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

2º Teste — 9 de Junho de 2022
9h00–11h00, 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.*

PROVA COM CONSULTA (2 horas)

Questão 1 Mostre que tanto a injectividade como a simplicidade de uma relação R são preservadas por $R \upharpoonright S$, qualquer que seja a relação S.

RESOLUÇÃO: Por

$$R \upharpoonright S \;=\; R \cap S/R^\circ$$

tem-se $R \upharpoonright S \subseteq R$. Como *menor que simples é simples*,[1] está provado. A mesma coisa para a injectividade. □

Questão 2 Verifique se a seguinte afirmação é válida:

$R \dagger S$ é simples sempre que R e S o são e S é também injectiva.

RESOLUÇÃO: *Calculemus* (completar justificações):

$R \dagger S$ é simples
$\equiv$ { ..... }
$S \cup R \cap \bot \,/\, S^\circ$ é simples
$\equiv$ { ..... }
S é simples, $R \cap \bot \,/\, S^\circ$ é simples e $(R \cap \bot \,/\, S^\circ) \cdot S^\circ \subseteq id$
$\Leftarrow$ { ..... }
S é simples, R é simples e $(R \cap \bot \,/\, S^\circ) \cdot S^\circ \subseteq id$
$\equiv$ { S e R assumidas simples; S° simples, logo distribui por.... }
$R \cdot S^\circ \cap (\bot \,/\, S^\circ) \cdot S^\circ \subseteq id$
$\Leftarrow$ { ..... }
$(\bot \,/\, S^\circ) \cdot S^\circ \subseteq \bot$
$\equiv$ { ..... }
$\bot \,/\, S^\circ \subseteq \bot \,/\, S^\circ$

[1] Cf. 5.12 - Rules of Thumb.

□

Questão 3 Nas aulas foi abordado o *relator* (= functor relacional) $Maybe$ de forma abstracta, fazendo-se $Maybe\ X = 1 + X$. Ora, o que acontece é o isomorfismo:

$$Maybe\ X \underset{\mathsf{in}=[\underline{\mathsf{Nothing}},\mathsf{Just}]}{\overset{\mathsf{out}=\mathsf{in}^\circ}{\cong}} 1 + X \tag{F1}$$

Derive a definição relacional *pointwise* de $y\ (Maybe\ R)\ x$,

$$\begin{array}{ccc} A & \cdots\cdots & Maybe\ A \\ {\scriptstyle R}\downarrow & & \downarrow{\scriptstyle Maybe\ R} \\ B & \cdots\cdots & Maybe\ B \end{array}$$

tendo em conta (F1).

RESOLUÇÃO: Tem-se (completar justificações):

$$\begin{array}{ll} & Maybe\ R = \mathsf{in} \cdot (id + R) \cdot \mathsf{in}^\circ \\ \equiv & \quad \{\ \ldots\ \} \\ & Maybe\ R \cdot \mathsf{in} = \mathsf{in} \cdot (id + R) \\ \equiv & \quad \{\ \ldots\ \} \\ & \left\{ \begin{array}{l} Maybe\ R \cdot nothing = nothing \\ Maybe\ R \cdot \mathsf{Just} = \mathsf{Just} \cdot R \end{array} \right. \\ \equiv & \quad \{\ \ldots\ \} \\ & \left\{ \begin{array}{l} y\ (Maybe\ R)\ \mathsf{Nothing} \Leftrightarrow y = \mathsf{Nothing} \\ y\ (Maybe\ R)\ (\mathsf{Just}\ a) = \langle \exists\ b\ :\ y = \mathsf{Just}\ b :\ b\ R\ a \rangle \end{array} \right. \end{array}$$

□

Questão 4 Em `hackage.haskell.org` lê-se, na biblioteca `Data.List`, o texto (adaptado para listas):

- $\mathsf{or} :: [\mathbb{B}] \to \mathbb{B}$ — or *returns the disjunction of a container of Bools. (...)*
- $any :: (a \to \mathbb{B}) \to [a] \to \mathbb{B}$ — *Determines whether any element of the structure satisfies the predicate.*

Questões:

1. Valerá a pena calcular o teorema grátis de or? Justifique a sua resposta.
2. Derive o teorema grátis de any e apresente a sua instância para funções.

RESOLUÇÃO:

- Não, pois não é paramétrico, dando como resultado or = or.
- Tem-se $t = \mathbb{B} \leftarrow [a] \leftarrow (\mathbb{B} \leftarrow a)$, logo $R_t = id \leftarrow R^* \leftarrow (id \leftarrow R)$. Então:

$$
\begin{array}{ll}
& any\ R_t\ any \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& any\ ((id \leftarrow R^*) \leftarrow (id \leftarrow R))\ any \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& any \cdot (id \leftarrow R)\ \subseteq\ (id \leftarrow R^*) \cdot any \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& p\ (id \leftarrow R)\ q \Rightarrow (any\ p)\ (id \leftarrow R^*)\ (any\ q) \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& p \cdot R\ \subseteq\ q \Rightarrow any\ p \cdot R^* \subseteq any\ q \\
\square &
\end{array}
$$

Funções: para $R := f$ tem-se $q = p \cdot f$, obtendo-se o corolário

$$any\ p \cdot \mathsf{map}\ f = any\ (p \cdot f).$$

□

Questão 5 Recorda-se, do 1º teste:

Nos inteiros ($\mathbb{Z}$), a operação de subtracção é um isomorfismo, $(\_ - b)^\circ = (\_ + b)$, isto é,

$$a - b = x \ \Leftrightarrow\ a = x + b$$

Mas, restrita aos naturais ($\mathbb{N}_0$) deixa de o ser. O que se verifica em $\mathbb{N}_0$ é a conexão de Galois

$$(\_ \ominus b)^\circ \cdot (\leqslant) = (\leqslant) \cdot (\_ + b)$$

que se expande para a equivalência

$$a \ominus b \leqslant x \ \Leftrightarrow\ a \leqslant x + b \qquad \text{(F2)}$$

que pode ser tomada como a ***especificação formal*** *de $a \ominus b$ em $\mathbb{N}_0$.*

Mostre, usando (F2) e a igualdade indirecta sobre $(\leqslant)$ em $\mathbb{N}_0$, que qualquer implementação (correcta!) de $a \ominus b$ deverá observar a propriedade:

$$((n + 1) \times a) \ominus a = a \times n \qquad \text{(F3)}$$

RESOLUÇÃO: Tem-se (completar justificações):

$$
\begin{array}{ll}
& ((n + 1) \times a) \ominus a \leqslant x \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& n \times a + a \leqslant x + a \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& n \times a \leqslant x \\
:: & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& ((n + 1) \times a) \ominus a = a \times n
\end{array}
$$

□

Questão 6 Recorda-se, do 1º teste:

> *Em linguagens como Haskell as listas (sequências finitas) podem ser manipuladas como estruturas recursivas* $A^* \cong 1 + A \times A^*$ *ou como estruturas indexadas, isto é relações simples em* $\mathbb{N}_0 \to A$ *que associam elementos a posições na lista, por exemplo* $[a, b, z, a] \,!!\, 2 = z$ *etc.*
>
> *Especificam-se de seguida algumas operações habituais sobre uma lista* $\mathbb{N}_0 \xrightarrow{L} A$ *encarada como estrutura indexada,*
>
> $$a : L = [\underline{a}, L] \cdot \mathsf{in}^\circ \tag{F4}$$
> $$\mathsf{tail}\ L = L \cdot \mathsf{succ} \tag{F5}$$
> $$\mathsf{head}\ L = L \cdot \mathsf{zero} \tag{F6}$$
>
> *onde* $a \in A$ *e* $\mathsf{in} = [\mathsf{zero}, \mathsf{succ}]$ *é o* isomorfismo *de construção dos números naturais (normalmente conhecido por "álgebra de Peano"), para* $\mathsf{zero}\ x = 0$ *e* $\mathsf{succ}\ n = n + 1$. *Demonstre a propriedade*

A forma como são construídas as listas sugere o seguinte invariante:

$$inv\ L = \mathsf{tail}\ L \subseteq \top \cdot L \tag{F7}$$

- Diga por palavras suas qual é o significado de $inv\ L$.
- Mostre que a operação $a : L$ preserva esse invariante, isto é, que $inv\ (a : L) \Leftrightarrow inv\ L$.

RESOLUÇÃO: Primeira parte: por (F5) tem-se

$$L \cdot \mathsf{succ} \subseteq \top \cdot L$$

isto é, para todo o a e i: $a\ L\ (i+1) \Rightarrow \langle \exists\ a' :: a'\ L\ i \rangle$. O que quer dizer que os índices são todos contíguos.[2]

Segunda parte (completar as justificações):

$$\begin{array}{ll}
 & inv\ (a : L) \\
\equiv & \{\ \ldots\ \} \\
 & \mathsf{tail}\ (a : L) \subseteq \top \cdot (a : L) \\
\equiv & \{\ \mathsf{tail}\ (a : L) = L \text{ cf. questão do 1º teste; (F4)}\ \} \\
 & L \subseteq \top \cdot [\underline{a}, L] \cdot \mathsf{in}^\circ \\
\equiv & \{\ \ldots\ \} \\
 & L \cdot \mathsf{in} \subseteq [\top \cdot \underline{a}, T \cdot L] \\
\equiv & \{\ \ldots\ \} \\
 & \left\{ \begin{array}{l} L \cdot \mathsf{zero} \subseteq \top \\ L \cdot \mathsf{succ} \subseteq T \cdot L \end{array} \right. \\
\equiv & \{\ \ldots\ \} \\
 & inv\ L
\end{array}$$

□

---

[2] Este invariante é idêntico ao do exercício 1 dos slides.

Questão 7 A propriedade seguinte, que envolve as duas divisões relacionais,

$$R \setminus (S \,/\, Q) = (R \setminus S) \,/\, Q \tag{F8}$$

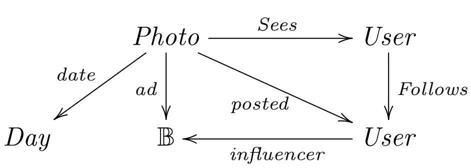
é muito útil, pois permite-nos escrever $R \setminus S \,/\, Q$ sem parênteses e sem nenhuma ambiguidade. Demonstre (F8) recorrendo, por exemplo, à igualdade indirecta.

RESOLUÇÃO: Tem-se (completar justificações):

$$\begin{array}{ll} & X \subseteq R \setminus (S \,/\, Q) \\ \equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & R \cdot X \subseteq S \,/\, Q \\ \equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & R \cdot X \cdot Q \subseteq S \\ \equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & X \cdot Q \subseteq R \setminus S \\ \equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & X \subseteq (R \setminus S) \,/\, Q \end{array}$$

□

Questão 8 Recorde o modelo 'Instagram' que foi assunto das aulas de MFES (1^o semestre) e do 1^o teste,



cuja relação *Follows* está sujeita aos seguintes invariantes:

$$inv31\ Follows = \frac{ad}{false} \cap Sees \ \subseteq \ Follows \cdot posted \tag{F9}$$

$$inv_2\ Follows = Follows \ \subseteq \ (\neq) \tag{F10}$$

Calcule a pré-condição mais fraca (em notação *pointwise*) para a seguinte operação — que regista um(a) novo(a) seguidor(a) no Instagram,

$$newFwlr\ v\ u\ Follows = Follows \cup \underline{v} \cdot \underline{u}^\circ \tag{F11}$$

("v passa a seguir u") — preservar cada um dos invariantes dados.

RESOLUÇÃO:

- Invariante (F9): como $Follows \ \subseteq \ newFlwr\ v\ u\ Follows$, $inv31$ está garantido por monotonia sem qualquer pré-condição.

- Quanto a (F10):

$$
\begin{array}{ll}
 & inv_2\ (newFwlr\ v\ u\ Follows) \\
\equiv & \quad \{\ \ldots\ \} \\
 & (newFwlr\ v\ u\ Follows)\ \subseteq\ (\neq) \\
\equiv & \quad \{\ \ldots\ \} \\
 & Follows \cup \underline{v} \cdot \underline{u}^{\circ}\ \subseteq\ (\neq) \\
\equiv & \quad \{\ \ldots\ \} \\
 & inv_2\ Follows \wedge \underbrace{\underline{v} \cdot \underline{u}^{\circ} \subseteq (\neq)}_{WP} \\
\equiv & \quad \{\ \ldots\ \} \\
 & inv_2\ Follows \wedge \underbrace{id \subseteq \underline{v}^{\circ} \cdot (\neq) \cdot \underline{u}}_{WP} \\
\equiv & \quad \{\ \ldots\ \} \\
 & inv_2\ Follows \wedge \underbrace{v \neq u}_{WP}
\end{array}
$$

□
