Functional Refinement

Using Z
Woodcock & Davies

Cancellation property

$$R \subseteq S \mathbin{;} f^{\sim} \quad \Leftrightarrow \quad R \mathbin{;} f \subseteq S$$

How does this work?

$$R \subseteq S \fatsemi f^{\sim}$$

$$\Leftrightarrow \forall x : X;\ y : Y \bullet x \mapsto y \in R \Rightarrow x \mapsto y \in S \fatsemi f^{\sim}$$

[by def of $\subseteq$]

$$\Leftrightarrow \forall x : X;\ y : Y \bullet$$
$$x \mapsto y \in R \Rightarrow$$
$$\exists z : Z \bullet x \mapsto z \in S \land z \mapsto y \in f^{\sim}$$

[by def of $\fatsemi$]

$$\Leftrightarrow \forall x : X;\ y : Y \bullet$$
$$x \mapsto y \in R \Rightarrow \exists z : Z \bullet x \mapsto z \in S \land y \mapsto z \in f$$

[by def of $^{\sim}$]

$$\Leftrightarrow \forall\, x : X;\ y : Y \bullet$$
$$x \mapsto y \in R \Rightarrow \exists\, z : Z \bullet x \mapsto z \in S \land z = f(y)$$

[f is a total function]

$$\Leftrightarrow \forall\, x : X;\ y : Y \bullet$$
$$x \mapsto y \in R \Rightarrow f(y) \in Z \land x \mapsto f(y) \in S$$

[by $\exists$-opr]

$$\Leftrightarrow \forall\, x : X;\ y : Y \bullet$$
$$x \mapsto y \in R \Rightarrow x \mapsto f(y) \in S$$

[f is a total function]

$$\Leftrightarrow \forall\, x : X;\ y : Y \bullet$$
$$f(y) \in Z \land x \mapsto y \in R \Rightarrow x \mapsto f(y) \in S$$

[f is a total function]

$$\Leftrightarrow \forall\, x : X;\ y : Y;\ z : Z \bullet$$
$$z = f(y) \land x \mapsto y \in R \Rightarrow x \mapsto z \in S$$

[by $\forall$-opr]

$$\Leftrightarrow \forall\, x : X;\ y : Y;\ z : Z \bullet$$
$$x \mapsto y \in R \land y \mapsto z \in f \Rightarrow x \mapsto z \in S$$

[f is a total function]

$$\Leftrightarrow \forall\, x : X;\ z : Z \bullet$$
$$(\exists\, y : Y \bullet x \mapsto y \in R \land y \mapsto z \in f) \Rightarrow$$
$$x \mapsto z \in S$$

[by predicate calculus]

$$\Leftrightarrow \forall x : X; z : Z \bullet$$
$$x \mapsto z \in R \mathbin{;} f \Rightarrow x \mapsto z \in S$$

[by def of $\mathbin{;}$]

$$\Leftrightarrow R \mathbin{;} f \subseteq S$$

[by def of $\subseteq$]

Forwards simulation

relational:

$$\operatorname{dom} ao \lhd f^{\sim} \mathbin{⨾} co \subseteq ao \mathbin{⨾} f^{\sim}$$

functional:

$$\operatorname{dom} ao \lhd f^{\sim} \mathbin{⨾} co \mathbin{⨾} f \subseteq ao$$

Rules for retrieve functions

$$ci \mathbin{;} f \subseteq ai$$

$$f^{\sim} \mathbin{;} cf \subseteq af$$

$$\mathrm{dom}\, ao \lhd f^{\sim} \mathbin{;} co \mathbin{;} f \subseteq ao$$

$$\mathrm{ran}((\mathrm{dom}\, ao) \lhd f^{\sim}) \subseteq \mathrm{dom}\, co$$

With schemas

$$\forall\, C \bullet \exists_1\, A \bullet R$$

$$\forall\, A';\ C' \mid CI \land R' \bullet AI$$

$$\forall\, A;\ A';\ C;\ C' \mid \mathrm{pre}\ AO \land R \land CO \land R' \bullet AO$$

$$\forall\, A;\ C \bullet \mathrm{pre}\ AO \land R \Rightarrow \mathrm{pre}\ CO$$

Example

$$
\begin{array}{|l}
\hline
\multicolumn{1}{l}{\textit{ListRetrieveSet}} \\
\hline
ASystem \\
CSystem \\
\hline
s = \operatorname{ran} l \\
\hline
\end{array}
$$

$$\forall\, CSystem \bullet \exists_1\, ASystem \bullet ListRetrieveSet$$

$$\begin{array}{l}\forall\, CSystem'; \; ASystem' \mid \\ \quad CSystemInit \land ListRetrieveSet' \bullet ASystemInit\end{array}$$

$$\begin{array}{l}\forall\, ASystem; \; CSystem \mid \\ \quad \mathrm{pre}\; AEnterBuilding \land ListRetrieveSet \bullet \\ \qquad \mathrm{pre}\; CEnterBuilding\end{array}$$

$$\begin{array}{l}\forall\, ASystem; \; ASystem'; \; CSystem; \; CSytems' \mid \\ \quad \mathrm{pre}\; AEnterBuilding \land \\ \quad ListRetrieveSet \land \\ \quad CEnterBuilding \land \\ \quad ListRetrieveSet' \\ \qquad \bullet AEnterBuilding\end{array}$$

Calculation

If the retrieve relation is a total surjective function from concrete to abstract, we can

- write down the concrete state
- record the retrieve relation
- calculate the rest of the concrete system

The result is the weakest refinement $\mathcal{W}$.

How to find $\mathcal{W}$

$$
\begin{aligned}
& f^{\sim} \mathbin{;} wo \\
& \quad = f^{\sim} \mathbin{;} f \mathbin{;} ao \mathbin{;} f^{\sim} && \text{[by definition]} \\
& \quad = \mathrm{id}[\operatorname{ran} f\,] \mathbin{;} ao \mathbin{;} f^{\sim} && \text{[by relational calculus]} \\
& \quad = ao \mathbin{;} f^{\sim} && \text{[since } f \text{ is surjective]}
\end{aligned}
$$

Rules for calculation

- $wi = ai \mathbin{;} f^{\sim}$
- $wo = f \mathbin{;} ao \mathbin{;} f^{\sim}$

With schemas

$$F \mathrel{\widehat=} [\, A;\ C \mid \theta A = f(\theta C) \,]$$

- $CI \;=\; AI \fatsemi F'$
- $CO \;=\; F \fatsemi AO \fatsemi F'$

Example

specification:

$$s' = s \cup \{p?\}$$

retrieve relation:

$$s = \operatorname{ran} l$$

weakest refinement:

$$\operatorname{ran} l' = \operatorname{ran} l \cup \{p?\}$$

Farenheit

$$^\circ F == \{ f : \mathbb{R} \mid -459.4 \leq f \leq 5{,}000 \}$$

$$\begin{array}{|l}
\multicolumn{1}{l}{\textit{FTemp}} \\
\hline
f : {}^\circ F \\
\hline
\end{array}$$

$$StdTemp == 65$$

$$
\begin{array}{|l}
\hline
\textit{FTempInit} \\
FTemp' \\
\hline
f' = StdTemp \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{FTInc} \\
\Delta FTemp \\
\hline
f \leq 4,999 \\
f' = f + 1 \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
\hline
\textit{FTDec} \\
\Delta FTemp \\
\hline
f \geq -458.4 \\
f' = f - 1 \\
\hline
\end{array}
$$

Celsius

$$Celsius == \{\, t : \mathbb{R} \mid -273 \leq t \leq 2760 \,\}$$

$$CTemp \mathrel{\widehat=} [\, c : C \,]$$

$$
\begin{array}{|l}
\hline
\textit{RetrieveFC} \\
\hline
FTemp \\
CTemp \\
\hline
f = \frac{9}{5} * c + 32 \\
\hline
\end{array}
$$

$$
\begin{array}{|l}
CTemp' \\
\hline
\frac{9}{5} * c' + 32 = StdTemp
\end{array}
$$

CTempInit

$$
\begin{array}{|l}
CTemp' \\
\hline
c' = \frac{5}{9} * (StdTemp - 32)
\end{array}
$$

$$\Delta CTemp$$

$$\frac{9}{5} * c + 32 \leq 4,999$$

$$\frac{9}{5} * c' + 32 = \frac{9}{5} * c + 32 + 1$$

$CTInc$

$$\Delta CTemp$$

$$c \leq 2759\frac{4}{9}$$

$$c' = c + \frac{5}{9}$$

$$\Delta CTemp$$

$$\frac{9}{5} * c + 32 \geq -458.4$$
$$\frac{9}{5} * c' + 32 = \frac{9}{5} * c + 32 - 1$$

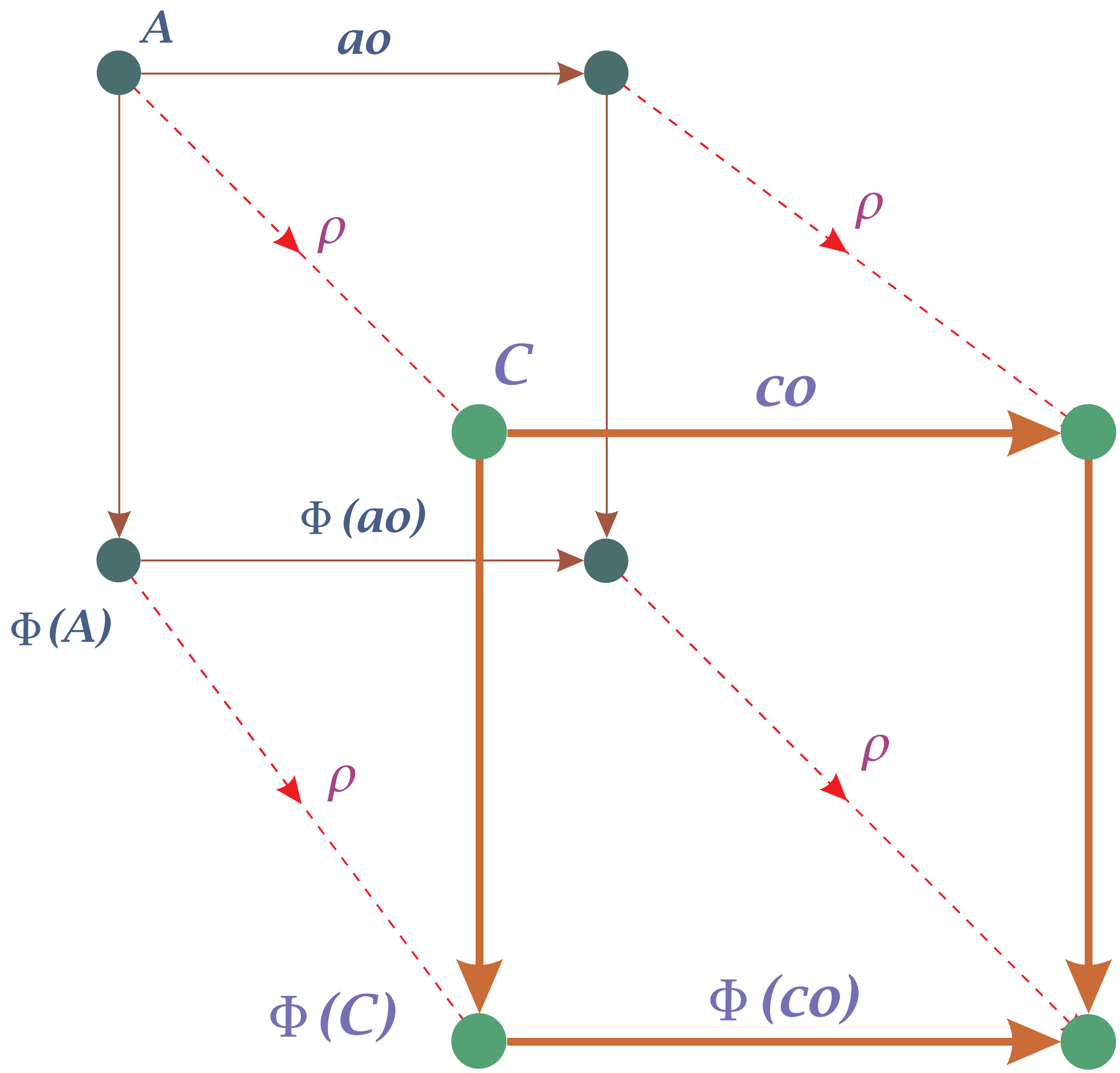
CTDec

$$\Delta CTemp$$

$$c > 272\frac{4}{9}$$
$$c' = c - \frac{5}{9}$$

Promotion

'the refinement of a promotion is the promotion of the refinement'


A
ao
ρ
ρ
C
co
Φ (ao)
Φ (A)
ρ
ρ
Φ (C)
Φ (co)

$$P \mathrel{\widehat=} [\, f : I \pinj S \,]$$

$$\begin{array}{|l}
\hline
\textit{Promote} \\
\Delta S \\
\Delta P \\
i? : I \\
\hline
i? \in \operatorname{dom} f \\
\theta S = f(i?) \\
f' = f \oplus \{ i? \mapsto \theta S' \} \\
\hline
\end{array}$$

$$PO \mathrel{\widehat=} \exists\, \Delta S \bullet Promote \land SO$$

Example

$$FTDisplay \mathrel{\widehat=} [\, fd : Ind \rightarrow FTemp \,]$$

$$
\begin{array}{|l}
\textit{FTPromote} \\
\hline
\Delta FTDisplay \\
\Delta FTemp \\
i? : Ind \\
\hline
\theta FTemp = fd\ i? \\
fd' = fd \oplus \{ i? \mapsto \theta FTemp' \} \\
\hline
\end{array}
$$

Promoted operations

$$FTDisplayInc \mathrel{\widehat=} \exists \Delta FTemp \bullet FTPromote \land FTInc$$

$$FTDisplayDec \mathrel{\widehat=} \exists \Delta FTemp \bullet FTPromote \land FTDec$$

Concrete state

$$CTDisplay \mathrel{\widehat{=}} [\, cd : Ind \rightarrow CTemp \,]$$

Refinement of promoted system

$$
\begin{array}{l}
\textbf{CTPromote} \\
\hline
\Delta CTDisplay \\
\Delta CTemp \\
i? : Ind \\
\hline
\theta CTemp = cd\ i? \\
cd' = cd \oplus \{ i? \mapsto \theta CTemp' \}
\end{array}
$$

Refined, promoted operations

$$CTDisplayInc \mathrel{\widehat=} \exists \Delta CTemp \bullet CTPromote \land CTInc$$

$$CTDisplayDec \mathrel{\widehat=} \exists \Delta CTemp \bullet CTPromote \land CTDec$$

Summary

- cancellation property
- retrieve functions
- calculating refinements
- refinement of promotion