Cálculo de Sistemas de Informação
Perfil: MÉTODOS FORMAIS DE PROGRAMAÇÃO

1.º Ano de MEI e MMC, Universidade do Minho
Ano Lectivo de 2022/23

2º Teste — 01 de Junho 2023
14h00–16h00, Sala E1-0.22

---

*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.*

Recomenda-se que os alunos leiam a prova antes de decidirem por que ordem querem responder às questões que são colocadas.

PROVA COM CONSULTA (2 horas)

Questão 1 Recorde o requisito

> *I would like to have an Alloy model for this simple problem: (a) a bicycle always has two wheels, the front and the rear wheel; (b) these wheels can never be the same; (c) no two bicycles have a wheel in common.*

que foi assunto de uma questão no primeiro teste. Verifica-se que basta $[\mathit{frontWheel}, \mathit{rearWheel}]$ ser injectiva para captar as três cláusulas, cf.

$$\mathit{Bicycle} \xrightarrow{\mathit{rearWheel}} \mathit{Wheel} \xleftarrow{\mathit{frontWheel}} \mathit{Bicycle}$$

O Alloy que o chatGPT gerou inclui (em notação *pointwise*) as cláusulas

$$\mathit{frontWheel} \cap \mathit{rearWheel} = \bot \tag{F1}$$

$$\frac{\mathit{rearWheel}}{\mathit{frontWheel}} = \bot \tag{F2}$$

mas (F1) é redundante em face de (F2), como mostra o facto *genérico* seguinte:

$$f \cap g = \bot \Leftarrow \frac{g}{f} = \bot \tag{F3}$$

Sabendo que a lei seguinte se verifica,

$$S \cdot R \cap Q = S \cdot (R \cap S^\circ \cdot Q) \quad \Leftarrow \quad S \text{ is simple} \tag{F4}$$

complete a seguinte dedução de (F3):

$$\begin{array}{ll}
& f \cap g = \bot \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \ldots \\
\equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& id \cap \dfrac{g}{f} \subseteq \bot \\
\Leftarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \dfrac{g}{f} = \bot
\end{array}$$

RESOLUÇÃO: tem-se:

$$
\begin{array}{cl}
& f \cap g = \bot \\
\equiv & \qquad \{ \text{ Fazendo } S, R, Q := f, id, g \text{ em (F4) uma vez que } f \text{ é simples } \} \\
& f \cdot (id \cap f^\circ \cdot g) = \bot \\
\equiv & \qquad \{ \ X = \bot \ \Leftrightarrow \ X \ \subseteq \ \bot\text{; shunting de } f\text{; } X \cdot \bot = \bot \ \} \\
& id \cap \dfrac{g}{f} \ \subseteq \ \bot \\
\Leftarrow & \qquad \{ \text{ "subida do lado inferior" } \} \\
& \dfrac{g}{f} = \bot
\end{array}
$$

□

Questão 2 Sempre que escrevemos $a \neq b$ estamos a usar a relação binária

$$A \xleftarrow{(\neq)} A \quad = \quad id \Rightarrow \bot \tag{F5}$$

que está sempre bem definida uma vez que todo o tipo A está equipado com a relação identidade $A \xleftarrow{id} A$. Mostre, usando cálculo relacional, que a relação $(\neq)$ é simétrica e irreflexiva.

RESOLUÇÃO: Simétrica (acrescentar justificações):

$$
\begin{array}{cl}
& (id \Rightarrow \bot)^\circ \ \subseteq \ (id \Rightarrow \bot) \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (id \Rightarrow \bot)^\circ \cap id \ \subseteq \ \bot \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (id \Rightarrow \bot) \cap id \ \subseteq \ \bot \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& id \Rightarrow \bot \ \subseteq \ id \Rightarrow \bot
\end{array}
$$

□

Irreflexiva:

$$
\begin{array}{cl}
& (\neq) \text{ irreflexiva} \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (\neq) \cap id \ \subseteq \ \bot \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (\neq) \ \subseteq \ id \Rightarrow \bot \\
\equiv & \qquad \{ \text{ pois } (\neq) = id \Rightarrow \bot \ \} \\
& \mathit{true}
\end{array}
$$

□

Questão 3 Recorde que f se diz "ponto-a-ponto" menor que g, escrevendo-se $f \stackrel{\cdot}{\leqslant} g$, se se verificar

$$\langle \forall\ a\ ::\ f\ a \leqslant g\ a \rangle$$

isto é

$$f \subseteq (\leqslant) \cdot g \tag{F6}$$

Prove a equivalência:

$$f \stackrel{\cdot}{\leqslant} g \Leftrightarrow g \stackrel{\cdot}{\geqslant} f \tag{F7}$$

RESOLUÇÃO: Tem-se:

$$\begin{array}{ll}
& f \stackrel{\cdot}{\leqslant} g \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& f \subseteq (\leqslant) \cdot g \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& g^{\circ} \subseteq f^{\circ} \cdot (\leqslant) \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& g \subseteq (\geqslant) \cdot f \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& g \stackrel{\cdot}{\geqslant} f
\end{array}$$

□

Questão 4 Recorde a especificação da função take (Haskell) que foi abordada nas aulas,

$$\underbrace{\mathsf{length}\ ys \leqslant n \wedge ys \sqsubseteq xs}_{easy} \;\Leftrightarrow\; \underbrace{ys \sqsubseteq \mathsf{take}\ n\ xs}_{hard} \tag{F8}$$

onde $x \sqsubseteq y$ é a relação x é prefixo de y. Mostre que (F8) se pode escrever sob a forma da seguinte igualdade de relações, em notação *pointfree*,

$$\langle \mathsf{length}, id \rangle^{\circ} \cdot ((\leqslant) \times (\sqsubseteq)) = (\sqsubseteq) \cdot \widehat{\mathsf{take}} \tag{F9}$$

onde, como sabe, $\widehat{f}\ (a, b) = f\ a\ b$. (**Sugestão**: introduza variáveis e simplifique.)

RESOLUÇÃO: Tem-se (adicionar justificações):

$$\begin{array}{ll}
& \langle \mathsf{length}, id \rangle^{\circ} \cdot ((\leqslant) \times (\sqsubseteq)) = (\sqsubseteq) \cdot \widehat{\mathsf{take}} \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& ys\ (\langle \mathsf{length}, id \rangle^{\circ} \cdot ((\leqslant) \times (\sqsubseteq)))\ (n, xs) \Leftrightarrow ys\ ((\sqsubseteq) \cdot \widehat{\mathsf{take}})\ (n, xs) \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& (\mathsf{length}\ ys, ys)\ ((\leqslant) \times (\sqsubseteq))\ (n, xs) \Leftrightarrow ys \sqsubseteq \widehat{\mathsf{take}}\ (n, xs) \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \left\{ \begin{array}{l} \mathsf{length}\ ys \leqslant n \\ ys \sqsubseteq xs \end{array} \right. \Leftrightarrow ys \sqsubseteq \mathsf{take}\ n\ xs
\end{array}$$

□

Questão 5 Considere-se um sistema de informação bancário básico inicialmente modelado por uma relação *simples* e *injectiva*

$$Nr \xrightarrow{S} Account$$

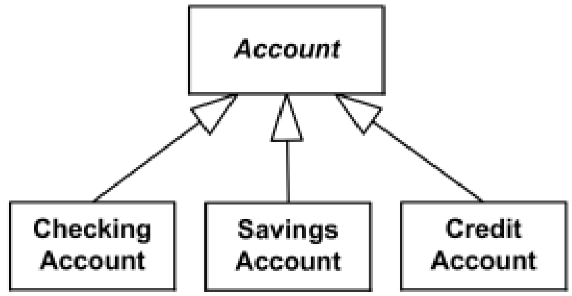
que associa a números de conta (Nr) a informação respectiva ($Account$).

Surgindo mais tarde a necessidade de especializar contas nas três sub-classes que se mostram na figura, definiu-se

$$S' = \langle S, R \rangle$$

que acrescenta a S uma relação R (também simples) que categoriza contas:

$$Nr \xrightarrow{R} Checking + Savings + Credit$$



A pergunta é: será a nova versão S' do sistema uma relação injectiva quando R o não é? Justifique a sua resposta.

RESOLUÇÃO: Pela (5.236) é o facto é imediato, pois os "splits" aumentam sempre a injectividade. Por extenso:

$$
\begin{array}{cl}
 & S' \text{ injectiva} \\
\equiv & \qquad \{ \; S' = \langle S, R \rangle ; \text{(5.36)} \; \} \\
 & \ker \langle S, R \rangle \; \subseteq \; id \\
\equiv & \qquad \{ \; \text{(5.111)} \; \} \\
 & \ker S \cap \ker R \; \subseteq \; id \\
\equiv & \qquad \{ \; S \text{ é injectiva (5.36)} \; \} \\
 & id \cap \ker R \; \subseteq \; id \\
\equiv & \qquad \{ \; \text{cancelamento-}\cap \; \} \\
 & \text{TRUE}
\end{array}
$$

Logo S' é injectiva mesmo quando R o não é. $\square$

Questão 6 Um modelo habitual para guardar informação é sob a forma de pares chave (Key) / valor ($Data$) — isto é, sob a forma de relações simples $S : Key \to Data$. Em memórias de estado sólido, vulgarmente designadas por memórias *flash*, esse tipo de informação toma a forma

$$Addr \times Key \to Data + 1 \tag{F10}$$

onde $Addr$ é o espaço de endereçamento disponível e $Data + 1$ regista informação activa *ou* apagada.

Evita-se apagar ou (re)escrever nas mesmas células pois isso acaba por danificá-las. Em vez disso, vão-se usando endereços seguintes livres para registar a informação actualizada.

No exemplo da figura ao lado, começou por guardar-se no endereço 1 informação associada a *KEY4*, que mais tarde se apagou (endereço 9). E a informação da chave *KEY1*, inicialmente guardada no endereço 3, foi alterada no endereço 7, por exemplo.

Flash Store

1	KEY4	DATA
2	KEY2	DATA
3	KEY1	DATA
4	KEY1a	DATA
5	KEY3	DATA
6	KEY3	DATA
7	KEY1	DATA
8	KEY1b	DATA
9	KEY4	DEL

Para se extrair de uma memória flash $M : Addr \times Key \rightarrow Data + 1$ a relação $S : Key \rightarrow Data$ contendo a informação mais recente, alguém propôs

$$S = i_1^\circ \cdot M \cdot \pi_2^\circ \tag{F11}$$

que é um "caminho" do diagrama:

$$\begin{tikzcd} Addr & Addr \times Key \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] \arrow[d, "M"'] & Key \\ Data \arrow[r, "i_1"'] & Data + 1 & 1 \arrow[l, "i_2"] \end{tikzcd}$$

Concorda com a solução proposta? Justifique a sua resposta introduzindo variáveis e comentando o resultado.

RESOLUÇÃO: *Pointwise*, como sugerido:

$$\begin{array}{cl} & d\ S\ k \\ \equiv & \quad \{ \text{ justificar... } \} \\ & (i_1\ d)\ (M \cdot \pi_2^\circ)\ k \\ \equiv & \quad \{ \text{ justificar... } \} \\ & \langle \exists\ a\ ::\ (i_1\ d)\ M\ (a, k) \rangle \end{array}$$

Vê-se assim que S relaciona cada chave k com todos os valores d que tem (ou teve), correspondentes a endereços $a \in Addr$ que perde via π_2. Ora, para se saber quais os ds mais recentes é preciso aceder aos endereços. Logo, S não tem informação suficiente para selecionar o passado mais recente de cada chave (Key). $\square$

Questão 7 Recorde a projecção $snd : (a, b) \rightarrow b$ e, por *currying*, $\overline{snd} : t$ onde $t = a \rightarrow (b \rightarrow b)$. Mostre que o teorema grátis de $\overline{snd}$ é

$$y\ R\ x \Rightarrow \overline{snd}\ y \cdot S \subseteq S \cdot \overline{snd}\ x \tag{F12}$$

(para todo o R, S, x e y devidamente tipados) e instancie-o por forma a obter o corolário:

$$\overline{snd} \cdot r = \overline{snd} \tag{F13}$$

Que conclui sobre $\overline{snd}$?

RESOLUÇÃO: Tem-se (completar com justificações):

$$\begin{array}{cl} & \overline{snd}\ ((S \leftarrow S) \leftarrow R)\ \overline{snd} \\ \equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\ & \overline{snd} \cdot R \subseteq (S \leftarrow S) \cdot \overline{snd} \\ \equiv & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \end{array}$$

$$R \subseteq \overline{snd}^{\circ} \cdot (S \leftarrow S) \cdot \overline{snd}$$

$$\equiv \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \}$$

$$y \; R \; x \Rightarrow \overline{snd} \; y \cdot S \subseteq S \cdot \overline{snd} \; x$$

Fazendo $S := id$ e $R := r$ (completar com justificações):

$$\overline{snd} \; (r \; x) \cdot id = id \cdot \overline{snd} \; x$$

$$\equiv \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \}$$

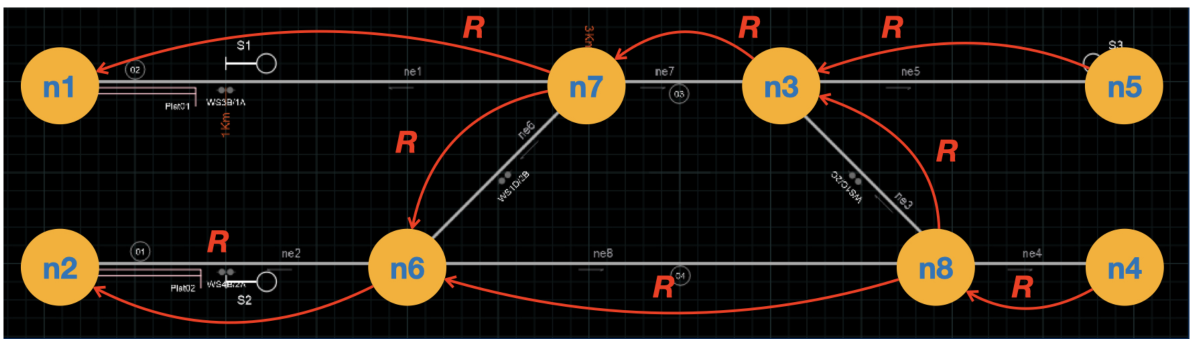
$$\overline{snd} \; (r \; x) = \overline{snd} \; x$$

$$\equiv \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \}$$

$$\overline{snd} \cdot r = \overline{snd}$$

Conclui-se quw $\overline{snd}$ é uma função constante. $\square$

Questão 8 Recorde a modelação relacional da pequena rede ferroviária que foi abordada nas aulas:



Há necessidade de mais invariantes no modelo. Por exemplo,

$$enoughSwitches \; (S, R, P) = id \cap R^{\circ} \cdot (\neq) \cdot R \;\subseteq\; S^{\circ} \cdot S \tag{F14}$$

é necessário para garantir que, onde houver bifurcações, tem de haver agulhas. (É oposto ao dado nas aulas.)

Suponha que R está em construção usando um CAD que oferece uma operação que permite acrescentar novos elementos X à rede R:

$$addNElem \; X \; (S, R, P) = (S, R \cup X, P) \tag{F15}$$

Complete o cálculo seguinte da précondição mais fraca (WP) que garante que $addNElem$ não viola (F14):

$$enoughSwitches \; (addNElem \; X \; (S, R, P))$$

$$\equiv \quad \{ \text{ (F15) } \}$$

$$enoughSwitches \; (S, R \cup X, P)$$

$$\equiv \quad \{ \text{ (F14) } \}$$

$$id \cap (R^{\circ} \cup X^{\circ}) \cdot (\neq) \cdot (R \cup X) \;\subseteq\; S^{\circ} \cdot S$$

$$\equiv \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \}$$

$$\vdots$$

$$\equiv \quad \{ \quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \quad \}$$

$$enoughSwitches \; (S, R, P) \wedge \underbrace{\dots\dots\dots\dots}_{WP}$$

RESOLUÇÃO: Propõe-se:[1]

$$
\begin{array}{ll}
& enoughSwitches\ (addNElem\ X\ (S,R,P)) \\
\equiv & \qquad \{\ \text{(F15)}\ \} \\
& enoughSwitches\ (S, R \cup X, P) \\
\equiv & \qquad \{\ \text{(F14)}\ \} \\
& id \cap (R^{\circ} \cup X^{\circ}) \cdot (\neq) \cdot (R \cup X)\ \subseteq\ S^{\circ} \cdot S \\
\equiv & \qquad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& \left\{ \begin{array}{l} \left\{ \begin{array}{l} id \cap R^{\circ} \cdot (\neq) \cdot R\ \subseteq\ S^{\circ} \cdot S \\ id \cap R^{\circ} \cdot (\neq) \cdot X\ \subseteq\ S^{\circ} \cdot S \end{array} \right. \\ \left\{ \begin{array}{l} id \cap X^{\circ} \cdot (\neq) \cdot R\ \subseteq\ S^{\circ} \cdot S \\ id \cap X^{\circ} \cdot (\neq) \cdot X\ \subseteq\ S^{\circ} \cdot S \end{array} \right. \end{array} \right. \\
\equiv & \qquad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& \left\{ \begin{array}{l} enoughSwitches\ (S,R,P) \\ id \cap R^{\circ} \cdot (\neq) \cdot X\ \subseteq\ S^{\circ} \cdot S \\ id \cap X^{\circ} \cdot (\neq) \cdot X\ \subseteq\ S^{\circ} \cdot S \end{array} \right. \\
\equiv & \qquad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& enoughSwitches\ (S,R,P) \wedge \underbrace{id \cap ((R \cup X)^{\circ} \cdot (\neq) \cdot X)\ \subseteq\ S^{\circ} \cdot S\ (WP)}_{.}
\end{array}
$$

$\square$

[1] Acrescentar as justificações que faltam.