Métodos Formais em Engenharia de Software

1.º Ano de Mestrado (Eng. Informática / Matemática e Computação)
Universidade do Minho
Ano Lectivo de 2013/14

Teste de frequência (módulo CSI) — 26 de Fevereiro de 2014
10h00
Sala DI 1.07

NB: *Esta prova consta de **8** alíneas todas com as mesma cotação. Os alunos que desejem responder directamente sobre o enunciado da **Questão 6** devem ter o cuidado de rubricar as respectiva folha e indicarem o seu **número**.*

PROVA COM CONSULTA (2 horas)

Questão 1 (1 alínea) Seja $\mathbb{R} \xleftarrow{R} \mathbb{R}$ a relação binária sobre os números reais definida da forma seguinte:

$$y\ R\ x \quad \stackrel{\text{def}}{=} \quad y^2 + x^2 = 1 \tag{F1}$$

Recorra a cálculos com variáveis para mostrar que

- R é simétrica mas não é nem inteira nem simples (logo nem injectiva e nem sobrejectiva). **Sugestão:** dê contra-exemplos e/ou apoie a sua resolução desenhando R no plano Cartesiano.
- $R \cdot R \subseteq \mathsf{ker}\ sq$ se verifica, onde $\mathbb{R} \xleftarrow{sq} \mathbb{R}$ é a função $sq\ x = x^2$.

RESOLUÇÃO: Primeira parte:

- R é simétrica, pois

$$\begin{array}{ll} & R = R^\circ \\ \equiv & \quad \{ \text{ (F1) ; definição de converso } \} \\ & y^2 + x^2 = 1 \equiv x^2 + y^2 = 1 \\ \equiv & \quad \{ \text{ soma é comutativa } \} \\ & true \\ \Box & \end{array}$$

- R não é inteira: como se pode ver re-escrevendo $y\ R\ x \equiv y = \pm\sqrt{1-x^2}$ tem-se que $y\ R\ x$ só está definida em $\mathbb{R}$ para $x \leqslant 1$ — logo R não é inteira.
- R não é simples: para $x \leqslant 1$ tem-se $y\ R\ x \equiv y = +\sqrt{1-x^2} \vee y = -\sqrt{1-x^2}$, logo não é simples.
- R não é injectiva nem sobrejectiva: sendo R simétrica, $\mathsf{ker}\ R^\circ = \mathsf{ker}\ R$ e $\mathsf{img}\ R^\circ = \mathsf{img}\ R$ logo não ser simples é o mesmo que não ser injectiva e não ser sobrejectiva é o mesmo que não ser inteira.

Segunda alínea: tem-se

$$y\ R\ x \equiv y^2 = 1 - x^2$$

Logo, pela regra do guardanapo:[1]

$$R = sq^\circ \cdot (1-) \cdot sq \tag{F2}$$

Então (pointfree):

$$\begin{array}{ll}
 & R \cdot R \ \subseteq\ \mathsf{ker}\ sq \\
\equiv & \quad \{\ R \text{ é simétrica, } R = R^\circ\ \} \\
 & R^\circ \cdot R \ \subseteq\ \mathsf{ker}\ sq \\
\equiv & \quad \{\ \text{(F2)}\ \} \\
 & sq^\circ \cdot (1-)^\circ \cdot sq \cdot sq^\circ \cdot (1-) \cdot sq \ \subseteq\ sq^\circ \cdot sq \\
\Leftarrow & \quad \{\ \text{monotonia da composição}\ \} \\
 & (1-)^\circ \cdot \mathsf{img}\ sq \cdot (1-) \ \subseteq\ id \\
\Leftarrow & \quad \{\ sq \text{ é simples}\ \} \\
 & (1-)^\circ \cdot (1-) \ \subseteq\ id \\
\equiv & \quad \{\ y = 1 - x \text{ é injectiva}\ \} \\
 & true \\
\Box &
\end{array}$$

Pointwise:

$$\begin{array}{ll}
 & R \ \subseteq\ \mathsf{ker}\ sq\ /\ R \\
\equiv & \quad \{\ \text{definições (divisão e núcleo)}\ \} \\
 & y\ R\ x \Rightarrow \langle \forall\ z\ :\ x\ R\ z :\ y\ (sq^\circ \cdot sq)\ z \rangle \\
\equiv & \quad \{\ \text{definições } \textit{pointwise} \text{ de } R \text{ e } \mathsf{ker}\ sq\ \} \\
 & x^2 = 1 - y^2 \Rightarrow \langle \forall\ z\ :\ x^2 + z^2 = 1 :\ y^2 = z^2 \rangle \\
\equiv & \quad \{\ \text{substituindo } x^2 = 1 - y^2\ \} \\
 & \langle \forall\ z\ :\ 1 - y^2 + z^2 = 1 :\ y^2 = z^2 \rangle) \\
\equiv & \quad \{\ \text{trivia}\ \} \\
 & \langle \forall\ z\ ::\ (y^2 = z^2) \Rightarrow (y^2 = z^2) \rangle \\
\equiv & \quad \{\ P \Rightarrow P \equiv true\ \} \\
 & true \\
\Box &
\end{array}$$

$\Box$

Questão 2 (1 alínea) Partindo das respectivas conecções de Galois, recorra à igualdade indirecta para provar a seguinte propriedade associativa (generalizada) das duas divisões relacionais

$$R \setminus (S/Q) \quad = \quad (R \setminus S)/Q \tag{F3}$$

A que regra do cálculo de quantificadores de Eindhoven corresponde esta propriedade? Justifique a sua resposta por introdução de variáveis.

[1] Por aqui se vê também que R é simétrica: $R^\circ = sq^\circ \cdot (1-)^\circ \cdot sq = R$ pois $(1-)^\circ = (1-)$, cf. $1 - y = x \equiv y = 1 - x$.

RESOLUÇÃO:

$$
\begin{array}{ll}
 & X \subseteq R \setminus (S/Q) \\
\equiv & \quad \{ \text{ GCs das duas divisões } \} \\
 & (R \cdot X) \cdot Q \subseteq S \\
\equiv & \quad \{ \text{ associatividade } \} \\
 & R \cdot (X \cdot Q) \subseteq S \\
\equiv & \quad \{ \text{ GCs das duas divisões } \} \\
 & X \subseteq (R \setminus S)/Q \\
:: & \quad \{ \text{ igualdade indirecta } \} \\
 & R \setminus (S/Q) = (R \setminus S)/Q \\
\Box &
\end{array}
$$

$\Box$

Questão 3 (1 alínea) Considere a função

$$\mathit{diff} : Eq\ a \Rightarrow [a] \rightarrow [a] \rightarrow [a]$$

que calcula a diferença de duas listas, eg. $\mathit{diff}\ [1,2,3]\ [4,2] = [1,3]$, desde que se saiba quando dois elementos são iguais. Re-escrevendo o seu tipo por forma a tornar o predicado de igualdade explícito,

$$\mathit{diff} : ((a^* \leftarrow a^*) \leftarrow a^*) \leftarrow (Bool \leftarrow a \times a)$$

(note que a função passa agora a ter esse predicado como parâmetro) calcule o corolário para funções do respectivo teorema grátis.

RESOLUÇÃO: Atribua-se ao tipo a a relação $R_a = R$. Tem-se então:

$$
\begin{array}{ll}
 & \mathit{diff}\ (((R^* \leftarrow R^*) \leftarrow R^*) \leftarrow (id \leftarrow R \times R))\ \mathit{diff} \\
\equiv & \quad \{ \text{ seta de Reynolds (191) } \} \\
 & \mathit{diff} \cdot (id \leftarrow R \times R) \subseteq ((R^* \leftarrow R^*) \leftarrow R^*) \cdot \mathit{diff} \\
\equiv & \quad \{ \text{ introdução de variáveis (43) ; (51) ; quantificadores } \forall \text{ assumidos } \} \\
 & p\ (id \leftarrow R \times R)\ q \Rightarrow (\mathit{diff}\ p)\ ((R^* \leftarrow R^*) \leftarrow R^*)\ (\mathit{diff}\ q) \\
\equiv & \quad \{ \text{ seta de Reynolds (191) duas vezes } \} \\
 & p \cdot (R \times R) \subseteq q \Rightarrow (\mathit{diff}\ p) \cdot R^* \subseteq (R^* \leftarrow R^*) \cdot (\mathit{diff}\ q) \\
\equiv & \quad \{ \text{ introdução de variáveis (43) ; (51) ; } \forall \text{ assumidos } \} \\
 & p \cdot (R \times R) \subseteq q \Rightarrow (y\ R^*\ x \Rightarrow (\mathit{diff}\ p\ y)\ (R^* \leftarrow R^*)\ (\mathit{diff}\ q\ x)) \\
\equiv & \quad \{ \text{ seta de Reynolds (191) } \} \\
 & p \cdot (R \times R) \subseteq q \Rightarrow (y\ R^*\ x \Rightarrow (\mathit{diff}\ p\ y) \cdot R^* \subseteq R^* \cdot (\mathit{diff}\ q\ x)) \\
\Box &
\end{array}
$$

Coroloário ($R := r$, onde r é uma função, logo só temos igualdades):

$$
\begin{array}{ll}
 & p \cdot (r \times r) = q \Rightarrow (y = r^* \ x \Rightarrow (\mathit{diff}\ p\ y) \cdot r^* = r^* \cdot (\mathit{diff}\ q\ x)) \\
\equiv & \quad \{ \text{ substrituição de } q \text{ e de } y \text{ (“one point”) } \} \\
 & (\mathit{diff}\ p\ (r^*\ x)) \cdot r^* = r^* \cdot (\mathit{diff}\ (p \cdot (r \times r))\ x) \\
\equiv & \quad \{ \text{ igualdade extensional (aplicação de ambos os membros a } z) \} \\
 & \mathit{diff}\ p\ (r^*\ x)\ (r^*\ z) = r^*\ (\mathit{diff}\ (p \cdot (r \times r))\ x\ z) \\
\square &
\end{array}
$$

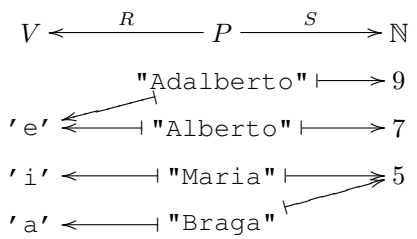
$\square$

Questão 4 (1 alínea) O núcleo de uma relação, $\mathsf{ker}\ R = R^\circ \cdot R$ é uma medida da sua injectividade e da sua definição, fazendo sentido a ordem

$$R \leqslant S \quad \equiv \quad \mathsf{ker}\ S \subseteq \mathsf{ker}\ R \tag{F4}$$

para indicar que R é *menos injectiva* ou *mais definida* (inteira) que S.

- Dadas as duas relações R (vogal tónica de palavra) e S (número de letras de palavra) seguintes



  verifique qual das seguintes asserções é válida: (a) $R \leqslant S$; (b) $S \leqslant R$; (c) Ambas: (d) Nenhuma delas.

- Prove que $\langle R, S \rangle$ é supremo da ordem (F4), isto é, que

$$\langle R, S \rangle \leqslant P \quad \equiv \quad R \leqslant P \ \wedge \ S \leqslant P \tag{F5}$$

  se verifica, recordando a lei

$$\mathsf{ker}\ \langle R, S \rangle = \mathsf{ker}\ R \cap \mathsf{ker}\ S. \tag{F6}$$

RESOLUÇÃO: É fácil calcular à mão as relações seguintes (aqui geradas a partir de uma biblioteca relational em Haskell onde relações são representadas por listas de pares):

```
*Main> ker r
[("Adalberto","Adalberto"),("Adalberto","Alberto"),("Alberto","Adalberto"),
 ("Alberto","Alberto"),("Braga","Braga"),("Maria","Maria")]
*Main> ker s
[("Adalberto","Adalberto"),("Alberto","Alberto"),("Braga","Braga"),
 ("Braga","Maria"),("Maria","Braga"),("Maria","Maria")]
```

A differença $\mathsf{ker}\ S - \mathsf{ker}\ R$ é

```
[("Braga","Maria"),("Maria","Braga")]
```

e $\mathsf{ker}\ R - \mathsf{ker}\ S$ é

```
[("Adalberto","Alberto"),("Alberto","Adalberto")]
```

Logo os núcleos não se incluem em nenhuma das direcções e (d) é a escolha a fazer.
Segunda parte:

$$
\begin{array}{ll}
 & \langle R, S\rangle \leqslant P \\
\equiv & \quad \{ \text{ (F4) } \} \\
 & \mathsf{ker}\ P \subseteq \mathsf{ker}\ \langle R, S\rangle \\
\equiv & \quad \{ \text{ (F6) } \} \\
 & \mathsf{ker}\ P \subseteq \mathsf{ker}\ R \cap \mathsf{ker}\ S \\
\equiv & \quad \{ \text{ universal-}\cdot\cap\cdot \} \\
 & \mathsf{ker}\ P \subseteq \mathsf{ker}\ R \ \wedge\ \mathsf{ker}\ P \subseteq \mathsf{ker}\ S \\
\equiv & \quad \{ \text{ (F4) duas vezes } \} \\
 & R \leqslant P \ \wedge\ S \leqslant P \\
\square &
\end{array}
$$

$\square$

Questão 5 (1 alínea) A palavra chave disj em Alloy garante que duas relações do mesmo tipo são mutuamente disjuntas à saída. Por exemplo, no modelo

$$
\begin{array}{l}
\mathsf{sig}\ Aluno\ \{ \\
\quad name : \mathsf{one}\ Nome, \\
\quad \mathsf{disj}\ opI, opII : \mathsf{lone}\ UCE \\
\} \\
\mathsf{sig}\ UCE, Nome\ \{\}
\end{array}
$$

disj garante que se um aluno de mestrado opta por fazer duas opções, estas têm que ser diferentes. Em geral,

$$\mathsf{sig}\ A\ \{\mathsf{disj}\ R, S : \mathsf{set}\ B\}$$

declara duas relações $A \xrightarrow{R,S} B$ tais que a propriedade $\langle \forall\, a, b\ :\ bRa :\ \langle \forall\, b'\ :\ b'Sa :\ b' \neq b\rangle\rangle$ se verifica.

- Mostre que garantir este invariante é rigorosamente o mesmo que garantir

$$S \cdot R^{\circ}\ \subseteq\ (id \Rightarrow \bot) \tag{F7}$$

- Qual é, no modelo das escolhas de UCEs acima esboçado, a expressão *pointfree* que reconstitui a relação que existe entre cada UCE e os alunos que a frequentam?

- Suponha que $AC \xleftarrow{ac} UCE$ é uma função que classifica UCEs por área científica (AC) e que surge a restrição seguinte: *nenhum aluno pode optar por UCEs da mesma área científica*. Adapte (F7) por forma a captar também esta nova restrição e mostre que a propriedade exigida por disj no modelo continua a verificar-se.

RESOLUÇÃO: Em três partes:

- Tem-se:

$$
\begin{array}{ll}
 & S \cdot R^\circ \ \subseteq \ (id \Rightarrow \bot) \\
\equiv & \quad \{ \text{ GC da divisão } \} \\
 & R^\circ \ \subseteq \ S \setminus (id \Rightarrow \bot) \\
\equiv & \quad \{ \text{ pointwise } \} \\
 & \langle \forall\ a, b \ : \ a \ R^\circ \ b : \ a \ S \setminus (id \Rightarrow \bot) \ b \rangle \\
\equiv & \quad \{ \text{ pointwise: conversos e } X \setminus Y \ \} \\
 & \langle \forall\ a, b \ : \ b \ R \ a : \ \langle \forall\ b' \ : \ b' \ S \ a : \ b' \ ((id \Rightarrow \bot)) \ b \rangle \rangle \\
\equiv & \quad \{ \text{ pointwise: } R \Rightarrow S \ \} \\
 & \langle \forall\ a, b \ : \ b \ R \ a : \ \langle \forall\ b' \ : \ b' \ S \ a : \ b' = b \Rightarrow \mathit{false} \rangle \rangle \\
\equiv & \quad \{ \ p \Rightarrow \mathit{false} \equiv \neg\ p \ \} \\
 & \langle \forall\ a, b \ : \ b \ R \ a : \ \langle \forall\ b' \ : \ b' \ S \ a : \ b' \neq b \rangle \rangle \\
\Box &
\end{array}
$$

- Do Alloy dado infere-se o diagrama de tipos

$$
\mathit{Nome} \xleftarrow{nome} \mathit{Aluno} \xrightarrow[opI, opII]{} \mathit{UCE}
$$

Logo a relação pretendida é $X = opI \cup opII$, tal que

$$
u \ X \ a \equiv (u \ opI \ a) \vee (u \ opII \ a)
$$

- Basta relaxar id em cima, a saber

$$
opI \cdot opII^\circ \ \subseteq \ (\mathsf{ker}\ ac \Rightarrow \bot)
$$

uma vez que $u \ (\mathsf{ker}\ ac \Rightarrow \bot) \ u' \equiv (ac \ u \neq ac \ u')$.

$\Box$

Questão 6 (1 alínea) O domínio de uma relação R, $\delta\, R$, é a coreflexiva que representa os valores à entrada para os quais R reage. O *complemento do domínio* de R, designado por $\overline{\delta R}$, é a coreflexiva que representa os valores para os quais R *não reage* e que se define pela GC seguinte:

$$
\top \cdot \overline{\delta R} \supseteq X \quad \equiv \quad R \subseteq \bot / X^\circ \tag{F8}
$$

Apresente justificações para os passos em branco dos cálculos de duas igualdades úteis envolvendo $\overline{\delta R}$:

$$
\bot \ / \ R^\circ \quad = \quad \top \cdot \overline{\delta R} \tag{F9}
$$

$$
R \cdot \overline{\delta R} \quad = \quad \bot \tag{F10}
$$

Cálculo de (F9):

$$
\begin{array}{ll}
 & X \subseteq \top \cdot \overline{\delta R} \\
\equiv & \quad \{ \ \ldots\ldots\ldots\

$\equiv$ { ..... }

$X \cdot R^\circ \subseteq \bot$

$\equiv$ { ..... }

$X \subseteq \bot / R^\circ$

$::$ { igualdade indirecta }

$\bot / R^\circ = \top \cdot \overline{\delta R}$

Cálculo de (F10):

$X \subseteq R \cdot \overline{\delta R}$

$\equiv$ { ..... }

$X \subseteq R \cap \top \cdot \overline{\delta R}$

$\equiv$ { ..... }

$X \subseteq R \wedge X \subseteq \bot / R^\circ$

$\equiv$ { ..... }

$X \subseteq R \wedge (\delta X \cap \delta R) \subseteq \bot$

$\equiv$ { ..... }

$X \subseteq R \wedge (\delta X \subseteq \delta R) \wedge (\delta X \cap \delta R) \subseteq \bot$

$\equiv$ { ..... }

$X \subseteq R \wedge (\delta X \cap \delta R = \delta X) \wedge (\delta X \cap \delta R) \subseteq \bot$

$\equiv$ { ..... }

$X \subseteq R \wedge X \subseteq \bot$

$\equiv$ { ..... }

$X \subseteq \bot$

$::$ { igualdade indirecta }

$R \cdot \overline{\delta R} = \bot$

RESOLUÇÃO: Cálculo de (F9):

$X \subseteq \top \cdot \overline{\delta R}$

$\equiv$ { (F8) }

$R \subseteq \bot / X^\circ$

$\equiv$ { GC da divisão }

$R \cdot X^\circ \subseteq \bot$

$\equiv$ { aplicando converso a ambos os lados }

$X \cdot R^\circ \subseteq \bot$

$\equiv$ { GC da divisão }

$X \subseteq \bot / R^\circ$

$::$ { igualdade indirecta }

$\bot / R^\circ = \top \cdot \overline{\delta R}$

Cálculo de (F10):

$$
\begin{array}{ll}
 & X \subseteq R \cdot \overline{\delta R} \\
\equiv & \quad \{ \text{ pré-condições (122) } \} \\
 & X \subseteq R \cap \top \cdot \overline{\delta R} \\
\equiv & \quad \{ \text{ universal-}\cap \text{ e (F8) } \} \\
 & X \subseteq R \ \wedge \ X \subseteq \bot \,/\, R^{\circ} \\
\equiv & \quad \{ \text{ exercício 105 } \} \\
 & X \subseteq R \ \wedge \ (\delta\, X \cap \delta\, R) \subseteq \bot \\
\equiv & \quad \{ \ \delta\, X \subseteq \delta\, R \text{ é consequência de } X \subseteq R \ \} \\
 & X \subseteq R \ \wedge \ (\delta\, X \subseteq \delta\, R) \ \wedge \ (\delta\, X \cap \delta\, R) \subseteq \bot \\
\equiv & \quad \{ \ R \subseteq S \ \Leftrightarrow \ R \cap S = R \ \} \\
 & X \subseteq R \ \wedge \ (\delta\, X \cap \delta\, R = \delta\, X) \ \wedge \ (\delta\, X \cap \delta\, R) \subseteq \bot \\
\equiv & \quad \{ \text{ substituição de } \delta\, X \cap \delta\, R \text{ por } \delta\, X;\ \delta\, X \subseteq \bot \equiv X \subseteq \bot \} \\
 & X \subseteq R \ \wedge \ X \subseteq \bot \\
\equiv & \quad \{ \text{ universal-}\cap;\ \bot \subseteq R \} \\
 & X \subseteq \bot \\
:: & \quad \{ \text{ igualdade indirecta } \} \\
 & R \cdot \overline{\delta R} = \bot
\end{array}
$$

□

Questão 7 (1 alínea) Atente no fragmento de Alloy dado, que modela um sistema de inscrição em turnos práticos (TP) de alunos de uma unidade curricular (UC).

Para além do seu $nome$, cada UC inclui uma relação $turnos$ que aloca alunos ($Aluno$) a turnos práticos (TP).

Os alunos só podem mudar de turno por troca entre colegas, cf. operação $troca$. Findo o prazo para pedir trocas, estas são compiladas numa relação R que é passada como parâmetro a $troca$ e cujo significado é: $a'\ R\ a$ = aluno a' pretende trocar com aluno a.

Como um aluno terá que estar num e só num turno, a relação $Aluno \xrightarrow{u \cdot turno} TP$ deve ser uma *função*, qualquer que seja u: daí o predicado que é *checked*.

Usando o "método-CSI", o autor do modelo começou por ignorar a pré-condição e usou o *model checker* para a encontrar, após uma (talvez longa) série de contra-exemplos:

```
-- pre
R.~R in iden     -- R injectiva
~R.R in iden     -- R simples
R.R in iden
```

Esta não é, contudo a *pré-condição mais fraca* (WP) da função seguinte

$$f\ (turnos, R) = turnos \cdot (id \dagger R^{\sigma})$$
$$\textbf{where } R^{\sigma} = R \cup R^{\circ}$$

que capta a parte mais importante do predicado $troca$ usando a notação (F11) para sobreposição relacional (plus em Alloy). Esta função deve preservar o invariante que impõe que $turnos$ seja função (inteira e simples).

```
sig UC {
  turnos : Aluno → TP,
  nome : one Nome
}
sig TP, Nome { }
sig Aluno {
  id : one Aluno }
fact { id = Aluno → Aluno & iden }
pred troca [u, u' : UC, R : Aluno → Aluno] {
  -- pre
  -- post
  u' · nome = u · nome
  u' · turnos = plus [id, R +~ R] · (u · turnos)
}
fun plus [S, R : Aluno → Aluno] : Aluno → Aluno {
  R + (Aluno − R.Aluno) <: S
}
pred function [R : Aluno → TP] {
  ~R.R in iden
  id in R.~R
}
check { all u, u' : UC, R : Aluno → Aluno |
  function [u · turnos] and
    troca [u, u', R] ⇒ function [u' · turnos]
}
```

Importante: a função plus em Alloy corresponde, em álgebra relacional, ao operador de *sobreposição* de relações

$$S \dagger R \quad = \quad R \cup S \cdot \overline{\delta R} \qquad \text{(F11)}$$

Que $turnos \cdot (id \dagger R^{\sigma})$ é inteira é imediato (porquê?). Resta então resolver a condição

$$turnos \cdot (id \dagger R^{\sigma}) \text{ é simples}$$

para obter a WP da operação. **Sugestão**: recorra a (F10) onde achar oportuno.

RESOLUÇÃO: Que $turnos \cdot (id \dagger R^{\sigma})$ é inteira decorre imediatamente de ser uma composição de relações inteiras. Quanto a ser simples:

$$\begin{array}{ll}
 & turnos \cdot (id \dagger R^{\sigma}) \text{simples} \\
\equiv & \quad \{ \text{ fácil de provar: } f \cdot R \text{ simples é equivalente a img } R \subseteq \ker f \ \} \\
 & (id \dagger R^{\sigma}) \cdot (id \dagger R^{\sigma})^{\circ} \subseteq \ker turnos \\
\equiv & \quad \{ \ \text{(F11) ; identidade ; } (R^{\sigma})^{\circ} = R^{\sigma} \ \} \\
 & (R^{\sigma} \cup \overline{\delta R^{\sigma}}) \cdot (R^{\sigma} \cup \overline{\delta R^{\sigma}}) \subseteq \ker turnos \\
\equiv & \quad \{ \ (R \cup S) \cdot (P \cup Q) = R \cdot P \cup R \cdot Q \cup S \cdot P \cup S \cdot Q \text{ ; (F10) duas vezes; coreflexivas } \}
\end{array}$$

$$
\begin{array}{ll}
& R^\sigma \cdot R^\sigma \cup \overline{\delta R^\sigma} \subseteq \mathsf{ker}\ turnos \\
\equiv & \qquad \{ \text{ universal-}\cup\text{; coreflexivas: } \Phi \ \subseteq\ id \ \subseteq\ \mathsf{ker}\ f \ \} \\
& R^\sigma \cdot R^\sigma \subseteq \mathsf{ker}\ turnos \\
\Box &
\end{array}
$$

Pode ainda simplificar-se a WP obtida em:

$$R \cdot R \ \subseteq\ \mathsf{ker}\ turnos \ \wedge\ \mathsf{ker}\ R \ \subseteq\ \mathsf{ker}\ turnos \ \wedge\ \mathsf{img}\ R \ \subseteq\ \mathsf{ker}\ turnos$$

Como $id \subseteq \mathsf{ker}\ turnos$, tem-se que a WP calculada é efectivamente mais geral do que a pré-condição sugerida pelo Alloy. $\Box$

Questão 8 (1 alínea) Considere as funções max e min de dois números naturais,

$$
\begin{array}{l}
max\ x\ y = \mathbf{if}\ x > y\ \mathbf{then}\ x\ \mathbf{else}\ y \\
min\ x\ y = \mathbf{if}\ x < y\ \mathbf{then}\ x\ \mathbf{else}\ y
\end{array}
$$

e a propriedade

$$k \div max\ x\ y = min\ (k \div x)\ (k \div y) \tag{F12}$$

onde $\cdot \div \cdot$ é a divisão inteira de naturais:

$$x \div y = \mathbf{if}\ x < y\ \mathbf{then}\ 0\ \mathbf{else}\ (x - y \div y) + 1 \tag{F13}$$

Mostre que a definição (F13) não é necessária para provar (F12), bastando usar igualdade indirecta sobre a GC

$$z \times y \leqslant x \ \Leftrightarrow\ z \leqslant x \div y \qquad (y > 0) \tag{F14}$$

e interpretar max / min como supremo / ínfimo da ordem $\leqslant$ nos naturais.

RESOLUÇÃO: Supremos e ínfimos são captados por propriedades universais:

$$max\ x\ y \leqslant z \equiv x \leqslant z \wedge y \leqslant z \tag{F15}$$

$$z \leqslant min\ x\ y \equiv z \leqslant x \wedge z \leqslant y \tag{F16}$$

Logo:

$$
\begin{array}{ll}
& z \leqslant k \div (max\ x\ y) \\
\equiv & \qquad \{ \text{ (F14) } \} \\
& z \times (max\ x\ y) \leqslant k \\
\equiv & \qquad \{ \text{ adjunto inferior } (z\times) \text{ distribui por supremos } \} \\
& max\ (z \times x)\ (z \times y) \leqslant k \\
\equiv & \qquad \{ \text{ (F15) } \} \\
& z \times x \leqslant k \ \wedge\ z \times y \leqslant k \\
\equiv & \qquad \{ \text{ (F14) duas vezes } \} \\
& z \leqslant k \div x \ \wedge\ z \leqslant k \div y \\
\equiv & \qquad \{ \text{ (F16) } \} \\
& z \leqslant min\ (k \div x)\ (k \div y) \\
\Box &
\end{array}
$$

$\Box$