Métodos Formais de Programação I

Exame Final (1ª Chamada)
21 de Janeiro de 2005

I
Recorde o seguinte operador sobre correspondências disponível em VDM-SL:

Operator	Name	Semantics description
m `:->` s	Range restrict by	Creates the map consisting of the elements in m whose information value is not in s. s need not be a subset of $rng\, m$

1. Formalize a sua semântica $[\![$`m :-> s`$]\!]$ no cálculo relacional.

Resolução
Uma formalização possível é $[\![\texttt{:->}]\!] = (rng\,[\![m]\!] - [\![s]\!]) \cdot [\![m]\!]$.

2. Com base na formalização que fez na alínea anterior, prove ou refute as seguintes leis:

   (a) $((m \texttt{ :-> } s) \texttt{ :-> } t) = m \texttt{ :-> } (s \cup t)$

Resolução

$$
\begin{array}{ll}
 & [\![((m \texttt{ :-> } s) \texttt{ :-> } t)]\!] \\
= & \quad \{ \text{ definição } \} \\
 & (rng\,[\![m \texttt{ :-> } s]\!] - [\![t]\!]) \cdot [\![m \texttt{ :-> } s]\!] \\
= & \quad \{ \text{ lema auxiliar: } rng\,[\![s \texttt{ :-> } m]\!] = rng\,[\![m]\!] - [\![s]\!], \text{ definição } \} \\
 & ((rng\,[\![m]\!] - [\![s]\!]) - [\![t]\!]) \cdot ((rng\,[\![m]\!] - [\![s]\!]) \cdot [\![m]\!]) \\
= & \quad \{ \text{ composição de coreflexivas é } \cap, \text{ associativadade } \} \\
 & (((rng\,[\![m]\!] - [\![s]\!]) - [\![t]\!]) \cap (rng\,[\![m]\!] - [\![s]\!])) \cdot [\![m]\!] \\
= & \quad \{ \ (R - S) - T \subseteq R - S, \ \cap\text{-cancelamento } \} \\
 & ((rng\,[\![m]\!] - [\![s]\!]) - [\![t]\!]) \cdot [\![m]\!] \\
= & \quad \{ \ (R - S) - T = R - (S \cup T) \ \} \\
 & (rng\,[\![m]\!] - ([\![s]\!] \cup [\![t]\!])) \cdot [\![m]\!] \\
= & \quad \{ \text{ definição } \} \\
 & [\![m \texttt{ :-> } (s \cup t)]\!]
\end{array}
$$

Note-se que $(R - S) - T \subseteq R - S$ se prova facilmente:

$$
\begin{array}{ll}
 & (R - S) - T \subseteq R - S \\
= & \quad \{ \text{ Galois: } X - R \subseteq Y \equiv X \subseteq R \cup Y \ \} \\
 & R - S \subseteq T \cup (R - S) \\
= & \quad \{ \ \cup \text{ cancelamento } \} \\
 & \text{TRUE}
\end{array}
$$

Resolução (continuação)
Verifiquemos, agora, o lema auxiliar:

$$
\begin{array}{ll}
 & rng\,[\![m]\!] - [\![s]\!] \;\subseteq\; rng\,[\![m \mathtt{:->} s]\!] \\
\equiv & \quad \{ \text{ definição } \} \\
 & rng\,[\![m]\!] - [\![s]\!] \;\subseteq\; rng\,((rng\,[\![m]\!] - [\![s]\!]) \cdot [\![m]\!]) \\
\equiv & \quad \{ \text{ Galois } \} \\
 & rng\,[\![m]\!] \;\subseteq\; [\![s]\!] \cup rng\,((rng\,[\![m]\!] - [\![s]\!]) \cdot [\![m]\!]) \\
\equiv & \quad \{ \; rng\,[\![m]\!] - [\![s]\!] \subseteq rng\,[\![m]\!] \text{ (Galois) e o que permite aplicar a lei } X \subseteq rng\,R \Rightarrow rng\,(X \cdot R) \subseteq rng\,R \; \} \\
 & rng\,[\![m]\!] \;\subseteq\; [\![s]\!] \cup rng\,[\![m]\!] \\
= & \quad \{ \; \cup \text{ cancelamento } \} \\
 & \textsc{True}
\end{array}
$$

A direcção oposta decorre trivialmente de $rng\,(R \cdot S) \subseteq rng\,R$.
Por fim verifiquemos o facto $X \subseteq rng\,R \Rightarrow rng\,(X \cdot R) \subseteq rng\,R$.

$$
\begin{array}{ll}
 & X \;\subseteq\; rng\,R \\
\Rightarrow & \quad \{ \text{ monotonia } \} \\
 & X \cdot R \;\subseteq\; rng\,R \cdot R \\
\equiv & \quad \{ \; rng\,S \cdot S = S \} \\
 & X \cdot R \;\subseteq\; R \\
\Rightarrow & \quad \{ \text{ monotonia } \} \\
 & rng\,(X \cdot R) \;\subseteq\; rng\,R
\end{array}
$$

(b) $m \mathtt{:->} \emptyset \;=\; m$

Resolução

$$
\begin{array}{ll}
 & [\![m \mathtt{:->} \emptyset]\!] \\
= & \quad \{ \text{ definição } \} \\
 & (rng\,[\![m]\!] - [\![\emptyset]\!]) \cdot [\![m]\!] \\
= & \quad \{ \text{ conjuntos como co-reflexivas } \} \\
 & (rng\,[\![m]\!] - \bot) \cdot [\![m]\!] \\
= & \quad \{ \; R - \bot = R \; \} \\
 & rng\,[\![m]\!] \cdot [\![m]\!] \\
= & \quad \{ \; rng\,S \cdot S = S \; \} \\
 & [\![m]\!]
\end{array}
$$

Note-se que $R - \bot = R$ se verifica por indirecção:

$$
\begin{array}{ll}
 & R - \bot \;\subseteq\; X \\
\equiv & \quad \{ \text{ Galois } \} \\
 & R \;\subseteq\; \bot \cup X \\
\equiv & \quad \{ \; \bot \text{ neutro de } \cup \; \} \\
 & R \;\subseteq\; X
\end{array}
$$

II

Partindo da definição *pointfree* de injectividade, mostre que a *regra de Leibniz*

$$x = y \Rightarrow fx = fy \tag{1}$$

pode ser generalizada a uma equivalência se a função f for injectiva.

Resolução

Uma função é injectiva se $ker\, f = \mathsf{id}$. Então,

$$\begin{array}{cl} & ker\, f \;=\; \mathsf{id} \\ \equiv & \quad \{ \text{ definição de kernel } \} \\ & f^\circ \cdot f \;=\; \mathsf{id} \\ \equiv & \quad \{ \text{ introdução de variáveis} \} \\ & x\,(f^\circ \cdot f)\,y \;=\; x \;=\; y \\ \equiv & \quad \{ \text{ shunting } \} \\ & fx \;=\; fy \;=\; x \;=\; y \end{array}$$

III

O *complemento* de uma relação R é uma relação V que verifica as seguintes propriedades:

$$R \cup V \;=\; \top \qquad \text{e} \qquad R \cap V \;=\; \bot \tag{2}$$

1. Suponha que duas relações S e T satisfazem as duas equações acima. Complete

$$\begin{array}{cl} & S \\ = & \quad \{ \; R \cup T = \top \; \} \\ & \ldots \\ = & \quad \{ \; \ldots \; \} \\ & (S \cap R) \cup (S \cap T) \\ \subseteq & \quad \{ \; \ldots \; \} \\ & (S \cap R) \cup T \\ = & \quad \{ \; \ldots \; \} \\ & T \end{array}$$

Resolução

$$\begin{array}{cl} & S \\ = & \quad \{ \; R \cup T = \top,\ \top \text{ neutro de } \cap \; \} \\ & S \cap (R \cup T) \\ = & \quad \{ \; \cap \text{ é adjunto inferior } \} \\ & (S \cap R) \cup (S \cap T) \\ \subseteq & \quad \{ \; S \cap T \subseteq T, \text{ monotonia } \} \\ & (S \cap R) \cup T \\ = & \quad \{ \; R \cap S = \bot,\ \bot \text{ neutro de } \cup \; \} \\ & T \end{array}$$

2. A partir da alínea anterior conclua que cada relação R tem um *único* complemento (que designaremos, de seguida, por $\neg R$) e que $\neg\neg R = R$.

Resolução
A resolução é imediata: basta notar que pelo raciocínio anterior concluimos ainda $T \subseteq S$ e, logo, $T = S$ o que dá a unicidade do complemento. O segundo facto decorre da definição de complemento (2) ser simétrica nos dois argumentos. Assim, R e $\neg\neg R$ são complementos de $\neg R$ e, logo, iguais, pela unicidade dos complementos.

3. Prove a seguinte regra de *shunting* para o complemento de uma relação

$$R \subseteq S \cup T \;\equiv\; R \cap \neg S \subseteq T \tag{3}$$

Resolução

$$\begin{array}{ll}
 & R \subseteq S \cup T \\
\Rightarrow & \quad \{ \text{ monotonia } \} \\
 & \neg S \cap R \subseteq \neg S \cap (S \cup T) \\
\equiv & \quad \{ \text{ } \cap \text{ é adjunto inferior } \} \\
 & \neg S \cap R \subseteq (\neg S \cap S) \cup (\neg S \cap T) \\
\equiv & \quad \{ \text{ } \neg S \cap S = \bot,\ \bot \text{ neutro de } \cup \} \\
 & \neg S \cap R \subseteq \neg S \cap T \\
\Rightarrow & \quad \{ \text{ } \neg S \cap T \subseteq T, \text{ monotonia } \} \\
 & \neg S \cap R \subseteq T
\end{array}$$

Verificamos, assim, que $R \subseteq S \cup T \Rightarrow \neg S \cap R \subseteq T$. Por dualidade, vem,

$$R \supseteq S \cap T \Rightarrow \neg S \cup R \supseteq T$$

Instanciando esta equação R por T, S por $\neg S$ e T por R vem

$$T \supseteq \neg S \cap R \Rightarrow \neg\neg S \cup T \supseteq R$$

que por $\neg\neg S = S$ re-escreve em

$$R \subseteq S \cup T \Leftarrow \neg S \cap R \subseteq T$$

concluindo-se por *ping-pong*.

4. Utilizando a regra de *shunting* que demonstrou na alínea anterior, verifique a seguinte conexão de Galois:

$$R \subseteq \neg S \;\equiv\; \neg R \supseteq S \tag{4}$$

e enuncie as leis de preservação de infímos e supremos dela derivadas.

Resolução
A conexão de Galois resulta de

$$
\begin{array}{ll}
 & R \subseteq \neg S \\
\equiv & \quad \{ \ \bot \text{ neutro de } \cup \ \} \\
 & R \subseteq \neg S \cup \bot \\
\equiv & \quad \{ \ \text{lei de shunting provada na alínea anterior} \ \} \\
 & \neg\neg S \cap R \subseteq \bot \\
\equiv & \quad \{ \ \neg\neg X = X, \text{ comutatividade de } \cup \ \} \\
 & \neg\neg R \cap S \subseteq \bot \\
\equiv & \quad \{ \ \text{lei de shunting provada na alínea anterior} \ \} \\
 & S \subseteq \neg R \cup \bot \\
\equiv & \quad \{ \ \bot \text{ neutro de } \cup \ \} \\
 & S \subseteq \neg R
\end{array}
$$

Os resultados de preservação associados a esta conexão são as leis de de Morgan:

$$
\begin{array}{rcl}
\neg(R \cup S) & = & \neg R \cap \neg S \\
\neg(R \cap S) & = & \neg R \cup \neg S \\
\neg\top & = & \bot \\
\neg\bot & = & \top
\end{array}
$$

IV
As técnicas de *slicing*, muito populares na análise de código legado, baseiam-se na construção de um grafo de dependências entre diversas entidades computacionais (por exemplo, módulos, procedimentos ou variáveis) extraídos do código em consideração. O grafo é posteriomente usado para determinar as dependências transitivas de uma determinada entidade.

Para cada nodo nodo n, a operação de *forward slicing*, que representamos por $G \otimes n$, retorna o subgrafo dos nodos que dependem directa ou indirectamente de n. Dualmente, uma *backward slicing*, representada por $n \oplus G$, corresponde ao subgrafo dos nodos dos quais n directa ou indirectamente depende. Suponha que a noção de nodo é especificada pelo seguinte tipo em VDM-SL

```
Nd  ::  T:NType     L:SourceCodeLocation     I:Information
```

e que o grafo de dependências é dado por uma relação $G : \texttt{Nd} \longleftarrow \texttt{Nd}$, onde nGm significa *nodo n depende do nodo m*. O significado concreto dessa dependência é, na prática, função dos tipos de n e m. Suponha que alguém propôs a seguinte definição de *forward slice* de G relativa ao nodo n:

$$G \otimes n \ \triangleq \ \mu\, x \,.\, (G \cdot \lfloor n \rceil \ \cup \ \mathsf{next}_G\, x) \tag{5}$$

onde $\mathsf{next}_G\, x = G \cdot rng\, x$ e para cada $v \in V$, $\lfloor v \rceil : V \longleftarrow V$ é a co-reflexiva singular $v \lfloor v \rceil v$.

1. Diga, justificando, se a definição proposta capta adequadamente a noção intuitiva de *forward slice* de G relativa a n, corrigindo-a se tal achar necessário.

2. Complete a definição

$$n \oplus G \ \triangleq \ \ldots \otimes \ldots \tag{6}$$

Resolução

$$n \oplus G \;\triangleq\; G^{\circ} \otimes n$$

3. Complete as justificações do seguinte raciocínio sobre a definição (5):

$$\begin{array}{ll}
 & G \otimes n \\
= & \quad \{ \ \ldots \ \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (G \cdot rng\,(G \cdot \lfloor n \rceil \cup x)) \\
= & \quad \{ \ \ldots \ \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (G \cdot (rng\,(G \cdot \lfloor n \rceil) \cup rng\, x)) \\
= & \quad \{ \ \ldots \ \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (\mathsf{next}_G\,(G \cdot \lfloor n \rceil) \cup \mathsf{next}_G\, x\,)
\end{array}$$

Resolução

$$\begin{array}{ll}
 & G \otimes n \\
= & \quad \{ \text{ definição, rolling rule com } g\,x \;=\; G \cdot \lfloor n \rceil \cup x \text{ e } h\,x \;=\; \mathsf{next}_G\, x \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (G \cdot rng\,(G \cdot \lfloor n \rceil \cup x)) \\
= & \quad \{ \ rng \ \text{ preserva } \cup \ \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (G \cdot (rng\,(G \cdot \lfloor n \rceil) \cup rng\, x)) \\
= & \quad \{ \ \cdot \text{ distribui sobre } \cup\text{, definição } \} \\
 & G \cdot \lfloor n \rceil \cup \mu\, x \,.\, (\mathsf{next}_G\,(G \cdot \lfloor n \rceil) \cup \mathsf{next}_G\, x\,)
\end{array}$$

4. Com base na alínea anterior especifique em VDM-SL as operações de *forward slicing* e *backward slicing* a partir de um nodo.

5. Como modificaria a definição de *forward slicing* de modo a parametriza-la por um conjunto $V \subseteq$ `NType` de tipos de nodo, garantindo assim que no subgrafo resultante apenas aparecessem nodos dos tipos em V? Reflicta esta alteração na especificação em VDM-SL deste problema.

Resolução (primeira parte)

A definição do operador torna-se paramétrica em V. Seja $\phi_V = \in_V \cdot \pi_1$ o predicado sobre os nodos que realiza a restrição sobre os tipos permitidos (introduzindo-se variáveis ϕ_V vem $\phi_V\, n \;=\; \pi_1(n) \in V$). Então,

$$G \otimes_V n \;\triangleq\; \mu\, x \,.\, (G \cdot \lfloor n \rceil \cup G \cdot (rng\, x \cap [\![\phi_V]\!]))$$