MFES/1314 — CSI: Exercises of the slides

Exercise 1. *Let $l\ n$ denote the n-th element of a list l. Complete the following alternative formulation of clause (b) of inv-$ListOfCalls$:*

> Should $(l\ i)$ and $(l\ j)$ be the same, then .... for all ....

□

Exercise 2. *For $Date$ defined solely by (73,74) above, give definitions for the auxiliary functions y, m and d of*

> $tomorrow : Date \to Date$
> $tomorrow\ x \triangleq\ (y\ x, m\ x, d\ x)$

*which respectively give tomorrow's year, month and day. Then consider the effort required by repeating the exercise while ensuring **full** date **validity** within the Gregorian calender.*

□

Exercise 3. *(adapted from exercise 5.1.4 in C.B. Jones's* Systematic Software Development Using VDM*):*

> *Hotel room numbers are pairs (f, d) where f indicates a floor and d a door number in floor f. 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.*

***NB:** assume predicate $even$ on natural numbers.*

□

Exercise 4. *Write clause (b) of inv-$ListOfCalls$ (recall exercise 1) using $\forall$ notation.*

□

Exercise 5. *Check rule*

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

□

Exercise 6. *Infer tautologies*

$$S = \{a \mid a \in S\} \quad , \quad p\ a\ \equiv\ a \in \{a \mid p\ a\}$$

from (75).

□

Exercise 7. *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

$$\langle \forall\, c, a \;:\; r(c, a) :\; s(f\; c, a)\rangle$$

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

□

Exercise 8. *Calculate the weakest precondition $wp(f, inv\text{-}Y)$ for each situation below:*

X	Y	$f\ x$	$inv\text{-}Y\,y$
$\mathbb{N}_0$	$\mathbb{N}$	$f\ x \triangleq\ x^2 + 1$	$y \leq 10$
$\mathbb{N}_0$	$\mathbb{N}$	*the same*	$1 \leq y$
$\mathbb{N}_0$	$\mathbb{N}$	$f = succ$	$even\ y$
$\mathbb{N} \times \mathbb{N}^\star$	$\mathbb{N}^\star$	$f(n, x) \triangleq\ n : x$	$\langle \forall\, m \;:\; m \in\ elems\,y :\; m \leq 10\rangle$

□

Exercise 9. *Indicate which predicates p below are stronger (or weaker) than the weakest precondition (WP) on each f with respect to the corresponding output invariant:*

X	Y	f	$inv\text{-}Y(y)$	$p(x)$
$\mathbb{R}$	$\mathbb{R}$	$f\ x \triangleq\ x^2 + 1$	$0 \leq y \leq 10$	$0 < x < 3$
$\mathbb{N}^\star$	$\mathbb{N}^\star$	$f = map\ \underline{1}$	$\langle \forall\, i \;:\; i \in inds\,y :\; y\ i > 10\rangle$	$\textsc{True}$
$A^\star$	$A^\star$	$f = tail$	$length\ y > 0$	$x \neq [\,]$
$BTree\ A$	$BTree\ A$	$f = mirror$	$depth\ y \geq 1$	$depth\ x > 1$

where map and $tail$ are well known list operators and $mirror$ and $depth$ are the obvious functions over binary trees.

□

Exercise 10. *Complete the following (inductive) specification of $isOrdered$:*

$$isOrdered(\leq)[\,] = \textsc{True}$$
$$isOrdered(\leq)(a : x) = \ldots isOrdered(\leq)x \ldots$$

□

Exercise 11. *Give an implicit definition for function $f\ x \triangleq\ x^2 + 1$ over the natural numbers.*

□

Exercise 12. *A* golden multiple *of a given length is obtained by multiplying this length by a real number whose square equals its "successor". Write an implicit specification for* golden multiple.

□

Exercise 13. *Write implicit and explicit specifications for function* $inseq : \mathbb{N}_0 \to \mathbb{N}^\star$ *which, for argument* n*, yields the sequence* $[1, \ldots, n]$.
□

Exercise 14. *Assuming that the implicit definition of a total function* $B \xleftarrow{f} A$ *uniquely determines* f*, that is*

$$\textit{post-}f(r, a) \quad \equiv \quad r = f\ a \tag{3}$$

holds, use the Eindhoven quantifier calculus to show that (76) reduces to $\langle \forall\ a\ :\ a \in A :\ (f\ a) \in B \rangle$ *for* $Spec := f$*. In summary: in the case of functions,* satisfiability *is the same as* invariant preservation.
□

Exercise 15. *Consider datatype*

$$\begin{array}{l} NRSeq\ A = A^\star \\ \textbf{\textit{inv}}\ \ x \triangleq\ length\ x = card(elems\ x) \end{array}$$

1. *What is the informal meaning of the type's invariant?*
2. *Tell which of the following new types for* $Permutes$ *(7),*

$$Permutes : (s : NRSeq\ A) \leftarrow (r : A^\star) \tag{4}$$

$$Permutes : (s : NRSeq\ A) \leftarrow (r : NRSeq\ A) \tag{5}$$

   would lead to a non satisfiable specification.

□

Exercise 16. *Back to*

$$\begin{array}{l} Permutes : (s : A^\star) \leftarrow (r : A^\star) \\ \textbf{\textit{post}}\ \ \langle \forall\ a\ :\ a \in elems(s \frown r) :\ count\ a\ s = count\ a\ r \rangle \end{array}$$

show that

1. $Permutes$ *is a* ***reflexive*** *relation:* $x\ Permutes\ x \equiv \text{TRUE}$ *for all* x.
2. $Permutes$ *is a* **symmetric** *relation:* $y\ Permutes\ x \equiv x\ Permutes\ y$ *for all* x, y.

□

Exercise 17. *How would you write an explicit definition of (partial) function* $Maxs$*?*
□

Exercise 18. *We want to compare*

$$\begin{array}{l} IsPrefixOf : (s : A^\star) \to (r : A^\star) \\ \textbf{\textit{post}}\ \ length\ r \leq length\ s\ \wedge\ \langle \forall\ i\ :\ i \leq length\ r :\ r\ i = s\ i \rangle \end{array} \tag{6}$$

with

$$\begin{array}{l} Permutes : (s : A^\star) \to (r : A^\star) \\ \textbf{\textit{post}}\ \ \langle \forall\ e\ :\ e \in elems\ s \cup elems\ r :\ count\ e\ s = count\ e\ r \rangle \end{array} \tag{7}$$

and with partial function $Tail$*, all of type* $A^\star \longleftarrow A^\star$ *. Check which of the following hold:*

- $Tail \subseteq IsPrefixOf$
- $IsPrefixOf \subseteq Permutes$

□

Exercise 19. *Resort to (77), (78) and to the Eindhoven quantifier calculus to show that*

$$f \subseteq g \quad \equiv \quad f = g$$

holds (moral: for functions, inclusion and equality coincide).

□

Exercise 20. *Resort to PF-transform rule (79) and to the Eindhoven quantifier calculus to show that*

$$R \cdot id \;=\; R \;=\; id \cdot R \tag{8}$$

$$R \cdot \bot \;=\; \bot \;=\; \bot \cdot R \tag{9}$$

hold and that composition is associative:

$$R \cdot (S \cdot T) \quad = \quad (R \cdot S) \cdot T \tag{10}$$

□

Exercise 21. *Let K be a nonempty data domain, $k \in K$ and $\underline{k}$ be the* "everywhere k" *function:*

$$\begin{array}{rcl} \underline{k} & : & A \longrightarrow K \\ \underline{k}\, a & \triangleq & k \end{array} \tag{11}$$

Compute which relations are defined by the following PF-expressions:

$$ker\, \underline{k} \quad , \quad \underline{b} \cdot \underline{c}^{\circ} \quad , \quad img\, \underline{k} \tag{12}$$

□

Exercise 22. *Resort to (80,81) and (82) to prove the following rules of thumb:*

- *converse of* ***injective*** *is* ***simple*** *(and vice-versa)*
- *converse of* ***entire*** *is* ***surjective*** *(and vice-versa)*

□

Exercise 23. *Prove the following fact*

$$\text{A function } f \text{ is a bijection } \textbf{iff} \text{ its converse } f^{\circ} \text{ is a function} \tag{13}$$

by completing:

$$
\begin{array}{ll}
& f \text{ and } f^{\circ} \text{ are functions} \\
\equiv & \quad \{ \ldots \} \\
& (id \subseteq ker\ f \ \wedge\ img\ f \subseteq id) \ \wedge\ (id \subseteq ker\ (f^{\circ}) \ \wedge\ img\ (f^{\circ}) \subseteq id) \\
\equiv & \quad \{ \ldots \} \\
& \vdots \\
\equiv & \quad \{ \ldots \} \\
& f \text{ is a bijection}
\end{array}
$$

□

Exercise 24. *Check which of the following properties,*

simple , entire , injective , surjective , transitive , (co)reflexive , (anti)symmetric , connected

hold for relation $Eats$ (83), which is the food chain $Fox > Goose > Beans$.

□

Exercise 25. *Relation $cross$ (83) is defined by:*

$$
\begin{array}{rcl}
cross\ Left & = & Right \\
cross\ Right & = & Left
\end{array}
$$

It therefore is a bijection. Why?

□

Exercise 26. *Relation $where : Being \rightarrow Bank$ should obey the following constraints:*

- everyone is somewhere in a bank
- no one can be in both banks at the same time.

Encode such constraints in relational terms. Conclude that $where$ should be a function.

□

Exercise 27. *There are only two constant functions in the type $Being \longrightarrow Bank$. Identify them and explain the role they play in the puzzle.*

□

Exercise 28. *Infer $id \subseteq ker\ f$ (f is total) and $img\ f \subseteq id$ (f is simple) from any of shunting rules (99) or (100).*

□

Exercise 29. *Check the meaning of shunting rules (99) and (100) by converting them to pointwise (Eindhoven) notation.*

Show that they indeed hold by resorting to the rules of the Eindhoven calculus.
□

Exercise 30. *Let* $s\ S\ n$ *mean:* "student s is assigned number n". *Check the meaning of assertion:* $S \cdot \leq \subseteq \top \cdot S$.
□

Exercise 31. *As generalization of exercise 30, draw the most general type diagram which accommodates relational assertion:*

$$M \cdot R^{\circ} \quad \subseteq \quad \top \cdot M \tag{14}$$

□

Exercise 32. *Type the following relational assertions*

$$M \cdot N^{\circ} \quad \subseteq \quad \bot \tag{15}$$
$$M \cdot N^{\circ} \quad \subseteq \quad id \tag{16}$$
$$M^{\circ} \cdot \top \cdot N \quad \subseteq \quad > \tag{17}$$

and check their pointwise meaning.
□

Exercise 33. *Expand all criteria in the previous slides to pointwise notation.*
□

Exercise 34. *A relation* R *is said to be* co-transitive *iff the following holds:*

$$\langle \forall\, b, a \ :\ b\, R\, a :\ \langle \exists\, c \ :\ b\, R\, c :\ c\, R\, a \rangle \rangle \tag{18}$$

Compute the PF-transform of the formula above. Find a relation (eg. over numbers) which is co-transitive and another which is not.
□

Exercise 35. *Show that*

$$(b, c)\langle R, S\rangle a \quad \equiv \quad b\, R\, a \ \wedge\ c\, S\, a$$

PF-transforms to

$$\langle R, S\rangle \quad = \quad \pi_1^{\circ} \cdot R \cap \pi_2^{\circ} \cdot S \tag{19}$$

□

Exercise 36. *Infer universal property*

$$\pi_1 \cdot X \subseteq R \;\wedge\; \pi_2 \cdot X \subseteq S \quad \equiv \quad X \subseteq \langle R, S \rangle \tag{20}$$

from (19) via indirect equality (103).

□

Exercise 37. *Unconditional distribution laws*

$$\begin{array}{rcl} (P \cap Q) \cdot S & = & (P \cdot S) \cap (Q \cdot S) \\ R \cdot (P \cap Q) & = & (R \cdot P) \cap (R \cdot Q) \end{array}$$

will hold provide one of R or S is simple and the other injective. Tell which (justifying).

□

Exercise 38. *Derive from*

$$\langle R, S \rangle^\circ \cdot \langle X, Y \rangle \quad = \quad (R^\circ \cdot X) \cap (S^\circ \cdot Y) \tag{21}$$

the following properties:

$$ker\ \langle R, S \rangle \;=\; ker\ R \cap ker\ S \tag{22}$$

$\langle R, id \rangle$ *is always injective, for whatever* R

□

Exercise 39. *Show that:*

$$img\ [R\ , S] \quad = \quad img\ R \cup img\ S \tag{23}$$

$$img\ i_1 \cup img\ i_2 \quad = \quad id \tag{24}$$

□

Exercise 40. *Start by proving the fusion law*

$$\langle R, S \rangle \cdot f \;=\; \langle R \cdot f, S \cdot f \rangle \tag{25}$$

where f is a function. Then, relying on both (105) and (25) infer the ***exchange law****,*

$$[\langle R, S \rangle\ , \langle T, V \rangle] \quad = \quad \langle [R\ , T], [S\ , V] \rangle \tag{26}$$

holding for all relations as in diagram

$$\begin{tikzcd}
A \arrow[r, "i_1"] \arrow[d, "R"'] \arrow[drr, "S"' near end] & A + B & B \arrow[l, "i_2"'] \arrow[d, "V"] \arrow[dll, "T" near end] \\
C & C \times D \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & D
\end{tikzcd}$$

□

Exercise 41. *Prove the following rules of thumb:*

- *smaller than injective (simple) is injective (simple)*
- *larger than entire (surjective) is entire (surjective)*

□

Exercise 42. *Check which of the following hold:*

- *If relations R and S are simple, then so is $R \cap S$*
- *If relations R and S are injective, then so is $R \cup S$*
- *If relations R and S are entire, then so is $R \cap S$*

□

Exercise 43. *Prove that relational composition preserves* all *relational classes in the taxonomy of (84).*
□

Exercise 44. *Show that the following condional fusion law holds:*

$$\langle R, S \rangle \cdot T = \langle R \cdot T, S \cdot T \rangle \quad \Leftarrow \quad R \cdot (img\, T) \subseteq R \vee S \cdot (img\, T) \subseteq S$$

□

Exercise 45. *Recalling (13), prove that*

$$swap \triangleq \langle \pi_2, \pi_1 \rangle \tag{27}$$

is a bijection. (Assume property $(R \cap S)^\circ = R^\circ \cap S^\circ$.)
□

Exercise 46. *Let $\leq$ be a preorder and f be a function taking values on the carrier set of $\leq$.*

1. *Define the pointwise version of relation $\sqsubseteq \;\triangleq\; f^\circ \cdot \leq \cdot f$*
2. *Show that $\sqsubseteq$ is a preorder.*
3. *Show that $\sqsubseteq$ is not (in general) a total order even in the case $\leq$ is so.*

□

Exercise 47. *Let students in a course have two numeric marks,*

$$\mathbb{N} \xleftarrow{mark1} Student \xrightarrow{mark2} \mathbb{N}$$

and define the preorders:

$$\begin{array}{rcl} \leq_{mark1} & \triangleq & mark1^\circ \cdot \leq \cdot \, mark1 \\ \leq_{mark2} & \triangleq & mark2^\circ \cdot \leq \cdot \, mark2 \end{array}$$

Spell out in pointwise notation the meaning of lexicographic ordering

$$\leq_{mark1} ; \leq_{mark2}$$

□

Exercise 48. *From (**??**) infer:*

$$\perp \Rightarrow R \quad = \quad \top \tag{28}$$

$$R \Rightarrow \top \quad = \quad \top \tag{29}$$

□

Exercise 49. *Via indirect equality over (**??**) show that*

$$\top ; S \quad = \quad S \tag{30}$$

holds for any S and that, for R symmetric, we have:

$$R ; R \quad = \quad R \tag{31}$$

□

Exercise 50. *Add variables to both squares in (106) so that the same conditions are expressed pointwise. Then show that the conjunction of the two squares means the same as $R \subseteq \top \cdot M \cdot \pi_1 \ \wedge \ R \subseteq \top \cdot N \cdot \pi_2$ assertion*

$$R^\circ \quad \subseteq \quad \langle M^\circ \cdot \top, N^\circ \cdot \top \rangle \tag{32}$$

and draw this in a diagram.

□

Exercise 51. *Consider implementing M, R and N as files in a relational database. Before that, think of operations on the database such as, for example, that which records new loans (K):*

$$borrow(K, (M, R, N)) \quad \triangleq \quad (M, R \cup K, N) \tag{33}$$

It can be checked that the pre-condition

$$\textit{pre-borrow}(K, (M, R, N)) \quad \triangleq \quad R \cdot K^\circ \subseteq id$$

captures a necessary condition for maintaining (106) (why?) but it is not enough. Calculate for a rectangle in (106) at your choice the corresponding clause to add to pre-borrow.

□

Exercise 52. *Let $false$ be the "everywhere false" predicate such that $false\ x = \textsc{False}$ for all x, that is, $false = \underline{\textsc{False}}$. Show that $\Phi_{false} = \bot$.*
$\square$

Exercise 53. *Given a set S, let Φ_S abbreviate coreflexive $\Phi_{(\in S)}$. Use (85) to unfold $\Phi_{\{1,2\}} \cdot \Phi_{\{2,3\}}$ to pointwise notation.*
$\square$

Exercise 54. *Show that (86) follows from (85).*
$\square$

Exercise 55. *Solve (86) for p under substitution $\Phi := id$.*
$\square$

Exercise 56. *Combinator*

$$R \,\square\, S \quad \triangleq \quad R \cdot \top \cdot S \tag{34}$$

is known as the "rectangular" combinator. Recalling that $ker\,! = \top$, show that $! \,\square\, !^\circ \ = \ id$
$\square$

Exercise 57. *Check (87).*
$\square$

Exercise 58. *A relation R is said to satisfy* ***functional dependency*** *(FD) $g \to f$, written $\ g \xrightarrow{R} f\ $ wherever projection $\pi_{f,g} R$ (88) is simple.*

1. *Show that*

$$g \xrightarrow{R} f \quad \equiv \quad ker\,(g \cdot R^\circ) \subseteq ker\, f \tag{35}$$

2. *Show that (35) trivially holds wherever g is injective and R is simple, for all (suitably typed) f.*
3. *Prove the* ***composition rule*** *of FDs:*

$$h \xleftharpoondown{S \cdot R} g \quad \Leftarrow \quad h \xleftharpoondown{S} f \quad \wedge \quad f \xleftharpoondown{R} g \tag{36}$$

$\square$

Exercise 59. *Recalling (107), (108) and other properties of relation algebra, show that: (a) (109) and (110) can be re-written with R replacing $\top$; (b) $\Phi \subseteq \Psi \equiv ! \cdot \Phi \subseteq ! \cdot \Psi$ holds.*
$\square$

Exercise 60. *Recall diagram (106) of a library loan data model:*

$$\begin{tikzcd}
ISBN \arrow[d, "M"'] \arrow[dr, phantom, "\supseteq"] & ISBN \times UID \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[d, "R"] \arrow[dr, phantom, "\subseteq"] & UID \arrow[d, "N"] \\
Title \times Publisher \arrow[r, "\top"'] & Date & Name \times Address \times Phone \arrow[l, "\top"]
\end{tikzcd}$$

Show that the invariants captured by the two rectangles can be alternatively expressed by

$$\delta\,(\pi_{id,\pi_1} R) \subseteq \delta\, M \quad \wedge \quad \delta\,(\pi_{id,\pi_2} R) \subseteq \delta\, N$$

clearly exhibiting the ***foreign/primary****-key relationships of the data model ($ISBN$ and UID).*

□

Exercise 61. *Rely on the* ***absorption*** *property*

$$\langle R \cdot T, S \cdot U \rangle \quad = \quad (R \times S) \cdot \langle T, U \rangle \tag{37}$$

in showing that

$$\Psi \times \Upsilon \xleftarrow{\langle f,g \rangle} \Phi \qquad \equiv \qquad \Psi \xleftarrow{f} \Phi \;\;\wedge\;\; \Upsilon \xleftarrow{g} \Phi \tag{38}$$

holds.

□

Exercise 62. *From (89) and properties (99), etc infer the following* ***DbC*** *rules*

$$\Upsilon \xleftarrow{f} \Phi \cup \Psi \quad \equiv \quad \Upsilon \xleftarrow{f} \Phi \;\;\wedge\;\; \Upsilon \xleftarrow{f} \Psi \tag{39}$$

$$\Phi \cdot \Psi \xleftarrow{f} \Upsilon \quad \equiv \quad \Phi \xleftarrow{f} \Upsilon \;\;\wedge\;\; \Psi \xleftarrow{f} \Upsilon \tag{40}$$

*You will also need $(R\cdot)$-distribution (**??**).*

□

Exercise 63. *Show that (91) means the same as*

$$Pre \cdot \Phi_A \subseteq Post^{\circ} \cdot \Phi_B \cdot Post \tag{41}$$

□

Exercise 64. *Consider the relational version of McCarthy's conditional combinator which follows:*

$$p \rightarrow f, g \;=\; f \cdot \Phi_p \cup g \cdot \Phi_{\neg p} \tag{42}$$

*(a) Using (92) infer the following **DbC** rule for* conditionals*:*

$$\Upsilon \xleftarrow{p\rightarrow f,g} \Psi \quad \equiv \quad \Upsilon \xleftarrow{f} \Psi \cdot \Phi_p \;\wedge\; \Upsilon \xleftarrow{g} \Psi \cdot \Phi_{\neg p} \tag{43}$$

(b) Now try and define a rule for handling contracts involving conditional conditions:

$$\Upsilon \xleftarrow{p\rightarrow f,g} (p \rightarrow \Psi, \Phi) \;= .... \tag{44}$$

□

Exercise 65. *Recall that our motivating ESC assertion (94) was stated but not proved. Now that we know that (94) PF-transforms to* $\Phi_{even} \xleftarrow{twice} \Phi_{even}$ *and that* $\Phi_{even} = \rho\, twice$*, complete the following* "almost no work at all" *PF-calculation of (94):*

$$\begin{array}{cl} & \Phi_{even} \xleftarrow{twice} \Phi_{even} \\ \equiv & \quad \{ .... \} \\ & twice \cdot \Phi_{even} \subseteq \Phi_{even} \cdot twice \\ \equiv & \quad \{ .... \} \\ & twice \cdot \Phi_{even} \subseteq \rho\, twice \cdot twice \end{array} \qquad \begin{array}{cl} \equiv & \quad \{ .... \} \\ & twice \cdot \Phi_{even} \subseteq twice \\ \Leftarrow & \quad \{ .... \} \\ & \Phi_{even} \subseteq id \\ \equiv & \quad \{ .... \} \\ & \textsc{True} \end{array}$$

□

Exercise 66. *Prove the **union simplicity** rule:*

$$M \cup N \textit{ is simple} \quad \equiv \quad M, N \textit{ are simple and } M \cdot N^{\circ} \subseteq id \tag{45}$$

□

Exercise 67. *Tell which of the rules (95), (96), (97) could have been written with right-hand side* $\top \subseteq \top \cdot [\![R]\!] \cdot \top$.
□

Exercise 68. *The assertion in the following fragment of Alloy,*

```
sig A { f : one B }
sig B {}

assert GC {
    all x: set A, y: set B | x.f in y <=> x in f.y
}
```

captures a "shunting rule" valid in such a language. Resort to the semantic rules given above to prove the validity of this assertion.
□

Exercise 69. *Check that* $\underline{n} \cdot \langle \underline{a}, \underline{p} \rangle^{\circ} = \{(n, (a, p))\}$.
□

Exercise 70. *The pre-condition of method* `rever` *includes yet another condition. Guess where this arises from.*
□

Exercise 71. *Define a method which accepts papers, $Ac' = Ac \cup New$, and calculate the corresponding contract entiled by the invariants of the model.*
□

Exercise 72. *Derive the Alloy code for the contract of the previous exercise for $New = \underline{a} \cdot \underline{a}^\circ$, that is, for the method which accepts one paper a at a time.*
□

Exercise 73. *The original Alloy model enforces Nt simple, cf.* `nota :  Artigo -> Pessoa -> lone Nota`*; that is, no reviewer can assign more than one mark to a given paper. Simplicity of Nt is therefore another invariant "hidden in the notation". Resort to the the union-simplicity rule (45) to calculate the contract to impose on method $Nt' = Nt \cup New$ with respect to this requirement.*
□

Exercise 74. *Recall the diagram of the* starving *invariant of problem* PROPOSITIO DE HOMINE ET CAPRA ET LVPO*:*

$$\begin{tikzcd}
Being \arrow[d, "where"'] \arrow[dr, phantom, "\subseteq"] & Being \arrow[l, "CanEat"'] \arrow[d, "\underline{Farmer}"] \\
Bank & Being \arrow[l, "where"]
\end{tikzcd}$$

Write the same in Alloy syntax.
□

Exercise 75. *Consider the following examples of file system operations:*

- ***edit*** *an existing file without changing its attributes*
- ***open*** *a file for editing*
- ***create*** *a file in the current directory*
- ***rename*** *an existing file system object (file or directory)*

Tell which operations call for contracts with respect to the two invariants ri and pc.
□

Exercise 76. *Prove (98). Can this equivalence be generalized?*
□

Exercise 77. *Encode the calculated contract (weakest pre-condition) in Alloy.*
□

Exercise 78. *Recalling exercise 75, calculate the contract required by the operation*

$$open\ K\ (M, N) \triangleq\ (M \cup K, N)$$

□

Exercise 79. *Specify the POSIX* `mkdir` *operation and calculate its contract.*
□

Exercise 80. *Check properties (111) and (113) for the list relator defined above.*
□

Exercise 81. *Let C be a nonempty data domain and let and $c \in C$. Let $\underline{c}$ be the* "everywhere c" *function:*

$$\begin{array}{rcl} \underline{c} & : & A \longrightarrow C \\ \underline{c}\, a & \triangleq & c \end{array} \tag{46}$$

Show that the free theorem of $\underline{c}$ reduces to

$$\langle \forall\ R\ ::\ R \subseteq \top \rangle \tag{47}$$

□

Exercise 82. *Calculate the free theorem associated with the projections $A \xleftarrow{\pi_1} A \times B \xrightarrow{\pi_2} B$ and instantiate it to (a) functions; (b) coreflexives. Introduce variables and derive the corresponding pointwise expressions.*
□

Exercise 83. *Consider higher order function* `const: a -> b -> a` *such that, given any x of type a, produces the constant function $const\ x$. Show that the equalities*

$$const(f\ x) = f \cdot (const\ x) \tag{48}$$
$$(const\ x) \cdot f = const\ x \tag{49}$$
$$(const\ x)^\circ \cdot (const\ x) = \top \tag{50}$$

arise as corollaries of the free theorem *of $const$.*
□

Exercise 84. *The following is a well-known Haskell function*

```
filter ::  forall a.  (a -> Bool) -> [a] -> [a]
```

Calculate the free theorem associated with its type

$$filter : a^\star \leftarrow a^\star \leftarrow (Bool \leftarrow a)$$

and instantiate it to the case where all relations are functions.
□

Exercise 85. *In many sorting problems, data are sorted according to a given* ranking *function which computes each datum's numeric rank (eg. students marks, credits, etc). In this context one may parameterize sorting with an extra parameter f ranking data into a fixed numeric datatype, eg. the integers: $serial : (a \to \mathbb{N}) \to a^\star \to a^\star$.*

Calculate the FT of $serial$.
□

Exercise 86. *Consider the following function from Haskell's Prelude:*

```
findIndices ::  (a -> Bool) -> [a] -> [Int]
findIndices p xs = [ i | (x,i) <- zip xs [0..], p x ]
```

which yields the indices of elements in a sequence xs which satisfy p. For instance, $findIndices\ (< 0)\ [1, -2, 3, 0, -5] = [1, 4]$. Calculate the FT of this function.
□

Exercise 87. *Choose arbitrary functions from Haskell's Prelude and calculate their FT.*
□

Exercise 88. *Wherever two equally typed functions f, g such that $f\ a \leq g\ a$, for all a, we say that f is* pointwise at most *g and write $f \stackrel{.}{\leq} g$. In symbols:*

$$f \stackrel{.}{\leq} g \quad \triangleq \quad f \subseteq (\leq) \cdot g \qquad \textit{cf. diagram} \quad \begin{tikzcd} & A \arrow[dl, "f"'] \arrow[dr, "g"] \arrow[d, phantom, "\subseteq"] & \\ B & & B \arrow[ll, "\leq"] \end{tikzcd} \tag{51}$$

Show that implication

$$f \stackrel{.}{\leq} g \quad \Rightarrow \quad (map\ f) \stackrel{.}{\leq}^\star (map\ g) \tag{52}$$

follows from the FT *of the function $map : (a \to b) \to a^\star \to b^\star$.*
□

Exercise 89. *Infer the FT of the following function, written in Haskell syntax,*

```
while ::  (a -> Bool) -> (a -> a) -> (a -> b) -> a -> b
while p f g x = if not(p x) then g x else while p f g (f x)
```

which implements a generic `while`*-loop. Derive its corollary for functions and compare your result with that produced by the tool above.*
$\square$

Exercise 90. *Let* $iprod = (\![\underline{1}\,, (\times)]\!)$ *be the function which multiplies all natural numbers in a given list;* $even$ *be the predicate which tests natural numbers for evenness; and* $exists = (\![\underline{\text{FALSE}}\,, (\vee)]\!)$.
From (114) infer

$$even \cdot iprod \quad = \quad exists \cdot even^{\star}$$

meaning that product $n_1 \times n_2 \times \ldots \times n_m$ *is even iff some* n_i *is so.*
$\square$

Exercise 91. *Show that the* identity *relator* Id*, which is such that* $\mathsf{Id}\,R \;=\; R$ *and the* constant *relator* K *(for a given data type* K*) which is such that* $\mathsf{K}\,R \;=\; id_K$ *are indeed relators.*
$\square$

Exercise 92. *Show that product*

$$\begin{array}{ccccc} A & & C & \cdots\cdots & \mathsf{G}(A,C) = A \times C \\ {\scriptstyle R}\downarrow & & {\scriptstyle S}\downarrow & & \downarrow{\scriptstyle \mathsf{G}(R,S)=R\times S} \\ B & & D & \cdots\cdots & \mathsf{G}(B,D) = B \times D \end{array}$$

is a (binary) relator.
$\square$

Exercise 93. *The type of functional composition* $(\cdot)$ *is*

```
(.)  ::  (b -> c) -> (a -> b) -> a -> c
```

Show that ***contract composition*** *(115) is a corollary of the free theorem (FT) of this type.*
$\square$

Exercise 94. *Show that contract* $\Psi^{\star} \xleftarrow{map\ f} \Phi^{\star}$ *holds provided contract* $\Psi \xleftarrow{f} \Phi$ *holds.*
$\square$

Exercise 95. *Suppose a functional programmer wishes to prove the following property of lists:*

$$\left\langle \begin{array}{c} \forall\, a, s \\ (\phi\, a) \;\wedge\; \langle \forall\, a' \;:\; a' \in elems\, s :\; \phi\, a' \rangle : \\ \langle \forall\, a'' \;:\; a'' \in elems(a:s) :\; \phi\, a'' \rangle \end{array} \right\rangle$$

Show that this property is a contract arising (for free) from the polymorphic type of operation $(\_ : \_)$ on lists.
□

Exercise 96. *Derive from (116) the two* cancellation *laws*

$$\begin{array}{rcl} q & \leq & (q \times d) \div d \\ (n \div d) \times d & \leq & n \end{array}$$

and reflexion *law:*

$$n \div d \geq 1 \quad \equiv \quad d \leq n \tag{53}$$

□

Exercise 97. *Resort to indirect equality to prove any of (117) or (118).*
□

Exercise 98. *Derive from (119) that both f and g are monotonic.*
□

Exercise 99. *Why is it that converse-monotonicity can be strengthened to an equivalence?*
□

Exercise 100. *Prove the equalities*

$$X \cdot f \quad = \quad X/f^{\circ} \tag{54}$$

$$X/\bot \quad = \quad \top \tag{55}$$

$$\top/Y \quad = \quad \top \tag{56}$$

and check their pointwise meaning.
□

Exercise 101. *Define*

$$X \setminus Y \quad = \quad (Y^{\circ}/X^{\circ})^{\circ} \tag{57}$$

and infer:

$$a(R \setminus S)c \quad \equiv \quad \langle \forall\, b \;:\; b\, R\, a :\; b\, S\, c \rangle \tag{58}$$

$$R \cdot X \subseteq Y \quad \equiv \quad X \subseteq R \setminus Y \tag{59}$$

□

Exercise 102. *Show that* $R \cap (R \Rightarrow Y) \subseteq Y$ *("modus ponens") holds and that* $R - R = \bot - R = \bot$.
□

Exercise 103. *Let* $\mathbb{P}A = \{S \mid S \subseteq A\}$ *and let* $A \xleftarrow{\in} \mathbb{P}A$ *denote the membership relation* $a \in S$*, for any* a *and* S*. What does the relation* $\in \setminus \in$ *mean?*
□

Exercise 104. *Show that the relation* $\in \setminus \in$ *of the previous exercise is reflexive and transitive.*
□

Exercise 105. *Prove that equality*

$$(R \setminus S) \cdot f \quad = \quad R \setminus (S \cdot f) \tag{60}$$

holds.
□

Exercise 106. *(a) Show that* $R \subseteq \bot / S^\circ \equiv \delta\, R \cap \delta\, S = \bot$*; (b) Then use indirect equality to infer the universal property of term* $R \cap \bot / S^\circ$ *— the largest sub-relation of* R *whose domain is disjoint of that of* S.
□

Exercise 107. *The relational* overriding *combinator,*

$$R \dagger S \;=\; S \cup R \cap \bot / S^\circ \tag{61}$$

means the relation which contains the whole of S *and that part of* R *where* S *is undefined — read* $R \dagger S$ *as "*R *overridden by* S*". (a) Show that* $\bot \dagger S = S$ *and that* $R \dagger \bot = R$*; (b) Infer the universal property:*

$$X \subseteq R \dagger S \quad \equiv \quad X - S \subseteq R \;\wedge\; \delta\,(X - S) \cdot \delta\, S = \bot \tag{62}$$

□

Exercise 108. *Prove*

$$id \xleftarrow{R} \Phi \qquad \equiv \qquad \textsc{True} \qquad \equiv \;\; \Phi \xleftarrow{R} \bot \tag{63}$$

□

Exercise 109. *Prove the special cases:*

- *WP of a function f:*

$$f \mathbin{\backslash\!\!\bullet} \Phi_q \quad = \quad \lambda a.q(f\ a) \tag{64}$$

-

$$\rho\,(f \cdot \Phi_p) \quad = \quad \lambda b.b \in \{f\ a \mid p\ a\} \tag{65}$$

NB: *recall that (64) has been used several times earlier on in contract calculation.*

$\square$

Exercise 110. *The formal meaning of (imperative) code sequential composition is*

$$[\![\mathtt{P;Q}]\!] \quad = \quad [\![\mathtt{Q}]\!] \cdot [\![\mathtt{P}]\!]$$

Show that the following rule of the Hoare logic of programs,

$$\frac{\{p\}P\{q\}\ ,\ \{q\}Q\{s\}}{\{p\}P;Q\{s\}}$$

is an instance of the following relational typing rule:

$$\Psi \xleftarrow{R \cdot S} \Phi \quad \Leftarrow \quad \Psi \xleftarrow{R} \Upsilon \ \wedge\ \Upsilon \xleftarrow{S} \Phi \tag{66}$$

$\square$

Exercise 111. *Prove the "trading rule":*

$$\Upsilon \xleftarrow{R} \Phi \cdot \Psi \quad \equiv \quad \Upsilon \xleftarrow{R \cdot \Phi} \Psi \tag{67}$$

$\square$

Exercise 112. *Re-write the following "contract splitting" rule,*

$$\Psi_1 \cdot \Psi_2 \xleftarrow{R} \Phi \quad \equiv \quad \Psi_1 \xleftarrow{R} \Phi \ \wedge\ \Psi_2 \xleftarrow{R} \Phi \tag{68}$$

in Hoare logic. Then prove (68).

$\square$

Exercise 113. *Show that* $\rho\,R \xleftarrow{R} \delta\,R$ *holds. However, WP* $R \mathbin{\backslash\!\!\bullet} (\rho\,R) = id$ *rather than* $\delta\,R$*. Explain why.*

$\square$

Exercise 114. *Show that* $\rho\,R \xleftarrow{R} \delta\,R$ *holds. However, WP* $R \mathbin{\backslash\!\!\bullet} (\rho\,R) = id$ *rather than* $\delta\,R$*. Explain why.*

$\square$

Exercise 115. *The two "shunting" rules for S a simple relation,*

$$S \cdot R \subseteq Q \quad \equiv \quad (\delta\, S) \cdot R \quad \subseteq \quad S^\circ \cdot Q \tag{69}$$
$$R \cdot S^\circ \subseteq Q \quad \equiv \quad R \cdot \delta\, S \quad \subseteq \quad Q \cdot S \tag{70}$$

are "almost" Galois connections. (a) Derive the following variants concerning coreflexives,

$$R \cdot \Phi \subseteq S \quad \equiv \quad R \cdot \Phi \subseteq S \cdot \Phi$$
$$\Phi \cdot R \subseteq S \quad \equiv \quad \Phi \cdot R \subseteq \Phi \cdot S$$

referred to earlier on as the closure properties *(120) and (121), respectively; (b) prove either (69) or (70) by cyclic implication (vulg. "ping-pong").*

□

Exercise 116. *Before implementing $take$ one can start proving properties about this function solely relying on (122):*

- *Show that*

  $$take\ (length\, xs)\ xs = xs$$

  holds.

- *Resort to indirect equality over $\preceq$ in proving*

  $$take\ n\ (take\ m\ xs) \quad = \quad take\ (\min nm)\ xs$$

  where min, the minimum of two natural numbers, is given by the obvious Galois connection.

□

Exercise 117. *Prove the two first equalities above.*

□

Exercise 118. *Show that, for S a preorder, S_f above is also a preorder.*

□

Exercise 119. *Show that f monotonicity, $x \sqsubseteq y \;\Rightarrow\; f\ x \leq f\ y$, can be written point-free as*

$$(\sqsubseteq) \cdot f^\circ \subseteq f^\circ \cdot (\leq), \tag{71}$$

□

Exercise 120. *Show that, once (71) is assumed, the following equivalence holds:*

$$g \;\subseteq\; f^\circ \cdot (\leq) \quad \equiv \quad (\sqsubseteq) \cdot g \;\subseteq\; f^\circ \cdot (\leq) \tag{72}$$

Suggestion: do a "ping-pong" proof.

□

Formulas referred to in the exercises

$$Date = Year \times Month \times Day \tag{73}$$

where

$$\begin{array}{l} Year = \mathbb{N} \\ \\ Month = \mathbb{N} \\ \textbf{inv}\ m \triangleq\ m \leq 12 \\ \\ Day = \mathbb{N} \\ \textbf{inv}\ d \triangleq\ d \leq 31 \end{array} \tag{74}$$

$$p = (\in S)\ \equiv\ S = \{a \mid p\ a\} \tag{75}$$

$$\langle \forall\ a\ :\ a \in A :\ \text{pre-}Spec\ a \Rightarrow \langle \exists\ b\ :\ b \in B :\ \text{post-}Spec(b, a)\rangle\rangle \tag{76}$$

$$f = g \quad \equiv \quad \langle \forall\ a\ :\ a \in A :\ f\ a\ =_B\ g\ a\rangle \tag{77}$$

$$R \subseteq S \quad \equiv \quad \langle \forall\ b, a\ :\ b\ R\ a :\ b\ S\ a\rangle \tag{78}$$

$$b(R \cdot S)c \quad \equiv \quad \langle \exists\ a\ ::\ b\ R\ a\ \ \wedge\ \ a\ S\ c\rangle \tag{79}$$

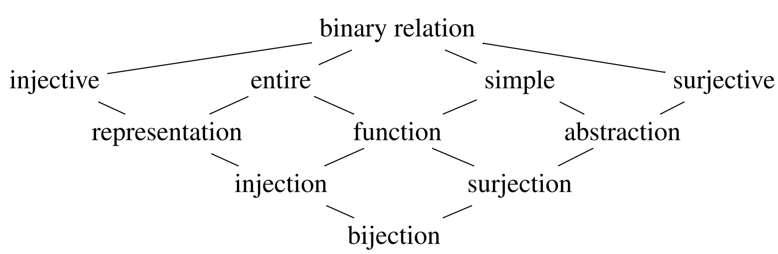
$$ker\,(R^\circ) \quad = \quad img\,R \tag{80}$$

$$img\,(R^\circ) \quad = \quad ker\,R \tag{81}$$

	Reflexive	*Coreflexive*
$ker\ R$	entire R	injective R
$img\ R$	surjective R	simple R

(82)

$$\begin{tikzcd} Being \arrow[r, "Eats"] & Being \arrow[d, "where"'] & \\ & Bank \arrow[r, "cross"] & Bank \end{tikzcd} \tag{83}$$



(84)

$$y\ \Phi_p\ x\ \equiv\ y = x\ \wedge\ p\ y \tag{85}$$

$$\Phi = \Phi_p\ \equiv\ (y\ \Phi\ x \equiv y = x\ \wedge\ p\ y) \tag{86}$$

$$\pi_{g,f} R \quad = \quad \{(g\ b, f\ a) \mid b\ R\ a\} \tag{87}$$

$$\pi_{g,f} R \stackrel{\mathrm{def}}{=} g \cdot R \cdot f^{\circ} \qquad \begin{tikzcd} B \arrow[d, "g"'] & A \arrow[l, "R"'] \arrow[d, "f"] \\ C & D \arrow[l, "\pi_{g,f} R"] \end{tikzcd} \tag{88}$$

$$\begin{tikzcd} \Phi_B & \Phi_A \arrow[l, "f"'] \end{tikzcd} \tag{89}$$

to mean

$$f \cdot \Phi_A \;\subseteq\; \Phi_B \cdot f \quad \text{cf. diagram} \qquad \begin{tikzcd} A \arrow[d, "f"'] & A \arrow[l, "\Phi_A"'] \arrow[d, "f"] \\ B & B \arrow[l, "\Phi_B"] \end{tikzcd} \tag{90}$$

$$\begin{tikzcd} A \arrow[d, "Pre"'] & & A \arrow[ll, "\Phi_A"'] \arrow[d, "Post"] \\ A & B \arrow[l, "\top"] & B \arrow[l, "\Phi_B"] \end{tikzcd} \qquad Pre \cdot \Phi_A \subseteq \top \cdot \Phi_B \cdot Post \tag{91}$$

$$f \cdot \Phi_A \quad \subseteq \quad \Phi_B \cdot \top \tag{92}$$

$$\rho\,(f \cdot \Phi_A) \quad \subseteq \quad \Phi_B \tag{93}$$

$$\langle \forall\, x, y \;:\; y = 2x \;\wedge\; even\; x :\; even\; y \rangle \tag{94}$$

$$[\![\mathtt{no\ R}]\!] \quad = \quad [\![\mathtt{R}]\!] \subseteq \bot \tag{95}$$

$$[\![\mathtt{some\ R}]\!] \quad = \quad [\![\mathtt{R}]\!] \supset \bot \tag{96}$$

$$[\![\mathtt{lone\ R}]\!] \quad = \quad \langle \exists\, a, b \;::\; [\![\mathtt{R}]\!] \subseteq \underline{b} \cdot \underline{a}^{\circ} \rangle \tag{97}$$

$$f \cdot R \subseteq \top \cdot S \;\equiv\; R \subseteq \top \cdot S \tag{98}$$

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^{\circ} \cdot S \tag{99}$$

$$R \cdot f^{\circ} \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{100}$$

$$R = S \quad \equiv \quad \langle \forall\, X \;::\; (X \subseteq R \equiv X \subseteq S) \rangle \tag{101}$$

$$\equiv \quad \langle \forall\, X \;::\; (R \subseteq X \equiv S \subseteq X) \rangle \tag{102}$$

$$R = S \quad \equiv \quad \langle \forall\, X \;::\; (X \subseteq R \equiv X \subseteq S) \rangle \tag{103}$$

$$\equiv \quad \langle \forall\, X \;::\; (R \subseteq X \equiv S \subseteq X) \rangle \tag{104}$$

$$[R\,, S] = X \quad \equiv \quad R = X \cdot i_1 \;\;\wedge\;\; S = X \cdot i_2 \tag{105}$$

$$\begin{tikzcd} ISBN \arrow[d, "M"'] \arrow[dr, phantom, "\supseteq"] & ISBN \times UID \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[d, "R"'] \arrow[dr, phantom, "\subseteq"] & UID \arrow[d, "N"] \\ \begin{matrix} Title\, \times \\ Publisher \end{matrix} \arrow[r, "\top"'] & Date & \begin{matrix} Name \times \\ Address \times \\ Phone \end{matrix} \arrow[l, "\top"] \end{tikzcd} \tag{106}$$

$$R \cdot \Phi = R \cap \top \cdot \Phi \tag{107}$$
$$\Psi \cdot R = R \cap \Psi \cdot \top \tag{108}$$

$$\delta\, R \subseteq \Phi \equiv R \subseteq \top \cdot \Phi \tag{109}$$
$$\rho\, R \subseteq \Phi \equiv R \subseteq \Phi \cdot \top \tag{110}$$

$$\mathsf{G}\, id = id \tag{111}$$
$$\mathsf{G}\,(R \cdot S) = (\mathsf{G}\, R) \cdot (\mathsf{G}\, S) \tag{112}$$
$$\mathsf{G}\,(R^\circ) = (\mathsf{G}\, R)^\circ \tag{113}$$

$$f \cdot \mathsf{B}\,(R, S) \subseteq S \cdot g \quad \Rightarrow \quad (\!|f|\!) \cdot \mathsf{F}\, R \subseteq S \cdot (\!|g|\!) \tag{114}$$

$$\Psi \xleftarrow{f \cdot g} \Phi \quad \Leftarrow \quad \Psi \xleftarrow{f} \Upsilon \;\wedge\; \Upsilon \xleftarrow{g} \Phi \tag{115}$$

$$z \times y \leq x \;\Leftrightarrow\; z \leq x \div y \qquad (y > 0) \tag{116}$$

$$f(b \sqcup b') = (f\ b) \vee (f\ b') \tag{117}$$
$$g(a \wedge a') = (g\ a) \sqcap (g\ a') \tag{118}$$

$$\underbrace{f}_{\text{lower adjoint}}\ b \leq a \equiv b \sqsubseteq \underbrace{g}_{\text{upper adjoint}}\ a \tag{119}$$

$$R \cdot \Phi \subseteq S \equiv R \cdot \Phi \subseteq S \cdot \Phi \tag{120}$$
$$\Phi \cdot R \subseteq S \equiv \Phi \cdot R \subseteq \Phi \cdot S \tag{121}$$

$$length\, ys \leq n \;\wedge\; ys \preceq xs \quad \equiv \quad ys \preceq take\ n\ xs \tag{122}$$