Especificação e Modelação
Perfil: MÉTODOS FORMAIS EM ENGENHARIA DE SOFTWARE

1/4.º Ano de MEI & MMC / MIEi, Universidade do Minho
Ano Lectivo de 2016/17

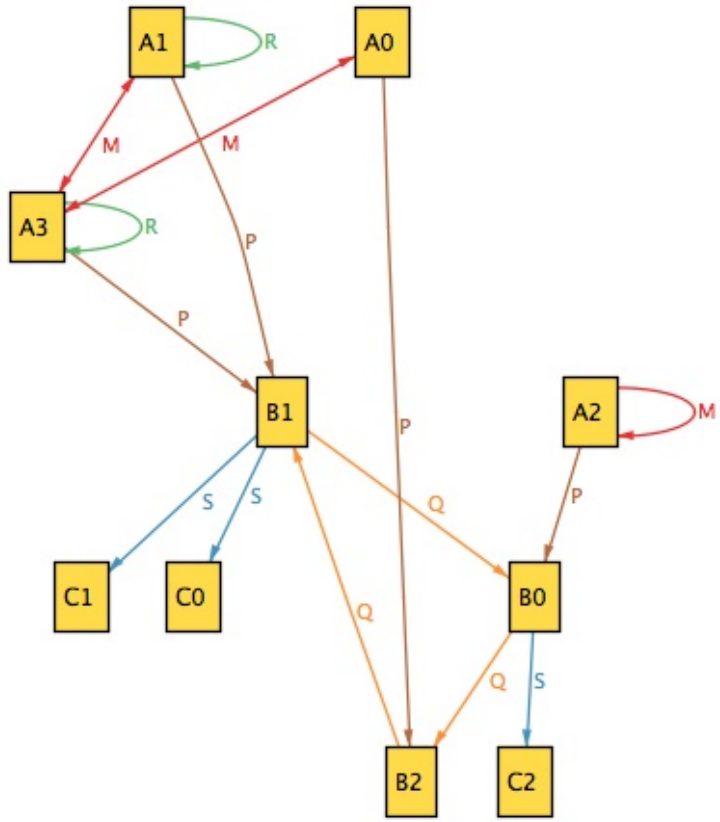
Teste — 12 de Janeiro de 2017
14h00
Sala DI 0.03

Importante — *Ler antes de iniciar a prova: Este exame consta de **8 alíneas** que valem, cada uma, 2.5 valores. O tempo médio estimado para resolução de cada questão é de 15 min.*

PROVA COM CONSULTA (2 horas)

Questão 1 (1 alínea) Considere o problema clássico de implementar uma máquina de trocar uma certa quantia em moedas. Modele esta máquina em SMV e indique como pode usar o respectivo model checker para determinar a sequência de moedas que troca uma certa quantia. Assuma que existe um stock limitado de moedas com as seguintes denominações: 1, 3 e 4.

Questão 2 (1 alínea) 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, tal como se regista no diagrama Alloy que se segue:



- Identifique, no diagrama (justificando):
  1. Uma relação **coreflexiva**.
  2. Uma relação que não seja nem **simples** nem **inteira**.
  3. Uma relação **simétrica**
  4. Uma **sobrejecção** não **injectiva**
  5. Uma **injecção**.
- Calcule a relação $S \cdot P \cdot R$ enumerando-a sob a forma de um conjunto de pares.

RESOLUÇÃO: Primeira parte:

1. R – pois está contida em id (em A)
2. S — pois diverge em B_1 e não está definida para B_2
3. M — pois todas as suas setas têm retorno
4. P — pois está totalmente definida em A, converge em B_1, chegam setas a todos os Bs
5. Q — pois é função sem qualquer convergência.

Segunda parte:

$$
\begin{array}{ll}
 & S \cdot P \cdot R \\
= & \qquad \{ \text{ expansão de } P \text{ e } R \text{ de acordo com diagrama } \} \\
 & S \cdot \{\text{B}_2 \leftarrow \text{A}_0, \text{B}_1 \leftarrow \text{A}_1, \text{B}_0 \leftarrow \text{A}_2, \text{B}_1 \leftarrow \text{A}_3\} \cdot \{\text{A}_1 \leftarrow \text{A}_1, \text{A}_3 \leftarrow \text{A}_3\} \\
= & \qquad \{ \text{ composição (pointwise) } \} \\
 & S \cdot \{\text{B}_1 \leftarrow \text{A}_1, \text{B}_1 \leftarrow \text{A}_3\} \\
= & \qquad \{ \text{ expansão de } S \text{ de acordo com diagrama } \} \\
 & \{\text{C}_2 \leftarrow \text{B}_0, \text{C}_0 \leftarrow \text{B}_1, \text{C}_1 \leftarrow \text{B}_1\} \cdot \{\text{B}_1 \leftarrow \text{A}_1, \text{B}_1 \leftarrow \text{A}_3\} \\
= & \qquad \{ \text{ composição } \} \\
 & \{\text{C}_0 \leftarrow \text{A}_1, \text{C}_1 \leftarrow \text{A}_1, \text{C}_0 \leftarrow \text{A}_3, \text{C}_1 \leftarrow \text{A}_3\}
\end{array}
$$

□

Questão 3 (1 alínea) Nesta disciplina estudou-se a noção de **tipo relacional** (107): diz-se que uma função h tem tipo $R \rightarrow S$ sempre que $h \cdot R \subseteq S \cdot h$ se verifica. Mostre que qualquer função tem tipo relacional $\bot \rightarrow R$ e tipo relacional $R \rightarrow \top$.

RESOLUÇÃO:

Primeira parte é imediata: $h : \bot \rightarrow R$ quer dizer $h \cdot \bot \subseteq R \cdot h \Leftrightarrow \bot \subseteq R \cdot h \Leftrightarrow \mathit{true}$.

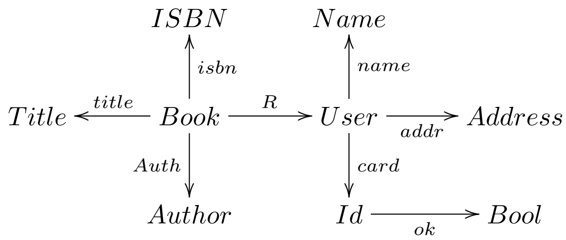
Segunda parte (completar as justificações):

$$
\begin{array}{ll}
 & h : R \rightarrow \top \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & h \cdot R \subseteq \top \cdot h \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & h \cdot R \cdot h^\circ \subseteq \top \\
\equiv & \qquad \{ \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ \} \\
 & \mathit{true}
\end{array}
$$

□

□

Questão 4 (1 alínea) Recorde o caso de estudo dos empréstimos domiciliários de uma biblioteca,



ao qual se acrescentou um predicado ok que indica que cartões estão activos. Este predicado induz um novo invariante no sistema — *só se podem emprestar livros a utentes com cartão activo*:

$$cardsOk\ R \stackrel{\text{def}}{=} card \cdot R \ \subseteq\ (ok?) \cdot \top \tag{F1}$$

- Calcule a pré-condição mais fraca que garante que a operação de empréstimo de livros

$$borrow\ S\ R = S \cup R \tag{F2}$$

satisfaz o invariante (F1).

- Suponha que alguém especifica esse novo invariante sob a forma

$$R\ \subseteq\ \frac{true}{ok \cdot card} \tag{F3}$$

Será que (F3) é equivalente a (F1)? Justifique a sua resposta.

RESOLUÇÃO:

Primeira parte: $wp\ (borrow\ S, cardsOk) = cardsOk \cdot (borrow\ S)$; logo (completar as justificações):

$$p = cardsOk \cdot (borrow\ S)$$
$\equiv$ { .... }
$$p\ R = cardsOk\ (borrow\ S\ R)$$
$\equiv$ { .... }
$$p\ R = card \cdot (R \cup S)\ \subseteq\ ok? \cdot \top$$
$\equiv$ { .... }
$$p\ R = (card \cdot R) \cup (card \cdot S)\ \subseteq\ ok? \cdot \top$$
$\equiv$ { .... }
$$p\ R = cardOk\ R \wedge card \cdot S\ \subseteq\ ok? \cdot \top$$
□

Logo a pré-condição mais fraca para $borrow\ S$ manter $cardOk$ é o que sobra de $cardOk\ R$ no cálculo acima: $card \cdot S\ \subseteq\ ok? \cdot \top$.

Segunda parte (completar as justificações):

$$card \cdot R\ \subseteq\ ok? \cdot \top$$
$\equiv$ { facto (78) dos slides }
$$card \cdot R\ \subseteq\ \frac{true}{ok}$$
$\equiv$ { .... }

$$
\begin{array}{ll}
 & R \subseteq card^\circ \cdot ok^\circ \cdot true \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & R \subseteq \dfrac{true}{ok \cdot card}
\end{array}
$$

□

□

Questão 5 (1 alínea) As equipas (E) de um campeonato têm jogos (J) em casa e jogos fora, e todo o jogo ocorre numa data:

$$
\begin{array}{ccccc}
E & \xleftarrow{casa} & J & \xrightarrow{fora} & E \\
 & & {\scriptstyle data}\downarrow & & \\
 & & D & &
\end{array}
$$

Mais ainda:

(a) Nenhuma equipa deverá fazer dois jogos na mesma data.

(b) Nenhuma equipa pode jogar consigo própria.

(c) A um jogo em casa corresponde outro jogo fora com a mesma equipa.

Para captar estas restrições, alguém postulou os invariantes:

A relação $\langle casa \cup fora, data \rangle$ é injectiva. (F4)

A relação $casa \cdot fora^\circ$ é simétrica e irreflexiva. (F5)

Pergunta-se:

Os invariantes (F4,F5) cobrem as propriedades (a,b,c) desejáveis neste modelo de campeonato?

Justifique a sua resposta. Mostre ainda que a simetria da relação $casa \cdot fora^\circ$ se pode escrever da forma

$$id \subseteq \frac{fora}{casa} \cdot \frac{fora}{casa}$$

e exprima esta mesma propriedade usando lógica quantificada, após introdução de variáveis seguida de simplificação.

RESOLUÇÃO: O que se pedia na primeira parte era a indicação de contra-exemplos simples que ajudassem a identificar os requisitos formais com os informais. Por exemplo, o contra-exemplo $e_1 \underset{casa}{\overset{fora}{\leftleftarrows}} j_1$ contraria (b), pois $e_1(casa \cdot fora^\circ)e_1$ verifica-se. Logo esta relação tem que ser irreflexiva (não pode ter lacetes); etc. (Completar.)[1] Quanto à

---

[1] Uma outra resolução, mais elaborada, traduziria os textos em predicados e mostraria como eles se reduzem aos invariantes dados:

(c) Há sempre um jogo em que as equipas trocam de casa — isto traduz-se no predicado
$\langle \forall\, e, e' \;:\; \langle \exists\, j \;::\; e = casa\ j \wedge e' = fora\ j \rangle : \langle \exists\, j' \;::\; e = fora\ j' \wedge e' = casa\ j \rangle \rangle$
que se reduz a
$\langle \forall\, e, e' \;:\; e\ (casa \cdot fora^\circ)\ e' : e\ (fora \cdot casa^\circ)\ e' \rangle$
isto é, $casa \cdot fora^\circ$ é simétrica.

(b) É traduzida no predicado
$\neg \langle \exists\, e \;::\; \langle \exists\, j \;::\; e = casa\ j \wedge e = fora\ j \rangle \rangle$
que é o mesmo que dizer que nenhuma equipa e é tal que $e\ (casa \cdot fora^\circ)\ e$, isto é, $casa \cdot fora^\circ$ é ireflexiva.

(a) Seja R a relação entre equipas e seus jogos, isto é: $e\ R\ j \;\Leftrightarrow\; e = fora\ j \vee e = casa\ j$. O requisito corresponde a $\neg \langle \exists\, j'\ j \;:\; \neg (j = j') \wedge data\ j' = data\ j : \langle \exists\, e \;:\; e\ R\ j' : e\ R\ j \rangle \rangle$ que sucessivamente se transforma, pelas leis do cálculo de Eindhoven, em:
$\langle \forall\, j'\ j \;:\; \langle \exists\, e \;:\; e\ R\ j' : e\ R\ j \rangle \wedge data\ j' = data\ j : j = j' \rangle$
$\langle \forall\, j'\ j \;:\; j'\ (\ker R)\ j \wedge j'\ (\ker data)\ j : j = j' \rangle$
$\langle \forall\, j'\ j \;:\; j'\ (\ker \langle R, data \rangle)\ j : j = j' \rangle$
$\langle R, data \rangle$ injectiva, isto é, a (F4).

segunda parte (completar as justificações):

$$
\begin{array}{ll}
& casa \cdot fora^{\circ} \subseteq (casa \cdot fora^{\circ})^{\circ} \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& casa \cdot fora^{\circ} \subseteq fora \cdot casa^{\circ} \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& id \subseteq casa^{\circ} \cdot fora \cdot casa^{\circ} \cdot fora \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& id \subseteq \frac{fora}{casa} \cdot \frac{fora}{casa}
\end{array}
$$

O mesmo em notação pointwise (completar as justificações):

$$
\begin{array}{ll}
& id \subseteq \frac{fora}{casa} \cdot \frac{fora}{casa} \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& \langle \forall\, j, k \ : \ j = k : \ \langle \exists\, j' \ : \ j \ \frac{fora}{casa} \ j' : \ j' \ \frac{fora}{casa} \ k \rangle \rangle \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& \langle \forall\, j \ :: \ \langle \exists\, j' \ : \ casa\ j = fora\ j' : \ casa\ j' = fora\ j \rangle \rangle
\end{array}
$$

□

Questão 6 (1 alínea) Na sequência da questão anterior, usando as leis da álgebra relacional que estudou nesta disciplina verifique se os invariantes (F4,F5) estão bem codificados no fragmento Alloy que se segue:

```
sig J {
  casa : one E,
  fora : one E,
  data : one D
}
sig E, D { }
run {
  ~fora . casa = ~casa . fora
  no ~fora . casa & iden
  (fora + casa) . ~(fora + casa) & data . ~data in iden
}
```

RESOLUÇÃO: Abrevie-se por R a relação $casa \cup fora$.

As primeiras duas são a transcrição imediata de notação relacional para Alloy, tendo cuidado em inverter a ordem da composição etc.[2] Quanto à terceira:

$$
\begin{array}{ll}
& \ker \langle R, data \rangle \subseteq id \\
\equiv & \{ \ (105) \ \} \\
& \ker R \cap \ker data \subseteq id \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& (fora \cup casa)^{\circ} \cdot (fora \cup casa) \cap data^{\circ} \cdot data \subseteq id
\end{array}
$$

[2] Irreflexiva significa ausência total de lacetes: $id \cap R = \bot$.

que se escreve em Alloy como vem no enunciado. □

Questão 7 (2 alíneas) Considere o seguinte refinamento do modelo anterior, escrito em Alloy, onde foi acrescentada uma relação mutável $vencedor$ que regista qual a equipa vencedora de um determinado jogo (no caso de empate ambas são vencedoras):

$open\ util\ /\ ordering\ [State]$
$open\ util\ /\ ordering\ [D]$
sig $State\ \{\}$
sig $J\ \{$
  $casa$: one E,
  $fora$: one E,
  $data$: one D,
  $vencedor : E \rightarrow State$
$\}$
sig $E, D\ \{\}$
pred $inv\ [s : State]\ \{$
  $\sim fora \cdot casa = \sim casa \cdot fora$
  no $\sim fora \cdot casa\ \&$ iden
  $(fora + casa) \cdot \sim (fora + casa)\ \&\ data \cdot \sim data$ **in** iden
  ...
$\}$

1. Complete o invariante por forma a garantir que todos os jogos já com vencedores ocorreram antes dos jogos que ainda não tem vencedores registados. Acrescente também outros invariantes que julgue necessários.
2. Especifique a operação que regista o resultado de um determinado jogo, garantindo que a mesma preserva os invariantes definidos.
