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

4.º Ano de LMCC (7008N2) + LESI (5308P3)
Ano Lectivo de 2006/07

Exame (época de recurso) — 20 de Julho 2007
14H00
Salas 1313, 2207

NB*: Esta prova consta de* ***8*** *alíneas todas com a mesma cotação.*

PROVA SEM CONSULTA (2 horas)

Questão 1 Sejam dadas duas especificações satisfiáveis S e R, com o mesmo tipo e a mesma pré-condição.

1. Mostre que a asserção $S \vdash R$ é equivalente, neste caso, ao predicado

$$\text{pre-}S(x) \ \wedge \ \text{post-}R(y, x) \quad \Rightarrow \quad \text{post-}S(y, x) \tag{1}$$

universalmente quantificado em x e y.

2. Use o resultado da alínea anterior para mostrar que $S \vdash R$ se verifica para os casos particulares

$S(x : \mathbb{R})\ y : \mathbb{R}$ **pre** $x \geq 0$ **post** $y \leq x + 3$	e	$R(x : \mathbb{R})\ y : \mathbb{R}$ **pre** $x \geq 0$ **post** $y + x \leq 2$

Questão 2 A proeminência da construção `map` K `to` ... em modelos formais de dados leva-nos a considerar tal construção como um tipo de dados de pleno direito, isto é, como um *relator*

$$\begin{array}{ccc} B & \cdots\cdots & K \rightharpoonup B \\ {\scriptstyle R}\downarrow & & \downarrow{\scriptstyle K \rightharpoonup R} \\ C & \cdots\cdots & K \rightharpoonup C \end{array} \tag{2}$$

onde o tipo K está fixo e a relação entre *mappings* $K \rightharpoonup R$ se define com se segue:

$$N(K \rightharpoonup R)M \quad \stackrel{\text{def}}{=} \quad \delta\, M = \delta\, N \ \wedge \ N \cdot M^{\circ} \subseteq R \tag{3}$$

1. Mostre que, vertida para notação VDM-SL *pointwise*, a relação $K \rightharpoonup R$ se transforma em

```
MapRelator(M: map K to B) N: map K to C
post dom M = dom N and forall k in set dom N & post_R(N(k),M(k))
```

2. Mostre que a instância $R := f$ em (3) conduz a $N = f \cdot M$ no corpo de (3), e logo à função de projecção

$$(K \rightharpoonup f)M = f \cdot M \tag{4}$$

Questão 3 Considere o seguinte modelo VDM-SL que especifica, abstractamente, a estrutura de um sistema de informação que, baseado no 'World Wide Web', dá a garantia de **integridade referencial**:

```
WWW  = map Ref to URL           -- URL=Universal Resource Location
       inv M == forall k in set dom M &
                   (exists i in set inds M(k) &
                       is_HyperLink(M(k)(i))) => M(k)(i).link in set dom M;
URL  = seq of Unit;
Unit = PlainText | HyperLink;
PlainText = seq of Word;
Word = seq of char;
HyperLink :: link: Ref
             txt: PlainText;     -- "underlined text"
Ref = token ;
```

Complete o cálculo que se segue e que mostra que o invariante sobre o tipo `WWW` é a conversão para VDM *pointwise* de

$$inv\ M \stackrel{\mathrm{def}}{=} (\in \cdot M)^\circ \preceq M$$

$$\begin{tikzcd}
Ref \arrow[r, "M"] \arrow[dr, "\in \cdot M"'] & (Word^\star + Ref \times Word^\star)^\star \arrow[d, "\in"] \\
& Ref
\end{tikzcd}$$

$$\begin{array}{ll}
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& \delta\,((\in \cdot M)^\circ) \subseteq \delta\, M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (\in \cdot M)^\circ \subseteq \top \cdot M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& k'(\in \cdot M)k \ \Rightarrow\ k(\top \cdot M)k' \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& \langle \exists\, x \ ::\ k' \in x \ \wedge\ x\ M\ k \rangle \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ k' \in M\ k) \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ \langle \exists\, i \ :\ i \in inds(Mk) :\ k' \in (M\ k)i \rangle) \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ \langle \exists\, i \ :\ i \in inds(Mk) :\ k'[\bot\,, \in]\ (M\ k)i \rangle) \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ \langle \exists\, i \ :\ i \in inds(Mk) :\ k'\ (\in \cdot i_2^\circ)\ (M\ k)i \rangle) \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ \langle \exists\, i \ :\ i \in inds(Mk) :\ \langle \exists\, y \ ::\ (M\ k)i = i_2\ y \ \wedge\ k' = \pi_1\ y \rangle\rangle) \ \Rightarrow\ k' \in dom\ M \\
\equiv & \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \} \\
& (k \in dom\ M \ \wedge\ \langle \exists\, i \ :\ i \in inds(Mk) :\ \langle \exists\, y \ ::\ (M\ k)i = i_2\ y \rangle\rangle) \ \Rightarrow\ (\pi_1\ y) \in dom\ M
\end{array}$$

Questão 4 Embora contra-intuitivo, o refinamento

$$
\begin{tikzcd}
A^\star \times A^\star \arrow[rr, bend left, "R"] \arrow[rr, phantom, "\leq"] & & 2^\star \times A^\star \arrow[ll, bend left, "f"]
\end{tikzcd}
\tag{5}
$$

verifica-se mesmo para A com cardinalidade superior a 2. Considere a seguinte abstracção funcional f para (5):

```
f(b,l) == mk_(sel(b,l),sel([ not b(i) | i in set inds b ],l));
```

onde

```
sel(b,l) = [ l(i) | i in set inds l inter inds b & b(i) ];
```

1. Defina duas funções de representação $r \neq r'$ que sejam, na sua opinião, ambas inversas à direita de f. (Não precisa de provar esses factos.) Deduza daí que f não é um isomorfismo.
2. Represente a função auxiliar sel sob a forma de um hilomorfismo de listas e mostre que tal hilomorfismo pode ser transformado num ciclo-`while` em VDM. Não se esqueça de escrever o resultado dessa transformação em sintaxe VDM.

Questão 5 Na especificação formal de um sistema de gestão de conhecimento, escrita em VDM-SL, encontra-se o seguinte modelo para expressões sintáticas arbitrárias:

```
Exp    = Var | Term ;
Var    :: variable: Symbol ;
Term   :: operator: Symbol
          arguments: seq of Exp
          inv t == len t.arguments <= 20 ;
Symbol = seq of char
         inv s == len s <= 10 ;
```

Inspeccionando a sua implementação em SQL, verificamos que a este fragmento de VDM-SL corresponde o seguinte código:

```
CREATE TABLE EXPRESSIONS (
       FatherId  NUMERIC (10) NOT NULL,
       ArgNr     NUMERIC (20) NOT NULL,
       ChildId   NUMERIC (10) NOT NULL
       CONSTRAINT EXPRESSIONS_pk PRIMARY KEY (FatherId,ArgNr)
       );

CREATE TABLE OPERATORS (
       NodeId   NUMERIC (10) NOT NULL,
       Operator CHAR    (10) NOT NULL
       CONSTRAINT OPERATORS_pk PRIMARY KEY(NodeId)
       );

CREATE TABLE VARIABLES (
       NodeId   NUMERIC (10) NOT NULL,
       Variable CHAR    (10) NOT NULL
       CONSTRAINT VARIABLES_pk PRIMARY KEY(NodeId)
       );
```

Concorda com as decisões que foram tomadas nesta codificação? Se a sua resposta é afirmativa, exponha o respectivo processo de cálculo. Se é negativa, indique quais as deficiências encontradas e refaça o respectivo processo de cálculo. Em qualquer dos casos, indique as leis de refinamento de dados que foram aplicadas em cada passo do seu raciocínio e/ou as respectivas relações de abstracção/representação.

Anexo–Algumas leis de cálculo que podem ser úteis

Refinamento algorítmico:

$$S \vdash R \quad \equiv \quad (\delta\, S \subseteq \delta\, R) \ \wedge \ (R \cdot \delta\, S \subseteq S) \tag{6}$$

Ordem de definição de relações:

$$R \preceq S \quad \equiv \quad \delta\, R \subseteq \delta\, S \tag{7}$$

Refinamento de dados:

$$\begin{aligned}
A \rightharpoonup 1 \quad &\cong \quad \mathcal{P}A && (8)\\
A \rightarrow B \times C \quad &\leq \quad (A \rightarrow B) \times (A \rightarrow C) && (9)\\
A \rightarrow B \quad &\leq \quad A \rightharpoonup \mathcal{P}B && (10)\\
(B \times C) \rightharpoonup A \quad &\leq \quad B \rightharpoonup (C \rightharpoonup A) && (11)\\
A \rightharpoonup (D \times (B \rightharpoonup C)) \quad &\leq \quad (A \rightharpoonup D) \times ((A \times B) \rightharpoonup C) && (12)\\
\mu \mathsf{F} \quad &\leq \quad (K \rightharpoonup \mathsf{F}\, K) \times K && (13)
\end{aligned}$$

Hilomorfismos:

$$[\![\, R, S \,]\!] \quad = \quad R \cdot \mathsf{F}\, [\![\, R, S \,]\!] \cdot S \tag{14}$$

$$[\![\, R, S \,]\!] \subseteq T \quad \Leftarrow \quad R \cdot \mathsf{F}\, T \cdot S \subseteq T \tag{15}$$

$$V \cdot [\![\, S, H \,]\!] \subseteq [\![\, T, H \,]\!] \quad \Leftarrow \quad V \cdot S \subseteq T \cdot (\mathsf{G}\, V) \tag{16}$$

$$[\![\, R, S \,]\!]^{\circ} = [\![\, S^{\circ}, R^{\circ} \,]\!] \tag{17}$$

$$V \cdot [\![\, S, R \,]\!] = [\![\, T, R \,]\!] \quad \Leftarrow \quad V \cdot S = T \cdot (\mathsf{F}\, V) \tag{18}$$

$$[\![\, S, R \,]\!] \cdot V = [\![\, S, U \,]\!] \quad \Leftarrow \quad R \cdot V = \mathsf{F}\, V \cdot U \tag{19}$$

Factorização iterativa: para θ associativa, tem-se

$$\begin{aligned}
\langle \mu\, f \ :: \ p \rightarrow b \,,\, \theta \cdot \langle d, f \cdot e \rangle \rangle \quad = \quad & p \rightarrow b \,,\, \theta \cdot (id \times b) \cdot w \cdot \langle d, e \rangle \\
& onde \\
& w = \underline{while}\ (\neg \cdot p \cdot \pi_2)\ \underline{do}\ \langle \theta \cdot (id \times d), e \cdot \pi_2 \rangle
\end{aligned} \tag{20}$$

Sendo (θ, u) um monoide, tem-se

$$\langle \mu\, f \ :: \ p \rightarrow \underline{u} \,,\, \theta \cdot \langle d, f \cdot e \rangle \rangle \quad = \quad \pi_1 \cdot w \cdot \langle \underline{u}, id \rangle \tag{21}$$

onde w é o mesmo que em (20).