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 2018/19

Teste — 17 de Janeiro
14h00
Sala DI 0.05

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 não queiram manter a nota do **miniteste** devem responder a todas as questões, entregando a prova ao fim de duas horas.*
- *Os alunos que desejam manter a nota do **miniteste** devem responder apenas à parte B (questões 5, 6, 7, 8), devendo nesse caso entregar a prova ao fim de uma hora.*

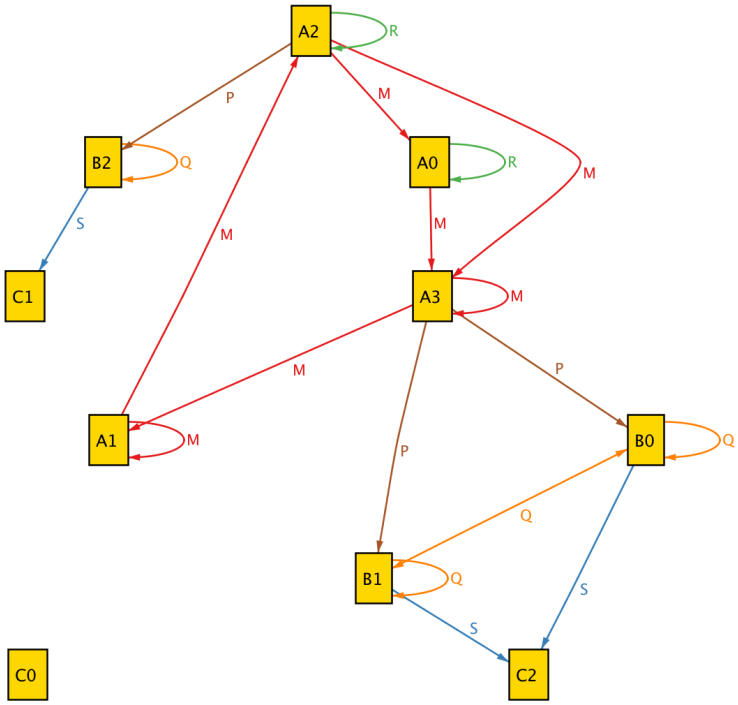
PROVA COM CONSULTA (1 ou 2 horas)

Parte A

Questão 1 Sejam dados os tipos de dados A (com quatro elementos) e B, C (ambos com três elementos) e as relações M, R, S, Q e P entre eles registadas no diagrama Alloy em baixo.

Identifique no diagrama, **justificando**:

1. duas endorelações do mesmo tipo, uma coreflexiva e outra não
2. uma função não injectiva
3. uma relação injectiva que não é simples
4. uma relação de equivalência.



RESOLUÇÃO: A identificação é fácil de encontrar olhando para o código Alloy que gerou a instância:

```
open RelCalc
sig B {S : set C, Q : set B}
sig A {R : set A, M : set A, P : set B}
sig C { }
run {
   some S
   some R
   some M
   some P
   Coreflexive [R, A] and ¬ Coreflexive [M, A]
   ¬ Simple [P, B] and ¬ Entire [P, A] and Injective [P, A]
   Simple [S, C] and Entire [S, B] and ¬ Injective [S, B]
   Q = ker [S]
} for · · exactly 4 A, exactly 3 B, exactly 3 C
```

□

Questão 2 Em 23 de Junho de 1991, E.W. Dijkstra escreveu uma das suas (hoje célebres) notas, a EWD1102-5, intitulada *Why preorders are beautiful*. O resultado que aí é demonstrado, usando cálculo de predicados[1]

> *Uma relação R é uma pré-ordem se e só se satisfizer a definição (recursiva)* $R = R \,/\, R$

fica ainda mais simples (e *beautiful*) quando expresso em álgebra relacional. Apresente justificações para os seguintes 6 passos do respectivo cálculo *pointfree*:

$$
\begin{array}{cl}
 & R = R \,/\, R \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \left\{ \begin{array}{l} X \subseteq R \Leftrightarrow X \cdot R \subseteq R \\ X \subseteq R \Leftrightarrow X \cdot R \subseteq R \end{array} \right. \\
\Rightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \left\{ \begin{array}{l} id \subseteq R \Leftrightarrow R \subseteq R \\ R \subseteq R \Leftrightarrow R \cdot R \subseteq R \end{array} \right. \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \left\{ \begin{array}{l} id \subseteq R \\ R \cdot R \subseteq R \end{array} \right. \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \left\{ \begin{array}{l} id \subseteq R \wedge (R \,/\, R) \cdot R \subseteq R \\ R \subseteq R \,/\, R \end{array} \right. \\
\Rightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \left\{ \begin{array}{l} R \,/\, R \subseteq R \\ R \subseteq R \,/\, R \end{array} \right. \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & R = R \,/\, R
\end{array}
$$

□

[1] 6 páginas manuscritas.

RESOLUÇÃO:

$$
\begin{array}{ll}
& R = R \,/\, R \\
\equiv & \quad \{ \text{ igualdade indirecta + universal-/ ; } p \wedge p = p \} \\
& \left\{ \begin{array}{l} X \subseteq R \Leftrightarrow X \cdot R \subseteq R \\ X \subseteq R \Leftrightarrow X \cdot R \subseteq R \end{array} \right. \\
\Rightarrow & \quad \{ \ X := id \text{ e } X := R \text{ na primeira e segunda equivalência } \} \\
& \left\{ \begin{array}{l} id \subseteq R \Leftrightarrow R \subseteq R \\ R \subseteq R \Leftrightarrow R \cdot R \subseteq R \end{array} \right. \\
\equiv & \quad \{ \text{ reflexividade da inclusão } \times 2 \text{, chegando-se às propriedades de uma pré-ordem } \} \\
& \left\{ \begin{array}{l} id \subseteq R \\ R \cdot R \subseteq R \end{array} \right. \\
\equiv & \quad \{ \ p \wedge \mathsf{True} = p \text{, para } p = (R \,/\, R) \cdot R \subseteq R \text{, que se verifica por cancelamento-/ ; universal-/ } \} \\
& \left\{ \begin{array}{l} id \subseteq R \wedge (R \,/\, R) \cdot R \subseteq R \\ R \subseteq R \,/\, R \end{array} \right. \\
\Rightarrow & \quad \{ \text{ monotonia da composição com } R \,/\, R \text{; transitividade } \} \\
& \left\{ \begin{array}{l} R \,/\, R \subseteq R \\ R \subseteq R \,/\, R \end{array} \right. \\
\equiv & \quad \{ \text{ “ping-pong” } \} \\
& R = R \,/\, R \\
& \Box
\end{array}
$$

$\Box$

Questão 3 (1 alínea) Seja $\mathbb{R} \xleftarrow{R} \mathbb{R}$ a relação binária sobre os números reais que define a circunferência unitária centrada na origem,

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

isto é

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

onde $sq : \mathbb{R} \to \mathbb{R}$ e $(1-) : \mathbb{R} \to \mathbb{R}$ são as funções $y = x^2$ e $y = 1 - x$.

Mostre — sem recorrer directamente a (F1) — que R é uma relação simétrica.

RESOLUÇÃO: Calcule-se R°:

$$
\begin{array}{ll}
& R^\circ \\
= & \quad \{ \text{ converso de uma divisão de funções } \} \\
& \dfrac{sq}{(1-) \cdot sq} \\
= & \quad \{ \text{ definição de divisão de funções } \} \\
& sq^\circ \cdot (1-)^\circ \cdot sq \\
= & \quad \{ \ (1-)^\circ \text{ é simétrica, } (1-)^\circ = (1-) \text{, cf. } y = 1 - x \ \Leftrightarrow \ x = 1 - y \ \}
\end{array}
$$

$$sq^\circ \cdot (1-) \cdot sq$$

$=$ { definição de divisão de funções }

R

□

□

Questão 4 A sobreposição de relações

$$R \dagger S \;=\; S \cup R \cap \bot / S^\circ \tag{F3}$$

é um combinador muito útil para exprimir operações de *updating* em modelos relacionais. Mostre que as igualdades

$$R \dagger \bot = R \tag{F4}$$

$$R \dagger \top = \top \tag{F5}$$

se verificam para qualquer relação R.

RESOLUÇÃO: Tem-se:

$R \dagger \bot$

$=$ { (F3) ; $\bot \cup X = X$; $\bot^\circ = \bot$ }

$R \cap \bot / \bot$

$=$ { $Y / \bot = \top$ pois $X.\bot \subseteq Y$ para todo o X, Y }

$R \cap \top$

$=$ { $R \subseteq \top$ }

R

□

e

$R \dagger \top$

$=$ { .... }

$\top \cup (R \cap \bot / \top)$

$=$ { }

$\top$

□

□

Parte B

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

sig $Aluno$ {
  $name$: one $Nome$,

$$\begin{array}{l}\quad \mathsf{disj}\ OpI, OpII : \mathsf{lone}\ Perfil\\ \}\\ \mathsf{sig}\ Perfil, Nome\ \{\}\end{array}$$

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 $\langle \forall\ a, b\ :\ b\ R\ a :\ \langle \forall\ b'\ :\ b'\ S\ a :\ b' \neq b\rangle\rangle$ se verifica.

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

$$S \cdot R^{\circ}\ \subseteq\ \neg\ id \tag{F6}$$

- Qual é, no modelo das escolhas de *Perfil*s acima esboçado, a expressão *pointfree* que dá a relação que existe entre cada *Perfil* e os nomes dos alunos que a frequentam?

RESOLUÇÃO: Em duas partes:

- Tem-se (sabendo-se que $\neg\ id = id \Rightarrow \bot$):

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

- Do Alloy dado infere-se o diagrama de tipos

$$Nome \xleftarrow{nome} Aluno \xrightarrow[OpI, OpII]{} Perfil$$

Logo a relação pretendida é $Nome \xleftarrow{X} Perfil\ = nome \cdot (OpI \cup OpII)^{\circ}$, i.e. tal que

$$n\ X\ p\ \Leftrightarrow\ \langle \exists\ a\ :\ n = nome\ a :\ p\ OpI\ a \vee p\ OpII\ a\rangle$$

$\Box$

Questão 6 Considere a função

$$\mathsf{splitAt} : (A^* \times A^*) \leftarrow A^* \leftarrow \mathbb{N}_0$$

que parte uma lista pelo seu n-ésimo elemento, por exemplo

splitAt 3 "mfes" = ("mfe", "s")
splitAt 0 "mfes" = ("", "mfes")
etc.

Calcule o teorema grátis de splitAt e derive dele o corolário

$$\mathsf{all}\ p\ x \Rightarrow (\mathsf{all}\ p\ x_1) \wedge (\mathsf{all}\ p\ x_2)\ \mathbf{where}\ (x_1, x_2) = \mathsf{splitAt}\ n\ x \tag{F7}$$

onde $\mathsf{all} : (A \to \mathbb{B}) \to A^* \to \mathbb{B}$ é tal que $\mathsf{all}\ p\ x = \langle \forall\ i\ :\ 1 \leqslant i \leqslant \mathsf{length}\ x :\ p\ (x\ i) \rangle$.
Sugestão: instancie a relação associada ao tipo A com a coreflexiva Φ_p e simplifique.

RESOLUÇÃO: Começa-se por desenvolver a formulação inicial do teorema grátis,

$$\mathsf{splitAt}\ ((R^* \times R^*) \leftarrow R^* \leftarrow id)\ \mathsf{splitAt}$$

a saber:

$$\mathsf{splitAt}\ ((R^* \times R^*) \leftarrow R^* \leftarrow id)\ \mathsf{splitAt}$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$\mathsf{splitAt} \subseteq ((R^* \times R^*) \leftarrow R^*) \cdot \mathsf{splitAt}$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$(\mathsf{splitAt}\ n) \cdot R^* \subseteq (R^* \times R^*) \cdot (\mathsf{splitAt}\ n)$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$x'\ R^*\ x \Rightarrow (\mathsf{splitAt}\ n\ x')\ (R^* \times R^*)\ (\mathsf{splitAt}\ n\ x)$$

Fazendo $R = \Phi_p$ tem-se $x'\ {\Phi_p}^*\ x \ \Leftrightarrow\ x' = x \wedge \mathsf{all}\ p\ x$. Continuando:

$$x'\ {\Phi_p}^*\ x \Rightarrow (\mathsf{splitAt}\ n\ x')\ ({\Phi_p}^* \times {\Phi_p}^*)\ (\mathsf{splitAt}\ n\ x)$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$\mathsf{all}\ p\ x \Rightarrow (x_1, x_2)\ ({\Phi_p}^* \times {\Phi_p}^*)\ (x_1, x_2)\ \mathbf{where}\ (x_1, x_2) = \mathsf{splitAt}\ n\ x$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$\mathsf{all}\ p\ x \Rightarrow x_1\ {\Phi_p}^*\ x_1 \wedge x_2\ {\Phi_p}^*\ x_2\ \mathbf{where}\ (x_1, x_2) = \mathsf{splitAt}\ n\ x$$
$$\equiv \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}$$
$$\mathsf{all}\ p\ x \Rightarrow \mathsf{all}\ p\ x_1 \wedge \mathsf{all}\ p\ x_2\ \mathbf{where}\ (x_1, x_2) = \mathsf{splitAt}\ n\ x$$

□

□

Questão 7 O anexo desta prova transcreve um modelo relacional que foi já assunto de várias questões em provas anteriores desta disciplina. O que se pretende calcular desta vez é a pre-condição mais fraca para a função $apuraC$ satisfazer o invariante inv_1.
Sugestão: recorde o exercício 5.15 dos apontamentos.
Valorização: garantirá essa pré-condição que um eleitor não vota mais do que uma vez? Responda *informalmente* a esta valorização, se o desejar fazer.

RESOLUÇÃO: Definindo

$$injective\ V \Leftrightarrow \ker V \subseteq id$$

completar as justificações em:

$$\begin{array}{ll} & inv_1\ (apuraC\ (V, V', e, c)) \\ \equiv & \{\ \ldots\ \} \\ & injective\ V \wedge injective\ (V' \cup \underline{e} \cdot \underline{c}^\circ) \\ \equiv & \{\ \ldots\ \} \\ & injective\ V \wedge injective\ V' \wedge injective\ (\underline{e} \cdot \underline{c}^\circ) \wedge V'^\circ \cdot (\underline{e} \cdot \underline{c}^\circ) \subseteq id \\ \equiv & \{\ \ldots\ \} \\ & injective\ V \wedge injective\ V' \wedge V'^\circ \cdot \underline{e} \subseteq \underline{c} \\ \equiv & \{\ \ldots\ \} \\ & inv_1\ (V, V') \wedge \underline{e}^\circ \cdot V' \subseteq \underline{c}^\circ \\ \Box & \end{array}$$

Logo, a WP é (em pointwise):

$$e\ V'\ x \Rightarrow c = x.$$

□

Questão 8 Recordando a função length : $A^* \to \mathbb{N}_0$ que calcula o comprimento de uma lista finita, que é tal que length $(a : x) = 1 +$ length x, seja dado o predicado

$$nempty = (>0) \cdot \mathsf{length} \tag{F8}$$

que testa se uma lista é vazia ou não. Pretendendo-se mostrar que $(a:)$ preserva $nempty$,

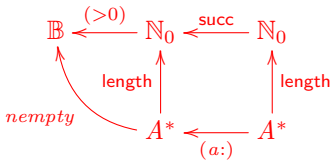
$$nempty \xleftarrow{(a:)} nempty \tag{F9}$$

por interpretação abstracta sobre length, comece por mostrar que succ $n = 1 + n$ é a correspondente simulação abstracta de $(a:)$; de seguida, mostre que o facto (óbvio!)

$$\langle \forall\ n\ :\ n > 0 :\ n + 1 > 0 \rangle$$

é suficiente para que (F9) se verifique.

RESOLUÇÃO: O processo de interpretação abstracta é descrito no diagrama:



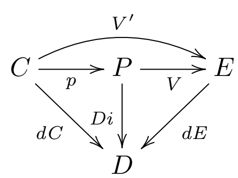
O quadrado comuta pois length $\cdot\ (a:) =$ succ $\cdot$ length resulta da propriedade de length que foi apresentada — logo succ simula $(a:)$.

Então, segundo o princípio da interpretação abstracta[2], para $nempty \xleftarrow{(a:)} nempty$ se verificar bastará que se verifique $(>0) \xleftarrow{\mathsf{succ}} (>0)$, isto é (apresente as justificações):

$$
\begin{array}{ll}
& \mathsf{succ} \cdot \Phi_{(>0)} \subseteq \Phi_{(>0)} \cdot \mathsf{succ} \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \Phi_{(>0)} \subseteq \mathsf{succ}^{\circ} \cdot \Phi_{(>0)} \cdot \top \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \langle \forall\ n \ : \ n > 0 : \ n + 1 > 0 \rangle \\
\square &
\end{array}
$$

□

ANEXO — Recorde de testes e exames anteriores o modelo de um sistema eleitoral electrónico de inspiração uni-nominal (i.e., em que se pode votar directamente nos candidatos e não apenas nos respectivos partidos) cujo diagrama relacional se apresenta de seguida,



onde

- $p \ c$ designa o partido a que o candidato c pertence
- $dC \ c$ designa o distrito pelo qual c é candidato
- $dE \ e$ designa o distrito do eleitor e
- $d \ Di \ p$ regista que o partido p concorre às eleições no distrito d
- $e \ V \ p$ indica que o eleitor e votou no partido p
- $e \ V' \ c$ indica que o eleitor e votou directamente no candidato c.

Neste modelo há vários invariantes, a saber:

$$inv_1 \ (V, V') = V : E \leftarrow P \text{ e } V' : E \leftarrow C \text{ são injectivas} \tag{F10}$$

$$inv_2 \ (V, V') = V^{\circ} \cdot V' = \bot \tag{F11}$$

pois um eleitor não pode votar em mais do que um candidato ou partido; e

$$inv_3 \ (V, V') \quad = \quad dE \cdot [V, V'] \subseteq [Di, dC] \tag{F12}$$

pois cada eleitor está registado num distrito e só pode votar em candidatos ou partidos que concorram pelo seu distrito.

No acto eleitoral, as relações p, dC, dE e Di são estáticas, pois os cadernos eleitorais ficam definidos antes das eleições. Sempre que um eleitor vota, corre uma de duas funções:

$$apuraP \ (V, V', e, p) = (V \cup \underline{e} \cdot \underline{p}^{\circ}, V')$$

se tiver optado por votar num partido, ou

$$apuraC \ (V, V', e, c) = (V, V' \cup \underline{e} \cdot \underline{c}^{\circ})$$

se tiver optado por votar num candidato.

---

[2]A sobrejectividade de length está a ser assumida.