Cálculo de Programas

2.º Ano de LCC (Universidade do Minho)
Ano Lectivo de 2023/24

1º teste — 20 de Março de 2024, 16h00–18h00
Salas 1.05 + 1.07 do Edifício 2

PROVA PRESENCIAL INDIVIDUAL SEM CONSULTA (2h)

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

Questão 1 O formulário desta UC inclui as duas equivalências seguintes, válidas para qualquer isomorfismo α:

$$\alpha \cdot g = h \equiv g = \alpha^\circ \cdot h \tag{E1}$$

$$g \cdot \alpha = h \equiv g = h \cdot \alpha^\circ \tag{E2}$$

Recorra a essas propriedades para mostrar que a igualdade

$$h \cdot \mathsf{distr} \cdot (g \times (id + \beta)) = k$$

é equivalente à igualdade:

$$h \cdot (g \times id + g \times \beta) = k \cdot \mathsf{undistr}$$

(**Sugestão:** não ignore a propriedade natural (i.e. *grátis*) do isomorfismo distr.)

RESOLUÇÃO: Do tipo $\mathsf{distr} : A \times (B + C) \to A \times B + A \times C$ infere-se a propriedade grátis

$$\mathsf{distr} \cdot (f \times (g + h)) = (f \times g + f \times h) \cdot \mathsf{distr}$$

(Desenvolver em casa.) Tem-se então (justificar os passos com reticências):

$$\begin{array}{cl} & h \cdot \mathsf{distr} \cdot (g \times (id + \beta)) = k \\ \equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & h \cdot (g \times id + g \times \beta) \cdot \mathsf{distr} = k \\ \equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & h \cdot (g \times id + g \times \beta) = k \cdot \mathsf{undistr} \end{array}$$

□

Questão 2 Recorde o isomorfismo

$$\begin{tikzcd} Maybe\ B \arrow[rr, bend left, "\mathsf{out}=\mathsf{in}^\circ"] \arrow[rr, phantom, "\cong"] & & 1+B \arrow[ll, bend left, "\mathsf{in}=[\underline{\mathsf{Nothing}}\,,\mathsf{Just}]"] \end{tikzcd}$$

e considere a função:

$$\begin{array}{l} \mathsf{fromMaybe} :: a \to Maybe\ a \to a \\ \mathsf{fromMaybe}\ a = [\underline{a}\,, id] \cdot \mathsf{out} \end{array}$$

Derive a versão *pointwise* de fromMaybe por forma a não recorrer ao combinador de alternativa (vulg. 'either') de funções nem a funções constantes.

RESOLUÇÃO: Tem-se (justificar os passos com reticências):

$$\begin{array}{cl} & \mathsf{fromMaybe}\ a = [\underline{a}\,, id] \cdot \mathsf{out} \\ \equiv & \quad \{\ \mathsf{in}\ /\ \mathsf{out};\ inMaybe\ \} \\ & \mathsf{fromMaybe}\ a \cdot [\underline{\mathsf{Nothing}}\,, \mathsf{Just}] = [\underline{a}\,, id] \\ \equiv & \quad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\ & \left\{ \begin{array}{l} \mathsf{fromMaybe}\ a \cdot \underline{\mathsf{Nothing}} = \underline{a} \\ \mathsf{fromMaybe}\ a \cdot \mathsf{Just} = id \end{array} \right. \\ \equiv & \quad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\ & \left\{ \begin{array}{l} \mathsf{fromMaybe}\ a\ \mathsf{Nothing} = a \\ \mathsf{fromMaybe}\ a\ (\mathsf{Just}\ a') = a' \end{array} \right. \end{array}$$

$\square$

Questão 3 Resolva em ordem a α a equação,

$$\alpha \cdot [id + i_1\,, i_2 \cdot i_2] = id \qquad \text{(E3)}$$

identificando o tipo mais geral de α e fazendo um diagrama que descreva a equação dada.

RESOLUÇÃO: Tem-se o tipo $[id + i_1\,, i_2 \cdot i_2] : (A + B) + C \to A + (B + C)$. Logo ter-se-á

$$\alpha : A + (B + C) \to (A + B) + C.$$

Cálculo de α (justificar os passos com reticências):

$$\begin{array}{cl} & \alpha \cdot [id + i_1\,, i_2 \cdot i_2] = id \\ \equiv & \quad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\ & [\alpha \cdot (id + i_1)\,, \alpha \cdot i_2 \cdot i_2] = id \\ \equiv & \quad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\ & \left\{ \begin{array}{l} \alpha \cdot (id + i_1) = i_1 \\ \alpha \cdot i_2 \cdot i_2 = i_2 \end{array} \right. \\ \equiv & \quad \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \end{array}$$

$$\left\{\begin{array}{l}[\alpha \cdot i_1 , \alpha \cdot i_2 \cdot i_1] = i_1 \\ \alpha \cdot i_2 \cdot i_2 = i_2\end{array}\right.$$

$\equiv \quad \{ \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; \}$

$$\left\{\begin{array}{l}\alpha \cdot i_1 = i_1 \cdot i_1 \\ \alpha \cdot i_2 \cdot i_1 = i_1 \cdot i_2 \\ \alpha \cdot i_2 \cdot i_2 = i_2\end{array}\right.$$

$\equiv \quad \{ \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; \}$

$$\left\{\begin{array}{l}\alpha \cdot i_1 = i_1 \cdot i_1 \\ \alpha \cdot i_2 = [i_1 \cdot i_2 , i_2]\end{array}\right.$$

$\equiv \quad \{ \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; \}$

$$\alpha = [i_1 \cdot i_1 , i_2 + id]$$

□

Questão 4 Em Haskell, a função $divMod\ x\ y$ dá como resultado um par (q, r) tal que $x = q \times y + r$. Para $y = 2$ (em $\mathbb{N}_0$), r ou é 0 ou é 1, o que quer dizer que podemos pensar numa função

$$divMod2 : \mathbb{N}_0 \to \mathbb{N}_0 \times \mathbb{B}$$

que satisfaz as propriedades seguintes:

$$divMod2\ (2\ n) = (n, \text{TRUE}) \tag{E4}$$
$$divMod2\ (2\ n + 1) = (n, \text{FALSE}) \tag{E5}$$

(Ou seja, $divMod2\ x$ dá não só a divisão inteira $x \div 2$ mas também a paridade de x.)

Encontre α em

$$\begin{tikzcd} \mathbb{N}_0 \arrow[r, "divMod2"] & \mathbb{N}_0 \times \mathbb{B} \arrow[r, "\alpha^\circ"] & \mathbb{N}_0 + \mathbb{N}_0 \arrow[ll, bend left, "\beta"] \end{tikzcd}$$

tal que

$$\alpha^\circ \cdot divMod2 \cdot \beta = id \tag{E6}$$

para

$$\beta = [even , odd] \tag{E7}$$
$$even\ n = 2\ n \tag{E8}$$
$$odd\ n = 2\ n + 1 \tag{E9}$$

NB: proponha α e demonstre que (E6) se verifica.

RESOLUÇÃO: Como só os isomorfismos têm conversos, assume-se que α é um isomorfismo. Tem-se então:[1]

$$\alpha^\circ \cdot divMod2 \cdot [even , odd] = id$$

$\equiv \quad \{ \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; \}$

$$divMod2 \cdot [even , odd] = \alpha$$

$\equiv \quad \{ \;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\; \}$

[1] Justificar os passos com reticências.

$$
\begin{array}{ll}
 & \alpha = [\mathit{divMod2} \cdot \mathit{even} \, , \mathit{divMod2} \cdot \mathit{odd}] \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} \alpha \cdot i_1 = \mathit{divMod2} \cdot \mathit{even} \\ \alpha \cdot i_2 = \mathit{divMod2} \cdot \mathit{odd} \end{array} \right. \\
\equiv & \quad \{ \text{ como } \mathit{divMod2} \text{ está definida } \textit{pointwise}\text{, temos de usar variáveis } \} \\
 & \left\{ \begin{array}{l} \alpha \; (i_1 \; n) = \mathit{divMod2} \; (2 \; n) \\ \alpha \; (i_2 \; n) = \mathit{divMod2} \; (2 \; n + 1) \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} \alpha \; (i_1 \; n) = (n, \mathrm{TRUE}) \\ \alpha \; (i_2 \; n) = (n, \mathrm{FALSE}) \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \left\{ \begin{array}{l} \alpha \cdot i_1 = \langle \mathit{id}, \underline{\mathrm{TRUE}} \rangle \\ \alpha \cdot i_2 = \langle \mathit{id}, \underline{\mathrm{FALSE}} \rangle \end{array} \right. \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & \alpha = [\langle \mathit{id}, \underline{\mathrm{TRUE}} \rangle \, , \langle \mathit{id}, \underline{\mathrm{FALSE}} \rangle]
\end{array}
$$

(**NB**: pode observar-se que α é o isomorfismo que participa na definição do guarda $p?$.) □

Questão 5 Duas funções f e g dizem-se permutativas entre si sempre que a igualdade

$$f \cdot g \quad = \quad g \cdot f \tag{E10}$$

se verifica. Identifique os tipos mais gerais de f e g e verifique em que condições as seguintes funções são permutativas:

$$\left\{ \begin{array}{l} f = (a+) \\ g = (b+) \end{array} \right. \tag{E11}$$

$$\left\{ \begin{array}{l} f = \mathsf{assocr} \\ g = \mathsf{assocl} \end{array} \right. \tag{E12}$$

NB: $(+)$ é a operação de adição num qualquer tipo numérico.

RESOLUÇÃO: Tipos:

Façamos $f : A \to B$ e $g : C \to D$.

Por $f \cdot g$ terá que ser $D = A$, ficando-se com $f \cdot g : C \to B$.

Por $g \cdot f$ terá que ser $B = C$, ficando-se com $g \cdot f : A \to A$.

Pela igualdade $g \cdot f = f \cdot g$ teremos $A = C$ e $A = B$.

Logo, tanto f como g têm tipo $A \to A$.

Casos:

- O caso (E11) é imediato pois a soma é associativa e comutativa: $(a+) \cdot (b+) = (b+) \cdot (a+)$ é o mesmo que $a + (b + x) = b + (a + x)$.
- O caso (E12) é garantido pelo respectivo isomorfismo, mas exige o tipo $(A \times B) \times (C \times D) \to (A \times B) \times (C \times D)$ para ambas as funções.

□

Questão 6 Demonstre a lei do condicional de McCarthy que se segue

$$p \rightarrow (q \rightarrow a\ ,\ b)\ ,\ b \quad = \quad (p \wedge q) \rightarrow a\ ,\ b \tag{E13}$$

sabendo que

$$(p \wedge q)? \quad = \quad p \rightarrow q?\ ,\ i_2 \tag{E14}$$

é uma propriedade da conjunção de predicados.

RESOLUÇÃO: Ter-se-á, pegando no lado direito da igualdade a provar:

$$
\begin{array}{cl}
& (p \wedge q) \rightarrow a\ ,\ b \\
= & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& [a\,,b] \cdot (p \rightarrow q?\ ,\ i_2) \\
= & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& p \rightarrow ([a\,,b] \cdot q?)\ ,\ ([a\,,b] \cdot i_2) \\
= & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& p \rightarrow (q \rightarrow a\ ,\ b)\ ,\ b \\
\Box &
\end{array}
$$

$\Box$

Questão 7 Seja dada uma função de ordem superior α que satisfaz a propriedade:

$$\widehat{\alpha\, f} = \widehat{f} \cdot \mathsf{swap} \tag{E15}$$

Mostre, usando as propriedades da exponenciação, que

$$\alpha\ (\alpha\ f) = f$$

se verifica.

RESOLUÇÃO: Tem-se (justificar os passos com reticências):

$$
\begin{array}{cl}
& \alpha\ (\alpha\ f) = f \\
\equiv & \quad \{ \text{ (E15), pois pelo isomorfismo curry/uncurry tem-se: } \alpha\ f = \overline{\widehat{f} \cdot \mathsf{swap}} \ \} \\
& \alpha\ \overline{(\widehat{f} \cdot \mathsf{swap})} = f \\
\equiv & \quad \{ \text{ de novo } \alpha\ f = \overline{\widehat{f} \cdot \mathsf{swap}} \ \} \\
& \overline{\widehat{\overline{(\widehat{f} \cdot \mathsf{swap})}} \cdot \mathsf{swap}} = f \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \overline{\widehat{f} \cdot \mathsf{swap} \cdot \mathsf{swap}} = f \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& f = f
\end{array}
$$

$\Box$

Questão 8 A função seguinte

$$
\begin{aligned}
&sq\ 0 = 0\\
&sq\ (n+1) = n + n + 1 + sq\ n
\end{aligned}
$$

calcula o quadrado de um número natural (em $\mathbb{N}_0$) sem fazer quaisquer multiplicações. Mostre que sq satisfaz a equação

$$sq \cdot \mathsf{in} = [\underline{0}, add] \cdot (id + id \times sq) \cdot (id + odd \times id) \cdot (id + \langle id, id \rangle) \tag{E16}$$

onde $\overline{\mathsf{add}} = (+)$, $odd\ n = 2\ n + 1$ e in é dada por:

$$
\begin{tikzcd}
1 \arrow[r, "i_1"] \arrow[dr, "\underline{0}"'] & 1 + \mathbb{N}_0 \arrow[d, "\mathsf{in}=[\underline{0},\mathsf{succ}]"] & \mathbb{N}_0 \arrow[l, "i_2"'] \arrow[dl, "\mathsf{succ}"] \\
& \mathbb{N}_0 &
\end{tikzcd}
\tag{E17}
$$

RESOLUÇÃO: Basta simplificar (E16) e passar para pointwise, sabendo-se que $2\ n = n + n$. $\square$