Métodos Formais em Engenharia de Software

1.º Ano de Mestrado de Informática e de Eng. Informática da Universidade do Minho
Ano Lectivo de 2009/10

Prova de avaliação individual — 18 de Fevereiro 2009
09h00
Sala DI 1.08

NB: *Esta prova consta de **8** alíneas todas com as mesma cotação. A questão 3 deve ser lida antes da questão 4, e esta antes da 5, podendo ser resolvidas por qualquer ordem apesar disso.*

PROVA COM CONSULTA (2 horas)

Questão 1 Apresenta-se em baixo o início do cálculo de uma de duas igualdades do cálculo relacional,

$$R / \bot = \top \tag{1}$$
$$\top / R = \top \tag{2}$$

usando o princípio da igualdade indirecta. Após completar esse cálculo, (a) apresente o cálculo semelhante para a outra igualdade acima e (b) indique que leis da quantificação universal é que essas igualdades registam, em notação-PF.

Segue-se o cálculo de (1), a completar:

$$
\begin{array}{ll}
 & R / \bot = \top \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \langle \forall\, X \ :: \ X \subseteq R / \bot \ \Leftrightarrow \ X \subseteq \top \rangle \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \vdots \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & true
\end{array}
$$

Questão 2 Uma das funcionalidades básicas da programação funcional é aquela que combina duas listas numa só, processando-as elemento a elemento usando uma função que é passada como parâmetro. Em Haskell essa função dá pelo nome

```
zipWith :: (a -> b -> c) -> [a] -> [b] -> [c]
```

Por exemplo, `zipWith(+) [1,2] [3,4,5]` resulta na lista `[4,6]`. Se se submeter o tipo de `zipWith` ao calculador de *teoremas grátis* disponibilizado em `http://linux.tcs.inf.tu-dresden.de/~voigt/ft/`, obter-se-á, para o caso em que todas as relações são funções, o corolário

```
forall r :: t1 -> t2.
 forall h :: t3 -> t4.
  forall t :: t5 -> t6.
   forall g :: t1 -> t3 -> t5.
    forall f :: t2 -> t4 -> t6.
     (forall x :: t1. forall y :: t3. t (g x y) = f (r x) (h y))
     ==> (forall m :: [t1].
           forall v :: [t3]. map t (z g m v) = z f (map r m) (map h v))
```

No cálculo deste corolário que se segue há quatro passos omitidos e quatro justificações por dar. Complete estas e apresente aqueles, justificados também:

$$
\begin{array}{ll}
 & zipWith :: c^\star \leftarrow b^\star \leftarrow a^\star \leftarrow (c \leftarrow b \leftarrow a) \\
\Leftrightarrow & \quad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \}
\end{array}
$$

$$zipWith\ (R_{c^\star \leftarrow b^\star \leftarrow a^\star \leftarrow (c \leftarrow b \leftarrow a)})\ zipWith$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$zipWith\ (R_{c^\star \leftarrow b^\star \leftarrow a^\star} \leftarrow R_{c \leftarrow b \leftarrow a})\ zipWith$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$zipWith \cdot R_{c \leftarrow b \leftarrow a} \subseteq R_{c^\star \leftarrow b^\star \leftarrow a^\star} \cdot zipWith$$

$$\Leftrightarrow \quad \{ \text{ 4 passos de cálculo omitidos } \}$$

$$(y\ R_a\ x\ \wedge\ w\ R_b\ z \Rightarrow (f\ y\ w) R_c (g\ x\ z))\ \wedge\ l\ R_{a^\star} m\ \wedge\ k R_{b^\star} p \Rightarrow (zipWith\ f\ l\ k) R_{c^\star} (zipWith\ g\ m\ p)$$

$$\Rightarrow \quad \{\ R_a, R_b, R_c := r, h, t\ ;\ f^\star = map\ f, \text{ para qualquer } f\ \}$$

$$f\ (r\ x)\ (h\ z) = t(g\ x\ z)\ \wedge\ l = map\ r\ m\ \wedge\ k = map\ h\ p \Rightarrow (zipWith\ f\ l\ k) = map\ t\ (zipWith\ g\ m\ p)$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$f\ (r\ x)\ (h\ z) = t(g\ x\ z)\ \Rightarrow\ zipWith\ f\ (map\ r\ m)\ (map\ h\ p) = map\ t\ (zipWith\ g\ m\ p)$$

Questão 3 Dados dois tipos A e B, construa-se a sua *união disjunta* definindo $A + B \triangleq \{i_1\ a \mid a \in A\} \cup \{i_2\ b \mid b \in B\}$, onde $i_1\ a \triangleq (1, a)$ e $i_2\ b \triangleq (2, b)$ são designadas as *injecções* dessa construção, que são ortogonais entre si: $i_2^\circ \cdot i_1 = \bot$. Sobre esta construção define-se o combinador relacional *"alternativa"*

$$[R\ , S] \quad \triangleq \quad R \cdot i_1^\circ\ \cup\ S \cdot i_2^\circ \tag{3}$$

que goza de muitas propriedades, por exemplo

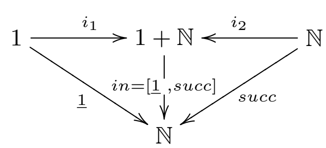
$$[i_1\ , i_2] \quad = \quad id \tag{4}$$

$$[R\ , S] \cdot [T\ , U]^\circ \quad = \quad (R \cdot T^\circ) \cup (S \cdot U^\circ) \tag{5}$$

$$X \cdot [R\ , S] \quad = \quad [X \cdot R\ , X \cdot S] \tag{6}$$

$$[R\ , S] \subseteq [X\ , Y] \quad \Leftrightarrow \quad \left\{ \begin{array}{l} R \subseteq X \\ S \subseteq Y \end{array} \right. \tag{7}$$

Em baixo mostra-se o diagrama da função $in = [\underline{1}\ , succ]$ que exprime a forma como se constroem os números naturais, onde $\underline{1}$ designa a função constante que dá sempre 1 como resultado e $succ\ n \triangleq n + 1$ (o tipo 1 é habitado por um só elemento, fixado à partida).



(8)

Verifica-se que in é um isomorfismo, logo uma função injectiva e sobrejectiva.

1. Um facto assumido nas aulas,

$$succ^\circ \cdot \underline{1} = \bot \tag{9}$$

mostra-se essencial para que in (8) seja injectiva. Complete o respectivo processo de cálculo:

$$in^\circ \cdot in \subseteq id$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$[in^\circ \cdot \underline{1}\ , in^\circ \cdot succ] \subseteq [i_1\ , i_2]$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$\left\{ \begin{array}{l} in^\circ \cdot \underline{1} \subseteq i_1 \\ in^\circ \cdot succ \subseteq i_2 \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$\left\{ \begin{array}{l} i_1 \cdot \underline{1}^\circ \cdot \underline{1} \cup i_2 \cdot succ^\circ \cdot \underline{1} \subseteq i_1 \\ i_1 \cdot \underline{1}^\circ \cdot succ \cup i_2 \cdot succ^\circ \cdot succ \subseteq i_2 \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \}$$

$$
\left\{\begin{array}{l} i_1 \cdot \underline{1}^\circ \cdot \underline{1} \subseteq i_1 \\ i_2 \cdot succ^\circ \cdot \underline{1} \subseteq i_1 \\ i_1 \cdot \underline{1}^\circ \cdot succ \subseteq i_2 \\ i_2 \cdot succ^\circ \cdot succ \subseteq i_2 \end{array}\right.
$$

$\Leftrightarrow$ { ..... }

$$
\left\{\begin{array}{l} \underline{1}^\circ \cdot \underline{1} \subseteq \ker i_1 \\ succ^\circ \cdot \underline{1} \subseteq i_2^\circ \cdot i_1 \\ \underline{1}^\circ \cdot succ \subseteq i_1^\circ \cdot i_2 \\ succ^\circ \cdot succ \subseteq \ker i_2 \end{array}\right.
$$

$\Leftrightarrow$ { ..... }

$$
\left\{\begin{array}{l} \underline{1}^\circ \cdot \underline{1} \subseteq id \\ succ^\circ \cdot \underline{1} \subseteq i_2^\circ \cdot i_1 \\ succ^\circ \cdot succ \subseteq id \end{array}\right.
$$

$\Leftrightarrow$ { ..... }

$$
\left\{\begin{array}{l} succ^\circ \cdot \underline{1} = \bot \\ succ \text{ é injectiva} \end{array}\right.
$$

2. Recorra à propriedade (5) para mostrar que outro facto a que se aludiu nas aulas,

$$img\ \underline{1} \cup img\ succ = id \tag{10}$$

mais não é do que a declaração que in é sobrejectiva.

Questão 4 Como se viu nas aulas, a modelação de sequências no módulo `sequence.als` do Alloy,

```
sig Seq { seqElems: SeqIdx → lone elem }
```

sugere o tipo paramétrico

$$\begin{array}{l} Seq\ A \triangleq \mathbb{N} \longrightarrow\!\!\!\!\!\!\rightarrow A \\ \textbf{inv}\ L \triangleq noHoles\ L \end{array} \tag{11}$$

onde

$$noHoles\ L \quad \triangleq \quad L \cdot succ \subseteq \top \cdot L \tag{12}$$

sobre o qual se definem as operações

$$tail\ L \quad \triangleq \quad L \cdot succ \tag{13}$$

$$head\ L \quad \triangleq \quad L \cdot img\ \underline{1} \tag{14}$$

$$c : L \quad \triangleq \quad \underline{c} \cdot \underline{1}^\circ \cup L \cdot succ^\circ \tag{15}$$

1. Mostre que a definição (15) pode (com vantagem) ser substituída por

$$c : L \quad \triangleq \quad [\underline{c}\ , L] \cdot in^\circ \tag{16}$$

onde in é o isomorfismo representado no diagrama (8).

2. Essa vantagem pode ser apreciada na prova de que (15) preserva o invariante (12), feita nas aulas, a partir da altura em que se passa a calcular o termo

$$L \subseteq \top \cdot (c : L) \tag{17}$$

Apresente as justificações para o seguinte cálculo alternativo dessa parte da prova, baseado na definição (16):

$L \subseteq \top \cdot (c : L)$

$\Leftrightarrow$ { ..... }

$L \subseteq \top \cdot [\underline{c}\ , L] \cdot in^\circ$

$\Leftrightarrow$ { ..... }

$$
\begin{array}{ll}
& L \cdot in \subseteq [\top \cdot \underline{c}\,, \top \cdot L] \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& [L \cdot \underline{1}\,, L \cdot succ] \subseteq [\top \cdot \underline{c}\,, \top \cdot L] \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \left\{ \begin{array}{l} L \cdot \underline{1} \subseteq \top \cdot \underline{c} \\ L \cdot succ \subseteq \top \cdot L \end{array} \right. \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \left\{ \begin{array}{l} L \cdot \underline{1} \subseteq \top \\ noHoles\ L \end{array} \right. \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& noHoles\ L
\end{array}
$$

Questão 5 Suponha que $A \xleftarrow{\sqsubseteq} A$ é uma ordem total sobre os elementos das sequências declaradas em (11), e que $\top$ no invariante (12) é substituído por $\sqsubseteq$, cf:

$$
noHoles'\ L \quad \triangleq \quad L \cdot succ \subseteq \sqsubseteq \cdot L \tag{18}
$$

Que propriedade adicional é que $noHoles'$ força nas sequências de que é invariante? Identificada essa propriedade, que outro nome escolheria para $noHoles'$? Justifique a sua resposta introduzindo variáveis em (18) e simplificando.

Questão 6 A asserção do fragmento de código Alloy que se segue

```
sig A { f : one B }
sig B {}

assert GC { all x: set A, y: set B | x·f in y ⇔ x in f·y }
```

traduz uma "regra de *shunting*" válida nessa linguagem. Partindo das regras semânticas que se seguem para a notação Alloy,

$$
[\![s.R]\!] = \rho\,([\![R]\!] \cdot [\![s]\!]) \tag{19}
$$
$$
[\![s]\!] = \Phi_s \tag{20}
$$
$$
[\![R.s]\!] = [\![s.\tilde{\ }R]\!] \tag{21}
$$
$$
[\![\tilde{\ }R]\!] = [\![R]\!]^\circ \tag{22}
$$

em que s é um conjunto e R uma relação binária, complete o cálculo que se segue da referida regra, feito à luz dessa semântica:

$$
\begin{array}{ll}
& [\![x.f]\!] \subseteq [\![y]\!] \;\Leftrightarrow\; [\![x]\!] \subseteq [\![f.y]\!] \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \rho\,([\![f]\!] \cdot [\![x]\!]) \subseteq [\![y]\!] \;\Leftrightarrow\; [\![x]\!] \subseteq [\![y.\tilde{\ }f]\!] \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \rho\,([\![f]\!] \cdot \Phi_x) \subseteq \Phi_y \;\Leftrightarrow\; \Phi_x \subseteq \rho\,([\![f]\!]^\circ \cdot \Phi_y) \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& [\![f]\!] \cdot \Phi_x \subseteq \Phi_y \cdot \top \;\Leftrightarrow\; \Phi_x \subseteq img\,([\![f]\!]^\circ \cdot \Phi_y) \cap id \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& [\![f]\!] \cdot \Phi_x \subseteq \Phi_y \cdot \top \cap [\![f]\!] \;\Leftrightarrow\; \Phi_x \subseteq [\![f]\!]^\circ \cdot \Phi_y \cdot \Phi_y^\circ \cdot [\![f]\!] \\
\Leftrightarrow & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& [\![f]\!] \cdot \Phi_x \subseteq \Phi_y \cdot [\![f]\!] \;\Leftrightarrow\; [\![f]\!] \cdot \Phi_x \subseteq \Phi_y \cdot [\![f]\!]
\end{array}
$$
