Cálculo de Sistemas de Informação
Perfil: MÉTODOS FORMAIS EM ENGENHARIA DE SOFTWARE

1.º/4.º Ano de MEI & MMC / MiEI, Universidade do Minho
Ano Lectivo de 2019/20

Exame de recurso — 30 de Janeiro
09h00
Sala E2-1.10

Importante — *Ler antes de iniciar a prova:*

- *Esta prova consta de **8** questões que valem, cada uma, 2.5 valores. O tempo **médio** estimado para resolução de cada questão é de 15 min.*
- *Os alunos que desejem fazer melhoria apenas uma parte devem assinalá-lo na prova, que deverão entregar ao fim de uma hora.*

PROVA COM CONSULTA (1 ou 2 horas)

Parte A

Questão 1 Considere a relação $R : X \to Y$ definida pela seguinte matriz Booleana

$$R \quad = \quad \begin{array}{c|ccccc} & A & B & C & D & E \\ \hline 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 & 0 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 \end{array}$$

onde $X = \{A, B, C, D, E\}$ e $Y = \{1 \,..\, 5\}$. Investigue a veracidade das seguintes afirmações:

1. R é uma função
2. R é difuncional
3. R é injectiva
4. R é sobrejectiva

Questão 2 Muitas funções binárias $A \times B \xrightarrow{f} C$ não são injectivas (por exemplo, a soma de inteiros) mas, se lhe fixarmos um dos argumentos (por exemplo o primeiro), são-no quanto ao outro argumento:

$$f\ (a, b) = f\ (a, b') \Rightarrow b = b'$$

Mostre que isso acontece se e só se

$$id \leqslant \langle \pi_1, f \rangle \tag{F1}$$

se verificar, onde $R \leqslant S$ compara relações quanto à sua injectividade.

Questão 3 Considere o operador relacional

$$slice\ S\ R \quad = \quad R \cap S \,/\, R^{\circ} \tag{F2}$$

definido em Alloy como se segue:

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

É possível implementar *slice* em Haskell, com tipo

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

onde a primeira relação é representada por um predicado binário. Calcule o teorema grátis de *slice*, instanciando-o para funções.

Questão 4 Mostre que a diferença de relações satisfaz a propriedade

$$(Q - R) - S = (Q - S) - R \tag{F3}$$

Parte B

Questão 5 Dada uma qualquer relação $B \xleftarrow{R} A$, a chamada *diagonal* $B \xleftarrow{R_d} A$ de R define-se por

$$R_d \quad = \quad R \cap (R \setminus R \,/\, R)^{\circ} \tag{F4}$$

e exibe a propriedade universal:

$$X \ \subseteq\ R_d \quad \equiv \quad \left\{ \begin{array}{l} X \ \subseteq\ R \\ R \cdot X^{\circ} \cdot R \ \subseteq\ R \end{array} \right. \tag{F5}$$

Avalie a veracidade da afirmação seguinte:

A diagonal R_d é reflexiva se e só se R for uma pré-ordem.

Questão 6 Apresente justificações para a demonstração da propriedade

$$\delta\ \langle f \cdot R, \underline{k} \rangle = \delta\ R$$

que se segue:

$$\begin{array}{ll}
 & \delta\ \langle f \cdot R, \underline{k} \rangle \\
= & \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
 & \ker\ (f \cdot R) \cap \ker\ \underline{k} \cap id \\
= & \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
 & \delta\ (f \cdot R) \\
= & \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
 & \delta\ (\delta\ f \cdot R) \\
= & \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
 & \delta\ R
\end{array}$$

$\Box$

Questão 7 O seguinte modelo em Alloy, que foi assunto das aulas da disciplina de Especificação e Modelação,

– File system trash can.

$$
\begin{array}{l}
\mathsf{sig}\ \mathit{File}\ \{\\
\quad \mathit{link} : \mathsf{lone}\ \mathit{File}\\
\}\\
\mathsf{sig}\ \mathit{Trash}\ \mathsf{extends}\ \mathit{File}\ \{\,\}\\
\mathsf{sig}\ \mathit{Protected}\ \mathsf{extends}\ \mathit{File}\ \{\,\}
\end{array}
$$

pode ser expresso pelo diagrama relacional,

$$
\begin{tikzcd}
\mathbb{B} & \mathit{File} \arrow[l, "\mathit{trash}"'] \arrow[r, "L"] \arrow[d, "\mathit{protected}"'] & \mathit{File} \\
 & \mathbb{B} &
\end{tikzcd}
$$

onde L abrevia link: há ficheiros (File) que podem estar ligados entre si (L), apagados (trash) ou protegidos ($\mathit{protected}$). Converta para notação pointwise os *tipos relacionais* seguintes

$$\Phi_{active} \xleftarrow{L} \Phi_{active} \tag{F6}$$

$$\Phi_{active} \xleftarrow{id} \Phi_{protected} \tag{F7}$$

(onde $\mathit{active} = \neg \cdot \mathit{trash}$), e exprima por palavras suas, em cada caso, a propriedade do sistema que está a ser especificada.

Questão 8 Uma lista de pares $x \in (A \times A)^*$ pode ser representada simplesmente por $y \in A^*$ desde que o comprimento de y seja um número par (even). Seja $\theta :: A^* \to A^*$ a operação que remove o primeiro par de uma tal representação, quando esse par existe: $\theta = \mathsf{drop}\ 2$.

Num dispositivo médico em que esta representação vai ser usada pretende-se garantir que θ preserva o invariante concreto:

$$\mathit{inv} = \mathit{even} \cdot \mathsf{length} \tag{F8}$$

Por *interpretação abstracta*, a prova pode ser feita encontrando uma *simulação* abstracta ϕ de θ no diagrama

$$
\begin{tikzcd}
\mathbb{B} & \mathbb{N}_0 \arrow[l, "\mathit{even}"'] & \mathbb{N}_0 \arrow[l, "\phi"'] \\
 & A^* \arrow[u, "\mathsf{length}"] \arrow[ul, bend left, "\mathit{inv}"] & A^* \arrow[l, "\theta"] \arrow[u, "\mathsf{length}"']
\end{tikzcd}
$$

que preserve even. Suponha que alguém conjecturou

$$
\begin{array}{l}
\phi\ 0 = 0\\
\phi\ 1 = 0\\
\phi\ (n+2) = n
\end{array}
$$

(que claramente preserva even) e que, para demonstrar que ϕ simula θ, re-definiu ϕ de forma seguinte

$$\phi \cdot \mathsf{in} = [\underline{0}, \alpha] \tag{F9}$$

$$\alpha \cdot \mathsf{in} = [\underline{0}, id] \tag{F10}$$

onde $\mathsf{in} = [\underline{0}, \mathsf{succ}]$.

Apresente justificações para os passos da prova apresentada de que ϕ simula θ:

$$
\begin{array}{ll}
& \mathsf{length} \cdot \theta = \phi \cdot \mathsf{length} \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \mathsf{length} \cdot \theta \cdot \mathsf{length}^\circ \cdot \mathsf{in} \ \subseteq \ [\underline{0}, \alpha] \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \left\{ \begin{array}{l} \mathsf{length}^\circ \cdot \underline{0} \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \cdot \underline{0} \\ \mathsf{length}^\circ \cdot \mathsf{succ} \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \cdot \alpha \end{array} \right. \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \left\{ \begin{array}{l} y = [\,] \Rightarrow \theta\ y = [\,] \\ \mathsf{length}^\circ \cdot \mathsf{succ} \cdot \mathsf{in} \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \cdot [\underline{0}, id] \end{array} \right. \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \left\{ \begin{array}{l} \mathsf{drop}\ 2\ [\,] = [\,] \\ \left\{ \begin{array}{l} \mathsf{length}^\circ \cdot \underline{1} \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \cdot \underline{0} \\ \mathsf{length}^\circ \cdot (2+) \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \end{array} \right. \end{array} \right. \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \left\{ \begin{array}{l} \mathsf{length}\ y = 1 \Rightarrow \mathsf{length}\ (\theta\ y) = 0 \\ \mathsf{length}^\circ \cdot (2+) \ \subseteq \ (\mathsf{length} \cdot \theta)^\circ \end{array} \right. \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& \left\{ \begin{array}{l} \mathsf{drop}\ 2\ [\_] = [\,] \\ \mathsf{length}\ y = 2 + n \Rightarrow \mathsf{length}\ (\mathsf{drop}\ 2\ y) = n \end{array} \right. \\
\equiv & \qquad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \} \\
& true
\end{array}
$$

NB: assuma propriedades básicas da função drop.
