**Cálculo de Sistemas de Informação**
Perfil: MÉTODOS FORMAIS DE PROGRAMAÇÃO

1.º Ano de MEI e MMC, Universidade do Minho
Ano Lectivo de 2021/22

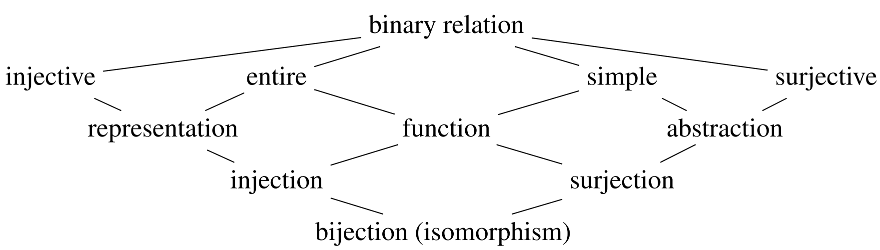
1º Teste — 5 de Maio de 2022
16h00–18h00
Sala E1-1.19

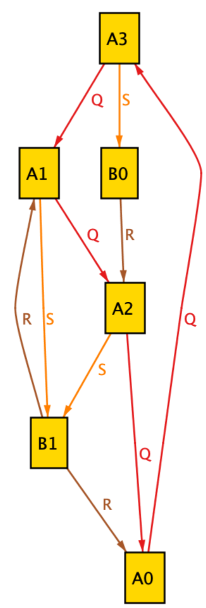
---

*Esta prova consta de **8** questões 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** Sejam dados os tipos de dados $A$ (com quatro elementos) e $B$ (com dois elementos) que constam do diagrama Alloy que se mostra ao lado. Tendo em conta a taxonomia relacional básica estudada nesta disciplina,




verifique (justificando) se alguma das três relações visualizadas no diagrama

1. é uma injecção
2. é uma representação
3. é uma abstração.

---

RESOLUÇÃO: Tem-se:

$Q$ =

| | A0 | A1 | A2 | A3 |
|---|---|---|---|---|
| A0 | | | 1 | |
| A1 | | | | 1 |
| A2 | | 1 | | |
| A3 | 1 | | | |

$R$ =

| | B0 | B1 |
|---|---|---|
| A0 | | 1 |
| A1 | | 1 |
| A2 | 1 | |
| A3 | | |

$S$ =

| | A0 | A1 | A2 | A3 |
|---|---|---|---|---|
| B0 | | | | 1 |
| B1 | | 1 | 1 | |

$\underbrace{Inj, Ent, Sim, Srj}_{Bij}$ $\qquad$ $\underbrace{Inj, Ent}_{Rep}, \neg\, Sim, \neg\, Srj$ $\qquad$ $\neg\, Inj, \neg\, Ent, \underbrace{Sim, Srj}_{Abs}$

Logo:

| | $Q$ | $R$ | $S$ |
|---|---|---|---|
| 1 | ✓ | | |
| 2 | ✓ | ✓ | |
| 3 | ✓ | | ✓ |

□

**Questão 2** Justifique a prova que se segue do facto elementar $id^\circ = id$:

$$
\begin{array}{ll}
& X \subseteq id \\
\equiv & \quad \{ \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; \} \\
& id \cdot X \subseteq id \\
\equiv & \quad \{ \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; \} \\
& X \subseteq id^\circ \cdot id \\
\equiv & \quad \{ \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; \} \\
& X \subseteq id^\circ \\
:: & \quad \{ \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; \} \\
& id \;=\; id^\circ
\end{array}
$$

---

RESOLUÇÃO: Tem-se:

$$
\begin{array}{ll}
& X \subseteq id \\
\equiv & \quad \{ \; id \text{ elemento neutro da composição relacional } \} \\
& id \cdot X \subseteq id \\
\equiv & \quad \{ \; \text{shunting: } (f\cdot) \dashv (f^\circ\cdot) \; \} \\
& X \subseteq id^\circ \cdot id \\
\equiv & \quad \{ \; id \text{ elemento neutro da composição relacional } \} \\
& X \subseteq id^\circ \\
:: & \quad \{ \; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \; \} \\
& id \;=\; id^\circ
\end{array}
$$

□

---

**Questão 3** Em linguagens como Haskell as listas (sequências finitas) podem ser manipuladas como estruturas recursivas $A^* \cong 1 + A \times A^*$ ou como estruturas indexadas, isto é relações simples em $\mathbb{N}_0 \to A$ que associam elementos a posições na lista, por exemplo $[a, b, z, a] \,!!\, 2 = z$ etc.

Especificam-se de seguida algumas operações habituais sobre uma lista $\mathbb{N}_0 \xrightarrow{L} A$ encarada como estrutura indexada,

$$a : L = [\underline{a}, L] \cdot \mathsf{in}^\circ \tag{F1}$$

$$\mathsf{tail}\ L = L \cdot \mathsf{succ} \tag{F2}$$

$$\mathsf{head}\ L = L \cdot \mathsf{zero} \tag{F3}$$

onde $a \in A$ e $\mathsf{in} = [\mathsf{zero}, \mathsf{succ}]$ é o *isomorfismo* de construção dos números naturais (normalmente conhecido por "álgebra de Peano"), para $\mathsf{zero}\ x = 0$ e $\mathsf{succ}\ n = n + 1$. Demonstre a propriedade

$$\mathsf{tail}\ (a : L) = L$$

usando o cálculo relacional e as definições dadas.

---

RESOLUÇÃO: Tem-se:

$$
\begin{array}{ll}
& \mathsf{tail}\ (a : L) = L \\
\equiv & \quad \{\ \text{(F1) e (F2)}\ \} \\
& [\underline{a}\,, \underline{L}] \cdot \mathsf{in}^\circ \cdot \mathsf{succ} = L \\
\equiv & \quad \{\ \mathsf{in} = [\mathsf{zero}\,, \mathsf{succ}]\ \} \\
& [\underline{a}\,, \underline{L}] \cdot \mathsf{in}^\circ \cdot \mathsf{in} \cdot i_2 = L \\
\equiv & \quad \{\ \mathsf{in}\ \text{é uma bijecção}\ \} \\
& [\underline{a}\,, \underline{L}] \cdot i_2 = L \\
\equiv & \quad \{\ \text{cancelamento-}+\ \} \\
& L = L \\
\Box &
\end{array}
$$

A igualdade indirecta não é necessária neste caso. A alternativa que expande in e simplifica tem bastantes mais passos: $\mathsf{in}^\circ \cdot \mathsf{succ} = (\mathsf{succ}^\circ \cdot \mathsf{in})^\circ = [\mathsf{succ}^\circ \cdot \mathsf{zero}\,, \mathsf{succ}^\circ \cdot \mathsf{succ}]^\circ = [\bot\,, id]^\circ = i_2$ $\Box$

---

**Questão 4** Tal como se viu nas aulas, uma relação $R$ diz-se *difuncional* sempre que satisfaz a propriedade

$$R \cdot R^\circ \cdot R \ \subseteq \ R.$$

Suponha que $Q = S^\circ \cdot P$, onde $S$ e $P$ são relações *simples*. Mostre que $Q$ é necessariamente difuncional.

---

RESOLUÇÃO:

$$
\begin{array}{ll}
& S^\circ \cdot P \cdot P^\circ \cdot S \cdot S^\circ \cdot P \ \subseteq \ S^\circ \cdot P \\
\Leftarrow & \quad \{\ S\ \text{é simples e}\ P\ \text{também: duas vezes subida do lado inferior}\ \} \\
& S^\circ \cdot id \cdot id \cdot P \ \subseteq \ S^\circ \cdot P \\
\equiv & \quad \{\ R \cdot id = R = id \cdot R\ \} \\
& S^\circ \cdot P \ \subseteq \ S^\circ \cdot P \\
\equiv & \quad \{\ \text{trivial}\ \} \\
& \mathit{true} \\
\Box &
\end{array}
$$

$\Box$

---

**Questão 5** Nos inteiros ($\mathbb{Z}$), a operação de subtracção é um isomorfismo, $(\_ - b)^\circ = (\_ + b)$, isto é,

$$a - b = x \ \Leftrightarrow \ a = x + b$$

Mas, restrita aos naturais ($\mathbb{N}_0$) deixa de o ser. O que se verifica em $\mathbb{N}_0$ é a conexão de Galois

$$(\_ \ominus b)^\circ \cdot (\leqslant) = (\leqslant) \cdot (\_ + b)$$

que se expande para a equivalência

$$a \ominus b \leqslant x \;\Leftrightarrow\; a \leqslant x + b \tag{F4}$$

que pode ser tomada como a **especificação formal** de $a \ominus b$ em $\mathbb{N}_0$.

Mostre, usando (F4) e a igualdade indirecta sobre $(\leqslant)$ em $\mathbb{N}_0$, que qualquer implementação (correcta!) de $a \ominus b$ deverá observar as seguintes propriedades:

$$a \ominus 0 = a \tag{F5}$$

$$a \ominus a = 0 \tag{F6}$$

$$a \leqslant (a \ominus b) + b \tag{F7}$$

**Sugestão**: recordar raciocínios semelhantes feitos nas aulas sobre a função `take`.

---

RESOLUÇÃO: Propriedade (F5):

$$
\begin{array}{ll}
 & a \ominus 0 \leqslant x \\
\equiv & \quad \{ \text{ (F4) } \} \\
 & a \leqslant x + 0 \\
\equiv & \quad \{ \ x + 0 = x \ \} \\
 & a \leqslant x \\
:: & \quad \{ \text{ igualdade indirecta } \} \\
 & a \ominus 0 = a \\
\Box &
\end{array}
$$

Propriedade (F6):

$$
\begin{array}{ll}
 & a \ominus a \leqslant x \\
\equiv & \quad \{ \text{ (F4) } \} \\
 & a \leqslant x + a \\
\equiv & \quad \{ \text{ 0 é elemento neutro de } + \ \} \\
 & 0 + a \leqslant x + a \\
\equiv & \quad \{ \ (+a) \text{ é injectiva em } \mathbb{N}_0 \ \} \\
 & 0 \leqslant x \\
:: & \quad \{ \text{ igualdade indirecta } \} \\
 & a \ominus a = 0 \\
\Box &
\end{array}
$$

Propriedade (F7):

$$
\begin{array}{ll}
 & a \leqslant (a \ominus b) + b \\
\equiv & \quad \{ \text{ (F4) } \} \\
 & a \ominus b \leqslant a \ominus b \\
\equiv & \quad \{ \text{ trivial } \} \\
 & \mathit{true} \\
\Box &
\end{array}
$$

$\Box$

---

**Questão 6** Em anexo dá-se um modelo Alloy ('Instagram') que foi assunto das aulas de MFES (1º semestre) e para o qual se mostra a seguir o diagrama de tipos relacional, seguindo a convenção de se designarem funções por minúsculas:

$$\begin{tikzcd}
 & Photo \arrow[dl, "date"'] \arrow[d, "ad"'] \arrow[drr, "posted"] \arrow[rr, "Sees"] & & User \arrow[d, "Follows"] \\
Day & \mathbb{B} & & User \arrow[ll, "influencer"]
\end{tikzcd}$$

São dadas as definições:

$$Is\_ad = \frac{ad}{true} \tag{F8}$$

$$Is\_not\_ad = \frac{ad}{false} \tag{F9}$$

$$Is\_inf = \frac{influencer}{true} \tag{F10}$$

$$(\neq) = id \Rightarrow \bot \tag{F11}$$

O modelo em Alloy prevê seis propriedades invariantes que são enunciadas verbalmente no anexo. As inequações relacionais seguintes são candidatas a exprimir essas propriedades, quando escritas em notação relacional "point-free":

$$Is\_ad \cdot \frac{posted}{posted} \subseteq Is\_ad \tag{F12}$$

$$Is\_not\_ad \cap Sees \subseteq Follows \cdot posted \tag{F13}$$

$$\top \setminus Follows \subseteq Is\_inf \tag{F14}$$

$$Is\_ad \subseteq Sees \tag{F15}$$

$$date \cdot posted^{\circ} \subseteq Is\_inf \tag{F16}$$

$$Follows \subseteq (\neq) \tag{F17}$$

Indique, para cada inequação, se algum dos invariantes pedidos é por ela adequadamente modelado, justificando a sua resposta em cada caso.

---

RESOLUÇÃO:

- (F12) $\mapsto inv_4$,

  $inv_4$: *If an user posts an ad then all its posts should be labelled as ads*

  pois, para quaisquer $p, q$,

  $$\langle \forall\ q\ :\ \langle \exists\ p\ :\ ad\ p :\ posted\ p = posted\ q \rangle :\ ad\ q \rangle$$

- (F13) $\mapsto inv31$,

  *An user only sees (non ad) photos posted by followed users*

  cf.

  $$Is\_not\_ad \cap Sees \subseteq Follows \cdot posted$$

  equivalente a:

  $$\langle \forall\ u, p\ :\ ad\ p \wedge u\ Sees\ p :\ u\ Follows\ (posted\ p) \rangle$$

- (F14) tem a ver com $inv_5$,

  *Influencers are followed by everyone else* mas $\top$ é liberal de mais, teria que ser $(\neq)$, o que daria, para todo o user $u$:

$$\langle \forall\ v\ :\ v \neq u :\ v\ \mathit{Follows}\ u \rangle \Rightarrow \mathit{influencer}\ u$$

- (F15) $\mapsto \mathit{inv32}$;
- (F16): para corresponder ao $\mathit{inv_6}$,

  *Influencers post every day*

  a desigualdade está ao contrário, devendo ser

  $$\mathit{Is\_inf} \ \subseteq\ \mathit{date} \cdot \mathit{posted}^\circ$$

  que exprime a obrigação pedida.
- (F17) $\mapsto \mathit{inv_2}$;

  *An user cannot follow itself.*
- $\mathit{inv_1}$ é captado por $\mathit{posted}$ ser função.

$\square$

---

**Questão 7** A semântica da linguagem de processos CCS (estudada em PCF) define-se com base nos chamados "*labelled transition systems*" (LTS) não-determinísticos. Tais LTS podem ser vistos como relações binárias $X \xleftarrow{R} X \times \Lambda$ onde $x'\ R\ (x, \alpha)$ indica que o LTS $R$ admite a **transição** $x' \xleftarrow{\alpha} x$ .

Dados dois LTS, $Y \xleftarrow{R} Y \times \Lambda$ e $X \xleftarrow{S} X \times \Lambda$ , uma relação $X \xleftarrow{P} Y$ diz-se uma simulação de $S$ por $R$ se se tiver:

$$\begin{tikzcd} X \times \Lambda \arrow[d, "S"'] & Y \times \Lambda \arrow[l, "P \times id"'] \arrow[d, "R"] \\ X & Y \arrow[l, "P"] \arrow[ul, phantom, "\subseteq"] \end{tikzcd} \qquad S \cdot (P \times id) \subseteq P \cdot R$$

Mostre que:

- A relação vazia $P = \bot$ é sempre uma simulação entre quaisquer $S$ e $R$, e $P = id$ é uma simulação entre $S$ e ele próprio.
- Sempre que a simulação $P = \frac{f}{g}$ é um quociente de duas observações $X \xrightarrow{g} Z \xleftarrow{f} Y$ , então tem-se que $f$ é uma simulação de $S' = g \cdot S \cdot (g^\circ \times id)$ por $R$. (Identifique também o tipo de $S'$).

---

RESOLUÇÃO: Primeira alínea: $\bot \subseteq P \cdot R$ e $S \cdot (id \times id) \subseteq id \cdot S$.
Segunda alínea:

$$\begin{array}{cl} & S \cdot (g^\circ \cdot f \times id) \subseteq g^\circ \cdot f \cdot R \\ \equiv & \quad \{ \text{ functor } \times \text{ em Rel } \} \\ & S \cdot (g^\circ \times id) \cdot (f \times id) \subseteq g^\circ \cdot f \cdot R \\ \equiv & \quad \{ \text{ shunting } \} \\ & \underbrace{g \cdot S \cdot (g^\circ \times id)}_{S'} \cdot (f \times id) \subseteq f \cdot R \end{array}$$

Tipo: $S' : Z \times \Lambda \to Z$.
□

---

**Questão 8** Vamos designar por $\mathcal{P}\ A$ o tipo habitado pelos subconjuntos de $A$, isto é, $\mathcal{P}\ A = \{S \mid S \subseteq A\}$ em

$$A \xrightarrow{(\geqslant)} A \xleftarrow{\in} \mathcal{P}\ A$$

onde se assume que a ordem $(\geqslant)$ é linear e onde $a \in S$ designa a relação de pertença entre elementos de $A$ e subconjuntos de $A$. Seja agora $M$ a relação:

$$M = \in \upharpoonright (\geqslant) \tag{F18}$$

Que relação é essa? Trata-se de uma relação *inteira* ou não? Justifique a sua resposta interpretando o significado de $a\ M\ x$.

---

RESOLUÇÃO: Tem-se:

$$\begin{array}{ll} & a\ M\ x \\ \equiv & \quad \{\ \text{expansão da definição dada: } M = \in \upharpoonright (\geqslant)\ \} \\ & a\ (\in \cap\ (\geqslant)/\in^{\circ})\ x \\ \equiv & \quad \{\ \text{intersecção pointwise}\ \} \\ & a \in x \wedge a\ ((\geqslant)/\in^{\circ})\ x \\ \equiv & \quad \{\ \text{divisão pointwise}\ \} \\ & a \in x \wedge \langle \forall\ a' : a' \in x : a \geqslant a' \rangle \end{array}$$

Logo $M$ é a relação máximo de um conjunto linearmente ordenado. Não é inteira pois $a \in \{\ \} = $ FALSE (o conjunto vazio não tem máximo).
□

---

## Anexo — modelo Instagram (em Alloy) ©MFES 2022

```
sig User {
  follows : set User,
  sees : set Photo,
  posts : set Photo
}
sig Influencer extends User { }
sig Photo {
  date : one Day
}
sig Ad extends Photo { }
sig Day { }
// Specify the following properties
// You can check their correctness with the different commands and
// when specifying each property you can assume all the previous ones to be true
pred inv1 {
  // Every image is posted be one user
```

```
}
pred inv2 {
  // An user cannot follow itself ·
}
pred inv3 {
  // An user only sees (non ad) photos posted by followed users ·
  // Ads can be seen by everyone ·
}
pred inv4 {
  // If an user posts an ad then all its posts should be labelled as ads
}
pred inv5 {
  // Influencers are followed by everyone else
}
pred inv6 {
  // Influencers post every day
}
```