Cálculo de Sistemas de Informação
Perfil: MÉTODOS FORMAIS EM ENGENHARIA DE SOFTWARE

4.º Ano de MiEI, Universidade do Minho
Ano Lectivo de 2017/18

Teste — 4 de Janeiro
14h00
Sala DI 1.16

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 sem nota mínima no **miniteste** devem responder a todas as questões, entregando a prova ao fim de duas horas.*
- *Os alunos com nota mínima no **miniteste** podem optar por responder apenas à parte II (questões 5, 6, 7, 8), devendo nesse caso entregar a prova ao fim de uma hora.*

PROVA COM CONSULTA (1 ou 2 horas)

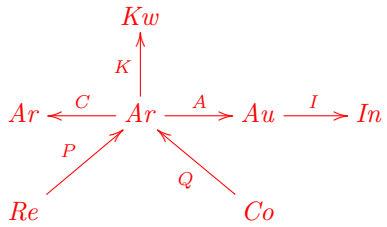
Parte I

Questão 1 Considere a seguinte lista de requisitos para a construção de um sistema de avaliação científica:

1. O sistema tem a ver com artigos (Ar), revistas (Re), conferências (Co) e instituições (In) científicas.
2. Um artigo científico tem sempre pelo menos um autor (Au), que deverá estar sempre associado a pelo menos uma instituição científica.
3. A cada artigo está associado um conjunto de palavras chave (Kw), indicadoras das áreas científicas nas quais o artigo se insere.
4. Cada artigo aparece sempre publicado, exclusivamente, numa revista ou nas actas de uma dada conferência.
5. Os artigos citam-se mutuamente; contudo, um artigo nunca se pode citar a si próprio.

Faça um diagrama que inclua todas as relações envolvidas no modelo deste sistema. Identifique-as dando-lhes nomes e associando-lhes classes relacionais (inteira, sobrejectiva, ... etc). Codifique sob a forma de desigualdades relacionais as restrições que os requisitos impõem ao sistema que se pretende modelar.

RESOLUÇÃO: Diagrama de relações propostas:



(F1)

Cláusula 2: $A : Ar \to Au$ e $I : Au \to In$ são inteiras.
Cláusula 3: $K : Ar \to Kw$ é livre — nem sempre são exigidas "keywords"
Cláusula 4: $[P, Q]^\circ$ é uma função.
Cláusula 5: C é irreflexiva, $C \subseteq (id \Rightarrow \bot)$ — ou $C \cap id \subseteq \bot$. $\Box$

Questão 2 Diz-se que duas funções f e g são *complementares* entre si sempre que $\langle f, g\rangle$ é uma função injectiva. Mostre que:

- π_1 e π_2 são complementares entre si;
- se f e g são complementares e $g \leqslant h$, então f e h são também complementares entre si.

NB: recorde que a ordem de injectividade usada em $g \leqslant h$ é definida por:

$$R \leqslant S \quad \equiv \quad \ker S \subseteq \ker R \tag{F2}$$

RESOLUÇÃO: Primeira parte: $\langle \pi_1, \pi_2\rangle = id$ por reflexão, o que de imediato garante que $\langle \pi_1, \pi_2\rangle$ é injectiva. Cálculo da segunda parte (preencham as justificações):

f e h complementares

$\equiv$ { ..... }

$\ker \langle f, h\rangle \subseteq id$

$\equiv$ { ..... }

$\ker f \cap \ker h \subseteq id$

$\equiv$ { ..... }

$\ker h \subseteq \ker f \Rightarrow id$

$\Leftarrow$ { ..... }

$\ker h \subseteq \ker g \wedge \ker g \subseteq \ker f \Rightarrow id$

$\equiv$ { ..... }

$g \leqslant h \wedge \ker g \cap \ker f \subseteq id$

$\equiv$ { ..... }

$g \leqslant h \wedge \ker \langle f, g\rangle \subseteq id$

□

□

Questão 3 Uma relação R diz-se *difuncional* sempre que $R \cdot R^\circ \cdot R \subseteq R$. As relações $\bot$ e $\top$ são exemplos de relações difuncionais. Mostre que uma divisão de funções $R = \frac{f}{g}$ é sempre difuncional, quaisquer que sejam f e g devidamente tipadas.

RESOLUÇÃO: Justificar os passos da demonstração proposta:

$\frac{f}{g} \cdot \frac{g}{f} \cdot \frac{f}{g} \subseteq \frac{f}{g}$

$\equiv$ { ..... }

$g^\circ \cdot f \cdot f^\circ \cdot g \cdot g^\circ \cdot f \subseteq \frac{f}{g}$

$\Leftarrow$ { ..... }

$g^\circ \cdot f \subseteq \frac{f}{g}$

$\equiv$ { ..... }

$\frac{f}{g} \subseteq \frac{f}{g}$

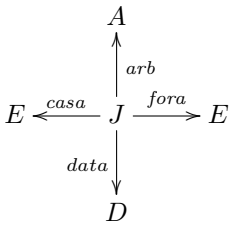
$\equiv$ { ..... }

$true$

□

□

Questão 4 As equipas (E) de um campeonato têm jogos (J) em casa e jogos fora; todo o jogo ocorre numa data (D) e tem um árbitro (A):



A divisão $\frac{cf}{fc}$ onde $cf = \langle casa, fora\rangle$ e $fc = \langle fora, casa\rangle$ relaciona dois jogos "simétricos", isto é, em que as equipas trocam de casa:

$$j' \ \frac{cf}{fc} \ j \ \Leftrightarrow \ casa\ j' = fora\ j \wedge fora\ j' = casa\ j$$

Uma das regras do campeonato é a de que cada jogo tem sempre um e um só jogo "simétrico": $\frac{cf}{fc}$ tem de ser uma bijecção. Isto quer dizer que $\frac{cf}{fc}$ e $\frac{fc}{cf}$ têm de ser funções.

Generalizando esta situação, mostre que para a divisão $\frac{f}{g}$ de duas funções (que é uma relação) ser ela própria uma função, basta que g seja injectiva e que $g^\circ \leqslant f^\circ$, onde $\leqslant$ é a ordem de injectividade que conhece das aulas e que vem dada nesta prova por (F2).

RESOLUÇÃO: Preencher justificações em:

$\frac{f}{g}$ é função

$\equiv$ { ..... }

$id \subseteq \ker \frac{f}{g} \wedge \mathrm{img}\ \frac{f}{g} \subseteq id$

$\equiv$ { ..... }

$id \subseteq \frac{g}{f} \cdot \frac{f}{g} \wedge \frac{f}{g} \cdot \frac{g}{f} \subseteq id$

$\equiv$ { ..... }

$\mathrm{img}\ f \subseteq \mathrm{img}\ g \wedge g^\circ \cdot \mathrm{img}\ f \cdot g \subseteq id$

$\equiv$ { ..... }

$g^\circ \leqslant f^\circ \wedge g^\circ \cdot \mathrm{img}\ f \cdot g \subseteq id$

$\Leftarrow$ { ..... }

$g^\circ \leqslant f^\circ \ \wedge \ g^\circ \cdot g \ \subseteq \ id$

$\equiv$ { ..... }

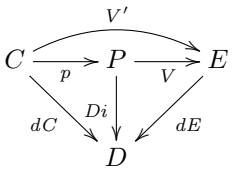
$g^\circ \leqslant f^\circ \ \wedge \ g$ injectiva

□

□

Parte II

Questão 5 Recorde do miniteste o modelo de um sistema eleitoral electrónico de inspiração uninominal (i.e., em que se pode votar directamente nos candidatos e não apenas nos respectivos partidos) cujo diagrama relacional se apresenta de seguida,



onde

- $p \ c$ designa o partido a que o candidato c pertence
- $dC \ c$ designa o distrito pelo qual c é candidato
- $dE \ e$ designa o distrito do eleitor e
- $d \ Di \ p$ regista que o partido p concorre às eleições no distrito d
- $e \ V \ p$ indica que o eleitor e votou no partido p
- $e \ V' \ c$ indica que o eleitor e votou directamente no candidato c.

Neste modelo há vários invariantes, a saber:

$$inv_1 \ (V, V') = V : E \leftarrow P \text{ e } V' : E \leftarrow C \text{ são injectivas} \tag{F3}$$

$$inv_2 \ (V, V') = V^\circ \cdot V' = \bot \tag{F4}$$

pois um eleitor não pode votar em mais do que um candidato ou partido;

$$inv_3 \ (V, V') \quad = \quad dE \cdot [V, V'] \ \subseteq \ [Di, dC] \tag{F5}$$

pois cada eleitor está registado num distrito e só pode votar em candidatos ou partidos que concorram pelo seu distrito.

No acto eleitoral, as relações p, dC, dE e Di são estáticas, pois os cadernos eleitorais ficam definidos antes das eleições. Para apuramento dos votos correm duas funções,

$$apuraP \ (V, V', e, p) = (V \cup \underline{e} \cdot \underline{p}^\circ, V')$$
$$apuraC \ (V, V', e, c) = (V, V' \cup \underline{e} \cdot \underline{c}^\circ)$$

Mostre que a pré-condição mais fraca ("weakest precondition") para $apuraP$ preservar o invariante inv_2 é o predicado

$$pre2 \ (V, V', e, p) = \neg \ \langle \exists \ c \ :: \ e \ V' \ c \rangle$$

isto é: para se apurar o voto de e no partido p é preciso que e não tenha votado já num candidato c.

RESOLUÇÃO: Justificar os passos da resolução proposta:

$inv_2 \ (apuraP \ (V, V', e, p))$

$\equiv$ { ..... }

$inv_2 \ (V \cup \underline{e} \cdot \underline{p}^\circ, V')$

$\equiv$ { ..... }

$(V^\circ \cup \underline{p} \cdot \underline{e}^\circ) \cdot V' \ \subseteq \ \bot$

$\equiv$ { ..... }

$$\left\{ \begin{array}{l} V^\circ \cdot V' \subseteq \bot \\ \underline{p} \cdot \underline{e}^\circ \cdot V' \subseteq \bot \end{array} \right.$$

$\equiv$ { ..... }

$$\underline{e}^\circ \cdot V' \subseteq \bot$$

$\equiv$ { ..... }

$$\langle \forall\ c\ :\ e\ V'\ c :\ false \rangle$$

$\equiv$ { ..... }

$$\neg \langle \exists\ c\ ::\ e\ V'\ c \rangle$$

□

□

Questão 6 A verificação de código envolvendo cálculos de números reais é muitas vezes feita com base numa *interpretação abstracta* chamada *análise de sinal*:

$$\begin{array}{l} sign : \mathbb{R} \to \{-, 0, +\} \\ sign\ 0 = 0 \\ sign\ x = \mathbf{if}\ x > 0\ \mathbf{then}\ +\ \mathbf{else}\ - \end{array}$$

Suponha que alguém prova que a operação $\theta : \{-, 0, +\}^2 \to \{-, 0, +\}$ definida por

θ	$-$	0	$+$
$-$	$+$	0	$-$
0	0	0	0
$+$	$-$	0	$+$

(F6)

é a simulação abstracta induzida por $sign$ de uma dada operação concreta $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, isto é, que

$$\theta \cdot (sign \times sign) = sign \cdot f \tag{F7}$$

se verifica. É fácil de ver, por inspecção de (F6), que θ é uma operação comutativa, isto é, que

$$\mathsf{swap} \subseteq \frac{\theta}{\theta} \tag{F8}$$

se verifica.

- Mostre que $sign \cdot f$ é necessariamente comutativa também. (Sugestão: o "free theorem" de swap pode ser-lhe útil.)
- Dará a alínea anterior garantias de que a operação concreta f é também comutativa? Jutifique informalmente.

RESOLUÇÃO: Primeira parte (justificar):

$$\mathsf{swap} \subseteq \frac{sign \cdot f}{sign \cdot f}$$

$\equiv$ { ..... }

$$\mathsf{swap} \subseteq \frac{\theta \cdot (sign \times sign)}{\theta \cdot (sign \times sign)}$$

$\equiv$ { ..... }

$\theta \cdot (sign \times sign) \cdot \mathsf{swap} = \theta \cdot (sign \times sign)$

$\equiv$ { ..... }

$\theta \cdot \mathsf{swap} \cdot (sign \times sign) = \theta \cdot (sign \times sign)$

$\equiv$ { ..... }

$\theta \cdot (sign \times sign) = \theta \cdot (sign \times sign)$

$\equiv$ { ..... }

$true$

$\square$

Segunda parte: o objectivo é ver se $\mathsf{swap} \subseteq \frac{f}{f}$ deriva de $\mathsf{swap} \subseteq \frac{sign \cdot f}{sign \cdot f}$, que é equivalente a $\mathsf{swap} \subseteq f^\circ \cdot \frac{sign}{sign} \cdot f$. Para isso bastaria que $sign$ fosse injectiva, mas não o é. Todos os positivos são mapeados em $+$ e todos os negativos em $-$. $\square$

Questão 7 Sabendo que a soma de relações tem as propriedades de um *relator* (binário), mostre que:

$$\ker\ (R + S) = \ker\ R + \ker\ S \tag{F9}$$

De seguida, recordando $[R, S] = R \cdot i_1^\circ \cup S \cdot i_2^\circ$, mostre que

$$[R, S] \leqslant (R + S) \tag{F10}$$

onde $\leqslant$ é a ordem de injectividade que conhece das aulas e que vem dada nesta prova por (F2).

RESOLUÇÃO: Primeira parte:

$\ker\ (R + S)$

$=$ { definição $\ker\ R = R^\circ \cdot R$ }

$(R + S)^\circ \cdot (R + S)$

$=$ { relator $+$ preserva conversos }

$(R^\circ + S^\circ) \cdot (R + S)$

$=$ { relator $+$ respeita a composição }

$R^\circ \cdot R + S^\circ \cdot S$

$=$ { $\ker\ R = R^\circ \cdot R$ (duas vezes) }

$\ker\ R + \ker\ S$

$\square$

Segunda parte (completar justificações):

$[R, S] \leqslant (R + S)$

$\equiv$ { ..... }

$\ker\ R + \ker\ S\ \subseteq\ \ker\ [R, S]$

$\equiv$ { ..... }

$\ker\ R + \ker\ S\ \subseteq\ (i_1 \cdot R^\circ \cup i_2 \cdot S^\circ) \cdot (R \cdot i_1^\circ \cup S \cdot i_2^\circ)$

$\equiv$ { ..... }

$\ker\ R + \ker\ S\ \subseteq\ i_1 \cdot (R^\circ \cdot R) \cdot i_1^\circ \cup i_1 \cdot (R^\circ \cdot S) \cdot i_2^\circ \cup i_2 \cdot (S^\circ \cdot R) \cdot i_1^\circ \cup i_2 \cdot (S^\circ \cdot S) \cdot i_2^\circ$

$$
\begin{array}{ll}
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& \ker R + \ker S \ \subseteq \ (\ker R + \ker S) \cup i_1 \cdot (R^\circ \cdot S) \cdot i_2^\circ \cup i_2 \cdot (S^\circ \cdot R) \cdot i_1^\circ \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& true \\
\Box &
\end{array}
$$

$\Box$

Questão 8 Considere listas de elementos indexados por números naturais. Dado um índice, pretendemos obter o primeiro elemento de uma tal lista que tem esse índice, caso exista, definindo a função:

$$get : \mathbb{N}_0 \to (\mathbb{N}_0 \times A)^* \to (A + 1)$$

Mostre que a propriedade

$$get\ n\ [(i, r\ a) \mid (i, a) \leftarrow x] = (r + id)\ (get\ n\ x) \tag{F11}$$

é um corolário do teorema grátis da função get, onde r é uma função.

RESOLUÇÃO: Propõe-se:

$$
\begin{array}{ll}
& get\ ((R + id) \leftarrow (id \times R)^* \leftarrow id)\ get \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& get \ \subseteq \ ((R + id) \leftarrow (id \times R)^*) \cdot get \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& (get\ n)\ ((R + id) \leftarrow (id \times R)^*)\ (get\ n) \\
\equiv & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \} \\
& (get\ n) \cdot (id \times R)^* \ \subseteq \ (R + id) \cdot (get\ n)
\end{array}
$$

Caso $R := r$ (função):

$$(get\ n) \cdot \mathsf{map}\ (id \times r) = (r + id) \cdot (get\ n)$$

que é o mesmo que $get\ n\ [(i, r\ a) \mid (i, a) \leftarrow x] = (r + id)\ (get\ n\ x)$ introduzindo variáveis e expandindo $\mathsf{map}\ (id \times r)$ (map de listas). $\Box$
