Métodos Formais em Engenharia de Software

1.º Ano de Mestrado (Eng. Informática / Matemática e Computação)
Universidade do Minho
Ano Lectivo de 2012/13

Teste individual — 01 de Março de 2013
10h00
Sala DI 1.08

NB: *Esta prova consta de* ***8*** *alíneas todas com as mesma cotação. Os alunos que desejem responder directamente sobre o enunciado da* ***Questão 4*** *devem ter o cuidado de rubricar as respectiva folha e indicarem o seu* ***número***.

PROVA COM CONSULTA (2 horas)

Questão 1 (1 alínea) Como sabe, uma função f é constante sse $ker\ f = \top$. Este conceito pode estender-se a uma qualquer relação R, da forma seguinte: R dir-se-á *constante* sse coincidir com o seu rectângulo, $R \,\square\, R = R$, onde

$$R \,\square\, S \quad \triangleq \quad R \cdot \top \cdot S \tag{F1}$$

Mostre que as duas definições coincidem para funções. (**NB:** atente que, para toda a função f, $\top \cdot f = \top$.)

RESOLUÇÃO:

$$\begin{array}{ll} & f \,\square\, f = f \\ \equiv & \quad \{\ \text{definição (F1)}\ \} \\ & f \cdot \top \cdot f = f \\ \equiv & \quad \{\ \text{igualdade de funções: } f = g \equiv f \subseteq g \text{ (56)}\ \} \\ & f \cdot \top \cdot f \subseteq f \\ \equiv & \quad \{\ \text{shunting (54)}\ \} \\ & \top \cdot f \subseteq f^\circ \cdot f \\ \equiv & \quad \{\ \top \cdot f = \top \text{ (acima) ; kernel: } ker\ f = f^\circ \cdot f\ \} \\ & \top = ker\ f \end{array}$$

□

Questão 2 (1 alínea) Recorde um dos desafios de Alcuino de York — *Propositio de homine et capra et lvpo* — que foi dado nas aulas como exemplo de modelação relacional de situações da vida real. Recorde, em particular, o diagrama

$$\begin{array}{ccc} Being & \xleftarrow{CanEat} & Being \\ {\scriptstyle where}\downarrow & \subseteq & \downarrow{\scriptstyle \underline{Farmer}} \\ Bank & \xleftarrow[where]{} & Being \end{array} \tag{F2}$$

que descreve o invariante do problema: *se alguém pode comer alguém, então* $Farmer$ *lá estará para o impedir.*

Suponha agora os seguintes "enganos" na formulação (F2) desse invariante:

1. As setas $CanEat$ e $\underline{Farmer}$ estão trocadas entre si.
2. Em lugar das seta $CanEat$ está a seta $SameBank$. (Recorde que $SameBank \triangleq ker\ where$.)
3. Em lugar da seta $\underline{Farmer}$ está a seta $CanEat$.

Mostre que não é preciso recorrer ao Alloy para verificar que uma das três situações acima é uma trivialidade e que as outras bloqueiam o puzzle. Justifique a sua resposta raciocinando sobre o diagrama em cada caso.

RESOLUÇÃO:

1. Tem-se:

$$\begin{array}{ll} & where \cdot \underline{Farmer} \subseteq where \cdot (Eat \cap SameBank) \\ \equiv & \quad \{ \text{ definição: } SameBank = ker\ where \text{ ; ver NB abaixo } \} \\ & \underline{Farmer} \subseteq (ker\ where \cdot Eat) \cap (ker\ where) \\ \equiv & \quad \{ \text{ definição: } SameBank = ker\ where \text{ ; shunting (54) ; função constante } \} \\ & \underline{Farmer} \subseteq SameBank \cdot Eat\ \wedge\ \underline{where\ Farmer} = where \end{array}$$

   Logo, o puzzle fica bloqueado pois $where$ é forçada a ser constante (ninguém pode sair da margem onde está $Farmer$). NB: a igualdade usada acima

$$(ker\ f) \cdot (S \cap ker\ f) = (ker\ f \cdot S) \cap (ker\ f)$$

   deriva-se facilmente da lei (226) do exercício 107.

2. Tem-se:

$$\begin{array}{ll} & where \cdot SameBank \subseteq where \cdot \underline{Farmer} \\ \equiv & \quad \{ \text{ definição: } SameBank = ker\ where \text{ ; função constante } \} \\ & where \cdot where^{\circ} \cdot where \subseteq \underline{where\ Farmer} \\ \equiv & \quad \{ \text{ difuncionalidade: } f \cdot f^{\circ} \cdot f = f \} \\ & where = \underline{where\ Farmer} \end{array}$$

   A situação é idêntica à anterior.

3. Tem-se $where \cdot CanEat \subseteq where \cdot CanEat$ sempre verdadeira pois a inclusão é reflexiva.

□

Questão 3 (1 alínea) Considere a função de ordem superior $const : a \to b \to a$ que, dado um qualquer habitante x do tipo a, produz a função constante $const\ x$ que dá sempre x como resultado. Mostre que as igualdades

$$const(f\ x) = f \cdot (const\ x) \quad \text{(F3)}$$
$$(const\ x) \cdot f = const\ x \quad \text{(F4)}$$
$$(const\ x)^{\circ} \cdot (const\ x) = \top \quad \text{(F5)}$$

decorrem do *teorema grátis* de $const$.

RESOLUÇÃO: Teorema grátis do tipo $t = (a \leftarrow b) \leftarrow a$:

$$
\begin{array}{ll}
& const(R_{(a\leftarrow b)\leftarrow a})const \\
\equiv & \{\ R_{(a\leftarrow b)\leftarrow a} = R_a \leftarrow R_{(a\leftarrow b)} \text{ ; seta de Reynolds (92) } \} \\
& const \cdot R_a \subseteq R_{(a\leftarrow b)} \cdot const \\
\equiv & \{\ \text{shunting (54) ; } R_{a\leftarrow b} = R_a \leftarrow R_b\ \} \\
& R_a \subseteq const^\circ \cdot (R_a \leftarrow R_b) \cdot const \\
\equiv & \{\ \text{introdução de } \forall y, x \text{ ; regra do ``guardanapo'' (47) } \} \\
& y(R_a)x \ \Rightarrow\ (const\ y) \cdot R_b \subseteq R_a \cdot (const\ x)
\end{array}
$$

Caso (F3): faça-se $R_a = f$ e $R_b = id$ e tem-se

$$
\begin{array}{ll}
& y = f\ x \ \Rightarrow\ (const\ y) \subseteq f \cdot (const\ x) \\
\equiv & \{\ \text{one point-}\forall \text{ ; igualdade de funções: } f = g \equiv f \subseteq g \text{ (56) } \} \\
& (F3)
\end{array}
$$

Caso (F4): simétrico ao anterior, com $R_b = f$ e $R_a = id$, tendo-se

$$
\begin{array}{ll}
& y = x \ \Rightarrow\ (const\ y) \cdot f \subseteq const\ x \\
\equiv & \{\ \text{one point-}\forall \text{ ; igualdade de funções: } f = g \equiv f \subseteq g \text{ (56) } \} \\
& (F4)
\end{array}
$$

Caso (F5): faça-se $R_a = id$ e $R_b = \top$:

$$
\begin{array}{ll}
& y = x \ \Rightarrow\ (const\ y) \cdot \top \subseteq const\ x \\
\equiv & \{\ \text{one point-}\forall\ \} \\
& (const\ x) \cdot \top \subseteq const\ x \\
\equiv & \{\ \text{shunting (54) } \} \\
& \top \subseteq (const\ x)^\circ \cdot (const\ x) \\
\equiv & \{\ X \subseteq \top \text{, qualquer que seja } X\ \} \\
& \top = (const\ x)^\circ \cdot (const\ x)
\end{array}
$$

□

Questão 4 (2 alíneas) Provam-se facilmente (eg. por igualdade indirecta) os factos

$$R/id = R \qquad \text{(F6)}$$
$$R/(S \cup Q) = (R/S) \cap (R/Q) \qquad \text{(F7)}$$
$$R/(f^\circ \cdot S) = (R/S) \cdot f \qquad \text{(F8)}$$

em que os dois primeiros captam, na álgebra relacional, as regras *one-point* (9) e *splitting* (27) do cálculo de quantificadores de Eindhoven, respectivamente.

1. Recorra aos factos dados (entre outros) para justificar os seguintes passos de um cálculo que mostra que, sendo R uma **pré-ordem**, então $R/R = R$:

$$
\begin{array}{ll}
& R/R = R \\
\equiv & \{\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \}
\end{array}
$$

$$
\begin{array}{ll}
& R/R \subseteq R \ \ \wedge \ \ R \subseteq R/R \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (R/R) \cap R = R/R \ \ \wedge \ \ R \cdot R \subseteq R \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (R/R) \cap (R/id) = R/R \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& R/(R \cup id) = R/R \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& R/R = R/R \\
\equiv & \quad \{ \text{ igualdade é reflexiva } \} \\
& \textsc{True}
\end{array}
$$

2. As propriedades $\langle \forall\, n \ :: \ 0 \leq n \rangle$ e $\langle \forall\, n \ :: \ n \leq 0 \equiv n = 0 \rangle$, válidas para qualquer número natural $n \in \mathbb{N}_0$, podem-se escrever, respectivamente, sob a forma:

$$
\begin{aligned}
\underline{0}^{\circ} \cdot \leq \quad &= \quad \top && \text{(F9)} \\
\leq \cdot\, \underline{0} \quad &= \quad \underline{0} && \text{(F10)}
\end{aligned}
$$

Sendo assim 0 o menor de todos os números naturais, não surpreende a igualdade

$$
\top \upharpoonright \leq \quad = \quad \underline{0} \qquad \text{(F11)}
$$

em que $R \upharpoonright S$ (232) exprime a optimização ("shrinking") de R por S. Apresente justificações para o seguinte cálculo de (F11):

$$
\begin{array}{ll}
& \top \upharpoonright \leq \, = \underline{0} \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \top \cap (\leq / \top) = \underline{0} \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \leq / (\underline{0}^{\circ} \cdot \leq) = \underline{0} \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& (\leq / \leq) \cdot \underline{0} = \underline{0} \\
\equiv & \quad \{ \ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
& \underline{0} = \underline{0}
\end{array}
$$

RESOLUÇÃO:

1. (a) inclusão cíclica (68), vulg. "ping-pong";
   (b) $X \subseteq Y \equiv X \cap Y = X$; GC da divisão (194) ;
   (c) $R \cdot R \subseteq R$, pois pré-ordem R é transitiva; (F6);
   (d) (F7);
   (e) $id \subseteq R$ pois R é pré-ordem, logo $R \cup id = R$.

2. (a) definição de "shrink" (231) ; $\top^{\circ} = \top$
   (b) $\top \cap R = R$; (F9);
   (c) (F8);
   (d) $\leq / \leq \, = \, \leq$ pela alínea anterior, pois $\leq$ é uma pré-ordem ; (F10)

□

Questão 5 (2 alíneas) O domínio $\delta\, R = ker\, R \cap id$ de uma relação R é uma construção universal que satisfaz a propriedade

$$\delta\, R \subseteq \Phi \quad \equiv \quad R \subseteq \top \cdot \Phi \tag{F12}$$

(conecção de Galois) em que $\top$ pode ser substituída, como sabe, por R.

1. Demonstre a igualdade

$$\top \cdot (\top \cdot R \cap S) \quad = \quad \top \cdot R \cap \top \cdot S \tag{F13}$$

2. O facto

$$\delta\, R \quad = \quad \top \cdot R \cap id \tag{F14}$$

fornece uma definição alternativa para o domínio de uma relação. Demonstre-o por inclusão cíclica (vulg. "ping-pong").

RESOLUÇÃO:

1. Tem-se:

$$\begin{array}{ll} & \top \cdot (\top \cdot R \cap S) = \top \cdot R \cap \top \cdot S \\ \equiv & \quad \{\ \top \cdot \top = \top\ \} \\ & \top \cdot (\top \cdot R \cap S) = \top \cdot (\top \cdot R) \cap \top \cdot S \\ \Leftarrow & \quad \{\ \text{(226) — distributividade de composição por intersecção}\ \} \\ & (ker\, \top) \cdot (\top \cdot R) \subseteq (\top \cdot R) \ \vee\ (ker\, \top) \cdot S \subseteq S \\ \Leftarrow & \quad \{\ \top \cdot \top = \top = \top^{\circ}\ \} \\ & \top \cdot R \subseteq \top \cdot R \end{array}$$

2. *Ping*:

$$\begin{array}{ll} & \delta\, R \ \subseteq\ \top \cdot R \cap id \\ \equiv & \quad \{\ \text{GC (F12), pois } \top \cdot R \cap id \text{ é coreflexiva}\ \} \\ & R \ \subseteq\ \top \cdot (\top \cdot R \cap id) \\ \equiv & \quad \{\ \text{(F13)}\ ;\ \top \cdot id = \top;\ X \cap \top = X\ \} \\ & R \ \subseteq\ \top \cdot R \\ \equiv & \quad \{\ \top = !^{\circ} \cdot !\ ;\ \text{shunting (54)}\ \} \\ & ! \cdot R \ \subseteq\ ! \cdot R \\ \equiv & \quad \{\ \text{reflexividade}\ \} \\ & \text{TRUE} \end{array}$$

Pong:

$$\top \cdot R \cap id \ \subseteq\ \delta\, R$$

$$
\begin{array}{ll}
\equiv & \{ \text{ para toda a coreflexiva } \Phi,\ \delta\,\Phi = \Phi \ \} \\
& \delta\,(\top \cdot R \cap id) \ \subseteq \ \delta\,R \\
\equiv & \{ \text{ GC (F12) } ;\ \top \cdot R = \top \cdot \delta\,R \ \} \\
& \top \cdot R \cap id \ \subseteq \ \top \cdot R \\
\equiv & \{ \ X \cap Y \subseteq X \ \} \\
& \text{TRUE}
\end{array}
$$

□

Questão 6 (1 alínea) O diagrama relacional seguinte,

$$Mq \xrightarrow{fase} Fa \xleftarrow{fas} Cp \xrightarrow{i_1} Cp + Mt \xleftarrow{i_2} Mt \qquad Cp \xrightarrow{Pts} Cp + Mt \tag{F15}$$

foi extraído do seguinte modelo em Alloy,

```
open util/ordering[Fase]

sig Fase {}

abstract sig Produto {}

sig Componente extends Produto {
  partes : set Produto,
  fas : one Fase
}

sig Material extends Produto {}

sig Maquina { fase : one Fase }
```

captando a estrutura do sistema de informação de uma empresa que fabrica componentes numa linha de montagem organizada em fases de fabrico sucessivas [1]. Para economia de texto, abreviaram-se os identificadores $partes$ para Pts, $Componente$ para Cp, $Material$ para Mt, $Maquina$ para Mq, $Produto$ para Pr e $Fase$ para Fa. Assim, $Pr = Cp + Mt$ significa o mesmo que $Produto = Componente + Material$, etc.

Desse modelo constam ainda os invariantes seguintes — (a) *um componente não pode ser fabricado a partir do nada*:

$$id \quad \subseteq \quad \top \cdot Pts \tag{F16}$$

(b) *um componente não pode ser um dos seus sub-componentes*:

$$i_1^\circ \cdot Pts \quad \subseteq \quad id \Rightarrow \bot \tag{F17}$$

(c) *todos os sub-componentes de um componente tem que ser fabricados em fases prévias* (assumindo uma ordem total $\leq$ sobre Fa):

$$fas \cdot i_1^\circ \cdot Pts \quad \dot{\leq} \quad fas \tag{F18}$$

(d) *todas as fases envolvidas no fabrico de algum componente tem que ser suportadas por máquinas*:

$$fas \quad \subseteq \quad fase \cdot \top \tag{F19}$$

Mostre que a operação que acrescenta um novo material m a um componente c,

$$\text{post-}NewM(c, m) \quad \triangleq \quad Pts' \ = \ Pts \ \cup \ i_2 \cdot \underline{m} \cdot \underline{c}^\circ \tag{F20}$$

[1] Problema extraído do teste de Alloy de 7.2.2013.

satisfaz todos esses invariantes e calcule o **contrato** que deve observar-se na operação que adiciona dependências entre componentes,

$$\text{post-}AddDep(K) \quad \triangleq \quad Pts' \;=\; Pts \cup i_1 \cdot K \tag{F21}$$

no que diz respeito ao terceiro invariante (F18).
NB: atente no facto de a união-disjunta $Cp + Mt$ ser assegurada por duas **injecções** disjuntas no contra-domínio, isto é, tais que $i_1^\circ \cdot i_2 \subseteq \bot$.

RESOLUÇÃO: Análise de $NewM(c, m)$:

a) Invariante (F16) — Pts está no lado superior, logo "pode sempre crescer" para $Pts' \;=\; Pts \;\cup\; i_2 \cdot \underline{m} \cdot \underline{c}^\circ$

b) Invariante (F17), cálculo da WP:

$$\begin{array}{ll} & i_1^\circ \cdot Pts' \;\subseteq\; id \Rightarrow \bot \\ \equiv & \quad \{ \text{ pós-condição (F20) } \} \\ & i_1^\circ \cdot (Pts \;\cup\; i_2 \cdot \underline{m} \cdot \underline{c}^\circ) \;\subseteq\; id \Rightarrow \bot \\ \equiv & \quad \{ \text{ distributividade da composição pela reunião ; universal-}\cup \} \\ & (F17) \;\wedge\; i_1^\circ \cdot i_2 \cdot \underline{m} \cdot \underline{c}^\circ \;\subseteq\; id \Rightarrow \bot \\ \equiv & \quad \{ \; i_1^\circ \cdot i_2 = \bot \; \} \\ & (F17) \;\wedge\; \bot \;\subseteq\; id \Rightarrow \bot \\ \equiv & \quad \{ \; \bot \text{ é ínfimo } \} \\ & (F17) \end{array}$$

logo o contracto verifica-se.

c) Invariante (F18) — em tudo igual ao anterior, pois $fas \cdot i_1^\circ \cdot Pts \;\dot{\leq}\; fas$ é a mesma coisa que $fas \cdot i_1^\circ \cdot Pts \subseteq (\leq) \cdot fas$.

d) Invariante (F19) — a operação não interfere nem com fas nem com $fase$.

Finalmente, cálculo do contrato de $AddDep(K)$ com respeito a (F18):

$$\begin{array}{ll} & fas \cdot i_1^\circ \cdot Pts' \;\dot{\leq}\; fas \\ \equiv & \quad \{ \text{ pós-condição (F21) ; lifting: } R \;\dot{\leq}\; S = R \subseteq (\leq) \cdot S \; \} \\ & fas \cdot i_1^\circ \cdot (Pts \cup i_1 \cdot K) \subseteq (\leq) \cdot fas \\ \equiv & \quad \{ \text{ distributividade da composição pela reunião ; universal-}\cup \} \\ & (F18) \;\wedge\; fas \cdot i_1^\circ \cdot i_1 \cdot K \subseteq (\leq) \cdot fas \\ \equiv & \quad \{ \; i_i \text{ é função injectiva, logo } ker\, i_1 = id \; \} \\ & (F18) \;\wedge\; fas \cdot K \subseteq (\leq) \cdot fas \\ \equiv & \quad \{ \text{ seta de Reynolds (92) } \} \\ & (F18) \;\wedge\; (\leq) \xleftarrow{fas} K \end{array}$$

A WP é $(\leq) \xleftarrow{fas} K$, que é o mesmo que: $yKx \Rightarrow (fas\; y) \leq (fas\; x)$. $\Box$
