

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	$b \perp a$

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

$$\langle \forall x, y : y = 2x \wedge \text{even } x : \text{even } y \rangle \quad (1)$$

expressing the fact that function $y = 2x$ preserves even numbers, where $\text{even } x \triangleq \text{rem}(x, 2) = 0$ 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:

$$\langle \forall x : \phi x : \phi (f x) \rangle \quad (2)$$

- Proposition (2) is itself a particular case of

$$\langle \forall x : \phi x : \psi (f x) \rangle \quad (3)$$

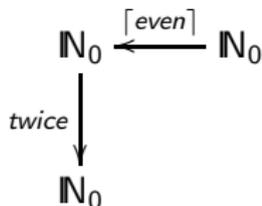
which states that f **ensures** property ψ on its output everytime property ϕ holds on its input.

Answer

First PF-transform scope:

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

cf. diagram



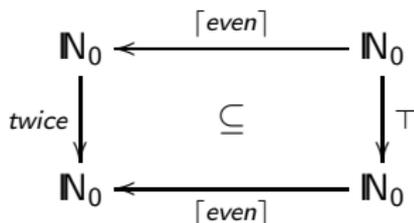
Now the whole thing

$$\begin{aligned}
 & \langle \forall x, y : y = 2x \wedge \text{even } x : \text{even } y \rangle \\
 \equiv & \quad \{ \text{above} \} \\
 & \langle \forall x, y : y(\text{twice} \cdot \lceil \text{even} \rceil)x : \text{even } y \rangle \\
 \equiv & \quad \{ \exists\text{-one-point} \} \\
 & \langle \forall x, y : y(\text{twice} \cdot \lceil \text{even} \rceil)x : \langle \exists z : z = y : \text{even } z \rangle \rangle \\
 \equiv & \quad \{ \text{predicate calculus: } p \wedge \text{TRUE} = p \} \\
 & \langle \forall x, y : y(\text{twice} \cdot \lceil \text{even} \rceil)x : \langle \exists z :: z = y \wedge \text{even } z \wedge \text{TRUE} \rangle \rangle \\
 \equiv & \quad \{ \top \text{ is the top relation} \} \\
 & \langle \forall x, y : y(\text{twice} \cdot \lceil \text{even} \rceil)x : \langle \exists z :: y \lceil \text{even} \rceil z \wedge z \top x \rangle \rangle \\
 \equiv & \quad \{ \text{composition} \}
 \end{aligned}$$

Now the whole thing

$$\begin{aligned}
 & \langle \forall x, y : y(\textit{twice} \cdot [\textit{even}])x : y([\textit{even}] \cdot \top)x \rangle \\
 \equiv & \quad \{ \textit{go pointfree (inclusion)} \} \\
 & \textit{twice} \cdot [\textit{even}] \subseteq [\textit{even}] \cdot \top
 \end{aligned}$$

cf. diagram



In summary

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

- $\llbracket \textit{even} \rrbracket$ such that

$$z \llbracket \textit{even} \rrbracket x \triangleq z = x \wedge \textit{even} z$$

— that is, $\llbracket \textit{even} \rrbracket$ is a **coreflexive** relation;

- $\llbracket \textit{even} \rrbracket \cdot \top$, which is such that

$$z(\llbracket \textit{even} \rrbracket \cdot \top)x \equiv \textit{even} z$$

— a so-called (left) *condition*.

Coreflexives

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

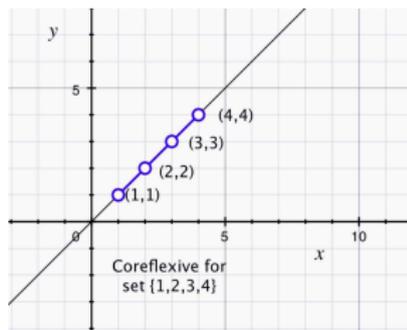
$$\Phi = [p] \equiv (y \Phi x \equiv y = x \wedge p y) \quad (4)$$

Via cancellation, (4) yields

$$y [p] x \equiv y = x \wedge p y \quad (5)$$

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

$$[1 \leq x \leq 4] =$$



Exercises

Exercise 1: Let *false* be the “everywhere false” predicate such that $\text{false } x = \text{FALSE}$ for all x , that is, $\text{false} = \underline{\text{FALSE}}$. Use (4) to show that $\llbracket \text{false} \rrbracket = \perp$.



Exercise 2: Given a set S , let Φ_S abbreviate coreflexive $\llbracket (\in S) \rrbracket$. 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:

$$[p \wedge q] = [p] \cdot [q] \quad (6)$$

$$[p \vee q] = [p] \cup [q] \quad (7)$$

$$[\neg p] = id - [p] \quad (8)$$

$$[false] = \perp \quad (9)$$

$$[true] = id \quad (10)$$

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**:

$$\Phi^\circ = \Phi = \Phi \cdot \Phi \quad (11)$$

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

$$\Phi \cap \Psi = \Phi \cdot \Psi \quad (12)$$

- Closure properties:

$$R \cdot \Phi \subseteq S \equiv R \cdot \Phi \subseteq S \cdot \Phi \quad (13)$$

$$\Phi \cdot R \subseteq S \equiv \Phi \cdot R \subseteq \Phi \cdot S \quad (14)$$

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 $\Phi = [\phi]$ and $\Psi = [\psi]$:

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

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

- Guarded **inclusion**:

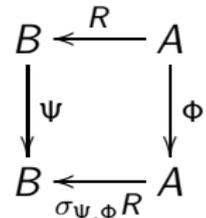
$$\begin{aligned} \langle \forall b, a : \phi b \wedge \psi a : b R a \Rightarrow b S a \rangle \\ \equiv \Phi \cdot R \cdot \Psi \subseteq S \end{aligned} \quad (16)$$

See next slide for some related terminology.

Projection and selection

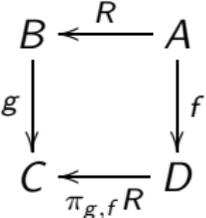
The following relational operators capture two useful relational patterns involving relations, coreflexives and functions:

- Selection:

$$\sigma_{\psi, \phi} R \triangleq \psi \cdot R \cdot \phi \quad (17)$$


The diagram shows a square with nodes B at the top-left and bottom-left, and A at the top-right and bottom-right. A horizontal arrow labeled R points from A to B at the top. A horizontal arrow labeled $\sigma_{\psi, \phi} R$ points from A to B at the bottom. A vertical arrow labeled ψ points from the top B to the bottom B . A vertical arrow labeled ϕ points from the top A to the bottom A .

- Projection:

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


The diagram shows a square with nodes B at the top-left and bottom-left, and A at the top-right and bottom-right. A horizontal arrow labeled R points from A to B at the top. A horizontal arrow labeled $\pi_{g, f} R$ points from D to C at the bottom. A vertical arrow labeled g points from the top B to the bottom C . A vertical arrow labeled f points from the top A to the bottom D .

Projection and selection

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

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

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

Let us check (19):

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

Projection and selection

$$\begin{aligned}
 & \{(b, a) : \langle \exists c : b \Psi c : c(R \cdot \Phi)a \rangle\} \\
 = & \quad \{ \text{coreflexive } \Psi = [\psi] \text{ (4) ; } \exists\text{-trading} \} \\
 & \{(b, a) : \langle \exists c : b = c : \psi b \wedge c(R \cdot \Phi)a \rangle\} \\
 = & \quad \{ \exists\text{-one-point ; composition again} \} \\
 & \{(b, a) : \psi b \wedge \langle \exists d :: b R d \wedge d \Phi a \rangle\} \\
 = & \quad \{ \text{coreflexive } \Phi = [\phi] \text{ (4) ; } \exists\text{-trading} \} \\
 & \{(b, a) : \psi b \wedge \langle \exists d : d = a : b R d \wedge \phi a \rangle\} \\
 = & \quad \{ \exists\text{-one-point ; trivia} \} \\
 & \{(b, a) : \psi b \wedge b R a \wedge \phi a\}
 \end{aligned}$$

Exercise 4: Check (20).



Two useful coreflexives

Domain:

$$\delta R \triangleq \ker R \cap id \quad (21)$$

Range:

$$\rho R \triangleq \text{img } R \cap id \quad (22)$$

Facts:

$$\delta R = \rho(R^\circ) \quad (23)$$

$$\delta(R \cdot S) = \delta(\delta R \cdot S) \quad (24)$$

$$\rho(R \cdot S) = \rho(R \cdot \rho S) \quad (25)$$

$$R = R \cdot (\delta R) \quad (26)$$

$$R = (\rho R) \cdot R \quad (27)$$

Relating coreflexives with conditions

Pre and post restriction:

$$R \cdot \Phi = R \cap T \cdot \Phi \quad (28)$$

$$\Psi \cdot R = R \cap \Psi \cdot T \quad (29)$$

Domain/range elimination:

$$T \cdot \delta R = T \cdot R \quad (30)$$

$$\rho R \cdot T = R \cdot T \quad (31)$$

Mapping back and forward:

$$\Phi \subseteq \Psi \equiv \Phi \subseteq T \cdot \Psi \quad (32)$$

Exercise 5: Show that

$$\delta R \subseteq \delta S \equiv R \subseteq T \cdot S \quad (33)$$

holds.

□

Application — satisfiability

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

$$Spec : (b : B) \leftarrow (a : A)$$

pre ...

post ...

we mean the definition of two predicates

$$\text{pre-}Spec : A \rightarrow \mathbb{B}$$

$$\text{post-}Spec : B \times A \rightarrow \mathbb{B}$$

such that the **satisfiability** condition holds:

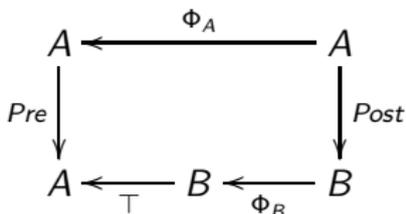
$$\langle \forall a : a \in A : \text{pre-}Spec a \Rightarrow \langle \exists b : b \in B : \text{post-}Spec(b, a) \rangle \rangle (34)$$

Application — satisfiability

Let us abbreviate

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

Then (34) PF-transforms to



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

Application — functional satisfiability

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

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

What does this mean?

Functional satisfiability \equiv invariant preservation

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

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

Invariant preservation

Another way to put it:

$$\begin{aligned}
 & f \cdot \Phi_A \subseteq \Phi_B \cdot f \\
 \equiv & \quad \{ \text{shunting} \} \\
 & f \cdot \Phi_A \cdot f^\circ \subseteq \Phi_B \\
 \equiv & \quad \{ \text{coreflexives} \} \\
 & f \cdot \Phi_A \cdot \Phi_A^\circ \cdot f^\circ \subseteq \Phi_B \\
 \equiv & \quad \{ \text{image definition} \} \\
 & \text{img}(f \cdot \Phi_A) \subseteq \Phi_B \\
 \equiv & \quad \{ f \cdot \Phi_A \text{ is simple} \} \\
 & \rho(f \cdot \Phi_A) \subseteq \Phi_B
 \end{aligned}$$

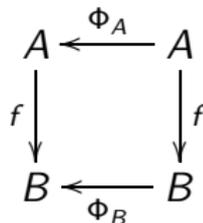
Invariant preservation

We will write “type declaration”

$$\Phi_B \xleftarrow{f} \Phi_A \quad (36)$$

to mean

$$f \cdot \Phi_A \subseteq \Phi_B \cdot f \quad \text{cf. diagram}$$



equivalent to both

$$f \cdot \Phi_A \subseteq \Phi_B \cdot \top \quad (37)$$

$$\rho(f \cdot \Phi_A) \subseteq \Phi_B \quad (38)$$

Exercises (ESC rules)

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

$$\Phi_B \xleftarrow{f} \Phi_{A_1} \cup \Phi_{A_2} \quad \equiv \quad \Phi_B \xleftarrow{f} \Phi_{A_1} \wedge \Phi_B \xleftarrow{f} \Phi_{A_2} \quad (39)$$

$$\Phi_{B_1} \cdot \Phi_{B_2} \xleftarrow{f} \Phi_A \quad \equiv \quad \Phi_{B_1} \xleftarrow{f} \Phi_A \wedge \Phi_{B_2} \xleftarrow{f} \Phi_A \quad (40)$$

□

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

$$p \rightarrow f, g = f \cdot [p] \cup g \cdot [\neg p] \quad (41)$$

infer the *conditional ESC* rule which follows:

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

□

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

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

$$\begin{array}{lcl}
 & \lceil \text{even} \rceil \xleftarrow{\text{twice}} \lceil \text{even} \rceil & \equiv \{ \dots\dots\dots \} \\
 \equiv & \{ \dots\dots\dots \} & \text{twice} \cdot \lceil \text{even} \rceil \subseteq \text{twice} \\
 & \text{twice} \cdot \lceil \text{even} \rceil \subseteq \lceil \text{even} \rceil \cdot \text{twice} & \leftarrow \{ \dots\dots\dots \} \\
 \equiv & \{ \dots\dots\dots \} & \lceil \text{even} \rceil \subseteq \text{id} \\
 & \text{twice} \cdot \lceil \text{even} \rceil \subseteq \rho \text{ twice} \cdot \text{twice} & \equiv \{ \dots\dots\dots \} \\
 & & \text{TRUE}
 \end{array}$$

□

Background

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

- Shunting rules:

$$f \cdot R \subseteq S \equiv R \subseteq f^\circ \cdot S \quad (43)$$

$$R \cdot f^\circ \subseteq S \equiv R \subseteq S \cdot f \quad (44)$$

- \cap -universal:

$$X \subseteq R \cap S \equiv X \subseteq R \wedge X \subseteq S \quad (45)$$

- \cup -universal:

$$R \cup S \subseteq X \equiv R \subseteq X \wedge S \subseteq X \quad (46)$$

- $(R \cdot)$ -distribution:

$$R \cdot (S \cup T) = R \cdot S \cup R \cdot T \quad (47)$$