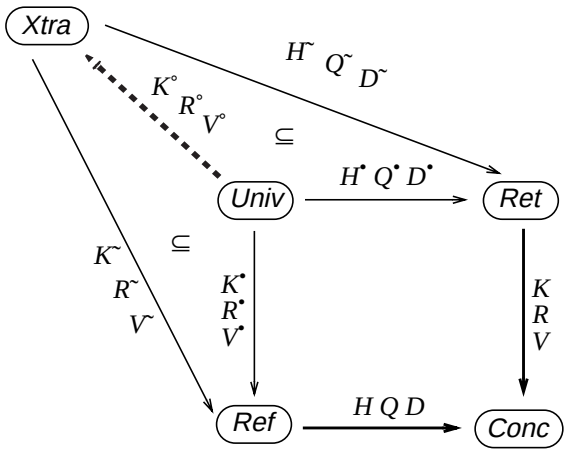
Reconciling Retrenchments and Refinements II: Proofs

This document presents the proofs for the construction presented in Section 5 of *Reconciling Retrenchments and Refinements II*. 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 *Ref* to *Conc*, and a refinement from *Ret* to *Conc*, as shown in Figure 1.1, which satisfy conditions (1.30) to (1.33) given below.



All arrows labelled with a *H Q D* are retrenchments.
All arrows labelled with a *K R V* are refinements.

Figure 1.1: Reconciliation II

Then the following hold.

(1) There is a universal system *Univ* for which there is a retrenchment from *Univ* to *Ret* and an I/O-filtered refinement from *Univ* to *Ref* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Univ* to *Conc*, and which satisfies (U1) to (U11) below.

(2) Whenever there is a system *Xtra* and a retrenchment from *Xtra* to *Ret* and an I/O-filtered refinement from *Xtra* to *Ref* whose compositions with the original refinement and retrenchment respectively are equal as retrenchments from *Xtra* to *Conc*, and which satisfies (X1) to (X11) below, then there is an I/O-filtered refinement from *Univ* to *Xtra* such that $K^\circ;H^\sim \Rightarrow H^\bullet$, $(K^\circ \wedge R^\circ);(H^\sim \wedge Q^\sim) \Rightarrow (H^\bullet \wedge Q^\bullet)$, $(K^{\circ\prime} \wedge V^\circ \wedge R^\circ \wedge K^\circ);(H^\sim \wedge Q^\sim \wedge D^\sim) \Rightarrow (H^\bullet \wedge Q^\bullet \wedge D^\bullet)$, and such that $K^\circ;K^\sim \Rightarrow K^\bullet$, $R^\circ;R^\sim \Rightarrow R^\bullet$, $V^\circ;V^\sim \Rightarrow V^\bullet$.

(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 *Ref* to *Conc* and the refinement from *Ret* to *Conc*, and build a new, universal, system *Univ*, from which there is both a retrenchment to *Ret* and a refinement to *Ref*. See Figure 1.1. First let

$$HD(w, t) = H(w, t) \vee \bigvee_{Op} (\exists \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(w, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \tag{1.1}$$

$$QI_{Op}(k, h) = (\exists \underline{w}, \underline{t} \bullet Q_{Op}(k, h, \underline{w}, \underline{t})) \tag{1.2}$$

$$DO_{Op}(q, s) = (\exists \underline{w}', \underline{t}', \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(\underline{w}', \underline{t}', q, s; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \tag{1.3}$$

Given these, we now introduce the following equivalence relations.

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

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

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

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

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

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

The operation names set of *Univ* is Ops_U with elements Op_U. The state space is U with elements u, inputs are $i \in \mathsf{I}$, outputs $o \in \mathsf{O}$. These are all constructed from the systems *Ret* and *Ref* as follows. Let $\mathsf{Ops}_U = \mathsf{Ops}_F$. The state space U is $\mathsf{V}/\sim_V \times \mathsf{W}/\sim_W$. Similarly the input and output spaces for each Op_U are $\mathsf{I}_{Op} = \mathsf{J}_{Op}/\sim_{J_{Op}} \times \mathsf{K}_{Op}/\sim_{K_{Op}}$ and $\mathsf{O}_{Op} = \mathsf{P}_{Op}/\sim_{P_{Op}} \times \mathsf{Q}_{Op}/\sim_{Q_{Op}}$.

Now for some more definitions.

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

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

$$KD_{Op}(\underline{v}, [w]) = (\forall\, t \bullet K(\underline{v}, t) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge (\exists\, \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(\underline{w}, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})))) \tag{1.12}$$

$$DK_{Op}([v], [w]) = (\forall\, \underline{w}, t \bullet \underline{w} \in [w] \wedge (\exists\, \underline{q}, \underline{s}, \underline{k}, \underline{h}, \underline{w}, \underline{t} \bullet D_{Op}(\underline{w}, t, \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})) \Rightarrow (\exists\, \underline{v} \bullet \underline{v} \in [v] \wedge K(\underline{v}, t) \wedge KD_{Op}(\underline{v}, [w]))) \tag{1.13}$$

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

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

$$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) = (\forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))) \tag{1.16}$$

$$DV_{Op}([p], [q]) = (\forall\, t', s, h, t, \underline{w}', \underline{q}, \underline{k}, \underline{w}, v', w', j, k, v, w \bullet \underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$$

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$
$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))) \quad (1.17)$$

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

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

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

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

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

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

$$D^{\bullet}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) =$$
$$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$$
$$(\exists\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge$$
$$VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge DV_{Op}([p], [q])$$
$$HK([v'], [w']) \wedge \bigwedge_{Op} DK_{Op}([v'], [w']) \quad (1.23)$$

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

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

We write this for short as

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

Secondly,

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

or more briefly

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

Thirdly,

$$\begin{aligned}
&\mathbf{(}K^{\bullet}(([v'], [w']), \underline{w}') \wedge V^{\bullet}{}_{Op}(([p], [q]), \underline{q}) \wedge R^{\bullet}{}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w})\mathbf{)};\\
&\quad \mathbf{(}H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)\mathbf{)}\\
&=\\
&\mathbf{(}H^{\bullet}(([v], [w]), \underline{v}) \wedge Q^{\bullet}{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge\\
&\quad D^{\bullet}{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})\mathbf{)};\\
&\quad \mathbf{(}K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)\mathbf{)} \,,
\end{aligned} \tag{1.28}$$

or

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

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.

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

Proof.

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

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

$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge$

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

= [meaning of ∀, idempotency]

$\underline{w} \in [w] \wedge H(\underline{w}, t) \wedge$

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

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

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

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

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

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

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

Proof.

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

= [definition of KH, (1.10)]

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

= [meaning of $\forall$, idempotency]

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

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

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

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

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

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

Lemma 1.4.

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

Proof.

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

= [definition of QR, (1.15)]

$\underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

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

= [meaning of $\forall$, idempotency]

$\underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

$\quad (\underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))) \wedge$

$\quad (\forall\, h, t, \underline{k}, \underline{w}, v, w \bullet \underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))$

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

$\underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge$

$\quad (\underline{k} \in [k] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge K^{\bullet}(([v], [w]), \underline{w}) \Rightarrow$

$\quad\quad (\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w])))$

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

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

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

Proof.

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

$= [\text{definition of } RQ, (1.14)]$

$R_{Op}(\underline{j}, h) \wedge (\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

$= [(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t)) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))]$

$R_{Op}(\underline{j}, h) \wedge (\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad (\ (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t)) \wedge$

$\quad\quad (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ )\ )$

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

$R_{Op}(\underline{j}, h) \wedge (\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\, \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ ) \wedge$

$\quad (\ \forall\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad\quad (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

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

$R_{Op}(j, h) \wedge (\ \forall\ h, t \bullet R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ )$

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

$R_{Op}(j, h) \wedge (\ \forall\ t \bullet R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ ) \wedge$

$(\ \forall\ h, t \bullet R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ )$

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

$R_{Op}(j, h) \wedge (\ \forall\ t \bullet R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ )$

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

$R_{Op}(j, h) \wedge (\ \forall\ t \bullet K(\underline{v}, t) \Rightarrow (\exists\ \underline{w} \bullet \underline{w} \in [w] \wedge H(\underline{w}, t))\ )$

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

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

$\Rightarrow$ [(1.10)]

$KH(\underline{v}, [w])$ □

Lemma 1.6.

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

Proof.

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

= [definition of RQ, (1.14)]

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

= [meaning of $\forall$, idempotency]

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

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

$R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge$

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

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

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))$ □

Lemma 1.7.

$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$
$\quad K^{\bullet}(([v'], [w']), \underline{w}') \wedge R^{\bullet}_{Op}(([j], [k]), \underline{k}) \wedge K^{\bullet}(([v], [w]), \underline{w}) \wedge DV_{Op}([p], [q]) \Rightarrow$
$\quad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$
$\quad\quad V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))$

Proof.

$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

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

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

$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

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

$\quad (\forall\, t', s, h, t, \underline{w}', \underline{q}, \underline{k}, \underline{w}, v', w', j, k, v, w \bullet$

$\quad\quad \underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

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

$\quad\quad\quad (\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$

$\quad\quad\quad V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))$

= [meaning of $\forall$, idempotency]

$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

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

$\quad (\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

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

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))) \wedge$$

$$(\forall\, t', s, h, t, \underline{w}', \underline{q}, \underline{k}, \underline{w}, v', w', j, k, v, w \bullet$$

$$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$$

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

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))$$

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

$$\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$$

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

$$(\underline{q} \in [q] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$$

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

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge$$

$$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])))$$

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

$$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$$

$$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])) \qquad \square$$

Lemma 1.8.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \Rightarrow RQ_{Op}(\underline{j}, \underline{v}, [k], [w])$$

Proof.

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])$$

$$= [\text{definition of } VD, (1.16)]$$

$$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$$

$$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$$

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

$$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)))$$

$= [(\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H \wedge Q \wedge D) \Rightarrow (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H \wedge Q)]$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))\ \wedge$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )\ )$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))\ ) \wedge$

$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$(\ \forall\, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ ) \wedge$

$(\ \forall\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$(\ \forall\, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

$(\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ )$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge \mathbf{(}\ \forall\ h, t \bullet R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow$

$\quad (\exists\ \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))\ \mathbf{)}$

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

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

$\Rightarrow$ [(1.14)]

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

Lemma 1.9.

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, j, \underline{v}, [w'], [q], [k], [w]) \Rightarrow$
$\quad (\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$
$\quad\quad H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))$

Proof.

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v}', \underline{p}, j, \underline{v}, [w'], [q], [k], [w])$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge$
$\quad \mathbf{(}\ \forall\ t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow$
$\quad\quad (\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$
$\quad\quad H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))\ \mathbf{)}$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \wedge$
$\quad \mathbf{(}\ \forall\ t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow$
$\quad\quad (\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$
$\quad\quad H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))\ \mathbf{)} \wedge$
$\quad \mathbf{(}\ K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(j, h) \wedge K(\underline{v}, t) \Rightarrow$
$\quad\quad (\exists\ \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{w}' \in [w'] \wedge \underline{q} \in [q] \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge$
$\quad\quad H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))\ \mathbf{)}$

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

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

($K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t))$ **)**

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

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$ **)** □

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

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

= [definition of composition]

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

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

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

= [Lemma 1.2]

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

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

= [rewriting in prenex normal form]

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

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

= [rearranging]

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

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

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

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

= [definition of composition]

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

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

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

= [$K(\underline{v}, t) \Rightarrow (\exists\, t \bullet K(\underline{v}, t))$]

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

= [Lemma 1.3]

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

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

= [rewriting in prenex normal form]

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

$\underline{w} \in [w] \wedge H(\underline{w}, t)$ **)**

= [rearranging]

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

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

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

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

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

= [definition of composition]

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

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

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

= [Lemma 1.4]

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

$(\exists\, \underline{j}, \underline{v} \bullet \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))$ **)**

= [rewriting in prenex normal form]

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

$\underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]))$

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

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

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

= [Lemma 1.5]

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

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

= [rearranging]

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

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

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

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

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

= [definition of composition]

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

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

$(\exists \underline{v}, \underline{j} \bullet H^{\bullet}(([v], [w]), \underline{v}) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge (\exists h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge$

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

= [$K(\underline{v}, t) \wedge R_{Op}(\underline{j}, h) \Rightarrow (\exists h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$]

$(\exists \underline{v}, \underline{j} \bullet H^{\bullet}(([v], [w]), \underline{v}) \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

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

= [Lemma 1.6]

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

$K(\underline{v}, t) \wedge R_{Op}(j, h) \wedge (\exists\, \underline{k}, \underline{w} \bullet \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t))$ **)**

= [rewriting in prenex normal form]

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

$K(\underline{v}, t) \wedge R_{Op}(j, h) \wedge \underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t)$ **)**

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

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

$j \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(j, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge K(\underline{v}, t) \wedge R_{Op}(j, h) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t)$ **)**

= [$K(\underline{v}, t) \Rightarrow (\exists\, t \bullet K(\underline{v}, t))$]

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

$j \in [j] \wedge \underline{v} \in [v] \wedge RQ_{Op}(j, \underline{v}, [k], [w]) \wedge QR_{Op}([j], [k]) \wedge K(\underline{v}, t) \wedge R_{Op}(j, h) \wedge$

$\underline{k} \in [k] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t)$ **)**

[rearranging, idempotency]

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

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

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

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

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

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

($H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$**)**

= [definition of composition]

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

$K^{\bullet}(([v], [w]), \underline{w}) \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$ **)**

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

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

$K^{\bullet}(([v], [w]), \underline{w}) \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$ **)**

$= [\text{Lemma 1.7}]$

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

$K^{\bullet}(([v], [w]), \underline{w}) \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$(\exists\, \underline{v'}, \underline{p}, \underline{j}, \underline{v} \bullet \underline{v'} \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v'}, t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v'}, \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]))$)

$= [\text{rewriting in prenex normal form}]$

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

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

$D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge \underline{v'} \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v'}, t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v'}, \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w])$)

$= [\text{Lemma 1.8}]$

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

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

$D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge \underline{v'} \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v'}, t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v'}, \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

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

$= [\text{Lemma 1.5}]$

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

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

$D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge \underline{v'} \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v'}, t') \wedge$

$V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge VD_{Op}(\underline{v'}, \underline{p}, \underline{j}, \underline{v}, [w'], [q], [k], [w]) \wedge$

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

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

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

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

$DK_{Op}([v], [w]) \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w'}, t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$\underline{v'} \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge K(\underline{v'}, t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

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

= [rearranging]

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

$\underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

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

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

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

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

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

($K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$**)**

= [definition of composition]

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

$D^{\bullet}{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge$

$R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$**)**

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

$(\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v} \bullet \underline{v} \in [v] \wedge$ **(**$\exists\, t \bullet K(\underline{v}, t)$**)** $\wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

$\underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$ **(**$\exists\, h, t \bullet R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)) \wedge RQ_{Op}(\underline{j}, \underline{v}, [k], [w]) \wedge$

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

($\exists\, t', s, h, t \bullet K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$**)** $\wedge$

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

$DK_{Op}([v'], [w']) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$)

= [$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \Rightarrow$ **(** $(\exists\, t', s, h, t \bullet K' \wedge V \wedge R \wedge K) \wedge (\exists\, h, t \bullet R \wedge K) \wedge (\exists\, t \bullet K)$ **)**]

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

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

$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

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

$DK_{Op}([v'], [w']) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t)$ **)**

= [Lemma 1.9]

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

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

$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

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

$DK_{Op}([v'], [w']) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$) **)**

= [rewriting in prenex normal form]

($\exists\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet \underline{v} \in [v] \wedge KH(\underline{v}, [w]) \wedge HK([v], [w]) \wedge DK_{Op}([v], [w]) \wedge$

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

$\underline{v}' \in [v'] \wedge \underline{p} \in [p] \wedge \underline{j} \in [j] \wedge \underline{v} \in [v] \wedge$

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

$DK_{Op}([v'], [w']) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge$

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

$H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t)$ **)**

[rearranging, idempotency]

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

$\underline{v} \in [v] \wedge \underline{w} \in [w] \wedge H(\underline{w}, t) \wedge Q_{Op}(\underline{k}, h, \underline{w}, t) \wedge D_{Op}(\underline{w}', t', \underline{q}, s; \underline{k}, h, \underline{w}, t) \wedge$

$K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t) \wedge HK([v'], [w']) \wedge DK_{Op}([v'], [w']) \wedge$

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

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

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

We now state conditions (1.30) to (1.33), which the initialisation and step relations of the refinement from *Univ* to *Ref* and the retrenchment from *Univ* to *Ret* must satisfy.

$$Init_T(\underline{v}') \Rightarrow (\exists\, v', w' \bullet H^\bullet(([v'], [w']), \underline{v}')) \tag{1.30}$$

$$\begin{aligned} &H^\bullet(([v], [w]), \underline{v}) \wedge Q^\bullet{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow \\ &\quad (\exists\, v', w', p, q \bullet H^\bullet(([v'], [w']), \underline{v}') \vee \\ &\quad\quad D^\bullet{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})) \end{aligned} \tag{1.31}$$

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

$$\begin{aligned} &K^\bullet(([v], [w]), \underline{w}) \wedge R^\bullet{}_{Op}(([j], [k]), \underline{k}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \Rightarrow \\ &\quad (\exists\, v', w', p, q \bullet K^\bullet(([v'], [w']), \underline{w}') \wedge V^\bullet{}_{Op}(([p], [q]), \underline{q})) \end{aligned} \tag{1.33}$$

Now we give the transitions of *Univ*. For each operation Op_U a typical transition is u -(i, Op_U, o)-› u' or, more explicitly,

$$([v], [w]) \text{-}(([j], [k]), Op_U, ([p], [q]))\text{-›} ([v'], [w']) \tag{1.34}$$

iff [v], [w], [j], [k], [p], [q], [v'], [w'] satisfy

$$\begin{aligned} &\mathbf{(}\exists\, \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^\bullet(([v], [w]), \underline{w}) \wedge R^\bullet{}_{Op}(([j], [k]), \underline{k}) \wedge \\ &\quad\quad stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge K^\bullet(([v'], [w']), \underline{w}') \wedge V^\bullet{}_{Op}(([p], [q]), \underline{q}))\mathbf{)} \qquad \text{(a)} \\ &\vee \\ &\mathbf{(}\exists\, \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^\bullet(([v], [w]), \underline{v}) \wedge Q^\bullet{}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v}) \wedge \\ &\quad stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge (H^\bullet(([v'], [w']), \underline{v}') \vee \\ &\quad D^\bullet{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}))\mathbf{)} \qquad \text{(b)} \end{aligned} \tag{1.35}$$

The initialization predicate $Init_U(u')$ sets u' to any value ([v'], [w']) for which

$$(\exists\, \underline{w}' \bullet Init_F(\underline{w}') \wedge K^\bullet(([v'], [w']), \underline{w}')) \vee (\exists\, \underline{v}' \bullet Init_T(\underline{v}') \wedge H^\bullet(([v'], [w']), \underline{v}')) \tag{1.36}$$

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

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

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

$$Init_F(\underline{w}') \Rightarrow (\exists\, u' \bullet Init_U(u') \wedge K^\bullet(u', \underline{w}')) \,. \tag{1.37}$$

Let $\underline{w}'$ be an initial value. By (1.32) we have values, v' and w' say, for which $K^\bullet(([v'], [w']), \underline{w}')$ holds. Let $u' = ([v'], [w'])$. Then, since $Init_F(\underline{w}')$ holds, $Init_U(u')$ holds by (1.36). Hence the consequent of (1.37) holds as required.

Now consider the Op PO

$$\begin{aligned} &K^\bullet(u, \underline{w}) \wedge R^\bullet{}_{Op}(i, \underline{k}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', q) \Rightarrow \\ &\qquad (\exists\, u', o \bullet stp_{Op_U}(u, i, u', o) \wedge K^\bullet(u', \underline{w}') \wedge V^\bullet{}_{Op}(o, q)) \,. \end{aligned} \tag{1.38}$$

Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From (1.33) we know there are values, which we fix as v', w', p and q, such that $K^\bullet(([v'], [w']), \underline{w}')$ and $V^\bullet{}_{Op}(([p], [q]), q)$ both hold. Let $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then (1.35a) and thus $stp_{Op_U}(u, i, u', o)$ holds. Hence (1.38) holds.

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

$$Init_T(\underline{v}') \Rightarrow (\exists\, u' \bullet Init_U(u') \wedge H^\bullet(u', \underline{v}')) \,. \tag{1.39}$$

Assume the antecedent. By (1.30) we have values, v' and w' say, for which $H^\bullet(([v'], [w']), \underline{v}')$ holds. Let $u' = ([v'], [w'])$. Then, since $Init_T(\underline{v}')$ holds, $Init_U(u')$ holds by (1.36). Hence the consequent of (1.39) holds as required.

For the Op PO we have to establish that

$$\begin{aligned} &H^\bullet(u, \underline{v}) \wedge Q^\bullet{}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \Rightarrow \\ &\qquad (\exists\, u', o \bullet stp_{Op_U}(u, i, u', o) \wedge (H^\bullet(u', \underline{v}') \vee D^\bullet{}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) \,. \end{aligned} \tag{1.40}$$

Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. From (1.31) we know there are values, which we fix as v', w', p and q, such that $H^\bullet(([v'], [w']), \underline{v}') \vee D^\bullet{}_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds. Let $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then (1.35b) and thus $stp_{Op_U}(u, i, u', o)$ holds. Hence (1.40) holds. Done.

The final piece of the construction is to show that either the composition of the *Univ* to *Ret* retrenchment and the *Ret* to *Conc* refinement on the one hand, or the *Univ* to *Ref*

refinement and the *Ref* to *Conc* retrenchment on the other, do indeed yield a retrenchment from *Univ* to *Conc*. For if so then (1.25), (1.27) and (1.29) show they both give the *same* retrenchment, with retrieves, within, and concedes relations given respectively by G, P_{Op} and C_{Op}.

To prove the Init PO we have to show

$$Init_C(t') \Rightarrow (\exists\, u' \bullet Init_U(u') \wedge G(u', t')) \,. \tag{1.41}$$

Assume $Init_C(t')$. Then the Init PO for the refinement from *Ret* to *Conc*,

$$Init_C(t') \;\Rightarrow\; (\exists\, \underline{v}' \bullet Init_T(\underline{v}') \wedge K(\underline{v}', t')) \,, \tag{1.42}$$

implies the existence of a state, let it be $\underline{v}'$, such that $Init_T(\underline{v}')$ and $K(\underline{v}', t')$ are true. From $Init_T(\underline{v}')$ we can assert, by (1.39), u' for which $Init_U(u')$ and $H^\bullet(u', \underline{v}')$ hold. All we need now is $G(u', t')$, and this follows from $H^\bullet(u', \underline{v}');K(\underline{v}', t')$. Done.

Next consider the Op PO. Here we have to show

$$\begin{aligned} &G(u, t) \wedge P_{Op}(i, h, u, t) \wedge stp_{Op_C}(t, h, t', s) \Rightarrow \\ &\qquad (\exists\, u', o \bullet stp_{Op_U}(u, i, u', o) \wedge (G(u', t') \vee C_{Op}(u', t', o, s; i, h, u, t))) \,. \end{aligned} \tag{1.43}$$

Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. Now $P_{Op}(i, h, u, t) = (H^\bullet(u, \underline{v}) \wedge Q^\bullet{}_{Op}(i, \underline{j}, u, \underline{v}));(R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$. Thus we have K, R_{Op} and stp_{Op_C}. These are the antecedents of the Op PO for the refinement from *Ret* to *Conc*,

$$\begin{aligned} &K(\underline{v}, t) \wedge R_{Op}(\underline{j}, h) \wedge stp_{Op_C}(t, h, t', s) \;\Rightarrow \\ &\qquad (\exists\, \underline{v}', \underline{p} \bullet stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s)) \,. \end{aligned} \tag{1.44}$$

Hence we have values, $\underline{v}'$ and $\underline{p}$ say, such that $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $K(\underline{v}', t')$ and $V_{Op}(\underline{p}, s)$ hold. So stp_{Op_T}, $H^\bullet$ and $Q^\bullet{}_{Op}$ are true. These are the antecedents of PO (1.40). Therefore we have values, u' and o say, such that $stp_{Op_U}(u, i, u', o)$, which we require, and $H^\bullet(u', \underline{v}') \vee D^\bullet{}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$ hold. It remains to show $G' \vee C_{Op}$. This follows from $H^{\bullet\prime} \vee D^\bullet{}_{Op}$. Assume $H^\bullet(u', \underline{v}')$. Then $H^\bullet(u', \underline{v}');K(\underline{v}', t')$ gives $G(u', t')$. Alternatively assume $D^\bullet{}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$. Then $(H^\bullet(u, \underline{v}) \wedge Q^\bullet{}_{Op}(i, \underline{j}, u, \underline{v}) \wedge D^\bullet{}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v});(K(\underline{v}', t') \wedge V_{Op}(\underline{p}, s) \wedge R_{Op}(\underline{j}, h) \wedge K(\underline{v}, t))$ gives $C_{Op}(u', t', o, s; i, h, u, t)$. 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 (U11) of *Univ*.

$$Init_{U}(u') \Rightarrow \big((\exists\, \underline{w}' \bullet Init_{F}(\underline{w}') \wedge K^{\bullet}(u', \underline{w}')) \vee (\exists\, \underline{v}' \bullet Init_{T}(\underline{v}') \wedge H^{\bullet}(u', \underline{v}')) \big) \tag{U1}$$

$$\begin{aligned} &stp_{Op_U}(u, i, u', o) \Rightarrow \\ &\quad \big((\exists\, \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K^{\bullet}(u, \underline{w}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \\ &\qquad K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q})) \;\vee \\ &\quad (\exists\, \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \\ &\qquad (H^{\bullet}(u', \underline{v}') \vee D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))) \big) \end{aligned} \tag{U2}$$

$$K^{\bullet}(u', w') \wedge K^{\bullet}(u', \underline{w}') \Rightarrow w' \sim \underline{w}' \tag{U3}$$

$$(H^{\bullet}(u', v') \vee D^{\bullet}_{Op}(u', v', ...)) \wedge (H^{\bullet}(u', \underline{v}') \vee D^{\bullet}_{Op}(u', \underline{v}', ...)) \Rightarrow v' \sim \underline{v}' \tag{U4}$$

$$V^{\bullet}_{Op}(o, q) \wedge V^{\bullet}_{Op}(o, \underline{q}) \Rightarrow q \sim \underline{q} \tag{U5}$$

$$D^{\bullet}_{Op}(..., o, p; ...) \wedge D^{\bullet}_{Op}(..., o, \underline{p}; ...) \Rightarrow p \sim \underline{p} \tag{U6}$$

$$H^{\bullet}(u', \underline{v}') \Rightarrow (\exists\, \underline{w} \bullet K^{\bullet}(u', \underline{w}')) \tag{U7}$$

$$H^{\bullet}(u', \underline{v}') \wedge K^{\bullet}(u', \underline{w}') \Rightarrow H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{v}') \tag{U8}$$

$$\begin{aligned} &H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \Rightarrow \\ &\quad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge K^{\bullet}(u, \underline{w})) \end{aligned} \tag{U9}$$

$$\begin{aligned} &K^{\bullet}(u', \underline{w}') \wedge V^{\bullet}_{Op}(o, \underline{q}) \wedge R^{\bullet}_{Op}(i, \underline{k}) \wedge K^{\bullet}(u, \underline{w}) \wedge \\ &\quad H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge D^{\bullet}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}) \Rightarrow \\ &\qquad H^{\bullet}(([\underline{v}], [\underline{w}]), \underline{v}) \wedge Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v}) \wedge \\ &\qquad\quad D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})) \end{aligned} \tag{U10}$$

$$V^{\bullet}_{Op}(o, q) \Rightarrow (\exists\, p \bullet V^{\bullet}_{Op}(([p], [q]), q)) \tag{U11}$$

Proofs.

(U1): Assume $Init_{U}(u')$ and let $u' = ([v'], [w'])$. Then the consequent follows immediately from (1.36).

(U2): Assume $stp_{Op_U}(u, i, u', o)$ and let $u = ([v], [w])$, $i = ([j], [k])$, $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then the consequent follows immediately from (1.35).

(U3): Assume the antecedents and let $u' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. By (1.18) $w' \in [\underline{\underline{w}}']$ and $\underline{w}' \in [\underline{\underline{w}}']$. Thus $w' \sim \underline{w}'$.

(U4): Assume the antecedents and let $u' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$. Now, for each conjunct, either $H^\bullet$ or $D^\bullet_{Op}$ holds, so by (1.19) or (1.23), $v' \in [\underline{\underline{v}}']$ and $\underline{v}' \in [\underline{\underline{v}}']$. Thus $v' \sim \underline{v}'$.

(U5) and (U6): Similar to the previous two proofs.

(U7): Assume $H^\bullet(u', \underline{v}')$ with $u' = ([v'], [w'])$. By (1.19) we have $HK([v], [w])$ and $DK_{Op}([v], [w])$. Moreover, since $w' \in [w']$, it follows from (1.18) that $K^\bullet(([v'], [w']), w')$ is true. Thus the consequent of (U7) holds.

(U8): Assume the antecedents and let $u' = ([v'], [w'])$. From $H^\bullet(([v'], [w'])\ \underline{v}')$ and (1.19), $\underline{v}' \sim v'$; from $K^\bullet(([v'], [w']), \underline{w}')$ and (1.18), $\underline{w}' \sim w'$. Thus, because $H^\bullet(([v'], [w'])\ \underline{v}')$ holds, $H^\bullet(([\underline{v}'], [\underline{w}'])\ \underline{v}')$ also holds.

(U9): Assume the antecedents and let $u' = ([v'], [w'])$, $o = ([p], [q])$, $i = ([j], [k])$ and $u = ([v], [w])$. From $H^\bullet(u, \underline{v})$, by (1.19), $HK([v], [w])$ and $DK_{Op}([v], [w])$ hold, and since $w \in [w]$, (1.18) yields $K^\bullet(u', w')$. From $Q^\bullet_{Op}(i, \underline{j}, u, \underline{v})$, by (1.21), $QR_{Op}([j], [k])$ holds, and since $k \in [k]$, (1.20) yields $R^\bullet_{Op}(i, k)$. Similarly, from $D^\bullet_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v})$, by (1.23), $DV_{Op}([p], [q])$ holds, and since $q \in [q]$, (1.22) yields $V^\bullet_{Op}(o, q)$. From (1.23) we also get $HK([v'], [w'])$ and $DK_{Op}([v'], [w'])$, and since $w' \in [w']$, by (1.18) $K^\bullet(u, w)$ holds. Thus there are values, w', q, k and w, such that the consequent of (U9) holds.

(U10): Assume the antecedents and let $u' = ([v'], [w'])$, $o = ([p], [q])$, $i = ([j], [k])$ and $u = ([v], [w])$. Then, $K^{\bullet\prime}$ and (1.18) say $\underline{w}' \sim w'$; $V^\bullet_{Op}$ and (1.22) say $\underline{q} \sim q$; $R^\bullet_{Op}$ and (1.20) say $\underline{k} \sim k$; $K^\bullet$ and (1.18) say $\underline{w} \sim w$. Similarly, $D^\bullet_{Op}$ and (1.23) say $\underline{v}' \sim v'$, $\underline{p} \sim p$, $\underline{j} \sim j$ and $\underline{v} \sim v$. Hence, since $H^\bullet(([v], [w]), \underline{v})$, $Q^\bullet_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ and $D^\bullet_{Op}(([v'], [w']), \underline{v}', ([p], [q]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v}))$ hold, $H^\bullet(([\underline{v}], [\underline{w}]), \underline{v})$, $Q^\bullet_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ and $D^\bullet_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v}))$ hold.

(U11): Assume $V^\bullet_{Op}(o, q)$ with $o = ([\underline{p}], [\underline{q}])$. Then by (1.22) $\underline{q} \sim q$. So as $V^\bullet_{Op}(([\underline{p}], [\underline{q}]), q)$ holds, $V^\bullet_{Op}(([\underline{p}], [q]), q)$ and thus the consequent of (U11) holds too.

Part (2) of Theorem 1.1 is concerned with the refinement from *Univ* to *Xtra*. Suppose there is an I/O-filtered refinement from *Xtra* to *Ref* given by retrieve relation $K\tilde{}$, within

relation $R\tilde{}$, and nevertheless relation $V\tilde{}$; and a retrenchment from *Xtra* to *Ret* given by retrieve relation $H\tilde{}$, within relation $Q\tilde{}$, and concedes relation $D\tilde{}$. Let the state, input and output spaces of *Xtra* be given by $u\tilde{} \in \mathsf{U}\tilde{}$, $i\tilde{} \in \mathsf{I}\tilde{}$, $o\tilde{} \in \mathsf{O}\tilde{}$ and let the initialisation and step predicates for *Xtra* be $Init_X$ and stp_{Op_X}. Finally let *Xtra* have properties (X1) to (X11) below.

$$Init_X(u\tilde{}') \Rightarrow \big((\exists\, \underline{w}' \bullet Init_F(\underline{w}') \wedge K\tilde{}(u\tilde{}', \underline{w}')) \vee (\exists\, \underline{v}' \bullet Init_T(\underline{v}') \wedge H\tilde{}(u\tilde{}', \underline{v}')) \big) \quad \text{(X1)}$$

$$\begin{aligned} &stp_{Op_X}(u\tilde{}, i\tilde{}, u\tilde{}', o\tilde{}) \Rightarrow \\ &\quad \big((\exists\, \underline{w}, \underline{k}, \underline{w}', \underline{q} \bullet K\tilde{}(u\tilde{}, \underline{w}) \wedge R\tilde{}_{Op}(i\tilde{}, \underline{k}) \wedge stp_{Op_F}(\underline{w}, \underline{k}, \underline{w}', \underline{q}) \wedge \\ &\qquad K\tilde{}(u\tilde{}', \underline{w}') \wedge V\tilde{}_{Op}(o\tilde{}, \underline{q})) \ \vee \\ &\qquad (\exists\, \underline{v}, \underline{j}, \underline{v}', \underline{p} \bullet H\tilde{}(u\tilde{}, \underline{v}) \wedge Q\tilde{}_{Op}(i\tilde{}, \underline{j}, u\tilde{}, \underline{v}) \wedge stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p}) \wedge \\ &\qquad (H\tilde{}(u\tilde{}', \underline{v}') \vee D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v}))) \big) \end{aligned} \quad \text{(X2)}$$

$$K\tilde{}(u\tilde{}', w') \wedge K\tilde{}(u\tilde{}', \underline{w}') \Rightarrow w' \sim \underline{w}' \quad \text{(X3)}$$

$$(H\tilde{}(u\tilde{}', v') \vee D\tilde{}_{Op}(u\tilde{}', v', ...)) \wedge (H\tilde{}(u\tilde{}', \underline{v}') \vee D\tilde{}_{Op}(u\tilde{}', \underline{v}', ...)) \Rightarrow v' \sim \underline{v}' \quad \text{(X4)}$$

$$V\tilde{}_{Op}(o\tilde{}, q) \wedge V\tilde{}_{Op}(o\tilde{}, \underline{q}) \Rightarrow q \sim \underline{q} \quad \text{(X5)}$$

$$D\tilde{}_{Op}(..., o\tilde{}, p; ...) \wedge D\tilde{}_{Op}(..., o\tilde{}, \underline{p}; ...) \Rightarrow p \sim \underline{p} \quad \text{(X6)}$$

$$H\tilde{}(u\tilde{}', \underline{v}') \Rightarrow (\exists\, \underline{w}' \bullet K\tilde{}(u\tilde{}', \underline{w}')) \quad \text{(X7)}$$

$$H\tilde{}(u\tilde{}', \underline{v}') \wedge K\tilde{}(u\tilde{}', \underline{w}') \Rightarrow H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{v}') \quad \text{(X8)}$$

$$\begin{aligned} &H\tilde{}(u\tilde{}, \underline{v}) \wedge Q\tilde{}_{Op}(i\tilde{}, \underline{j}, u\tilde{}, \underline{v}) \wedge D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v}) \Rightarrow \\ &\quad (\exists\, \underline{w}', \underline{q}, \underline{k}, \underline{w} \bullet K\tilde{}(u\tilde{}', \underline{w}') \wedge V\tilde{}_{Op}(o\tilde{}, \underline{q}) \wedge R\tilde{}_{Op}(i\tilde{}, \underline{k}) \wedge K\tilde{}(u\tilde{}, \underline{w})) \end{aligned} \quad \text{(X9)}$$

$$\begin{aligned} &K\tilde{}(u\tilde{}', \underline{w}') \wedge V\tilde{}_{Op}(o\tilde{}, \underline{q}) \wedge R\tilde{}_{Op}(i\tilde{}, \underline{k}) \wedge K\tilde{}(u\tilde{}, \underline{w}) \wedge \\ &\quad H\tilde{}(u\tilde{}, \underline{v}) \wedge Q\tilde{}_{Op}(i\tilde{}, \underline{j}, u\tilde{}, \underline{v}) \wedge D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v}) \Rightarrow \\ &\qquad H^{\bullet}(([\underline{v}], [\underline{w}]), \underline{v}) \wedge Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v}) \wedge \\ &\qquad\quad D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v}) \end{aligned} \quad \text{(X10)}$$

$$V\tilde{}_{Op}(o\tilde{}, q) \Rightarrow (\exists\, p \bullet V^{\bullet}_{Op}(([p], [q]), q)) \quad \text{(X11)}$$

Notice properties (U1) to (U11)correspond to properties (X1) to (X11). 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°, R°_{Op}, V°_{Op}, and prove that they are the retrieve, within and nevertheless relations of the desired refinement.

$$
\begin{aligned}
&K^{\circ}(u, \tilde{u}) \;=\; K^{\circ}(([v], [w]), \tilde{u}) \;= \\
&\quad (\forall\, \underline{w} \bullet K^{\tilde{}}(\tilde{u}, \underline{w}) \Rightarrow K^{\bullet}(([v], [w]), \underline{w})) \;\wedge \\
&\quad (\forall\, \underline{v} \bullet H^{\tilde{}}(\tilde{u}, \underline{v}) \Rightarrow H^{\bullet}(([v], [w]), \underline{v}) \;\wedge \\
&\quad (\forall\, \underline{v}, \underline{\tilde{o}}, \underline{p}, \underline{\tilde{i}}, \underline{j}, \underline{\tilde{u}}, \underline{v} \bullet H^{\tilde{}}(\underline{\tilde{u}}, \underline{v}) \wedge Q^{\tilde{}}_{Op}(\underline{\tilde{i}}, \underline{j}, \underline{\tilde{u}}, \underline{v}) \wedge \\
&\qquad D^{\tilde{}}_{Op}(\tilde{u}, \underline{v}, \underline{\tilde{o}}, \underline{p}; \underline{\tilde{i}}, \underline{j}, \underline{\tilde{u}}, \underline{v}) \Rightarrow \\
&\qquad\quad (\exists\, \underline{o}, \underline{i}, \underline{u} \bullet H^{\bullet}(\underline{u}, \underline{v}) \wedge Q^{\bullet}_{Op}(\underline{i}, \underline{j}, \underline{u}, \underline{v}) \wedge D^{\bullet}_{Op}(([v], [w]), \underline{v}, \underline{o}, \underline{p}; \underline{i}, \underline{j}, \underline{u}, \underline{v}))) \qquad (1.45)
\end{aligned}
$$

$$
\begin{aligned}
&R^{\circ}_{Op}(i, \tilde{i}) \;=\; R^{\circ}_{Op}(([j], [k]), \tilde{i}) \;= \\
&\quad (\forall\, \underline{k} \bullet R^{\tilde{}}_{Op}(\tilde{i}, \underline{k}) \Rightarrow R^{\bullet}_{Op}(([j], [k]), \underline{k})) \;\wedge \\
&\quad (\forall\, \underline{j}, \underline{v}, u, \tilde{u} \bullet K^{\circ}(u, \tilde{u}) \Rightarrow \\
&\qquad (\, H^{\tilde{}}(\tilde{u}, \underline{v}) \wedge Q^{\tilde{}}_{Op}(\tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \Leftrightarrow H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(([j], [k]), \underline{j}, u, \underline{v}) \,)) \qquad (1.46)
\end{aligned}
$$

$$
\begin{aligned}
&V^{\circ}_{Op}(o, \tilde{o}) \;=\; V^{\circ}_{Op}(([p], [q]), \tilde{o}) \;= \\
&\quad (\forall\, \underline{q} \bullet V^{\tilde{}}_{Op}(\tilde{o}, \underline{q}) \Rightarrow V^{\bullet}_{Op}(([p], [q]), \underline{q})) \;\wedge \\
&\quad (\forall\, \underline{v}', \underline{p}, \underline{j}, \underline{v}, u', \tilde{u}', i, \tilde{i}, u, \tilde{u} \bullet H^{\tilde{}}(\tilde{u}, \underline{v}) \wedge Q^{\tilde{}}_{Op}(\tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge \\
&\qquad D^{\tilde{}}_{Op}(\tilde{u}', \underline{v}', \tilde{o}, \underline{p}; \tilde{i}, \underline{j}, \tilde{u}, \underline{v}) \wedge K^{\circ}(u', \tilde{u}') \wedge R^{\circ}_{Op}(i, \tilde{i}) \wedge K^{\circ}(u, \tilde{u}) \Rightarrow \\
&\qquad\quad H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}_{Op}(i, \underline{j}, u, \underline{v}) \wedge D^{\bullet}_{Op}(u', \underline{v}', ([p], [q]), \underline{p}; i, \underline{j}, u, \underline{v}))) \qquad (1.47)
\end{aligned}
$$

We start by showing the above satisfy the inclusions stated in Theorem 5.1.

Take $K^{\circ}(u, \tilde{u}); K^{\tilde{}}(\tilde{u}, \underline{w}) \Rightarrow K^{\bullet}(u, \underline{w})$. Assume the antecedents with $u = ([v], [w])$. Then the consequent follows from the first conjunct of (1.45). Similar arguments establish $R^{\circ}; R^{\tilde{}} \Rightarrow R^{\bullet}$, $V^{\circ}; V^{\tilde{}} \Rightarrow V^{\bullet}$.

Now consider $K^{\circ}(u, \tilde{u}); H^{\tilde{}}(\tilde{u}, \underline{v}); \Rightarrow H^{\bullet}(u, \underline{v})$. Assume the antecedents and let $u = ([v], [w])$. Then the consequent follows from the second conjunct of (1.45).

Next take $(K^{\circ}(u, u^{\sim}) \wedge R^{\circ}{}_{Op}(i, i^{\sim}));(H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}{}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})) \Rightarrow (H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}{}_{Op}(i, \underline{j}, u, \underline{v}))$. Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. Then the consequent follows from the second conjunct of (1.46).

Finally take $(K^{\circ}(u', u^{\sim\prime}) \wedge V^{\circ}{}_{Op}(o, o^{\sim}) \wedge R^{\circ}{}_{Op}(i, i^{\sim}) \wedge K^{\circ}(u, u^{\sim}));(H^{\sim}(u^{\sim}, \underline{v}) \wedge Q^{\sim}{}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v}) \wedge D^{\sim}{}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v})) \Rightarrow (H^{\bullet}(u, \underline{v}) \wedge Q^{\bullet}{}_{Op}(i, \underline{j}, u, \underline{v}) \wedge D^{\bullet}{}_{Op}(u', \underline{v}', o, \underline{p}; i, \underline{j}, u, \underline{v}))$. Assume the antecedents with $u' = ([v'], [w'])$, $o = ([p], [q])$, $i = ([j], [k])$ and $u = ([v], [w])$. Then the consequent follows from the second conjunct of (1.47).

To discharge the POs for the refinement from *Univ* to *Xtra*, we will use the following lemmas.

Lemma 1.10. Suppose $H^{\bullet}(([v'], [w']), v')$ and $K^{\bullet}(([\underline{v}'], [w']), w')$ hold. Then $v' \sim \underline{v}'$.

Proof. From $H^{\bullet}(([v'], [w']), v')$, using (1.19), we get $KH(v', [w'])$ and, picking a suitable value $\underline{t}'$, $K(v', \underline{t}')$. Then by (1.10), we can pick a value, $\underline{w}'$ say, such that $H(\underline{w}', \underline{t}')$ holds, with $\underline{w}' \in [w']$. From $K^{\bullet}(([\underline{v}'], [w']), w')$, by (1.18), we get $HK(([\underline{v}'], [w']))$. Therefore because we have $H(\underline{w}', \underline{t}')$ and $\underline{w}' \in [w']$, by (1.11) we can choose a value, let it be $\underline{v}'$, for which $K(\underline{v}', \underline{t}')$ and $\underline{v}' \in [\underline{v}']$ are true. Now, $H(\underline{w}', \underline{t}')$, $K(v', \underline{t}')$ and $K(\underline{v}', \underline{t}')$ all hold. So by (1.4) $v' \sim \underline{v}'$. But $\underline{v}' \in [\underline{v}']$, so $\underline{v}' \sim \underline{v}'$, and thus $v' \sim \underline{v}'$. □

Lemma 1.11. Suppose $D^{\bullet}{}_{Op}(([v'], [w']), v', ([p], [q]), p; ([j], [k]), j, ([v], [w]), v)$ and $K^{\bullet}(([\underline{v}'], [w']), w')$ hold. Then $v' \sim \underline{v}'$.

Proof. From $D^{\bullet}{}_{Op}$, using (1.23), we get $VD_{Op}(v', p, j, v, [w'], [q], [k], [w])$ and, picking suitable values $\underline{t}'$, $\underline{s}$, $\underline{h}$ and $\underline{t}$, $K(v', \underline{t}')$, $V_{Op}(p, \underline{s})$, $R_{Op}(j, \underline{h})$ and $K(v, \underline{t})$. Therefore by (1.16), we have values, which we fix as $\underline{w}'$, $\underline{q}$, $\underline{k}$ and $\underline{w}$, such that $D_{Op}(\underline{w}', \underline{t}', \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})$ holds, with $\underline{w}' \in [w']$. From $K^{\bullet}(([\underline{v}'], [w']), w')$, by (1.18), we get $DK_{Op}(([\underline{v}'], [w']))$. Therefore because we have $D_{Op}(\underline{w}', \underline{t}', \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})$ and $\underline{w}' \in [w']$, by (1.13), we can choose a value, let it be $\underline{v}'$, for which $K(\underline{v}', \underline{t}')$ and $\underline{v}' \in [\underline{v}']$ are true. Now, $D_{Op}(\underline{w}', \underline{t}', \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})$, $K(v', \underline{t}')$ and $K(\underline{v}', \underline{t}')$ hold. So by (1.4) $v' \sim \underline{v}'$. But $\underline{v}' \in [\underline{v}']$, so $\underline{v}' \sim \underline{v}'$, and thus $v' \sim \underline{v}'$. □

Lemma 1.12. Suppose $H^{\bullet}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$, $Q^{\bullet}{}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ and $D^{\bullet}{}_{Op}(([\underset{\sim}{v}'], [\underset{\sim}{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ and $V^{\bullet}{}_{Op}(([p], [\underline{q}]), \underline{q})$ hold. Then $\underline{p} \sim p$.

Proof. From $D^{\bullet}_{Op}$, using (1.23), we get $VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [\underset{\sim}{w}'], [\underline{q}], [\underset{\sim}{k}], [\underset{\sim}{w}])$ and, picking suitable values $\underline{t}'$, $\underline{s}$, $\underline{h}$ and $\underline{t}$, $K(\underline{v}', \underline{t}')$, $V_{Op}(\underline{p}, \underline{s})$, $R_{Op}(\underline{j}, \underline{h})$ and $K(\underline{v}, \underline{t})$. Therefore by (1.16), we have values, which we fix as $\underline{w}'$, $\underline{q}$, $\underline{k}$ and $\underline{w}$, such that $H(\underline{w}, \underline{t})$, $Q_{Op}(\underline{k}, \underline{h}, \underline{w}, \underline{t})$, $D_{Op}(\underline{w}', \underline{t}', \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})$ hold, with $\underline{w}' \in [\underset{\sim}{w}']$, $\underline{q} \in [\underline{q}]$, $\underline{k} \in [\underset{\sim}{k}]$ and $\underline{w} \in [\underset{\sim}{w}]$. Furthermore, from (1.23) we also get $HK([\underset{\sim}{v}'], [\underset{\sim}{w}'])$ and $DK_{Op}([\underset{\sim}{v}'], [\underset{\sim}{w}'])$. Thus since $\underline{w}' \in [\underset{\sim}{w}']$, $K^{\bullet}(([\underset{\sim}{v}'], [\underset{\sim}{w}']), \underline{w}')$ holds by (1.18). Next, from $Q^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ and (1.21), $QR_{Op}([\underset{\sim}{j}], [\underset{\sim}{k}])$ holds. Thus since $\underline{k} \in [\underset{\sim}{k}]$, $R^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{k})$ holds by (1.20). Similarly, from $H^{\bullet}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ and (1.19), $HK([\underset{\sim}{v}], [\underset{\sim}{w}])$ and $DK_{Op}([\underset{\sim}{v}], [\underset{\sim}{w}])$ hold. Thus since $\underline{w} \in [\underset{\sim}{w}]$, $K^{\bullet}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{w})$ holds by (1.18). Finally, from $V^{\bullet}_{Op}(([p], [\underline{q}]), \underline{q})$, by (1.22), we get $DV_{Op}([p], [\underline{q}])$. Therefore, because $\underline{q} \in [\underline{q}]$ and $H(\underline{w}, \underline{t})$, $Q_{Op}(\underline{k}, \underline{h}, \underline{w}, \underline{t})$, $D_{Op}(\underline{w}', \underline{t}', \underline{q}, \underline{s}; \underline{k}, \underline{h}, \underline{w}, \underline{t})$, $K^{\bullet}(([\underset{\sim}{v}'], [\underset{\sim}{w}']), \underline{w}')$, $R^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{k})$ and $K^{\bullet}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{w})$ all hold, by (1.17) we can choose a value, let it be $\underline{p}$, such that $V_{Op}(\underline{p}, \underline{s})$ is true, where $\underline{p} \in [p]$. Now, $D_{Op}(..., \underline{q}, \underline{s}; ...)$, $V_{Op}(\underline{p}, \underline{s})$ and $V_{Op}(\underline{p}, \underline{s})$ hold. Therefore by (1.8), $\underline{p} \sim \underline{p}$. But $\underline{p} \in [p]$, i.e. $\underline{p} \sim p$, thus $\underline{p} \sim p$. □

Lemma 1.13. Suppose $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $D^{\sim}_{Op}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $K^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{w}}')$, $V^{\sim}_{Op}(o^{\sim}, \underline{\underline{q}})$, $R^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$, $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$, $K^{\circ}(([\underset{\sim}{v}'], [\underset{\sim}{w}']), \underline{\underline{u}}^{\sim\prime})$, $R^{\circ}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{\underline{i}}^{\sim})$ and $K^{\circ}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{\underline{u}}^{\sim})$ hold. Then $H^{\bullet}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$, $Q^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ and $D^{\bullet}_{Op}(([\underset{\sim}{v}'], [\underset{\sim}{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$ hold.

Proof. From $H^{\sim}$, $Q^{\sim}_{Op}$, $D^{\sim}_{Op}$, $K^{\sim\prime}$, $V^{\sim}_{Op}$, $R^{\sim}_{Op}$ and $K^{\sim}$, by (X10), $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}_{Op}(([\underline{\underline{j}}], [\underline{\underline{k}}]), \underline{\underline{j}}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{\underline{j}}], [\underline{\underline{k}}]), \underline{\underline{j}}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ hold. Therefore, if we can show $\underline{\underline{v}} \sim \underline{v}$, $\underline{\underline{w}} \sim \underline{w}$, $\underline{\underline{j}} \sim \underline{j}$, $\underline{\underline{k}} \sim \underline{k}$, $\underline{\underline{v}}' \sim \underline{v}'$ and $\underline{\underline{w}}' \sim \underline{w}'$, then $H^{\bullet}(([\underline{v}], [\underline{w}]), \underline{v})$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ and $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ hold as required.First note we have $K^{\circ}(([\underline{v}'], [\underline{w}']), \underline{\underline{u}}^{\sim\prime})$, $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $D^{\sim}_{Op}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$ and $K^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{w}}')$. Hence by (1.45), $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ...)$ and $K^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{\underline{w}}')$ hold. From the former, by (1.23), $\underline{\underline{v}}' \sim \underline{v}'$; from the latter, by (1.18), $\underline{\underline{w}}' \sim \underline{w}'$. Next, $R^{\circ}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{\underline{i}}^{\sim})$, $K^{\circ}(([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{\underline{u}}^{\sim})$, $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$ and (1.46) give $Q^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{j}, ([\underset{\sim}{v}], [\underset{\sim}{w}]), \underline{v})$. Thus by (1.21), $\underline{\underline{j}} \sim \underline{j}$ and $\underline{\underline{v}} \sim \underline{v}$. Similarly, $R^{\circ}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{\underline{i}}^{\sim})$, $R^{\sim}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$ and (1.46) give $R^{\bullet}_{Op}(([\underset{\sim}{j}], [\underset{\sim}{k}]), \underline{\underline{k}})$, so by (1.20) $\underline{\underline{k}} \sim \underline{k}$. Last, $K^{\circ}(([\underline{v}], [\underline{w}]), \underline{\underline{u}}^{\sim})$, $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$ and (1.45) give $K^{\bullet}(([\underline{v}], [\underline{w}]), \underline{\underline{w}})$. Thus by (1.18) $\underline{\underline{w}} \sim \underline{w}$. □

Lemma 1.14. Suppose $Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ and $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ hold. Then $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds.

Proof. From $Q^{\bullet}_{Op}$, by (1.21), we get $\underline{j} \sim j$, $\underline{v} \sim v$, $RQ_{Op}(j, \underline{v}, [k], [w])$ and, for chosen values $\underline{h}$ and $\underline{t}$, $R_{Op}(j, \underline{h})$ and $K(\underline{v}, \underline{t})$. Applying (1.14) then gives $H(\underline{\underline{w}}, \underline{t})$ and $Q_{Op}(\underline{k}, \underline{h}, \underline{\underline{w}}, \underline{t})$, for chosen values $\underline{\underline{w}}$ and $\underline{\underline{k}}$, with $\underline{\underline{w}} \in [w]$ and $\underline{\underline{k}} \in [k]$. From $D^{\bullet}_{Op}$, by (1.23), we get $VD_{Op}(\underline{v}', \underline{p}, \underline{j}, \underline{v}, [\underline{q}], [\underline{w}'], [\underline{q}], [\underline{k}], [\underline{w}])$ and, for chosen values $\underline{\underline{t}}'$, $\underline{\underline{s}}$, $\underline{\underline{h}}$ and $\underline{\underline{t}}$, $K(\underline{v}', \underline{\underline{t}}')$, $V_{Op}(\underline{p}, \underline{\underline{s}})$, $R_{Op}(\underline{j}, \underline{\underline{h}})$ and $K(\underline{v}, \underline{\underline{t}})$. Applying (1.16) then gives $H(\underline{\underset{\sim}{w}}, \underline{\underline{t}})$ and $Q_{Op}(\underline{\underset{\sim}{k}}, \underline{\underline{h}}, \underline{\underset{\sim}{w}}, \underline{\underline{t}})$, for chosen values $\underline{\underset{\sim}{w}}$ and $\underline{\underset{\sim}{k}}$, with $\underline{\underset{\sim}{w}} \in [\underline{w}]$ and $\underline{\underset{\sim}{k}} \in [\underline{k}]$. Hence, as $K(\underline{v}, \underline{t})$, $H(\underline{\underline{w}}, \underline{t})$, $K(\underline{v}, \underline{t})$ and $H(\underline{\underset{\sim}{w}}, \underline{\underline{t}})$ all hold, by (1.5), $\underline{\underline{w}} \sim \underline{\underset{\sim}{w}}$. But $\underline{\underset{\sim}{w}} \sim \underline{w}$, therefore $\underline{\underline{w}} \sim \underline{w}$; and since $\underline{\underline{w}} \sim w$, $\underline{w} \sim w$. Similarly, because $R_{Op}(j, \underline{h})$, $Q_{Op}(\underline{k}, \underline{h}, \underline{\underline{w}}, \underline{t})$, $R_{Op}(j, \underline{\underline{h}})$ and $Q_{Op}(\underline{\underset{\sim}{k}}, \underline{\underline{h}}, \underline{\underset{\sim}{w}}, \underline{\underline{t}})$ hold, by (1.7), $\underline{\underline{k}} \sim \underline{\underset{\sim}{k}}$. But $\underline{\underset{\sim}{k}} \sim \underline{k}$, therefore $\underline{\underline{k}} \sim \underline{k}$; and since and $\underline{\underline{k}} \sim k$, $\underline{k} \sim k$. So using the equivalences we have established, given that $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$ holds, $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ must also hold. □

We can now establish the POs. First, we have the Init PO

$$Init_{X}(u\tilde{}') \Rightarrow (\exists\, u' \bullet Init_{U}(u') \wedge K^{\circ}(u', u\tilde{}')) \,. \tag{1.48}$$

Assume $Init_{X}(u\tilde{}')$. By (X1) either $(\exists\, \underline{w}' \bullet Init_{F}(\underline{w}') \wedge K\tilde{}(u\tilde{}', \underline{w}'))$ or $(\exists\, \underline{v}' \bullet Init_{T}(\underline{v}') \wedge H\tilde{}(u\tilde{}', \underline{v}'))$ is true. Hence there are two cases to consider, one for each disjunct.

Case 1. Assume the first disjunct for suitable value $\underline{w}'$. So we have $Init_{F}(\underline{w}')$ and $K\tilde{}(u\tilde{}', \underline{w}')$. From the former, by (1.32) we have values, which we fix as v' and w', for which $K^{\bullet}(([v'], [w']), \underline{w}')$ holds. Let $u' = ([v'], [w'])$. Then by (1.36) $Init_{U}(u')$ holds.

We now show $K^{\circ}(u', u\tilde{}')$ holds. To do this we establish each conjunct of (1.45) in turn. Take the first conjunct and assume $K\tilde{}(u\tilde{}', \underline{\underline{w}}')$. We have to demonstrate $K^{\bullet}(([v'], [w']), \underline{\underline{w}}')$. Since we also have $K\tilde{}(u\tilde{}', \underline{w}')$, by (X3), $\underline{w}' \sim \underline{\underline{w}}'$. Furthermore, as $K^{\bullet}(([v'], [w']), \underline{w}')$ holds, by (1.18), $HK([v'], [w'])$ and $DK_{Op}([v'], [w'])$ hold and $\underline{w}' \in [w']$. From the latter, since $\underline{w}' \sim \underline{\underline{w}}'$, $\underline{\underline{w}}' \in [w']$. Consequently $K^{\bullet}(([v'], [w']), \underline{\underline{w}}')$ holds as required.

Take the second conjunct and assume $H\tilde{}(u\tilde{}', \underline{\underline{v}}')$. We need to verify $H^{\bullet}(([v'], [w']), \underline{\underline{v}}')$ holds. Since we have $K\tilde{}(u\tilde{}', \underline{w}')$, by (X8), we also have $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$. So if we can

show $\underline{\underline{v'}} \sim v'$ and $\underline{\underline{w'}} \sim w'$, then $H^{\bullet}(([v'], [w']), \underline{\underline{v'}})$ follows. To establish the second equivalence, note we have $K^{\bullet}(([v'], [w']), \underline{w'})$. Hence by (1.18), $\underline{w'} \in [w']$, and thus $\underline{w'} \sim w'$. Now this result means we also have $K^{\bullet}(([v'], [\underline{w'}]), \underline{w'})$. So, given that $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$ holds too, the first equivalence follows from Lemma 1.10. We are done.

To show the third conjunct assume $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge Q^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge D^{\sim}{}_{Op}(u^{\sim\prime}, \underline{\underline{v'}}, \underline{\underline{o}}^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$. This time we need to establish $(\exists\, \underline{\underline{o}}, \underline{\underline{i}}, \underline{\underline{u}} \bullet H^{\bullet}(\underline{\underline{u}}, \underline{\underline{v}}) \wedge Q^{\bullet}{}_{Op}(\underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}) \wedge D^{\bullet}{}_{Op}(([v'], [w']), \underline{\underline{v'}}, \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}))$. Given $H^{\sim} \wedge Q^{\sim}{}_{Op} \wedge D^{\sim}{}_{Op}$, we can use (X9) to assert there are values, which we fix as $\underline{\underline{q}}$, $\underline{\underline{k}}$ and $\underline{\underline{w}}$, such that $V^{\sim}{}_{Op}(\underline{\underline{o}}^{\sim}, \underline{\underline{q}})$, $R^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$ and $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$ hold. We also have $K^{\sim}(u^{\sim\prime}, \underline{w'})$. So by (X10), $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}{}_{Op}(([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}{}_{Op}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}}, ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ hold. We now show $\underline{\underline{v'}} \sim v'$ and $\underline{w'} \sim w'$. To verify the latter, recall we have $K^{\bullet}(([v'], [w']), \underline{w'})$. Hence by (1.18), $\underline{w'} \in [w']$, and thus $\underline{w'} \sim w'$. Next, from this equivalence we can deduce $K^{\bullet}(([v'], [\underline{w'}]), \underline{w'})$. Since $D^{\bullet}{}_{Op}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}}, ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ is true as well, by Lemma 1.11, $\underline{\underline{v'}} \sim v'$. Hence $D^{\bullet}{}_{Op}(([v'], [w']), \underline{\underline{v'}}, ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ holds and, together with $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $Q^{\bullet}{}_{Op}(([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, satisfies the consequent of the third conjunct. This completes the first case.

Case 2. Assume the second disjunct. Hence $Init_{\mathrm{T}}(\underline{\underline{v'}})$ and $H^{\sim}(u^{\sim\prime}, \underline{\underline{v'}})$ hold for suitable value $\underline{\underline{v'}}$. From the latter, using (X7), we can pick a value, $\underline{w'}$ say, such that $K^{\sim}(u^{\sim\prime}, \underline{w'})$ holds. Hence, by (X8), $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$ holds. Let $u' = ([\underline{\underline{v'}}], [\underline{w'}])$. Then by (1.36) $Init_{\mathrm{U}}(u')$ holds.

We now show $K^{\circ}(u', u^{\sim\prime})$ holds by once again establishing each conjunct of (1.45). Take the first conjunct and assume $K^{\sim}(u^{\sim\prime}, \underline{\underline{w'}})$. We want to derive $K^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{w'}})$. We have $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$, so by (1.19) we conclude $HK([\underline{\underline{v'}}], [\underline{w'}])$ and $DK_{Op}([\underline{\underline{v'}}], [\underline{w'}])$ hold. Now, $K^{\sim}(u^{\sim\prime}, \underline{w'})$, $K^{\sim}(u^{\sim\prime}, \underline{\underline{w'}})$ and (X3) assert $\underline{w'} \sim \underline{\underline{w'}}$, so $\underline{\underline{w'}} \in [\underline{w'}]$. Therefore, by (1.18), $K^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{w'}})$ holds as required.

Take the second conjunct and assume $H^{\sim}(u^{\sim\prime}, \underline{\underline{v'}})$. We want to deduce $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$. Now, in addition to $H^{\sim}(u^{\sim\prime}, \underline{\underline{v'}})$ we have $K^{\sim}(u^{\sim\prime}, \underline{w'})$. Therefore (X8) says $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$ holds. Furthermore, we also have $H^{\sim}(u^{\sim\prime}, \underline{v'})$. Hence by (X4) $\underline{v'} \sim \underline{\underline{v'}}$. Thus, since $H^{\bullet}(([\underline{\underline{v'}}], [\underline{w'}]), \underline{\underline{v'}})$ holds, $H^{\bullet}(([\underline{v'}], [\underline{w'}]), \underline{\underline{v'}})$ holds too.

To show the third conjunct assume $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge Q^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}}) \wedge D^{\sim}{}_{Op}(u^{\sim\prime}, \underline{\underline{v}}', \underline{\underline{o}}^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$. Our goal is to establish $(\exists\, \underline{\underline{o}}, \underline{\underline{i}}, \underline{\underline{u}} \bullet H^{\bullet}(\underline{\underline{u}}, \underline{\underline{v}}) \wedge Q^{\bullet}{}_{Op}(\underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}) \wedge D^{\bullet}{}_{Op}(([\underline{v}'], [\underline{w}']), \underline{\underline{v}}', \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}}))$. Since we have $H^{\sim} \wedge Q^{\sim}{}_{Op} \wedge D^{\sim}{}_{Op}$, we can use (X9) to assert there are values, say $\underline{\underline{q}}$, $\underline{\underline{k}}$ and $\underline{\underline{w}}$, such that $V^{\sim}{}_{Op}(\underline{\underline{o}}^{\sim}, \underline{\underline{q}})$, $R^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$ and $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$ are all true. We also have $K^{\sim}(u^{\sim\prime}, \underline{w}')$. So by (X10), $H^{\bullet}(([\underline{v}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}{}_{Op}(([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{v}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}{}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{\underline{k}}]), \underline{j}, ([\underline{v}], [\underline{\underline{w}}]), \underline{\underline{v}})$ hold. Let $\underline{\underline{o}} = ([\underline{p}], [\underline{q}])$, $\underline{\underline{i}} = ([\underline{j}], [\underline{\underline{k}}])$ and $\underline{\underline{u}} = ([\underline{v}], [\underline{\underline{w}}])$. This gives $H^{\bullet}(\underline{\underline{u}}, \underline{\underline{v}})$, $Q^{\bullet}{}_{Op}(\underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})$ and $D^{\bullet}{}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})$. But as we have $D^{\sim}{}_{Op}(u^{\sim\prime}, \underline{v}', \underline{\underline{o}}^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{\underline{j}}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$ and $H^{\sim}(u^{\sim\prime}, \underline{v}')$, by (X4), $\underline{v}' \sim \underline{v}'$. Hence $D^{\bullet}{}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', \underline{\underline{o}}, \underline{\underline{p}}; \underline{\underline{i}}, \underline{\underline{j}}, \underline{\underline{u}}, \underline{\underline{v}})$ holds too and therefore the consequent of the third conjunct holds as required.

Second we validate the Op PO

$$K^{\circ}(u, u^{\sim}) \wedge R^{\circ}{}_{Op}(i, i^{\sim}) \wedge stp_{Op_{\mathrm{X}}}(u^{\sim}, i^{\sim}, u^{\sim\prime}, o^{\sim}) \Rightarrow$$
$$(\exists\, u', o \bullet stp_{Op_{\mathrm{U}}}(u, i, u', o) \wedge K^{\circ}(u', u^{\sim\prime}) \wedge V^{\circ}{}_{Op}(o, o^{\sim})) \,. \qquad (1.49)$$

Assume the antecedents with $u = ([v], [w])$ and $i = ([j], [k])$. By (X2) either $(\exists\, \underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}} \bullet K^{\sim}(u^{\sim}, \underline{\underline{w}}) \wedge R^{\sim}{}_{Op}(i^{\sim}, \underline{\underline{k}}) \wedge stp_{Op_{\mathrm{F}}}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}}) \wedge K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}') \wedge V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}}))$ or $(\exists\, \underline{\underline{v}}, \underline{\underline{j}}, \underline{\underline{v}}', \underline{\underline{p}} \bullet H^{\sim}(u^{\sim}, \underline{\underline{v}}) \wedge Q^{\sim}{}_{Op}(i^{\sim}, \underline{\underline{j}}, u^{\sim}, \underline{\underline{v}}) \wedge stp_{Op_{\mathrm{T}}}(\underline{\underline{v}}, \underline{\underline{j}}, \underline{\underline{v}}', \underline{\underline{p}}) \wedge (H^{\sim}(u^{\sim\prime}, \underline{\underline{v}}') \vee D^{\sim}{}_{Op}(u^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{\underline{p}}; i^{\sim}, \underline{\underline{j}}, u^{\sim}, \underline{\underline{v}}))$ holds. Thus once more there are two cases to consider, one for each disjunct.

Case 1. Assume the first disjunct for values $\underline{\underline{w}}$, $\underline{\underline{k}}$, $\underline{\underline{w}}'$ and $\underline{\underline{q}}$. Hence $K^{\sim}(u^{\sim}, \underline{\underline{w}})$, $R^{\sim}{}_{Op}(i^{\sim}, \underline{\underline{k}})$, $stp_{Op_{\mathrm{F}}}(\underline{\underline{w}}, \underline{\underline{k}}, \underline{\underline{w}}', \underline{\underline{q}})$, $K^{\sim}(u^{\sim\prime}, \underline{\underline{w}}')$ and $V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}})$ all hold. Now, $K^{\sim}(u^{\sim}, \underline{\underline{w}})$, $K^{\circ}(u, u^{\sim})$ and (1.45) give $K^{\bullet}(([v], [w]), \underline{\underline{w}})$. Similarly, $R^{\sim}{}_{Op}(i^{\sim}, \underline{\underline{k}})$, $R^{\circ}{}_{Op}(i, i^{\sim})$ and (1.46) give $R^{\bullet}{}_{Op}(([j], [k]), \underline{\underline{k}})$. Therefore by (1.33), there are values, we choose v', w', p and q, for which $K^{\bullet}(([v'], [w']), \underline{w}')$ and $V^{\bullet}{}_{Op}(([p], [q]), \underline{\underline{q}})$ hold. Let $u' = ([v'], [w'])$ and $o = ([p], [q])$. Then (1.35a) and thus $stp_{Op_{\mathrm{U}}}(u, i, u', o)$ holds.

It remains to show $K^{\circ}(u', u^{\sim\prime})$ and $V^{\circ}{}_{Op}(o, o^{\sim})$ are both true. The proof for $K^{\circ}(u', u^{\sim\prime})$ is the same as for PO (1.48) Case 1.

To verify $V^{\circ}{}_{Op}(o, o^{\sim})$ we establish each conjunct of (1.47) in turn. For the first conjunct we assume $V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}})$ and need to show $V^{\bullet}{}_{Op}(([p], [q]), \underline{\underline{q}})$. We have $V^{\bullet}{}_{Op}(([p], [q]), \underline{\underline{q}})$, so, by (1.22), $DV_{Op}([p], [q])$ holds and $\underline{\underline{q}} \in [q]$. Now since we have $V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}})$ and

$V^{\sim}_{Op}(o^{\sim}, \underline{q})$, by (X5), we know $\underline{q} \sim q$. It therefore follows that $\underline{q} \in [q]$, and thus that $V^{\bullet}_{Op}(([p], [q]), \underline{q})$ holds as required.

For the second conjunct assume its antecedent $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}_{Op}(\underline{i}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $D^{\sim}_{Op}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{p}; \underline{i}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $K^{\circ}(\underline{\underline{u}}', \underline{\underline{u}}^{\sim\prime})$, $R^{\circ}_{Op}(\underline{i}, \underline{i}^{\sim})$ and $K^{\circ}(\underline{\underline{u}}, \underline{\underline{u}}^{\sim})$. Let $\underline{\underline{u}}' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$, $\underline{i} = ([\underline{j}], [\underline{k}])$ and $\underline{\underline{u}} = ([\underline{\underline{v}}], [\underline{\underline{w}}])$. We seek to establish $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([p], [q]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$. By rule (X9) we can derive $K^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{w}}')$, $V^{\sim}_{Op}(o^{\sim}, \underline{q})$, $R^{\sim}_{Op}(\underline{i}^{\sim}, \underline{k})$ and $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$ for chosen values $\underline{\underline{w}}'$, $\underline{q}$, $\underline{k}$ and $\underline{\underline{w}}$. Thus by Lemma 1.13 $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ are true. So to get the desired consequent, all we need do is show $\underline{p} \sim p$ and $\underline{q} \sim q$. First, $V^{\sim}_{Op}(o^{\sim}, \underline{q})$, $V^{\sim}_{Op}(o^{\sim}, \underline{q})$ and (X5) give $\underline{q} \sim \underline{q}$, and as $V^{\bullet}_{Op}(([p], [q]), \underline{q})$ holds, by (1.22), $\underline{q} \sim q$ and thus $\underline{q} \sim q$. From this result it follows that $V^{\bullet}_{Op}(([p], [\underline{q}]), \underline{q})$ must also hold. Hence second, since we also have $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, by Lemma 1.12, $\underline{p} \sim p$. This completes case 1.

Case 2. Assume the second disjunct for values $\underline{v}$, $\underline{j}$, $\underline{v}'$ and $\underline{p}$. Thus firstly $H^{\sim}(u^{\sim}, \underline{v})$ and $Q^{\sim}_{Op}(i^{\sim}, \underline{j}, u^{\sim}, \underline{v})$ hold. From these, $K^{\circ}(u, u^{\sim})$, $R^{\circ}_{Op}(i, i^{\sim})$ and (1.46) we also get $H^{\bullet}(([v], [w]), \underline{v})$ and $Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v})$. Secondly, $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$ and $(H^{\sim}(u^{\sim\prime}, \underline{v}') \vee D^{\sim}_{Op}(u^{\sim\prime}, \underline{v}', o^{\sim}, \underline{p}; i^{\sim}, \underline{j}, u^{\sim}, \underline{v}))$ hold. Since the latter is a disjunction, we break the proof up into two further cases, one for each disjunct.

Case (i). Assume $H^{\sim}(u^{\sim\prime}, \underline{v}')$ holds. By (X7) there is a value, let it be $\underline{w}'$, for which $K^{\sim}(u^{\sim\prime}, \underline{w}')$ holds, and thence by (X8) $H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{v}')$ holds. Let $u' = ([\underline{v}'], [\underline{w}'])$. Then by the same proof as for PO (1.48) case 2, $K^{\circ}(u', u^{\sim\prime})$ holds.

Now consider V°_{Op}. From the structure of (1.47) there are three possibilities: (a) there are no values for which the antecedents of either conjunct are true; (b) there are no values for which the antecedent of the second conjunct is true, but there is a $\underline{q}$ for which $V^{\sim}_{Op}$ is true; (c) there are values for which the antecedent of the second conjunct is true, and thus by (X9) there must be a $\underline{q}$ for which $V^{\sim}_{Op}$ is also true.

Case (a). Let $o = ([\underline{p}], [\underline{q}])$, where $\underline{q} \in \mathsf{Q}_{Op_F}$. (We have assumed such an output exists. If not, we can simply augment the output space of *Ref* with a dummy value and use that.) Then $V^{\circ}_{Op}(o, o\tilde{})$ holds since the antecedent of each conjunct of (1.47) is always false.

Case (b). Suppose $V^{\sim}_{Op}(o\tilde{}, \underline{q})$ holds. Then by (X11) there is a value, which we fix as $\underline{p}$, such that $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{q})$ is true. Let $o = ([\underline{p}], [\underline{q}])$. We must now verify that $V^{\circ}_{Op}(o, o\tilde{})$ holds for this choice of o. We already know the second conjunct of (1.47) holds trivially, so that leaves just the first to prove. Assume $V^{\sim}_{Op}(o\tilde{}, \underline{q})$. We want to derive $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{q})$. We also have $V^{\sim}_{Op}(o\tilde{}, \underline{q})$. Hence by (X5) $\underline{q} \sim \underline{q}$, and so $\underline{q} \in [\underline{q}]$. Thus, because $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{q})$ holds, the required consequent follows by (1.22).

Case (c). Suppose $H^{\sim}(\underline{u}\tilde{}, \underline{v})$, $Q^{\sim}_{Op}(\underline{i}\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$ and $D^{\sim}_{Op}(\underline{u}\tilde{}', \underline{v}', o\tilde{}, \underline{p}; \underline{i}\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$ hold. Then (X5) allows us to pick values $\underline{w}'$, $\underline{q}$, $\underline{k}$ and $\underline{w}$, such that $K^{\sim}(\underline{u}\tilde{}', \underline{w}')$, $V^{\sim}_{Op}(o\tilde{}, \underline{q})$, $R^{\sim}_{Op}(\underline{i}\tilde{}, \underline{k})$, and $K^{\sim}(\underline{u}\tilde{}, \underline{w})$ hold. By (X10) we therefore also have $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{v}], [\underline{w}]), \underline{v})$. Let $o = ([\underline{p}], [\underline{q}])$. We now prove $V^{\circ}_{Op}(o, o\tilde{})$. To do this we verify each conjunct of (1.47). Take the first conjunct and assume $V^{\sim}_{Op}(o\tilde{}, \underline{q})$. Because $V^{\sim}_{Op}(o\tilde{}, \underline{q})$ holds, by (X5), $\underline{q} \sim \underline{q}$ and therefore $\underline{q} \in [\underline{q}]$. Furthermore, $D^{\bullet}_{Op}$ and (1.23) give $DV_{Op}([\underline{p}], [\underline{q}])$. Thus by (1.22), $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{q})$ holds as required.

To establish the second conjunct assume $H^{\sim}(\underline{u}\tilde{}, \underline{v})$, $Q^{\sim}_{Op}(\underline{i}\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$, $D^{\sim}_{Op}(\underline{u}\tilde{}', \underline{v}', o\tilde{}, \underline{p}; \underline{i}\tilde{}, \underline{j}, \underline{u}\tilde{}, \underline{v})$, $K^{\circ}(\underline{u}', \underline{u}\tilde{}')$, $R^{\circ}_{Op}(\underline{i}, \underline{i}\tilde{})$ and $K^{\circ}(\underline{u}, \underline{u}\tilde{})$. Let $\underline{u}' = ([\underline{v}'], [\underline{w}'])$, $\underline{i} = ([\bar{j}], [\bar{k}])$ and $\underline{u} = ([\bar{v}], [\bar{w}])$. The objective is to derive $H^{\bullet}(([\bar{v}], [\bar{w}]), \underline{v})$, $Q^{\bullet}_{Op}(([\bar{j}], [\bar{k}]), \underline{j}, ([\bar{v}], [\bar{w}]), \underline{v})$ and $D^{\bullet}_{Op}(([\bar{v}'], [\bar{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\bar{j}], [\bar{k}]), \underline{j}, ([\bar{v}], [\bar{w}]), \underline{v})$. As we have $H^{\sim}$, $Q^{\sim}_{Op}$ and $D^{\sim}_{Op}$, (X9) permits us to pick values $\underline{w}'$, $\underline{q}$, $\underline{k}$ and $\underline{w}$, such that we have $K^{\sim}(\underline{u}\tilde{}', \underline{w}')$, $V^{\sim}_{Op}(o\tilde{}, \underline{q})$, $R^{\sim}_{Op}(\underline{i}\tilde{}, \underline{k})$, and $K^{\sim}(\underline{u}\tilde{}, \underline{w})$. Then by Lemma 1.13 $H^{\bullet}(([\bar{v}], [\bar{w}]), \underline{v})$, $Q^{\bullet}_{Op}(([\bar{j}], [\bar{k}]), \underline{j}, ([\bar{v}], [\bar{w}]), \underline{v})$ and $D^{\bullet}_{Op}(([\bar{v}'], [\bar{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([\bar{j}], [\bar{k}]), \underline{j}, ([\bar{v}], [\bar{w}]), \underline{v})$ hold. This is nearly what we require. It just remains to show $\underline{p} \sim p$ and $\underline{q} \sim q$. The former follows from $D^{\sim}_{Op}(..., o\tilde{}, \underline{p}; ...)$ and $D^{\sim}_{Op}(..., o\tilde{}, p; ...)$ by (X6); the latter from $V^{\sim}_{Op}(o\tilde{}, \underline{q})$ and $V^{\sim}_{Op}(o\tilde{}, q)$ by (X5). We are done.

To complete case (i) we need to verify $stp_{Op_U}(u, i, u', o)$ holds. We have $H^{\bullet}(([v], [w]), \underline{v})$, $Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v})$, $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$ and $H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{v}')$, with $u = ([v], [w])$,

$i = ([j], [k])$ and $u' = ([\underline{v}'], [\underline{w}'])$. So regardless of the value of o (in cases (a) to (c)), (1.35b) is true, giving $stp_{Op_U}(u, i, u', o)$.

Case (ii). Assume $D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v})$. Since we have $H\tilde{}(u\tilde{}, \underline{v})$ and $Q\tilde{}_{Op}(i\tilde{}, \underline{j}, u\tilde{}, \underline{v})$, by (X9), we also have $K\tilde{}(u\tilde{}', \underline{w}')$, $V\tilde{}_{Op}(o\tilde{}, \underline{q})$, $R\tilde{}_{Op}(i\tilde{}, \underline{k})$ and $K\tilde{}(u\tilde{}, \underline{w})$ for chosen values $\underline{w}', \underline{q}, \underline{k}, \underline{w}$. Hence, by (X10), $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [\underline{k}]), \underline{j}, ([v], [\underline{w}]), \underline{v})$ holds. But because $Q^{\bullet}_{Op}(([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds, Lemma 1.14 says $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds. Let $u' = ([\underline{v}'], [\underline{w}'])$ and $o = ([\underline{p}], [\underline{q}])$. Then since we have $H^{\bullet}(([v], [w]), \underline{v})$, $stp_{Op_T}(\underline{v}, \underline{j}, \underline{v}', \underline{p})$, $u = ([v], [w])$ and $i = ([j], [k])$, (1.35b) and thus $stp_{Op_U}(u, i, u', o)$ holds.

Only $K^{\circ}(u', u\tilde{}')$ and $V^{\circ}_{Op}(o, o\tilde{})$ remain. To show $K^{\circ}(u', u\tilde{}')$ we once again prove each conjunct of (1.45). Take the first conjunct and assume $K\tilde{}(u\tilde{}', \underline{\underline{w}}')$. We want to derive $K^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{\underline{w}}')$. We argue thus. $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ and (1.23) give $HK([\underline{v}'], [\underline{w}'])$ and $DK_{Op}([\underline{v}'], [\underline{w}'])$. $K\tilde{}(u\tilde{}', \underline{w}')$, $K\tilde{}(u\tilde{}', \underline{\underline{w}}')$ and (X3) give $\underline{w}' \sim \underline{\underline{w}}'$. Hence $\underline{\underline{w}}' \in [\underline{w}']$ and therefore, by (1.18), $K^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{\underline{w}}')$ holds as required.

Take the second conjunct and assume $H\tilde{}(u\tilde{}', \underline{\underline{v}}')$. We want to deduce $H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{\underline{v}}')$. In addition to $H\tilde{}(u\tilde{}', \underline{\underline{v}}')$ we have $K\tilde{}(u\tilde{}', \underline{w}')$. Therefore (X8) says $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$ holds. Furthermore, we also have $D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v})$. Hence by (X4), $\underline{v}' \sim \underline{\underline{v}}'$. Thus, since $H^{\bullet}(([\underline{\underline{v}}'], [\underline{w}']), \underline{\underline{v}}')$ holds, $H^{\bullet}(([\underline{v}'], [\underline{w}']), \underline{\underline{v}}')$ holds too.

The proof for the third conjunct mirrors the corresponding proof given for PO (1.48) case 2, except that we use $D\tilde{}_{Op}(u\tilde{}', \underline{\underline{v}}', \underline{\underline{o}}\tilde{}, \underline{\underline{p}}; \underline{\underline{i}}\tilde{}, \underline{\underline{j}}, \underline{\underline{u}}\tilde{}, \underline{\underline{v}})$ and $D\tilde{}_{Op}(u\tilde{}', \underline{v}', o\tilde{}, \underline{p}; i\tilde{}, \underline{j}, u\tilde{}, \underline{v})$ (the latter in place of $H\tilde{}(u\tilde{}', \underline{v}')$), to establish $\underline{\underline{v}}' \sim \underline{v}'$ by rule (X4).

Finally we turn to $V^{\circ}_{Op}(o, o\tilde{})$. As anticipated, we prove each conjunct of (1.47) in turn.

For the first conjunct we assume $V\tilde{}_{Op}(o\tilde{}, \underline{\underline{q}})$ and propose to establish $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{\underline{q}})$. First, since we also have $V\tilde{}_{Op}(o\tilde{}, \underline{q})$, by (X5), $\underline{\underline{q}} \sim \underline{q}$. Second, as $D^{\bullet}_{Op}(([\underline{v}'], [\underline{w}']), \underline{v}', ([\underline{p}], [\underline{q}]), \underline{p}; ([j], [k]), \underline{j}, ([v], [w]), \underline{v})$ holds, by (1.23), we have $DV_{Op}([\underline{p}], [\underline{q}])$. Thus $V^{\bullet}_{Op}(([\underline{p}], [\underline{q}]), \underline{\underline{q}})$ holds by (1.22).

To establish the second conjunct assume $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $D^{\sim}{}_{Op}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $K^{\circ}(\underline{\underline{u}}', \underline{\underline{u}}^{\sim\prime})$, $R^{\circ}{}_{Op}(\underline{\underline{i}}, \underline{\underline{i}}^{\sim})$ and $K^{\circ}(\underline{\underline{u}}, \underline{\underline{u}}^{\sim})$. Let $\underline{\underline{u}}' = ([\underline{\underline{v}}'], [\underline{\underline{w}}'])$, $\underline{\underline{i}} = ([\underline{j}], [\underline{k}])$ and $\underline{\underline{u}} = ([\underline{\underline{v}}], [\underline{\underline{w}}])$. The objective is to derive $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}{}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}{}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$. As we have $H^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, $Q^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$ and $D^{\sim}{}_{Op}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{v}}', o^{\sim}, \underline{\underline{p}}; \underline{\underline{i}}^{\sim}, \underline{j}, \underline{\underline{u}}^{\sim}, \underline{\underline{v}})$, (X9) permits us to pick values $\underline{\underline{w}}'$, $\underline{\underline{q}}$, $\underline{\underline{k}}$ and $\underline{\underline{w}}$, such that we have $K^{\sim}(\underline{\underline{u}}^{\sim\prime}, \underline{\underline{w}}')$, $V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}})$, $R^{\sim}{}_{Op}(\underline{\underline{i}}^{\sim}, \underline{\underline{k}})$, and $K^{\sim}(\underline{\underline{u}}^{\sim}, \underline{\underline{w}})$. Then by Lemma 1.13 $H^{\bullet}(([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$, $Q^{\bullet}{}_{Op}(([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ and $D^{\bullet}{}_{Op}(([\underline{\underline{v}}'], [\underline{\underline{w}}']), \underline{\underline{v}}', ([\underline{\underline{p}}], [\underline{\underline{q}}]), \underline{\underline{p}}; ([\underline{j}], [\underline{k}]), \underline{j}, ([\underline{\underline{v}}], [\underline{\underline{w}}]), \underline{\underline{v}})$ hold. From this our objective ensues if we can show $\underline{\underline{p}} \sim \underline{p}$ and $\underline{\underline{q}} \sim \underline{q}$. The former we get from $D^{\sim}{}_{Op}(..., o^{\sim}, \underline{\underline{p}}; ...)$ and $D^{\sim}{}_{Op}(..., o^{\sim}, \underline{p}; ...)$ by (X6); the latter from $V^{\sim}{}_{Op}(o^{\sim}, \underline{\underline{q}})$ and $V^{\sim}{}_{Op}(o^{\sim}, \underline{q})$ by (X5). We are done. We have now proved 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*. ☺