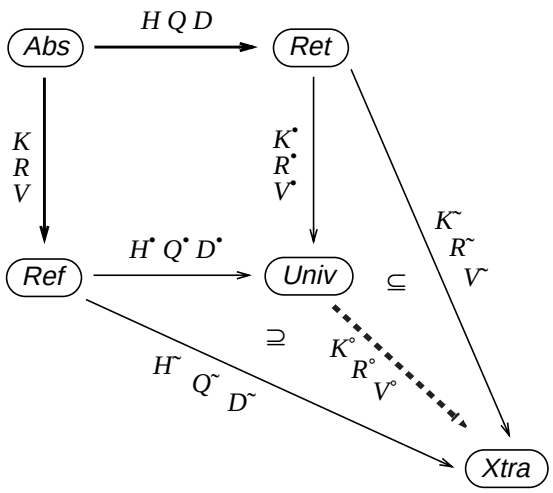
# Reconciling Retrenchments and Refinements I: Proofs

This document presents the proofs for the construction presented in Section 5 of *Reconciling Retrenchments and Refinements I*. Note that the equation numbers do not correspond to those used in the paper.

## The Reconciliation

**Theorem 1.1.** Let there be a retrenchment from *Abs* to *Ret*, and a refinement from *Abs* to *Ref*, as shown in Figure 1.1. Then the following hold.




All arrows labelled *H*, *Q*, *D* are retrenchments,
all arrows labelled *K*, *R*, *V* are refinements.

Figure 1.1:

(1) There is a universal system *Univ* such that there is a retrenchment from *Ref* to *Univ* and an I/O-filtered refinement from *Ret* to *Univ* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Abs* to *Univ*, and which satisfies (U1) to (U10) below.

(2) Whenever there is a system *Xtra* and a retrenchment from *Ref* to *Xtra* and an I/O-filtered refinement from *Ret* to *Xtra* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Abs* to *Xtra*, and which satisfies (X1) to (X10) below, then there is an I/O-filtered refinement from *Univ* to *Xtra* such that $H^{\bullet};K^{\circ} \Rightarrow H^{\sim}$, $(H^{\bullet} \wedge Q^{\bullet});(K^{\circ} \wedge R^{\circ}) \Rightarrow (H^{\sim} \wedge Q^{\sim})$, $(H^{\bullet} \wedge Q^{\bullet} \wedge D^{\bullet});(K^{\circ\prime} \wedge V^{\circ} \wedge R^{\circ} \wedge K^{\circ}) \Rightarrow (H^{\sim} \wedge Q^{\sim} \wedge D^{\sim})$, and such that $K^{\bullet};K^{\circ} \Rightarrow K^{\sim}$, $R^{\bullet};R^{\circ} \Rightarrow R^{\sim}$, $V^{\bullet};V^{\circ} \Rightarrow V^{\sim}$.

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

In what follows we will take the retrenchment from *Abs* to *Ret* and the refinement from *Abs* to *Ref*, and build a new, universal, system *Univ*, to which there is *both* a retrenchment from *Ret* and a refinement from *Ref*. See Figure 1.1. First let

$$HD(u, v) = H(u, v) \vee \bigvee_{Op} (\exists \underline{\underline{o}}, \underline{\underline{p}}, \underline{i}, \underline{j}, \underline{\underline{u}}, \underline{\underline{v}} \bullet D_{Op}(u, v, \underline{\underline{o}}, \underline{\underline{p}}; \underline{i}, \underline{j}, \underline{\underline{u}}, \underline{\underline{v}})) \tag{1.1}$$

$$QI_{Op}(i, j) = (\exists \underline{\underline{u}}, \underline{\underline{v}} \bullet Q_{Op}(i, j, \underline{\underline{u}}, \underline{\underline{v}})) \tag{1.2}$$

$$DO_{Op}(o, p) = (\exists \underline{\underline{u}}', \underline{\underline{v}}', \bullet D_{Op}(\underline{\underline{u}}', \underline{\underline{v}}', o, p; \underline{i}, \underline{j}, \underline{\underline{u}}, \underline{\underline{v}})) \tag{1.3}$$

Given these, we now introduce the following equivalence relations.

$$\sim_{V} = ((K^{T};HD)^{T};(K^{T};HD))^{*} \tag{1.4}$$

$$\sim_{W} = ((HD^{T};K)^{T};(HD^{T};K))^{*} \tag{1.5}$$

$$\sim_{J_{Op}} = ((R_{Op}^{T};QI_{Op})^{T};(R_{Op}^{T};QI_{Op}))^{*} \tag{1.6}$$

$$\sim_{K_{Op}} = ((QI_{Op}^{T};R_{Op})^{T};(QI_{Op}^{T};R_{Op}))^{*} \tag{1.7}$$

$$\sim_{P_{Op}} = ((V_{Op}^{T};DO_{Op})^{T};(V_{Op}^{T};DO_{Op}))^{*} \tag{1.8}$$

$$\sim_{Q_{Op}} = ((DO_{Op}^{T};V_{Op})^{T};(DO_{Op}^{T};V_{Op}))^{*} \tag{1.9}$$

The operation names set of *Univ* is $\mathsf{Ops}_U$ with elements $Op_U$. The state space is $\mathsf{T}$ with elements $t$, inputs are $h \in \mathsf{H}$, outputs $s \in \mathsf{S}$. These are all constructed from the systems *Ret* and *Ref* as follows. Firstly $\mathsf{Ops}_U = \mathsf{Ops}_T = \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$. So each $Op_U$ is either an $Op_A$ or an $Op_U \in (\mathsf{Ops}_U - \mathsf{Ops}_A)$. Next $\mathsf{T} = \mathsf{V}/\sim_V \times \mathsf{W}/\sim_W$. For $Op_U \in \mathsf{Ops}_A$ the input and output spaces are $\mathsf{H}_{Op} = \mathsf{J}_{Op}/\sim_{J_{Op}} \times \mathsf{K}_{Op}/\sim_{K_{Op}}$ and $\mathsf{S}_{Op} = \mathsf{P}_{Op}/\sim_{P_{Op}} \times \mathsf{Q}_{Op}/\sim_{Q_{Op}}$, while for $Op_U \notin \mathsf{Ops}_A$, $\mathsf{H}_{Op} = \mathsf{J}_{Op}$ and $\mathsf{S}_{Op} = \mathsf{P}_{Op}$.

Now for some more definitions.

$$KH(\underline{w}, [v]) = (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \tag{1.10}$$

$$HK([v], [w]) = (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))) \tag{1.11}$$

$$KD_{Op}(\underline{w}, [v]) = (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge (\exists\, \underline{o}, \underline{p}, \underline{i}, \underline{j}, \underline{u}, \underline{v} \bullet D_{Op}(u, \underline{v}, \underline{o}, \underline{p}; \underline{i}, \underline{j}, \underline{u}, \underline{v})))) \tag{1.12}$$

$$DK_{Op}([v], [w]) = (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge (\exists\, \underline{o}, \underline{p}, \underline{i}, \underline{j}, \underline{u}, \underline{v} \bullet D_{Op}(u, \underline{v}, \underline{o}, \underline{p}; \underline{i}, \underline{j}, \underline{u}, \underline{v})) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KD_{Op}(\underline{w}, [v]))) \tag{1.13}$$

$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) = (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))) \tag{1.14}$$

$$QR_{Op}([j], [k]) = (\forall\, i, u, \underline{j}, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))) \tag{1.15}$$

$$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) = (\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) \tag{1.16}$$

$$DV_{Op}([p], [q]) = (\forall\, u', o, i, u, \underline{v}', \underline{p}, \underline{j}, \underline{v}, v', w', j, k, v, w \bullet \underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$

$$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))) \quad (1.17)$$

We can now define the component relations for the refinement from *Abs* to *Ref* and the retrenchment from *Abs* to *Ret*; see Figure 1.1 again.

$$K^\bullet(\underline{v}, ([v], [w])) = \underline{v} \in [v] \wedge HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \quad (1.18)$$

$$H^\bullet(\underline{w}, ([v], [w])) = \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge$$
$$HK([v], [w]) \wedge \bigwedge_{Op} DK_{Op}([v], [w]) \quad (1.19)$$

$$R^\bullet{}_{Op}(\underline{j}, ([j], [k])) = \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \quad (1.20)$$

$$Q^\bullet{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) =$$
$$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$$
$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \quad (1.21)$$

$$V^\bullet{}_{Op}(\underline{p}, ([p], [q])) = \underline{p} \in [p] \wedge DV_{Op}([p], [q]) \quad (1.22)$$

$$D^\bullet{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])) =$$
$$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$$
$$(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$$
$$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge DV_{Op}([p], [q]) \wedge$$
$$HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \quad (1.23)$$

In the above, *Op* ranges over $\mathsf{Ops}_A$. For operations not in $\mathsf{Ops}_A$, we define $R^\bullet{}_{Op}$ and $V^\bullet{}_{Op}$ as identities on inputs and outputs respectively.

With these definitions Figure 1.1 commutes in the following sense. Firstly,

$$H(u, \underline{v});K^\bullet(\underline{v}, ([v], [w])) = K(u, \underline{w});H^\bullet(\underline{w}, ([v], [w])) = G(u, ([v], [w])) \,. \quad (1.24)$$

We write this for short as

$$H;K^\bullet \equiv K;H^\bullet \equiv G \quad (1.25)$$

Secondly,

$$(H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})); (K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])))) =$$
$$(K(u, \underline{w}) \wedge R_{Op}(i, \underline{k})); (H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])))\ , \qquad (1.26)$$

or more briefly

$$(H \wedge Q_{Op}); (K^{\bullet} \wedge R^{\bullet}{}_{Op}) \equiv (K \wedge R_{Op}); (H^{\bullet} \wedge Q^{\bullet}{}_{Op}) \equiv P_{Op}\ . \qquad (1.27)$$

Thirdly,

$$\begin{aligned}
&(H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})); \\
&\quad (K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}{}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])))) \\
&= \\
&(K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})); \\
&\quad (H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge \\
&\qquad D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w])))\ , \qquad (1.28)
\end{aligned}$$

or

$$\begin{aligned}
&(H \wedge Q_{Op} \wedge D_{Op}); (K^{\bullet\prime} \wedge V^{\bullet}{}_{Op} \wedge R^{\bullet}{}_{Op} \wedge K^{\bullet}) \equiv \\
&\quad (K' \wedge V_{Op} \wedge R_{Op} \wedge K); (H^{\bullet} \wedge Q^{\bullet}{}_{Op} \wedge D^{\bullet}{}_{Op}) \equiv C_{Op}\ . \qquad (1.29)
\end{aligned}$$

To simplify the proofs in this chapter, we will always assume our systems only have one operation *Op*.

To prove the above compositions, we will make use of the following lemmas.

**Lemma 1.2.**

$$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge HK([v], [w]) \ \Rightarrow\ (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))$$

*Proof.*

$$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge HK([v], [w])$$

$=$ [definition of *HK*, (1.11)]

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

$=$ [meaning of $\forall$, idempotency]

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge$

$\quad (\underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))) \wedge$

$\quad (\forall\, u, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v])))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{v} \in [v] \wedge H(u, \underline{v}) \wedge (\underline{v} \in [v] \wedge H(u, \underline{v}) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v])))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))$ c

**Lemma 1.3.** $K(u, \underline{w}) \wedge KH(\underline{w}, [v]) \;\Rightarrow\; (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$

*Proof.*

$K(u, \underline{w}) \wedge KH(\underline{w}, [v])$

$=$ [definition of $KH$, (1.10)]

$K(u, \underline{w}) \wedge (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$=$ [meaning of $\forall$, idempotency]

$K(u, \underline{w}) \wedge (K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))) \wedge$

$\quad (\forall\, u \bullet K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$K(u, \underline{w}) \wedge (K(u, \underline{w}) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})))$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$(\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$ □

**Lemma 1.4.**

$\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge QR_{Op}([j], [k]) \Rightarrow$
$\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$

*Proof.*

$\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge QR_{Op}([j], [k])$

$=$ [definition of $QR$, (1.15)]

$\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$

$$(\forall\ i, u, \underline{j}, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$

$$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\big)$$

$=$ [meaning of $\forall$, idempotency]

$$\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$

$$\big(\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$

$$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\big) \wedge$$

$$\big(\forall\ i, u, \underline{j}, \underline{v}, v, w \bullet \underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$

$$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\big)$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$

$$\big(\underline{j} \in [j] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$

$$(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\big)$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$\big(\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])\big)$$ □

**Lemma 1.5.** $R_{Op}(i, \underline{k}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \Rightarrow KH(\underline{w}, [v])$

*Proof.*

$$R_{Op}(i, \underline{k}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$$

$=$ [definition of $RQ$, (1.14)]

$$R_{Op}(i, \underline{k}) \wedge \big(\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\ \big)$$

$=$ [$\big(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\big) \Rightarrow \big(\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})\big)$]

$$R_{Op}(i, \underline{k}) \wedge (\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\ \big(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\big) \wedge$$

$$\big(\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v})\big)\ )\ )$$

$=$ [meaning of $\forall$, $a \Rightarrow (b \wedge c) \equiv (a \Rightarrow b) \wedge (a \Rightarrow c)$]

$$R_{Op}(i, \underline{k}) \wedge \big(\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \big) \wedge$$

$$\mathbf{(}\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$R_{Op}(i, \underline{k}) \wedge \mathbf{(}\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, idempotency]

$$R_{Op}(i, \underline{k}) \wedge \mathbf{(}\ \forall\ u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)} \wedge$$

$$\mathbf{(}\ \forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow a$]

$$R_{Op}(i, \underline{k}) \wedge \mathbf{(}\ \forall\ u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [meaning of $\forall$, idempotency, $a \wedge (a \wedge b \Rightarrow c) \equiv a \wedge (b \Rightarrow c)$]

$$R_{Op}(i, \underline{k}) \wedge \mathbf{(}\ \forall\ u \bullet K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$$\mathbf{(}\ \forall\ u \bullet K(u, \underline{w}) \Rightarrow (\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))\ \mathbf{)}$$

$\Rightarrow$ [(1.10)]

$KH(\underline{v}, [w])$ □

**Lemma 1.6.**

$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \Rightarrow$$
$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$$

*Proof.*

$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$$

= [definition of $RQ$, (1.14)]

$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$\mathbf{(}\forall\ i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\ \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\mathbf{)}$$

= [meaning of $\forall$, idempotency]

$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$(R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))) \wedge$$

$$(\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})))$$

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$$R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$$

$$(R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})))$$

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))$$ □

**Lemma 1.7.**

$$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge DV_{Op}([p], [q]) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$$

*Proof.*

$$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge DV_{Op}([p], [q])$$

$=$ [definition of *DV*, (1.17)]

$$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$
$$(\forall\, u', o, i, u, \underline{v}', \underline{p}, \underline{j}, \underline{v}, v', w', j, k, v, w \bullet$$
$$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$
$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$
$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$$

$=$ [meaning of $\forall$, idempotency]

$$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$

$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \wedge$

**(** $\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \Rightarrow$

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$ **)** $\wedge$

**(** $\forall\, u', o, i, u, \underline{v}', \underline{p}, \underline{j}, \underline{v}, v', w', j, k, v, w \bullet$

$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \Rightarrow$

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$ **)**

$\Rightarrow$ [$a \wedge b \wedge c \Rightarrow a \wedge b$]

$\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \wedge$

**(** $\underline{p} \in [p] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K^\bullet(\underline{v}', ([v'], [w'])) \wedge R^\bullet{}_{Op}(\underline{j}, ([j], [k])) \wedge K^\bullet(\underline{v}, ([v], [w])) \Rightarrow$

$(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]))$ **)**

$\Rightarrow$ [$(a \wedge (a \Rightarrow b)) \Rightarrow b$]

**(** $\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$

$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$ **)** □

**Lemma 1.8.**

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \Rightarrow RQ_{Op}(\underline{k}, \underline{w}, [j], [v])$

*Proof.*

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$

= [definition of *VD*, (1.16)]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})) )$$

$$= [(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H \wedge Q \wedge D) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H \wedge Q)]$$

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$( (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})) \wedge$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) ) )$$

$$= [\text{meaning of } \forall,\ a \Rightarrow (b \wedge c) \equiv (a \Rightarrow b) \wedge (a \Rightarrow c)]$$

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$

$$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})) ) \wedge$$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) )$$

$$\Rightarrow [a \wedge b \wedge c \Rightarrow a \wedge c]$$

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) )$$

$$\Rightarrow [\text{meaning of } \forall,\ \text{idempotency}]$$

$$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$$

$$( \forall\, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) ) \wedge$$

$$( \forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$$

$$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})) )$$

$$\Rightarrow [a \wedge b \wedge c \Rightarrow a \wedge b]$$

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge$

$\quad (\forall\, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\ )$

$\Rightarrow$ [meaning of $\forall$, idempotency, $a \wedge (a \wedge b \Rightarrow c) \equiv a \wedge (b \Rightarrow c)$]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge (\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\ )$

$\Rightarrow$ [$a \wedge b \Rightarrow b$]

$(\forall\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\ )$

$\Rightarrow$ [(1.14)]

$RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$ □

**Lemma 1.9.**

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \Rightarrow$
$\quad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$
$\quad\quad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))$

*Proof.*

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])$

= [definition of *VD*, (1.16)]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$\quad\quad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ )$

= [meaning of $\forall$, idempotency]

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\quad (\forall\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$\quad\quad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ ) \wedge$

$$
\begin{array}{l}
\quad \mathbf{(}\ K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\
\qquad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
\qquad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ \mathbf{)} \\
\Rightarrow [a \wedge b \wedge c \Rightarrow a \wedge c] \\
K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \\
\quad \mathbf{(}\ K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow \\
\qquad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
\qquad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))\ \mathbf{)} \\
\Rightarrow [(a \wedge (a \Rightarrow b)) \Rightarrow b] \\
\mathbf{(}\ \exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \\
\qquad H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})\ \mathbf{)} \qquad \square
\end{array}
$$

We now prove the compositions. Take (1.24). We expand each part in turn. Take $H;K^{\bullet}$ first.

$$
\begin{array}{l}
\quad H(u, \underline{v});K^{\bullet}(\underline{v}, ([v], [w])) \\
= [\text{definition of composition}] \\
\mathbf{(}\ \exists\, \underline{v} \bullet H(u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\ \mathbf{)} \\
= [\text{definition of } K^{\bullet}, (1.18)] \\
\mathbf{(}\ \exists\, \underline{v} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])\ \mathbf{)} \\
= [\text{Lemma 1.2}] \\
\mathbf{(}\ \exists\, \underline{v} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \\
\qquad (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))\ \mathbf{)} \\
= [\text{rewriting in prenex normal form}] \\
\mathbf{(}\ \exists\, \underline{v}, \underline{w} \bullet H(u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \\
\qquad \underline{w} \in [w] \wedge K(u, \underline{w}) \wedge KH(\underline{w}, [v]))\ \mathbf{)} \\
= [\text{rearranging}] \\
\mathbf{(}\ \exists\, \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge K(u, \underline{w}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge
\end{array}
$$

$KH(\underline{w}, [v])$ **)** .

Now for $K;H^{\bullet}$.

$K(u, \underline{w});H^{\bullet}(\underline{w}, ([v], [w]))$

= [definition of composition]

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

= [definition of $H^{\bullet}$, (1.19)]

**(** $\exists\ \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge (\exists\ u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge$

$DK_{Op}([v], [w])$ **)**

= [$K(u, \underline{w}) \Rightarrow (\exists\ u \bullet K(u, \underline{w}))$]

**(** $\exists\ \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$ **)**

= [Lemma 1.3]

**(** $\exists\ \underline{w} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$(\exists\ \underline{v} \bullet \underline{v} \in [v] \wedge H(u, \underline{v}))$ **)**

= [rewriting in prenex normal form]

**(** $\exists\ \underline{w}, \underline{v} \bullet K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{v} \in [v] \wedge H(u, \underline{v})$ **)**

= [rearranging]

**(** $\exists\ \underline{v}, \underline{w} \bullet \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge K(u, \underline{w}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w])$

$\wedge\ KH(\underline{w}, [v])$**)**

Hence $K^{\bullet};H \equiv H^{\bullet};K$ holds.

(1.26) is next. Consider $(H \wedge Q_{Op});(K^{\bullet} \wedge R^{\bullet}{}_{Op})$.

**(**$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})$**);(**$K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k]))$**)**

= [definition of composition]

**(** $\exists\ \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k]))$ **)**

= [definition of $R^{\bullet}{}_{Op}$, (1.20)]

$(\exists\, \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]))$

= [Lemma 1.4]

$(\exists\, \underline{v}, \underline{j} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge$
$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))\,)$

= [rewriting in prenex normal form]

$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge$
$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$

= [definition of $K^{\bullet}$, (1.18)]

$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$
$\underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$
$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]))$

= [Lemma 1.5]

$(\exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$
$\underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$
$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v]))$

= [rearranging]

$(\exists\, \underline{j}, \underline{k}, \underline{v}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{k} \in [k] \wedge \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge$
$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge QR_{Op}([j], [k]) \wedge$
$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v]))$

Next, we expand $(K \wedge R_{Op});(H^{\bullet} \wedge Q^{\bullet}{}_{Op})$.

$(K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}));(H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])))$

= [definition of composition]

$(\exists\, \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])))$

= [definition of $Q^{\bullet}$ (1.21)]

$(\exists\, \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$
$(\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]))$

$= [K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \Rightarrow (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}))]$

$\mathbf{(}\ \exists\, \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k])\ \mathbf{)}$

$=$ [Lemma 1.6]

$\mathbf{(}\ \exists\, \underline{w}, \underline{k} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge$

$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}))\ \mathbf{)}$

$=$ [rewriting in prenex normal form]

$\mathbf{(}\ \exists\, \underline{w}, \underline{k}, \underline{j}, \underline{v} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge H^{\bullet}(\underline{w}, ([v], [w])) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\ \mathbf{)}$

$=$ [definition of $H^{\bullet}$ (1.19)]

$\mathbf{(}\ \exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge \underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge$

$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\ \mathbf{)}$

$=$ [$K(u, \underline{w}) \Rightarrow (\exists\, u \bullet K(u, \underline{w}))$]

$\mathbf{(}\ \exists\, \underline{v}, \underline{j}, \underline{k}, \underline{w} \bullet K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge$

$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v})\ \mathbf{)}$

[rearranging, idempotency]

$\mathbf{(}\ \exists\, \underline{j}, \underline{k}, \underline{v}, \underline{w} \bullet \underline{j} \in [j] \wedge \underline{k} \in [k] \wedge \underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge$

$K(u, \underline{w}) \wedge R_{Op}(i, \underline{k}) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge QR_{Op}([j], [k]) \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])\ \mathbf{)}$

Hence $(H \wedge Q_{Op});(K^{\bullet} \wedge R^{\bullet}{}_{Op}) = (K \wedge R_{Op});(H^{\bullet} \wedge Q^{\bullet}{}_{Op})$.

Last, we prove (1.28). Consider $(H \wedge Q_{Op} \wedge D_{Op});(K^{\bullet\prime} \wedge V^{\bullet}{}_{Op} \wedge R^{\bullet}{}_{Op} \wedge K^{\bullet})$ first.

$\mathbf{(}\ H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})\ \mathbf{)}$;

$\mathbf{(}\ K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}{}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\ \mathbf{)}$

= [definition of composition]

$$\mathbf{(}\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$$

$$V^{\bullet}{}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\ \mathbf{)}$$

= [definition of $V^{\bullet}{}_{Op}$, (1.12)]

$$\mathbf{(}\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$$

$$\underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))\ \mathbf{)}$$

= [Lemma 1.7]

$$(\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge$$

$$\underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w])) \wedge$$

$$\mathbf{(}\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])\mathbf{)}\ )$$

= [rewriting in prenex normal form]

$$(\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$

$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$

$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v])\ )$$

= [Lemma 1.8]

$$(\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$

$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$

$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge$$

$$RQ_{Op}(\underline{k}, \underline{w}, [j], [v])\ )$$

= [Lemma 1.5]

$$(\ \exists\ \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$$

$$K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge \underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge R^{\bullet}{}_{Op}(\underline{j}, ([j], [k])) \wedge$$

$$K^{\bullet}(\underline{v}, ([v], [w])) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge$$

$$V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge$$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ )

= [definition of $K^{\bullet}$, $K^{\bullet\prime}$ and $R^{\bullet}$ ((1.18) and (1.20))]

**(** $\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$\underline{v}' \in [v'] \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge \underline{p} \in [p] \wedge DV_{Op}([p], [q]) \wedge$

$\underline{j} \in [j] \wedge QR_{Op}([j], [k]) \wedge \underline{v} \in [v] \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge$

$K(u, \underline{w}) \wedge VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

= [rearranging]

**(** $\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$DV_{Op}([p], [q]) \wedge QR_{Op}([j], [k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

Finally, we expand $(K' \wedge V_{Op} \wedge R_{Op} \wedge K);(H^{\bullet} \wedge Q^{\bullet}{}_{Op} \wedge D^{\bullet}{}_{Op})$.

**(**$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})$**)**;

**(**$H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge$

$D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$**)**

= [definition of composition]

**(**$\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}{}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \wedge$

$D^{\bullet}{}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$**)**

= [definition of $H^{\bullet}$, $Q^{\bullet}$ and $D^{\bullet}$ ((1.19), (1.21) and (1.23))]

**(** $\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge$

$\underline{w} \in [w] \wedge (\exists\, u \bullet K(u, \underline{w})) \wedge KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge$

$\underline{w} \in [w] \wedge (\exists\, i, u \bullet R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge$

$\underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$(\exists\, u', o, i, u \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w})) \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w'])$ **)**

= [$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \Rightarrow$ **(** $(\exists\, u', o, i, u \bullet K' \wedge V \wedge R \wedge K) \wedge (\exists\, i, u \bullet R \wedge K) \wedge (\exists\, u \bullet K)$ **)**]

**(** $\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge$

$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w'])$ **)**

= [Lemma 1.9]

**(** $\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge KH(\underline{w}, [v]) \wedge$

$HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge$

$QR_{Op}([j], [k]) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge DV_{Op}([p], [q]) \wedge$

$HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

( $\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ ) **)**

= [rewriting in prenex normal form]

**(** $\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w}, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge \underline{w} \in [w] \wedge$

$KH(\underline{w}, [v]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge QR_{Op}([j], [k]) \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge DV_{Op}([p], [q]) \wedge HK([v'], [w']) \wedge$

$DK_{Op}([v'], [w']) \wedge \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

$H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ **)**

[rearranging, idempotency]

**(** $\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \wedge$

$K(u', \underline{w}') \wedge V_{Op}(o, \underline{q}) \wedge R_{Op}(i, \underline{k}) \wedge K(u, \underline{w}) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

$DV_{Op}([p], [q]) \wedge QR_{Op}([j], [k]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$VD_{Op}(\underline{w}', \underline{q}, \underline{k}, \underline{w}, [v'], [p], [j], [v]) \wedge RQ_{Op}(\underline{k}, \underline{w}, [j], [v]) \wedge KH(\underline{w}, [v])$ **)**

Hence $(H \wedge Q \wedge D);(K^{\bullet\prime} \wedge V^{\bullet} \wedge R^{\bullet} \wedge K^{\bullet}) = (K' \wedge V \wedge R \wedge K);(H^{\bullet} \wedge Q^{\bullet} \wedge D^{\bullet})$.

Now we give the transitions of *Univ*. The operation names set $\mathsf{Ops}_U$ decomposes as $\mathsf{Ops}_U = \mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$. There are therefore two possibilities. For $Op_U \in (\mathsf{Ops}_U - \mathsf{Ops}_A)$ we have a transition $t$ -$(h, Op_U, s)$-› $t'$ or, more explicitly, $([v], [w])$ -$(\underline{j}, Op_U, \underline{p})$-› $([v'], [w'])$, iff $[v], [w], \underline{j}, \underline{p}, [v'], [w']$ satisfy

$$\textbf{(}\ \forall\ \underline{v} \bullet \underline{v} \in [v] \Rightarrow (\ \exists\ \underline{v}' \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K^{\bullet}(\underline{v}', ([v'], [w']))\ )\ \textbf{)}\ . \tag{1.30}$$

For $Op_A \in \mathsf{Ops}_A$, we have $t$ -$(h, Op_A, s)$-› $t'$ or $([v], [w])$ -$(([j], [k]), Op_U, ([p], [q]))$-› $([v'], [w'])$, iff $[v], [w], [j], [k], [p], [q], [v'], [w']$ satisfy

$$\begin{aligned}
&\textbf{(}\ \forall\ \underline{v}, \underline{j} \bullet \underline{v} \in [v] \wedge \underline{j} \in [j] \Rightarrow (\exists\ \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \\
&\quad K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}_{Op}(\underline{p}, ([p], [q])))\ \textbf{)} \qquad \text{(a)} \\
&\wedge \\
&\textbf{(}\ \forall\ \underline{w}, \underline{k} \bullet H^{\bullet}(\underline{w}, ([v], [w])) \wedge Q^{\bullet}_{Op}(\underline{k}, ([j], [k]), \underline{w}, ([v], [w])) \Rightarrow \\
&\quad (\ \exists\ \underline{w}', \underline{q} \bullet stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \textbf{(}H^{\bullet}(\underline{w}', ([v'], [w'])) \vee \\
&\qquad D^{\bullet}_{Op}(\underline{w}', ([v'], [w']), \underline{q}, ([p], [q]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))\textbf{)}\ )\ \textbf{)}\ . \qquad \text{(b)}
\end{aligned} \tag{1.31}$$

The initialization predicate $Init_U(t')$ sets $t'$ to any value $([v'], [w'])$ for which

$$(\exists\ \underline{v}' \bullet Init_T(\underline{v}') \wedge K^{\bullet}(\underline{v}', ([v'], [w']))) \ \wedge\ (\exists\ \underline{w}' \bullet Init_F(\underline{w}') \wedge H^{\bullet}(\underline{w}', ([v'], [w']))) \tag{1.32}$$

is true. This completes the definition of *Univ*.

We now establish that the components introduced define a retrenchment from *Ref* to *Univ* and an I/O-filtered refinement from *Ret* to *Univ*, by showing that the appropriate POs are satisfied.

Take *Ret* to *Univ* first. The Init PO is

$$Init_U(t') \Rightarrow (\exists\, \underline{v}' \bullet Init_T(\underline{v}') \wedge K^\bullet(\underline{v}', t'))\,. \tag{1.33}$$

Assume $Init_U(t')$ with $t' = ([v'], [w'])$. Then by (1.32) the consequent is immediate.

Now consider the Op PO

$$K^\bullet(\underline{v}, t) \wedge R^\bullet{}_{Op}(\underline{j}, h) \wedge stp_{Op_U}(t, h, t', s) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K^\bullet(\underline{v}', t') \wedge V^\bullet{}_{Op}(\underline{p}, s))\,. \tag{1.34}$$

Since $\mathsf{Ops}_U$ decomposes as $\mathsf{Ops}_A \cup (\mathsf{Ops}_U - \mathsf{Ops}_A)$, there are two cases to consider. Case $Op_U \in \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$. Then $K^\bullet$ and (1.18) give $\underline{v} \in [v]$; $R^\bullet{}_{Op}$ and (1.20) give $\underline{j} \in [j]$. The consequent now follows from (1.31a). Case $Op_U \notin \mathsf{Ops}_A$. Assume the antecedents with $t = ([v], [w])$, $h = \underline{j}$, $t' = ([v'], [w'])$ and $s = \underline{p}$. As before $\underline{v} \in [v]$. So from $stp_{Op_U}(t, h, t', s)$, by (1.30), $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$ and $K^\bullet(\underline{v}', t')$ hold, and since $s = \underline{p}$, $V^\bullet{}_{Op}(\underline{p}, s)$ holds too. We are done.

We turn to the POs of the retrenchment from *Ret* to *Univ*. The Init PO states

$$Init_U(t') \Rightarrow (\exists\, \underline{w}' \bullet Init_F(\underline{w}') \wedge H^\bullet(\underline{w}', t'))\,. \tag{1.35}$$

Assume $Init_U(t')$ with $t' = ([v'], [w'])$. Then by (1.32) the consequent is immediate.

For the Op PO we have to establish

$$H^\bullet(\underline{w}, t) \wedge Q^\bullet{}_{Op}(\underline{k}, h, \underline{w}, t) \wedge stp_{Op_U}(t, h, t', s) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q} \bullet stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge (H^\bullet(\underline{w}', t') \vee D^\bullet{}_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)))\,. \tag{1.36}$$

For this relationship $Op_U$ only ranges over $\mathsf{Ops}_A$. Choose values $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$ for which the antecedent holds. Then the consequent follows immediately from (1.31b). Done.

The final piece of the construction is to show that either the composition of the *Abs* to *Ret* retrenchment and the *Ret* to *Univ* refinement on the one hand, or the *Abs* to *Ref* refinement and the *Ref* to *Univ* retrenchment on the other, do indeed yield a retrenchment from *Abs* to *Univ*. For if so then (1.25), (1.27) and (1.29) show that they both give the *same* retrenchment, with retrieves, within, and concedes relations given respectively by $G$, $P_{Op}$, $C_{Op}$.

To prove the Init PO we have to show

$$Init_{\mathrm{U}}(t') \Rightarrow (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge G(u', t')) \,. \tag{1.37}$$

Assume $Init_{\mathrm{U}}(t')$ with $t' = ([v'], [w'])$. Then by (1.33) there is a value, $\underline{v}'$ say, for which $Init_{\mathrm{T}}(\underline{v}')$ and $K^{\bullet}(\underline{v}', t')$ hold. Given $Init_{\mathrm{T}}(\underline{v}')$, the Init PO for the retrenchment from *Abs* to *Ret*,

$$Init_{\mathrm{T}}(\underline{v}') \Rightarrow (\exists\, u' \bullet Init_{\mathrm{A}}(u') \wedge H(u', \underline{v}')) \,, \tag{1.38}$$

gives $Init_{\mathrm{A}}(u')$, one of the things we want, and also $H(u', \underline{v}')$. Finally, since we now have $H(u', \underline{v}')$ and $K^{\bullet}(\underline{v}', t')$, then by composition (1.24) we also have $G(u', t')$. We are done.

Next consider the Op PO. Here we have to show

$$\begin{aligned} &G(u, t) \wedge P_{Op}(i, h, u, t) \wedge stp_{Op_{\mathrm{U}}}(t, h, t', s) \Rightarrow \\ &\qquad (\exists\, u', o \bullet stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge (G(u', t') \vee C_{Op}(u', t', o, s; i, h, u, t))) \,. \end{aligned} \tag{1.39}$$

For this $Op_{\mathrm{U}}$ only ranges over $\mathsf{Ops}_{\mathrm{A}}$. Assume the antecedents with $t = ([v], [w])$, $h = ([j], [k])$, $t' = ([v'], [w'])$ and $s = ([p], [q])$. Now $P_{Op}(i, ([j], [k]), u, ([v], [w])) = (H(u, \underline{v}) \wedge Q_{Op}(i, j, u, \underline{v}));(K^{\bullet}(\underline{v}, ([v], [w])) \wedge R^{\bullet}{}_{Op}(j, ([j], [k])))$. Thus we have $K^{\bullet}(\underline{v}, ([v], [w]))$, $R^{\bullet}{}_{Op}(j, ([j], [k]))$ and $stp_{Op_{\mathrm{U}}}(t, h, t', s)$. Hence we can use (1.34) to derive $stp_{Op_{\mathrm{T}}}(\underline{v}, j, \underline{v}', \underline{p})$, $K^{\bullet}(\underline{v}', t')$ and $V^{\bullet}{}_{Op}(\underline{p}, s)$, for chosen values $\underline{v}'$ and $\underline{p}$. Next, $H(u, \underline{v})$, $Q_{Op}(i, j, u, \underline{v})$ and $stp_{Op_{\mathrm{T}}}(\underline{v}, j, \underline{v}', \underline{p})$ make up the antecedent of the Op PO for the retrenchment from *Abs* to *Ret*,

$$\begin{aligned} &H(u, \underline{v}) \wedge Q_{Op}(i, j, u, \underline{v}) \wedge stp_{Op_{\mathrm{T}}}(\underline{v}, j, \underline{v}', \underline{p}) \Rightarrow \\ &\qquad (\exists\, u', o \bullet stp_{Op_{\mathrm{A}}}(u, i, u', o) \wedge (H(u', \underline{v}') \vee D_{Op}(u', \underline{v}', o, \underline{p}; i, j, u, \underline{v}))) \,. \end{aligned} \tag{1.40}$$

Therefore we have values, $u'$ and $o$ say, such that $stp_{Op_{\mathrm{A}}}(u, i, u', o)$ and $(H(u', \underline{v}') \vee D_{Op}(u', \underline{v}', o, \underline{p}; i, j, u, \underline{v}))$ hold. Thus to establish (1.39) for these values all we need is $G' \vee C_{Op}$, which we derive from $H' \vee D_{Op}$ as follows. Assume $H(u', \underline{v}')$. Then as $K^{\bullet}(\underline{v}', t')$ holds, we have $H(u', \underline{v}');K^{\bullet}(\underline{v}', t')$ and thus $G(u', t')$, by (1.24). Now assume $D_{Op}(u', \underline{v}', o, \underline{p}; i, j, u, \underline{v})$. As $H$, $Q_{Op}$, $K^{\bullet\prime}$, $V^{\bullet}{}_{Op}$, $R^{\bullet}{}_{Op}$ and $K^{\bullet}$ all hold, we have $(H(u, \underline{v}) \wedge Q_{Op}(i, j, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o, \underline{p}; i, j, u, \underline{v}));(K^{\bullet}(\underline{v}', t') \wedge V^{\bullet}{}_{Op}(\underline{p}, s) \wedge R^{\bullet}{}_{Op}(j, h) \wedge K^{\bullet}(\underline{v}, t))$ and thus $C_{Op}(u', t', o, s; i, h, u, t)$, by (1.29). Hence $G' \vee C_{Op}$ holds and we are done.

To complete part (1) of the theorem we now state and prove properties (U1) to (U10) of *Univ.*

$$K^{\bullet}(v', t') \wedge K^{\bullet}(\underline{v}', t') \;\Rightarrow\; v' \sim \underline{v}' \tag{U1}$$

$$(H^{\bullet}(w', t') \vee D^{\bullet}_{Op}(w', t', ...)) \wedge (H^{\bullet}(\underline{w}', t') \vee D^{\bullet}_{Op}(\underline{w}', t', ...)) \Rightarrow\; w' \sim \underline{w}' \tag{U2}$$

$$V^{\bullet}_{Op}(p, s) \wedge V^{\bullet}_{Op}(\underline{p}, s) \Rightarrow\; p \sim \underline{p} \tag{U3}$$

$$D^{\bullet}_{Op}(w', t', q, s; k, h, w, t) \wedge D^{\bullet}_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \;\Rightarrow\; q \sim \underline{q} \tag{U4}$$

$$K^{\bullet}(v', t') \wedge \underline{v}' \in [v'] \Rightarrow\; K^{\bullet}(\underline{v}', t') \tag{U5}$$

$$V^{\bullet}_{Op}(p, s) \wedge \underline{p} \in [p] \Rightarrow V^{\bullet}_{Op}(\underline{p}, s) \tag{U6}$$

$$K^{\bullet}(v', t') \;\Rightarrow\; (H^{\bullet}(w', t') \Leftrightarrow H^{\bullet}(w', ([v'], [w'])))\tag{U7}$$

$$\begin{aligned} &K^{\bullet}(v', t') \wedge V^{\bullet}_{Op}(p, s) \wedge R^{\bullet}_{Op}(j, h) \wedge K^{\bullet}(v, t) \Rightarrow \\ &\quad \big( H^{\bullet}(w, t) \wedge Q^{\bullet}_{Op}(k, h, w, t) \wedge D^{\bullet}_{Op}(w', t', q, s; k, h, w, t) \Leftrightarrow \\ &\qquad H^{\bullet}(w, ([v], [w])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge \\ &\qquad D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w])) \big) \end{aligned} \tag{U8}$$

$$K^{\bullet}(v', t') \;\Rightarrow\; (\exists\, w' \bullet K^{\bullet}(v', ([v'], [w'])))\tag{U9}$$

$$V^{\bullet}_{Op}(p, s\tilde{}) \;\Rightarrow\; (\exists\, q \bullet V^{\bullet}_{Op}(p, ([p], [q])))\tag{U10}$$

*Proofs.*

(U1): Assume the antecedent and let $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then by (1.18) $v' \in [\underline{\underline{v}}']$ and $\underline{v}' \in [\underline{\underline{v}}']$. Hence $v' \sim \underline{v}'$.

(U2) to (U4): Similar to proof for (U1).

(U5): Suppose $K^{\bullet}(v', t')$ and $\underline{v}' \in [v']$ hold with $t' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Then (1.18) asserts $v' \in [\underline{\underline{v}}']$, $HK([\underline{\underline{v}}'], [\underline{\underline{w}}'])$ and $DK_{Op}([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. But $\underline{v}' \in [v']$, so $\underline{v}' \in [\underline{\underline{v}}']$. Hence $K^{\bullet}(\underline{v}', ([\underline{\underline{v}}'], [\underline{\underline{w}}']))$ holds and we are done.

(U6): Similar to (U5).

(U7): First we assume $K^{\bullet}(v', t')$ and $H^{\bullet}(w', t')$, and prove $H^{\bullet}(w', ([v'], [w']))$. Let $t' = ([\underline{v}'], [\underline{\underline{w}}'])$. Then from $H^{\bullet}(w', t')$ and (1.19) we have $w' \in [\underline{\underline{w}}']$, $(\exists\, u \bullet K(u, w'))$, $KH(w', [\underline{v}'])$, $HK([\underline{v}'], [\underline{\underline{w}}'])$ and $DK_{Op}([\underline{v}'], [\underline{\underline{w}}'])$; and from $K^{\bullet}(v', t')$ and (1.18), we have $v' \in [\underline{v}']$. Thus $w' \sim \underline{\underline{w}}'$ and $v' \sim \underline{v}'$. Hence $KH(w', [v'])$, $HK([v'], [w'])$ and $DK_{Op}([v'], [w'])$ are also true. We now have enough to obtain $H^{\bullet}(w', ([v'], [w']))$ by (1.19).

Now we assume $K^{\bullet}(v', t')$ and $H^{\bullet}(w', ([v'], [w']))$, and prove $H^{\bullet}(w', t')$. Let $t' = ([\underline{v}'], [\underline{\underline{w}}'])$. From $K^{\bullet}(v', ([\underline{v}'], [\underline{\underline{w}}']))$, by (1.18), $v' \in [\underline{v}']$, and $HK([\underline{v}'], [\underline{\underline{w}}'])$ holds. Thus $v' \sim \underline{v}'$ and so $HK([v'], [\underline{\underline{w}}'])$ holds too. From $H^{\bullet}(w', ([v'], [w']))$, by (1.19), $K(u', w')$ holds for chosen value $u'$. Then as $K(u', w')$;$H^{\bullet}(w', ([v'], [w']))$ holds, by (1.24), there must be a value, $\underline{v}'$ say, for which $H(u', \underline{v}')$;$K^{\bullet}(\underline{v}', ([v'], [w']))$ holds, with $\underline{v}' \in [v']$. From $H(u', \underline{v}')$ and $HK([v'], [\underline{\underline{w}}'])$, by (1.11), there must be a value, $\underline{w}'$ say, such that $K(u', \underline{w}')$ holds, with $\underline{w}' \in [\underline{\underline{w}}']$. Thus $\underline{w}' \sim \underline{\underline{w}}'$. Now notice we have $K(u', w')$, $K(u', \underline{w}')$ and $H(u', \underline{v}')$. So by (1.5) $w' \sim \underline{w}'$. But as $\underline{w}' \sim \underline{\underline{w}}'$, $w' \sim \underline{\underline{w}}'$. Finally recall that $v' \sim \underline{v}'$. Therefore because $H^{\bullet}(w', ([v'], [w']))$ holds, $H^{\bullet}(w', ([\underline{v}'], [\underline{\underline{w}}']))$ also holds and we are done.

(U8): First we assume $K^{\bullet}(v', t')$, $V^{\bullet}_{Op}(p, s)$, $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $H^{\bullet}(w, t)$, $Q^{\bullet}_{Op}(k, h, w, t)$ and $D^{\bullet}_{Op}(w', t', q, s; k, h, w, t)$, and prove $H^{\bullet}(w, ([v], [w]))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w]))$. Let $t' = ([\underline{v}'], [\underline{\underline{w}}'])$, $s = ([\underline{p}], [\underline{q}])$, $h = ([\underline{j}], [\underline{k}])$ and $t = ([\underline{v}], [\underline{\underline{w}}])$. From the assumed $D^{\bullet}_{Op}$ and (1.23) we have $w' \sim \underline{\underline{w}}'$, $q \sim \underline{q}$, $k \sim \underline{k}$ and $w \sim \underline{\underline{w}}$. Furthermore $K^{\bullet\prime}$, $V^{\bullet}_{Op}$, $R^{\bullet}_{Op}$, $K^{\bullet}$, (1.18), (1.20) and (1.22) give $v' \sim \underline{v}'$, $p \sim \underline{p}$, $j \sim \underline{j}$ and $v \sim \underline{v}$. Hence, since $H^{\bullet}(w, ([\underline{v}], [\underline{\underline{w}}]))$, $Q^{\bullet}_{Op}(k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{\underline{w}}]))$ and $D^{\bullet}_{Op}(w', ([\underline{v}'], [\underline{\underline{w}}']), q, ([\underline{p}], [\underline{q}]); k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{\underline{w}}]))$ hold, $H^{\bullet}(w, ([v], [w]))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w]))$ follow from the established equivalences.

Now we assume $K^{\bullet}(v', t')$, $V^{\bullet}_{Op}(p, s)$, $R^{\bullet}_{Op}(j, h)$, $K^{\bullet}(v, t)$, $H^{\bullet}(w, ([v], [w]))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w]))$, and prove $H^{\bullet}(w, t)$, $Q^{\bullet}_{Op}(k, h, w, t)$ and $D^{\bullet}_{Op}(w', t', q, s; k, h, w, t)$. We proceed as follows. Let $t' = ([\underline{v}'], [\underline{\underline{w}}'])$, $s = ([\underline{p}], [\underline{q}])$, $h = ([\underline{j}], [\underline{k}])$ and $t = ([\underline{v}], [\underline{\underline{w}}])$. By (1.23), the given $D^{\bullet}_{Op}$ lets us assert values $u'$, $o$, $i$ and $u$, such that $K(u', w')$, $V_{Op}(o, q)$, $R_{Op}(i, k)$ and $K(u, w)$ are true. Then as $(K(u', w') \wedge V_{Op}(o, q) \wedge R_{Op}(i, k) \wedge K(u, w))$;$(H^{\bullet}(w, ([v], [w])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w])))$ holds, by (1.28), there must be values, $\underline{v}'$, $\underline{p}$, $\underline{j}$ and $\underline{v}$ say, such that $(H(u, \underline{v}) \wedge Q_{Op}(i, \underline{j}, u, \underline{v}) \wedge D_{Op}(u', \underline{v}', o,$

$\underline{p}$; $i$, $\underline{j}$, $u$, $\underline{v}$));($K^{\bullet}(\underline{v}', ([v'], [w'])) \wedge V^{\bullet}_{Op}(\underline{p}, ([p], [q])) \wedge R^{\bullet}_{Op}(\underline{j}, ([j], [k])) \wedge K^{\bullet}(\underline{v}, ([v], [w]))$ holds. Hence, by (1.18), (1.20) and (1.22), $\underline{v}' \in [v']$, $\underline{p} \in [p]$, $\underline{j} \in [j]$ and $\underline{v} \in [v]$.

Now take $K^{\bullet}(v', ([\underline{v}'], [\underline{\underline{w}}']))$. From this, by (1.18), we immediately get $v' \sim \underline{v}'$ and also $DK_{Op}([\underline{v}'], [\underline{\underline{w}}'])$, from which $DK_{Op}([v'], [\underline{\underline{w}}'])$ follows. Therefore by (1.13), $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$, $\underline{v}' \in [v']$ and $DK_{Op}([v'], [\underline{\underline{w}}'])$ give $K(u', \underline{w}')$ with $\underline{w}' \sim \underline{\underline{w}}'$, for chosen value $\underline{w}$. So we have $K(u', w')$, $K(u', \underline{w}')$ and $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. Hence by (1.5) $w' \sim \underline{w}'$. But as $\underline{w}' \sim \underline{\underline{w}}'$ then $w' \sim \underline{\underline{w}}'$.

Next take $V^{\bullet}_{Op}(p, ([\underline{p}], [\underline{q}]))$. By (1.22) we get $p \sim \underline{p}$ and $DV_{Op}([\underline{p}], [\underline{q}])$, from which $DV_{Op}([p], [\underline{q}])$ follows. Since we also have $H(u, \underline{v})$, $Q_{Op}(i, \underline{j}, u, \underline{v})$, $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$, $K^{\bullet}(\underline{v}', ([\underline{v}'], [\underline{\underline{w}}']))$, $R^{\bullet}_{Op}(\underline{j}, ([\underline{j}], [\underline{k}]))$ and $K^{\bullet}(\underline{v}, ([\underline{v}], [\underline{\underline{w}}]))$, by (1.17), we derive $\underline{q}$ for which $V_{Op}(o, \underline{q})$ holds, with $\underline{q} \sim \underline{q}$. Now, $V_{Op}(o, q)$, $V_{Op}(o, \underline{q})$ and $D_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ all hold. So by (1.9), $q \sim \underline{q}$, and as $\underline{q} \sim \underline{q}$, then $q \sim \underline{q}$.

Similarly, $R^{\bullet}_{Op}(j, ([\underline{j}], [\underline{k}]))$, $\underline{j} \in [\underline{j}]$ and (1.20) give $j \sim \underline{j}$, $QR_{Op}([j], [\underline{k}])$ and $\underline{j} \in [j]$. The latter two, together with $H(u, \underline{v})$, $Q_{Op}(i, \underline{j}, u, \underline{v})$ and $K^{\bullet}(\underline{v}, ([\underline{v}], [\underline{\underline{w}}]))$ then give $R_{Op}(i, \underline{k})$ with $\underline{k} \sim \underline{k}$, by (1.15). Therefore because $R_{Op}(i, k)$, $R_{Op}(i, \underline{k})$ and $Q_{Op}(i, \underline{j}, u, \underline{v})$ hold, from (1.7) and $\underline{k} \sim \underline{k}$, we get $k \sim \underline{k}$.

Last, $K^{\bullet}(v, ([\underline{v}], [\underline{\underline{w}}]))$, $\underline{v} \in [\underline{v}]$, and (1.18) give $v \sim \underline{v}$, $HK([v], [\underline{\underline{w}}])$ and $\underline{v} \in [v]$. From here we use (1.11) to derive value $\underline{w}$, with $\underline{w} \sim \underline{\underline{w}}$, for which $K(u, \underline{w})$ holds. Then using (1.5) and $\underline{w} \sim \underline{\underline{w}}$, we get $w \sim \underline{\underline{w}}$.

So altogether we have $v' \sim \underline{v}'$, $w' \sim \underline{\underline{w}}'$, $p \sim \underline{p}$, $q \sim \underline{q}$, $j \sim \underline{j}$, $k \sim \underline{k}$, $v \sim \underline{v}$ and $w \sim \underline{\underline{w}}$. Hence, because $H^{\bullet}(w, ([v], [w]))$, $Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w]))$ and $D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w]))$ hold, then $H^{\bullet}(w, ([\underline{v}], [\underline{\underline{w}}]))$, $Q^{\bullet}_{Op}(k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{\underline{w}}]))$ and $D^{\bullet}_{Op}(w', ([\underline{v}'], [\underline{\underline{w}}']), q, ([\underline{p}], [\underline{q}]); k, ([\underline{j}], [\underline{k}]), w, ([\underline{v}], [\underline{\underline{w}}]))$ must also hold.

(U9): Assume $K^{\bullet}(v', t')$ with $t' = ([\underline{v}'], [\underline{\underline{w}}'])$. Then by (1.18) $v' \sim \underline{v}'$, which means $K^{\bullet}(v', ([v'], [\underline{\underline{w}}']))$ holds and therefore so does the consequent of (U9).

(U10): Similar to (U9).

Part (2) of Theorem 1.1 is concerned with the refinement from *Univ* to *Xtra*. Suppose there is an I/O-filtered refinement from *Ret* to *Xtra* given by retrieve relation $K^{\sim}$, within relation $R^{\sim}$, and nevertheless relation $V^{\sim}$; and a retrenchment from *Ref* to *Xtra* given by retrieve relation $H^{\sim}$, within relation $Q^{\sim}$, and concedes relation $D^{\sim}$. Let the state, input and output spaces of *Xtra* be given by $t^{\sim} \in \mathsf{T}^{\sim}$, $h^{\sim} \in \mathsf{H}^{\sim}$, $s^{\sim} \in \mathsf{S}^{\sim}$ and let the initialisation and step predicates of *Xtra* be $Init_X$ and $stp_{Op_X}$. Finally let *Xtra* have properties (X1) to (X10) below.

$$K^{\sim}(v', t^{\sim}') \wedge K^{\sim}(\underline{v}', t^{\sim}') \Rightarrow v' \sim \underline{v}' \tag{X1}$$

$$(H^{\sim}(w', t^{\sim}') \vee D^{\sim}_{Op}(w', t^{\sim}', ...)) \wedge (H^{\sim}(\underline{w}', t^{\sim}') \vee D^{\sim}_{Op}(\underline{w}', t^{\sim}', ...)) \Rightarrow w' \sim \underline{w}' \tag{X2}$$

$$V^{\sim}_{Op}(p, s^{\sim}) \wedge V^{\sim}_{Op}(\underline{p}, s^{\sim}) \Rightarrow p \sim \underline{p} \tag{X3}$$

$$D^{\sim}_{Op}(w', t^{\sim}', q, s^{\sim}; k, h^{\sim}, w, t^{\sim}) \wedge D^{\sim}_{Op}(\underline{w}', t^{\sim}', \underline{q}, s^{\sim}; \underline{k}, h^{\sim}, \underline{w}, t^{\sim}) \Rightarrow q \sim \underline{q} \tag{X4}$$

$$K^{\sim}(v', t^{\sim}') \wedge \underline{v}' \in [v'] \Rightarrow K^{\sim}(\underline{v}', t^{\sim}') \tag{X5}$$

$$V^{\sim}_{Op}(p, s^{\sim}) \wedge \underline{p} \in [p] \Rightarrow V^{\sim}_{Op}(\underline{p}, s^{\sim}) \tag{X6}$$

$$K^{\sim}(v', t^{\sim}') \Rightarrow (H^{\sim}(w', t^{\sim}') \Leftrightarrow H^{\bullet}(w', ([v'], [w']))) \tag{X7}$$

$$\begin{aligned} &K^{\sim}(v', t^{\sim}') \wedge V^{\sim}_{Op}(p, s^{\sim}) \wedge R^{\sim}_{Op}(j, h^{\sim}) \wedge K^{\sim}(v, t^{\sim}) \Rightarrow \\ &\quad (\, H^{\sim}(w, t^{\sim}) \wedge Q^{\sim}_{Op}(k, h^{\sim}, w, t^{\sim}) \wedge D^{\sim}_{Op}(w', t^{\sim}', q, s^{\sim}; k, h^{\sim}, w, t^{\sim}) \Leftrightarrow \\ &\qquad H^{\bullet}(w, ([v], [w])) \wedge Q^{\bullet}_{Op}(k, ([j], [k]), w, ([v], [w])) \wedge \\ &\qquad D^{\bullet}_{Op}(w', ([v'], [w']), q, ([p], [q]); k, ([j], [k]), w, ([v], [w]))\, ) \end{aligned} \tag{X8}$$

$$K^{\sim}(v', t^{\sim}') \Rightarrow (\exists\, w' \bullet K^{\bullet}(v', ([v'], [w']))) \tag{X9}$$

$$V^{\sim}_{Op}(p, s^{\sim}) \Rightarrow (\exists\, q \bullet V^{\bullet}_{Op}(p, ([p], [q]))) \tag{X10}$$

Notice properties (U1) to (U10) correspond to properties (X1) to (X10). Hence *Univ* and *Xtra* belong to the same class of systems that complete the square.

To prove part (2), we must show that there is an I/O-filtered refinement from *Univ* to *Xtra*. To this end we now define relations $K^{\circ}$, $R^{\circ}_{Op}$, $V^{\circ}_{Op}$, and prove that they are the retrieve, within and nevertheless relations of the desired refinement.

$$K^{\circ}(t, \tilde{t}) = K^{\circ}(([v], [w]), \tilde{t}) =$$
$$(\forall \underline{v} \bullet \underline{v} \in [v] \Rightarrow K^{\sim}(\underline{v}, \tilde{t})) \wedge (\forall \underline{w} \bullet H^{\bullet}(\underline{w}, ([v], [w])) \Rightarrow H^{\sim}(\underline{w}, \tilde{t})) \quad (1.41)$$

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

$$R^{\circ}_{Op}(h, \tilde{h}) = R^{\circ}_{Op}(([j], [k]), \tilde{h}) =$$
$$(\forall \underline{j} \bullet \underline{j} \in [j] \Rightarrow R^{\sim}_{Op}(\underline{j}, \tilde{h})) \wedge$$
$$(\forall \underline{k}, \underline{w}, t, \tilde{t} \bullet H^{\bullet}(\underline{w}, t) \wedge Q^{\bullet}_{Op}(\underline{k}, ([j], [k]), \underline{w}, t) \wedge K^{\circ}(t, \tilde{t}) \Rightarrow$$
$$H^{\sim}(\underline{w}, \tilde{t}) \wedge Q^{\sim}_{Op}(\underline{k}, \tilde{h}, \underline{w}, \tilde{t})), \quad (1.42)$$

$$V^{\circ}_{Op}(s, \tilde{s}) = V^{\circ}_{Op}(([p], [q]), \tilde{s}) =$$
$$(\forall \underline{p} \bullet \underline{p} \in [p] \Rightarrow V^{\sim}_{Op}(\underline{p}, \tilde{s})) \wedge$$
$$(\forall \underline{w}', \underline{q}, \underline{k}, \underline{w}, t', \tilde{t}', h, \tilde{h}, t, \tilde{t} \bullet$$
$$H^{\bullet}(\underline{w}, t) \wedge Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t) \wedge D^{\bullet}_{Op}(\underline{w}', t', \underline{q}, ([p], [q]); \underline{k}, h, \underline{w}, t) \wedge$$
$$K^{\circ}(t', \tilde{t}') \wedge R^{\circ}_{Op}(h, \tilde{h}) \wedge K^{\circ}(t, \tilde{t}) \Rightarrow$$
$$H^{\sim}(\underline{w}, \tilde{t}) \wedge Q^{\sim}_{Op}(\underline{k}, \tilde{h}, \underline{w}, \tilde{t}) \wedge D^{\sim}_{Op}(\underline{w}', \tilde{t}', \underline{q}, \tilde{s}; \underline{k}, \tilde{h}, \underline{w}, \tilde{t})). \quad (1.43)$$

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

$$R^{\circ}_{Op}(h, \tilde{h}) = (h = j \wedge R^{\sim}_{Op}(j, \tilde{h})), \quad (1.44)$$

$$V^{\circ}_{Op}(s, \tilde{s}) = (s = p \wedge V^{\sim}_{Op}(p, \tilde{s})). \quad (1.45)$$

We start by showing the above satisfy the inclusions stated in Theorem 1.1.

Take $K^{\bullet}(v, t); K^{\circ}(t, \tilde{t}) \Rightarrow K^{\sim}(v, \tilde{t})$. Assume the antecedents and let $t = ([\underline{v}], [\underline{w}])$. Then from $K^{\bullet}(v, ([\underline{v}], [\underline{w}]))$, by (1.18), $v \in [\underline{v}]$, and thus from $K^{\circ}(([\underline{v}], [\underline{w}]), \tilde{t})$, by (1.41), $K^{\sim}(v, \tilde{t})$ follows.

Next consider $R^{\bullet}_{Op}(j, h); R^{\circ}_{Op}(h, \tilde{h}) \Rightarrow R^{\sim}_{Op}(j, \tilde{h})$. There are two cases to deal with here. Case $Op \in \mathsf{Ops}_A$. Assume the antecedents and let $h = ([\underline{j}], [\underline{k}])$. Then from $R^{\bullet}_{Op}(j, ([\underline{j}], [\underline{k}]))$, by (1.20), $j \in [\underline{j}]$, and thus from $R^{\circ}_{Op}(([\underline{j}], [\underline{k}]), \tilde{h})$, by (1.42), $R^{\sim}_{Op}(j, \tilde{h})$ follows. Case $Op \notin \mathsf{Ops}_A$. Assume the antecedents. For this case $R^{\bullet}_{Op}$ is trivial with $h = j$. $R^{\circ}_{Op}(h, \tilde{h})$ and (1.44) then give $R^{\sim}(j, \tilde{h})$. We are done. A similar argument establishes $V^{\bullet}_{Op}(p, s); V^{\circ}_{Op}(s, \tilde{s}) \Rightarrow V^{\sim}_{Op}(p, \tilde{s})$.

Now for $H^{\bullet}(w, t);K^{\circ}(t, t\tilde{}) \Rightarrow H\tilde{}(w, t\tilde{})$. The consequent follows immediately from the antecedents by (1.41). The last two inclusions only apply to $Op$ in $\mathsf{Ops}_{\mathrm{A}}$. $(H^{\bullet}(w, t) \wedge Q^{\bullet}{}_{Op}(k, h, w, t));(R^{\circ}{}_{Op}(h, h\tilde{}) \wedge K^{\circ}(t, t\tilde{})) \Rightarrow (H\tilde{}(w, t\tilde{}) \wedge Q\tilde{}{}_{Op}(k, h\tilde{}, w, t\tilde{}))$ holds by (1.42). $(H^{\bullet}(w, t) \wedge Q^{\bullet}{}_{Op}(k, h, w, t) \wedge D^{\bullet}{}_{Op}(w', t', q, s; k, h, w, t));(K^{\circ}(t', t\tilde{}') \wedge V^{\circ}{}_{Op}(s, s\tilde{}) \wedge R^{\circ}{}_{Op}(h, h\tilde{}) \wedge K^{\circ}(t, t\tilde{})) \Rightarrow (H\tilde{}(w, t\tilde{}) \wedge Q\tilde{}{}_{Op}(k, h\tilde{}, w, t\tilde{}) \wedge D\tilde{}{}_{Op}(w', t\tilde{}', q, s\tilde{}; k, h\tilde{}, w, t\tilde{}))$ holds by (1.43).

The final task is to discharge the POs of the *Univ* to *Xtra* refinement. As usual, take the Init PO first. This says

$$Init_{\mathrm{X}}(t\tilde{}') \Rightarrow (\exists\, t' \bullet Init_{\mathrm{U}}(t') \wedge K^{\circ}(t', t\tilde{}')) \tag{1.46}$$

Assume the antecedent $Init_{\mathrm{X}}(t\tilde{}')$. In addition, we know we have the refinement from *Ret* to *Xtra* and the retrenchment from *Ref* to *Xtra* for which the Init POs are

$$Init_{\mathrm{X}}(t\tilde{}') \Rightarrow (\exists\, v' \bullet Init_{\mathrm{T}}(v') \wedge K\tilde{}(v', t\tilde{}')) \tag{1.47}$$

$$Init_{\mathrm{X}}(t\tilde{}') \Rightarrow (\exists\, w' \bullet Init_{\mathrm{F}}(w') \wedge H\tilde{}(w', t\tilde{}')) \tag{1.48}$$

respectively. These say that for the initial $t\tilde{}'$, there is a $v'$ for which $Init_{\mathrm{T}}(v')$ and a $w'$ for which $Init_{\mathrm{F}}(w')$ are true. Furthermore, we also get $K\tilde{}(v', t\tilde{}')$ and $H\tilde{}(w', t\tilde{}')$, from which, by (X7), we get $H^{\bullet}(w', (\lceil v' \rceil, \lceil w' \rceil))$. From this we can derive $K^{\bullet}(v', (\lceil v' \rceil, \lceil w' \rceil))$ by using (1.18) and (1.19). Now let $t' = (\lceil v' \rceil, \lceil w' \rceil)$. Then by (1.32) $Init_{\mathrm{U}}(t')$ is true. It remains to show $K^{\circ\prime}$ holds for this value of $t'$, i.e. that (1.41) holds. To show the first conjunct of (1.41), suppose $\underline{v}' \in \lceil v' \rceil$. Then as $K\tilde{}(v', t\tilde{}')$ holds, (X5) asserts $K\tilde{}(\underline{v}', t\tilde{}')$ holds as required. To establish the second conjunct, assume $H^{\bullet}(\underline{w}', t')$, i.e. $H^{\bullet}(\underline{w}', (\lceil v' \rceil, \lceil w' \rceil))$. But then $H^{\bullet}(\underline{w}', (\lceil v' \rceil, \lceil \underline{w}' \rceil))$ holds, and as $K\tilde{}(v', t\tilde{}')$ also holds, $H\tilde{}(\underline{w}', t\tilde{}')$ holds by (X7). We are done.

Now to the business of validating the Op PO. This states

$$\begin{aligned} &K^{\circ}(t, t\tilde{}) \wedge R^{\circ}{}_{Op}(h, h\tilde{}) \wedge stp_{Op_{\mathrm{X}}}(t\tilde{}, h\tilde{}, t\tilde{}', s\tilde{}) \Rightarrow \\ &\qquad (\exists\, t', s \bullet stp_{Op_{\mathrm{U}}}(t, h, t', s) \wedge K^{\circ}(t', t\tilde{}') \wedge V^{\circ}{}_{Op}(s, s\tilde{})) \end{aligned} \tag{1.49}$$

$\mathsf{Ops}_{\mathrm{X}}$ partitions into $\mathsf{Ops}_{\mathrm{A}}$ and non-$\mathsf{Ops}_{\mathrm{A}}$ operations. Take case $Op_{\mathrm{X}} \in \mathsf{Ops}_{\mathrm{A}}$ first. We will need the following lemmas.

**Lemma 1.10.** Suppose the antecedents of (1.49) hold with $t = (\lceil v \rceil, \lceil w \rceil)$ and $h = (\lceil j \rceil, \lceil k \rceil)$. Furthermore suppose $\underline{v} \in \lceil v \rceil$ and $\underline{j} \in \lceil j \rceil$. Then $K\tilde{}(\underline{v}, t\tilde{})$ and $R\tilde{}_{Op}(\underline{j}, h\tilde{})$ hold and moreover there are values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold.

*Proof.* From $K^{\circ}(t, t\tilde{})$ and $\underline{v} \in \lceil v \rceil$ we get $K\tilde{}(\underline{v}, t\tilde{})$ by (1.41); from $R^{\circ}_{Op}(h, h\tilde{})$ and $\underline{j} \in \lceil j \rceil$ we get $R\tilde{}_{Op}(\underline{j}, h\tilde{})$ by (1.42). $K\tilde{}$, $R\tilde{}_{Op}$ and $stp_{Op_X}$ are the antecedents of the Op PO for the refinement from *Ret* to *Xtra*,

$$K\tilde{}(\underline{v}, t\tilde{}) \wedge R\tilde{}_{Op}(\underline{j}, h\tilde{}) \wedge stp_{Op_X}(t\tilde{}, h\tilde{}, t\tilde{}', s\tilde{}) \Rightarrow$$
$$(\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K\tilde{}(\underline{v}', t\tilde{}') \wedge V\tilde{}_{Op}(\underline{p}, s\tilde{})) \,. \tag{1.50}$$

Thus we can pick values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold. Done. □

**Lemma 1.11.** Suppose the antecedents of (1.49) hold with $t = (\lceil v \rceil, \lceil w \rceil)$ and $h = (\lceil j \rceil, \lceil k \rceil)$. Furthermore suppose $H^{\bullet}(\underline{w}, t)$ and $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$ hold. Then there are values, which we fix as $\underline{w}'$ and $\underline{q}$, for which $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $H\tilde{}(\underline{w}', t\tilde{}') \vee D\tilde{}_{Op}(\underline{w}', t\tilde{}', \underline{q}, s\tilde{}; \underline{k}, h\tilde{}, \underline{w}, t\tilde{})$ hold.

*Proof.* From $R^{\circ}_{Op}(h, h\tilde{})$, $H^{\bullet}(\underline{w}, t)$, $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$ and $K^{\circ}(t, t\tilde{})$ we get $H\tilde{}(\underline{w}, t\tilde{})$ and $Q\tilde{}_{Op}(\underline{k}, h\tilde{}, \underline{w}, t\tilde{})$ by (1.42). $H\tilde{}$, $Q\tilde{}_{Op}$ and $stp_{Op_X}$ are the antecedents of the Op PO for the retrenchment from *Ref* to *Xtra*,

$$H\tilde{}(w, t\tilde{}) \wedge Q\tilde{}_{Op}(k, h\tilde{}, w, t\tilde{}) \wedge stp_{Op_X}(t\tilde{}, h\tilde{}, t\tilde{}', s\tilde{}) \Rightarrow$$
$$(\exists\, \underline{w}', \underline{q} \bullet stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge$$
$$(H\tilde{}(\underline{w}', t\tilde{}') \vee D\tilde{}_{Op}(\underline{w}', t\tilde{}', \underline{q}, s\tilde{}; \underline{k}, h\tilde{}, \underline{w}, t\tilde{}))) \,. \tag{1.51}$$

Thus we can pick values, which we fix as $\underline{w}'$ and $\underline{q}$, for which $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $H\tilde{}(\underline{w}', t\tilde{}') \vee D\tilde{}_{Op}(\underline{w}', t\tilde{}', \underline{q}, s\tilde{}; \underline{k}, h\tilde{}, \underline{w}, t\tilde{})$ hold. Done. □

To prove (1.49) assume the antecedents with $t = (\lceil v \rceil, \lceil w \rceil)$ and $h = (\lceil j \rceil, \lceil k \rceil)$. First we will establish that there are $t'$ and $s$ for which $stp_{Op_U}(t, h, t', s)$ holds, i.e. for which (1.31) holds. Consider (1.31b). For all values $\underline{k}$ and $\underline{w}$ for which the antecedent holds, Lemma 1.11 asserts we have values $\underline{w}'$ and $\underline{q}$ for which $H\tilde{}'$ or $D\tilde{}_{Op}$ and $stp_{Op_F}$ hold. Thus we have three

possibilities: (i) there are no values for which the antecedent of (b) holds; (ii) for all values for which the antecedent holds, $H\tilde{}'$ always holds; and (iii) there is at least one pair of values for which the antecedent holds for which $D\tilde{}_{Op}$ holds.

To begin, we establish the following. Since $v \in [v]$ and $j \in [j]$, by Lemma 1.10, $K\tilde{}(v, t\tilde{})$ and $R\tilde{}_{Op}(j, h\tilde{})$ hold, and furthermore there are values, which we fix as $v'$ and $p$, for which $stp_{Op_T}(v, j, v', p)$, $K\tilde{}(v', t\tilde{}')$ and $V\tilde{}_{Op}(p, s\tilde{})$ hold.

Case (i). (1.31b) holds trivially. We move on to (1.31a). Its antecedent holds for values $v$ and $j$, so from the previous paragraph we know $stp_{Op_T}(v, j, v', p)$, $K\tilde{}(v', t\tilde{}')$ and $V\tilde{}_{Op}(p, s\tilde{})$ hold. As we have $K\tilde{}'$, (X9) states we have a value, $\underline{w}'$ say, for which $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds. Similarly, $V\tilde{}_{Op}$ and (X10) give $V^{\bullet}_{Op}(p, ([p], [\underline{q}]))$. Let $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Then the consequent of (a) holds. Having fixed $t'$ and $s$, we now need to show that for any other choice of values for which the antecedent of (a) holds the consequent does too. So suppose $\underline{v} \in [v]$ and $\underline{j} \in [j]$. Then by Lemma 1.10 we can derive $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$. Since we now have both $K\tilde{}(v', t\tilde{}')$ and $K\tilde{}(\underline{v}', t\tilde{}')$, by (X1) $v' \sim \underline{v}'$ and thus $\underline{v}' \in [v']$. Therefore, as $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds, by (5.18), $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ and hence $K^{\bullet}(\underline{v}', t')$ holds. Likewise, from $V\tilde{}_{Op}(p, s\tilde{})$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$, by (X3) and (5.22) we establish $V^{\bullet}_{Op}(\underline{p}, s)$ holds. Done.

Case (ii). Let the antecedent of (1.31b) hold for $H^{\bullet}(\underline{w}, t)$ and $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$. Then by Lemma 1.11 $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $H\tilde{}(\underline{w}', t\tilde{}')$ hold ($D\tilde{}_{Op}$ is false for this case). Recalling that we also have $K\tilde{}(v', t\tilde{}')$, we can thus derive $H^{\bullet}(\underline{w}', ([v'], [\underline{w}']))$ by (X7). Now let $t' = ([v'], [\underline{w}'])$. Then the consequent of (b) holds. Furthermore, for any other choice, say $H^{\bullet}(\underline{\underline{w}}, t)$ and $Q^{\bullet}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$, for which the antecedent of (b) holds, by Lemma 1.11, $stp_{Op_F}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}})$ and $H\tilde{}(\underline{\underline{w}}', t\tilde{}')$ hold ($D\tilde{}_{Op}$ is false). Now since we have $H\tilde{}(\underline{\underline{w}}', t\tilde{}')$, $K\tilde{}(v', t\tilde{}')$ and (X7) allow us to derive $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}'])$. Moreover, because we also have $H\tilde{}(\underline{w}', t\tilde{}')$, (X2) says $\underline{w}' \sim \underline{\underline{w}}'$. But this means $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}'])$ and thus $H^{\bullet}(\underline{\underline{w}}', t')$ holds. Hence (b) always holds for our choice of $t'$. It remains to set the value of $s$. We already know $V\tilde{}_{Op}(p, s\tilde{})$ is true. Therefore by (X10) we can pick a value, $\underline{q}$ say, such that $V^{\bullet}_{Op}(p, ([p], [\underline{q}]))$ holds. We let $s = ([p], [\underline{q}])$. We now need to show that (a) always holds for these values of $t'$ and $s$. Assume the antecedent of (a) holds for $\underline{v} \in [v]$ and $\underline{j} \in [j]$. By Lemma 1.10 $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold. Now $K\tilde{}(v', t\tilde{}')$, $K\tilde{}(\underline{v}', t\tilde{}')$ and (X1) imply $v' \sim \underline{v}'$. So since $H^{\bullet}(\underline{w}', t')$ holds, by (1.19) and (1.18) we can show $K^{\bullet}(\underline{v}', t')$ holds

as well. Finally note we have $V\tilde{}_{Op}(p, s\tilde{})$ in addition to $V\tilde{}_{Op}(\underline{p}, s\tilde{})$. Therefore (X3) states $p \sim \underline{p}$, and so as $V^{\bullet}_{Op}(p, s)$ holds, by (5.22), $V^{\bullet}_{Op}(\underline{p}, s)$ does too. We are done.

Case (iii). Let the antecedent of (1.31b) hold for $H^{\bullet}(\underline{w}, t)$ and $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$. By Lemma 1.11 $stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q})$ and $H\tilde{}(\underline{w}', t\tilde{}')$ or $D\tilde{}_{Op}(\underline{w}', t\tilde{}', \underline{q}, s\tilde{}; \underline{k}, h\tilde{}, \underline{w}, t\tilde{})$ hold, but we will further assume that it is for this choice of antecedent that $D\tilde{}_{Op}$ holds. Now, from Lemma 1.10 we have $K\tilde{}(v, t\tilde{})$, $R\tilde{}_{Op}(j, h\tilde{})$, $K\tilde{}(v', t\tilde{}')$ and $V\tilde{}_{Op}(p, s\tilde{})$. From $R^{\circ}_{Op}(h, h\tilde{})$, $H^{\bullet}(\underline{w}, t)$, $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$ and $K^{\circ}(t, t\tilde{})$, by (1.42), we also have $H\tilde{}(\underline{w}, t\tilde{})$ and $Q\tilde{}_{Op}(\underline{k}, h\tilde{}, \underline{w}, t\tilde{})$. Thus we can apply (X8) and get $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [\underline{k}]), \underline{w}, ([v], [\underline{w}]))$. What is more, because $Q^{\bullet}_{Op}(\underline{k}, h, \underline{w}, t)$ holds with $t = ([v], [w])$ and $h = ([j], [k])$, by (1.21), $\underline{k} \sim k$ and $\underline{w} \sim w$. Thus $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ holds. Let $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Then the consequent of (b) holds for our choice of antecedent. We need to show (b) holds for any other choice. So assume $H^{\bullet}(\underline{\underline{w}}, t)$ and $Q^{\bullet}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$. By Lemma 1.11 $stp_{Op_F}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{q})$ and $H\tilde{}(\underline{\underline{w}}', t\tilde{}') \vee D\tilde{}_{Op}(\underline{\underline{w}}', t\tilde{}', \underline{q}, s\tilde{}; \underline{\underline{k}}, h\tilde{}, \underline{\underline{w}}, t\tilde{})$ hold. First assume $H\tilde{}(\underline{\underline{w}}', t\tilde{}')$. Then because we have $K\tilde{}(v', t\tilde{}')$, by (X7) we also have $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$. However, by (X2), $H\tilde{}(\underline{\underline{w}}', t\tilde{}')$ and $D\tilde{}_{Op}(\underline{\underline{w}}', t\tilde{}', ...)$ imply $\underline{\underline{w}}' \sim \underline{w}'$. Hence $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$ and thus $H^{\bullet}(\underline{\underline{w}}', t')$ holds, and therefore so does the consequent of (b). On the other hand assume $D\tilde{}_{Op}(\underline{\underline{w}}', t\tilde{}', \underline{q}, s\tilde{}; \underline{\underline{k}}, h\tilde{}, \underline{\underline{w}}, t\tilde{})$. From $R^{\circ}_{Op}(h, h\tilde{})$, $H^{\bullet}(\underline{\underline{w}}, t)$, $Q^{\bullet}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$ and $K^{\circ}(t, t\tilde{})$, by (1.42), we have $H\tilde{}(\underline{\underline{w}}, t\tilde{})$ and $Q\tilde{}_{Op}(\underline{\underline{k}}, h\tilde{}, \underline{\underline{w}}, t\tilde{})$. Then since we have $K\tilde{}(v, t\tilde{})$, $R\tilde{}_{Op}(j, h\tilde{})$, $K\tilde{}(v', t\tilde{}')$, and $V\tilde{}_{Op}(p, s\tilde{})$, $D^{\bullet}_{Op}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']), \underline{q}, ([p], [\underline{q}]); \underline{\underline{k}}, ([j], [\underline{\underline{k}}]), \underline{\underline{w}}, ([v], [\underline{\underline{w}}]))$ holds by (X8). But $D\tilde{}_{Op}(\underline{\underline{w}}', t\tilde{}', \underline{q}, s\tilde{}; ...)$ and $D\tilde{}_{Op}(\underline{\underline{w}}', t\tilde{}', \underline{q}, s\tilde{}; ...)$ imply $\underline{\underline{w}}' \sim \underline{w}'$ by (X2) and $\underline{q} \sim q$ by (X4). Moreover $Q^{\bullet}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$ and (1.21) give $\underline{\underline{k}} \sim k$ and $\underline{\underline{w}} \sim w$. As a result $D^{\bullet}_{Op}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']), \underline{q}, ([p], [\underline{q}]); \underline{\underline{k}}, ([j], [k]), \underline{\underline{w}}, ([v], [w]))$ or equivalently $D^{\bullet}_{Op}(\underline{\underline{w}}', t', \underline{q}, s; \underline{\underline{k}}, h, \underline{\underline{w}}, t)$ holds. Hence the consequent of (b) holds for $H^{\bullet}(\underline{\underline{w}}, t)$ and $Q^{\bullet}_{Op}(\underline{\underline{k}}, h, \underline{\underline{w}}, t)$.

We now show (1.31a) always holds for $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. Assume the antecedent holds for $\underline{v} \in [v]$ and $\underline{j} \in [j]$. By Lemma 1.10 $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold. Then $K\tilde{}(v', t\tilde{}')$, $K\tilde{}(\underline{v}', t\tilde{}')$ and (X1) say $v' \sim \underline{v}'$; $V\tilde{}_{Op}(p, s\tilde{})$, $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ and (X3) say $p \sim \underline{p}$. From above we know $D^{\bullet}_{Op}(\underline{w}', ([v'], [\underline{w}']), \underline{q}, ([p], [\underline{q}]); \underline{k}, ([j], [k]), \underline{w}, ([v], [w]))$ is true. Hence (1.23) gives $HK([v'], [\underline{w}'])$, $DK_{Op}([v'], [\underline{w}'])$. Therefore, as $v' \sim \underline{v}'$, $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ holds by (1.18). In addition (1.23) gives $DV_{Op}([p], [\underline{q}])$ and since $p \sim \underline{p}$, $V^{\bullet}_{Op}(\underline{p}, ([p], [\underline{q}]))$ or equivalently $V^{\bullet}_{Op}(\underline{p}, s)$ follows by (1.22). Ergo (a) holds for $t'$ and $s$.

All that remains is to show $K^{\circ}(t', t\tilde{}')$ and $V^{\circ}_{Op}(s, s\tilde{})$ for $t' = ([v'], [\underline{w}'])$ and $s = ([p], [\underline{q}])$. To show $K^{\circ\prime}$ we must demonstrate both conjuncts of (1.41) hold. Take the first conjunct and assume $\underline{v}' \in [v']$. Then because $K\tilde{}(v', t\tilde{}')$ is true, (X5) gives $K\tilde{}(\underline{v}', t\tilde{}')$. Hence the first conjunct holds. Now for the second. Assume $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{w}']))$. (1.19) says $\underline{\underline{w}}' \in [\underline{w}']$, which means $H^{\bullet}(\underline{\underline{w}}', ([v'], [\underline{\underline{w}}']))$ is also true. From this, by (X7), $H\tilde{}(\underline{\underline{w}}', t\tilde{}')$ holds, and as a result $K^{\circ}(t', t\tilde{}')$ holds. To show $V^{\circ}_{Op}$ we must verify both conjuncts of (1.43). To prove the first conjunct assume $\underline{p} \in [p]$. Then because $V\tilde{}_{Op}(p, s\tilde{})$ is true, (X6) states that $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ is true. To establish the second conjunct, we assume $H^{\bullet}(\underline{\underline{w}}, \underline{t})$, $Q^{\bullet}_{Op}(\underline{\underline{k}}, \underline{h}, \underline{\underline{w}}, \underline{t})$ $D^{\bullet}_{Op}(\underline{\underline{w}}', \underline{t}', \underline{q}, ([p], [\underline{q}]); \underline{\underline{k}}, \underline{h}, \underline{\underline{w}}, \underline{t})$, $K^{\circ}(\underline{t}', \underline{t}\tilde{}')$, $R^{\circ}_{Op}(\underline{h}, \underline{h}\tilde{})$ and $K^{\circ}(\underline{t}, \underline{t}\tilde{})$ where $\underline{t}' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$, $\underline{h} = ([\underline{\underline{j}}], [\underline{\underline{k}}])$, $\underline{t} = ([\underline{\underline{v}}], [\underline{\underline{w}}])$ and $([p], [\underline{q}]) = s = ([p], [\underline{q}])$. Now, $\underline{\underline{v}}' \in [\underline{\underline{v}}']$, $K^{\circ}(\underline{t}', \underline{t}\tilde{}')$ and (1.41) give $K\tilde{}(\underline{\underline{v}}', \underline{t}\tilde{}')$; $\underline{\underline{j}} \in [\underline{\underline{j}}]$, $R^{\circ}_{Op}(\underline{h}, \underline{h}\tilde{})$ and (1.42) give $R\tilde{}_{Op}(\underline{\underline{j}}, \underline{h}\tilde{})$; and $\underline{\underline{v}} \in [\underline{\underline{v}}]$, $K^{\circ}(\underline{t}, \underline{t}\tilde{})$ and (1.41) give $K\tilde{}(\underline{\underline{v}}, \underline{t}\tilde{})$. Then because we also have $V\tilde{}_{Op}(p, s\tilde{})$ (X8) gives $H\tilde{}(\underline{\underline{w}}, \underline{t}\tilde{})$, $Q\tilde{}_{Op}(\underline{\underline{k}}, \underline{h}\tilde{}, \underline{\underline{w}}, \underline{t}\tilde{})$ and $D\tilde{}_{Op}(\underline{\underline{w}}', \underline{t}\tilde{}', \underline{q}, s\tilde{}; \underline{\underline{k}}, \underline{h}\tilde{}, \underline{\underline{w}}, \underline{t}\tilde{})$. Therefore the second conjunct holds and we are done.

Case $Op_X \notin \mathsf{Ops}_A$. We will use the following lemma.

**Lemma 1.12.** Suppose the antecedents of (1.49) hold with $t = ([v], [w])$ and $h = \underline{j}$. Furthermore suppose $\underline{v} \in [v]$. Then there are values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold.

*Proof.* From $K^{\circ}(t, t\tilde{})$ and $\underline{v} \in [v]$ we get $K\tilde{}(\underline{v}, t\tilde{})$ by (1.41); from $R^{\circ}_{Op}(h, h\tilde{})$ and $h = \underline{j}$ we get $R\tilde{}_{Op}(\underline{j}, h\tilde{})$ by (1.44). $K\tilde{}$, $R\tilde{}_{Op}$ and $stp_{Op_X}$ are the antecedents of PO (1.50), so we can pick values, which we fix as $\underline{v}'$ and $\underline{p}$, for which $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ hold. Done. □

To prove (1.49) assume the antecedent with $t = ([v], [w])$ and $h = j$. Since $v \in [v]$, by Lemma 1.12, there are values, which we fix as $v'$ and $p$, such that $stp_{Op_T}(v, j, v', p)$, $K\tilde{}(v', t\tilde{}')$ and $V\tilde{}_{Op}(p, s\tilde{})$ hold. Then $K\tilde{}(v', t\tilde{}')$ and (X9) allow us to pick a value, say $\underline{w}'$, for which $K^{\bullet}(v', ([v'], [\underline{w}']))$ holds. Let $t' = ([v'], [\underline{w}'])$ and $s = p$. We now show that for these values of $t'$ and $s$, (1.30) and thus $stp_{Op_U}$ holds. Suppose $\underline{v} \in [v]$. Then using Lemma 1.12 we can derive $stp_{Op_T}(\underline{v}, j, \underline{v}', \underline{p})$, $K\tilde{}(\underline{v}', t\tilde{}')$ and $V\tilde{}_{Op}(\underline{p}, s\tilde{})$. Now since $K\tilde{}(v', t\tilde{}')$ and $K\tilde{}(\underline{v}', t\tilde{}')$ are true, by (X1), $v' \sim \underline{v}'$. Therefore, because $K^{\bullet}(v', ([v'], [\underline{w}']))$ is true, $K^{\bullet}(\underline{v}', ([v'], [\underline{w}']))$ is also true. Furthermore, $V\tilde{}_{Op}(p, s\tilde{})$, $V\tilde{}_{Op}(\underline{p}, s\tilde{})$ and (X3) imply $\underline{p} = p$ (because the equivalence class is a singleton). Hence $stp_{Op_U}(t, h, t', s)$ holds for values $t'$ and $s$. Finally we show

that $K^{\circ}(t', t\tilde{}')$ and $V^{\circ}_{Op}(s, s\tilde{})$ hold. The proof for $K^{\circ}(t', t\tilde{}')$ is identical case $Op_X \in \mathsf{Ops}_A$. We move on to $V^{\circ}_{Op}(s, s\tilde{})$. For this we must verify (1.45) which we do easily as we already have $V\tilde{}_{Op}(p, s\tilde{})$ and $s = p$. Done. This completes part (2) of the theorem.

Part (3) follows readily by observing that for a system *Univ** having the same properties as *Univ*, there will be an I/O-filtered refinement from *Univ* to *Univ** and an I/O-filtered refinement from *Univ** to *Univ*. ☺