UCE: MFES-09/10

(`http://wiki.di.uminho.pt/twiki/bin/view/Education/MFES`)

CSI Module — Exercise list nr.1

M.Sc. Degree in Informatics
and Informatics Engineering
University of Minho

NB: Proposed solutions are given in red. Equation numbers of the form ([3]:n) are taken from [3]. **Notation conventions:** outfix notation such as that used in *splits* and *juncs* provides for unambiguous parsing of relational algebra expressions. Concerning infix operators (such as eg. composition, $\cup$) and unary ones (eg. converse) the following conventions will be adopted for saving parentheses: (a) unary and prefix operators (eg. δ, ρ) bind tighter than binary; (b) composition binds tighter than any other binary operator.

1 2009.11.26

Exercise 1. (adapted from exercise 5.1.4 in C.B. Jones's *Systematic Software Development Using VDM* [1]):

> Hotel room numbers are pairs (l, r) where l indicates a floor and r a door number in floor l. Write the invariant on room numbers which captures the following rules valid in a particular hotel with 25 floors, 60 rooms per floor:
> 1. there is no floor number 13; (guess why)
> 2. level 1 is an open area and has no rooms;
> 3. the top five floors consist of large suites and these are numbered with even integers.

Proposed solution:

$$Floor = \mathbb{N}$$
$$\textbf{inv}\ \ l \triangleq l \in 26 - \{13\}$$

$$Room = \mathbb{N}$$
$$\textbf{inv}\ \ r \triangleq r \in 60$$

$$HotelRoom = Floor \times Room$$
$$\textbf{inv}\ \ (l, r) \triangleq l \neq 1\ \wedge\ (l > 21 \Rightarrow even\ r)$$

□

Exercise 2. Check rule

$$\langle \exists\, i\ :\ R :\ T \rangle = \langle \exists\, i\ :\ T :\ R \rangle \tag{1}$$

□

Proposed solution:

$$
\begin{array}{ll}
 & \langle \exists\, i \;:\; R :\; T \rangle \\
\Leftrightarrow & \qquad \{\;\; \wedge\text{-unit is } \textsc{True} \;\; \} \\
 & \langle \exists\, i \;:\; \textsc{True} \,\wedge\, R :\; T \rangle \\
\Leftrightarrow & \qquad \{\;\; \exists\text{-trading ([3]:174)} \;\; \} \\
 & \langle \exists\, i \;::\; R \,\wedge\, T \rangle \\
\Leftrightarrow & \qquad \{\;\; \wedge\text{-commutativity} \;\; \} \\
 & \langle \exists\, i \;::\; T \,\wedge\, R \rangle \\
\Leftrightarrow & \qquad \{\;\; \exists\text{-trading ([3]:174)} \;\; \} \\
 & \langle \exists\, i \;:\; T :\; R \rangle
\end{array}
$$

□

Exercise 3. Check **carefully** which rules of the quantifier calculus need to be applied to prove that predicate

$$\langle \forall\, b, a \;:\; \langle \exists\, c \;:\; b = f\ c :\; r(c, a) \rangle :\; s(b, a) \rangle \tag{2}$$

is the same as

$$\langle \forall\, c, a \;:\; r(c, a) :\; s(f\ c, a) \rangle \tag{3}$$

where f is a function and r, s are binary predicates.

□

Proposed solution: check the following steps —

$$
\begin{array}{ll}
 & \langle \forall\, b, a \;:\; \langle \exists\, c \;:\; b = f\ c :\; r(c, a) \rangle :\; s(b, a) \rangle \\
\Leftrightarrow & \qquad \{\;\; \forall\text{-nesting ([3]:179)} \;\; \} \\
 & \langle \forall\, a \;::\; \langle \forall\, b \;:\; \langle \exists\, c \;:\; b = f\ c :\; r(c, a) \rangle :\; s(b, a) \rangle \rangle \\
\Leftrightarrow & \qquad \{\;\; \exists\text{-trading ([3]:174)} \;\; \} \\
 & \langle \forall\, a \;::\; \langle \forall\, b \;:\; \langle \exists\, c \;:\; r(c, a) :\; b = f\ c \rangle :\; s(b, a) \rangle \rangle \\
\Leftrightarrow & \qquad \{\;\; \text{splitting ([3]:183)} \;\; \} \\
 & \langle \forall\, a \;::\; \langle \forall\, c \;:\; r(c, a) :\; \langle \forall\, b \;:\; b = f\ c :\; s(b, a) \rangle \rangle \rangle \\
\Leftrightarrow & \qquad \{\;\; \forall\text{-one-point ([3]:175)} \;\; \} \\
 & \langle \forall\, a \;::\; \langle \forall\, c \;:\; r(c, a) :\; s(f\ c, a) \rangle \rangle \\
\Leftrightarrow & \qquad \{\;\; \forall\text{-nesting ([3]:179)} \;\; \} \\
 & \langle \forall\, c, a \;:\; r(c, a) :\; s(f\ c, a) \rangle
\end{array}
$$

□

Exercise 4. Define relations $C \xleftarrow{R} A$, $A \xleftarrow{S} B$ such that $cRa = r(c,a)$ and $bSa = s(b,a)$. Then PF-transform (2) and (3), showing that the equivalence proved above is nothing but the rule

$$f \cdot R \subseteq S \Leftrightarrow R \subseteq f^{\circ} \cdot S \tag{4}$$

which is number ([3]:67) in the tutorial. □

Proposed solution:

- PF-transform of (2) —

$$\begin{aligned}
& \langle \forall\, b,a \;:\; \langle \exists\, c \;:\; b = f\ c :\ r(c,a)\rangle :\ s(b,a)\rangle \\
\Leftrightarrow \quad & \{\ f \text{ is a function; introducing relations } R \text{ and } S\ \} \\
& \langle \forall\, b,a \;:\; \langle \exists\, c \;:\; b\ f\ c :\ cRa)\rangle :\ bSa\rangle \\
\Leftrightarrow \quad & \{\ \text{composition ([3]:12)}\ \} \\
& \langle \forall\, b,a \;:\; b(f \cdot R)a :\ bSa\rangle \\
\Leftrightarrow \quad & \{\ \text{entailment is inclusion ([3]:13)}\ \} \\
& f \cdot R \subseteq S
\end{aligned}$$

- PF-transform of (3) —

$$\begin{aligned}
& \langle \forall\, c,a \;:\; r(c,a) :\ s(f\ c,a)\rangle \\
\Leftrightarrow \quad & \{\ \text{introducing relations } R \text{ and } S\ \} \\
& \langle \forall\, c,a \;:\; cRa :\ (f\ c)Sa\rangle \\
\Leftrightarrow \quad & \{\ \text{([3]:27)}\ \} \\
& \langle \forall\, c,a \;:\; cRa :\ c(f^{\circ} \cdot S)a\rangle \\
\Leftrightarrow \quad & \{\ \text{entailment is inclusion ([3]:13)}\ \} \\
& R \subseteq f^{\circ} \cdot S
\end{aligned}$$

□

Exercise 5. (This is exercise [3]:5.) Given a function $B \xleftarrow{f} A$, show that *img* f is the coreflexive Φ_p of predicate $p\ x \triangleq \langle \exists\, a \;::\; x = f\ a\rangle$.
□

Proposed solution:

$$\begin{aligned}
& y(\mathit{img}\ f)x \\
\Leftrightarrow \quad & \{\ \text{def. image ([3]:29)}\ \} \\
& y(f \cdot f^{\circ})x \\
\Leftrightarrow \quad & \{\ \text{composition ([3]:12)}\ \} \\
& \langle \exists\, a \;::\; yfa \,\wedge\, af^{\circ}x\rangle \\
\Leftrightarrow \quad & \{\ f \text{ is a function (twice) ; converse of } f\ \} \\
& \langle \exists\, a \;::\; y = fa \,\wedge\, x = f\ a\rangle
\end{aligned}$$

$$
\begin{array}{ll}
\Leftrightarrow & \{\ \text{equality is transitive ; predicate logic: } p \Rightarrow q \text{ iff } p = p \wedge q\ \} \\
& \langle \exists\, a\ ::\ y = f a\ \wedge\ x = f\ a\ \wedge\ y = x \rangle \\
\Leftrightarrow & \{\ \text{equality is transitive ; predicate logic: } p \Rightarrow q \text{ iff } p = p \wedge q\ \} \\
& \langle \exists\, a\ ::\ y = x\ \wedge\ x = f\ a \rangle \\
\Leftrightarrow & \{\ \exists\text{-trading ([3]:174)}\ \} \\
& \langle \exists\, a\ :\ y = x :\ x = f\ a \rangle \\
\Leftrightarrow & \{\ x, y \text{ are free}\ \} \\
& (y = x)\ \wedge\ \underbrace{\langle \exists\, a\ ::\ x = f\ a \rangle}_{p} \\
\Leftrightarrow & \{\ \text{definition of coreflexive of predicate } p\ \} \\
& \Phi_p
\end{array}
$$

□

Exercise 6. Justify the following PF calculation of ([3]:67), where the equivalence is proved by cyclic implication ("ping-pong"):

$$
\begin{array}{ll}
& f \cdot R \subseteq S \\
\Rightarrow & \{\ \text{monotonicity of composition}\ \} \\
& f^\circ \cdot f \cdot R \subseteq f^\circ \cdot S \\
\Rightarrow & \{\ \text{functions are entire ([3]:30) ; monotonicity ; transitivity}\ \} \\
& R \subseteq f^\circ \cdot S \\
\Rightarrow & \{\ \text{monotonicity of composition}\ \} \\
& f \cdot R \subseteq f \cdot f^\circ \cdot S \\
\Rightarrow & \{\ \text{functions are simple ([3]:30) ; monotonicity ; transitivity}\ \} \\
& f \cdot R \subseteq S
\end{array}
$$

□

Exercise 7. So, for f entire and simple ($\Leftrightarrow$ a function) rule ([3]:67) holds. Now, suppose that rule ([3]:67) holds for f replaced by an arbitrary relation X:

$$X \cdot R \subseteq S \Leftrightarrow R \subseteq X^\circ \cdot S \qquad (5)$$

Check what you can infer about this rule for the particular instantiations:

- $R, S := id, X$ (left-cancellation)
- $S, R := id, X^\circ$ (right-cancellation)

Conclude that (5) holds **if and only if** X is a function.
□

Proposed solution:

– Substitution $R, S := id, X$:

$$
\begin{array}{ll}
& X \cdot id \subseteq X \Leftrightarrow id \subseteq X^\circ \cdot X \\
\Leftrightarrow & \quad \{ \text{ natural-}id\text{; } X \subseteq X \text{ always true } (\subseteq \text{ is reflexive}) \} \\
& \textsc{True} \Leftrightarrow id \subseteq X^\circ \cdot X \\
\Leftrightarrow & \quad \{ \text{ trivia } \} \\
& id \subseteq X^\circ \cdot X \\
\Leftrightarrow & \quad \{ \text{ ([3]:30) } \} \\
& X \text{ is entire}
\end{array}
$$

– Substitution $S, R := id, X^\circ$:

$$
\begin{array}{ll}
& X \cdot X^\circ \subseteq id \Leftrightarrow X^\circ \subseteq X^\circ \cdot id \\
\Leftrightarrow & \quad \{ \text{ natural-}id\text{; } X^\circ \subseteq X^\circ \text{ always true } \} \\
& X \cdot X^\circ \subseteq id \\
\Leftrightarrow & \quad \{ \text{ ([3]:30) } \} \\
& X \text{ is simple}
\end{array}
$$

Thus:

- The previous exercise shows that, for X simple and entire (a function), (5) holds
- The current exercise shows that, if (5) holds, then X is a function,

Thus:

*Conclude that (5) holds **if and only if** X is a function.*

□ □

Exercise 8. Complete the following calculation about functions:

$$
\begin{array}{ll}
& f \subseteq g \\
\Leftrightarrow & \quad \{ \text{ natural-}id \} \\
& f \cdot id \subseteq g \\
\Leftrightarrow & \quad \{ \text{ shunting on } f \text{ ([3]:67) } \} \\
& id \subseteq f^\circ \cdot g \\
\Leftrightarrow & \quad \{ \text{ shunting on } g \text{ ([3]:68) } \} \\
& id \cdot g^\circ \subseteq f^\circ \\
\Leftrightarrow & \quad \{ \text{ natural-}id\text{; converses } \} \\
& g \subseteq f
\end{array}
$$

So $f \subseteq g \;\Leftrightarrow\; g \subseteq f$. Therefore

$$
f \subseteq g \Leftrightarrow f = g \Leftrightarrow f \supseteq g \qquad (6)
$$

Why?

□

Proposed solution:

$$
\begin{array}{ll}
& f = g \\
\Leftrightarrow & \quad \{ \text{“ping-pong ([3]:14)} \} \\
& f \subseteq g \ \wedge \ g \subseteq f \\
\Leftrightarrow & \quad \{ \text{previous calculation} \} \\
& f \subseteq g \\
\Leftrightarrow & \quad \{ \text{previous calculation} \} \\
& g \subseteq f
\end{array}
$$

□

2 2010.02.11

Exercise 9. Recalling universal properties (Galois connections)

$$X \subseteq R \cap S \ \Leftrightarrow \ X \subseteq R \wedge X \subseteq S \tag{7}$$

$$R \cup S \subseteq X \ \Leftrightarrow \ R \subseteq X \wedge S \subseteq X \tag{8}$$

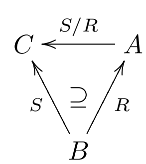
$$X \cdot R \subseteq Y \ \Leftrightarrow \ X \subseteq Y \,/\, R \tag{9}$$

resort to the *indirect equality* (IE) rule to calculate the following property of relation (right) division:

$$U \,/\, (R \cup S) = (U \,/\, R) \cap (U \,/\, S) \tag{10}$$

Moreover, resort to

$$\langle \forall\, b \ : \ a \, R \, b : \ c \, S \, b \rangle \tag{11}$$



in converting (10) to PW-notation. Which rule of universal quantification have you calculated?

Proposed solution: calculation of (10) is as follows

$$
\begin{array}{ll}
& X \subseteq U \,/\, (R \cup S) \\
\Leftrightarrow & \quad \{ \text{(9) ; distribution of lower-adjoint } (X \cdot) \} \\
& X \cdot R \cup X \cdot S \subseteq U \\
\Leftrightarrow & \quad \{ \text{(8) ; (9) twice} \} \\
& X \subseteq U \,/\, R \ \wedge \ X \subseteq U \,/\, S \\
\Leftrightarrow & \quad \{ \text{(7)} \} \\
& X \subseteq U \,/\, R \cap U \,/\, S \\
:: & \quad \{ \text{IE} \} \\
& U \,/\, (R \cup S) = (U \,/\, R) \cap (U \,/\, S)
\end{array}
$$

Literally, the PW conversion of this is, for all suitably typed a and c :

$$\langle \forall\, b \;:\; a\,R\,b \vee a\,S\,b :\; c\,U\,b\rangle \Leftrightarrow \langle \forall\, b \;:\; a\,R\,b :\; c\,U\,b\rangle \;\wedge\; \langle \forall\, b \;:\; a\,S\,b :\; c\,U\,b\rangle$$

This is known as the ∀-Splitting rule, usually written as

$$\langle \forall\, b \;:\; R \vee S :\; U\rangle \quad\Leftrightarrow\quad \langle \forall\, b \;:\; R :\; U\rangle \;\wedge\; \langle \forall\, b \;:\; S :\; U\rangle$$

regarding R, S and U as predicate expressions and assuming dummies a,b,c implicit. □

Exercise 10. Resort to

$$\Phi_q \xleftarrow{R} \Phi_p \quad\Leftrightarrow\quad R \cdot \Phi_p \;\subseteq\; \Phi_q \cdot \top \tag{12}$$

in calculating the **split by conjunction** rule of the PO calculus of [3]:

$$\Phi_{q_1} \cdot \Phi_{q_2} \xleftarrow{R} \Phi_p \quad\Leftrightarrow\quad \Phi_{q_1} \xleftarrow{R} \Phi_p \;\wedge\; \Phi_{q_2} \xleftarrow{R} \Phi_p \tag{13}$$

NB: you will need the following distribution property,

$$(\Phi \cap \Psi) \cdot \top = (\Phi \cdot \top) \cap (\Psi \cdot \top) \tag{14}$$

easy to prove using indirect equality and GC $(f = \rho, g = (\cdot\top))$ — do it.

Proposed solution:

$$\begin{array}{ll}
& \Phi_{q_1} \cdot \Phi_{q_2} \xleftarrow{R} \Phi_p \\
\Leftrightarrow & \quad \{ \text{ (12) ; ([3]:60) } \} \\
& R \cdot \Phi_p \;\subseteq\; (\Phi_{q_1} \cap \Phi_{q_2}) \cdot \top \\
\Leftrightarrow & \quad \{ \text{ (14) ; (7) } \} \\
& R \cdot \Phi_p \;\subseteq\; \Phi_{q_1} \cdot \top \;\wedge\; R \cdot \Phi_p \;\subseteq\; \Phi_{q_2} \cdot \top \\
\Leftrightarrow & \quad \{ \text{ (12) twice } \} \\
& \Phi_{q_1} \xleftarrow{R} \Phi_p \;\wedge\; \Phi_{q_2} \xleftarrow{R} \Phi_p
\end{array}$$

□

Exercise 11. (This is exercise [3]:10.) From the free theorem of $1 \xleftarrow{!} A$ and fact $ker\,! = \top$ infer

$$f \cdot R \subseteq \top \cdot S \Leftrightarrow R \subseteq \top \cdot S \tag{15}$$

Proposed solution: FT of $1 \xleftarrow{!} A$ first:

$$\begin{array}{ll}
& !(\; 1 \longleftarrow A\;)! \\
\Leftrightarrow & \quad \{ \text{ clause ([3]:105) } \} \\
& ! \cdot R_A \subseteq R_1 \cdot ! \\
\Leftrightarrow & \quad \{ \; R_1 = id \text{ (1 is a constant type) and abbreviating } R_A \text{ by } R \; \} \\
& ! \cdot R \subseteq !
\end{array}$$

For functions:

$$! \cdot f = ! \qquad (16)$$

recall (6). Then we calculate (15):

$$\begin{array}{ll} & f \cdot R \subseteq \top \cdot S \\ \Leftrightarrow & \{ \ \top = ker\, ! \ \} \\ & f \cdot R \subseteq !^{\circ} \cdot ! \cdot S \\ \Leftrightarrow & \{ \text{ shunting on ! ([3]:67) followed by (16) } \} \\ & ! \cdot R \subseteq ! \cdot S \\ \Leftrightarrow & \{ \text{ shunting on ! ([3]:67) ; } \top = ker\, ! \ \} \\ & R \subseteq \top \cdot S \end{array}$$

□

Exercise 12. (This is the second part of exercise [3]:8.) A relation S is said to satisfy functional dependency $g \rightarrow f$ wherever projection $f \cdot S \cdot g^{\circ}$ is simple, that is, iff

$$ker\,(g \cdot S^{\circ}) \subseteq ker\, f \qquad (17)$$

holds [2]. Resort to ([3]:86), (17) and to the rules of both the PF-transform and the Eindhoven quantifier calculus to show that healthiness condition (17) imposed on mapping comprehension ([3]:88) is equivalent to

$$\langle \forall\, b, a \ : \ b, a \in dom\ S \ \wedge \ g\, b = g\, a : \ f(S\ b) = f(S\ a) \rangle$$

Proposed solution: The following rule, taken from [2]

Given two binary relations $B \xleftarrow{R,S} A$ *and two predicates* $2 \xleftarrow{\psi} A$ *and* $2 \xleftarrow{\phi} B$ *(coreflexively denoted by* Ψ *and* Φ*, respectively), then*

$$\Phi \cdot R \cdot \Psi \subseteq S \quad \Leftrightarrow \quad \langle \forall\, b, a \ : \ \phi\, b \ \wedge \ \psi\, a \ \wedge \ b\, R\, a : \ b\, S\, a \rangle \qquad (18)$$

□

saves some steps in the calculation:

$$\begin{array}{ll} & ker\,(g \cdot S^{\circ}) \subseteq ker\, f \\ \Leftrightarrow & \{ \text{ kernel (twice) ; converses } \} \\ & S \cdot g^{\circ} \cdot g \cdot S^{\circ} \subseteq f^{\circ} \cdot f \\ \Leftrightarrow & \{ \text{ ([3]:82, [3]:83) since } S \text{ is assumed simple } \} \\ & \delta\, S \cdot g^{\circ} \cdot g \cdot \delta\, S \subseteq S^{\circ} \cdot f^{\circ} \cdot f \cdot S \\ \Leftrightarrow & \{ \text{ (18) ; abbreviating notation } \} \\ & \langle \forall\, b, a \ : \ b, a \in dom\ S \ \wedge \ g\, b = g\, a : \ b(S^{\circ} \cdot f^{\circ} \cdot f \cdot S)a \rangle \\ \Leftrightarrow & \{ \text{ (18) ; compressing notation } \} \\ & \langle \forall\, b, a \ : \ b, a \in dom\ S \ \wedge \ g\, b = g\, a : \ b(S^{\circ} \cdot f^{\circ} \cdot f \cdot S)a \rangle \\ \Leftrightarrow & \{ \text{ see expansion of } b(S^{\circ} \cdot f^{\circ} \cdot f \cdot S)a \text{ below } \} \\ & \langle \forall\, b, a \ : \ b, a \in dom\ S \ \wedge \ g\, b = g\, a : \ b, a \in dom\ S \ \wedge \ f(S\ b) = f(S\ a) \rangle \\ \Leftrightarrow & \{ \text{ trading (31) on } b, a \in dom\ S \text{ so as to get rid of it in the body of the } \forall \ \} \\ & \langle \forall\, b, a \ : \ b, a \in dom\ S \ \wedge \ g\, b = g\, a : \ f(S\ b) = f(S\ a) \rangle \end{array}$$

Expansion of $b(S^\circ \cdot f^\circ \cdot f \cdot S)a$:

$$
\begin{aligned}
& b(S^\circ \cdot f^\circ \cdot f \cdot S)a \\
\Leftrightarrow \quad & \{ \text{ ([3]:12) twice ; compressing notation } \} \\
& \langle \exists\, y, x \ :: \ bS^\circ y \ \wedge \ f\ y = f\ x \ \wedge \ xSa \rangle \\
\Leftrightarrow \quad & \{ \text{ ([3]:86) twice ; converses } \} \\
& \langle \exists\, y, x \ :: \ b \in \mathit{dom}\ S \ \wedge \ y = S\ b \ \wedge \ f\ y = f\ x \ \wedge \ a \in \mathit{dom}\ S \ \wedge \ x = S\ a \rangle \\
\Leftrightarrow \quad & \{ \text{ quantifier calculus } \} \\
& b, a \in \mathit{dom}\ S \ \wedge \ \langle \exists\, y, x \ : \ y = S\ b \ \wedge \ x = S\ a : \ f\ y = f\ x \rangle \\
\Leftrightarrow \quad & \{ \text{ quantifier calculus ([3]:176) } \} \\
& b, a \in \mathit{dom}\ S \ \wedge \ f(S\ b) = f(S\ a)
\end{aligned}
$$

□

Exercise 13. Calculating with Alloy sequences, cf. eg. `sequence.als`:

```
sig Seq {
   seqElems: SeqIdx → lone elem
}
```

that is, sequences are $\mathbb{N}$ to A simple relations ($0 \notin \mathbb{N}$):

$$
\begin{aligned}
\mathit{Seq}\ A = & \ \mathbb{N} \longrightarrow A \\
\mathbf{inv}\ \ L \triangleq & \ \mathit{noHoles}\ L
\end{aligned}
$$

where

$$\mathit{noHoles}\ L \triangleq \ L \cdot \mathit{succ} \subseteq \top \cdot L \tag{19}$$

Operators:

$$\mathit{tail}\ L \triangleq \ L \cdot \mathit{succ} \tag{20}$$

$$\mathit{head}\ L \triangleq \ L \cdot \mathit{img}\ \underline{1} \tag{21}$$

$$c : L \triangleq \ \underline{c} \cdot \underline{1}^\circ \cup L \cdot \mathit{succ}^\circ \tag{22}$$

1. Transform (19) to PW-notation and check which of the following sequences represent sequence $[a, b, a]$:

$$
\begin{array}{c|c} A & \mathbb{N} \\ \hline a & 2 \\ a & 3 \\ b & 1 \end{array} ,
\begin{array}{c|c} A & \mathbb{N} \\ \hline a & 2 \\ a & 4 \\ b & 3 \end{array} ,
\begin{array}{c|c} A & \mathbb{N} \\ \hline a & 3 \\ a & 1 \\ b & 2 \end{array}
$$

Proposed solution:

$$
\begin{aligned}
& (19) \\
\Leftrightarrow \quad & \{ \text{ ([3]:13) ; ([3]:27) } \} \\
& \mathit{noHoles}\ L \ \Leftrightarrow \ \langle \forall\, a, n \ : \ a\ L\ (\mathit{succ}\ n) : \ a(\top \cdot L)n \rangle \\
\Leftrightarrow \quad & \{ \ \mathit{succ}\ n \triangleq n + 1 \text{; composition and } y \top x = \mathit{true} \ \} \\
& \mathit{noHoles}\ L \ \Leftrightarrow \ \langle \forall\, a, n \ : \ a\ L\ (n+1) : \ \langle \exists\, a' \ :: \ a'\ L\ n \rangle \rangle
\end{aligned} \tag{23}
$$

Right-case, as mid-case violates (23) for $n = 1$ and left-case corresponds to $[b, a, a]$.
□

2. Knowing that

$$img\,\underline{1} \cup img\,succ = id \tag{24}$$

show that $L = head\ L \cup (tail\ L) \cdot succ^\circ$.
NB: add variables to (24) beforehand just to see what it means.
Proposed solution: conversion of (24) to PW-notation:

$$\begin{array}{ll}
& (24) \\
\Leftrightarrow & \{\ \text{adding variables ; } b(R \cup S)a \Leftrightarrow bRa \vee bSa\ \} \\
& \langle \forall\, n, m\ ::\ n(img\,\underline{1})m \vee n(img\,succ)m\ \Leftrightarrow\ n = m \rangle \\
\Leftrightarrow & \{\ \text{substitution } m := n \text{ ; composition (twice) ; converses of functions}\ \} \\
& \langle \forall\, n\ ::\ \langle \exists\, a\ ::\ n = \underline{1}\ k\ \wedge\ n = \underline{1}\ k \rangle \vee \langle \exists\, k\ ::\ n = succ\ k \wedge\ = succ\ k \rangle \rangle \\
\Leftrightarrow & \{\ \text{constant functions ; predicate logic ; } succ\ k \triangleq\ k + 1\ \} \\
& \langle \forall\, n\ ::\ \langle \exists\, k\ ::\ n = 1 \rangle \vee \langle \exists\, k\ ::\ n = k + 1 \rangle \rangle \\
\Leftrightarrow & \{\ \text{drop redundant quantifier}\ \} \\
& \langle \forall\, n\ ::\ n = 1 \vee \langle \exists\, k\ ::\ n = k + 1 \rangle \rangle
\end{array}$$

(Cf. Peano algebra for the natural numbers.) Now the main part of the exercise:

$$\begin{array}{ll}
& L = head\ L \cup (tail\ L) \cdot succ^\circ \\
\Leftrightarrow & \{\ \text{definitions of } head \text{ and } tail\ \} \\
& L = L \cdot img\,\underline{1} \cup (L \cdot succ) \cdot succ^\circ \\
\Leftrightarrow & \{\ \text{associativity of composition ; distribution of lower-adjoint } (L\cdot)\ \} \\
& L = L \cdot (img\,\underline{1} \cup succ \cdot succ^\circ) \\
\Leftrightarrow & \{\ (24) \text{ ; } id\text{-natural}\ \} \\
& L = L
\end{array}$$

□

Exercise 14. Show that $\Phi_{noHoles} \xleftarrow{tail} \Phi_{noHoles}$ holds, that is, $tail\ L$ preserves invariant $noHoles$, that is, complete:

$$\begin{array}{ll}
& \Phi_{noHoles} \xleftarrow{tail} \Phi_{noHoles} \\
\Leftrightarrow & \{\ \text{go pointwise } (tail \text{ is a function})\ \} \\
& \langle \forall\, L\ :\ noHoles\ L :\ noHoles(tail\ L) \rangle \\
\Leftrightarrow & \{\ \text{inline (19) ; trading 091125b' (\textbf{??}) ; assume quantifier}\ \} \\
& L \cdot succ \subseteq \top \cdot L\ \Rightarrow\ ..... \\
\cdots & \{\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\ \} \\
& .....
\end{array}$$

Proposed solution:

$$\Leftrightarrow \quad \{ \text{ definition (20) twice } \}$$

$$L \cdot succ \subseteq \top \cdot L \Rightarrow (L \cdot succ) \cdot succ \subseteq \top \cdot (L \cdot succ)$$

$$\Leftrightarrow \quad \{ \text{ associativity of composition } \}$$

$$L \cdot succ \subseteq \top \cdot L \Rightarrow (L \cdot succ) \cdot succ \subseteq (\top \cdot L) \cdot succ)$$

$$\Leftrightarrow \quad \{ \text{ monotonicity of lower-adjoint } (\cdot succ) \}$$

$$L \cdot succ \subseteq \top \cdot L \Rightarrow (L \cdot succ) \cdot succ \subseteq (\top \cdot L) \cdot succ)$$

□

Exercise 15. Complete the proof below so as to show that $\Phi_{noHoles} \xleftarrow{(c:)} \Phi_{noHoles}$ holds:

$$L \cdot succ \subseteq \top \cdot L \Rightarrow (c : L) \cdot succ \subseteq \top \cdot (c : L)$$

We show that consequent $(c : L) \cdot succ \subseteq \top \cdot (c : L)$ is entailed by antecedent $L \cdot succ \subseteq \top \cdot L$:

$$(c : L) \cdot succ \subseteq \top \cdot (c : L)$$

$$\Leftrightarrow \quad \{ \text{ definition (22) } \}$$

$$(\underline{c} \cdot \underline{1}^{\circ} \cup L \cdot succ^{\circ}) \cdot succ \subseteq \top \cdot (c : L)$$

$$\Leftrightarrow \quad \{ \text{ distribution of lower-adjoint } (\cdot succ) \}$$

$$\underline{c} \cdot \underline{1}^{\circ} \cdot succ \cup L \cdot succ^{\circ} \cdot succ \subseteq \top \cdot (c : L)$$

$$\Leftrightarrow \quad \{ \text{ (8) followed by (15) } \}$$

$$\begin{cases} \underline{1}^{\circ} \cdot succ \subseteq \top \cdot (c : L) \\ L \cdot succ^{\circ} \cdot succ \subseteq \top \cdot (c : L) \end{cases}$$

$$\Leftrightarrow \quad \{ \ succ \text{ and } \underline{1} \text{ have disjoint images (there is no } n \in \mathbb{N} \text{ such that } 1 = n + 1) \text{ ; (24) } \}$$

$$\begin{cases} \bot \subseteq \top \cdot (c : L) \\ L \cdot (img\, \underline{1} \cup img\, succ) \subseteq \top \cdot (c : L) \end{cases}$$

$$\Leftrightarrow \quad \{ \ \bot \text{ is below anything ; (8) ; (22) } \}$$

$$\begin{cases} L \cdot img\, \underline{1} \subseteq \top \cdot (\underline{c} \cdot \underline{1}^{\circ} \cup L \cdot succ^{\circ}) \\ L \cdot (img\, succ) \subseteq \top \cdot (\underline{c} \cdot \underline{1}^{\circ} \cup L \cdot succ^{\circ}) \end{cases}$$

$$\Leftarrow \quad \{ \text{ distribution of } (\top \cdot) \text{ ; } R \subseteq X \text{ implies } R \subseteq X \cup Y \text{ (twice) } \}$$

$$\begin{cases} L \cdot img\, \underline{1} \subseteq \top \cdot \underline{1}^{\circ} \\ L \cdot (img\, succ) \subseteq \top \cdot L \cdot succ^{\circ} \end{cases}$$

$$\Leftrightarrow \quad \{ \text{ shunting on } \underline{1}^{\circ} \text{ ([3]:68) ; kernel of ! ; } succ \text{ is simple } \}$$

$$\begin{cases} L \cdot \underline{1} \cdot \subseteq \top \cdot \top \\ L \cdot (\rho\, succ) \subseteq \top \cdot L \cdot succ^{\circ} \end{cases}$$

$$\Leftrightarrow \quad \{ \ \top \cdot \top = \top \text{ ; domain / range duality } \}$$

$$\begin{cases} L \cdot \underline{1} \cdot \subseteq \top \\ L \cdot (\delta\,(succ^\circ)) \subseteq \top \cdot L \cdot succ^\circ \end{cases}$$

$\Leftrightarrow$ { $\top$ is above anything ; ([3]:83) }

$$L \cdot succ \subseteq \top \cdot L$$

Proposed solution: the calculation above is an improvement over that given in the classroom — only one strengthening (implication) step is needed. □

Exercise 16. Consider the definition of a new relation operator

$$slice(R, S) \triangleq R \cap S/R^\circ \tag{25}$$

1. Add variables to this definition and check the following encoding of this combinator in Alloy:

```
fun slice[r: K → A, s: A → A] : K → A {
  { a : r·dom, b : a·r | (all b' : a·r | b' in s·b) }
}
```

2. Check the outcome of $slice(R, \leq)$ for R the relation

$\mathbb{N}$	A
10	$John$
11	$Mary$
12	$John$
15	$Arthur$

NB: The aim of the *slice* combinator is to convert a given relation R into a simple relation by looking at particular (eg. maximal) elements of its range relative to some ordering (eg. $\leq$).

3. Use indirect equality to show that definition (25) is equivalent to the universal property (Galois connection)

$$X \subseteq slice(R, S) \Leftrightarrow X \subseteq R \;\wedge\; X \cdot R^\circ \subseteq S \tag{26}$$

4. Resort to (26) in showing that
   (a) $slice(R, \top) = R$ for all R.
   (b) $slice(R, id) = R$ if R is simple.

Proposed solution:

1. PF to PW transform of (25) is as follows:

$$b(slice(R, S))a \Leftrightarrow b\,R\,a \wedge b(S/R^\circ)a$$

$\Leftrightarrow$ { (11) }

$$b(slice(R, S))a \Leftrightarrow b\,R\,a \wedge \langle \forall\, b' \;:\; a\,R^\circ\,b' : b\,S\,b' \rangle$$

$\Leftrightarrow$ { converse }

$$b(slice(R, S))a \Leftrightarrow b\,R\,a \wedge \langle \forall\, b' \;:\; b'\,R\,a : b\,S\,b' \rangle$$

In Alloy, `b:a.r` (resp. `b':a.r`) encodes bRa (resp. $b'Ra$); moreover, $b'\ in\ s.b$ encodes $b'S\,b$.

2. Only $John$ concerns us, since for the other entries the relation is univocal. Let us calculate:

$$
\begin{array}{ll}
& b(slice(R, \leq))John \\
\Leftrightarrow & \quad \{ \ \} \\
& b \, R \, John \ \wedge \ \langle \forall \, b' \ : \ b' = 10 \vee b = 12 : \ b \leq b' \rangle \\
\Leftrightarrow & \quad \{ \ \} \\
& (b = 10 \vee b = 12) \ \wedge \ b \leq 10 \ \wedge \ b \leq 12 \\
\Leftrightarrow & \quad \{ \ \} \\
& b = 10
\end{array}
$$

So,

$$
slice(R, \leq) \ = \ \begin{array}{r|c} \mathbb{N} & A \\ \hline 10 & John \\ 11 & Mary \\ 15 & Arthur \end{array}
$$

3. We calculate:

$$
\begin{array}{ll}
& slice(R, S) \ = \ R \cap S / R^{\circ} \\
\Leftrightarrow & \quad \{ \text{ IE ([3]:15) } \} \\
& \langle \forall \, X \ :: \ X \subseteq slice(R, S) \Leftrightarrow X \subseteq R \cap S / R^{\circ} \rangle \\
\Leftrightarrow & \quad \{ \text{ (7) } \} \\
& \langle \forall \, X \ :: \ X \subseteq slice(R, S) \Leftrightarrow X \subseteq R \ \wedge \ X \subseteq S / R^{\circ} \rangle \\
\Leftrightarrow & \quad \{ \text{ (9) } \} \\
& \langle \forall \, X \ :: \ X \subseteq slice(R, S) \Leftrightarrow X \subseteq R \ \wedge \ X \cdot R^{\circ} \subseteq S \rangle
\end{array}
$$

4. Concerning (a):

$$
\begin{array}{ll}
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \ \wedge \ X \cdot R^{\circ} \subseteq \top \\
\Leftrightarrow & \quad \{ \text{ everything is below } \top \ \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \\
\Leftrightarrow & \quad \{ \text{ IE ([3]:15) } \} \\
& slice(R, \top) = R
\end{array}
$$

Concerning (b), fill in what's missing:

$$
\begin{array}{ll}
& X \subseteq slice(R, id) \Leftrightarrow X \subseteq R \ \wedge \ X \cdot R^{\circ} \subseteq id \\
\Leftrightarrow & \quad \{ \ R \cdot R^{\circ} \subseteq id \text{ since } R \text{ is simple } \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \ \wedge \ X \cdot R^{\circ} \subseteq id \ \wedge \ R \cdot R^{\circ} \subseteq id \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \ \wedge \ (X \cdot R^{\circ} \cup R \cdot R^{\circ}) \subseteq id \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \ \wedge \ (X \cup R) \cdot R^{\circ} \subseteq id
\end{array}
$$

$$
\begin{array}{ll}
\Leftrightarrow & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \wedge R \cdot R^{\circ} \subseteq id \\
\Leftrightarrow & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& X \subseteq slice(R, \top) \Leftrightarrow X \subseteq R \\
\Leftrightarrow & \{ \text{ IE ([3]:15), } R \text{ is simple assumed } \} \\
& slice(R, id) = R
\end{array}
$$

□

Exercise 17. Suppose you want to adapt $slice$ so as to work over lists of pairs:

```
slice      :: [(b,a)] -> ((b,b) -> Bool) -> [(b,a)]
```

Calculate the FT of `slice`.

Exercise 18. Consider the definition which follows,

$$f \mathrel{\dot{\leq}} g \triangleq f \subseteq (\leq) \cdot g \tag{27}$$

where $\leq$ is a partial order.

– Convert this definition to pointwise notation and check its meaning.
– Show that $f \mathrel{\dot{\leq}} g$ means the same as $f(\leq \longleftarrow id)g$

□

Exercise 19. Consider the following requirements for a $\mathbb{N}$ to $\mathbb{N}$ function:

> *Given a set $S \subseteq \mathbb{N}$, $\mathbb{N} \xrightarrow{reindex\ S} \mathbb{N}$ is the least function, in the sense of (27), which maps all numbers in S to an initial segment of $\mathbb{N}$.*

Consider the following specification of $reindex\ S$ (universal property): for all k, S

$$k \text{ monotone } \wedge\ k \cdot \Phi_S \text{ injective} \Leftrightarrow reindex\ S \mathrel{\dot{\leq}} k \tag{28}$$

1. Spell out "k monotone" and "$k \cdot \Phi_S$ injective" using relational algebra notation.
2. From (28) show that, for all S, function $reindex\ S$ is a subrelation of the $\leq$ ordering on $\mathbb{N}$, that is, for all $n \in \mathbb{N}$, $(reindex\ S)n \leq n$.
3. Using an informal drawing, sketch function $reindex\{2, 3, 6\}$.
4. Show that $reindex\ \emptyset = reindex\{i\} = \underline{1}$.

Nesting:

$$\langle \forall\, a, b \ :\ R \wedge S :\ T \rangle = \langle \forall\, a \ :\ R :\ \langle \forall\, b \ :\ S :\ T \rangle \rangle \tag{29}$$
$$\langle \exists\, a, b \ :\ R \wedge S :\ T \rangle = \langle \exists\, a \ :\ R :\ \langle \exists\, b \ :\ S :\ T \rangle \rangle \tag{30}$$

Trading:

$$\langle \forall\, i \,:\, R \wedge S :\, T \rangle = \langle \forall\, i \,:\, R :\, S \Rightarrow T \rangle \tag{31}$$

$$\langle \exists\, i \,:\, R \wedge S :\, T \rangle = \langle \exists\, i \,:\, R :\, S \wedge T \rangle \tag{32}$$

Splitting:

$$\langle \forall\, j \,:\, R :\, \langle \forall\, k \,:\, S :\, T \rangle\rangle = \langle \forall\, k \,:\, \langle \exists\, j \,:\, R :\, S \rangle :\, T \rangle \tag{33}$$

$$\langle \exists\, j \,:\, R :\, \langle \exists\, k \,:\, S :\, T \rangle\rangle = \langle \exists\, k \,:\, \langle \exists\, j \,:\, R :\, S \rangle :\, T \rangle \tag{34}$$

References

1. C.B. Jones. *Systematic Software Development Using VDM*. Series in Computer Science. Prentice-Hall Int., 1990. 1st edition (1986).
2. J.N. Oliveira. Functional dependency theory made 'simpler'. Technical Report DI-PURe-05.01.01, DI/CCTC, University of Minho, Gualtar Campus, Braga, 2005. PUReCafé, 2005.01.18 [talk]; available from `http://wiki.di.uminho.pt/twiki/bin/view/Research/PURe/PUReCafe`.
3. J.N. Oliveira. *Extended Static Checking by Calculation using the Pointfree Transform* . In A. Bove et al., editor, *LerNet ALFA Summer School 2008*, volume 5520 of *LNCS*, pages 195–251. Springer-Verlag, 2009.