

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

Teste — 28 de Janeiro de 2015

15h00

Sala CPII-201

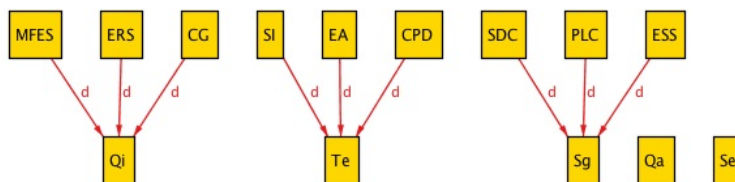
Importante — Ler antes de iniciar a prova:

- Este teste consta de 8 questões que valem, cada uma, 2.5 valores. O tempo médio estimado para resolução de cada questão é de 15 min.
- Os alunos com nota mínima no **miniteste** só podem responder à parte II (questões 5, 6, 7, 8), devendo entregar a prova ao fim de uma hora.
- Os restantes alunos devem responder a todas as questões, entregando a prova ao fim de duas horas.

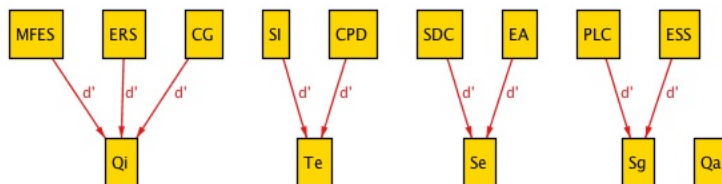
PROVA COM CONSULTA (1 ou 2 horas)

Parte I

Questão 1 Recorde a função d do modelo do problema do NOVO PLANO DE ESTUDOS DO MEI que foi abordado nas aulas desta disciplina e vem dado em anexo. Actualmente essa função é a seguinte, para os 9 perfis activos no MEI:



Suponha que, por entretanto terem surgido salas disponíveis à sexta-feira, a mesma função passa a ser:



Indique, justificando formalmente, quais das quatro situações seguintes

1. $d \leq d'$
2. $d' \leq d$
3. tanto 1 como 2
4. nem 1 nem 2

se verificam, onde a ordem

$$f \leq g \equiv \ker g \subseteq \ker f \tag{F1}$$

exprime que a função f é *menos injectiva* que a função g .

RESOLUÇÃO: Tem-se:

1. $d \leq d'$ significa $\ker d' \leq \ker d$ isto é $(\forall q, p : d' q = d' p : d q = d p)$. Não se verifica pois, por exemplo, $SDC(\ker d') EA$ — são ao mesmo dia em d' — e não se tem $SDC(\ker d) EA$ — são em dias diferentes em d .
2. $d' \leq d$ significa $\ker d \leq \ker d'$: não se verifica pois, por exemplo, $EA(\ker d) CPD$ — são ao mesmo dia em d — e não se tem $EA(\ker d') CPD$ — são em dias diferentes.
3. Falso pelos dois casos acima.
4. Verdadeiro pelos mesmos casos.

□

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

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

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:

$$a \ominus b \leq x \equiv a \leq b + x \tag{F2}$$

Use (F2) para demonstrar as igualdades

$$0 \ominus b = 0$$

$$a \ominus 0 = a$$

sem recorrer ao algoritmo dado acima.

RESOLUÇÃO: Por igualdade indirecta nos dois casos. Primeira igualdade:

$$\begin{aligned} & 0 \ominus b \leq x \\ \equiv & \quad \{ (F2) \} \\ & 0 \leq b + x \\ \equiv & \quad \{ \text{como os números são naturais, } 0 \leq b + x \equiv 0 \leq x \equiv \text{true} \} \\ & 0 \leq x \\ \therefore & \quad \{ \text{igualdade indirecta sobre ordem parcial} \} \\ & 0 \ominus b = 0 \end{aligned}$$

□

Segunda igualdade:

$$\begin{aligned} & a \ominus 0 \leq x \\ \equiv & \quad \{ (F2) \} \\ & a \leq 0 + x \\ \equiv & \quad \{ 0 \text{ é o elemento neutro da adição} \} \\ & a \leq x \\ \therefore & \quad \{ \text{igualdade indirecta sobre ordem parcial} \} \\ & a \ominus 0 = a \end{aligned}$$

□

□

Questão 3 Considere a definição do combinador condicional

$$p \rightarrow R, S \stackrel{\text{def}}{=} [R, S] \cdot [\Phi_p, \Phi_{(\neg p)}]^\circ \quad (\text{F3})$$

onde $A \xrightarrow{p} \mathbb{B}$ é um predicado (função booleana), Φ_p a respectiva coreflexiva e $A \xrightarrow{R, S} B$ duas relações. Recordando a lei (134),

$$[R, S] \cdot [T, U]^\circ = (R \cdot T^\circ) \cup (S \cdot U^\circ)$$

mostre que

$$y = (p \rightarrow f, g) x \equiv (y = f x \wedge p x) \vee (y = g x \wedge \neg(p x))$$

é a conversão para notação *pointwise* de (F3) para o caso funcional.

RESOLUÇÃO: Repare-se que:

$$\begin{aligned} & y = (p \rightarrow f, g) x \\ \equiv & \quad \{ (52) \} \\ & y (p \rightarrow f, g) x \\ \equiv & \quad \{ (F3) \} \\ & y ([f, g] \cdot [\Phi_p, \Phi_{(\neg p)}]^\circ) x \\ \equiv & \quad \{ (134); (151) \} \\ & y (f \cdot \Phi_p \cup g \cdot \Phi_{(\neg p)}) x \\ \equiv & \quad \{ (95) \} \\ & y (f \cdot \Phi_p) x \vee y (g \cdot \Phi_{(\neg p)}) x \\ \equiv & \quad \{ (57) \text{ e } (144), \text{ ambas duas vezes} \} \\ & \langle \exists z : y f z : z = x \wedge p z \rangle \vee \langle \exists z : y g z : z = x \wedge \neg p z \rangle \\ \equiv & \quad \{ \text{'trading' (8) e (52), repetidas vezes} \} \\ & \langle \exists z : z = x : y = f z \wedge p z \rangle \vee \langle \exists z : z = x : y = g z \wedge \neg p z \rangle \\ \equiv & \quad \{ \text{'one-point' (15) duas vezes} \} \\ & (y = f x \wedge p x) \vee (y = g x \wedge \neg p x) \\ & \square \end{aligned}$$

□

Questão 4 Recordando o invariante do problema PROPOSITIO DE HOMINE ET CAPRA ET LVPO,

$$\begin{array}{ccc} \textit{Being} & \xleftarrow{\textit{CanEat}} & \textit{Being} \\ \textit{where} \downarrow & \subseteq & \downarrow \textit{Farmer} \\ \textit{Bank} & \xleftarrow{\textit{where}} & \textit{Being} \end{array} \quad (\text{F4})$$

considere a operação que, em qualquer momento da execução do “puzzle”, faz regressar tudo ao estado inicial:

post $where' = \underline{Left}$

Demonstre formalmente que essa operação preserva o invariante (F4).

RESOLUÇÃO: Pegue-se no termo **inv** $where'$ e simplifique-se:

$$\begin{aligned} & \mathbf{inv} \, where' \\ \equiv & \quad \{ where' = \underline{Left} \} \\ & \underline{Left} \cdot \underline{CanEat} \subseteq \underline{Left} \cdot \underline{Farmer} \\ \equiv & \quad \{ \text{funções constantes: } \underline{f} \cdot g = \underline{f} \} \\ & \underline{Left} \cdot \underline{CanEat} \subseteq \underline{Left} \\ \equiv & \quad \{ 'shunting' \} \\ & \underline{CanEat} \subseteq \underline{Left}^\circ \cdot \underline{Left} \\ \equiv & \quad \{ \ker \underline{k} = \top \} \\ & \underline{CanEat} \subseteq \top \\ \equiv & \quad \{ \text{qualquer relação é menor que } \top \} \\ & \text{true} \\ & \square \end{aligned}$$

Logo o invariante é sempre válido após a operação, independentemente de o ser antes — típico de uma operação de “restart” (voltar ao início). \square

Parte II

Questão 5 Considere o fragmento de Alloy

```
sig Aula {
  doc : one Docente,
  dh  : one DHora,
  sala : one Sala
}
sig Docente, DHora, Sala { }
```

que caracteriza uma aula associando-lhe um docente, uma data/hora (*DHora*) de funcionamento e uma sala.

Suponha ainda que alguém escreve o seguinte invariante sobre *Aula*,

$$sala \leq \langle doc, dh \rangle \quad (\text{F5})$$

onde a ordem

$$R \leq S \equiv \ker S \subseteq \ker R \quad (\text{F6})$$

exprime que a relação *R* é *menos injectiva* ou *mais definida* (inteira) que a relação *S*.

Indique, justificando através da expansão *pointwise* de (F5), qual dos seguintes textos é captado por esse invariante:

1. Um docente *doc*, para toda a data/hora *dh*, está sempre numa sala.
2. Se duas aulas (eg. de cursos diferentes) são na mesma sala então têm o mesmo docente e começam à mesma hora.
3. Se duas aulas (eg. de cursos diferentes) têm o mesmo docente e começam à mesma hora, então têm lugar na mesma sala
4. Se duas aulas (eg. de cursos diferentes) são na mesma sala e começam à mesma hora então têm o mesmo docente.

RESOLUÇÃO: Comece-se por expandir a definição do invariante:

$$\begin{aligned}
 & sala \leq \langle doc, dh \rangle \\
 \equiv & \quad \{ (F6) \} \\
 & \ker \langle doc, dh \rangle \subseteq \ker sala \\
 \equiv & \quad \{ (123) \} \\
 & \ker doc \cap \ker dh \subseteq \ker sala \\
 \equiv & \quad \{ \text{definição de kernel, pela lei (70)} \} \\
 & \langle \forall a', a : doc\ a' = doc\ a \wedge dh\ a' = dh\ a : sala\ a' = sala\ a \rangle
 \end{aligned}$$

Logo vemos que, se as aulas a' e a têm o mesmo docente e começam ao mesmo tempo, então as salas previstas para a e a' terão que ser as mesmas. \square

Questão 6 Considere a equivalência relacional

$$(f \cdot g^\circ) \cap R \subseteq \perp \equiv R \cdot g \subseteq (\neq) \cdot f \tag{F7}$$

onde f e g são funções e (\neq) abrevia $id \Rightarrow \perp$.

- Escreva $R \cdot g \subseteq (\neq) \cdot f$ em notação *pointwise*.
- Demonstre a equivalência (F7) recorrendo, entre outras, às leis de “shunting”, à propriedade universal da implicação de relações e à propriedade distributiva seguinte:

$$f^\circ \cdot (R \Rightarrow S) \cdot g = (f^\circ \cdot R \cdot g) \Rightarrow (f^\circ \cdot S \cdot g) \tag{F8}$$

RESOLUÇÃO:

- Conversão:

$$\begin{aligned}
 & R \cdot g \subseteq (\neq) \cdot f \\
 \equiv & \quad \{ (59), \text{ seguida de (70) duas vezes} \} \\
 & \langle \forall b, a : b\ R\ (g\ a) : b \neq (f\ a) \rangle
 \end{aligned}$$

- Cálculo (acrescentar as justificações):

$$\begin{aligned}
 & (f \cdot g^\circ) \cap R \subseteq \perp \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & f \cdot g^\circ \subseteq (R \Rightarrow \perp) \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & f \subseteq (R \Rightarrow \perp) \cdot g \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & f \subseteq (R \cdot g \Rightarrow \perp) \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & R \cdot g \subseteq (f \Rightarrow \perp)
 \end{aligned}$$

$$\begin{aligned} &\equiv \{ \dots\dots\dots \} \\ &R \cdot g \subseteq (id \cdot f \Rightarrow \perp \cdot f) \\ &\equiv \{ \dots\dots\dots \} \\ &R \cdot g \subseteq (id \Rightarrow \perp) \cdot f \\ &\square \end{aligned}$$

□

Questão 7 Considere, no contexto do problema O NOVO PLANO DE ESTUDOS DO MEI que foi abordado nas aulas desta disciplina e vem dado em apêndice, a operação que inscreve o aluno a na opção complementar c , dada pelo par **pre/post** seguinte:

$$\begin{aligned} \text{pre} &\langle \forall x : x R a : d x \neq d (p c) \rangle \\ \text{post} &R' = R \wedge S' = S \cup \{(c, a)\} \end{aligned}$$

Atente no significado da pré-condição: *qualquer que seja o perfil x em que o aluno a esteja inscrito, o dia desse perfil é sempre diferente do dia da opção complementar c .*

Complete as justificações do cálculo que se segue e que mostra que essa pré-condição é a mais fraca possível para garantir um dos invariantes do problema, a saber:

$$\text{inv} (R, S) = d \cdot R \cap d \cdot p \cdot S \subseteq \perp \text{ — os perfis ocupam dias inteiros}$$

Cálculo a justificar:

$$\begin{aligned} &\text{inv} (R', S') \\ \equiv & \{ \dots\dots\dots \} \\ &d \cdot R' \cap d \cdot p \cdot S' \subseteq \perp \\ \equiv & \{ \dots\dots\dots \} \\ &d \cdot R \cap d \cdot p \cdot (S \cup c \cdot a^\circ) \subseteq \perp \\ \equiv & \{ \dots\dots\dots \} \\ &d \cdot R \cap (d \cdot p \cdot S \cup d \cdot p \cdot c \cdot a^\circ) \subseteq \perp \\ \equiv & \{ \dots\dots\dots \} \\ &\text{inv} (R, S) \wedge \underbrace{d \cdot R \cap (d \cdot p \cdot c \cdot a^\circ) \subseteq \perp}_{WP} \\ \equiv & \{ (F7) \} \\ &\text{inv} (R, S) \wedge \underbrace{d \cdot R \cdot a \subseteq (\neq) \cdot d \cdot p \cdot c}_{WP} \\ \equiv & \{ \dots\dots\dots \} \\ &\text{inv} (R, S) \wedge \underbrace{R \cdot a \subseteq d^\circ \cdot (\neq) \cdot d \cdot p \cdot c}_{WP} \\ \equiv & \{ \dots\dots\dots \} \\ &\text{inv} (R, S) \wedge \underbrace{\langle \forall x : x R a : d x \neq d (p c) \rangle}_{WP} \\ &\square \end{aligned}$$

RESOLUÇÃO: Justificações:

$$\begin{aligned}
 & \mathbf{inv} (R', S') \\
 \equiv & \quad \{ \text{definição de } \mathbf{inv} \cdot \} \\
 & d \cdot R' \cap d \cdot p \cdot S' \subseteq \perp \\
 \equiv & \quad \{ \text{pós-condição ; (73) do exercício 24 } \} \\
 & d \cdot R \cap d \cdot p \cdot (S \cup \underline{c} \cdot \underline{a}^\circ) \subseteq \perp \\
 \equiv & \quad \{ \text{distributividade (101)} \} \\
 & d \cdot R \cap (d \cdot p \cdot S \cup d \cdot p \cdot \underline{c} \cdot \underline{a}^\circ) \subseteq \perp \\
 \equiv & \quad \{ \text{distributividade da interseção pela reunião ; universal-} \cup \cdot \text{(97) ; definição de } \mathbf{inv} \cdot \} \\
 & \mathbf{inv} (R, S) \wedge \underbrace{d \cdot R \cap (d \cdot p \cdot \underline{c} \cdot \underline{a}^\circ) \subseteq \perp}_{WP} \\
 \equiv & \quad \{ (F7) \} \\
 & \mathbf{inv} (R, S) \wedge \underbrace{d \cdot R \cdot \underline{a} \subseteq (\neq) \cdot d \cdot p \cdot \underline{c}}_{WP} \\
 \equiv & \quad \{ \text{'shunting' (79)} \} \\
 & \mathbf{inv} (R, S) \wedge \underbrace{R \cdot \underline{a} \subseteq d^\circ \cdot (\neq) \cdot d \cdot p \cdot \underline{c}}_{WP} \\
 \equiv & \quad \{ \text{passagem a } \textit{pointwise} \text{ (59); (70) duas vezes; função constante (72) duas vezes} \} \\
 & \mathbf{inv} (R, S) \wedge \underbrace{\langle \forall x : x R a : d x \neq d (p c) \rangle}_{WP} \\
 \square & \\
 \square &
 \end{aligned}$$

Questão 8 A sobreposição de relações

$$R \dagger S = S \cup R \cap \perp / S^\circ, \tag{F9}$$

é um combinador muito útil para exprimir operações de *updating* em modelos relacionais. Mostre que a igualdade

$$R \dagger f = f \tag{F10}$$

se verifica para qualquer relação R e função f . (**Sugestão:** comece por simplificar o termo \perp / f° .)

RESOLUÇÃO: Cálculo de \perp / f° (justificar ao estudar):

$$\begin{aligned}
 & X \subseteq \perp / f^\circ \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & X \cdot f^\circ \subseteq \perp \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & X \subseteq \perp \cdot f \\
 \equiv & \quad \{ \dots\dots\dots \} \\
 & X \subseteq \perp
 \end{aligned}$$

\therefore { igualdade indirecta }

$$\perp / f^\circ = \perp$$

□

Logo:

$$R \dagger f = f$$

$$\equiv \{ (F9) \}$$

$$f \cup R \cap \perp / f^\circ = f$$

$$\equiv \{ \perp / f^\circ = \perp; R \cap \perp = \perp \}$$

$$f \cup \perp = f$$

$$\equiv \{ X \cup \perp = X \}$$

$$f = f$$

□

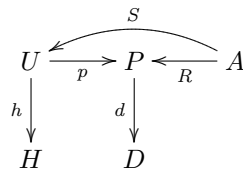
□

Apêndice: CASO DE ESTUDO — O NOVO PLANO DE ESTUDOS DO MEI

Tipos:

A – Aluno
P – Perfil
D – Dia
H – Hora
U – Unidade curricular

Relações:



Legenda:

p — dá o perfil de cada UC
h — dá a hora a que uma UC funciona
d — o dia ocupado por cada perfil
R — relaciona alunos com os seus perfis
S — relaciona alunos com as suas UCs complementares.