

Functional Refinement

Cancellation property

$$R \subseteq S \circ f^\sim \Leftrightarrow R \circ f \subseteq S$$

jsing Z

18-3

How does this work?

$$R \subseteq S \circ f^\sim$$

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

[by def of \subseteq]

$$\Leftrightarrow \forall x:X; y:Y \bullet$$

$$x \mapsto y \in R \Rightarrow f(y) \in Z \wedge x \mapsto f(y) \in S$$

[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]

$$\Leftrightarrow \forall x:X; y:Y \bullet$$

$$f(y) \in Z \wedge x \mapsto y \in R \Rightarrow x \mapsto f(y) \in S$$

[f is a total function]

jsing Z

18-4

$$\Leftrightarrow \forall x:X; y:Y \bullet$$

$$x \mapsto y \in R \Rightarrow \exists z:Z \bullet x \mapsto z \in S \wedge z = f(y)$$

[f is a total function]

$$\Leftrightarrow \forall x:X; y:Y \bullet$$

$$x \mapsto y \in R \Rightarrow f(y) \in Z \wedge x \mapsto f(y) \in S$$

[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]

jsing Z

18-5

$$\Leftrightarrow \forall x:X; y:Y; z:Z \bullet$$

$$z = f(y) \wedge x \mapsto y \in R \Rightarrow x \mapsto z \in S$$

[by \forall -opr]

$$\Leftrightarrow \forall x:X; y:Y; z:Z \bullet$$

$$x \mapsto y \in R \wedge y \mapsto z \in f \Rightarrow x \mapsto z \in S$$

[f is a total function]

$$\Leftrightarrow \forall x:X; z:Z \bullet$$

$$(\exists y:Y \bullet x \mapsto y \in R \wedge y \mapsto z \in f) \Rightarrow$$

[by predicate calculus]

jsing Z

18-6

Forwards simulation

$$\Leftrightarrow \forall x: X; z: Z \bullet \\ x \mapsto z \in R_g^o f \Rightarrow x \mapsto z \in S$$

[by def of \circ]

$$\Leftrightarrow R_g^o f \subseteq S$$

[by def of \subseteq]

$$\text{dom } ao \lhd f^\sim \circ co \circ f \subseteq ao$$

relational:

$$\text{dom } ao \lhd f^\sim \circ co \circ f \subseteq ao \circ f^\sim$$

functional:

$$\text{dom } ao \lhd f^\sim \circ co \circ f \subseteq ao$$

Rules for retrieve functions

$$ci \circ f \subseteq ai$$

$$f^\sim \circ cf \subseteq af$$

$$\text{dom } ao \lhd f^\sim \circ co \circ f \subseteq ao$$

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

with schemas

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

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

$$\forall A; A'; C; C' \mid \text{pre } AO \wedge R \wedge CO \wedge R' \bullet AO$$

$$\forall A; C \bullet \text{pre } AO \wedge R \Rightarrow \text{pre } CO$$

$$\begin{aligned} &\forall CSys \bullet \exists_1 ASys \bullet ListRetrieveSet \\ &\forall CSys'; ASys' \mid \\ &\quad CSysInit \wedge ListRetrieveSet' \bullet ASysInit \\ &\forall ASys; CSys \mid \\ &\quad \text{pre } AEnterBuilding} \wedge ListRetrieveSet \bullet \\ &\quad \text{pre } CenterBuilding} \\ &\forall ASys; ASys'; CSys; CSys' \mid \\ &\quad \text{pre } AEnterBuilding} \wedge \\ &\quad ListRetrieveSet \wedge \\ &\quad CenterBuilding} \wedge \\ &\quad ListRetrieveSet' \\ &\quad \bullet AEnterBuilding \end{aligned}$$

Example

<i>ListRetrieveSet</i>	<i>ASystem</i>	<i>CSys</i>
<i>s = ranI</i>		

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}

$$\begin{aligned} f^{\sim \circ wo} \\ = f^{\sim \circ f \circ ao \circ f^{\sim}} \end{aligned}$$

[by definition]

$$= id[\text{ran } f] \circ ao \circ f^{\sim}$$

[by relational calculus]

[since f is surjective]

Rules for calculation

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

with schemas

$$F \hat{=} [A : C \mid \theta A = f(\theta C)]$$

- $CI = AI \circ F'$
- $CO = F \circ AO \circ F'$

Example

specification:

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

retrieve relation:

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

weakest refinement:

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

Farenheit

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

$$\boxed{FTemp} \quad \boxed{f : {}^o F}$$

$StdTemp == 65$

$FITempInit$

$FITemp'$

$f' = StdTemp$

Jsing Z

Jsing Z

18-21

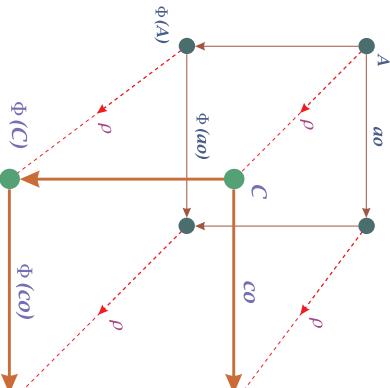
Jsing Z

Jsing Z

18-22

Promotion

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



$P \hat{=} [f : I \nrightarrow S]$

Promote

ΔS
ΔP
$i? : I$
$i? \in \text{dom } f$
$\partial S = f(i?)$
$f' = f \oplus \{i? \mapsto \partial S'\}$

$PO \hat{=} \exists \Delta S \bullet \text{Promote} \wedge SO$

Promoted operations

Concrete state

$FTDisplayInc \hat{=} \exists \Delta FTemp \bullet FTPromote \wedge FTInc$

$FTDisplayDec \hat{=} \exists \Delta FTemp \bullet FTPromote \wedge FTDec$

$FIPromote$
$\Delta FTDIplay$
$\Delta FTemp$
$i? : Ind$
$OFTemp = fd\ i?$
$fd' = fd \oplus \{i? \mapsto OFTemp'\}$

Refinement of promoted system

Refined, promoted operations

$CTPromote$	$\Delta CTDisplay$
$\Delta CTDisplay$	$\Delta CTTemp$
$i? : Ind$	$\theta CTTemp = cd\ i?$
$cd' = cd \oplus \{i? \mapsto \theta CTTemp'\}$	

Summary

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