PF transform: conditions and coreflexives for ESC

J.N. Oliveira

Dept. Informática,
Universidade do Minho
Braga, Portugal

DI/UM, 2007

Basic rules of the PF-transform

ϕ	$PF\ \phi$
$\langle \exists\ a\ ::\ b\ R\ a \wedge a\ S\ c \rangle$	$b(R \cdot S)c$
$\langle \forall\ a, b\ ::\ b\ R\ a \Rightarrow b\ S\ a \rangle$	$R \subseteq S$
$\langle \forall\ a\ ::\ a\ R\ a \rangle$	$id \subseteq R$
$b\ R\ a \wedge c\ S\ a$	$(b, c)\langle R, S \rangle a$
$b\ R\ a \wedge d\ S\ c$	$(b, d)(R \times S)(a, c)$
$b\ R\ a \wedge b\ S\ a$	$b\ (R \cap S)\ a$
$b\ R\ a \vee b\ S\ a$	$b\ (R \cup S)\ a$
$(f\ b)\ R\ (g\ a)$	$b(f^{\circ} \cdot R \cdot g)a$
TRUE	$b\ \top\ a$
FALSE	$b\ \bot\ a$

Question

- The PF-transform seems applicable to transforming **binary** predicates only, easily converted to binary relations, eg. $\phi(y,x) \triangleq\ y-1=2x$ which transforms to function $y=2x+1$, etc.

- What about transforming predicates such as the following

$$\langle \forall\ x,y\ \ :\ \ y=2x \wedge \mathit{even}\ x :\ \ \mathit{even}\ y\rangle \tag{1}$$

expressing the fact that function $y=2x$ preserves even numbers, where $\mathit{even}\ x \triangleq\ \mathit{rem}(x,2)=0$ is a **unary** predicate?

Observation

- As already noted, (1) is a proposition stating that function $y = 2x$ *preserves* even numbers.
- In general, a function $A \xleftarrow{f} A$ is said to **preserve** a given predicate ϕ iff the following holds:

$$\langle \forall\ x\ :\ \phi\ x :\ \phi\ (f\ x) \rangle \tag{2}$$

- Proposition (2) is itself a particular case of

$$\langle \forall\ x\ :\ \phi\ x :\ \psi\ (f\ x) \rangle \tag{3}$$

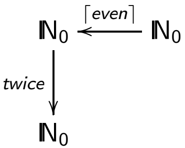
which states that f **ensures** property ψ on its output everytime property ϕ holds on its input.

Answer

First PF-transform scope:

$$
\begin{array}{cl}
 & y = 2x \wedge \mathit{even}\ x \\
\equiv & \qquad \{\ \exists\text{-one-point}\ \} \\
 & \langle \exists\ z\ :\ z = x :\ y = 2z \wedge \mathit{even}\ z \rangle \\
\equiv & \qquad \{\ \exists\text{-trading ; introduce } \lceil \mathit{even} \rceil\ \} \\
 & \langle \exists\ z\ ::\ y = 2z \wedge \underbrace{z = x \wedge \mathit{even}\ z}_{z \lceil \mathit{even} \rceil x} \rangle \\
\equiv & \qquad \{\ \text{composition ; introduce } \mathit{twice}\ z \triangleq 2z\ \} \\
 & y(\mathit{twice} \cdot \lceil \mathit{even} \rceil)x
\end{array}
$$

cf. diagram



Now the whole thing

$$\langle \forall\, x, y \;:\; y = 2x \wedge \mathit{even}\ x :\; \mathit{even}\ y \rangle$$

$\equiv$ { above }

$$\langle \forall\, x, y \;:\; y(\mathit{twice} \cdot \lceil \mathit{even} \rceil)x :\; \mathit{even}\ y \rangle$$

$\equiv$ { $\exists$-one-point }

$$\langle \forall\, x, y \;:\; y(\mathit{twice} \cdot \lceil \mathit{even} \rceil)x :\; \langle \exists\, z \;:\; z = y :\; \mathit{even}\ z \rangle \rangle$$

$\equiv$ { predicate calculus: $p \wedge \textsc{True} = p$ }

$$\langle \forall\, x, y \;:\; y(\mathit{twice} \cdot \lceil \mathit{even} \rceil)x :\; \langle \exists\, z \;::\; z = y \wedge \mathit{even}\ z \wedge \textsc{True} \rangle \rangle$$

$\equiv$ { $\top$ is the top relation }

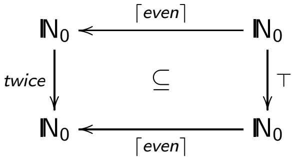
$$\langle \forall\, x, y \;:\; y(\mathit{twice} \cdot \lceil \mathit{even} \rceil)x :\; \langle \exists\, z \;::\; y \lceil \mathit{even} \rceil z \wedge z \top x \rangle \rangle$$

$\equiv$ { composition }

Now the whole thing

$$
\begin{array}{ll}
 & \langle \forall\ x, y \ :\ y(twice \cdot \lceil even \rceil)x :\ y(\lceil even \rceil \cdot \top)x \rangle \\
\equiv & \qquad \{ \ \text{go pointfree (inclusion)} \ \} \\
 & twice \cdot \lceil even \rceil \ \subseteq \ \lceil even \rceil \cdot \top
\end{array}
$$

cf. diagram



In summary

In the calculation above, **unary** predicate *even* has been PF-transformed in two ways:

- $\lceil even \rceil$ such that

$$z \lceil even \rceil x \quad \triangleq \quad z = x \wedge even\ z$$

  — that is, $\lceil even \rceil$ is a **coreflexive** relation;

- $\lceil even \rceil \cdot \top$, which is such that

$$z (\lceil even \rceil \cdot \top) x \;\equiv\; even\ z$$

  — a so-called (left) *condition*.

Coreflexives

The PF-transformation of **unary** predicates to fragments of *id* coreflexives) is captured by the following universal property:

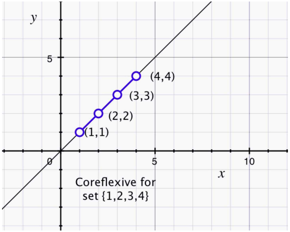
$$\Phi = \lceil p \rceil \;\equiv\; (y\;\Phi\;x \equiv y = x \wedge p\;y) \tag{4}$$

Via cancellation, (4) yields

$$y\;\lceil p \rceil\;x \;\equiv\; y = x \wedge p\;y \tag{5}$$

A set S can also be PF-transformed into a coreflexive by calculating $\lceil (\in S) \rceil$, cf. eg. the transform of set $\{1, 2, 3, 4\}$:

$$\lceil 1 \leq x \leq 4 \rceil \quad =$$



Exercises

Exercise 1: Let *false* be the "everywhere false" predicate such that $\mathit{false}\ x = \textsc{False}$ for all x, that is, $\mathit{false} = \underline{\textsc{False}}$. Use (4) to show that $\lceil \mathit{false} \rceil = \bot$.

□

Exercise 2: Given a set S, let Φ_S abbreviate coreflexive $\lceil (\in S) \rceil$. Calculate $\Phi_{\{1,2\}} \cdot \Phi_{\{2,3\}}$.

□

Exercise 3: Solve (4) for p under substitution $\Phi := id$.

□

Boolean algebra of coreflexives

Building up one the exercises above, from (4) one easily draws:

$$\lceil p \wedge q \rceil = \lceil p \rceil \cdot \lceil q \rceil \tag{6}$$
$$\lceil p \vee q \rceil = \lceil p \rceil \cup \lceil q \rceil \tag{7}$$
$$\lceil \neg p \rceil = id - \lceil p \rceil \tag{8}$$
$$\lceil false \rceil = \bot \tag{9}$$
$$\lceil true \rceil = id \tag{10}$$

where p, q are predicates.

(Note the slight, obvious abuse in notation.)

Basic properties of coreflexives

Let Φ, Ψ be coreflexive relations. Then the following properties hold:

- Coreflexives are **symmetric** and **transitive**:

$$\Phi^\circ = \Phi = \Phi \cdot \Phi \tag{11}$$

- **Meet** of two coreflexives is composition:

$$\Phi \cap \Psi = \Phi \cdot \Psi \tag{12}$$

- Closure properties:

$$R \cdot \Phi \subseteq S \quad \equiv \quad R \cdot \Phi \subseteq S \cdot \Phi \tag{13}$$

$$\Phi \cdot R \subseteq S \quad \equiv \quad \Phi \cdot R \subseteq \Phi \cdot S \tag{14}$$

Coreflexives for data flow control

Coreflexives are very handy in controlling information flow in PF-expressions, as the following two PF-transform rules show, given two suitably typed coreflexives $\Phi = \lceil \phi \rceil$ and $\Psi = \lceil \psi \rceil$:

- Guarded **composition**: for all b, c

$$\langle \exists\ a\ :\ \phi\ a :\ b\ R\ a \wedge a\ S c \rangle \quad \equiv \quad b(R \cdot \Phi \cdot S)c \qquad (15)$$

- Guarded **inclusion**:

$$\langle \forall\ b, a\ :\ \phi\ b \wedge \psi\ a :\ b\ R\ a \Rightarrow b\ S\ a \rangle \\ \equiv\ \Phi \cdot R \cdot \Psi \subseteq S \qquad (16)$$

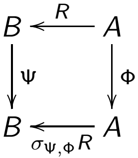
See next slide for some related terminology.

Projection and selection

The following relational operators capture two useful relational patterns involving relations, coreflexives and functions:

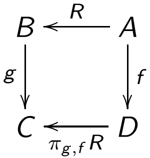
- Selection:

$$\sigma_{\Psi,\Phi} R \;\triangleq\; \Psi \cdot R \cdot \Phi \qquad (17)$$



- Projection:

$$\pi_{g,f} R \;\triangleq\; g \cdot R \cdot f^{\circ} \qquad (18)$$



Projection and selection

Set-theoretical meaning of selection and projection, for $\Psi = \lceil \psi \rceil$ and $\Phi = \lceil \phi \rceil$:

$$\sigma_{\Psi,\Phi} R = \{(b,a) : b\ R\ a \wedge \psi\ b \wedge \phi\ a\} \tag{19}$$

$$\pi_{g,f} R = \{(g\ b, f\ a) : b\ R\ a\} \tag{20}$$

Let us check (19):

$$
\begin{array}{ll}
 & \sigma_{\Psi,\Phi} R \\
= & \quad \{ \text{ set theoretical meaning of a relation } \} \\
 & \{(b,a) : b(\sigma_{\Psi,\Phi} R)a\} \\
= & \quad \{ \text{ definition (17) } \} \\
 & \{(b,a) : b(\Psi \cdot R \cdot \Phi)a\} \\
= & \quad \{ \text{ composition } \}
\end{array}
$$

Projection and selection

$$\{(b,a) : \langle \exists\ c \ :\ b\ \Psi\ c :\ c(R\cdot\Phi)a\rangle\}$$

$$= \quad \{\ \text{coreflexive } \Psi = \lceil \psi \rceil \text{ (4) ; } \exists\text{-trading}\ \}$$

$$\{(b,a) : \langle \exists\ c \ :\ b = c :\ \psi b \wedge c(R\cdot\Phi)a\rangle\}$$

$$= \quad \{\ \exists\text{-one-point ; composition again}\ \}$$

$$\{(b,a) : \psi\ b \wedge \langle \exists\ d \ ::\ b\ R\ d \wedge d\ \Phi\ a\rangle\}$$

$$= \quad \{\ \text{coreflexive } \Phi = \lceil \phi \rceil \text{ (4) ; } \exists\text{-trading}\ \}$$

$$\{(b,a) : \psi\ b \wedge \langle \exists\ d \ :\ d = a :\ b\ R\ d \wedge \phi\ a\rangle\}$$

$$= \quad \{\ \exists\text{-one-point ; trivia}\ \}$$

$$\{(b,a) : \psi\ b \wedge b\ R\ a \wedge \phi\ a\}$$

Exercise 4: Check (20).

□

Two useful coreflexives

Domain:

$$\delta\, R \quad \triangleq \quad \ker R \cap id \tag{21}$$

Range:

$$\rho\, R \quad \triangleq \quad \mathrm{img}\, R \cap id \tag{22}$$

Facts:

$$\delta\, R \quad = \quad \rho\,(R^\circ) \tag{23}$$
$$\delta\,(R \cdot S) \quad = \quad \delta\,(\delta\, R \cdot S) \tag{24}$$
$$\rho\,(R \cdot S) \quad = \quad \rho\,(R \cdot \rho\, S) \tag{25}$$
$$R \quad = \quad R \cdot (\delta\, R) \tag{26}$$
$$R \quad = \quad (\rho\, R) \cdot R \tag{27}$$

Relating coreflexives with conditions

Pre and post restriction:

$$R \cdot \Phi = R \cap \top \cdot \Phi \tag{28}$$

$$\Psi \cdot R = R \cap \Psi \cdot \top \tag{29}$$

Domain/range elimination:

$$\top \cdot \delta\, R = \top \cdot R \tag{30}$$

$$\rho\, R \cdot \top = R \cdot \top \tag{31}$$

Mapping back and forward:

$$\Phi \subseteq \Psi \equiv \Phi \subseteq \top \cdot \Psi \tag{32}$$

Exercise 5: Show that

$$\delta\, R \subseteq \delta\, S \equiv R \subseteq \top \cdot S \tag{33}$$

holds.

□

Application — satisfiability

In the **pre**/**post** specification style, by writing

$$\begin{array}{l} \mathit{Spec} : (b : B) \leftarrow (a : A) \\ \textbf{pre} \;\; \ldots \\ \textbf{post} \;\; \ldots \end{array}$$

we mean the definition of two predicates

$$\begin{array}{l} \text{pre-}\mathit{Spec} : A \longrightarrow \mathbb{B} \\ \text{post-}\mathit{Spec} : B \times A \longrightarrow \mathbb{B} \end{array}$$

such that the **satisfiability** condition holds:

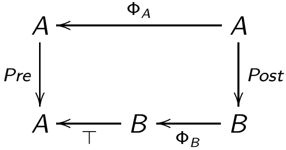
$$\langle \forall\ a\ :\ a \in A :\ \text{pre-}\mathit{Spec}\ a \Rightarrow \langle \exists\ b\ :\ b \in B :\ \text{post-}\mathit{Spec}(b, a) \rangle \rangle \qquad (34)$$

Application — satisfiability

Let us abbreviate

- $\lceil \text{pre-}Spec \rceil$ by Pre
- $\lceil \text{post-}Spec \rceil$ by $Post$
- $\lceil (\in A) \rceil$ by Φ_A, which in general encompasses an invariant associated to datatype A
- $\lceil (\in B) \rceil$ by Φ_B, which in general encompasses an invariant associated to datatype B

Then (34) PF-transforms to



$$Pre \cdot \Phi_A \subseteq \top \cdot \Phi_B \cdot Post \qquad (35)$$

Application — functional satisfiability

Case $Pre = id$, $Post = f$:

$$
\begin{array}{ll}
 & \Phi_A \subseteq \top \cdot \Phi_B \cdot f \\
\equiv & \quad \{ \text{ shunting (44) } \} \\
 & \Phi_A \cdot f^\circ \subseteq \top \cdot \Phi_B \\
\equiv & \quad \{ \text{ converses } \} \\
 & f \cdot \Phi_A \subseteq \Phi_B \cdot \top \\
\equiv & \quad \{ \text{ (45), since } f \cdot \Phi_A \subseteq f \ \} \\
 & f \cdot \Phi_A \subseteq f \cap \Phi_B \cdot \top \\
\equiv & \quad \{ \text{ (29) } \} \\
 & f \cdot \Phi_A \subseteq \Phi_B \cdot f
\end{array}
$$

What does this mean?

Functional satisfiability $\equiv$ invariant preservation

Let us introduce variables in $f \cdot \Phi_A \subseteq \Phi_B \cdot f$:

$$
\begin{array}{ll}
& f \cdot \Phi_A \subseteq \Phi_B \cdot f \\
\equiv & \quad \{ \text{ shunting (43) } \} \\
& \Phi_A \subseteq f^\circ \cdot \Phi_B \cdot f \\
\equiv & \quad \{ \text{ introduce variables } \} \\
& \langle \forall\ a, a' \ :\ a\ \Phi_A\ a' :\ (f\ a) \Phi_B (f\ a') \rangle \\
\equiv & \quad \{ \text{ coreflexives } (a = a') \ \} \\
& \langle \forall\ a \ ::\ a\ \Phi_A\ a \Rightarrow (f\ a) \Phi_B (f\ a) \rangle \\
\equiv & \quad \{ \text{ meaning of } \Phi_A,\ \Phi_B \ \} \\
& \langle \forall\ a \ :\ a \in A :\ (f\ a) \in B \rangle
\end{array}
$$

Invariant preservation

Another way to put it:

$$
\begin{array}{cl}
 & f \cdot \Phi_A \subseteq \Phi_B \cdot f \\
\equiv & \{ \text{ shunting } \} \\
 & f \cdot \Phi_A \cdot f^\circ \subseteq \Phi_B \\
\equiv & \{ \text{ coreflexives } \} \\
 & f \cdot \Phi_A \cdot \Phi_A^\circ \cdot f^\circ \subseteq \Phi_B \\
\equiv & \{ \text{ image definition } \} \\
 & \mathrm{img}\,(f \cdot \Phi_A) \subseteq \Phi_B \\
\equiv & \{ \; f \cdot \Phi_A \text{ is simple } \} \\
 & \rho\,(f \cdot \Phi_A) \subseteq \Phi_B
\end{array}
$$

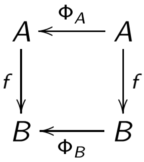
Invariant preservation

We will write "type declaration"

$$\Phi_B \xleftarrow{\;f\;} \Phi_A \tag{36}$$

to mean

$$f \cdot \Phi_A \;\subseteq\; \Phi_B \cdot f$$ cf. diagram



equivalent to both

$$f \cdot \Phi_A \;\subseteq\; \Phi_B \cdot \top \tag{37}$$

$$\rho\,(f \cdot \Phi_A) \;\subseteq\; \Phi_B \tag{38}$$

Exercises (ESC rules)

Exercise 6: Infer from (36) and properties (43) to (47) the following ESC (*extended static checking*) properties:

$$\Phi_B \xleftarrow{f} \Phi_{A1} \cup \Phi_{A2} \quad \equiv \quad \Phi_B \xleftarrow{f} \Phi_{A1} \ \wedge \ \Phi_B \xleftarrow{f} \Phi_{A2} \qquad (39)$$

$$\Phi_{B1} \cdot \Phi_{B2} \xleftarrow{f} \Phi_A \quad \equiv \quad \Phi_{B1} \xleftarrow{f} \Phi_A \ \wedge \ \Phi_{B2} \xleftarrow{f} \Phi_A \qquad (40)$$

□

Exercise 7: Using (37) and the relational version of McCarthy's conditional combinator which follows,

$$p \rightarrow f, g \ = \ f \cdot \lceil p \rceil \cup g \cdot \lceil \neg p \rceil \qquad (41)$$

infer the *conditional ESC* rule which follows:

$$\Phi_B \xleftarrow{p \rightarrow f, g} \Phi_A \quad \equiv \quad \Phi_B \xleftarrow{f} \Phi_A \cdot \lceil p \rceil \ \wedge \ \Phi_B \xleftarrow{g} \Phi_A \cdot \lceil \neg p \rceil \qquad (42)$$

□

Exercises (ESC by calculation)

Exercise 8: Recall that our motivating ESC assertion (1) was stated but not proved. Now that we know that (1) PF-transforms to

$\lceil even \rceil \xleftarrow{twice} \lceil even \rceil$ and that $\lceil even \rceil = \rho\, twice$, complete the following *"almost no work at all"* PF-calculation of (1):

$$
\begin{array}{cl}
 & \lceil even \rceil \xleftarrow{twice} \lceil even \rceil \\
\equiv & \{ \ \ldots\ldots\ldots \ \} \\
 & twice \cdot \lceil even \rceil \subseteq \lceil even \rceil \cdot twice \\
\equiv & \{ \ \ldots\ldots\ldots \ \} \\
 & twice \cdot \lceil even \rceil \subseteq \rho\, twice \cdot twice
\end{array}
\qquad
\begin{array}{cl}
\equiv & \{ \ \ldots\ldots\ldots \ \} \\
 & twice \cdot \lceil even \rceil \subseteq twice \\
\Leftarrow & \{ \ \ldots\ldots\ldots \ \} \\
 & \lceil even \rceil \subseteq id \\
\equiv & \{ \ \ldots\ldots\ldots \ \} \\
 & \textsc{True}
\end{array}
$$

□

Background

The following facts have been of help throughout this set of slides:

- Shunting rules:

$$f \cdot R \subseteq S \equiv R \subseteq f^\circ \cdot S \tag{43}$$

$$R \cdot f^\circ \subseteq S \equiv R \subseteq S \cdot f \tag{44}$$

- $\cap$-universal:

$$X \subseteq R \cap S \equiv X \subseteq R \wedge X \subseteq S \tag{45}$$

- $\cup$-universal:

$$R \cup S \subseteq X \equiv R \subseteq X \wedge S \subseteq X \tag{46}$$

- $(R\cdot)$-distribution:

$$R \cdot (S \cup T) = R \cdot S \cup R \cdot T \tag{47}$$