Cálculo de Sistemas de Informação
Perfil: MÉTODOS FORMAIS DE PROGRAMAÇÃO

1.º Ano de MEI e MMC, Universidade do Minho
Ano Lectivo de 2021/22

Exame de recurso — 25 de Junho de 2022
10h00–12h00, Sala E7-1.09

---

*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.*

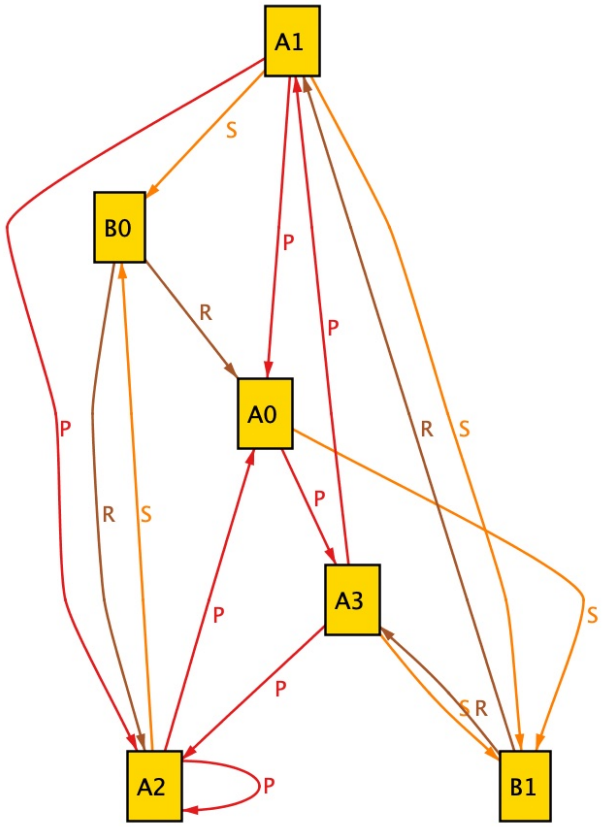
Recomenda-se que os alunos leiam a prova antes de decidirem por que ordem querem responder às questões que são colocadas.

PROVA COM CONSULTA (2 horas)

Questão 1 Sejam dados os tipos de dados A (com quatro elementos) e B (com dois elementos) e as relações $A \xrightarrow{P} A$, $A \xrightarrow{S} B$ e $A \xleftarrow{R} B$ que constam do diagrama Alloy que se mostra ao lado. Indique quais das relações do diagrama são:

1. injectivas
2. difuncionais

Sugestão: apoie a sua resolução na representação matricial das relações que se mostram no diagrama.



RESOLUÇÃO: R é difuncional e injectiva (TPC: justificar). □

Questão 2 Considere a seguinte definição de uma relação $A \xleftarrow{R} A^*$,

$$R \cdot \mathsf{in} = [\bot, \pi_1 \cup R \cdot \pi_2]$$

onde

$$\mathsf{in} = [\mathsf{nil}, \mathsf{cons}] \quad \text{(F1)}$$
$$\mathsf{nil}\ \_ = [\,] \quad \text{(F2)}$$
$$\mathsf{cons}\ (h, t) = h : t \quad \text{(F3)}$$

Baseie-se nas leis dos coprodutos para derivar (formalmente) a definição *pointwise* de R. Com base nesta, diga por palavras suas qual o significado de $a\ R\ x$.

RESOLUÇÃO: Tem-se (justificar):

$$
\begin{array}{ll}
 & R \cdot \mathsf{in} = [\bot\,, \pi_1 \cup R \cdot \pi_2] \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} R \cdot \mathsf{nil} = \bot \\ R \cdot \mathsf{cons} = \pi_1 \cup R \cdot \pi_2 \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} y\ R\ [\,] = \mathrm{FALSE} \\ y\ R\ (h:t) \ \Leftrightarrow\ y = \pi_1\ (h,t) \vee y\ R\ (\pi_2\ (h,t)) \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} y\ R\ [\,] = \mathrm{FALSE} \\ y\ R\ (h:t) \ \Leftrightarrow\ y = h \vee y\ R\ t \end{array} \right.
\end{array}
$$

R é a relação de pertença em listas: $a\ R\ x$ diz se a ocorre em alguma posição da lista x. □

Questão 3 Tendo num raciocínio relacional aparecido a expressão $((R - S) \cup S) - S$, alguém disse: *isso é igual a* R. Mas tal não é verdade, em geral — o que se verifica de facto é:

$$
((R - S) \cup S) - S \quad = \quad R - S \tag{F4}
$$

Como justifica (F4) sem recorrer à lei dos semi-inversos (5.146) dos apontamentos?

RESOLUÇÃO: Preencher justificações:

$$
\begin{array}{ll}
 & ((R - S) \cup S) - S \subseteq X \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & (R - S) \cup S \subseteq X \cup S \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} R - S \subseteq X \cup S \\ S \subseteq X \cup S \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & R \subseteq X \cup S \cup S \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & R - S \subseteq X \\
\square &
\end{array}
$$

□

Questão 4 Suponha que está a trabalhar numa empresa cujo sistema de informação segue o modelo **key-value-pair** e onde, para tornar possível a re-utilização de uma bilioteca *open-source*, é necessário juntar duas relações $K \xrightarrow{R} V$ e $K \xrightarrow{S} V$ numa só.

Construir $Q = R \cup S$ não é opção, pois R e S podem ter chaves em comum e haver confusão. Tendo-lhe sido pedido a si para tratar do problema, eis a sua sugestão: juntar as relações após prévia transformação das suas chaves por duas funções f e g, isto é, construir:

$$Q = R \cdot f^{\circ} \cup S \cdot g^{\circ}$$

Naturalmente, a equipa de implementação pergunta-lhe: que funções f e g são essas? Eis a sua resposta: *podem escolher as que quiserem desde que*

- *ambas sejam injectivas*
- *não existam duas chaves k e k' tal que $f\ k = g\ k'$.*

Tendo a sua sugestão funcionado bem, a chefia da sua equipa pediu-lhe para explicar a solução proposta. Escreva aqui os cálculos relacionais com que a justificou, tendo em conta que o modelo *key-value-pair* só admite relações *simples*.

RESOLUÇÃO:

$$Q = R \cdot f^{\circ} \cup S \cdot g^{\circ} \text{ simples}$$

$\equiv \quad \{$ exercício 5.15 $\}$

$$\begin{cases} \text{img } (R \cdot f^{\circ}) \subseteq id \\ \text{img } (S \cdot g^{\circ}) \subseteq id \\ R \cdot f^{\circ} \cdot (S \cdot g^{\circ})^{\circ} \subseteq id \end{cases}$$

$\equiv \quad \{$ conversos etc $\}$

$$\begin{cases} R \cdot f^{\circ} \cdot f \cdot R^{\circ} \subseteq id \\ S \cdot g^{\circ} \cdot g \cdot S^{\circ} \subseteq id \\ R \cdot f^{\circ} \cdot g \cdot S^{\circ} \subseteq id \end{cases}$$

$\equiv \quad \{$ a sua proposta foi f e g injectivas $\}$

$$\begin{cases} R \cdot R^{\circ} \subseteq id \\ S \cdot S^{\circ} \subseteq id \\ R \cdot f^{\circ} \cdot g \cdot S^{\circ} \subseteq id \end{cases}$$

$\equiv \quad \{$ R e S são simples à partida $\}$

$$R \cdot f^{\circ} \cdot g \cdot S^{\circ} \subseteq id$$

$\Leftarrow \quad \{$ $\bot$ é absorvente da composição $\}$

$$f^{\circ} \cdot g = \bot$$

$\equiv \quad \{$ o seu último requisito (guardanapo etc) $\}$

$$\neg \langle \exists\ k, k' :: f\ k = g\ k' \rangle$$

□

□

Questão 5 A sobreposição de relações é uma operação idempotente: $(R \dagger S) \dagger S = R \dagger S$. O cálculo relacional que se segue pretende provar essa afirmação:

$$(R \dagger S) \dagger S$$

$\equiv \quad \{$ .... $\}$

$$S \cup (R \dagger S) \cap \bot / S^{\circ}$$

$\equiv \quad \{$ .... $\}$

$$S \cup (S \cup R \cap \bot / S^{\circ}) \cap \bot / S^{\circ}$$

$\equiv \quad \{$ .... $\}$

$$S \cup S \cap \perp / S^\circ \cup R \cap \perp / S^\circ$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$S \cup R \cap \perp / S^\circ$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$R \dagger S$$

Valide com justificações apropriadas os seus passos. Na eventualidade de um passo injustificável, indique por que razão acha que esse passo é inválido.

RESOLUÇÃO:

$$(R \dagger S) \dagger S$$
$$\equiv \quad \{ \text{ definição de } \cdot \dagger \cdot \}$$
$$S \cup (R \dagger S) \cap \perp / S^\circ$$
$$\equiv \quad \{ \text{ definição de } \cdot \dagger \cdot \}$$
$$S \cup ((S \cup R \cap \perp / S^\circ) \cap \perp / S^\circ)$$
$$\equiv \quad \{ \text{ distributividade de } \cdot \cap \cdot \text{ por } \cdot \cup \cdot; \_ \cap X \text{ é idempotente } \}$$
$$S \cup (S \cap \perp / S^\circ \cup R \cap \perp / S^\circ)$$
$$\equiv \quad \{ \; S \cup S \cap \perp / S^\circ = S \; \}$$
$$S \cup R \cap \perp / S^\circ$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$R \dagger S$$

$\square$

$\square$

Questão 6 Considere-se um programa imperativo representado pela relação $S \xleftarrow{P} S$ que indica como o programa P modifica os valores das variáveis que estão guardadas no estado S do programa. Um triplo de Hoare,

$$\{p\} \; P \; \{q\}$$

é uma asserção sobre P que nos diz que, sempre que P arranca num estado que satisfaz a (pré)condição p, se terminar (pois pode não o fazer) deixa o estado a satisfazer a (pós)condição q. Formalmente,

$$\{p\} \; P \; \{q\} \;\Leftrightarrow\; P \cdot \Phi_p \subseteq \Phi_q \cdot \top \qquad \text{(F5)}$$

onde $\Phi_p = id \cap \frac{p}{true}$ é a representação de p sob a forma de uma relação coreflexiva.

Transforme a inclusão relacional de (F5) por forma a introduzir um operador de divisão (à sua escolha) e depois introduza-lhe variáveis. Confirma o significado de $\{p\} \; P \; \{q\}$ que acima se descreveu informalmente?

RESOLUÇÃO: Tem-se:

$$\{p\} \; P \; \{q\}$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$P \cdot \Phi_p \subseteq \Phi_q \cdot \top$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$\Phi_p \subseteq P \setminus (\Phi_q \cdot \top)$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$\langle \forall\, s \;:\; p\; s :\; s\; (P \setminus (\Phi_q \cdot \top))\; s \rangle$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$\langle \forall\, s \;:\; p\; s :\; \langle \forall\, s' \;:\; s'\; P\; s :\; s'\; ((\Phi_q \cdot \top))\; s \rangle \rangle$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$\langle \forall\, s \;:\; p\; s :\; \langle \forall\, s' \;:\; s'\; P\; s :\; q\; s' \rangle \rangle$$
$\square$

Corresponde ao que se descreveu informalmente.
$\square$

Questão 7 Recorde das aulas a GC que *especifica* a operação de **divisão inteira** em $\mathbb{N}_0$,

$$z \times y \leqslant x \;\Leftrightarrow\; z \leqslant x \div y \tag{F6}$$

onde se assume $y > 0$. A função seguinte (em Haskell) implementa o algoritmo bem conhecido que calcula a divisão inteira $x \div y$ por contagem do número de vezes que y "cabe" em x:

$x \div y =$
  if $x \geqslant y$
  then $1 + (x \ominus y) \div y$
  else 0

Nesta definição, $x \ominus y$ é a subtração truncada em $\mathbb{N}_0$ que, em testes anteriores desta disciplina, foi especificada por outra GC, recordar:

$$a \ominus b \leqslant x \;\Leftrightarrow\; a \leqslant x + b \tag{F7}$$

Assuma, sem as ter que provar, as seguintes propriedades dessa operação:

$$a \times (b \ominus 1) = (a \times b) \ominus a \tag{F8}$$
$$(a \ominus b) + b = a \text{ desde que } a \geqslant b \tag{F9}$$

Complete o cálculo que se segue do ramo recursivo do algoritmo dado, em que $x \geqslant y$ está garantido:

$$z \leqslant x \div y$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$z \times y \leqslant (x \ominus y) + y$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$(z \times y) \ominus y \leqslant x \ominus y$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$(z \ominus 1) \times y \leqslant x \ominus y$$
$$\equiv \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$
$$z \leqslant 1 + (x \ominus y) \div y$$
$$:: \quad \{ \text{ Igualdade indirecta sobre } \mathbb{N}_0 \xleftarrow{\leqslant} \mathbb{N}_0 \}$$
$$x \div y = 1 + (x \ominus y) \div y$$

RESOLUÇÃO:

$$
\begin{array}{ll}
& z \leqslant x \div y \\
\equiv & \{ \quad \dots \quad \} \\
& z \times y \leqslant x \\
\equiv & \{ \quad \dots \quad \} \\
& z \times y \leqslant x + (y \ominus y) \\
\equiv & \{ \quad \dots \quad \} \\
& z \times y \leqslant (x \ominus y) + y \\
\equiv & \{ \quad \dots \quad \} \\
& (z \times y) \ominus y \leqslant x \ominus y \\
\equiv & \{ \quad \dots \quad \} \\
& (z \ominus 1) \times y \leqslant x \ominus y \\
\equiv & \{ \quad \dots \quad \} \\
& z \ominus 1 \leqslant (x \ominus y) \div y \\
\equiv & \{ \quad \dots \quad \} \\
& z \leqslant 1 + (x \ominus y) \div y \\
:: & \{ \quad \dots \quad \} \\
& x \div y = 1 + (x \ominus y) \div y
\end{array}
$$

□

Questão 8 Considere uma função

$$hist :: Eq\ a \Rightarrow [a] \rightarrow [(a, \mathbb{Z})]$$

que calcula o histograma de uma sequência finita, por exemplo,

$$hist\ \texttt{"Monosialotetraesosilgangliosideo"} =$$
$$[(\texttt{'M'}, 1), (\texttt{'a'}, 3), (\texttt{'d'}, 1), (\texttt{'e'}, 3), (\texttt{'g'}, 2), (\texttt{'i'}, 4), (\texttt{'l'}, 3), (\texttt{'n'}, 2), (\texttt{'o'}, 6), (\texttt{'r'}, 1), (\texttt{'s'}, 4), (\texttt{'t'}, 2)]$$

Calcule o teorema grátis da função $hist$ e instancie-o para funções.

NB: a cláusula $Eq\ a$ é uma forma abreviada de exigir um predicado que teste quando dois elementos são iguais. Quer dizer, o tipo de $hist$ acaba por ser:

$$hist :: (a \rightarrow a \rightarrow \mathbb{B}) \rightarrow [a] \rightarrow [(a, \mathbb{Z})]$$

RESOLUÇÃO: Tem-se:

$$
\begin{array}{ll}
& hist\ R_{(a \rightarrow a \rightarrow \mathbb{B}) \rightarrow [a] \rightarrow [(a,\mathbb{Z})]}\ hist \\
\equiv & \{ \quad \dots \quad \} \\
& hist \cdot (id \leftarrow R \leftarrow R) \subseteq ((R \times id)^* \leftarrow R^*) \cdot hist \\
\equiv & \{ \quad \dots \quad \}
\end{array}
$$

$$
\begin{array}{ll}
& p\ ((id \leftarrow R) \leftarrow R)\ q\ \Rightarrow\ (hist\ p)\ ((R \times id)^{*} \leftarrow R^{*})\ (hist\ q) \\
\equiv & \quad \{\ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& p \cdot R \subseteq (id \leftarrow R) \cdot q\ \Rightarrow\ hist\ p \cdot R^{*} \subseteq (R \times id)^{*} \cdot (hist\ q) \\
\equiv & \quad \{\ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (b\ R\ a\ \Rightarrow\ p\ b\ (id \leftarrow R)\ (q\ a))\ \Rightarrow\ hist\ p \cdot R^{*} \subseteq (R \times id)^{*} \cdot (hist\ q) \\
\equiv & \quad \{\ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (b\ R\ a\ \Rightarrow\ p\ b \cdot R \subseteq q\ a)\ \Rightarrow\ hist\ p \cdot R^{*} \subseteq (R \times id)^{*} \cdot (hist\ q) \\
\equiv & \quad \{\ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (\left\{ \begin{array}{l} b\ R\ a \\ c\ R\ d \end{array} \right.\ \Rightarrow\ p\ b\ c = q\ a\ d)\ \Rightarrow\ hist\ p \cdot R^{*} \subseteq (R \times id)^{*} \cdot (hist\ q)
\end{array}
$$

Funções ($R := r$):

$$
p\ (r\ a)\ (r\ d) = q\ a\ d\ \Rightarrow\ hist\ p \cdot \mathsf{map}\ r = (r \times id) \cdot hist\ q
$$

□
