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 época especial — 25 de Julho de 2022
14h30–16h30, Sala E1-2.17

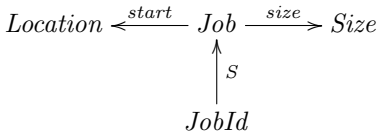
---

*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 Suponha que faz parte da equipa que está a desenvolver, com base no modelo



o módulo de gestão de memória do "kernel" de um sistema operativo, onde:

- $JobId$ identifica cada processo (Job) em execução, de forma única;
- $start$ dá o endereço onde começa o bloco de memória reservado a cada processo em execução;
- $size$ dá o tamanho desse bloco de memória (contígua);
- S(cheduled) é a relação simples que associa $JobId$s a Jobs;
- $Location$ e $Size$ são números naturais.

O mais importante dos invariantes deste modelo é o que vai garantir que nenhum processo executa em células de memória de outros processos. Para o especificar, definiu-se a relação $JobId \xleftarrow{Owns} Location$ que indica a "posse" (ou não) de um endereço a por parte de um processo k:

$$k\ Owns\ a\ \Leftrightarrow\ \langle \exists\ x\ :\ x\ S\ k :\ start\ x \leqslant a \leqslant start\ x + size\ x \rangle \qquad \text{(F1)}$$

A que propriedade(s) da relação $Owns$ recorreria para especificar o invariante pretendido? Justifique convenientemente a sua resposta.

Questão 2 Mostre que a expressão relacional $\bot\ /\ (S \cdot f^\circ)$ simplifica para $\bot\ /\ S$.

Questão 3 Considere a seguinte definição de uma relação $A^* \xleftarrow{R} A^*$,

$$R \cdot \mathsf{in} = \mathsf{in} \cdot [i_1\,, i_1 \cup i_2 \cdot (id \times R)]$$

onde

$$\mathsf{in} = [\mathsf{nil}, \mathsf{cons}] \tag{F2}$$

$$\mathsf{nil}\ \_ = [\,] \tag{F3}$$

$$\mathsf{cons}\ (h, t) = h : t \tag{F4}$$

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 $y\ R\ x$.

RESOLUÇÃO:

$$\begin{cases} R \cdot \mathsf{nil} = \mathsf{nil} \\ R \cdot \mathsf{cons} = \mathsf{in} \cdot i_1 \cup \mathsf{in} \cdot i_2 \cdot (id \times R) \end{cases}$$

$\equiv$ { }

$$\begin{cases} y\ R\ [\,] \Leftrightarrow y = [\,] \\ R \cdot \mathsf{cons} = \mathsf{nil} \cup \mathsf{cons} \cdot (id \times R) \end{cases}$$

$\equiv$ { }

$$\begin{cases} y\ R\ [\,] \Leftrightarrow y = [\,] \\ y\ R\ (h : t) \Leftrightarrow y = [\,] \vee y\ (\mathsf{cons} \cdot (id \times R))\ (h, t) \end{cases}$$

$\equiv$ { }

$$\begin{cases} y\ R\ [\,] \Leftrightarrow y = [\,] \\ y\ R\ (h : t) \Leftrightarrow y = [\,] \vee \langle \exists\ a, b\ :\ a = h \wedge b\ R\ t :\ y = (a : b) \rangle \end{cases}$$

$\equiv$ { }

$$\begin{cases} y\ R\ [\,] \Leftrightarrow y = [\,] \\ y\ R\ (h : t) \Leftrightarrow y = [\,] \vee \langle \exists\ b\ :\ b\ R\ t :\ y = (h : b) \rangle \end{cases}$$

□

Questão 4 No exame anterior desta disciplina pediu-se para mostrar que, para a relação

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

— que junta duas relações R e S numa só — ser simples, basta que R e S o sejam e que

$$\begin{cases} f \text{ e } g \text{ são injectivas} \\ \frac{f}{g} = \bot \end{cases} \tag{F5}$$

se verifique. Demonstre o facto seguinte, que permite extrair R e S de Q,

$$Q = R \cdot f^\circ \cup S \cdot g^\circ \quad \Rightarrow \quad \begin{cases} Q \cdot f = R \\ Q \cdot g = S \end{cases} \tag{F6}$$

assumindo que as condições de (**??**) se verificam.

RESOLUÇÃO:

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

$\Rightarrow$ { }

$$\begin{cases} Q \cdot f = (R \cdot f^\circ \cdot f) \cup (S \cdot g^\circ \cdot f) \\ Q \cdot g = (R \cdot f^\circ \cdot g) \cup (S \cdot g^\circ \cdot g) \end{cases}$$

$$
\begin{array}{ll}
\equiv & \{\ \} \\
& \left\{ \begin{array}{l} Q \cdot f = R \cdot id \cup S \cdot \bot \\ Q \cdot g = R \cdot \bot \cup S \cdot id \end{array} \right. \\
\equiv & \{\ \} \\
& \left\{ \begin{array}{l} Q \cdot f = R \\ Q \cdot g = S \end{array} \right. \\
\Box &
\end{array}
$$

$\Box$

Questão 5 Considere-se um qualquer programa imperativo P representado pela relação $S \xleftarrow{P} S$ que indica como o programa modifica os valores das variáveis que estão guardadas no seu estado de tipo S. 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,

$$\{p\}\ P\ \{q\}\ \Leftrightarrow\ P \cdot \Phi_p \subseteq \Phi_q \cdot P \tag{F7}$$

onde Φ_p (resp. Φ_q) é representação de p (resp. q) sob a forma de uma relação coreflexiva.

Demonstre, a partir de (**??**), a seguinte regra de composição de triplos de Hoare:

$$\{p\}\ P\ \{q\} \wedge \{q\}\ Q\ \{r\} \quad \Rightarrow \quad \{p\}\ (Q \cdot P)\ \{r\} \tag{F8}$$

RESOLUÇÃO: Tem-se:

$$
\begin{array}{ll}
& \{p\}\ P\ \{q\} \wedge \{q\}\ Q\ \{r\} \\
\equiv & \{\ \} \\
& \left\{ \begin{array}{l} P \cdot \Phi_p \subseteq \Phi_q \cdot P \\ Q \cdot \Phi_q \subseteq \Phi_r \cdot Q \end{array} \right. \\
\Rightarrow & \{\ \} \\
& \left\{ \begin{array}{l} Q \cdot P \cdot \Phi_p \subseteq Q \cdot \Phi_q \cdot P \\ Q \cdot \Phi_q \cdot P \subseteq \Phi_r \cdot Q \cdot P \end{array} \right. \\
\Rightarrow & \{\ \} \\
& Q \cdot P \cdot \Phi_p \subseteq \Phi_r \cdot Q \cdot P \\
\equiv & \{\ \} \\
& \{p\}\ (Q \cdot P)\ \{r\} \\
\Box &
\end{array}
$$

$\Box$

Questão 6 Num exame anterior, a divisão inteira de dois naturais foi implementada com base na subtração truncada em $\mathbb{N}_0$, operação essa que foi **especificada** pela GC:

$$a \ominus b \leqslant x\ \Leftrightarrow\ a \leqslant x + b \tag{F9}$$

Pode mostrar-se que a seguinte propriedade decorre da especificação (**??**):

$$(a+b) \ominus c = (a \ominus c) + b \quad \Leftarrow \quad a \geqslant c \tag{F10}$$

Pretendendo-se agora a **implementação** de $\ominus$, alguém escreveu, em Haskell:

$$a \ominus b = \textbf{if } a \leqslant b \textbf{ then } 0 \textbf{ else } 1 + (a \ominus (b+1)) \tag{F11}$$

Mostre que (**??**) satisfaz (**??**) para $a \leqslant b$; quanto ao caso $a > b$, faça o mesmo completando o seguinte raciocínio por igualdade indirecta:

$$\begin{array}{cl} & a \ominus b \leqslant x \\ \equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\ & (a+1) \ominus (b+1) \leqslant x \\ \equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\ & (a \ominus (b+1)) + 1 \leqslant x \\ :: & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\ & a \ominus b = 1 + (a \ominus (b+1)) \\ \Box & \end{array}$$

RESOLUÇÃO: Prova de (**??**), desde que $a \geqslant c$:

$$\begin{array}{cl} & (a+b) \ominus c \leqslant z \\ \equiv & \{ \ \} \\ & a + b \leqslant z + c \\ \equiv & \{ \ (\textbf{??}) \ \} \\ & (a \ominus c) + c + b \leqslant z + c \\ \equiv & \{ \ \} \\ & (a \ominus c) + b \leqslant z \\ \Box & \end{array}$$

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

$$a \times (b \ominus 1) = (a \times b) \ominus a$$

$$(a \ominus b) + b = a \text{ desde que } a \geqslant b$$

Caso $a \leqslant b$: corresponde a $x = 0$ em (**??**), $a \ominus b \leqslant 0 \ \Leftrightarrow \ a \leqslant b$ que é equivalente a $a \ominus b = 0$ pois estamos em $\mathbb{N}_0$.

Caso $a > b$:

$$\begin{array}{cl} & a \ominus b \leqslant x \\ \equiv & \{ \text{ GC } \} \\ & a \leqslant x + b \\ \equiv & \{ \ (+1) \text{ injectiva em } \mathbb{N}_0 \ \} \\ & a + 1 \leqslant x + (b+1) \\ \equiv & \{ \text{ GC } \} \\ & (a+1) \ominus (b+1) \leqslant x \\ \equiv & \{ \ (\textbf{??}), \text{ pois } a > b \ \Leftrightarrow \ a \geqslant b+1 \ \} \\ & (a \ominus (b+1)) + 1 \leqslant x \\ \Box & \end{array}$$

$\Box$

Questão 7 Demonstre o facto seguinte:

Para uma relação R ser injectiva basta que o seu núcleo esteja contido numa qualquer relação antissimétrica S:

$$\ker R \subseteq id \Leftarrow \ker R \subseteq S \wedge S \text{ é antissimétrica} \tag{F12}$$

Sugestão: assumir S antissimétrica e demonstrar a implicação $\ker R \subseteq id \Leftarrow \ker R \subseteq S$.

RESOLUÇÃO:

$$\begin{array}{ll} & \ker R \subseteq id \\ \Leftarrow & \quad \{ \ \dots\dots\dots \ \} \\ & \ker R \subseteq S \cap S^\circ \\ \equiv & \quad \{ \ \dots\dots\dots \ \} \\ & \ker R \subseteq S \wedge \ker R \subseteq S^\circ \\ \equiv & \quad \{ \ \dots\dots\dots \ \} \\ & \ker R \subseteq S \\ \Box & \end{array}$$

□

Questão 8 Considere a seguinte variante da função foldr da linguagem Haskell:

$$fldr :: ((a, b) \to b) \to b \to [a] \to b$$

Mostre que o cálculo do teorema grátis da função $fldr$ conduz a

$$f \cdot (R \times S) \subseteq S \cdot g \ \Rightarrow \ y \ S \ x \ \Rightarrow \ fldr \ f \ y \cdot R^* \subseteq S \cdot fldr \ g \ x \tag{F13}$$

(onde todas as variáveis se assumem universalmente quantificadas) e instancie-o para as funções $R, S := id, s$.

RESOLUÇÃO: Tem-se: $fldr :: ((b \leftarrow [a]) \leftarrow b) \leftarrow (b \leftarrow (a, b))$.

$$\begin{array}{ll} & fldr \ (((S \leftarrow R^*) \leftarrow S) \leftarrow (S \leftarrow (R \times S))) \ fldr \\ \equiv & \quad \{ \ \} \\ & fldr \cdot (S \leftarrow (R \times S)) \subseteq ((S \leftarrow R^*) \leftarrow S) \cdot fldr \\ \equiv & \quad \{ \ \} \\ & f \ (S \leftarrow (R \times S)) \ g \ \Rightarrow \ (fldr \ f) \ ((S \leftarrow R^*) \leftarrow S) \ (fldr \ g) \\ \equiv & \quad \{ \ \} \\ & f \cdot (R \times S) \subseteq S \cdot g \ \Rightarrow \ fldr \ f \cdot S \subseteq (S \leftarrow R^*) \cdot fldr \ g \\ \equiv & \quad \{ \ \} \\ & f \cdot (R \times S) \subseteq S \cdot g \ \Rightarrow \ y \ S \ x \ \Rightarrow \ fldr \ f \ y \cdot R^* \subseteq S \cdot fldr \ g \ x \\ \Box & \end{array}$$

Instância pedida — $R, S := id, s$:

$$
\begin{array}{ll}
 & f \cdot (id \times s) \subseteq s \cdot g \;\Rightarrow\; y\ s\ x \;\Rightarrow\; \mathit{fldr}\ f\ \ y \cdot \mathsf{seq}\ id \subseteq s \cdot \mathit{fldr}\ g\ x \\
\equiv & \quad \{\ \} \\
 & f \cdot (id \times s) = s \cdot g \;\Rightarrow\; \mathit{fldr}\ f\ (s\ x) = s \cdot (\mathit{fldr}\ g\ x)
\end{array}
$$

□
