8]

$$H^{\bullet}(u, t) \equiv (t = (u, v) \wedge G(u, v)) \tag{6.4}$$

$$Q^{\bullet}_{Op}(i, h, u, t) \equiv (h = (i, j) \wedge t = (u, v) \wedge P_{Op}(i, j, u, v)) \tag{6.5}$$

$$\begin{aligned}
&N^{\bullet}_{Op}(o, n\,; u', t', i, h, u, t) \equiv \\
&\quad (t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge \\
&\quad O_{Op}(o, p; u', v', i, j, u, v))
\end{aligned} \tag{6.6}$$

$$\begin{aligned}
&D^{\bullet}_{Op}(u', t', o, n\,; i, h, u, t) \equiv \\
&\quad (t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge \\
&\quad C_{Op}(u', v', o, p; i, j, u, v))
\end{aligned} \tag{6.7}$$

8. Equation (6.4) in fact abbreviates $H^{\bullet}(u, t) \equiv (t = (\underline{u}, v) \wedge u = \underline{u} \wedge G(\underline{u}, v))$ (and then applies the one-point rule). We use this kind of shortcut extensively in the rest of the paper.

The refinement $K^\bullet,R^\bullet,V^\bullet$ is given by the data:

$$K^\bullet(t, v) \;\equiv\; (t = (u, v)) \tag{6.8}$$

$$R^\bullet{}_{Op}(h, j) \;\equiv\; \begin{cases} (h = (i, j)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{AU}} \\ (h = j) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U\backslash AU}} \end{cases} \tag{6.9}$$

$$V^\bullet{}_{Op}(n, p) \;\equiv\; \begin{cases} (n = (o, p)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{AU}} \\ (n = p) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U\backslash AU}} \end{cases} \tag{6.10}$$

For (1).(i), we need to check that $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ is a retrenchment. It is easy to check that with the G,P,O,C retrenchment initialisation PO, (6.2) and (6.4) give the needed $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ initialisation PO. For the operation PO, assume $H^\bullet$, $Q^\bullet{}_{Op}$, and the $Op \in \mathsf{Ops}_{\mathrm{AU}}$ case of (6.3) (of which only the $G \wedge P_{Op}$ subcase is needed). It is easy to see that one can produce a u' and an o (the u' and o inside the t' and n in (6.3)), for which $stp_{Op_{\mathrm{A}}}$ and $(G' \wedge O_{Op}) \vee C_{Op}$ (which are also in the $G \wedge P_{Op}$ subcase) hold. Repackaging the $G' \wedge O_{Op}$ into $H^{\bullet\prime} \wedge N^\bullet{}_{Op}$, and repackaging C_{Op} into $D^\bullet{}_{Op}$, we get what we need.

For (1).(ii), we need to check that $K^\bullet,R^\bullet,V^\bullet$ is a refinement. For the initialisation PO, assume $Init_{\mathrm{C}}(v')$. By (3.1), $v' \in \mathrm{ran}(G)$; so we can find a u' and hence a t' that makes (6.2) true; this t' is obviously related to v' by $K^\bullet$. For the operation PO, there are two cases, depending on whether $Op \in \mathsf{Ops}_{\mathrm{AU}}$ or $Op \in \mathsf{Ops}_{\mathrm{U\backslash AU}}$; and the $Op \in \mathsf{Ops}_{\mathrm{AU}}$ case itself splits into the $G \wedge P_{Op}$ and $\neg(G \wedge P_{Op})$ subcases. For the $Op \in \mathsf{Ops}_{\mathrm{AU}}$ case, assume $K^\bullet$, $R^\bullet{}_{Op}$, and $stp_{Op_{\mathrm{C}}}$. Given $K^\bullet \wedge R^\bullet{}_{Op}$, either $G \wedge P_{Op}$ holds (for the i, j, u, v, inside the t and h chosen for $K^\bullet \wedge R^\bullet{}_{Op}$), or it does not. If it does, then since we have $G \wedge P_{Op} \wedge stp_{Op_{\mathrm{C}}}$, we can apply the G,P,O,C retrenchment's operation PO (3.2) to get satisfying u' and o values that make the G,P,O,C retrenchment's simulation condition $G \wedge P_{Op} \wedge stp_{Op_{\mathrm{A}}} \wedge stp_{Op_{\mathrm{C}}} \wedge ((G' \wedge O_{Op}) \vee C_{Op})$ true. This gives a $stp_{Op_{\mathrm{U}}}$ transition according to the $G \wedge P_{Op}$ subcase of the $Op \in \mathsf{Ops}_{\mathrm{AU}}$ case of (6.3). If it does not, the $\neg(G \wedge P_{Op})$ subcase of (6.3) offers us a $stp_{Op_{\mathrm{U}}}$ transition, $\neg(G \wedge P_{Op}) \wedge stp_{Op_{\mathrm{C}}}$, based on the $stp_{Op_{\mathrm{C}}}$ which we assumed. In either case, all that we require of this transition is the projection $K^{\bullet\prime} \wedge V^\bullet{}_{Op}$, which is immediate given the first two clauses of (6.3). The argument for the $Op \in \mathsf{Ops}_{\mathrm{U\backslash AU}}$ case is similar to the previous one, except that the $K^{\bullet\prime} \wedge V^\bullet{}_{Op}$ projection is simpler.

For the birefinement claim, we need to check the converse refinement. For the initialisation PO, assume $Init_{\mathrm{U}}(t')$. The t' obviously projects under $K^\bullet$ to a v' for which $Init_{\mathrm{C}}(v')$ holds. For the operation PO, let t -(h, Op_{U}, n)-› t' be a step of *Univ*. If t and h project to v and j under $K^\bullet \wedge R^\bullet{}_{Op}$, then t' and n project to v' and p under $K^{\bullet\prime} \wedge V^\bullet{}_{Op}$, and (6.3) confirms that v -(j, Op_{C}, p)-› v' is a step of *Conc* since every case of (6.3) includes $stp_{Op_{\mathrm{C}}}$, discharging the PO.

For (1).(iii), we need to check that the composition of $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ and $K^\bullet,R^\bullet,V^\bullet$ (according to (4.9)-(4.12)) yields $G,G \wedge P,O,C$. But this is obvious given that $K^\bullet,R^\bullet,V^\bullet$ are simple projections.

For (1).(iv), we note that since $K^\bullet \wedge R^\bullet{}_{Op}$ is a total function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, it follows that $(K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op}) \mathbin{⨾} (K^\bullet \wedge R^\bullet{}_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}$. Consequently, the definition of the APP_{Op} sets of *Univ* in (6.1) satisfies the stipulation in (3.15) regarding the $K^\bullet,R^\bullet,V^\bullet$ birefinement. This completes (1).

For (2), we start with the data for the refinement K°,R°,V° which is given by:

$$K^{\circ}(t^{\sim}, t) \;\equiv\; (\exists\, v \bullet K^{\sim}(t^{\sim}, v) \wedge K^{\bullet}(t, v)) \tag{6.11}$$

$$R^{\circ}{}_{Op}(h^{\sim}, h) \;\equiv\; (\exists\, j \bullet R^{\sim}{}_{Op}(h^{\sim}, j) \wedge R^{\bullet}{}_{Op}(h, j)) \tag{6.12}$$

$$V^{\circ}{}_{Op}(n^{\sim}, n) \;\equiv\; (\exists\, p \bullet V^{\sim}{}_{Op}(n^{\sim}, p) \wedge V^{\bullet}{}_{Op}(n, p)) \tag{6.13}$$

For (2).(i), we start with the initialisation PO. Assume $Init_{\text{U}}(t')$ which gives $Init_{\text{C}} \wedge G'$ which gives $Init_{\text{C}} \wedge K^{\bullet\prime}$ when projected to *Conc*. From $Init_{\text{C}}$ we can derive $Init_{\text{X}} \wedge K^{\sim\prime}$ from the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement initialisation PO. So we have $Init_{\text{X}} \wedge (K^{\sim\prime} \wedge K^{\bullet\prime})$ which gives $Init_{\text{X}} \wedge K^{\circ\prime}$, which is what we need. For the operation PO we argue as follows. Let t -(h, Op_{U}, n)-› t' be a step of *Univ*, and suppose that $K^{\circ}(t^{\sim}, t) \wedge R^{\circ}{}_{Op}(h^{\sim}, h)$ holds. This implies: firstly, $K^{\sim}(t^{\sim}, v) \wedge K^{\bullet}(t, v)$ for the unique v that t projects to under $K^{\bullet}$; and secondly, $R^{\sim}{}_{Op}(h^{\sim}, j) \wedge R^{\bullet}{}_{Op}(h, j)$ for the unique j that h projects to under $R^{\bullet}$. As in the birefinement proof above, we derive a v -(j, Op_{C}, p)-› v' step of *Conc* to which t -(h, Op_{U}, n)-› t' projects. With this, and $K^{\sim} \wedge R^{\sim}{}_{Op}$, and the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement operation PO, we derive a $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ step of *Xtra* such that $K^{\sim\prime} \wedge V^{\sim}{}_{Op}$ holds for $t^{\sim\prime}$ and $n^{\sim}$. Altogether, from step t -(h, Op_{U}, n)-› t' and $K^{\circ} \wedge R^{\circ}{}_{Op}$ we have derived step $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ such that $K^{\sim\prime} \wedge K^{\bullet\prime} \wedge V^{\sim}{}_{Op} \wedge V^{\bullet}{}_{Op}$, or in other words $K^{\circ\prime} \wedge V^{\circ}{}_{Op}$, holds. This is what we need.

Beyond this, if the notion of refinement requires the use of APP_{Op} sets, then we must show that if a dependency like (3.9) or (3.10) holds between the APP_{Op} sets of *Conc* and those of *Xtra* in the context of the $K^{\sim}, R^{\sim}, V^{\sim}$ refinement, then a similar dependency holds between the APP_{Op} sets of *Univ* and those of *Xtra* in the context of the $K^{\circ}, R^{\circ}, V^{\circ}$ refinement. For this, we note that the (3.15) stipulation means that, for a (3.9) type dependency, if $\text{APP}_{Op_{\text{X}}}(t^{\sim}, h^{\sim}) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\sim}{}_{Op}(h^{\sim}, j) \Rightarrow \text{APP}_{Op_{\text{C}}}(v, j)$ holds, then $\text{APP}_{Op_{\text{X}}}(t^{\sim}, h^{\sim}) \wedge K^{\circ}(t^{\sim}, t) \wedge R^{\circ}{}_{Op}(h^{\sim}, h) \Rightarrow \text{APP}_{Op_{\text{U}}}(t, h)$ will also hold, by composing $K^{\sim} \wedge R^{\sim}{}_{Op}$ with $K^{\bullet\text{T}} \wedge R^{\bullet\text{T}}{}_{Op}$. Similarly, for a (3.10) type dependency, again by composing $K^{\sim} \wedge R^{\sim}{}_{Op}$ with $K^{\bullet\text{T}} \wedge R^{\bullet\text{T}}{}_{Op}$, if $\text{APP}_{Op_{\text{X}}}(t^{\sim}, h^{\sim}) \Leftarrow K^{\sim}(t^{\sim}, v) \wedge R^{\sim}{}_{Op}(h^{\sim}, j) \wedge \text{APP}_{Op_{\text{C}}}(v, j)$ holds, then $\text{APP}_{Op_{\text{X}}}(t^{\sim}, h^{\sim}) \Leftarrow K^{\circ}(t^{\sim}, t) \wedge R^{\circ}{}_{Op}(h^{\sim}, h) \wedge \text{APP}_{Op_{\text{U}}}(t, h)$ will also hold.

For (2).(ii), since $K^{\circ} = K^{\sim} \fatsemi K^{\bullet\text{T}}$ and $H^{\sim} \fatsemi K^{\sim} = G$, then $H^{\sim} \fatsemi K^{\circ} = H^{\sim} \fatsemi K^{\sim} \fatsemi K^{\bullet\text{T}} = G \fatsemi K^{\bullet\text{T}} \Leftarrow H^{\bullet}$. The last implication holds because while every $t = (u, v)$ with $\neg G(u, v)$ is in $\text{ran}(K^{\bullet\text{T}})$, no such t is in $\text{ran}(H^{\bullet})$. The remaining results are similar.

For (2).(iii), since $K^{\circ} = K^{\sim} \fatsemi K^{\bullet\text{T}}$, then $K^{\circ} \fatsemi K^{\bullet} = K^{\sim} \fatsemi K^{\bullet\text{T}} \fatsemi K^{\bullet} = K^{\sim} \fatsemi \text{Id}_{\text{V}} = K^{\sim}$ (since $K^{\bullet\text{T}}$ is an inverse function). The remaining results are similar. This completes (2).

For (3), we note that *Univ* itself satisfies the criteria demanded of *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** satisfies the criteria demanded of *Xtra* too. Hence we can construct two instances of Fig. 3 as follows. In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there is a refinement $K^{\circ}, R^{\circ}, V^{\circ}$, from *Univ** to *Univ*. In the second, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there is a refinement K^{*}, R^{*}, V^{*}, from *Univ* to *Univ**. So *Univ* and *Univ** are inter-refinable. We are done. ☺

6.1 Remarks

Remark 6.2 Referring to the last clause of Theorem 6.1, the composition of K^{*}, R^{*}, V^{*}, with $K^{\circ}, R^{\circ}, V^{\circ}$, yields a refinement from *Univ* to itself (similarly for *Univ**). There is no necessity for this refinement to be the identity. In particular, if the *Univ* system contains internal symmetries of a suitable kind, then $K^{*} \fatsemi K^{\circ}$ may permute 'similar' states, or worse, map some of them to the same state, etc. Our notion of 'inter-refinable' does not prevent this. Of course, if it *is* a permutation, then composing it suitably with one of the two refinements yields a birefinement.

Remark 6.3 The last clause of Theorem 6.1, in effect, presents a notion of system equivalence, namely 'inter-refinability'. It is important to be aware that this is potentially a rather weak notion of equivalence, related to notions of bisimilarity, and much weaker than, say, set theoretic isomorphism of transition systems. Much hinges on how strong or weak the retrieve relation connecting the state spaces is. If it is strong, and relates a state in one system to few states in the other, then the correspondence established can be precise and informative. If it is weak, and relates a state in one system to many states in the other, then the correspondence established can be rather vague. In our particular case, we had a retrieve relation that was a projection — such a relation completely ignores what may or may not be going on in the 'orthogonal' component of the projected system. As a consequence of all this, the fact that a certain system might be appropriate for a certain set of requirements, does not automatically imply that a system inter-refinable with it is equally appropriate for those requirements — unless one takes great care over what one means by 'requirements' and 'appropriate'.

Remark 6.4 It is tempting to think that[9] the K°,R°,V°, arrow in Fig. 3 is the wrong way round. Looking at the diagram, and the relative dispositions of *Abs* and *Conc* within it, it seems that the most natural property of the *Univ* system to ask for is that it furnishes the most *abstract* system that accomplishes the factorisation. In such a case there ought to be a refinement *from Univ to* the system *Xtra* that accomplishes any alternative factorisation. This was the strategy pursued in [Jeske (2005)] and earlier investigations. However, looking into the mathematics of this approach, the details are neither simple nor do they suggest a straightforward integration with the other results we pursue in this paper *in terms of characterising the notion of universality that composite constructions might enjoy.* The alternative, described here, focuses on the most concrete system that accomplishes the factorisation. Now, the technical difficulties that plagued the earlier approaches just melt away. Furthermore, the composite constructions that one might imagine are much more understandable. For instance, imagine a commuting square of retrenchments and refinements (as occurs in Fig. 2) abutting the *Abs* to *Univ* retrenchment of Fig. 3. Then, in a natural way, *Univ* refines the system (call it *Xtra*) directly above it. Composing the converse refinement directly above *Abs*, with the retrenchment across the top of the square, yields, in benign cases, a retrenchment from *Abs* to *Xtra* which, with the *Xtra* to *Univ* refinement, can be understood to yield an instance of Fig. 3. The alternative approach, with *Univ* as the most abstract system, does not enjoy such natural properties. Another reason to prefer the current approach, is that it allows a very natural decoupling of the APP_{Op} sets discussion from the remainder of the construction, giving a very generic feel to this aspect of the theory. Again, this smooth genericity does not emerge using alternative approaches. In the end, the argument between 'most abstract' and 'most concrete' is not one that can be resolved unequivocally on meta- criteria alone, and it is the persuasiveness of the mathematics that sways our treatment in this paper.

9. Translation: 'For a long time the authors thought that ...'.

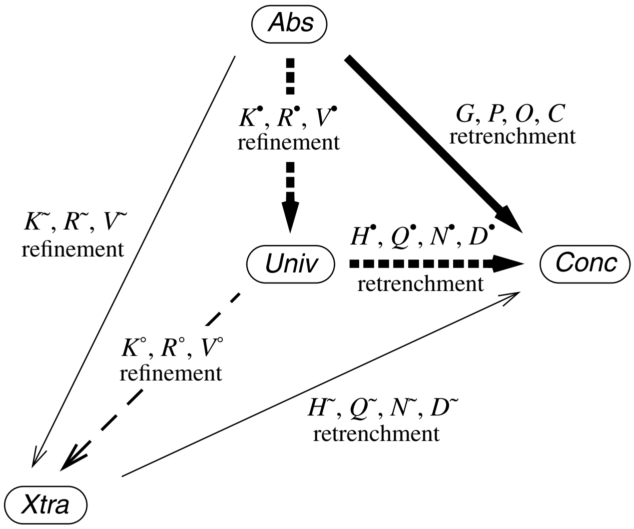


Fig. 4. The lowering construction in detail.

7 The Lowering Theorem

In this section we consider the Lowering Theorem in detail. It can be seen to be dual, in a suitable sense, to the Lifting Theorem. The relevant part of Fig. 1 is elaborated in Fig. 4. The given systems are *Abs* and *Conc*, with the usual retrenchment between them. The constructed system is *Univ* again, and the universal nature of its relationship with *Abs* and *Conc* is expressed by saying that whenever there is a system *Xtra*, enjoying similar properties to *Univ*, then *Xtra* is more concrete than *Univ*, i.e. there is a refinement from *Univ* to *Xtra*.

Theorem 7.1 Let *Abs* (with variables u, i, o) and *Conc* (with variables v, j, p) be two systems, and let there be a retrenchment from *Abs* to *Conc* with retrenchment data G, $\{P_{Op}, O_{Op}, C_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{AC}}\}$ where $\mathsf{Ops}_{\mathrm{AC}}$ is the set of common names of related operations of *Abs* and *Conc*. Then we have the following.

(1) There is a system *Univ* (with variables t, h, n), with operation name set $\mathsf{Ops}_{\mathrm{U}}$, where $\mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{A}}$, such that:

(i) there is a refinement from *Abs* to *Univ* (with refinement data $K^\bullet(u, t)$, $\{R^\bullet{}_{Op}, V^\bullet{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{A}}\}$ say), which is a birefinement;

(ii) there is a retrenchment from *Univ* to *Conc* (with retrenchment data $H^\bullet(t, v)$, $\{Q^\bullet{}_{Op}, N^\bullet{}_{Op}, D^\bullet{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{UC}}\}$ say);

(iii) the composition (in the sense of the dual of (4.9)-(4.12)) of the refinement $K^\bullet, R^\bullet, V^\bullet$ and retrenchment $H^\bullet, Q^\bullet, N^\bullet, D^\bullet$ yields the retrenchment $G, G \wedge P, O, C$;

(iv) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Univ* are given by:

$$\text{APP}_{Op_{\mathrm{U}}}(t, h) \;\equiv\; (\exists\, u, i \bullet K^{\bullet}(u, t) \wedge R^{\bullet}{}_{Op}(i, h) \wedge \text{APP}_{Op_{\mathrm{A}}}(u, i)) \qquad (7.1)$$

(2) Whenever there is a system *Xtra* (with variables $t^{\sim}$, $h^{\sim}$, $n^{\sim}$), with operation name set $\mathsf{Ops}_{\mathrm{X}}$ where $\mathsf{Ops}_{\mathrm{X}} = \mathsf{Ops}_{\mathrm{A}}$, with a refinement from *Abs* to *Xtra* given by $K^{\sim}$,$R^{\sim}$,$V^{\sim}$, with a retrenchment from *Xtra* to *Conc* given by $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$, where the composition of $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ and $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ yields G,$G \wedge P$,O,C, then:

(i) there is a refinement from *Univ* to *Xtra* (with refinement data $K^{\circ}(t, t^{\sim})$, $\{R^{\circ}{}_{Op}, V^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say);

(ii) $K^{\circ} \fatsemi H^{\sim} \Leftarrow H^{\bullet}$ and $(K^{\circ} \wedge R^{\circ}) \fatsemi (H^{\sim} \wedge Q^{\sim}) \Leftarrow (H^{\bullet} \wedge Q^{\bullet})$ and $(K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \fatsemi N^{\sim} \Leftarrow N^{\bullet}$ and $(K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \fatsemi D^{\sim} \Leftarrow D^{\bullet}$;

(iii) $K^{\bullet} \fatsemi K^{\circ} = K^{\sim}$ and $R^{\bullet} \fatsemi R^{\circ} = R^{\sim}$ and $V^{\bullet} \fatsemi V^{\circ} = V^{\sim}$.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-refinable.

Proof. For (1), we start by completing the details of *Univ*, and of the refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ and retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$. Assuming the usual conventions for *Abs* and *Conc*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V}$. There are two cases for the input and output spaces of *Univ*. If $Op \in \mathsf{Ops}_{\mathrm{UC}}$ (in other words $Op \in \mathsf{Ops}_{\mathrm{AC}}$), then we have $h \in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op}$. However if $Op \in \mathsf{Ops}_{\mathrm{U \setminus UC}}$ (in other words $Op \in \mathsf{Ops}_{\mathrm{A}} - \mathsf{Ops}_{\mathrm{AC}} = \mathsf{Ops}_{\mathrm{A \setminus AC}}$), then $h \in \mathsf{H}_{Op} = \mathsf{I}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{O}_{Op}$.

Initialisation in *Univ* is given by:

$$Init_{\mathrm{U}}(t') \;\equiv\; (t' = (u', v') \wedge Init_{\mathrm{A}}(u')) \qquad (7.2)$$

The operations of *Univ* are given by:

$$\begin{aligned} stp_{Op_{\mathrm{U}}}(t, h, t', n) \;\equiv\; & \\ & (t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge stp_{Op_{\mathrm{A}}}(u, i, u', o)) \\ & \qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UC}} \\ & (t' = (u', v') \wedge n = o \wedge h = i \wedge t = (u, v) \wedge stp_{Op_{\mathrm{A}}}(u, i, u', o)) \\ & \qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{U \setminus UC}} \end{aligned} \qquad (7.3)$$

The refinement $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is given by the data:

$$K^{\bullet}(u, t) \;\equiv\; (t = (u, v)) \qquad (7.4)$$

$$\begin{aligned} R^{\bullet}{}_{Op}(i, h) \;\equiv\; & (h = (i, j)) && \text{if } Op \in \mathsf{Ops}_{\mathrm{UC}} \\ & (h = i) && \text{if } Op \in \mathsf{Ops}_{\mathrm{U \setminus UC}} \end{aligned} \qquad (7.5)$$

$$\begin{aligned} V^{\bullet}{}_{Op}(o, n) \;\equiv\; & (n = (o, p)) && \text{if } Op \in \mathsf{Ops}_{\mathrm{UC}} \\ & (n = o) && \text{if } Op \in \mathsf{Ops}_{\mathrm{U \setminus UC}} \end{aligned} \qquad (7.6)$$

The retrenchment $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is given by the data:

$$H^{\bullet}(t, v) \;\equiv\; (t = (u, v) \wedge G(u, v)) \qquad (7.7)$$

$$Q^{\bullet}{}_{Op}(h, j, t, v) \;\equiv\; (h = (i, j) \wedge t = (u, v) \wedge P_{Op}(i, j, u, v)) \qquad (7.8)$$

$$N^{\bullet}{}_{Op}(n, p\ ;\ t', v', h, j, t, v)\ \equiv$$
$$(t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge$$
$$O_{Op}(o, p; u', v', i, j, u, v)) \tag{7.9}$$

$$D^{\bullet}{}_{Op}(t', v', n, p\ ;\ h, j, t, v)\ \equiv$$
$$(t' = (u', v') \wedge n = (o, p) \wedge h = (i, j) \wedge t = (u, v) \wedge$$
$$C_{Op}(u', v', o, p; i, j, u, v)) \tag{7.10}$$

For (1).(i), we need to check that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement. For the initialisation PO, suppose $Init_{\mathrm{U}}(t')$ holds. Since this implies $Init_{\mathrm{A}}(u')$ for the u' inside t', and $K^{\bullet}$ projects t' to u', the PO is discharged. For the operation PO, suppose we have a step of *Univ* t -(h, Op_{U}, n)-› t', and $K^{\bullet}(u, t) \wedge R^{\bullet}{}_{Op}(i, h)$. The *Univ* step clearly contains an *Abs* step, u -(i, Op_{A}, o)-› u', in which u' and o are the projections of t' and n under $K^{\bullet\prime} \wedge V^{\bullet}{}_{Op}$. The latter is regardless of whether the projections $R^{\bullet}{}_{Op}$ and $V^{\bullet}{}_{Op}$ belong to the $Op \in \mathsf{Ops}_{\mathrm{UC}}$ or $Op \in \mathsf{Ops}_{\mathrm{U\backslash UC}}$ cases. This gives us what we need.

Regarding the birefinement claim, for the initialisation PO, let $Init_{\mathrm{A}}(u')$ hold. Then $K^{\bullet}(u', t')$ holds for any v' where $t' = (u', v')$, which is enough for (7.2), discharging the PO. For the operation PO, suppose that we have a step u -(i, Op_{A}, o)-› u' of *Abs*, and $K^{\bullet}(u, t) \wedge R^{\bullet}{}_{Op}(i, h)$. The *Abs* step extends to any *Univ* step, t -(h, Op_{U}, n)-› t' such that t' and n project via $K^{\bullet\prime} \wedge V^{\bullet}{}_{Op}$ to u' and o, discharging the PO. Again, this works regardless of whether the projections $R^{\bullet}{}_{Op}$ and $V^{\bullet}{}_{Op}$ belong to the $Op \in \mathsf{Ops}_{\mathrm{UC}}$ or $Op \in \mathsf{Ops}_{\mathrm{U\backslash UC}}$ cases.

For (1).(ii), we need to check that $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is a retrenchment. For the initialisation PO, suppose $Init_{\mathrm{C}}(v')$ holds. Then by (3.1), there is a u' such that $Init_{\mathrm{A}}(u') \wedge G(u', v')$ holds. But this equivalent to $Init_{\mathrm{U}}(t') \wedge H^{\bullet}(t', v')$ for the obvious t', discharging the PO. For the operation PO, suppose that we have $H^{\bullet}$ and $Q^{\bullet}{}_{Op}$ and $stp_{Op_{\mathrm{C}}}$. Then we combine the G and P_{Op} inside $H^{\bullet}$ and $Q^{\bullet}{}_{Op}$ with $stp_{Op_{\mathrm{C}}}$ and the G,P,O,C retrenchment operation PO (3.2), to derive a step u -(i, Op_{A}, o)-› u' of the *Abs* system for which $(G' \wedge O_{Op}) \vee C_{Op}$ holds. Repackaging the $G' \wedge O_{Op}$ into $H^{\bullet\prime} \wedge N^{\bullet}{}_{Op}$, and repackaging C_{Op} into $D^{\bullet}{}_{Op}$, we get what we need.

For (1).(iii), we need to check that the composition of $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ and $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ (according to the dual of (4.9)-(4.12)) yields G,$G \wedge P$,O,C. But this is obvious given that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ are simple projections.

For (1).(iv), since $K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op}$ is a total function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{U} \times \mathsf{I}_{Op}$, we have $(K^{\bullet} \wedge R^{\bullet}{}_{Op}) \mathbin{⨾} (K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op}) = \mathrm{Id}_{\mathsf{U} \times \mathsf{I}_{Op}}$. Consequently, the definition of the APP_{Op} sets of *Univ* in (7.1) satisfies the stipulation in (3.15) as regards the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ birefinement. This completes (1).

For (2), we start with the data for the refinement K°,R°,V° which is given by:

$$K^{\circ}(t, t^{\sim})\ \equiv\ (\exists\, u \bullet K^{\bullet}(u, t) \wedge K^{\sim}(u, t^{\sim})) \tag{7.11}$$

$$R^{\circ}{}_{Op}(h, h^{\sim})\ \equiv\ (\exists\, i \bullet R^{\bullet}{}_{Op}(i, h) \wedge R^{\sim}{}_{Op}(i, h^{\sim})) \tag{7.12}$$

$$V^{\circ}{}_{Op}(n, n^{\sim})\ \equiv\ (\exists\, o \bullet V^{\bullet}{}_{Op}(o, n) \wedge V^{\sim}{}_{Op}(o, n^{\sim})) \tag{7.13}$$

For (2).(i), we must show that K°,R°,V° is a refinement. For the initialisation PO, let us assume $Init_{\mathrm{X}}(t^{\sim\prime})$. Since $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, there is a u' for which $Init_{\mathrm{A}}(u') \wedge K^{\sim}(u', t^{\sim\prime})$ holds. Since $Init_{\mathrm{A}}(u')$ holds, taking any v' and setting $t' = (u', v')$, we get $Init_{\mathrm{U}}(t')$ by (7.2). We also have $K^{\bullet}(u', t')$, so $K^{\circ}(t, t^{\sim})$ holds by (7.11) and we are done.

For the operation PO, let $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ be a step of ***Xtra*** such that $K^{\circ}(t, t^{\sim}) \wedge R^{\circ}_{Op}(h, h^{\sim})$ also holds. From $K^{\circ}\wedge R^{\circ}_{Op}$, which is $K^{\bullet}\wedge K^{\sim}\wedge R^{\bullet}_{Op}\wedge R^{\sim}_{Op}$, we get a u and i such that $K^{\sim}\wedge R^{\sim}_{Op}$ holds, whereby, since $K^{\sim},R^{\sim},V^{\sim}$ is a refinement, we can find a step of ***Abs***, u -(i, Op_{A}, o)-› u' such that $K^{\sim\prime}\wedge V^{\sim}_{Op}$ holds for u' and o. This ***Abs*** step, and $K^{\bullet}\wedge R^{\bullet}_{Op}$, can be combined with the fact that $K^{\bullet},R^{\bullet},V^{\bullet}$ is a birefinement, to derive a ***Univ*** step t -(h, Op_{U}, n)-› t' for which $K^{\bullet\prime}\wedge V^{\bullet}_{Op}$, and hence $K^{\circ\prime}\wedge V^{\circ}_{Op}$, holds for t' and n. This discharges the PO.

Beyond this, if the notion of refinement requires the use of APP_{Op} sets, then we must show that if a dependency as in (3.9) or (3.10) holds between the APP_{Op} sets of ***Abs*** and those of ***Xtra*** in the context of the $K^{\sim},R^{\sim},V^{\sim}$ refinement, then a similar dependency holds between the APP_{Op} sets of ***Univ*** and those of ***Xtra*** in the context of the $K^{\circ},R^{\circ},V^{\circ}$ refinement. For this, we note that the (3.15) stipulation means that, for a (3.9) type dependency, if $\mathrm{APP}_{Op_{\mathrm{A}}}(u, i) \wedge K^{\sim}(u, t^{\sim}) \wedge R^{\sim}_{Op}(i, h^{\sim}) \Rightarrow \mathrm{APP}_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim})$ holds, then $\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \wedge K^{\circ}(t, t^{\sim}) \wedge R^{\circ}_{Op}(h, h^{\sim}) \Rightarrow \mathrm{APP}_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim})$ will also hold, by composing $K^{\sim\mathrm{T}}\wedge R^{\sim\mathrm{T}}_{Op}$ with $K^{\bullet}\wedge R^{\bullet}_{Op}$. Similarly, for a (3.10) type dependency, by composing $K^{\sim\mathrm{T}}\wedge R^{\sim\mathrm{T}}_{Op}$ with $K^{\bullet}\wedge R^{\bullet}_{Op}$ again, if $\mathrm{APP}_{Op_{\mathrm{A}}}(u, i) \Leftarrow K^{\sim}(u, t^{\sim}) \wedge R^{\sim}_{Op}(i, h^{\sim}) \wedge \mathrm{APP}_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim})$ holds, then $\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \Leftarrow K^{\circ}(t, t^{\sim}) \wedge R^{\circ}_{Op}(h, h^{\sim}) \wedge \mathrm{APP}_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim})$ will also hold.

For (2).(ii), since $K^{\circ} = K^{\bullet\mathrm{T}} ⨾ K^{\sim}$ and $K^{\sim} ⨾ H^{\sim} = G$, then $K^{\circ} ⨾ H^{\sim} = K^{\bullet\mathrm{T}} ⨾ K^{\sim} ⨾ H^{\sim} = K^{\bullet\mathrm{T}} ⨾ G \Leftarrow H^{\bullet}$. The last implication holds because while every $t = (u, v)$ with $\neg G(u, v)$ is in $\mathrm{dom}(K^{\bullet\mathrm{T}})$, no such t is in $\mathrm{dom}(H^{\bullet})$. The remaining results are similar.

For (2).(iii), since $K^{\circ} = K^{\bullet\mathrm{T}} ⨾ K^{\sim}$, then $K^{\bullet} ⨾ K^{\circ} = K^{\bullet} ⨾ K^{\bullet\mathrm{T}} ⨾ K^{\sim} = \mathrm{Id}_{\mathrm{T}} ⨾ K^{\sim} = K^{\sim}$ (since $K^{\bullet\mathrm{T}}$ is a function). The remaining results are similar. This completes (2).

For (3), we note that ***Univ*** itself satisfies the criteria demanded of ***Xtra***. Therefore, if we have a system ***Univ***** with the properties (1) and (2) of ***Univ***, then ***Univ***** satisfies the criteria demanded of ***Xtra*** too. Hence we can construct two instances of Fig. 4 as follows. In the first, ***Univ*** is in its conventional place and ***Univ***** replaces ***Xtra***, and there is a refinement $K^{\circ},R^{\circ},V^{\circ}$ from ***Univ*** to ***Univ*****. In the second, ***Univ***** replaces ***Univ***, and ***Univ*** replaces ***Xtra***, and there is a refinement K^{*},R^{*},V^{*} from ***Univ***** to ***Univ***. So ***Univ*** and ***Univ***** are inter-refinable. We are done. ☺

7.1 Remarks

The following mimic corresponding remarks in Section 6, so are stated briefly.

Remark 7.2 As in Remark 6.2, the composition of K^{*},R^{*},V^{*} with $K^{\circ},R^{\circ},V^{\circ}$ need not be the identity. As there, if it happens to be a permutation, we can recover a birefinement.

Remark 7.3 As in Remark 6.3, the 'inter-refinability' notion of equivalence is weaker than a given requirements context might need, so should be used with care in an applications scenario.

Remark 7.4 As in Remark 6.4, it is tempting to think that the $K^{\circ},R^{\circ},V^{\circ}$ arrow in Fig. 4 is the wrong way round. However the comments in Remark 6.4 apply just as strongly here, though in a suitably dual sense.

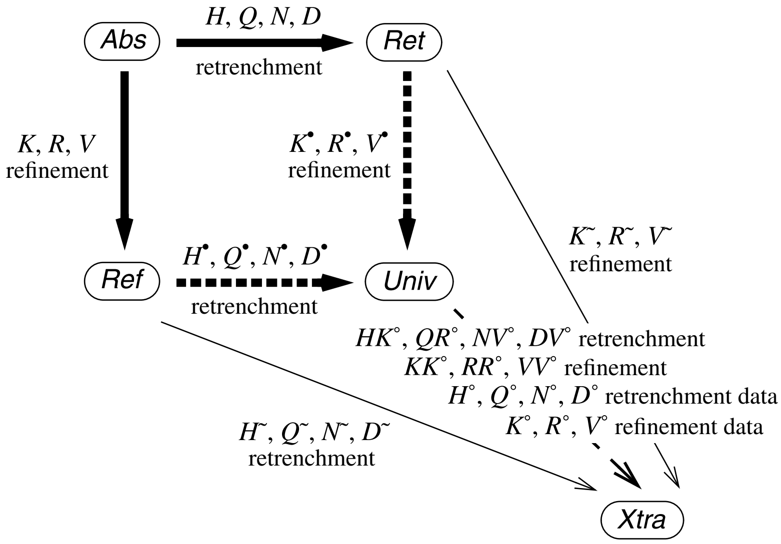


Fig. 5. The postjoin construction in detail. The pseudoretrenchment $G^{\times}$,$G^{\times}\wedge P^{\times}$,$O^{\times}$,$C^{\times}$ (not shown) connects *Ret* to *Ref*.

8 The Postjoin Theorem

In this section we consider the Postjoin Theorem in detail. The relevant part of Fig. 2 is elaborated in Fig. 5. The given systems are *Abs* together with *Ret* and *Ref*. There is a retrenchment from *Abs* to *Ret* and a refinement from *Abs* to *Ref*, the data for these being the usual ones. The constructed system is *Univ*, with a retrenchment from *Ref* to *Univ* and a refinement from *Ret* to *Univ*. The universal nature of the relationship between *Univ* and the other systems is expressed by saying that whenever there is a system *Xtra*, enjoying similar properties to *Univ*, then *Xtra* is more concrete than *Univ*, witnessed by 'in simulation' relationships between the transitions of *Univ* and *Xtra*, strengthened under relatively benign conditions, to a retrenchment —and still further to a refinement— from *Univ* to *Xtra*.

Theorem 8.1 Let *Abs* (with variables u, i, o, operation names $\mathsf{Ops}_{\mathrm{A}}$) and *Ret* (with variables v, j, p, operation names $\mathsf{Ops}_{\mathrm{T}}$) and *Ref* (with variables w, k, q, operation names $\mathsf{Ops}_{\mathrm{F}}$) be three systems. Let there be a retrenchment from *Abs* to *Ret* with retrenchment data H, $\{Q_{Op}, N_{Op}, D_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{AT}}\}$ where $\mathsf{Ops}_{\mathrm{AT}}$ is the set of common names of related operations of *Abs* and *Ret*. Let there be a refinement from *Abs* to *Ref* with refinement data K, $\{R_{Op}, V_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{A}} = \mathsf{Ops}_{\mathrm{F}}\}$ where $\mathsf{Ops}_{\mathrm{A}}$ is the set of operation names of both *Abs* and *Ref*. Suppose, for all Op, that $H \wedge Q_{Op}$ is a non-empty relation. Then we have the following.

(1) There is a system *Univ* (with variables t, h, n), with operation name set Ops_U, where $\mathsf{Ops}_\mathrm{U} = \mathsf{Ops}_\mathrm{T}$, such that:

(i) there is a refinement from *Ret* to *Univ* (with refinement data $K^\bullet(v, t)$, $\{R^\bullet{}_{Op}, V^\bullet{}_{Op} \mid Op \in \mathsf{Ops}_\mathrm{T} = \mathsf{Ops}_\mathrm{U}\}$ say);

(ii) there is a retrenchment from *Ref* to *Univ* (with retrenchment data $H^\bullet(w, t)$, $\{Q^\bullet{}_{Op}, N^\bullet{}_{Op}, D^\bullet{}_{Op} \mid Op \in \mathsf{Ops}_\mathrm{FU}\}$ say);

(iii) the composition of the pseudoretrenchment $H^\mathrm{T}, Q^\mathrm{T}, N^\mathrm{T}, D^\mathrm{T}$ with the refinement K, R, V yields a pseudoretrenchment $G^\times, G^\times \wedge P^\times, O^\times, C^\times$, which is also given by the composition of the refinement $K^\bullet, R^\bullet, V^\bullet$ with the pseudoretrenchment $H^{\bullet\mathrm{T}}, Q^{\bullet\mathrm{T}}, N^{\bullet\mathrm{T}}, D^{\bullet\mathrm{T}}$;

(iv) each transition of *Univ* is in simulation with a transition of *Ret*, and if $Op \in \mathsf{Ops}_\mathrm{FU}$, it is also in simulation with a transition of *Ref*, and in the latter case, any such pair of *Ret* and *Ref* transitions are in simulation via the pseudoretrenchment $G^\times, G^\times \wedge P^\times, O^\times, C^\times$;

(v) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Univ* are given by:

$$\mathrm{APP}_{Op_\mathrm{U}}(t, h) \equiv (\exists\, v, j \bullet K^\bullet(v, t) \wedge R^\bullet{}_{Op}(j, h) \wedge \mathrm{APP}_{Op_\mathrm{T}}(v, j)) \tag{8.1}$$

(2) Whenever there is a system *Xtra* (with variables $t^\sim$, $h^\sim$, $n^\sim$), with operation name set Ops_X where $\mathsf{Ops}_\mathrm{X} = \mathsf{Ops}_\mathrm{T}$, with a refinement from *Ret* to *Xtra* given by $K^\sim, R^\sim, V^\sim$, with a retrenchment from *Ref* to *Xtra* given by $H^\sim, Q^\sim, N^\sim, D^\sim$, where the composition of the refinement $K^\sim, R^\sim, V^\sim$ with the pseudoretrenchment $H^{\sim\mathrm{T}}, Q^{\sim\mathrm{T}}, N^{\sim\mathrm{T}}, D^{\sim\mathrm{T}}$ yields the pseudoretrenchment $G^\times, G^\times \wedge P^\times, O^\times, C^\times$, where each transition of *Xtra* is in simulation with a transition of *Ret*, and if $Op_\mathrm{X} \in \mathsf{Ops}_\mathrm{FX}$ it is also in simulation with a transition of *Ref*, and where in the latter case any such pair of *Ret* and *Ref* transitions are in simulation via the pseudoretrenchment $G^\times, G^\times \wedge P^\times, O^\times, C^\times$, then:

(i) there exist refinement data, $K^\circ(t, t^\sim)$, $\{R^\circ{}_{Op}, V^\circ{}_{Op} \mid Op \in \mathsf{Ops}_\mathrm{U}\}$ say, from *Univ* to *Xtra*, via which, every transition of *Xtra* is in simulation with a transition of *Univ*;

(ii) there exist retrenchment data, $H^\circ(t, t^\sim)$, $\{Q^\circ{}_{Op}, N^\circ{}_{Op}, D^\circ{}_{Op} \mid Op \in \mathsf{Ops}_\mathrm{U}\}$ say, from *Univ* to *Xtra*, via which, every $Op_\mathrm{X} \in \mathsf{Ops}_\mathrm{FX}$ transition of *Xtra* is in simulation with a transition of *Univ*, and if it also holds that $(\forall\, v \bullet \exists\, u, w \bullet \neg H(u, v) \wedge K(u, w))$, then every other transition of *Xtra* is also in simulation with a transition of *Univ*;

(iii) $K^\bullet \mathbin{⨾} K^\circ = K^\sim$ and $R^\bullet \mathbin{⨾} R^\circ = R^\sim$ and $V^\bullet \mathbin{⨾} V^\circ = V^\sim$;

(iv) $H^\bullet \mathbin{⨾} H^\circ = H^\sim$ and for $Op_\mathrm{X} \in \mathsf{Ops}_\mathrm{FX}$, $(H^\bullet \wedge Q^\bullet) \mathbin{⨾} (H^\circ \wedge Q^\circ) = (H^\sim \wedge Q^\sim)$ and $N^\bullet \mathbin{⨾} N^\circ = N^\sim$ and $D^\bullet \mathbin{⨾} D^\circ \Leftarrow D^\sim$;

(v) there exist retrenchment data, $HK^\circ(t, t^\sim)$, $\{QR^\circ{}_{Op}, NV^\circ{}_{Op}, DV^\circ{}_{Op} \mid Op \in \mathsf{Ops}_\mathrm{U}\}$ say, from *Univ* to *Xtra*, via which, every transition of *Xtra* is in simulation with a transition of *Univ*.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-simulable.

(4) There is a retrenchment from *Abs* to *Univ* (with retrenchment data $G(u, t)$, $\{P_{Op}, O_{Op}, C_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{AU}}\}$ say), given by the disjunctive fusion composition of two retrenchments (a) and (b): (a) is the vertical composition of H,Q,N,D with $K^\bullet,R^\bullet,V^\bullet$; (b) is the vertical composition of K,R,V with $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$.

(5) Suppose that:

$$
\begin{aligned}
&(\mathrm{dom}(K\wedge R\wedge K'\wedge V)\lhd H\wedge Q\wedge H'\wedge N)(\underline{u}, v, \underline{i}, j, u', v', o, p) \wedge \\
&(\mathrm{dom}(H\wedge Q\wedge H'\wedge N)\lhd K\wedge R\wedge K'\wedge V)(\underline{u}, w, \underline{i}, k, u', w', o, q) \wedge \\
&(\mathrm{dom}(K\wedge R)\lhd H\wedge Q)(i, j, u, v) \wedge (\mathrm{dom}(H\wedge Q)\lhd K\wedge R)(i, k, u, w) \;\Rightarrow \\
&\qquad (\mathrm{dom}(K\wedge R\wedge K'\wedge V)\lhd H\wedge Q\wedge H'\wedge N)(u, v, i, j, u', v', o, p) \wedge \\
&\qquad (\mathrm{dom}(H\wedge Q\wedge H'\wedge N)\lhd K\wedge R\wedge K'\wedge V)(u, w, i, k, u', w', o, q)
\end{aligned}
\tag{8.2}
$$

$$
\begin{aligned}
&(\mathrm{dom}(K\wedge R\wedge K'\wedge V)\lhd H\wedge Q\wedge D)(\underline{u}, v, \underline{i}, j, u', v', o, p) \wedge \\
&(\mathrm{dom}(H\wedge Q\wedge D)\lhd K\wedge R\wedge K'\wedge V)(\underline{u}, w, \underline{i}, k, u', w', o, q) \wedge \\
&(\mathrm{dom}(K\wedge R)\lhd H\wedge Q)(i, j, u, v) \wedge (\mathrm{dom}(H\wedge Q)\lhd K\wedge R)(i, k, u, w) \;\Rightarrow \\
&\qquad (\mathrm{dom}(K\wedge R\wedge K'\wedge V)\lhd H\wedge Q\wedge D)(u, v, i, j, u', v', o, p) \wedge \\
&\qquad (\mathrm{dom}(H\wedge Q\wedge D)\lhd K\wedge R\wedge K'\wedge V)(u, w, i, k, u', w', o, q)
\end{aligned}
\tag{8.3}
$$

then:

(i) there is a retrenchment from *Univ* to *Xtra*, with the data given in (2).(v).
[N.B. If the relations mentioned in (8.2) and (8.3) are functions (with *Ret* and *Ref* values as domain and *Abs* values as range), then (8.2) and (8.3) are satisfied.]

(6) Referring to the data given in (2).(v), provided that (in addition to (8.2) and (8.3)):

$$
\begin{aligned}
&(\exists\, \tilde{t}, \tilde{h}, \tilde{n} \bullet stp_{Op_{\mathrm{X}}}(\tilde{t}, \tilde{h}, \tilde{t}', \tilde{n})) \wedge (\exists\, \underline{t}' \bullet HK^\circ(\underline{t}', \tilde{t}')) \wedge \\
&(\exists\, t, \tilde{t}, h, \tilde{h}, n, \tilde{n} \bullet DV^\circ{}_{Op}(t', \tilde{t}', n, \tilde{n}; h, \tilde{h}, t, \tilde{t})) \;\Rightarrow \\
&\qquad HK^\circ(t', \tilde{t}')
\end{aligned}
\tag{8.4}
$$

then:

(i) the retrenchment of (5).(i) from *Univ* to *Xtra*, strengthens to a refinement, (with refinement data $KK^\circ(t, \tilde{t})$, $\{RR^\circ{}_{Op}, VV^\circ{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say);

(ii) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Xtra* need to satisfy:

$$
\begin{aligned}
&\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \wedge KK^\circ(t, \tilde{t}) \wedge RR^\circ{}_{Op}(h, \tilde{h}) \;\leftrightarrows \\
&\qquad KK^\circ(t, \tilde{t}) \wedge RR^\circ{}_{Op}(h, \tilde{h}) \wedge \mathrm{APP}_{Op_{\mathrm{X}}}(\tilde{t}, \tilde{h})
\end{aligned}
\tag{8.5}
$$

(7) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, and in addition the properties noted in (8.2)-(8.3) (further in (8.4), and if needed, (8.5)), then *Univ* and *Univ** are inter-retrenchable, (resp. further inter-refinable).

Proof. For (1), we start by completing the details of *Univ*, of the refinement $K^\bullet,R^\bullet,V^\bullet$, and of the retrenchment $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$. Adapting the usual notational conventions in the anticipated way for *Ret* and *Ref*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V} \times \mathsf{W}$

(where U is the state space of *Abs*, V is the state space of *Ret* and W is the state space of *Ref*). Predictably, there are two cases for the input and output spaces of *Univ*. If $Op \in \mathsf{Ops}_{\mathrm{FU}} = \mathsf{Ops}_{\mathrm{AT}}$, then $h \in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \times \mathsf{K}_{Op}$ and $n \in \mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op} \times \mathsf{Q}_{Op}$. However if $Op \in \mathsf{Ops}_{\mathrm{U\backslash FU}}$, then $h \in \mathsf{H}_{Op} = \mathsf{J}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{P}_{Op}$. We start by giving the data for the refinement and retrenchment.

The refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ is given by the data:

$$K^{\bullet}(v, t) \;\equiv\; (t = (u, v, w) \wedge K(u, w)) \tag{8.6}$$

$$R^{\bullet}{}_{Op}(j, h) \;\equiv\; \begin{cases} (h = (i, j, k) \wedge R_{Op}(i, k)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{FU}} \\ (h = j) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U\backslash FU}} \end{cases} \tag{8.7}$$

$$V^{\bullet}{}_{Op}(p, n) \;\equiv\; \begin{cases} (n = (o, p, q) \wedge V_{Op}(o, q)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{FU}} \\ (n = p) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U\backslash FU}} \end{cases} \tag{8.8}$$

The retrenchment $H^{\bullet}, Q^{\bullet}, N^{\bullet}, D^{\bullet}$ is given by the data:

$$H^{\bullet}(w, t) \;\equiv\; (t = (u, v, w) \wedge H(u, v)) \tag{8.9}$$

$$Q^{\bullet}{}_{Op}(k, h, w, t) \;\equiv\; (h = (i, j, k) \wedge t = (u, v, w) \wedge Q_{Op}(i, j, u, v)) \tag{8.10}$$

$$\begin{aligned} &N^{\bullet}{}_{Op}(q, n; w', t', k, h, w, t) \;\equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\ &\quad N_{Op}(o, p; u', v', i, j, u, v)) \end{aligned} \tag{8.11}$$

$$\begin{aligned} &D^{\bullet}{}_{Op}(w', t', q, n; k, h, w, t) \;\equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\ &\quad D_{Op}(u', v', o, p; i, j, u, v)) \end{aligned} \tag{8.12}$$

We need these relations to define the *Univ* system itself, so we start by checking (1).(iii). We first calculate $G^{\times}, G^{\times} \wedge P^{\times}, O^{\times}, C^{\times}$ for $Op \in \mathsf{Ops}_{\mathrm{FU}}$, as the composition of the pseudoretrenchment $H^{\mathrm{T}}, Q^{\mathrm{T}}, N^{\mathrm{T}}, D^{\mathrm{T}}$ with the refinement K, R, V. The fact that the result is also equal to the composition of the refinement $K^{\bullet}, R^{\bullet}, V^{\bullet}$ with the pseudoretrenchment $H^{\bullet\mathrm{T}}, Q^{\bullet\mathrm{T}}, N^{\bullet\mathrm{T}}, D^{\bullet\mathrm{T}}$ follows by inspection.

$$G^{\times}(v, w) \;\equiv\; H^{\mathrm{T}} \fatsemi K = (\exists\, u \bullet H(u, v) \wedge K(u, w)) = K^{\bullet} \fatsemi H^{\bullet\mathrm{T}} \tag{8.13}$$

$$\begin{aligned} &G^{\times} \wedge P^{\times}{}_{Op} \wedge ((G^{\times\prime} \wedge O^{\times}{}_{Op}) \vee C^{\times}{}_{Op})(v, w, j, k, v', w', p, q) \;\equiv \\ &(H^{\mathrm{T}} \wedge Q^{\mathrm{T}}{}_{Op} \wedge ((H^{\mathrm{T}\prime} \wedge N^{\mathrm{T}}{}_{Op}) \vee D^{\mathrm{T}}{}_{Op})) \fatsemi (K \wedge R_{Op} \wedge K' \wedge V_{Op}) = \\ &(\exists\, u, i, u', o \bullet H(u, v) \wedge Q_{Op}(i, j, u, v) \wedge \\ &\quad ((H(u', v') \wedge N_{Op}(o, p; u', v', i, j, u, v)) \vee D_{Op}(u', v', o, p; i, j, u, v)) \wedge \\ &\quad K(u, w) \wedge R_{Op}(i, k) \wedge K(u', w') \wedge V_{Op}(o, q)) = \\ &(K^{\bullet} \wedge R^{\bullet}{}_{Op} \wedge K^{\bullet\prime} \wedge V^{\bullet}{}_{Op}) \fatsemi (H^{\bullet\mathrm{T}} \wedge Q^{\bullet\mathrm{T}}{}_{Op} \wedge ((H^{\bullet\mathrm{T}\prime} \wedge N^{\bullet\mathrm{T}}{}_{Op}) \vee D^{\bullet\mathrm{T}}{}_{Op})) \end{aligned} \tag{8.14}$$

The *Univ* system itself is now given as follows. Initialisation in *Univ* is given by:

$$Init_{\mathrm{U}}(t') \;\equiv\; (t' = (u', v', w') \wedge Init_{\mathrm{T}}(v') \wedge K^{\bullet}(v', t') \wedge Init_{\mathrm{F}}(w') \wedge H^{\bullet}(w', t')) \tag{8.15}$$

The operations of *Univ* are given by:

$$
\begin{aligned}
&stp_{Op_{\mathrm{U}}}(t, h, t', n) \;\equiv \\
&\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\
&\quad [stp_{Op_{\mathrm{T}}}(v, j, v', p) \wedge K^{\bullet}(v, t) \wedge R^{\bullet}{}_{Op}(j, h) \wedge K^{\bullet}(v', t') \wedge V^{\bullet}{}_{Op}(p, n)] \wedge \\
&\quad [stp_{Op_{\mathrm{F}}}(w, k, w', q) \wedge H^{\bullet}(w, t) \wedge Q^{\bullet}{}_{Op}(k, h, w, t) \wedge \\
&\qquad ((H^{\bullet}(w', t') \wedge N^{\bullet}{}_{Op}(q, n; w', t', k, h, w, t)) \vee D^{\bullet}{}_{Op}(w', t', q, n; k, h, w, t))]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{FU}} \\
&\quad (t = (u, v, w) \wedge h = j \wedge t' = (u', v', w') \wedge n = p \wedge \\
&\quad [stp_{Op_{\mathrm{T}}}(v, j, v', p) \wedge K^{\bullet}(v, t) \wedge R^{\bullet}{}_{Op}(j, h) \wedge K^{\bullet}(v', t') \wedge V^{\bullet}{}_{Op}(p, n)]) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{U}\setminus\mathrm{FU}} \qquad (8.16)
\end{aligned}
$$

For (1).(i) we check that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement. For the initialisation PO, suppose we have $Init_{\mathrm{U}}(t')$. Then by (8.15), we have $Init_{\mathrm{T}}(v') \wedge K^{\bullet}(v', t')$ for the v' in t', which is enough. For the operation PO, suppose $Op \in \mathsf{Ops}_{\mathrm{FU}}$. Then, if we assume $K^{\bullet}(v, t) \wedge R^{\bullet}{}_{Op}(j, h) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', n)$, we see that (8.16) furnishes us a $stp_{Op_{\mathrm{T}}}(v, j, v', p)$ (with $K^{\bullet}(v', t') \wedge V^{\bullet}{}_{Op}(p, n)$ holding as required), which is what we need. If $Op \in \mathsf{Ops}_{\mathrm{U}\setminus\mathrm{FU}}$, the argument is similar.

For (1).(ii) we check that $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is a retrenchment. For the initialisation PO, suppose we have $Init_{\mathrm{U}}(t')$. Then by (8.15), we have $Init_{\mathrm{F}}(w') \wedge H^{\bullet}(w', t')$ for the w' in t', which is enough. For the operation PO, let us assume $H^{\bullet}(w, t) \wedge Q^{\bullet}{}_{Op}(k, h, w, t) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', n)$. Then we see that (8.16) furnishes us a $stp_{Op_{\mathrm{F}}}(w, k, w', q)$ (with $(H^{\bullet\prime} \wedge N^{\bullet}{}_{Op}) \vee D^{\bullet}{}_{Op}$ holding as required), which is what we need.

For (1).(iv), it is clear from the arguments above that each step t -(h, Op_{U}, n)-› t' of *Univ* is in simulation with (in the refinement sense) its constituent $stp_{Op_{\mathrm{T}}}$ transition, and, if $Op \in \mathsf{Ops}_{\mathrm{FU}}$, is in simulation with (in the retrenchment sense) its constituent $stp_{Op_{\mathrm{F}}}$ transition. (These $stp_{Op_{\mathrm{T}}}$ and $stp_{Op_{\mathrm{F}}}$ transitions are obviously unique since the data for the $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ retrenchment and the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement are functional from *Univ* to *Ref* and *Ret* respectively.) When $Op \in \mathsf{Ops}_{\mathrm{FU}}$, the fact that the mentioned $stp_{Op_{\mathrm{T}}}$ transition and $stp_{Op_{\mathrm{F}}}$ transition are in simulation via the pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ is evident, since the data for the latter is directly present in (8.16).

For (1).(v), since $K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op}$ is a function (in general partial) from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, we have $(K^{\bullet} \wedge R^{\bullet}{}_{Op}) \mathbin{⨾} (K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}$. Consequently, the definition of the APP_{Op} sets of *Univ* in (8.1) satisfies the condition in (3.15) as regards the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement, and consequently satisfies an APP_{Op} requirement of either the (3.9) or (3.10) form. This completes (1).

For (2).(i), we start with the refinement data K°,R°,V° which is given by:

$$K^{\circ}(t, t^{\sim}) \;\equiv\; (\exists\, v \bullet K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim})) \tag{8.17}$$

$$R^{\circ}{}_{Op}(h, h^{\sim}) \;\equiv\; (\exists\, j \bullet R^{\bullet}{}_{Op}(j, h) \wedge R^{\sim}{}_{Op}(j, h^{\sim})) \tag{8.18}$$

$$V^{\circ}{}_{Op}(n, n^{\sim}) \;\equiv\; (\exists\, p \bullet V^{\bullet}{}_{Op}(p, n) \wedge V^{\sim}{}_{Op}(p, n^{\sim})) \tag{8.19}$$

We must show that every transition of *Xtra* is in simulation with a transition of *Univ* via (8.17)-(8.19). Suppose that $Op \in \mathsf{Ops}_{\mathrm{FX}}$, and let $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ be a step of *Xtra*. By assumption, $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ is in simulation with some step of *Ret*, v -(j, Op_{T}, p)-› v' say, via $K^{\sim}$,$R^{\sim}$,$V^{\sim}$, and is also in simulation with some step of *Ref*, w -(k, Op_{F}, q)-› w' say, via $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$. These two steps are in simulation via $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$, also by assumption. But this means that they also determine a step of *Univ*, t -(h, Op_{U}, n)-› t' say, by (8.16), as seen above. This *Univ* step is in simulation with the ***Ret*** and ***Ref*** steps, via the $K^\bullet,R^\bullet,V^\bullet$ refinement and the $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ retrenchment. Composing the $K^\bullet,R^\bullet,V^\bullet$ simulation with the $K^\sim,R^\sim,V^\sim$ simulation now yields the result.

Suppose alternatively that $Op \in \mathsf{Ops}_{X\backslash FX}$, and let $t^\sim$ -($h^\sim$, Op_X, $n^\sim$)-› $t^{\sim\prime}$ be a step of ***Xtra***. By assumption, $t^\sim$ -($h^\sim$, Op_X, $n^\sim$)-› $t^{\sim\prime}$ is in simulation with some step of ***Ret***, v -(j, Op_T, p)-› v' say, via $K^\sim,R^\sim,V^\sim$. To get a simulation with a ***Univ*** step, referring to the $Op \in \mathsf{Ops}_{U\backslash FU}$ case of (8.16), it is sufficient to establish $K^\bullet \wedge R^\bullet{}_{Op} \wedge K^{\bullet\prime} \wedge V^\bullet{}_{Op}$ for the ***Ret*** step. For this, it is enough to find any u, w, u', w', such that $K(u, w)$ and $K(u', w')$ hold (whence we can get $K^\bullet \wedge K^{\bullet\prime}$ via (8.6)). Beyond this, v -(j, Op_T, p)-› v' gives us j, p, (whence we can get $R^\bullet{}_{Op} \wedge V^\bullet{}_{Op}$ via the $Op \in \mathsf{Ops}_{X\backslash FX}$ cases of (8.7) and (8.8)). Composing the $K^\bullet,R^\bullet,V^\bullet$ simulation with the $K^\sim,R^\sim,V^\sim$ simulation now yields the result.

For (2).(ii), we start with the retrenchment data $H^\circ,Q^\circ,N^\circ,D^\circ$. This is the vertical composition of the $H^\sim,Q^\sim,N^\sim,D^\sim$ and $H^{\bullet T},Q^{\bullet T},N^{\bullet T},D^{\bullet T}$ data, suitably modified by the refinement data K°,R°,V° just above, and is given by:

$$
\begin{aligned}
&H^\circ(t, t^\sim) \ \equiv \\
&\quad [(\exists\, w \bullet H^\bullet(w, t) \wedge H^\sim(w, t^\sim))] \vee \\
&\quad [\neg(\exists\, w \bullet H^\bullet(w, t)) \wedge \neg(\exists\, w \bullet H^\sim(w, t^\sim)) \wedge (\exists\, v \bullet K^\bullet(v, t) \wedge K^\sim(v, t^\sim))]
\end{aligned} \tag{8.20}
$$

$$
\begin{aligned}
&Q^\circ{}_{Op}(h, h^\sim, t, t^\sim) \ \equiv \\
&\quad (\exists\, k, w \bullet H^\bullet(w, t) \wedge H^\sim(w, t^\sim) \wedge Q^\bullet{}_{Op}(k, h, w, t) \wedge Q^\sim{}_{Op}(k, h^\sim, w, t^\sim)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{FX} \\
&\quad (\exists\, j \bullet R^\bullet{}_{Op}(j, h) \wedge R^\sim{}_{Op}(j, h^\sim)) \qquad\qquad \text{if } Op \in \mathsf{Ops}_{X\backslash FX}
\end{aligned} \tag{8.21}
$$

$$
\begin{aligned}
&N^\circ{}_{Op}(n, n^\sim; t', t^{\sim\prime}, h, h^\sim, t, t^\sim) \ \equiv \\
&\quad (\exists\, w, k, w', q \bullet N^\bullet{}_{Op}(q, n; w', t', k, h, w, t) \wedge N^\sim{}_{Op}(q, n^\sim; w', t^{\sim\prime}, k, h^\sim, w, t^\sim)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{FX} \\
&\quad (\exists\, p \bullet V^\bullet{}_{Op}(p, n) \wedge V^\sim{}_{Op}(p, n^\sim)) \qquad\qquad \text{if } Op \in \mathsf{Ops}_{X\backslash FX}
\end{aligned} \tag{8.22}
$$

$$
\begin{aligned}
&D^\circ{}_{Op}(t', t^{\sim\prime}, n, n^\sim; h, h^\sim, t, t^\sim) \ \equiv \ (\exists\, w, k, w', q \bullet \\
&\quad \{[H^\bullet(w', t') \wedge N^\bullet{}_{Op}(q, n; w', t', k, h, w, t) \wedge \\
&\qquad D^\sim{}_{Op}(w', t^{\sim\prime}, q, n^\sim; k, h^\sim, w, t^\sim)] \vee \\
&\quad [D^\bullet{}_{Op}(w', t', q, n\, ; k, h, w, t) \wedge \\
&\qquad H^\sim(w', t^{\sim\prime}) \wedge N^\sim{}_{Op}(q, n^\sim; w', t^{\sim\prime}, k, h^\sim, w, t^\sim)] \vee \\
&\quad [D^\bullet{}_{Op}(w', t', q, n\, ; k, h, w, t) \wedge \\
&\qquad D^\sim{}_{Op}(w', t^{\sim\prime}, q, n^\sim; k, h^\sim, w, t^\sim)]\}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{FX} \\
&\quad \mathsf{false} \qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{X\backslash FX}
\end{aligned} \tag{8.23}
$$

We must show that every step of ***Xtra*** is in simulation with a step of ***Univ*** via (8.20)-(8.23). Let $Op \in \mathsf{Ops}_{FX}$, and let $t^\sim$ -($h^\sim$, Op_X, $n^\sim$)-› $t^{\sim\prime}$ be a step of ***Xtra***. By assumption, $t^\sim$ -($h^\sim$, Op_X, $n^\sim$)-› $t^{\sim\prime}$ is in simulation with a step of ***Ret***, v -(j, Op_T, p)-› v' say, via $K^\sim,R^\sim,V^\sim$, and is also in simulation with a step of ***Ref***, w -(k, Op_F, q)-› w' say, via $H^\sim,Q^\sim,N^\sim,D^\sim$. These two steps are in simulation via $G^\times,G^\times \wedge P^\times,O^\times,C^\times$, also by assumption. Therefore they determine a step of ***Univ***, t -(h, Op_U, n)-› t' say, by (8.16), as we saw above. This ***Univ*** step is in simulation with the ***Ret*** and ***Ref*** steps, via the $K^\bullet,R^\bullet,V^\bullet$ refinement and the $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ retrenchment. Composing the $H^\bullet,Q^\bullet,N^\bullet,D^\bullet$ simulation with the $H^\sim,Q^\sim,N^\sim,D^\sim$ simulation now yields a formula of the shape

$H^{\bullet}\wedge Q^{\bullet}{}_{Op}\wedge H^{\sim}\wedge Q^{\sim}{}_{Op}\wedge((H^{\bullet\prime}\wedge N^{\bullet}{}_{Op})\vee D^{\bullet}{}_{Op})\wedge((H^{\sim\prime}\wedge N^{\sim}{}_{Op})\vee D^{\sim}{}_{Op})$ which relates the *Univ* and *Xtra* steps. We apply the distributive law to the last two conjuncts, getting $((H^{\bullet\prime}\wedge N^{\bullet}{}_{Op}\wedge H^{\sim\prime}\wedge N^{\sim}{}_{Op})\vee(H^{\bullet\prime}\wedge N^{\bullet}{}_{Op}\wedge D^{\sim}{}_{Op})\vee(H^{\sim\prime}\wedge N^{\sim}{}_{Op}\wedge D^{\bullet}{}_{Op})\vee(D^{\bullet}{}_{Op}\wedge D^{\sim}{}_{Op}))$. The last three disjuncts of this yield $D^{\circ}{}_{Op}$; the first disjunct gives $H^{\circ\prime}\wedge N^{\circ}{}_{Op}$ (utilising the first disjunct in (8.20) for $H^{\circ\prime}$); and the remainder of the earlier formula gives $H^{\circ}\wedge Q^{\circ}{}_{Op}$ (again utilising the first disjunct in (8.20) for H°). So we have what we need.

Now let $Op \in \mathsf{Ops}_{X\backslash FX}$, and let $t^{\sim}$ -($h^{\sim}$, Op_X, $n^{\sim}$)-› $t^{\sim\prime}$ be a step of *Xtra*. We have two things to do. Firstly, we must find some suitable values t, h, t', n, such that they make a *Univ* transition for the $Op \in \mathsf{Ops}_{X\backslash FX}$ case. For this it is enough (according to (8.16)) to establish $stp_{Op_T}(v, j, v', p)$ for the v, j, v', p in t, h, t', n, and also that $K^{\bullet}\wedge R^{\bullet}{}_{Op}\wedge K^{\bullet\prime}\wedge V^{\bullet}{}_{Op}$ holds for t, h, t', n — the latter splits into four independent subproblems, one each for $K^{\bullet}$, $R^{\bullet}{}_{Op}$, $K^{\bullet\prime}$, $V^{\bullet}{}_{Op}$, since (8.16) does not otherwise constrict the values in the $Op \in \mathsf{Ops}_{X\backslash FX}$ case. Secondly, for these same values t, h, t', n, we must establish the simulation relation, $H^{\circ}\wedge Q^{\circ}{}_{Op}\wedge H^{\circ\prime}\wedge N^{\circ}{}_{Op}$, (since $D^{\circ}{}_{Op}$ being false in the $Op \in \mathsf{Ops}_{X\backslash FX}$ case precludes establishing the concession variant) — noting that, via (8.21)-(8.22), $Q^{\circ}{}_{Op}$ and $N^{\circ}{}_{Op}$ depend only on inputs and outputs respectively in the $Op \in \mathsf{Ops}_{X\backslash FX}$ case, again splits this into four independent subproblems, one each for H°, $Q^{\circ}{}_{Op}$, $H^{\circ\prime}$, $N^{\circ}{}_{Op}$.

By assumption, the step $t^{\sim}$ -($h^{\sim}$, Op_X, $n^{\sim}$)-› $t^{\sim\prime}$ of *Xtra* is in simulation with a step of *Ret*, v -(j, Op_T, p)-› v' say (which gives us the first thing we need for (8.16)), via $K^{\sim}$,$R^{\sim}$,$V^{\sim}$. Noting that $R^{\bullet}{}_{Op}(j, h) \equiv (h = j)$ and also that $V^{\bullet}{}_{Op}(p, n) \equiv (n = p)$, together with $R^{\sim}$ and $V^{\sim}$ and (8.21)-(8.22), gives us $R^{\bullet}{}_{Op}$ and $V^{\bullet}{}_{Op}$ and $Q^{\circ}{}_{Op}$ and $N^{\circ}{}_{Op}$, leaving $K^{\bullet}$, $K^{\bullet\prime}$, H°, $H^{\circ\prime}$ to do. We consider $K^{\bullet}$ and H°, since the argument for $K^{\bullet\prime}$ and $H^{\circ\prime}$ will be similar. For the *Xtra* step, we have $K^{\sim}(v, t^{\sim})$ already. Now either $H^{\sim}(w, t^{\sim})$ holds for some w, or not. If it does, then $H^{\sim}(w, t^{\sim})$ and $K^{\sim}(v, t^{\sim})$ compose to give $G^{\times}(v, w)$, so by (8.13), there is a u such that both $K(u, w)$ and $H(u, v)$ hold. The latter is enough to give $H^{\bullet}(w, t)$, where $t = (u, v, w)$. Composing $H^{\sim}(w, t^{\sim})$ and $H^{\bullet}(w, t)$ gives the desired $H^{\circ}(t, t^{\sim})$ via the first disjunct of (8.20). Since $G^{\times}(v, w)$ also gives $K^{\bullet}(v, t)$ and $H^{\bullet}(w, t)$, we have the desired $K^{\bullet}(v, t)$ too, completing this case. Suppose now that $H^{\sim}(w, t^{\sim})$ does not hold for any w. Then we have to establish the second disjunct of (8.20). This means that as well as $\neg(\exists\, w \bullet H^{\sim}(w, t^{\sim}))$ which we assume, we have to prove $\neg(\exists\, w \bullet H^{\bullet}(w, t)) \wedge (\exists\, v \bullet K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim}))$ for suitable w and t — for this we use the additional assumption $(\forall\, v \bullet \exists\, u, w \bullet \neg H(u, v) \wedge K(u, w))$. Since we know $K^{\sim}(v, t^{\sim})$, we use the assumption to choose u and w such that $\neg H(u, v)$ and $K(u, w)$ both hold. From this, setting $t = (u, v, w)$, we deduce firstly that $\neg(\exists\, w \bullet H^{\bullet}(w, t))$ holds from (8.9), and secondly that $K^{\bullet}(v, t)$ holds from (8.6). This discharges the second disjunct of (8.20), completing (2).(ii).

For (2).(iii), since $K^{\circ} = K^{\bullet T} \fatsemi K^{\sim}$, then $K^{\bullet} \fatsemi K^{\circ} = K^{\bullet} \fatsemi K^{\bullet T} \fatsemi K^{\sim} = \mathrm{Id}_{\mathsf{V}} \fatsemi K^{\sim} = K^{\sim}$ (since $K^{\bullet T}$ is a partial function). The remaining results are similar.

For (2).(iv), since $H^{\circ} = [(H^{\bullet T} \fatsemi H^{\sim})\vee((\neg H^{\bullet T} \fatsemi \neg H^{\sim})\wedge(K^{\bullet T} \fatsemi K^{\sim}))]$, we derive that $H^{\bullet} \fatsemi H^{\circ} = H^{\bullet} \fatsemi [(H^{\bullet T} \fatsemi H^{\sim})\vee((\neg H^{\bullet T} \fatsemi \neg H^{\sim})\wedge(K^{\bullet T} \fatsemi K^{\sim}))] = \mathrm{Id}_{\mathsf{W}} \fatsemi H^{\sim} = H^{\sim}$ (since $H^{\bullet T}$ is a partial function, and $H^{\bullet}\ldots$ and $\neg H^{\bullet T}\ldots$ are disjoint). The derivation of $N^{\bullet} \fatsemi N^{\circ} = N^{\sim}$ is similar to that of the results in (2).(iii). Now, consider $D^{\bullet} \fatsemi D^{\circ}$ where D° is given by (8.23). The term $D^{\bullet T}\wedge D^{\sim}$, which occurs disjunctively in (8.23), shows that $D^{\bullet} \fatsemi D^{\circ}$ contains $D^{\bullet} \fatsemi D^{\bullet T} \fatsemi D^{\sim} = \mathrm{Id}_{\mathsf{W}\times\mathsf{K}_{Op}\times\mathsf{W}\times\mathsf{Q}_{Op}} \fatsemi D^{\sim} = D^{\sim}$. Since (8.23) also contains other disjuncts, we derive $D^{\bullet} \fatsemi D^{\circ} \Leftarrow D^{\sim}$. Finally, by assumption, $H\wedge Q$ is a non-empty relation. This makes $H^{\bullet\mathrm{T}} \wedge Q^{\bullet\mathrm{T}}$ a non-empty (partial) function which is onto $\mathsf{W} \times \mathsf{K}_{Op}$. Therefore $(H^{\bullet} \wedge Q^{\bullet}) \fatsemi (H^{\circ} \wedge Q^{\circ}) = (H^{\sim} \wedge Q^{\sim})$ can be shown in the same way as other similar results, such as $N^{\bullet} \fatsemi N^{\circ} = N^{\sim}$ and the ones in (2).(iii).[10] We are done.

For (2).(v), we start with the retrenchment data $HK^{\circ}, QR^{\circ}, NV^{\circ}, DV^{\circ}$ which is given by (8.24)-(8.27). Note that, aside from the retrieve relation HK°, which is disjunctive in structure and simpler than just a combination of the retrieve relations (8.17) and (8.20), the remaining data is a suitable conjunction of the data in (8.17)-(8.19) with the data in (8.20)-(8.23):

$$
\begin{aligned}
& HK^{\circ}(t, t^{\sim}) \;\equiv\; (t = (u, v, w) \wedge \\
& \qquad \{[(H^{\bullet}(w, t) \wedge H^{\sim}(w, t^{\sim})] \vee [K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim})]\}) && (8.24)
\end{aligned}
$$

$$
\begin{aligned}
& QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim}) \;\equiv \\
& \qquad (t = (u, v, w) \wedge h = (i, j, k) \wedge \\
& \qquad H^{\bullet}(w, t) \wedge H^{\sim}(w, t^{\sim}) \wedge Q^{\bullet}{}_{Op}(k, h, w, t) \wedge Q^{\sim}{}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge \\
& \qquad K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim}) \wedge R^{\bullet}{}_{Op}(j, h) \wedge R^{\sim}{}_{Op}(j, h^{\sim})) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{FX}} \\
& \qquad (t = (u, v, w) \wedge h = j \wedge \\
& \qquad K^{\bullet}(v, t) \wedge K^{\sim}(v, t^{\sim}) \wedge R^{\bullet}{}_{Op}(j, h) \wedge R^{\sim}{}_{Op}(j, h^{\sim})) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{X \backslash FX}} && (8.25)
\end{aligned}
$$

$$
\begin{aligned}
& NV^{\circ}{}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim}) \;\equiv \\
& \qquad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\
& \qquad N^{\bullet}{}_{Op}(q, n; w', t', k, h, w, t) \wedge N^{\sim}{}_{Op}(q, n^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim}) \wedge \\
& \qquad K^{\bullet}(v, t) \wedge R^{\bullet}{}_{Op}(j, h) \wedge K^{\bullet}(v', t') \wedge V^{\bullet}{}_{Op}(p, n) \wedge \\
& \qquad K^{\sim}(v, t^{\sim}) \wedge R^{\sim}{}_{Op}(j, h^{\sim}) \wedge K^{\sim}(v', t^{\sim\prime}) \wedge V^{\sim}{}_{Op}(p, n^{\sim})) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{FX}} \\
& \qquad (n = p \wedge V^{\bullet}{}_{Op}(p, n) \wedge V^{\sim}{}_{Op}(p, n^{\sim})) \qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{X \backslash FX}} && (8.26)
\end{aligned}
$$

$$
\begin{aligned}
& DV^{\circ}{}_{Op}(t', t^{\sim\prime}, n, n^{\sim}; h, h^{\sim}, t, t^{\sim}) \;\equiv \\
& \qquad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\
& \qquad \{[H^{\bullet}(w', t') \wedge N^{\bullet}{}_{Op}(q, n; w', t', k, h, w, t) \wedge \\
& \qquad\qquad D^{\sim}{}_{Op}(w', t^{\sim\prime}, q, n^{\sim}\,; k, h^{\sim}, w, t^{\sim})] \vee \\
& \qquad [D^{\bullet}{}_{Op}(w', t', q, n\,; k, h, w, t) \wedge \\
& \qquad\qquad H^{\sim}(w', t^{\sim\prime}) \wedge N^{\sim}{}_{Op}(q, n^{\sim}; w', t^{\sim\prime}, k, h^{\sim}, w, t^{\sim})] \vee \\
& \qquad [D^{\bullet}{}_{Op}(w', t', q, n\,; k, h, w, t) \wedge \\
& \qquad\qquad D^{\sim}{}_{Op}(w', t^{\sim\prime}, q, n^{\sim}\,; k, h^{\sim}, w, t^{\sim})]\} \wedge \\
& \qquad K^{\bullet}(v, t) \wedge R^{\bullet}{}_{Op}(j, h) \wedge K^{\bullet}(v', t') \wedge V^{\bullet}{}_{Op}(p, n) \wedge \\
& \qquad K^{\sim}(v, t^{\sim}) \wedge R^{\sim}{}_{Op}(j, h^{\sim}) \wedge K^{\sim}(v', t^{\sim\prime}) \wedge V^{\sim}{}_{Op}(p, n^{\sim})) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{FX}} \\
& \qquad \mathsf{false} \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{if } Op \in \mathsf{Ops}_{\mathrm{X \backslash FX}} && (8.27)
\end{aligned}
$$

In the terminology of [Banach et al. (2008)], and aside from the properties of the retrieve relation already noted, the composition of (8.24)-(8.27) is a blend of: on the one hand, conjunctive fusion composition (since the state and the I/O spaces are

10. For other similar results, the non-emptiness of the partial function follows from the assumed non-emptiness of the underlying relation, via Assumption 1.1. For $H \wedge Q$, non-emptiness does not follow from non-emptiness of H and Q individually.

(partly) the same), and on the other, synchronous parallel composition (since the state and the I/O spaces are (partly) different), of the refinement data (8.17)-(8.19) and the retrenchment data (8.20)-(8.23).

With the retrenchment data in place, the argument is now largely a replay of the proofs of (2).(i) and (2).(ii). Starting with an $Op \in \mathsf{Ops}_{\mathrm{FX}}$ step of *Xtra* we infer *Ret* and *Ref* steps from the refinement and retrenchment from *Ret* and *Ref* to *Xtra*. These are in simulation via $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ by assumption, and determine a step of *Univ*, as before. The conjunction of all the facts established along the way, via both *Ret* and *Ref*, establishes the simulation between the *Univ* and *Xtra* steps via (8.24)-(8.27). The $Op \in \mathsf{Ops}_{\mathrm{X \backslash FX}}$ case is a simplification of the analogous case in (2).(ii) because of the simpler structure of the retrieve relation here — it is sufficient to rely on the truth of $K^{\bullet}$ and $K^{\sim}$, without having to worry about whether $H^{\bullet}$ and $H^{\sim}$ do or do not hold for particular values of w. This completes part (2).

For (3), we note that *Univ* itself satisfies the criteria demanded of *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** satisfies the criteria demanded of *Xtra* too. Hence we can construct two instances of Fig. 5 as follows. In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there are refinement data K°,R°,V° and retrenchment data H°,Q°,N°,D° from *Univ* to *Univ**. In the second, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there are refinement data K^*,R^*,V^* and retrenchment data H^*,Q^*,N^*,D^* from *Univ** to *Univ*. So *Univ* and *Univ** are inter-simulable by the arguments above.

For (4), we just observe that disjunctive fusion composition of retrenchments, and the vertical composition between retrenchments and refinements (both ways round) are sound composition mechanisms. For the record, we present the composed retrenchment data:

$$G(u, t) \;\equiv\; (t = (\underline{u}, v, w) \wedge \{[H(u, v) \wedge K(\underline{u}, w)] \vee [K(u, w) \wedge H(\underline{u}, v)]\}) \tag{8.28}$$

$$\begin{aligned} &P_{Op}(i, h, u, t) \;\equiv\; (h = (\underline{i}, j, k) \wedge t = (\underline{u}, v, w) \wedge \\ &\quad \{[K(\underline{u}, w) \wedge R_{Op}(\underline{i}, k) \wedge H(u, v) \wedge Q_{Op}(i, j, u, v)] \vee \\ &\quad [K(u, w) \wedge R_{Op}(i, k) \wedge H(\underline{u}, v) \wedge Q_{Op}(\underline{i}, j, \underline{u}, v)]\}) \end{aligned} \tag{8.29}$$

$$\begin{aligned} &O_{Op}(o, n; u', t', i, h, u, t) \;\equiv \\ &\quad (t = (\underline{u}, v, w) \wedge h = (\underline{i}, j, k) \wedge t' = (\underline{u}', v', w') \wedge n = (\underline{o}, p, q) \wedge \\ &\quad \{[H(\underline{u}', v') \wedge K(u, w) \wedge R_{Op}(i, k) \wedge K(u', w') \wedge V_{Op}(o, q) \wedge \\ &\qquad N_{Op}(\underline{o}, p; \underline{u}', v', \underline{i}, j, \underline{u}, v)] \vee \\ &\quad [H(u', v') \wedge K(\underline{u}, w) \wedge R_{Op}(\underline{i}, k) \wedge K(\underline{u}', w') \wedge V_{Op}(\underline{o}, q) \wedge \\ &\qquad N_{Op}(o, p; u', v', i, j, u, v)] \vee \\ &\quad [K(u, w) \wedge R_{Op}(i, k) \wedge K(u', w') \wedge V_{Op}(o, q) \wedge \\ &\qquad N_{Op}(\underline{o}, p; \underline{u}', v', \underline{i}, j, \underline{u}, v) \wedge N_{Op}(o, p; u', v', i, j, u, v) \wedge \\ &\qquad K(\underline{u}, w) \wedge R_{Op}(\underline{i}, k) \wedge K(\underline{u}', w') \wedge V_{Op}(\underline{o}, q)]\}) \end{aligned} \tag{8.30}$$

$$\begin{aligned} &C_{Op}(u', t', o, n \,; i, h, u, t) \;\equiv \\ &\quad (t = (\underline{u}, v, w) \wedge h = (\underline{i}, j, k) \wedge t' = (\underline{u}', v', w') \wedge n = (\underline{o}, p, q) \wedge \\ &\quad \{[D_{Op}(u', v', o, p; i, j, u, v) \wedge K(\underline{u}, w) \wedge R_{Op}(\underline{i}, k) \wedge K(\underline{u}', w') \wedge V_{Op}(\underline{o}, q)] \vee \\ &\quad [K(u, w) \wedge R_{Op}(i, k) \wedge K(u', w') \wedge V_{Op}(o, q) \wedge D_{Op}(\underline{u}', v', \underline{o}, p; \underline{i}, j, \underline{u}, v)]\}) \end{aligned} \tag{8.31}$$

For the remainder of the theorem, we work under the additional assumptions stated in (5) and (6).

For (5), we must show that the retrenchment data in (8.24)-(8.27) supports an actual retrenchment from *Univ* to *Xtra*. So we must prove that the initialisation PO and the retrenchment operation PO both hold with (8.24)-(8.27).

For the initialisation PO, assume $Init_{\mathrm{X}}(t^{\sim\prime})$. We must find a t' such that $Init_{\mathrm{U}}(t') \wedge HK^{\circ}(t', t^{\sim\prime})$ holds. Since $K^{\sim},R^{\sim},V^{\sim}$ is a refinement, there is a v' for which $Init_{\mathrm{T}}(v') \wedge K^{\sim}(v', t^{\sim\prime})$ holds. Also, since $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$ is a retrenchment, there is a w' for which $Init_{\mathrm{F}}(w') \wedge H^{\sim}(w', t^{\sim\prime})$ holds. Since we have $K^{\sim}(v', t^{\sim\prime}) \wedge H^{\sim}(w', t^{\sim\prime})$, we also have $G^{\times}(v', w')$ by assumption. So there is a u' such that $H(u', v') \wedge K(u', w')$ holds by (8.13), and so, for this u', $K^{\bullet}(v', t') \wedge H^{\bullet}(w', t')$ holds, where $t' = (u', v', w')$. So we have $Init_{\mathrm{U}}(t')$, by (8.15). Along the way we have established $K^{\bullet}(v', t') \wedge K^{\sim}(v', t^{\sim\prime}) \wedge H^{\bullet}(w', t') \wedge H^{\sim}(w', t^{\sim\prime})$, which with $t' = (u', v', w')$, gives both disjuncts of $HK^{\circ}(t', t^{\sim\prime})$. So we are done.

For the operation PO, assume $Op \in \mathsf{Ops}_{\mathrm{FX}}$, and $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim}) \wedge stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$. We need a *Univ* step t -(h, Op_{U}, n)-› t', such that $((HK^{\circ}(t', t^{\sim\prime}) \wedge NV^{\circ}{}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim})) \vee DV^{\circ}{}_{Op}(t', t^{\sim\prime}, n, n^{\sim}; h, h^{\sim}, t, t^{\sim}))$ holds. Suppose $t = (u, v, w)$ and $h = (i, j, k)$. Our assumption $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim})$ gives us $K^{\sim}(v, t^{\sim}) \wedge R^{\sim}{}_{Op}(j, h^{\sim})$. Since $K^{\sim},R^{\sim},V^{\sim}$ is a refinement, from $stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$ we can get a *Ret* step, v -(j, Op_{T}, p)-› v' say, such that $K^{\sim} \wedge R^{\sim}{}_{Op} \wedge K^{\sim\prime} \wedge V^{\sim}{}_{Op}$ holds. Also, since $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim})$ gives us $H^{\sim}(w, t^{\sim}) \wedge Q^{\sim}{}_{Op}(k, h^{\sim}, w, t^{\sim})$, and since $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$ is a retrenchment, we get a *Ref* step, w -(k, Op_{F}, q)-› w' say, such that $H^{\sim} \wedge Q^{\sim}{}_{Op} \wedge ((H^{\sim\prime} \wedge N^{\sim}{}_{Op}) \vee D^{\sim}{}_{Op})$ holds. Since $K^{\sim} \wedge R^{\sim}{}_{Op} \wedge K^{\sim\prime} \wedge V^{\sim}{}_{Op}$ together with $H^{\sim} \wedge Q^{\sim}{}_{Op} \wedge ((H^{\sim\prime} \wedge N^{\sim}{}_{Op}) \vee D^{\sim}{}_{Op})$ leads to $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ as we saw above, which is witnessed by some *Abs* values $\underline{u}$, $\underline{i}$, u', o, the two *Ret* and *Ref* steps produce a *Univ* step, $\underline{t}$ -($\underline{h}$, Op_{U}, n)-› t' say, for which $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge ((HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}) \vee DV^{\circ}{}_{Op})$ holds, as in the proof of (2).(v), where we have $\underline{t} = (\underline{u}, v, w)$ and $\underline{h} = (\underline{i}, j, k)$. To establish the retrenchment, it is enough to show that we can safely replace $\underline{u}$ and $\underline{i}$ by the u and i we assumed to start with.

We now note that either $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}$ or $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge DV^{\circ}{}_{Op}$ holds. Let us take the former case. Then, unravelling the assumed $HK^{\circ} \wedge QR^{\circ}{}_{Op}$ for t, h, and unravelling $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}$ for $\underline{t}$, $\underline{h}$, t', n, we see that we have the assumptions of (8.2). This allows us to replace $\underline{u}$, $\underline{i}$, by u, i, in $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}$ (and in the *Univ* step $\underline{t}$ -($\underline{h}$, Op_{U}, n)-› t') as desired, completing the argument. The argument for the $HK^{\circ} \wedge QR^{\circ}{}_{Op} \wedge DV^{\circ}{}_{Op}$ case is similar, utilising (8.3) instead of (8.2). This completes the $Op \in \mathsf{Ops}_{\mathrm{FX}}$ case.

We turn to the $Op \in \mathsf{Ops}_{\mathrm{X \backslash FX}}$ case. We assume $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim}) \wedge stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$. It will be sufficient to find a *Univ* step t -(h, Op_{U}, n)-› t', such that $HK^{\circ}(t', t^{\sim\prime}) \wedge NV^{\circ}{}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim})$ holds. Assumption $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim})$ yields $K^{\sim}(v, t^{\sim}) \wedge R^{\sim}{}_{Op}(j, h^{\sim})$ for suitable v and j. Since $K^{\sim},R^{\sim},V^{\sim}$ is a refinement, from $stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$ we can get a *Ret* step, v -(j, Op_{T}, p)-› v' say, such that $K^{\sim} \wedge R^{\sim}{}_{Op} \wedge K^{\sim\prime} \wedge V^{\sim}{}_{Op}$ holds. If we now fix $n = p$ for the *Univ* step, then noting that $V^{\bullet}{}_{Op}(p, n) \equiv (p = n)$, and that $V^{\sim}{}_{Op}(p, n^{\sim})$ holds, we can deduce $NV^{\circ}{}_{Op}(\ldots)$, since $NV^{\circ}{}_{Op}(\ldots)$ is $V^{\bullet}{}_{Op}(p, n) \wedge V^{\sim}{}_{Op}(p, n^{\sim})$. We now have to find t', to show that $HK^{\circ}(t', t^{\sim\prime})$ holds, and to show that t, h, t', n, constitute a *Univ* step. For the retrieve relation, we already have $K^{\sim}(v', t^{\sim\prime})$. So if we choose u', w' such that $K(u', w')$ holds, then by (8.6), $K^{\bullet}(v', t')$ holds too, where $t' = (u', v', w')$, and this yields $HK^{\circ}(t', t^{\sim\prime})$ via the second disjunct of (8.24). Finally, to show that t, h, t', n constitute a ***Univ*** step, we note that, by (8.16), we just need $K^{\bullet}{\wedge}R^{\bullet}{}_{Op}{\wedge}K^{\bullet\prime}{\wedge}V^{\bullet}{}_{Op}$. We have $K^{\bullet}{\wedge}R^{\bullet}{}_{Op}$ from $HK^{\circ}{\wedge}QR^{\circ}{}_{Op}$, and have deduced $K^{\bullet\prime}{\wedge}V^{\bullet}{}_{Op}$. So we are done. This completes part (5).

For (6), we start with the refinement data KK°,RR°,VV°, which is given by (8.32)-(8.35).

$$KK^{\circ}(t, t^{\sim}) \;\equiv\; HK^{\circ}(t, t^{\sim}) \vee ZZ^{\circ}(t, t^{\sim}) \tag{8.32}$$

where:

$$\begin{aligned} &ZZ^{\circ}(t, t^{\sim}) \;\equiv \\ &\quad (\exists\, \underline{t}^{\sim}, h^{\sim}, n^{\sim} \bullet stp_{Op_{\mathrm{X}}}(\underline{t}^{\sim}, h^{\sim}, t^{\sim}, n^{\sim})) \wedge \neg(\exists\, \underline{t} \bullet HK^{\circ}(\underline{t}, t^{\sim})) \wedge \\ &\quad (\exists\, \underline{t}, \underline{t}^{\sim}, h, h^{\sim}, n, n^{\sim} \bullet DV^{\circ}{}_{Op}(t, t^{\sim}, n, n^{\sim}; h, h^{\sim}, \underline{t}, \underline{t}^{\sim})) \end{aligned} \tag{8.33}$$

$$RR^{\circ}{}_{Op}(h, h^{\sim}) \;\equiv\; (\forall\, t, t^{\sim} \bullet HK^{\circ}(t, t^{\sim}) \Rightarrow QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim})) \tag{8.34}$$

$$\begin{aligned} &VV^{\circ}{}_{Op}(n, n^{\sim}) \;\equiv\; (\exists\, t, t^{\sim}, h, h^{\sim}, t', t^{\sim\prime} \bullet \\ &\quad NV^{\circ}{}_{Op}(n, n^{\sim}; t', t^{\sim\prime}, h, h^{\sim}, t, t^{\sim}) \vee DV^{\circ}{}_{Op}(t', t^{\sim\prime}, n, n^{\sim}; h, h^{\sim}, t, t^{\sim})) \end{aligned} \tag{8.35}$$

To prove the refinement we start with the initialisation PO. This goes just as the analogous PO for the retrenchment HK°,QR°,NV°,DV°, in (5).

For the operation PO we assume $KK^{\circ}(t, t^{\sim}) \wedge RR^{\circ}{}_{Op}(h, h^{\sim}) \wedge stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$, and must prove there are values t', n, such that $stp_{Op_{\mathrm{U}}}(t, h, t', n)$ and $KK^{\circ\prime}{\wedge}VV^{\circ}{}_{Op}$ hold. To begin with, we note that by the assumptions of (2), every step of ***Xtra*** is in simulation with at least a step of ***Ret***. Therefore, every before-state of an ***Xtra*** transition is related to some ***Univ*** state via HK°, and consequently no before-state of an ***Xtra*** transition can be in the range of ZZ°, because of the middle conjunct of (8.33). Thus, from $KK^{\circ}(t, t^{\sim}) \wedge RR^{\circ}{}_{Op}(h, h^{\sim})$ we deduce that $HK^{\circ}(t, t^{\sim}) \wedge QR^{\circ}{}_{Op}(h, h^{\sim}, t, t^{\sim}) \wedge stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$ covers all the ways of making the operation PO hypothesis true. But this is the hypothesis of the operation PO for the HK°,QR°,NV°,DV° retrenchment. Therefore we can deduce $(HK^{\circ\prime}{\wedge}NV^{\circ}{}_{Op}){\vee}DV^{\circ}{}_{Op}$. If $HK^{\circ\prime}{\wedge}NV^{\circ}{}_{Op}$ holds, then so does $KK^{\circ\prime}{\wedge}VV^{\circ}{}_{Op}$ (since $HK^{\circ\prime}$ is a disjunct of $KK^{\circ\prime}$ and $NV^{\circ}{}_{Op}$ is a disjunct of $VV^{\circ}{}_{Op}$) and we are done. If $HK^{\circ\prime}{\wedge}NV^{\circ}{}_{Op}$ does not hold, then we must have that $DV^{\circ}{}_{Op}(t', t^{\sim\prime}, n, n^{\sim}; h, h^{\sim}, t, t^{\sim})$ holds instead. In that case, either $t^{\sim\prime}$ is in the range of HK° or it is not. If it is, then we utilise (8.4) to deduce $HK^{\circ}(t', t^{\sim\prime})$ (after which we get $KK^{\circ}(t', t^{\sim\prime})$ via (8.32)), and then we utilise (8.35) to deduce $VV^{\circ}{}_{Op}(n, n^{\sim})$, and we are done. If it is not, then we utilise (8.33) to deduce $ZZ^{\circ}(t', t^{\sim\prime})$ (after which we get $KK^{\circ}(t', t^{\sim\prime})$ via (8.32)), and then we utilise (8.35) to deduce $VV^{\circ}{}_{Op}(n, n^{\sim})$, and we are done.

For (6).(ii), we note that the condition stated in (8.5) is just the requirement from (3.11), so we are done. This completes part (6).

For (7), it is just a matter of replaying the arguments of (3) using the stronger relationships between ***Univ*** and ***Xtra*** afforded by the stronger assumptions in force. We are done. ☺

8.1 Remarks

Some of the following mimic earlier remarks, so are stated briefly. Observations new to the postjoin construction are discussed in more detail.

Remark 8.2 Observing that (given our formulation of refinement and retrenchment), every refinement K,R,V yields a retrenchment K,R,V,false, simply by reinterpreting the input and output relation in the obvious way, and adding a trivial concession (see [Banach et al. (2007)] for a more extensive discussion), we see that we could readily have extended the retrenchment data H°,Q°,N°,D° in (2).(ii) of the theorem to all operations, simply by reinterpreting the refinement data K°,R°,V° from (2).(i) and adding a false concession. While valid, this would not have been very interesting. Another way of achieving the same thing would have been to consider the pseudoretrenchment data $H^\circ \vee K^\circ$,$Q^\circ \vee R^\circ$,$N^\circ \vee V^\circ$,D° instead. This would have worked for the stated claim in (2).(ii) because that claim only mentioned the simulation relation (permitting the choice of the most convenient disjunct from the enlarged relations for each case). The main reason this approach was not pursued for (2).(ii) was that it would have spoiled the relative cleanness of the composition results in (2).(iv). The same approach to simulation would also have worked for the simulation relation of the data in (2).(v) — we avoided it to avoid excessive clutter. The approach would not have worked for the retrenchment claim in (5), since there, we need to prove the result for *every* way of satisfying the hypotheses, and the disjunctions introduce additional cases, that are not provable without additional assumptions. However, the approach we adopted, based on overriding, avoids all these difficulties, at the price of a little more complexity.

Remark 8.3 As a corollary, we note that if the vertical composition of concessions in (8.23) had satisfied the conditions of being *compatibly tidy* (in the terminology of [Banach and Jeske (2010)]), then we could have strengthened the $D^\bullet \mathbin{;} D^\circ \Leftarrow D^\sim$ implication in (2).(iv) to an equality, since the other two disjuncts of D° would have been absent. We again avoided the details to avoid excessive clutter.

Remark 8.4 In point (4) of the theorem we highlighted disjunctive fusion composition, since it is valid without restriction. The corresponding conjunctive composition is not as generally applicable —requiring a 'close to cosimulation' criterion to hold— which is not true in general under our hypotheses. See [Banach et al. (2008)] for details. The easiest way to get the needed criterion is to demand that the *Abs* system is deterministic, i.e. there is a unique after-state and output for each before-state and input. An alternative way, involves the use of conditions like (8.2) and (8.3), but this time permitting the replacement of after-states and outputs rather than before-states and inputs. We omitted the details.

Remark 8.5 As in earlier remarks, the composition of K^*,R^*,V^* with K°,R°,V° need not be the identity; still less the composition of H°,Q°,N°,D° and H^*,Q^*,N^*,D^*.

Remark 8.6 It is tempting to think that[11] the construction of *Univ* should involve the free use of the components of *Ret* and *Ref* alone (with *Univ* expected to play a more veiled role, its components typically existentially bound). The treatment in [Jeske (2005)] was developed with this view in mind, and shows just how arduous it is to obtain a postjoin result from such a perspective. More seriously, that treatment requires numerous restrictions to hold, and is tied to a particular use of APP_{Op} sets, something that a general account should strive to avoid if at all possible — all this certainly left the authors thinking that 'there must be a better way'. The clean, unrestricted and general nature of the construction of Theorem 8.1 confirms that the au-

11. Translation: same as footnote 9.

thors' earlier beliefs about the structure of the *Univ* system were less than ideal, and that a reappraisal of the whole issue, undertaken, as here, with the wisdom of hindsight, was thoroughly justified.

9 The Prejoin Theorem

In this section we consider the Prejoin Theorem in detail. The relevant part of Fig. 2 is elaborated in Fig. 6. The given systems are *Ret* and *Ref*, together with a system *Conc*. There is a retrenchment from *Ret* to *Conc* and a refinement from *Ref* to *Conc*, the data for these being adapted from usual notation (the reader should note that due to the geometrical arrangement of the three systems, our running notational conventions cannot be fully maintained — so he should be alert to the differences). The constructed system is *Univ*, with a retrenchment from *Univ* to *Ref* and a refinement from *Univ* to *Ret*. The universal nature of the relationship between *Univ* and the other systems is expressed by saying that whenever there is a system *Xtra*, enjoying similar properties to *Univ*, then *Xtra* is more abstract than *Univ*, witnessed by 'in simulation' relationships between the transitions of *Xtra* and *Univ*, strengthened under relatively benign conditions, to a retrenchment —and still further to a refinement— from *Xtra* to *Univ*.

In contrast to our preceding results, which assumed arbitrary refinements and retrenchments in their hypotheses, for Theorem 9.1 we need a mild additional assumption about the hypothesised retrenchment. For this we revert to the notation of Section 3. We say that a retrenchment G,P,O,C is accommodating iff:

$$\begin{aligned}
&G(u, v) \wedge P_{Op}(i, j, u, v) \;\Rightarrow \\
&\quad (\exists\, u', v', o, p \bullet ((G(u', v') \wedge O_{Op}(o, p; u', v', i, j, u, v)) \vee \\
&\qquad C_{Op}(u', v', o, p; i, j, u, v)))
\end{aligned} \tag{9.1}$$

Note that any retrenchment may be made accommodating by weakening the concession sufficiently.

Theorem 9.1 Let *Ret* (with variables v, j, p, operation names $\mathsf{Ops}_{\mathrm{T}}$) and *Ref* (with variables w, k, q, operation names $\mathsf{Ops}_{\mathrm{F}}$) and *Conc* (with variables u, i, o, operation names $\mathsf{Ops}_{\mathrm{C}}$) be three systems. Let there be a retrenchment from *Ret* to *Conc* with retrenchment data H, $\{Q_{Op}, N_{Op}, D_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{TC}}\}$ where $\mathsf{Ops}_{\mathrm{TC}}$ is the set of common names of related operations of *Ret* and *Conc*. Let there be a refinement from *Ref* to *Conc* with refinement data K, $\{R_{Op}, V_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{F}} = \mathsf{Ops}_{\mathrm{C}}\}$ where $\mathsf{Ops}_{\mathrm{F}}$ is the set of operation names of both *Ref* and *Conc*. Suppose, for all Op, that $H \wedge Q_{Op}$ is a non-empty relation, and that the retrenchment is accommodating. Then we have the following.

(1) There is a system *Univ* (with variables t, h, n), with operation name set $\mathsf{Ops}_{\mathrm{U}}$, where $\mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{T}}$, such that:

  (i) there is a refinement from *Univ* to *Ret* (with refinement data $K^{\bullet}(t, v)$, $\{R^{\bullet}_{Op}, V^{\bullet}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}} = \mathsf{Ops}_{\mathrm{T}}\}$ say);

  (ii) there is a retrenchment from *Univ* to *Ref* (with retrenchment data $H^{\bullet}(t, w)$, $\{Q^{\bullet}_{Op}, N^{\bullet}_{Op}, D^{\bullet}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{UF}}\}$ say);

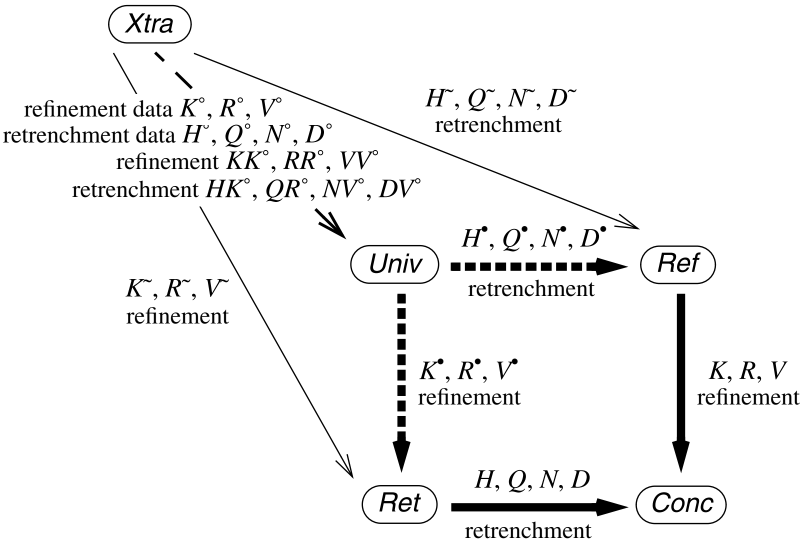


Fig. 6. The prejoin construction in detail. The pseudoretrenchment $G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times}$ (not shown) connects *Ret* to *Ref*.

(iii) the composition of the retrenchment H,Q,N,D with the pseudorefinement $K^{\mathrm{T}},R^{\mathrm{T}},V^{\mathrm{T}}$ yields a pseudoretrenchment $G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times}$, which is also given by the composition of the pseudorefinement $K^{\bullet\mathrm{T}},R^{\bullet\mathrm{T}},V^{\bullet\mathrm{T}}$ with the retrenchment $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$;

(iv) each transition of *Univ* is in simulation with a transition of *Ret*, or with a transition of *Ref*, or both, and in the last case, any such pair of *Ret* and *Ref* transitions are in simulation via the pseudoretrenchment $G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times}$;

(v) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Univ* are given by:

$$\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \;\equiv\; (\exists\, v, j \bullet K^{\bullet}(t, v) \wedge R^{\bullet}{}_{Op}(h, j) \wedge \mathrm{APP}_{Op_{\mathrm{T}}}(v, j)) \qquad (9.2)$$

(2) Whenever there is a system *Xtra* (with variables $t^{\sim}$, $h^{\sim}$, $n^{\sim}$), with operation name set $\mathsf{Ops}_{\mathrm{X}}$ where $\mathsf{Ops}_{\mathrm{X}} = \mathsf{Ops}_{\mathrm{T}}$, with a refinement from *Xtra* to *Ret* given by $K^{\sim},R^{\sim},V^{\sim}$, with a retrenchment from *Xtra* to *Ref* given by $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$, where the composition of the pseudorefinement $K^{\sim\mathrm{T}},R^{\sim\mathrm{T}},V^{\sim\mathrm{T}}$ with the retrenchment $H^{\sim},Q^{\sim},N^{\sim},D^{\sim}$ yields the pseudoretrenchment $G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times}$, where each transition of *Xtra* is in simulation with a transition of *Ret*, or with a transition of *Ref*, or both, and where in the last case, any such pair of *Ret* and *Ref* transitions are in simulation via the pseudoretrenchment $G^{\times},G^{\times} \wedge P^{\times},O^{\times},C^{\times}$, then:

(i) there exist refinement data, $K^{\circ}(t^{\sim}, t)$, $\{R^{\circ}{}_{Op}, V^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say, from *Xtra* to *Univ*, via which, every transition of *Xtra* that is in simulation with a transition of *Ret* is in simulation with a transition of *Univ*;

(ii) there exist retrenchment data, $H^{\circ}(t^{\sim}, t)$, $\{Q^{\circ}{}_{Op}, N^{\circ}{}_{Op}, D^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say, from *Xtra* to *Univ*, via which, every transition of *Xtra* that is in simulation with a transition of *Ref* is in simulation with a transition of *Univ*;

(iii) $K^{\circ} \mathbin{⨾} K^{\bullet} = K^{\sim}$ and $R^{\circ} \mathbin{⨾} R^{\bullet} = R^{\sim}$ and $V^{\circ} \mathbin{⨾} V^{\bullet} = V^{\sim}$;

(iv) $H^{\circ} \mathbin{⨾} H^{\bullet} = H^{\sim}$ and for $Op_{\mathrm{X}} \in \mathsf{Ops}_{\mathrm{XF}}$, $(H^{\circ} \wedge Q^{\circ}) \mathbin{⨾} (H^{\bullet} \wedge Q^{\bullet}) = (H^{\sim} \wedge Q^{\sim})$ and $N^{\circ} \mathbin{⨾} N^{\bullet} = N^{\sim}$ and $D^{\circ} \mathbin{⨾} D^{\bullet} \Leftarrow D^{\sim}$.

(v) there exist retrenchment data, $HK^{\circ}(t^{\sim}, t)$, $\{QR^{\circ}{}_{Op}, NV^{\circ}{}_{Op}, DV^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say, from *Xtra* to *Univ*, via which, every transition of *Xtra* that is in simulation with a transition of *Ret* or with a transition of *Ref*, is in simulation with a transition of *Univ*.

(3) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, then *Univ* and *Univ** are inter-simulable.

(4) There is a retrenchment from *Univ* to *Conc* (with retrenchment data $G(t, u)$, $\{P_{Op}, O_{Op}, C_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{UC}}\}$ say), given by the disjunctive fusion composition of two retrenchments (a) and (b): (a) is the vertical composition of $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$ with K,R,V; (b) is the vertical composition of $K^{\bullet},R^{\bullet},V^{\bullet}$ with H,Q,N,D.

(5) There is a retrenchment from *Xtra* to *Univ* (with retrenchment data $HH^{\circ}(t^{\sim}, t)$, $\{QQ^{\circ}{}_{Op}, NN^{\circ}{}_{Op}, DD^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say).

(6) Referring to the data given in (5), provided that:

$$(\exists\, t^{\sim}, h^{\sim}, n^{\sim} \bullet stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})) \wedge$$
$$(\exists\, t^{\sim}, t, h^{\sim}, h, n^{\sim}, n \bullet DD^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t)) \;\Rightarrow\; HH^{\circ}(t^{\sim\prime}, t') \quad (9.3)$$

then:

(i) the retrenchment of (5) from *Xtra* to *Univ*, strengthens to a refinement, (with refinement data $KK^{\circ}(t^{\sim}, t)$, $\{RR^{\circ}{}_{Op}, VV^{\circ}{}_{Op} \mid Op \in \mathsf{Ops}_{\mathrm{U}}\}$ say);

(ii) if the notion of refinement in question requires the use of APP_{Op} sets, then the APP_{Op} sets of *Xtra* need to satisfy:

$$\mathrm{APP}_{Op_{\mathrm{U}}}(t, h) \wedge KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}{}_{Op}(h^{\sim}, h) \;\Lleftarrow\!\!\!\Rrightarrow\; KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}{}_{Op}(h^{\sim}, h) \wedge \mathrm{APP}_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}) \quad (9.4)$$

(7) Whenever a system *Univ** has properties (1) and (2) above of *Univ*, (and further, the property noted in in (9.3) holds), then *Univ* and *Univ** are inter-retrenchable, (resp. and further, inter-refinable).

Proof. For (1), we start with the details of the refinement $K^{\bullet},R^{\bullet},V^{\bullet}$ and of the retrenchment $H^{\bullet},Q^{\bullet},N^{\bullet},D^{\bullet}$. Adapting the usual conventions for *Ret* and *Ref*, the state space of *Univ* is $t \in \mathsf{T} = \mathsf{U} \times \mathsf{V} \times \mathsf{W}$ (where U is the state space of *Conc*, V is the state space of *Ret* and W is the state space of *Ref*). There are two cases for the input and output spaces of *Univ*. If $Op \in \mathsf{Ops}_{\mathrm{UF}} = \mathsf{Ops}_{\mathrm{TC}}$, then $h \in \mathsf{H}_{Op} = \mathsf{I}_{Op} \times \mathsf{J}_{Op} \times \mathsf{K}_{Op}$ and $n \in$

$\mathsf{N}_{Op} = \mathsf{O}_{Op} \times \mathsf{P}_{Op} \times \mathsf{Q}_{Op}$. But if $Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}}$, then $h \in \mathsf{H}_{Op} = \mathsf{J}_{Op}$, $n \in \mathsf{N}_{Op} = \mathsf{P}_{Op}$. We start by giving the data for the refinement and retrenchment.

The refinement $K^\bullet, R^\bullet, V^\bullet$ is given by the data:

$$K^\bullet(t, v) \equiv (t = (u, v, w) \wedge K(w, u)) \tag{9.5}$$

$$R^\bullet{}_{Op}(h, j) \equiv \begin{cases} (h = (i, j, k) \wedge R_{Op}(k, i)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\ (h = j) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}} \end{cases} \tag{9.6}$$

$$V^\bullet{}_{Op}(n, p) \equiv \begin{cases} (n = (o, p, q) \wedge V_{Op}(q, o)) & \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\ (n = p) & \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}} \end{cases} \tag{9.7}$$

The retrenchment $H^\bullet, Q^\bullet, N^\bullet, D^\bullet$ is given by the data:

$$H^\bullet(t, w) \equiv (t = (u, v, w) \wedge H(v, u)) \tag{9.8}$$

$$Q^\bullet{}_{Op}(h, k, t, w) \equiv (h = (i, j, k) \wedge t = (u, v, w) \wedge Q_{Op}(j, i, v, u)) \tag{9.9}$$

$$\begin{aligned} &N^\bullet{}_{Op}(n, q; t', w', h, k, t, w) \equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\ &\quad N_{Op}(p, o; v', u', j, i, v, u)) \end{aligned} \tag{9.10}$$

$$\begin{aligned} &D^\bullet{}_{Op}(t', w', n, q; h, k, t, w) \equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\ &\quad D_{Op}(v', u', p, o; j, i, v, u)) \end{aligned} \tag{9.11}$$

Since we need these relations to define the *Univ* system itself, we start by checking (1).(iii). We first calculate $G^\times, G^\times \wedge P^\times, O^\times, C^\times$ for $Op \in \mathsf{Ops}_{\mathrm{UF}}$, as the composition of the retrenchment H,Q,N,D with the pseudorefinement $K^{\mathrm{T}}, R^{\mathrm{T}}, V^{\mathrm{T}}$. The fact that the result is also equal to the composition of the pseudorefinement $K^{\bullet\mathrm{T}}, R^{\bullet\mathrm{T}}, V^{\bullet\mathrm{T}}$ with the retrenchment $H^\bullet, Q^\bullet, N^\bullet, D^\bullet$ follows by inspection.

$$G^\times(v, w) \equiv H \mathbin{⨾} K^{\mathrm{T}} = (\exists\, u \bullet H(v, u) \wedge K(w, u)) = K^{\bullet\mathrm{T}} \mathbin{⨾} H^\bullet \tag{9.12}$$

$$\begin{aligned} &G^\times \wedge P^\times{}_{Op} \wedge ((G^{\times\prime} \wedge O^\times{}_{Op}) \vee C^\times{}_{Op})(v, w, j, k, v', w', p, q) \equiv \\ &(H \wedge Q_{Op} \wedge ((H' \wedge N_{Op}) \vee D_{Op})) \mathbin{⨾} (K^{\mathrm{T}} \wedge R^{\mathrm{T}}{}_{Op} \wedge K^{\mathrm{T}\prime} \wedge V^{\mathrm{T}}{}_{Op}) = \\ &(\exists\, u, i, u', o \bullet H(v, u) \wedge Q_{Op}(j, i, v, u) \wedge \\ &\quad ((H(v', u') \wedge N_{Op}(p, o; v', u', j, i, v, u)) \vee D_{Op}(v', u', p, o; j, i, v, u)) \wedge \\ &\quad K(w, u) \wedge R_{Op}(k, i) \wedge K(w', u') \wedge V_{Op}(q, o)) = \\ &(K^{\bullet\mathrm{T}} \wedge R^{\bullet\mathrm{T}}{}_{Op} \wedge K^{\bullet\mathrm{T}\prime} \wedge V^{\bullet\mathrm{T}}{}_{Op}) \mathbin{⨾} (H^\bullet \wedge Q^\bullet{}_{Op} \wedge ((H^{\bullet\prime} \wedge N^\bullet{}_{Op}) \vee D^\bullet{}_{Op})) \end{aligned} \tag{9.13}$$

The *Univ* system itself is given as follows. Initialisation in *Univ* is given by:

$$Init_{\mathrm{U}}(t') \equiv (t' = (u', v', w') \wedge \{[Init_{\mathrm{T}}(v') \wedge K^\bullet(t', v')] \vee [Init_{\mathrm{F}}(w') \wedge H^\bullet(t', w')]\}) \tag{9.14}$$

The operations of *Univ* are given by:

$$\begin{aligned} &stp_{Op_{\mathrm{U}}}(t, h, t', n) \equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\ &\quad \{[stp_{Op_{\mathrm{T}}}(v, j, v', p) \wedge K^\bullet(t, v) \wedge R^\bullet{}_{Op}(h, j) \wedge K^\bullet(t', v') \wedge V^\bullet{}_{Op}(n, p)] \vee \\ &\quad [stp_{Op_{\mathrm{F}}}(w, k, w', q) \wedge H^\bullet(t, w) \wedge Q^\bullet{}_{Op}(h, k, t, w) \wedge \\ &\qquad ((H^\bullet(t', w') \wedge N^\bullet{}_{Op}(n, q; t', w', h, k, t, w)) \vee D^\bullet{}_{Op}(t', w', n, q; h, k, t, w))]\}) \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \end{aligned}$$

$(t = (u, v, w) \wedge h = j \wedge t' = (u', v', w') \wedge n = p \wedge$
$[stp_{Op_T}(v, j, v', p) \wedge K^{\bullet}(t, v) \wedge R^{\bullet}_{Op}(h, j) \wedge K^{\bullet}(t', v') \wedge V^{\bullet}_{Op}(n, p)])$
$$\text{if } Op \in \mathsf{Ops}_{U\backslash UF} \qquad (9.15)$$

For (1).(i) we check that $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement. For the initialisation PO, suppose we have $Init_T(v')$. Then we just need to find w', u', such that $K(w', u')$ holds, and then we can set $t' = (u', v', w')$, after which we will have $Init_T(v') \wedge K^{\bullet}(t', v')$ which gives $Init_U(t') \wedge K^{\bullet}(t', v')$, discharging the PO.

For the operation PO, suppose $Op \in \mathsf{Ops}_{UF}$, and let us assume $K^{\bullet}(t, v) \wedge R^{\bullet}_{Op}(h, j) \wedge stp_{Op_T}(v, j, v', p)$. Then we just need to find w', u', such that $K(w', u')$ holds, and q, o, such that $V_{Op}(q, o)$ holds, and then we can set $t' = (u', v', w')$ and $n = (o, p, q)$, after which we will have enough for the first disjunct in the $Op \in \mathsf{Ops}_{UF}$ case of (9.15). If $Op \in \mathsf{Ops}_{U\backslash UF}$, the argument is similar.

For (1).(ii) we check that $H^{\bullet}$,$Q^{\bullet}$,$N^{\bullet}$,$D^{\bullet}$ is a retrenchment. For the initialisation PO, suppose we have $Init_F(w')$. Then we just need to find v', u', such that $H(v', u')$ holds, and then we can set $t' = (u', v', w')$, after which we will have $Init_F(w') \wedge H^{\bullet}(t', w')$ which gives $Init_U(t') \wedge H^{\bullet}(t', w')$, discharging the PO.

For the operation PO, let us assume $H^{\bullet}(t, w) \wedge Q^{\bullet}_{Op}(h, k, t, w) \wedge stp_{Op_F}(w, k, w', q)$. Then $H^{\bullet} \wedge Q^{\bullet}_{Op}$ gives us $H(v, u) \wedge Q_{Op}(j, i, v, u)$. Since the retrenchment H,Q,N,D is accommodating, (9.1) implies that we can find values v', u', p, o, such that $(H(v', u') \wedge N_{Op}(p, o; v', u', j, i, v, u)) \vee D_{Op}(v', u', p, o; j, i, v, u)$ holds, after which we can set $t' = (u', v', w')$ and $n = (o, p, q)$, and then we will have enough for the second disjunct in the $Op \in \mathsf{Ops}_{UF}$ case of (9.15).

For (1).(iv), it is clear from the arguments above that each step t -(h, Op_U, n)-› t' of *Univ* is in simulation with (in the refinement sense) its constituent stp_{Op_T} transition (if the first disjunct of the $Op \in \mathsf{Ops}_{UF}$ case of (9.15) holds, or we are in the $Op \in \mathsf{Ops}_{U\backslash UF}$ case), or alternatively is in simulation with (in the retrenchment sense) its constituent stp_{Op_F} transition (if the second disjunct of the $Op \in \mathsf{Ops}_{UF}$ case of (9.15) holds). If both disjuncts hold, then the *Ret* and *Ref* transitions are evidently in simulation via the pseudoretrenchment $G^{\times}$,$G^{\times} \wedge P^{\times}$,$O^{\times}$,$C^{\times}$ because of the values of u, i, u', o, that are common to the two transitions.

For (1).(v), since $K^{\bullet} \wedge R^{\bullet}_{Op}$ is a (partial) function from $\mathsf{T} \times \mathsf{H}_{Op}$ onto $\mathsf{V} \times \mathsf{J}_{Op}$, we have $(K^{\bullet T} \wedge R^{\bullet T}_{Op}) ⨾ (K^{\bullet} \wedge R^{\bullet}_{Op}) = \mathrm{Id}_{\mathsf{V} \times \mathsf{J}_{Op}}$. Consequently, the definition of the APP_{Op} sets of *Univ* in (9.2) satisfies the condition in (3.15) as regards the $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ refinement, and consequently satisfies an APP_{Op} requirement of either the (3.9) or (3.10) form. This completes (1).

For (2).(i), we start with the data for the refinement K°,R°,V° which is given by:

$$K^{\circ}(t^{\sim}, t) \equiv (\exists\, v \bullet K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v)) \qquad (9.16)$$

$$R^{\circ}_{Op}(h^{\sim}, h) \equiv (\exists\, j \bullet R^{\bullet}_{Op}(h, j) \wedge R^{\sim}_{Op}(h^{\sim}, j)) \qquad (9.17)$$

$$V^{\circ}_{Op}(n^{\sim}, n) \equiv (\exists\, p \bullet V^{\bullet}_{Op}(n, p) \wedge V^{\sim}_{Op}(n^{\sim}, p)) \qquad (9.18)$$

We must show that every transition of *Xtra* that is in simulation with a transition of *Ret* is in simulation with a transition of *Univ* via (9.16)-(9.18). Suppose we have an *Xtra* step, $t^{\sim}$ -($h^{\sim}$, Op_X, $n^{\sim}$)-› $t^{\sim\prime}$ say, which is in simulation with some step of *Ret*, v -(j, Op_T, p)-› v' say, via $K^{\sim}$,$R^{\sim}$,$V^{\sim}$. Since $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ is a refinement, and $K^{\bullet} \wedge R^{\bullet}_{Op}$ is onto $\mathsf{V} \times \mathsf{J}_{Op}$, step v -(j, Op_{T}, p)-› v' will be in simulation with some step of *Univ*, say t -(h, Op_{U}, n)-› t'. Composing the $K^\bullet$,$R^\bullet$,$V^\bullet$ simulation with the $K^\sim$,$R^\sim$,$V^\sim$ simulation now yields the result.

For (2).(ii), we start with the retrenchment data H°,Q°,N°,D°. This is the vertical composition of the $H^\sim$,$Q^\sim$,$N^\sim$,$D^\sim$ and $H^{\bullet\mathrm{T}}$,$Q^{\bullet\mathrm{T}}$,$N^{\bullet\mathrm{T}}$,$D^{\bullet\mathrm{T}}$ data, and is given by:

$$H^\circ(t^\sim, t) \;\equiv\; (\exists\, w \bullet H^\bullet(t, w) \wedge H^\sim(t^\sim, w)) \tag{9.19}$$

$$\begin{aligned} &Q^\circ{}_{Op}(h^\sim, h, t^\sim, t) \;\equiv\; (\exists\, k, w \bullet \\ &\qquad H^\bullet(t, w) \wedge H^\sim(t^\sim, w) \wedge Q^\bullet{}_{Op}(h, k, t, w) \wedge Q^\sim{}_{Op}(h^\sim, k, t^\sim, w)) \end{aligned} \tag{9.20}$$

$$\begin{aligned} &N^\circ{}_{Op}(n^\sim, n; t^{\sim\prime}, t', h^\sim, h, t^\sim, t) \;\equiv\; (\exists\, w, k, w', q \bullet \\ &\qquad N^\bullet{}_{Op}(n, q; t', w', h, k, t, w) \wedge N^\sim{}_{Op}(n^\sim, q; t^{\sim\prime}, w', h^\sim, k, t^\sim, w)) \end{aligned} \tag{9.21}$$

$$\begin{aligned} &D^\circ{}_{Op}(t^{\sim\prime}, t', n^\sim, n; h^\sim, h, t^\sim, t) \;\equiv\; (\exists\, w, k, w', q \bullet \\ &\qquad \{[H^\bullet(t', w') \wedge N^\bullet{}_{Op}(n, q; t', w', h, k, t, w) \wedge \\ &\qquad\qquad D^\sim{}_{Op}(t^{\sim\prime}, w', n^\sim, q; h^\sim, k, t^\sim, w)] \vee \\ &\qquad [D^\bullet{}_{Op}(t', w', n, q\,; h, k, t, w) \wedge \\ &\qquad\qquad H^\sim(t^{\sim\prime}, w') \wedge N^\sim{}_{Op}(n^\sim, q; t^{\sim\prime}, w', h^\sim, k, t^\sim, w)] \vee \\ &\qquad [D^\bullet{}_{Op}(t', w', n, q; h, k, t, w) \wedge \\ &\qquad\qquad D^\sim{}_{Op}(t^{\sim\prime}, w', n^\sim, q; h^\sim, k, t^\sim, w)]\}) \end{aligned} \tag{9.22}$$

We must show that every transition of *Xtra* that is in simulation with a transition of *Ref* is in simulation with a transition of *Univ* via (9.19)-(9.22). Suppose we have an *Xtra* step, $t^\sim$ -($h^\sim$, Op_{X}, $n^\sim$)-› $t^{\sim\prime}$ say, which is in simulation with some step of *Ref*, w -(k, Op_{F}, q)-› w' say, via $H^\sim$,$Q^\sim$,$N^\sim$,$D^\sim$. Since by assumption, $H \wedge Q_{Op}$ is a non-empty relation, $H^\bullet \wedge Q^\bullet{}_{Op}$ is necessarily a non-empty (partial) function onto $\mathsf{W} \times \mathsf{K}_{Op}$. Therefore, since $H^\bullet$,$Q^\bullet$,$N^\bullet$,$D^\bullet$ is a retrenchment, the transition w -(k, Op_{F}, q)-› w' will be in simulation with some *Univ* step, t -(h, Op_{U}, n)-› t' say. Now, composing the $H^\bullet$,$Q^\bullet$,$N^\bullet$,$D^\bullet$ simulation with the $H^\sim$,$Q^\sim$,$N^\sim$,$D^\sim$ simulation yields the desired result via the distributive law applied to $((H^{\sim\prime} \wedge N^\sim) \vee D^\sim) \wedge ((H^{\bullet\prime} \wedge N^\bullet) \vee D^\bullet)$.

For (2).(iii), since $K^\circ = K^\sim \mathbin{⨾} K^{\bullet\mathrm{T}}$, then $K^\circ \mathbin{⨾} K^\bullet = K^\sim \mathbin{⨾} K^{\bullet\mathrm{T}} \mathbin{⨾} K^\bullet = K^\sim \mathbin{⨾} \mathrm{Id}_{\mathsf{V}} = K^\sim$ (since $K^\bullet$ is a partial function). The remaining results are similar.

For (2).(iv), since $H^\circ = H^\sim \mathbin{⨾} H^{\bullet\mathrm{T}}$, we derive that $H^\circ \mathbin{⨾} H^\bullet = H^\sim \mathbin{⨾} H^{\bullet\mathrm{T}} \mathbin{⨾} H^\bullet = H^\sim \mathbin{⨾} \mathrm{Id}_{\mathsf{W}} = H^\sim$ (since $H^\bullet$ is a partial function). Deriving $N^\circ \mathbin{⨾} N^\bullet = N^\sim$ is similar. Now, consider $D^\circ \mathbin{⨾} D^\bullet$ where D° is given by (9.22). The term $D^\sim \wedge D^{\bullet\mathrm{T}}$, which occurs disjunctively in (9.22), shows that $D^\circ \mathbin{⨾} D^\bullet$ contains $D^\sim \mathbin{⨾} D^{\bullet\mathrm{T}} \mathbin{⨾} D^\bullet = D^\sim \mathbin{⨾} \mathrm{Id}_{\mathsf{W} \times \mathsf{K}_{Op} \times \mathsf{W} \times \mathsf{Q}_{Op}} = D^\sim$. The other disjuncts in (9.22) lead to $D^\circ \mathbin{⨾} D^\bullet \Leftarrow D^\sim$. Finally, by assumption, $H \wedge Q$ is a non-empty relation. This makes $H^{\bullet\mathrm{T}} \wedge Q^{\bullet\mathrm{T}}$ a non-empty (partial) function onto $\mathsf{W} \times \mathsf{K}_{Op}$. Therefore $(H^\circ \wedge Q^\circ) \mathbin{⨾} (H^\bullet \wedge Q^\bullet) = (H^\sim \wedge Q^\sim)$ can be shown in the same way as other similar results.[12] We are done.

For (2).(v), we start with the retrenchment data HK°,QR°,NV°,DV° given by (9.23)-(9.26). Note that this is a kind of disjunction of the data in (9.16)-(9.18) with the data in (9.19)-(9.22):

---

12. For other similar results, the non-emptiness of the partial function follows from the assumed non-emptiness of the underlying relation, via Assumption 1.1. For $H \wedge Q$, non-emptiness does not follow from non-emptiness of H and Q individually.

$$
\begin{aligned}
& HK^{\circ}(t^{\sim}, t) \;\equiv \\
& \quad (t = (u, v, w) \wedge \\
& \quad \{[(H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w)] \vee [K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v)]\})
\end{aligned}
\tag{9.23}
$$

$$
\begin{aligned}
& QR^{\circ}{}_{Op}(h^{\sim}, h, t^{\sim}, t) \;\equiv \\
& \quad (t = (u, v, w) \wedge h = (i, j, k) \wedge \\
& \quad \{[H^{\bullet}(t, w) \wedge H^{\sim}(t^{\sim}, w) \wedge Q^{\bullet}{}_{Op}(h, k, t, w) \wedge Q^{\sim}{}_{Op}(h^{\sim}, k, t^{\sim}, w)] \vee \\
& \quad [K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\bullet}{}_{Op}(h, j) \wedge R^{\sim}{}_{Op}(h^{\sim}, j)]\}) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\
& \quad (t = (u, v, w) \wedge h = j \wedge \\
& \quad K^{\bullet}(t, v) \wedge K^{\sim}(t^{\sim}, v) \wedge R^{\bullet}{}_{Op}(h, j) \wedge R^{\sim}{}_{Op}(h^{\sim}, j)) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}}
\end{aligned}
\tag{9.24}
$$

$$
\begin{aligned}
& NV^{\circ}{}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \;\equiv \\
& \quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\
& \quad \{[H^{\bullet}(t', w') \wedge H^{\sim}(t^{\sim\prime}, w') \wedge \\
& \qquad N^{\bullet}{}_{Op}(n, q; t', w', h, k, t, w) \wedge N^{\sim}{}_{Op}(n^{\sim}, q; t^{\sim\prime}, w', h^{\sim}, k, t^{\sim}, w)] \vee \\
& \quad [K^{\bullet}(t', v') \wedge K^{\sim}(t^{\sim\prime}, v') \wedge V^{\bullet}{}_{Op}(n, p) \wedge V^{\sim}{}_{Op}(n^{\sim}, p)]\}) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\
& \quad (n = p \wedge V^{\bullet}{}_{Op}(n, p) \wedge V^{\sim}{}_{Op}(n^{\sim}, p)) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}}
\end{aligned}
\tag{9.25}
$$

$$
\begin{aligned}
& DV^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t) \;\equiv \\
& \quad (t = (u, v, w) \wedge h = (i, j, k) \wedge t' = (u', v', w') \wedge n = (o, p, q) \wedge \\
& \quad \{[H^{\bullet}(t', w') \wedge N^{\bullet}{}_{Op}(n, q; t', w', h, k, t, w) \wedge \\
& \qquad D^{\sim}{}_{Op}(t^{\sim\prime}, w', n^{\sim}, q; h^{\sim}, k, t^{\sim}, w)] \vee \\
& \quad [D^{\bullet}{}_{Op}(t', w', n, q\ ; h, k, t, w) \wedge \\
& \qquad H^{\sim}(t^{\sim\prime}, w') \wedge N^{\sim}{}_{Op}(n^{\sim}, q; t^{\sim\prime}, w', h^{\sim}, k, t^{\sim}, w)] \vee \\
& \quad [D^{\bullet}{}_{Op}(t', w', n, q; h, k, t, w) \wedge \\
& \qquad D^{\sim}{}_{Op}(t^{\sim\prime}, w', n^{\sim}, q; h^{\sim}, k, t^{\sim}, w)]\}) \\
& \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\
& \quad \mathsf{false} \qquad\qquad\qquad\qquad\qquad\qquad\quad \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}}
\end{aligned}
\tag{9.26}
$$

In the terminology of [Banach et al. (2008)] the composition of (9.23)-(9.26) is a kind of blend of: disjunctive fusion composition (since the state and I/O spaces are (partly) the same), and synchronous parallel composition (since the state and I/O spaces are (partly) different), of the refinement data (9.16)-(9.18) and the retrenchment data (9.19)-(9.22).

With the retrenchment data in place, the argument is now an adaptation of the proofs of (2).(i) and (2).(ii). Let $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ be a step of *Xtra*. By assumption, it is in simulation with a transition of *Ret* or with a transition of *Ref*. By (2).(i) and (2).(ii) this extends to the step $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ being in simulation with a transition of *Univ* via either the refinement data (9.16)-(9.18) or the retrenchment data (9.19)-(9.22). In the former case, it is easy to see that $K^{\circ} \wedge R^{\circ}{}_{Op}$ implies $HK^{\circ} \wedge QR^{\circ}{}_{Op}$ and that $K^{\circ\prime} \wedge V^{\circ}{}_{Op}$ also implies $HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}$, as in (2).(i). In the latter case, it is easy to see that $H^{\circ} \wedge Q^{\circ}{}_{Op}$ implies $HK^{\circ} \wedge QR^{\circ}{}_{Op}$ and that $(H^{\circ\prime} \wedge N^{\circ}{}_{Op}) \vee D^{\circ}{}_{Op}$ also implies $(HK^{\circ\prime} \wedge NV^{\circ}{}_{Op}) \vee DV^{\circ}{}_{Op}$, as in (2).(ii). This completes part (2).

For (3), we note that *Univ* itself satisfies the criteria demanded of *Xtra*. Therefore, if we have a system *Univ** with the properties (1) and (2) of *Univ*, then *Univ** satisfies the criteria demanded of *Xtra* too. Hence we can construct two instances of Fig. 6 as follows. In the first, *Univ* is in its conventional place and *Univ** replaces *Xtra*, and there are refinement data $K^\circ, R^\circ, V^\circ$, and retrenchment data $H^\circ, Q^\circ, N^\circ, D^\circ$, from *Univ** to *Univ*. In the second, *Univ** replaces *Univ*, and *Univ* replaces *Xtra*, and there are refinement data K^*, R^*, V^*, and retrenchment data H^*, Q^*, N^*, D^*, from *Univ* to *Univ**. So *Univ* and *Univ** are inter-simulable by the arguments above.

For (4), we just observe that disjunctive fusion composition of retrenchments, and the vertical composition between retrenchments and refinements (both ways round) are sound composition mechanisms. For the record, we present the composed retrenchment data:

$$G(t, u) \equiv (t = (\underline{u}, v, w) \wedge \{[H(v, u) \wedge K(w, \underline{u})] \vee [K(w, u) \wedge H(v, \underline{u})]\}) \tag{9.27}$$

$$\begin{aligned} &P_{Op}(h, i, t, u) \equiv (h = (\underline{i}, j, k) \wedge t = (\underline{u}, v, w) \wedge \\ &\quad \{[K(w, \underline{u}) \wedge R_{Op}(k, \underline{i}) \wedge H(v, u) \wedge Q_{Op}(j, i, v, u)] \vee \\ &\quad [K(w, u) \wedge R_{Op}(k, i) \wedge H(v, \underline{u}) \wedge Q_{Op}(j, \underline{i}, v, \underline{u})]\}) \end{aligned} \tag{9.28}$$

$$\begin{aligned} &O_{Op}(n, o; t', u', h, i, t, u) \equiv \\ &\quad (t = (\underline{u}, v, w) \wedge h = (\underline{i}, j, k) \wedge t' = (\underline{u}', v', w') \wedge n = (\underline{o}, p, q) \wedge \\ &\quad \{[H(v', \underline{u}') \wedge K(w, u) \wedge R_{Op}(k, i) \wedge K(w', u') \wedge V_{Op}(q, o) \wedge \\ &\qquad N_{Op}(p, \underline{o}; v', \underline{u}', j, \underline{i}, v, \underline{u})] \vee \\ &\quad [H(v', u') \wedge K(w, \underline{u}) \wedge R_{Op}(k, \underline{i}) \wedge K(w', \underline{u}') \wedge V_{Op}(q, \underline{o}) \wedge \\ &\qquad N_{Op}(p, o; v', u', j, i, v, u)] \vee \\ &\quad [K(w, u) \wedge R_{Op}(k, i) \wedge K(w', u') \wedge V_{Op}(q, o) \wedge \\ &\qquad N_{Op}(p, \underline{o}; v', \underline{u}', j, \underline{i}, v, \underline{u}) \wedge N_{Op}(p, o; v', u', j, i, v, u) \wedge \\ &\qquad K(w, \underline{u}) \wedge R_{Op}(k, \underline{i}) \wedge K(w', \underline{u}') \wedge V_{Op}(q, \underline{o})]\}) \end{aligned} \tag{9.29}$$

$$\begin{aligned} &C_{Op}(t', u', n, o\, ; h, i, t, u) \equiv \\ &\quad (t = (\underline{u}, v, w) \wedge h = (\underline{i}, j, k) \wedge t' = (\underline{u}', v', w') \wedge n = (\underline{o}, p, q) \wedge \\ &\quad \{[D_{Op}(v', u', p, o; j, i, v, u) \wedge K(w, \underline{u}) \wedge R_{Op}(k, \underline{i}) \wedge K(w', \underline{u}') \wedge V_{Op}(q, \underline{o})] \vee \\ &\quad [K(w, u) \wedge R_{Op}(k, i) \wedge K(w', u') \wedge V_{Op}(q, o) \wedge D_{Op}(v', \underline{u}', p, \underline{o}; j, \underline{i}, v, \underline{u})]\}) \end{aligned} \tag{9.30}$$

For (5), we start with the retrenchment data $HH^\circ, QQ^\circ, NN^\circ, DD^\circ$, which is given by (9.31)-(9.34) below. Note that this differs from the earlier retrenchment data $HK^\circ, QR^\circ, NV^\circ, DV^\circ$ in (9.23)-(9.26), only by the replacement of the disjunction in the within relation QR° by a conjunction in the within relation QQ°.

$$HH^\circ(t^\sim, t) \equiv HK^\circ(t^\sim, t) \tag{9.31}$$

$$\begin{aligned} &QQ^\circ{}_{Op}(h^\sim, h, t^\sim, t) \equiv \\ &\quad (t = (u, v, w) \wedge h = (i, j, k) \wedge \\ &\quad \{[H^\bullet(t, w) \wedge H^\sim(t^\sim, w) \wedge Q^\bullet{}_{Op}(h, k, t, w) \wedge Q^\sim{}_{Op}(h^\sim, k, t^\sim, w)] \wedge \\ &\quad [K^\bullet(t, v) \wedge K^\sim(t^\sim, v) \wedge R^\bullet{}_{Op}(h, j) \wedge R^\sim{}_{Op}(h^\sim, j)]\}) \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{UF}} \\ &\quad (t = (u, v, w) \wedge h = j \wedge \\ &\quad K^\bullet(t, v) \wedge K^\sim(t^\sim, v) \wedge R^\bullet{}_{Op}(h, j) \wedge R^\sim{}_{Op}(h^\sim, j)) \\ &\qquad\qquad\qquad\qquad\qquad\qquad \text{if } Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}} \end{aligned} \tag{9.32}$$

$$NN^{\circ}{}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \equiv NV^{\circ}{}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \tag{9.33}$$

$$DD^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t) \equiv DV^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t) \tag{9.34}$$

To prove (5), we start with the initialisation. Suppose $Init_{\mathrm{U}}(t')$, in (9.14), holds. Suppose the $[Init_{\mathrm{T}}(v') \wedge K^{\bullet}(t', v')]$ disjunct of $Init_{\mathrm{U}}(t')$ holds. From $Init_{\mathrm{T}}(v')$, because $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ is a refinement, we can find a $t^{\sim\prime}$ such that $Init_{\mathrm{X}}(t^{\sim\prime}) \wedge K^{\sim}(t^{\sim\prime}, v')$ holds. Composing $K^{\sim}$ and $K^{\bullet}$ gives the second disjunct of HH°, so we have $Init_{\mathrm{X}}(t^{\sim\prime}) \wedge HH^{\circ}(t^{\sim\prime}, t')$ as needed. Alternatively, suppose the $H^{\bullet}$ disjunct of $Init_{\mathrm{U}}(t')$ holds. The argument is analogous. We are done.

For the operation PO, suppose we have $HH^{\circ} \wedge QQ^{\circ}{}_{Op} \wedge stp_{Op_{\mathrm{U}}}$. It is evident that QQ° strengthens HH°. Suppose that the $stp_{Op_{\mathrm{T}}} \wedge K^{\bullet}$ disjunct of $stp_{Op_{\mathrm{U}}}$ is true (whether this is for the $Op \in \mathsf{Ops}_{\mathrm{UF}}$ case or the $Op \in \mathsf{Ops}_{\mathrm{U \backslash UF}}$ case). Then $HH^{\circ} \wedge QQ^{\circ}{}_{Op}$ factors uniquely through v, j, in *Ret*, and the *Univ* step, t -(h, Op_{U}, n)-› t' say, projects via $K^{\bullet}$,$R^{\bullet}$,$V^{\bullet}$ to its enclosed *Ret* step v -(j, Op_{T}, p)-› v' say. If we now extract $K^{\sim} \wedge R^{\sim}{}_{Op}$ from our assumed $HH^{\circ} \wedge QQ^{\circ}{}_{Op}$, then with v -(j, Op_{T}, p)-› v', we can apply the $K^{\sim}$,$R^{\sim}$,$V^{\sim}$ refinement operation PO to derive a step of *Xtra*, $t^{\sim}$ -($h^{\sim}$, Op_{X}, $n^{\sim}$)-› $t^{\sim\prime}$ say, for which $K^{\sim\prime} \wedge V^{\sim}{}_{Op}$, and thence $K^{\bullet\prime} \wedge K^{\sim\prime} \wedge V^{\bullet}{}_{Op} \wedge V^{\sim}{}_{Op}$, and thence $HH^{\circ\prime} \wedge NN^{\circ}{}_{Op}$, all hold. The last of these discharges our goal. Alternatively, suppose that the $stp_{Op_{\mathrm{F}}} \wedge H^{\bullet}$ disjunct of $stp_{Op_{\mathrm{U}}}$ is true (which will only be for the $Op \in \mathsf{Ops}_{\mathrm{UF}}$ case). Then the argument is similar, except that the unique factorisation is through w, k, in *Ref*, we have a *Ref* step w -(k, Op_{F}, q)-› w', we use the $H^{\sim}$,$Q^{\sim}$,$N^{\sim}$,$D^{\sim}$ retrenchment, and we derive an *Xtra* step $t^{\sim}$ -($h^{\sim}$, Op_{U}, $n^{\sim}$)-› $t^{\sim\prime}$, for which $((H^{\sim\prime} \wedge N^{\sim}{}_{Op}) \vee D^{\sim}{}_{Op})$, and thence $((H^{\sim\prime} \wedge N^{\sim}{}_{Op}) \vee D^{\sim}{}_{Op}) \wedge ((H^{\bullet\prime} \wedge N^{\bullet}{}_{Op}) \vee D^{\bullet}{}_{Op})$ hold. We can rearrange the last of these to yield $(HH^{\circ\prime} \wedge NN^{\circ}{}_{Op}) \vee DD^{\circ}{}_{Op}$, discharging our goal. This completes part (5).

For (6), we work under the additional assumption stated. We start with the refinement data KK°,RR°,VV° given by (9.35)-(9.37).

$$KK^{\circ}(t^{\sim}, t) \equiv HH^{\circ}(t^{\sim}, t) \tag{9.35}$$

$$RR^{\circ}{}_{Op}(h^{\sim}, h) \equiv (\forall\, t^{\sim}, t \bullet HK^{\circ}(t^{\sim}, t) \Rightarrow QQ^{\circ}{}_{Op}(h^{\sim}, h, t^{\sim}, t)) \tag{9.36}$$

$$\begin{aligned} VV^{\circ}{}_{Op}(n^{\sim}, n) \equiv\ & (\exists\, t^{\sim}, t, h^{\sim}, h, t^{\sim\prime}, t' \bullet \\ & NN^{\circ}{}_{Op}(n^{\sim}, n; t^{\sim\prime}, t', h^{\sim}, h, t^{\sim}, t) \vee DD^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t)) \end{aligned} \tag{9.37}$$

To prove the refinement we start with the initialisation PO. This goes just as the analogous PO for the retrenchment HH°,QQ°,NN°,DD° in (5).

For the operation PO we assume $KK^{\circ}(t^{\sim}, t) \wedge RR^{\circ}{}_{Op}(h^{\sim}, h) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', n)$, and must prove there are values $t^{\sim\prime}$, $n^{\sim}$, such that $stp_{Op_{\mathrm{X}}}(t^{\sim}, h^{\sim}, t^{\sim\prime}, n^{\sim})$ and $KK^{\circ\prime} \wedge VV^{\circ}{}_{Op}$ hold. Consider $KK^{\circ} \wedge RR^{\circ}{}_{Op}$. This implies $HH^{\circ} \wedge QQ^{\circ}{}_{Op}$. With $stp_{Op_{\mathrm{U}}}(t, h, t', n)$ we have the hypothesis of the operation PO of the HH°,QQ°,NN°,DD° retrenchment. Therefore we can deduce $(HH^{\circ\prime} \wedge NN^{\circ}{}_{Op}) \vee DD^{\circ}{}_{Op}$. If $HH^{\circ\prime} \wedge NN^{\circ}{}_{Op}$ holds, then so does $KK^{\circ\prime} \wedge VV^{\circ}{}_{Op}$ (since $HH^{\circ\prime} = KK^{\circ\prime}$ and $NN^{\circ}{}_{Op}$ is a disjunct of $VV^{\circ}{}_{Op}$) and we are done. If $HH^{\circ\prime} \wedge NN^{\circ}{}_{Op}$ does not hold, we must have $DD^{\circ}{}_{Op}(t^{\sim\prime}, t', n^{\sim}, n; h^{\sim}, h, t^{\sim}, t)$ instead. In that case, (9.3) allows us to deduce $HH^{\circ}(t^{\sim\prime}, t')$ (which gives $KK^{\circ}(t^{\sim\prime}, t')$), and then we utilise (9.37) to deduce $VV^{\circ}{}_{Op}(n^{\sim}, n)$, and we are done.

For (6).(ii), we note that the condition stated in (9.4) is just the requirement from (3.11), so we are done. This completes part (6).

For (7), it is just a matter of replaying the arguments of (3) using the stronger relationships between *Univ* and *Xtra* afforded by the stronger assumptions in force. We are done. ☺

9.1 Remarks

Remark 9.2 In point (4) of the theorem we used disjunctive fusion composition, as in the Postjoin Theorem, since it is valid without restriction. Again as in the Postjoin Theorem, the corresponding conjunctive composition needs a 'close to cosimulation' criterion to hold.

Remark 9.3 We note the close structural similarity between HH° and $QQ^\circ{}_{Op}$ in (9.31)-(9.32), and HK° and $QR^\circ{}_{Op}$ in (8.24)-(8.25) of the Postjoin Theorem. The tempting alternative, of making $QQ^\circ{}_{Op}$ disjunctive as in (9.24), generates via the distributive law, a plethora of pathological and exceptional cases in the analysis of $HH^\circ \wedge QQ^\circ{}_{Op} \wedge stp_{Op_U}$, since the terms containing $K^\bullet$ say, in each of the contributing HH°, $QQ^\circ{}_{Op}$, stp_{Op_U}, are different — similar observations obviously apply to $H^\bullet$ of course. Hedging against the shortcomings of all of these possibilities is neither elegant, succinct, nor useful, particularly in view of the remarks regarding the Prejoin Theorem made in the next section.

Remark 9.4 As in earlier remarks, the composition of K^*,R^*,V^* with K°,R°,V° need not be the identity; still less the composition of $H^\circ,Q^\circ,N^\circ,D^\circ$ and H^*,Q^*,N^*,D^*.

10 Associativity, General Tower Constructions, and System Engineering

If we reinterpret the 'diagonal factorising' lifting and lowering constructions as square completions in their own right (which, when we view the composition of a refinement and retrenchment round an 'L' shape as a retrenchment, is what results, see Fig. 1), we now have a full set of square completion results available. (Equally, we can view the postjoin and prejoin constructions as 'co-diagonal factorising' constructions, that pull apart the pseudoretrenchment across the co-diagonal, and say that we have a full suite of those too.)

From an applications perspective, of these square completions, two are unquestionably more significant than the others, namely the lifting construction and the postjoin construction. This is because they deal with their constituent retrenchments in a 'forwards' manner — the others, the lowering and prejoin constructions, work, in essence, with converse retrenchments. Using a converse retrenchment during system construction amounts to a form of 'undevelopment', since the retrenchment relationship was purposely designed to be used during development in the forwards direction (regarding this point, see the discussion in Section 4.1 of [Banach, Poppleton et al. (2007)]). As a result of this, we would expect that should the results of this paper be mechanised, the focus would be on the lifting and postjoin constructions, these being the two that would most obviously repay the investment of effort needed to achieve the mechanisation.

One notable aspect of our work is that everything has been reduced to the composition of (collections of) relations. Composing relations is associative, so we can expect that our constructions themselves will compose associatively — up to the appro-

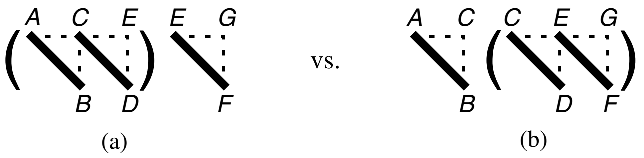


Fig. 7. Different association orders for the lifting construction.

priate notion of equivalence, that is. Let us illustrate this on a specific construction. Consider the lifting construction of Fig. 3. The state and I/O spaces of this construction are just cartesian products made from the abstract and concrete constituent spaces. Likewise, the transitions in (6.3) are made out of pairs of abstract and concrete constituent transitions. Consider Fig. 7, which illustrates applying the construction using two different association orders, and focus on Fig. 7.(a). This shows the leftmost A-to-B retrenchment lifted to C, this then being followed by the middle lifting, which lifts the C-to-D retrenchment to E. System E gives the result of the parenthesised liftings in Fig. 7.(a). The construction can be repeated to include the third piece of Fig. 7.(a), finally giving system G. A little thought shows that the state and I/O spaces of the result will be the cartesian products of the constituents, bracketed leftmost-innermost. Similar remarks apply to the core part of the transition relation, which will contain all the step relations from all the constituent systems, their logical definitions bracketed in an analogous leftmost-innermost way.

Now focus on Fig. 7.(b). Inside the parentheses we have a combined lifting, as above, consisting of the lifting of the C-to-D retrenchment to E, followed by the lifting of the E-to-F retrenchment to give G. System G coincides with the system constructed by lifting the A-to-B retrenchment to give C, and identifying C with the starting system of the parenthesised lifting just described. Thus, when the leftmost lifting is combined with the retrenchment constructed in the parentheses, we get another result for the overall construction. However, a moment's thought shows that this turns out to be the same as the previous case, but bracketed rightmost-innermost, for both the state and I/O spaces and the core part of the transition relation. These rebracketings amount to set theoretic isomorphism, a much stronger notion of equivalence than either inter-refinability, or the even weaker equivalence notions we encountered above. Similar remarks apply to the other constructions, to vertical as well as horizontal association, and to combinations of constructions of various kinds. The reader will appreciate that an exhaustive treatment of all the cases would be exhausting.

The good behaviour just noted allows us to envision a system development process built out of refinements and retrenchments, aided by the constructions made available to us in this paper: 'system development via theorem'. Fig. 8 shows a schematic example. The development starts at the top left corner with the most abstract model. Two refinement stages follow, after which more detailed requirement considerations necessitate a sideways jump, via a retrenchment, onto a more low level refinement strand. The square completion constructions, here lifting, permit the new low level detail to be exhibited at a level of abstraction comparable with the initial model. This might be needed, for example, for checking abstract formulations of the requirements properties that the low level system model modifications described by the retrench-

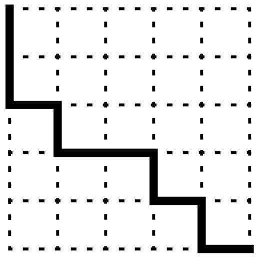
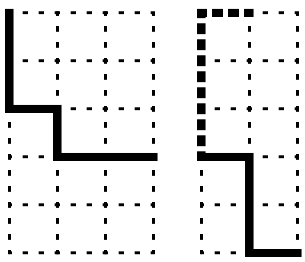


Fig. 8. A schematic development path consisting of refinements and retrenchments.

ment were intended to address. There follows another refinement stage. Then another retrenchment stage; then another retrenchment stage, the two separate retrenchments permitting piecemeal validation of the issues they were introduced into the process to address. In the same manner, the process reaches its end with a further refinement, retrenchment, refinement, and a last retrenchment.

Now suppose that the user environment changes, and the previously developed system is no longer adequate. Suppose that it has been identified that the requirements addressed up to the end of the third retrenchment still hold good, but that the remainder of the development needs to be modified. Fig. 9 shows what might happen next. The retained part of the original development is in Fig. 9.(a). Its right vertical side, a refinement path from most abstract level down to where the thick development path reaches the edge, gives the interface from the retained part of the original development to the new activity. This, reproduced as the heavy dashed vertical line in Fig. 9.(b), is the starting point for the new development.

Suppose that the new requirements have been described at the most abstract level. Then there will be a retrenchment, shown by the heavy dashed horizontal line in Fig. 9.(b), from the starting abstract model to a modified abstract model. Assuming the



(a) (b)

Fig. 9. A schematic system revision path.

three earlier refinements have been composed into one with the help of our square completion results (giving the heavy dashed vertical line in Fig. 9.(b)), an application of the postjoin construction then embeds the new requirements into the current development level. The development can subsequently complete via two further stages of refinement and a final retrenchment.

11 Conclusions

In the preceding sections, having introduced retrenchment and some context of its applications (including applications of the theory treated in detail in this paper), we motivated the need for square completion constructions in the context of retrenchment and refinement interworking, and then we formulated and proved the theorems relating to the four relevant completions. These were designed with simplicity and composability in mind, drawing extensively, and with the experience of hindsight, on the theorems reported in [Jeske (2005)] — a number of accompanying remarks to our four main theorems indicated that small variations on the results given are perfectly feasible. We outlined how such constructions could be used in a large scale formal development process to endow the process with greater flexibility in dealing with requirements issues than is afforded by refinement alone.

In all of this, we pursued a resolutely (1, 1) operation correspondence strategy. That is to say a single abstract step always corresponded to a single concrete step. But this is too restrictive for many practical applications. A 'quick fix' entails treating paths through the transition system as the individual steps of an associated system. The simple way that we have formulated our systems and our relationships between systems guarantees that this approach will go through unproblematically, given the usual care and attention to 'plumbing' considerations. Of course, more detailed treatments of such 'coarse-grained vs. fine-grained' formulations can uncover issues going beyond simple path-oriented reuse of the (1, 1) results. Such issues remain as work for the future, and will be addressed in appropriate publications.

In the period since [Jeske (2005)], the importance of results of this kind has only grown. Being able to place the retrenchment steps of some development, inside a development methodology that cleanly separates them from the more conventional refinement steps adds great clarity to the development process, distinguishing those steps with the potential to preserve system properties in a strong manner, from those steps where this capacity is curtailed. Experience has shown that in the vast majority of practical cases, the integration of retrenchment and refinement could be done by hand relatively straightforwardly (some of these were reviewed in Section 2), so one view of the challenge tackled in this paper is to see it as the desire to find an abstract formulation of the integration phenomenon that reflected the simplicity observed in practice. Given the experience of [Jeske (2005)] this was not a trivial undertaking, but one that has, we believe, been accomplished successfully in this paper.

References

Badeau F., Amelot A. (2005); Using B as a High Level Programming Language in an Industrial Project: Riossy VAL. *in*: Proc. ZB-05, Treharne, King, Henson, Schneider (eds.), LNCS **3455**, 334-354.

Banach R. (2009); Model Based Refinement and the Design of Retrenchments. *Submitted.*

Banach R. (2011); Retrenchment for Event-B: UseCase-wise Development and Rodin Integration. Form. Asp. Comp., **23**, 113-131.

Banach R., Jeske C. (2010); Stronger Compositions for Retrenchments. J. Log. Alg. Prog. **79**, 215-232.

Banach R., Jeske C., Poppleton M., Stepney S. (2006a); Retrenching the Purse: Finite Exception Logs, and Validating the Small. *in*: Hinchey (ed.), Proc. IEEE/NASA SEW30-06, 234-245.

Banach R., Jeske C., Poppleton M., Stepney S. (2006b); Retrenching the Purse: Hashing Injective CLEAR Codes, and Security Properties. *in*: Margaria, Steffen (eds.), Proc. IEEE ISOLA-06, 82-90.

Banach R., Jeske C., Poppleton M., Stepney S. (2007); Retrenching the Purse: The Balance Enquiry Quandary, and Generalised and (1,1) Forward Refinements. Fund. Inf., **77**, 29-69.

Banach R., Jeske C., Poppleton M. (2008); Composition Mechanisms for Retrenchment. J. Log. Alg. Prog. **75**, 209-229.

Banach R., Poppleton M., Jeske C., Stepney S. (2005); Retrenching the Purse: Finite Sequence Numbers, and the Tower Pattern. *in*: Proc. FM-05, Fitzgerald, Hayes, Tarlecki (eds.), LNCS **3582**, 382-398, Springer.

Banach R., Poppleton M., Jeske C., Stepney S. (2007); Engineering and Theoretical Underpinnings of Retrenchment. Sci. Comp. Prog. **67**, 301-329.

Banach R., Schellhorn G. (2010); Atomic Actions and their Refinements to Isolated Protocols. Form. Asp. Comp., **22**, 33-61.

Banach R., Zhu H., Su W., Huang R. (2012); Continuous KAOS, ASM, and Formal Control System Design Across the Continuous/Discrete Modeling Interface: A Simple Train Stopping Application. Form. Asp. Comp., *to appear.*

Behm P., Benoit P., Faivre A., Meynadier J-M. (1999); A Successful Application of B in a Large Project. *in*: Proc. FM-99 Vol I, Wing, Woodcock (eds.), LNCS **1708**, 369-387.

Behm P., Desforges P., Meynadier J-M. (2000); MÉTÉOR: An Industrial Success in Formal Development. *in*: Proc. ZB-00, Bowen, Dunne, Galloway, King (eds.), LNCS **1878**, 374-393.

de Roever W-P., Engelhardt K. (1998); Data Refinement: Model-Oriented Proof Methods and their Comparison. Cambridge University Press.

Dijkstra E. W. (1972); Notes on Structured Programming. *in*: Structured Programming, Academic Press.

Hoare C. A. R. (1972); Proof of Correctness of Data representations. Acta Inf. **1**, 271-281.

Jeffords R., Heitmeyer C., Archer M., Leonard E. (2009); A Formal Method for Developing Provably Correct Fault-Tolerant Systems Using Partial Refinement and Composition. *in*: Proc. FM-09, Cavalcanti, Dams (eds.), LNCS **5850**, 173-189, Springer.

Jeske C. (2005); Algebraic Theory of Retrenchment and Refinement. PhD. Thesis Manchester University Department of Computer Science.

Jones C., Woodcock J. (eds.) (2008); Special Issue on theMondex Verification. Formal Aspects of Computing, **20**, 1-139.

Jones C., O'Hearne P., Woodcock J. (2006); Verified Software: A Grand Challenge. IEEE Computer, **39**, 93-95.

Project Advance; `http://www.project-advance.eu`

Retrenchment Homepage; `http://www.cs.man.ac.uk/retrenchment`

Rodin; The Rodin Project. `http://rodin.cs.ncl.ac.uk`

Stepney S., Cooper D., Woodcock J. (1998); More Powerful Z Data Refinement: Pushing the State of the Art in Industrial Refinement. *in*: Proc. ZUM-98, Bowen, Fett, Hinchey (eds.), LNCS **1493**, 284-307, Springer.

Stepney S., Cooper D., Woodcock J. (2000); An Electronic Purse: Specification, Refinement and Proof. Oxford University Computing Laboratory Tech. Report PRG-126.

Wirth N. (1971); The Development of Programs by Stepwise Refinement. Comm. ACM **14**, 221-227.

Woodcock J. (2006); First Steps in the The Verified Software Grand Challenge. IEEE Computer, **39**(10):57-64.

Woodcock J., Banach R. (2007); The Verification Grand Challenge. JUCS, **13**, 661-668.