Especificação e Modelação

1.º Ano de Mestrado (Eng. Informática / Matemática e Computação)
Perfil: MÉTODOS FORMAIS EM ENGENHARIA DE SOFTWARE
Universidade do Minho
Ano Lectivo de 2014/15

Mini-teste — 7 de Janeiro
16h00
Sala CPII-208

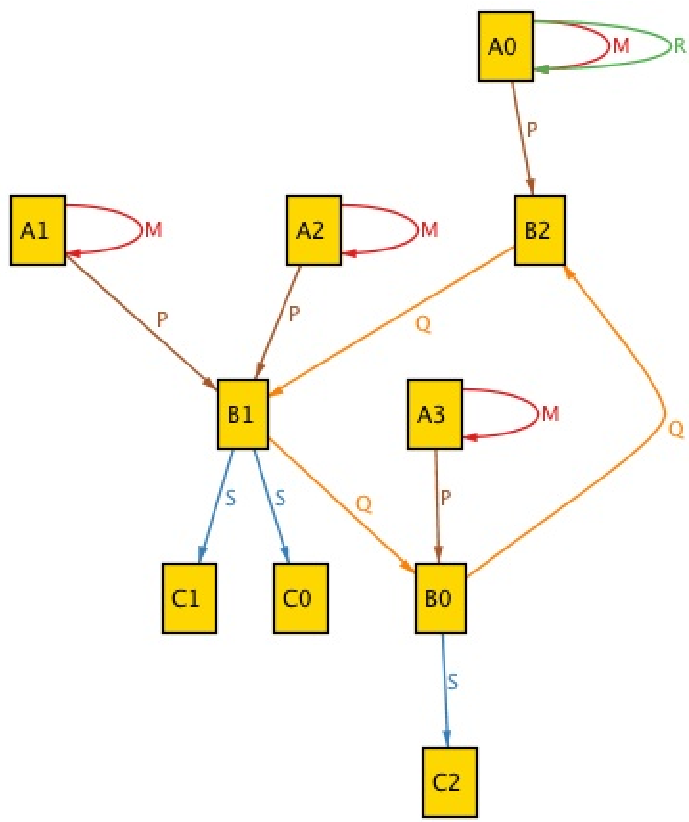
NB: *Este mini-teste consta de **4** questões todas com as mesma cotação (2.5 valores). A nota mínima para esta prova ser considerada é **7 valores**. Os alunos que desejem responder directamente sobre o enunciado da questão 3 devem ter o cuidado de rubricar as respectiva folha e indicarem aí o seu **número mecanográfico**.*

PROVA COM CONSULTA (1 hora)

Questão 1 Sejam dados os tipos de dados A (com quatro elementos) e B, C (ambos com três elementos) e as relações M, R, S, Q e P entre eles registadas no diagrama Alloy em baixo.

Identifique, no diagrama ao lado, justificando:

1. uma relação que não seja simples
2. uma sobrejecção
3. uma relação identidade
4. uma injecção
5. uma relação co-reflexiva que não seja inteira
6. uma bijecção que não seja a identidade.



RESOLUÇÃO: Identificam-se as relações seguintes, pela ordem do enunciado:

1. S não é simples — o contra-exemplo é $C1\ (\text{img}\ S)\ C0$, logo img S não é co-reflexiva.
2. Como uma sobrejecção é uma função sobrejectiva, há várias relações no diagrama que o são, a saber M, P e Q. A mais simples de justificar é $M = id$, logo uma bijecção e portanto sobrejecção.
3. Como se disse acima, $M = id$ é a identidade em A.
4. $M = id$ é injecção, assim como o é Q, pois ker $Q = id$ em B.
5. $R = \{(A0, A0)\}$ é uma parte estrita da identidade em A, logo coreflexiva não-inteira.
6. Q é uma função e a sua conversa também o é (basta mudar o sentido das setas) – logo Q é uma bijecção, cf. (78) dos slides. Mais ainda, $Q \cap id = \bot$.

$\square$

Questão 2 Considere a operação de subtracção (truncada) nos números naturais ($\mathbb{N}_0$)

$$a \ominus b = \textbf{if } b \geqslant a \textbf{ then } 0 \textbf{ else } (a \ominus (b+1)) + 1$$

cuja estrutura algorítmica faz lembrar a da divisão inteira. De facto, é possível mostrar que $a \ominus b$ se pode **especificar** sob a forma da seguinte propriedade universal:

$$a \ominus b \leqslant x \quad \equiv \quad a \leqslant b + x \tag{F1}$$

Use esta propriedade para demonstrar o facto seguinte:

$$a \ominus (b + c) \quad = \quad (a \ominus b) \ominus c \tag{F2}$$

Sugestão: Esta demonstração é análoga a uma que foi estudada nas aulas. Inspire-se nela.

RESOLUÇÃO: Tal como nesse caso (divisão inteira), vamos usar igualdade indirecta sobre (F1):

$$
\begin{array}{ll}
 & a \ominus (b+c) \leqslant x \\
\equiv & \qquad \{ \text{ propriedade universal (F1) } \} \\
 & a \leqslant (b+c) + x \\
\equiv & \qquad \{ \text{ associatividade da soma } \} \\
 & a \leqslant b + (c+x) \\
\equiv & \qquad \{ \text{ propriedade universal (F1) } \} \\
 & a \ominus b \leqslant c + x \\
\equiv & \qquad \{ \text{ propriedade universal (F1) de novo } \} \\
 & (a \ominus b) \ominus c \leqslant x \\
:: & \qquad \{ \text{ igualdade indirecta sobre a ordem parcial } \leqslant \} \\
 & a \ominus (b+c) = (a \ominus b) \ominus c
\end{array}
$$

$\square$

$\square$

Questão 3 Apresente justificações para os seguintes passos da demonstração, por igualdade indirecta, da propriedade

$$(\Phi \times id) \cap (id \times \Psi) \quad = \quad \Phi \times \Psi \tag{F3}$$

onde Φ e Ψ são relações co-reflexivas:

$$
\begin{array}{ll}
& X \subseteq (\Phi \times id) \cap (id \times \Psi) \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& X \subseteq \Phi \times id \;\wedge\; X \subseteq (id \times \Psi) \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \pi_1 \cdot X \subseteq \Phi \cdot \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \pi_2 \;\wedge\; \pi_1 \cdot X \subseteq \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \Psi \cdot \pi_2 \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \pi_1 \cdot X \subseteq \Phi \cdot \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \Psi \cdot \pi_2 \;\wedge\; X \subseteq id \times id \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& X \subseteq \Phi \times \Psi \;\wedge\; X \subseteq id \\
\equiv & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& X \subseteq \Phi \times \Psi \\
\Box &
\end{array}
$$

RESOLUÇÃO: Justificações propostas:

$$
\begin{array}{ll}
& X \subseteq (\Phi \times id) \cap id \times \Psi \\
\equiv & \quad \{ \text{ universal-}\cap \text{ (96) } \} \\
& X \subseteq \Phi \times id \;\wedge\; X \subseteq id \times \Psi \\
\equiv & \quad \{ \; R \times S = \langle R \cdot \pi_1, S \cdot \pi_2 \rangle \text{ e (116), 2 vezes; ``shunting'' (79) 4 vezes } \} \\
& \pi_1 \cdot X \subseteq \Phi \cdot \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \pi_2 \;\wedge\; \pi_1 \cdot X \subseteq \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \Psi \cdot \pi_2 \\
\equiv & \quad \{ \text{ leis do passo acima, aplicadas por ordem inversa } \} \\
& \pi_1 \cdot X \subseteq \Phi \cdot \pi_1 \;\wedge\; \pi_2 \cdot X \subseteq \Psi \cdot \pi_2 \;\wedge\; X \subseteq id \times id \\
\equiv & \quad \{ \text{ leis do passo acima, aplicadas por ordem inversa ; } id \times id = id \text{ (functor-}id\text{) } \} \\
& X \subseteq \Phi \times \Psi \;\wedge\; X \subseteq id \\
\equiv & \quad \{ \text{ por monotonia, produto de co-reflexivas é uma co-reflexiva ; lógica: } (p \Rightarrow q) \;\Leftrightarrow\; (p \wedge q = p) \; \} \\
& X \subseteq \Phi \times \Psi \\
\Box &
\end{array}
$$

$\Box$

Questão 4 Recorde o invariante do problema PROPOSITIO DE HOMINE ET CAPRA ET LVPO:

$$
\begin{tikzcd}
Being \arrow[d, "where"'] \arrow[dr, phantom, "\subseteq"] & Being \arrow[l, "CanEat"'] \arrow[d, "Farmer"] \\
Bank & Being \arrow[l, "where"]
\end{tikzcd}
\tag{F4}
$$

Embora não faça muito sentido no "puzzle" em questão, é possível imaginar uma operação em que todos os seres *trocam instantaneamente de margem*:

post $where' = cross \cdot where$

Intuitivamente, esta operação preserva o invariante (F4).

Demonstre esse facto recorrendo exclusivamente a álgebra relacional ('pointfree'). **Sugestão:** não se equeça de que *cross* — a função que *dá a outra margem* — é uma bijecção.

RESOLUÇÃO: Designemos o invariante por inv, ou seja,

$$\mathsf{inv}\ where \stackrel{\text{def}}{=} where \cdot CanEat \subseteq where \cdot \underline{Farmer}$$

Há ainda que expandir $CanEat$:

$$\mathsf{inv}\ where \stackrel{\text{def}}{=} where \cdot (Eats \cap \mathsf{ker}\ where) \subseteq where \cdot \underline{Farmer} \tag{F5}$$

Sabendo que não há nenhuma pré-condição, a obrigação de prova de preservação do invariante — fórmula (32) dos slides — reduz-se a:

$$\langle \forall\ where', where\ :\ \mathsf{inv}\ where \wedge where' = cross \cdot where :\ \mathsf{inv}\ where' \rangle$$

que pela regra 'one-point' ($\forall$) simplifica em

$$\langle \forall\ where\ :\ \mathsf{inv}\ where :\ \mathsf{inv}\ (cross \cdot where) \rangle$$

Queremos pois mostrar que inv $where$ é *suficiente* para inv $(cross \cdot where)$ se verificar. Pegando neste termo, como objectivo, tem-se:

$$\begin{array}{cl}
& \mathsf{inv}\ (cross \cdot where) \\
\equiv & \quad \{\ \text{definição de inv (F5)}\ \} \\
& (cross \cdot where) \cdot (Eats \cap \mathsf{ker}\ (cross \cdot where)) \subseteq (cross \cdot where) \cdot \underline{Farmer} \\
\equiv & \quad \{\ \mathsf{ker}\ (cross \cdot where) = \mathsf{ker}\ where \text{ pois } \mathsf{ker}\ cross = id \text{ (bijeccção)}\ \} \\
& cross \cdot where \cdot (Eats \cap \mathsf{ker}\ where) \subseteq cross \cdot where \cdot \underline{Farmer} \\
\equiv & \quad \{\ \text{associatividade de } (\cdot)\text{; shunting (79); def. } CanEat\ \} \\
& where \cdot CanEat \subseteq cross^{\circ} \cdot cross \cdot where \cdot \underline{Farmer} \\
\equiv & \quad \{\ cross^{\circ} \cdot cross = id \text{ pois } cross \text{ é uma bijecção ; natural-}id\ \} \\
& where \cdot CanEat \subseteq where \cdot \underline{Farmer} \\
\equiv & \quad \{\ \text{definição de inv}\ \} \\
& \mathsf{inv}\ where \\
\Box &
\end{array}$$

Logo inv $where$ é não só condição *suficiente* mas também *necessária* para inv $where'$ se verificar. $\Box$
