Métodos Formais de Programação II +
Opção - Métodos Formais de Programação II

4.º Ano da LMCC (7008N2) + LESI (5308P3)
Ano Lectivo de 2002/03

Exame (época recurso) — - 22 de Julho 2003
14h30
Salas 2202, 2208

NB: *Esta prova consta de **7** alíneas todas com a mesma cotação.*

PROVA SEM CONSULTA (2 horas)

Questão 1 O operador de sobreposição de funções finitas disponível em VDM-SL

```
s1 ++ s2 = { k |-> if k in set dom s2 then s2(k) else s1(k)
                 | k in set dom s2 union dom s1}
```

pode ser visto como um caso particular da operação de sobreposição de relações binárias definido como se segue:

$$R \dagger S \quad = \quad S \cup R \cdot (id - \mathit{dom}\, S) \tag{1}$$

1. Apresente as justificações do seguinte raciocínio que mostra que o código VDM-SL apresentado deriva de facto de (1):

$$\begin{array}{rcl}
\sigma_1 \dagger \sigma_2 & = & \sigma_2 \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (\mathit{dom}\,\sigma_1) \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \\
& = & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& & (\sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2)) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \\
& = & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& & (\mathit{dom}\,\sigma_2 \rightarrow \sigma_2\ ,\ \sigma_1) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1)
\end{array}$$

RESOLUÇÃO:

$$\begin{array}{rcl}
\sigma_1 \dagger \sigma_2 & = & \sigma_2 \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{\ R = R \cdot \mathit{dom}\, R \text{ (3 vezes)} \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (\mathit{dom}\,\sigma_1) \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{\ \mathit{dom}\, R \subseteq X \equiv R = R \cdot X, \text{ onde } X \text{ é coreflexiva } \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cdot (id - \mathit{dom}\,\sigma_2) \\
& = & \qquad \{ \text{ composição de coreflexivas é a sua intersecção, logo é comutativa} \} \\
& & \sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \\
& = & \qquad \{ \text{ Galois: } (\cdot(\mathit{dom}\,\sigma_1 \cup \mathit{dom}\,\sigma_2)) \text{ é adjunto inferior, logo distribui por } \cup \} \\
& & (\sigma_2 \cdot (\mathit{dom}\,\sigma_2) \cup \sigma_1 \cdot (id - \mathit{dom}\,\sigma_2)) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1) \\
& = & \qquad \{ \text{ introdução de condicional de McCarthy} \} \\
& & (\mathit{dom}\,\sigma_2 \rightarrow \sigma_2\ ,\ \sigma_1) \cdot (\mathit{dom}\,\sigma_2 \cup \mathit{dom}\,\sigma_1)
\end{array}$$

$\square$

2. O operador $\dagger$ ocorre em

$$\begin{tikzcd} \alpha \arrow[rr, bend left, "R"] \arrow[rr, phantom, "\cong"] & & \beta \arrow[ll, bend left, "(i_2\cdot!\dagger i_1\cdot)"] \end{tikzcd} \tag{2}$$

Identifique os domínios de dados α, β e a relação de representação R por forma a que (2) seja uma lei de isomorfismo que estudou nesta disciplina.
NB: leia $(i_2\cdot! \dagger i_1\cdot)x$ da forma habitual, isto é, $i_2\cdot! \dagger i_1 \cdot x$. O facto

$$dom\,(R \cdot S) = dom\,(dom\, R \cdot S) \tag{3}$$

pode ser útil para a sua resolução.

RESOLUÇÃO: Aplicando a função de abstracção e expandindo, tem-se

$$\begin{array}{rcl} (i_2\cdot! \dagger i_1\cdot)X & = & i_2\cdot! \dagger i_1 \cdot X \\ & = & \quad \{\ \text{por (1)}\} \\ & & i_1 \cdot X \cup i_2\cdot! \cdot (id - dom\,(i_1 \cdot X)) \\ & = & \quad \{\ \text{por (3)}\} \\ & & i_1 \cdot X \cup i_2\cdot! \cdot (id - dom\,(dom\, i_1 \cdot X)) \\ & = & \quad \{\ i_1 \text{ é inteira ; natural-}id\} \\ & & i_1 \cdot X \cup i_2\cdot! \cdot (id - dom\, X) \\ & = & \quad \{\ \text{definição de } tot\} \\ & & tot\ X \end{array}$$

Logo a lei que se identifica em (2) é

$$\begin{tikzcd} (B+1)^A \arrow[rr, bend left, "untot"] \arrow[rr, phantom, "\cong"] & & A \rightharpoonup B \arrow[ll, bend left, "tot"] \end{tikzcd}$$

$\square$

Questão 2 No refinamento relacional opta-se por vezes por representações não-normalizadas em situações em que o volume de dados não é preocupante. Uma lei que realiza um refinamento desse tipo é

$$\begin{tikzcd} (A \rightharpoonup B) \times (A \rightharpoonup C) \arrow[rr, bend left, "R"] \arrow[rr, phantom, "\leq"] & & A \rightharpoonup ((B+1) \times (C+1)) \arrow[ll, bend left, "f=\langle (i_1^\circ\cdot\pi_1\cdot), (i_1^\circ\cdot\pi_2\cdot)\rangle"] \end{tikzcd} \tag{4}$$

agregando duas tabelas numa só, por exemplo representando

NÚMERO	NOME
1010	Manuel
11230	Maria

e

NÚMERO	CURSO
11230	LESI
15234	LMCC

numa só estrutura:

NÚMERO	NOME	CURSO
1010	Manuel	`nil`
11230	Maria	LESI
15234	`nil`	LMCC

1. Mostre que $(\sigma_1, \sigma_2) = f\ \sigma$ significa

$$\sigma_1 = \{a \mapsto b \mid a \in \mathit{dom}\,\sigma \wedge \pi_1(\sigma\ a) = (i_1\ b)\} \tag{5}$$
$$\sigma_2 = \{a \mapsto c \mid a \in \mathit{dom}\,\sigma \wedge \pi_2(\sigma\ a) = (i_1\ c)\} \tag{6}$$

NB: prove apenas uma das duas igualdades anteriores.

RESOLUÇÃO: Aplicando a função de abstracção, tem-se

$$\begin{aligned}
& (\sigma_1, \sigma_2) = f\sigma \\
= & \quad \{ \text{ definição de } f \} \\
& (\sigma_1, \sigma_2) = ((i_1^\circ \cdot \pi_1 \cdot)\sigma, (i_1^\circ \cdot \pi_2 \cdot)\sigma) \\
= & \quad \{ \text{ aplicação de funções} \} \\
& (\sigma_1, \sigma_2) = (i_1^\circ \cdot \pi_1 \cdot \sigma, i_1^\circ \cdot \pi_2 \cdot \sigma) \\
= & \quad \{ \text{ igualdade de pares} \} \\
& \left\{ \begin{array}{l} \sigma_1 = i_1^\circ \cdot \pi_1 \cdot \sigma \\ \sigma_2 = i_1^\circ \cdot \pi_2 \cdot \sigma \end{array} \right.
\end{aligned}$$

Desenvolvimento da primeira igualdade acima:

$$\begin{aligned}
& \sigma_1 = i_1^\circ \cdot \pi_1 \cdot \sigma \\
\equiv & \quad \{ R \cdot \mathit{dom}\, R = R \} \\
& \sigma_1 = i_1^\circ \cdot \pi_1 \cdot \sigma \cdot \mathit{dom}\,\sigma \\
= & \quad \{ \text{ notação por compreensão após introdução de variáveis } \} \\
& \sigma_1 = \{(b, a) \mid b(i_1^\circ \cdot \pi_1 \cdot \sigma \cdot \mathit{dom}\,\sigma)a\} \\
= & \quad \{ \text{ composição relacional} \} \\
& \sigma_1 = \{(b, a) \mid b(i_1^\circ \cdot \pi_1 \cdot \sigma)a' \wedge a'(\mathit{dom}\,\sigma)a\} \\
= & \quad \{ \text{ regra } b(f^\circ \cdot R)a = (f\ b)Ra \text{ ; } \mathit{dom}\,\sigma \text{ é coreflexiva, logo } a'(\mathit{dom}\,\sigma)a \equiv a = a' \wedge a'(\mathit{dom}\,\sigma)a \ \} \\
& \sigma_1 = \{(b, a) \mid (i_1\ b)(\pi_1 \cdot \sigma)a \wedge a \in \mathit{dom}\,\sigma\} \\
= & \quad \{ \pi_1 \text{ é função; por hipótese } \sigma \text{ é simples; notação } a \mapsto b \text{ em VDM-SL } \} \\
& \sigma_1 = \{a \mapsto b \mid (i_1\ b) = \pi_1(\sigma\ a) \wedge a \in \mathit{dom}\,\sigma\}
\end{aligned}$$

□

2. Defina em notação VDM-SL uma função de representação $r \subseteq R$ adequada à lei (4) e explique (eg. por contra-exemplo) por que é que essa lei não é um isomorfismo.
NB: para não sobrecarregar a notação assuma a seguinte simplificação: A e B são tipos não anuláveis, isto é, `nil` $\notin A$ e `nil` $\notin B$.

RESOLUÇÃO: A simplificação proposta permite-nos representar, em VDM-SL, $C + 1$ por `[C]` e $B + 1$ por `[B]` e ignorar i_1 e i_2. Assim,

```
r :  (map A to B)*(map A to C) -> map A to ([B]*[C])
r(mk_(s1,s2)) ==
       {a |-> if a in set (dom s1 inter dom s2) then mk_(s1(a),s2(a))
              else if a in set dom s1 then mk_(s1(a),nil) else mk_(nil,s2(a))
       | a in set dom s1 union dom s2}
```

Para vermos que não há lugar a isomorfismo basta reparar que r não é sobrejectiva: em nenhuma circunstância se verifica `r(mk_(s1,s2))(a) = mk_(nil,nil)`. Da mesma maneira se verifica que f não é injectiva: `f(s)=f(s munion {a |-> mk_(nil,nil)})` para `a not in set dom s`. □

Questão 3 Deduza as propriedades

$$f \setminus S = f^\circ \cdot S \tag{7}$$
$$\mathit{ker}\ f = f \setminus f \tag{8}$$

a partir das seguintes conecções de Galois

$(f\ X) \subseteq Y \equiv X \subseteq (g\ Y)$	
$f = g^\flat$	$g = f^\sharp$
$(R\cdot)$	$(R\setminus\ )$
$(h\cdot)$	$(h^\circ\cdot)$

RESOLUÇÃO: Dedução de (7):

$$\begin{array}{cl} & X \subseteq f^\circ \cdot S \\ \equiv & \quad \{\ \text{“shunting rule” (segunda linha do quadro)}\ \} \\ & f \cdot X \subseteq S \\ \equiv & \quad \{\ \text{divisão (primeira linha do quadro)}\ \} \\ & X \subseteq f \setminus S \\ :: & \quad \{\ \text{indirecção}\ \} \\ & f^\circ \cdot S = f \setminus S \end{array}$$

Dedução de (8):

$$\begin{array}{cl} & \mathit{ker}\ f \\ = & \quad \{\ \text{definição de } \mathit{ker}\ \} \\ & f^\circ \cdot f \\ = & \quad \{\ \text{facto (7) para } S := f\ \} \\ & f \setminus f \end{array}$$

□

Questão 4 Atente no seguinte diálogo entre dois colegas seus:

A: O que se pretende é encontrar uma solução funcional para a especificação seguinte: *a lista resultado deverá ser uma permutação com os mesmos elementos (números naturais) da lista de entrada*.

B: Isso corresponde a resolver em ordem a f a equação $S \vdash f$, onde

```
S(i: seq of nat) r: seq of nat
post seq2bag(r) = seq2bag(i) and elems(r) = elems(i) ;
```

A: Exacto. Mas para efeitos de cálculo é melhor escrevermos

$$(\mathit{ker}\ seq2bag) \cap (\mathit{ker}\ elems) \vdash f \tag{9}$$

B: Para mim, isso é a mesma coisa que

$$(\mathit{ker}\ seq2bag) \vdash f \wedge (\mathit{ker}\ elems) \vdash f \tag{10}$$

A: Talvez tenhas razão. Mas olha que nos vai bastar resolver $(\mathit{ker}\ seq2bag) \vdash f \ldots$

B: Porquê?

A: Porque $elems = dom \cdot seq2bag$ e dom é inteira. Logo $\mathit{ker}\ seq2bag \subseteq \mathit{ker}\ elems$.

B: Bem visto. Já agora vamos avisar quem escreveu a pós-condição de S que pode remover a cláusula `elems(r) = elems(i)` — está nitidamante a mais!

1. Recordando

$$S \vdash R \quad \equiv \quad R \cdot \mathit{dom}\, S \subseteq S \wedge \mathit{dom}\, S \subseteq \mathit{dom}\, R \tag{11}$$

verifique se **B** tinha razão ao identificar (10) com (9).

RESOLUÇÃO: **B** tinha razão de facto, pois

$$(\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems) \vdash f \quad \equiv \quad (\mathit{ker}\ seq2bag \vdash f) \wedge (\mathit{ker}\ elems \vdash f) \tag{12}$$

verifica-se. Dedução de (12):

$$
\begin{array}{cl}
& (\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems) \vdash f \\
\equiv & \qquad \{\ \text{por (11), sabendo que } f \text{ é inteira, logo } \mathit{dom}\ f = id \} \\
& f \cdot \mathit{dom}(\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems) \subseteq (\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems) \\
\equiv & \qquad \{\ \mathit{dom}(\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems) = id \text{, ver (13) abaixo ; natural-}id\ \} \\
& f \subseteq \mathit{ker}\ seq2bag \cap \mathit{ker}\ elems \\
\equiv & \qquad \{\ \text{universal-}\cap\ \} \\
& (f \subseteq \mathit{ker}\ seq2bag) \wedge (f \subseteq \mathit{ker}\ elems) \\
\equiv & \qquad \{\ \text{(11) duas vezes, para } R := f \text{ e } S := \mathit{ker}\ seq2bag \text{, que é reflexiva, logo inteira}\ \} \\
& (\mathit{ker}\ seq2bag \vdash f) \wedge (\mathit{ker}\ elems \vdash f)
\end{array}
$$

Dois passos deste raciocínio basearam-se no facto de todas as relações reflexivas serem totais, isto é,

$$\mathit{dom}\ S = id \quad \Leftarrow \quad S \text{ é reflexiva} \tag{13}$$

Notar que $\mathit{ker}\ seq2bag \cap \mathit{ker}\ elems$ é reflexiva, já que a intersecção de duas relações reflexivas é reflexiva.

□

2. Deduza a lei geral em que **A** se baseou para reduzir $(\mathit{ker}\ seq2bag) \cap (\mathit{ker}\ elems)$ a $\mathit{ker}\ seq2bag$.

RESOLUÇÃO: A afirmação de **A** decorre do raciocínio seguinte:

$$
\begin{array}{cl}
& (\mathit{ker}\ seq2bag) \cap (\mathit{ker}\ elems) = \mathit{ker}\ seq2bag \\
\equiv & \qquad \{\ \text{pois } R \subseteq S \equiv R = R \cap S \text{ em geral}\ \} \\
& \mathit{ker}\ seq2bag \subseteq \mathit{ker}\ elems \\
\equiv & \qquad \{\ \text{por } elems = dom \cdot seq2bag\ \} \\
& \mathit{ker}\ seq2bag \subseteq \mathit{ker}\ (dom \cdot seq2bag) \\
\equiv & \qquad \{\ \text{definição de } \mathit{ker}\ \} \\
& \mathit{ker}\ seq2bag \subseteq (dom \cdot seq2bag)^\circ \cdot dom \cdot seq2bag \\
\equiv & \qquad \{\ (R \cdot S)^\circ = S^\circ \cdot R^\circ\ \} \\
& \mathit{ker}\ seq2bag \subseteq seq2bag^\circ \cdot dom^\circ \cdot dom \cdot seq2bag \\
\equiv & \qquad \{\ \text{definição de } \mathit{ker}\ \text{; natural-}id\ \} \\
& seq2bag^\circ \cdot id \cdot seq2bag \subseteq seq2bag^\circ \cdot dom^\circ \cdot dom \cdot seq2bag \\
\Leftarrow & \qquad \{\ (\cdot) \text{ é monótona}\ \} \\
& id \subseteq dom^\circ \cdot dom \\
\equiv & \qquad \{\ dom \text{ é inteira, logo por definição o seu núcleo é reflexivo}\ \} \\
& \mathrm{T}
\end{array}
$$

O facto *ker* $seq2bag \subseteq$ *ker* $(dom \cdot seq2bag)$ é a base do reciocínio. Abstraindo $seq2bag$ em R e dom em S, tem-se a lei geral

$$\mathit{ker}\ R \subseteq \mathit{ker}\ (S \cdot R) \quad \Leftarrow \quad S \text{ é inteira} \tag{14}$$

$\square$
