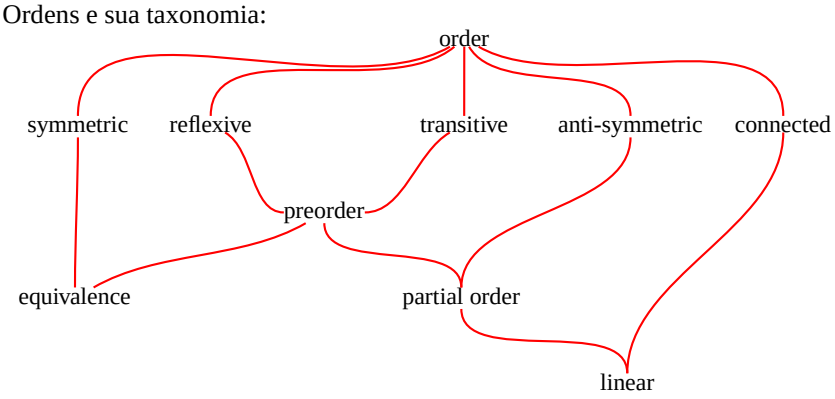
# Universidade do Minho

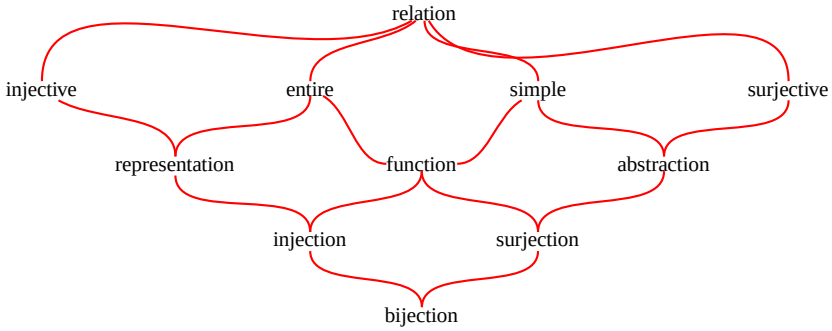
| 2005/2006 | 1.º Semestre ☒ | 2.º Semestre ☐ | Anual ☐ |
|---|---|---|---|
| DISCIPLINAS Métodos Formais de Programação I (7007N2) + Opção I — Métodos Formais de Programação I (5307P6)<br>CURSOS LMCC + LESI | DOCENTES J.N. Oliveira - 406006<br>L.S. Barbosa - 406023 | | |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.09.22<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Apresentação da disciplina. Equipa docente. Programa da disciplina e seu enquadramento no plano de estudos. Regime de avaliação. Informação electrónica sobre a disciplina: URL: `http://www.di.uminho.pt/~jno/html/mi.html`. Bibliografia. Introdução à especificação formal como método de *controlo de qualidade* em 'software'. Motivação: especificação formal — porquê e para quê? Introdução ao binómio *especificação /implementação*. Adopção do 'standard' ISO/IEC 13817-1 (VDM-SL).<br><br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.09.29<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Ciclo de vida do desenvolvimento formal de 'software'. Especificação formal construtiva. Modelação de um problema. Prototipagem e animação. Validação por teste. Importância da verificação formal das propriedades de um modelo. Não-determinismo e parcialidade. Necessidade de modelar com *relações*. Introdução ao cálculo de relações. Inclusão de relações:<br>$$R \subseteq S \quad \equiv \quad \langle \forall\, b, a \;::\; bRa \Rightarrow bSa \rangle \qquad (1)$$<br>Composição e intersecção de relações:<br>$$b(R \cdot S)c \quad \equiv \quad \langle \exists\, a \;::\; bRa \;\wedge\; aSc \rangle \qquad (2)$$<br>$$b(R \cap S)c \quad \equiv \quad bRc \;\wedge\; bSc \qquad (3)$$<br>Monotonia da composição:<br>$$\frac{\begin{array}{c} R \subseteq S \\ T \subseteq U \end{array}}{(R \cdot T) \subseteq (S \cdot U)} \qquad (4)$$<br><br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.10.06<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | *Cálculo de relações (cont.):* Conversa de uma relação<br>$$a(R^\circ)b \equiv bRa \quad (5)$$<br>e a propriedade de contravariância<br>$$(R \cdot S)^\circ = S^\circ \cdot R^\circ \quad (6)$$<br>Ordens e sua taxonomia:<br>  <br><br>As funções vistas como casos particulares de relações:<br>$$b\ f\ a \quad \equiv \quad b = f\ a \quad (7)$$<br>como caso particular de<br>$$b(f^\circ \cdot R \cdot g)a \quad \equiv \quad (f\ b)R(g\ a) \quad (8)$$<br>Formulação de propriedades em notação “pointfree”. Exemplo — injectividade de uma função $f$:<br>$$f^\circ \cdot f \quad \subseteq \quad id \quad (9)$$<br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.10.13<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | *Cálculo de relações (cont.):* Os operadores *ker* e *img*:<br>$$\mathsf{ker}\ R \stackrel{\text{def}}{=} R^\circ \cdot R \quad (10)$$<br>$$\mathsf{img}\ R \stackrel{\text{def}}{=} R \cdot R^\circ \quad (11)$$<br>*(v.s.f.f.)* |

| | |
|---|---|
| *(cont.)* | Relações inteiras (totais), sobrejectivas e simples (funcionais). Taxonomia de relações binárias:<br>  <br><br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.10.20<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | A igualdade entre relações, "pointwise"<br>$$R = S \quad \equiv \quad \langle \forall\ a, b\ ::\ bRa \equiv bSa \rangle \qquad (12)$$<br>e "pointfree":<br>-inclusão cíclica (vulg "ping-pong"):<br>$$R = S \quad \equiv \quad R \subseteq S \wedge S \subseteq R \qquad (13)$$<br>-igualdade indirecta:<br>$$R = S \quad \equiv \quad \forall X.(X \subseteq R \equiv X \subseteq S) \qquad (14)$$<br>$$\equiv \quad \forall X.(R \subseteq X \equiv S \subseteq X) \qquad (15)$$<br>*(v.s.f.f.)* |

*(cont.)*

Funções como casos particulares de relações: estudo do quadro

| Pointwise | Pointfree | |
|---|---|---|
| "Left" Uniqueness | | |
| $b\ f\ a\ \wedge\ b'\ f\ a \quad \Rightarrow \quad b = b'$ | $\mathsf{img}\ f \quad \subseteq \quad id$ | ($f$ is simple) (16) |
| Leibniz principle | | |
| $a = a' \quad \Rightarrow \quad f\ a = f\ a'$ | $id \quad \subseteq \quad \mathsf{ker}\ f$ | ($f$ is entire) |

e sua equivalência a qualquer uma das propriedades

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \tag{17}$$
$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{18}$$

(ver anexo.)
Igualdade de funções:

$$f \subseteq g \equiv f = g \equiv f \supseteq g \tag{19}$$

(ver anexo.)

O DOCENTE _____

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.10.27<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Estruturação do cálculo relacional com base em conecções de Galois (CG):<br><br>função adjunta superior<br>$\underbrace{f}\ b \leq a \quad \equiv \quad b \sqsubseteq \overbrace{g}\ a$<br>função adjunta inferior<br><br>Quadro das principais CG do cálculo relacional (ver pág. 8). As propriedades básicas de uma CG intuídas a partir da que define a divisão inteira de números naturais:<br><br>$q \times d \leq n \equiv q \leq n/d$ (20)<br><br>Exemplos: converso, regras de "shunting", divisão relacional. Intersecção e união. Versões relacionais de $\langle R, S\rangle$ e $[R\ ,S]$ como conecções de Galois.<br><br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.11.03<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Significado de uma especificação via pré/pós-condições em VDM-SL. Semântica relacional de um par **pre-** / **post-**:<br>$$Spec \stackrel{\text{def}}{=} Post \cdot Pre$$<br>Papel da pre-condição.<br>Representação de predicados unários (conjuntos) por coreflexivas ou por condições:<br>$$R \text{ é correflexiva} \equiv R \subseteq id$$<br>$$R \text{ é condição} \equiv R \subseteq !$$<br>Exemplos: $Sqrt = sq^\circ$ e $Sort = IsOrdered \cdot IsPermutation$.<br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.11.10<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Relações em compreensão. Relações simples finitas e sua representação em VDM-SL ("mappings"). Uso do operador ker $f$ em pós-condições para especificar relações de equivalência. Exemplo: $isPermutation = \ker seq2bag$.<br>Semântica relacional dos operadores de VDM-SL.<br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.11.17<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Versão relacional do condicional de McCarthy e sua utilização na semântica do operador de sobreposição de funções parciais finitas.<br>Definição de uma relação. Domínio e contradomínio como conecções de Galois:<br><br>**Descr.** \| $f = g^\flat$ \| $g = f^\sharp$ \| **Obs.**<br>domain \| dom \| $(\top \cdot)$ \| $\subseteq$ inferior restrita a coreflexivas<br>range \| rng \| $(\cdot \top)$ \| $\subseteq$ inferior restrita a coreflexivas<br><br>Significado informal de um *invariante* em VDM-SL. Preservação de um invariante $inv$ por uma função $Bool \xleftarrow{inv} A$ :<br>$$\langle \forall\ a\ :\ inv\ a :\ inv(f\ a) \rangle$$<br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.11.24<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Preservação de um invariante por um par pré/pós-condição $Spec = (pre, post)$ em VDM-SL.<br>Noção de *precondição mais fraca* que garante uma propriedade. Noção de propriedade como *tipo*. Noção de invariante como *tipo*.<br>Polimorfismo orientado à propriedade. Algumas regras da combinação de especificações que satisfazem propriedades: *identidade*, *composição*, *inclusão*.<br>A *integridade-referencial* como uma classe de invariantes sobre relações simples e finitas em bases de dados.<br>Diagramas Entidades-Relações (ER) e sua semântica *pointfree* baseada na preordem de definição de relações.<br>Exemplos: relacionamentos M:M e M:1.<br><br>O DOCENTE _____ |

| AULA | SUMÁRIO |
|---|---|
| Teórica<br>05.12.15<br>5.ª-feira, 09h00–11h00<br>Sala DI-A2 | Diagramas ER e sua semântica relacional (conclusão): Relacionamentos 1:1. Preservação de integridade referencial.<br>Síntese final. Revisão dos sumários. Articulação da disciplina com outras que se lhe seguem no plano de estudos. Preenchimento do questionário de avaliação. Encerramento da disciplina.<br><br>O DOCENTE _____ |

# Adenda aos sumários de MFP-I/0506

## Conteúdo

# A Ainda sobre *An Introduction to Relational Formal Modelling*

## A.1 Quadro de Conecções de Galois

| **Relational Operators as Galois Connections** |
|---|
| $(f\ X) \subseteq Y \equiv X \subseteq (g\ Y)$ |

| **Description** | $f = g^\flat$ | $g = f^\sharp$ | **Obs.** |
|---|---|---|---|
| converse | $(\_)^\circ$ | $(\_)^\circ$ | |
| shunting rule | $(f \cdot)$ | $(f^\circ \cdot)$ | NB: $f$ is a function |
| "converse" shunting rule | $(\cdot f^\circ)$ | $(\cdot f)$ | NB: $f$ is a function |
| left-division | $(R \cdot)$ | $(R \backslash\ )$ | $R$ under ... |
| right-division | $(\cdot R)$ | $(\ /R)$ | ... over $R$ |
| range | rng | $(\cdot \top)$ | lower $\subseteq$ restricted to coreflexives |
| domain | dom | $(\top \cdot)$ | lower $\subseteq$ restricted to coreflexives |
| implication | $(R \cap\ )$ | $(R \Rightarrow\ )$ | Note that $(R \Rightarrow) = (\neg R \cup\ )$ |
| difference | $(\_ - R)$ | $(R \cup\ )$ | |

| PROPERTIES | | | |
|---|---|---|---|
| cancellation | $X \subseteq (g \cdot f)X$ | $(f \cdot g)Y \subseteq Y$ | |
| definition | $f\ X = \bigcap\{Y \mid X \subseteq gY\}$ | $g\ Y = \bigcup\{X \mid f\ X \subseteq Y\}$ | |
| distribution | $f(X \cup Y) = (f\ X) \cup (f\ Y)$ | $g(X \cap Y) = (g\ X) \cap (g\ Y)$ | $f(\bigcup_i X_i) = \bigcup_i (f\ X_i)$<br>$g(\bigcap_i X_i) = \bigcap_i (g\ X_i)$ |

## A.2 Alguns exercícios

**Exercício 1.** Provar a equivalência

$$f \text{ é inteira e simples } \equiv \quad (17)$$

□

---

**Exercício 2.** Provar (19).
□

---

**Exercício 3.** Mostrar que o núcleo de uma função constante é $\top$

$$\ker \underline{k} \quad = \quad \top \qquad (21)$$

a partir da propriedade natural

$$\underline{k} \cdot R \subseteq \underline{k} \qquad (22)$$

□

---

**Exercício 4.** Converter a CG associada a $\mathsf{dom}$ em

$$\mathsf{dom}\, R \subseteq Y \quad \equiv \quad ! \cdot R \subseteq ! \cdot Y \qquad (23)$$

a partir de

$$\top \quad = \quad \ker ! \qquad (24)$$

□

---

**Exercício 5.** Demonstrar

$$! \cdot \mathsf{dom}\, R \quad = \quad ! \cdot R \qquad (25)$$

por igualdade indirecta.
□

---

# B Tipos de dados restringidos por propriedades

## B.1 Preservação de invariantes

Seja $Spec = (pre, post)$ um par pré/pós-condição em VDM-SL

```
Spec(a: A) r: A
pre ... a ...
post ... r ... a ... ;
```

cujo significado relacional é, como se viu,

$$Spec \stackrel{\text{def}}{=} Post \cdot Pre \tag{26}$$

onde $Pre$ e $Post$ são as relações que representam $pre$ e $post$, respectivamente.

Seja $inv$ o invariante associado ao tipo $A$:

```
A = .....
inv a == ... ;
```

A preservação do invariante $inv$ por $Spec$ é a seguinte *obrigação de prova*, clássica desde sempre na metodologia VDM:

$$\langle \forall\ r, a\ ::\ post(r, a)\ \wedge\ pre\ a\ \wedge\ inv\ a \Rightarrow inv\ r \rangle \tag{27}$$

A correspondente transformada *pointfree* obtém-se a partir de

$$\mathsf{rng}\ R \subseteq \Phi \quad \equiv \quad \langle \forall\ b, a\ ::\ b\ R\ a \Rightarrow \phi\ b \rangle \tag{28}$$

a versão da CG de que $\mathsf{rng}$ é adjunto inferior

$$\mathsf{rng}\ R \subseteq \Phi \quad \equiv \quad R \subseteq \Phi \cdot \top \tag{29}$$

em cuja parte superior foram introduzidas variáveis. Ter-se-á então:

$$\begin{array}{ll} & \langle \forall\ r, a\ ::\ post(r, a)\ \wedge\ pre\ a\ \wedge\ inv\ a \Rightarrow inv\ r \rangle \\ \equiv & \quad \{\ \text{introdução de } Post = [\![post]\!],\ Pre = [\![pre]\!] \text{ e } Inv = [\![inv]\!]\ \} \\ & \langle \forall\ r, a\ ::\ r\ (Post \cdot Pre \cdot Inv)\ a \Rightarrow inv\ r \rangle \\ \equiv & \quad \{\ (28)\ \} \\ & \mathsf{rng}\ (Post \cdot Pre \cdot Inv) \subseteq Inv \\ \equiv & \quad \{\ (26)\ \} \\ & \mathsf{rng}\ (Spec \cdot Inv) \subseteq Inv \end{array}$$

Em suma,

$$\mathsf{rng}\ (Spec \cdot Inv) \subseteq Inv \tag{30}$$

é quivalente a (27), ou ainda a

$$\langle \forall\ b, a\ :\ b\ Spec\ a :\ inv\ a \Rightarrow inv\ b \rangle \tag{31}$$

## B.2 Generalização

Noção de *precondição mais fraca* que garante uma propriedade: dada $B \xleftarrow{R} A$ e a propriedade $2 \xleftarrow{\phi} B$ , $R$ garante $\phi$ sse

$$bRa \quad \Rightarrow \quad \phi\, b$$

Mesmo para um dado $R$ que não garanta $\phi$, é sempre possível encontrar-lhe uma pre-condição $\psi$ por forma a garantir $\phi$:

$$bRa \ \wedge \ \psi\, a \quad \Rightarrow \quad \phi\, b \tag{32}$$

isto é

$$\mathsf{rng}\,(R \cdot \Psi) \quad \subseteq \quad \Phi \tag{33}$$

Compondo as duas CG ($\mathsf{rng}$ ,$(R\cdot)$) obtém-se

$$\mathsf{rng}\,(R \cdot \Psi) \subseteq \Phi \quad \equiv \quad \Psi \subseteq R \backslash\!\!\blacktriangleright \Phi \tag{34}$$

onde $R \backslash\!\!\blacktriangleright \Phi$ é a *maior* dessas pré-condições — a pré-condição mais fraca que leva $R$ a garantir $\Phi$:

$$R \backslash\!\!\blacktriangleright \Phi \quad = \quad \bigcup \{\Psi \mid \mathsf{rng}\,(R \cdot \Psi) \subseteq \Phi\}$$

Da distributividade de qualquer adjunto superior decorre

$$R \backslash\!\!\blacktriangleright (\Phi \cap \Psi) \quad = \quad (R \backslash\!\!\blacktriangleright \Phi) \cap (R \backslash\!\!\blacktriangleright \Psi)$$

isto é

$$R \backslash\!\!\blacktriangleright (\Phi \cdot \Psi) \quad = \quad (R \backslash\!\!\blacktriangleright \Phi) \cdot (R \backslash\!\!\blacktriangleright \Psi) \tag{35}$$

pois *meet* de coreflexivas coincide com a composição:

$$R \cap S = R \cdot S \quad \Leftarrow \quad R \subseteq id \ \wedge \ S \subseteq id \tag{36}$$

## B.3 Propriedades vistas como tipos

Noção de propriedade como *tipo*: a declaração $R : \ \phi \longrightarrow \psi$ — ou $\Psi \xleftarrow{R} \Phi$ — deve ser entendida como sinónimo de $\Phi \subseteq R \backslash\!\!\blacktriangleright \Psi$, isto é

$$\Psi \xleftarrow{R} \Phi \quad \equiv \quad \Phi \subseteq R \backslash\!\!\blacktriangleright \Psi \tag{37}$$

Noção de invariante como *tipo*:

$$R \text{ preserva o invariante } \phi \quad \equiv \quad \Phi \xleftarrow{R} \Phi$$

De facto:

$$\begin{array}{ll} & (27) \qquad (38) \\ \equiv & \quad \{ \text{ secção anterior } \} \\ & \mathsf{rng}\,(Spec \cdot Inv) \subseteq Inv \qquad (39) \\ \equiv & \quad \{ \text{ GC } \} \\ & Inv \subseteq Spec \backslash\!\!\blacktriangleright Inv \qquad (40) \\ \equiv & \quad \{ \text{ definição acima } \} \\ & Inv \xleftarrow{Spec} Inv \qquad (41) \end{array}$$

# C Polimorfismo orientado à propriedade

Diz-se que a especificação $R$ *habita* o tipo $\Psi \xleftarrow{} \Phi$ sse (37) se verifica. Por exemplo, tem-se sempre

$$id \xleftarrow{R} \Phi$$

— pois $\Phi \subseteq R \backslash id$ é uma trivialidade — e daí o caso limite

$$id \xleftarrow{R} id$$

que é o tipo mais geral que $R$ habita. Daí as regras de *subtipagem*

$$\frac{\Psi \xleftarrow{R} \Phi \ , \Phi' \subseteq \Phi}{\Psi \xleftarrow{R} \Phi'} \tag{42}$$

(reforço à entrada) e

$$\frac{\Psi' \subseteq \Psi, \ \Psi' \xleftarrow{R} \Phi}{\Psi \xleftarrow{R} \Phi} \tag{43}$$

(relaxe à saída).

Algumas regras da combinação de especificações que satisfazem propriedades: *identidade*

$$\Phi \xleftarrow{id} \Psi \quad \equiv \quad \Psi \subseteq \Phi \tag{44}$$

*composição*

$$\frac{\begin{array}{c}\Gamma \xleftarrow{S} \Psi \\ \Psi \xleftarrow{R} \Phi\end{array}}{\Gamma \xleftarrow{S \cdot R} \Phi} \tag{45}$$

*inclusão*

$$\frac{\Psi \xleftarrow{R} \Phi \ , \ S \subseteq R}{\Psi \xleftarrow{S} \Phi} \tag{46}$$

*intersecção*

$$\frac{\begin{array}{c}\Phi' \xleftarrow{R} \Phi \\ \Psi' \xleftarrow{R} \Psi\end{array}}{(\Phi' \cdot \Psi') \xleftarrow{R} (\Phi \cdot \Psi)} \tag{47}$$

**Exercício 6.** Prove as leis (45) a (47) acima
□

**Exercício 7.** Será $\mathsf{dom}\,(\Psi \cdot R)$ garantia suficiente para uma especificação relacional $R$ stisfzer $\Psi$ à saída, isto é, será $R$ sempre um habitante do tipo

$$\Psi \xleftarrow{\quad} \mathsf{dom}\,(\Psi \cdot R) \quad ?$$

□

---

# D Abordagem relacional à integridade referencial

A *integridade-referencial* pode ser vista como uma classe de invariantes sobre relações simples e finitas em bases de dados.

Para a exprimir usam-se habitualmente diagramas *Entidades-Relações* (ER). De seguida iremos exprimir a semântica destes diagramas em versão *pointfree* baseada na preordem de definição de relações

$$R \preceq S \quad \equiv \quad \mathsf{dom}\,R \subseteq \mathsf{dom}\,S \tag{48}$$

isto é

$$R \preceq S \quad \equiv \quad ! \cdot R \subseteq ! \cdot S \tag{49}$$

**Exercício 8.** Deduzir as CGs

$$R \cdot f^\circ \preceq S \quad \equiv \quad R \preceq S \cdot f \tag{50}$$
$$R \cup S \preceq T \quad \equiv \quad R \preceq T \ \wedge \ S \preceq T \tag{51}$$
$$(R \dagger S) \preceq T \quad \equiv \quad R \preceq T \ \wedge \ S \preceq T \tag{52}$$

□

---

## D.1 Entidades e atributos

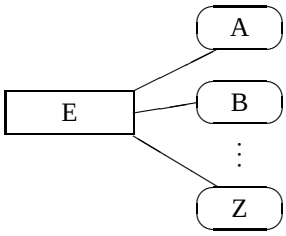
Nos diagramas ER que se seguem [1], $E$, $F$ são símbolos que designam entidades, $\#E$, $\#F$ designam os respectivos atributos chave (ie., atributos que participam na integridade referencial) e $A$, $B$, ... designam outros quaisquer atributos. Cada regra é da forma

$$d = e$$

onde $d$ é um diagrama ERA e $e$ é a correspondente "tradução semântica" relacional.

[1] Usam-se nestes diagramas as convenções gráficas propostas em [1].

### D.1.1 Entidades



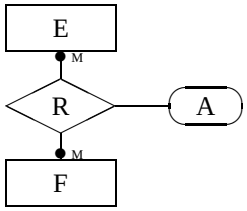

$$= \quad \#E \rightharpoonup A \times B \times \cdots \times Z \tag{53}$$

onde se usa a notação $A \rightharpoonup B$ para designar o espaço de relações simples finitas de $A$ para $B$.

### D.1.2 Relacionamentos

Genericamente, vamos supôr um atributo abstracto $A$ associado a cada relacionamento, desdobrável em tantos quantos necessários em cada caso.

## D.2 Relacionamentos M:M




$$\begin{array}{ll} = & ((\#E \times \#F \rightharpoonup A)\times \\ & (\#E \rightharpoonup \cdots)\times \\ & (\#F \rightharpoonup \cdots))_{\psi_{M:M}} \end{array} \tag{54}$$

A integridade referencial (pointwise) do diagrama é a que se segue:

$$\psi_{M:M}(R,S,T) \quad \equiv \quad \langle \forall\, x,y \,:\, \langle x,y\rangle \in \mathsf{dom}\, R :\; x \in \mathsf{dom}\, S \;\wedge\; y \in \mathsf{dom}\, T \rangle$$

Diagrama de tipos:

$$\begin{array}{ccccccccc} E & \xleftarrow{S} & \#E & \xleftarrow{\pi_1} & \#E \times \#F & \xrightarrow{\pi_2} & \#F & \xrightarrow{T} & F \\ & & & & \Big\downarrow{\scriptstyle R} & & & & \\ & & & & A & & & & \end{array}$$

Integridade referencial (pointfree):

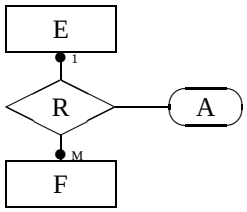
$$R \cdot \pi_1^\circ \preceq S \;\wedge\; R \cdot \pi_2^\circ \preceq T$$

isto é

$$R \preceq S \cdot \pi_1 \;\wedge\; R \preceq T \cdot \pi_2 \tag{55}$$

graças a (50).

## D.3 Relacionamentos M:1




$$= \quad ((\#F \rightharpoonup \#E \times A) \times \\ (\#E \rightharpoonup \cdots) \times \\ (\#F \rightharpoonup \cdots))_{\psi_{M:1}} \tag{56}$$

Integridade referencial (pointfree):

$$\psi_{M:1}(R,S,T) \quad \equiv \quad \mathsf{dom}\, R \subseteq \mathsf{dom}\, T \ \wedge \ \mathsf{rng}\, (\pi_1 \cdot R) \subseteq \mathsf{dom}\, S$$

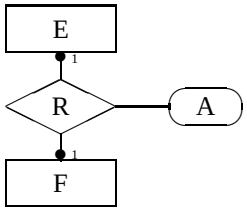
isto é

$$\begin{array}{rcl} \psi_{M:1}(R,S,T) & \equiv & R \preceq T \ \wedge \ R^\circ \cdot \pi_1^\circ \preceq S \\ & \equiv & R \preceq T \ \wedge \ R^\circ \preceq S \cdot \pi_1 \end{array}$$

Diagrama de tipos:

$$\begin{array}{ccccc} & & \#F & \xrightarrow[T]{} & F \\ & & {\scriptstyle R}\downarrow & & \\ E & \xleftarrow{S} \ \#E & \xleftarrow{\pi_1} & \#E \times A & \end{array}$$

## D.4 Relacionamentos 1:1




$$= \quad ((\#F \rightharpoonup \#E \times A) \times \\ (\#E \rightharpoonup \cdots) \times \\ (\#F \rightharpoonup \cdots))_{\psi_{1:1}} \tag{57}$$

Integridade referencial (pointfree):

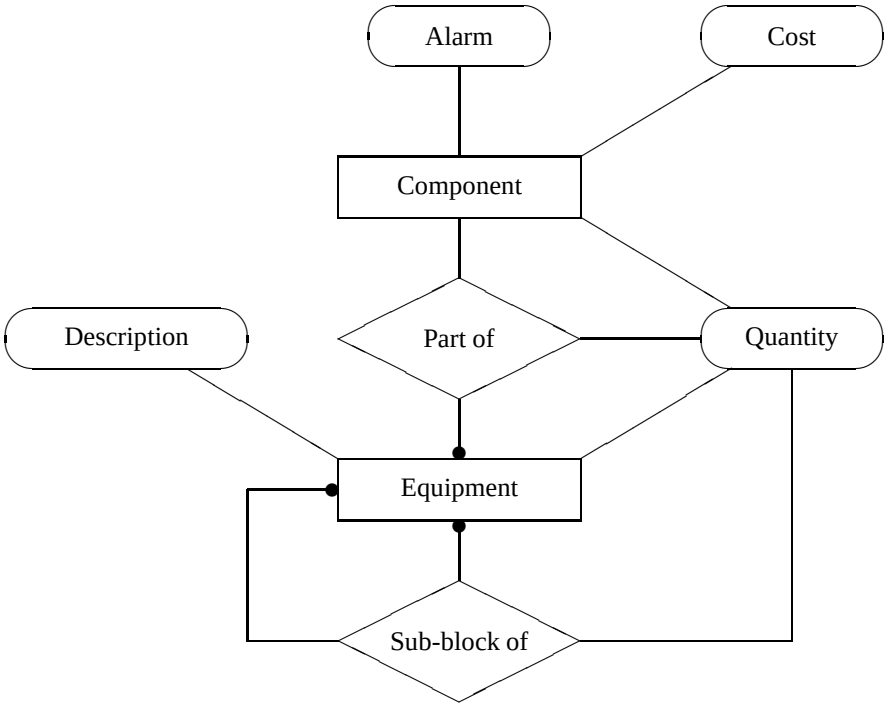
$$\psi_{1:1}(R,S,T) \quad \stackrel{\text{def}}{=} \quad \psi_{M:1}(R,S,T) \ \wedge \ id \sqsubseteq \pi_1 \cdot R \tag{58}$$

onde

$$R \sqsubseteq S \quad \equiv \quad \mathsf{ker}\, S \subseteq \mathsf{ker}\, R \tag{59}$$

é a preordem de injectividade ($R$ *menos* injectiva que $S$).

## D.5 Exemplo de Aplicação

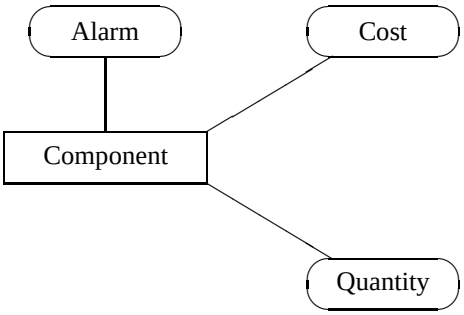



Na figura mostra-se um diagrama E-R que pretende registar a estrutura da base de dados de produção de uma fábrica de determinado tipo de equipamentos. Este diagrama pretende registar as seguintes intuições sobre o problema:

- a fábrica constrói um determinado tipo de *equipmento* cuja produção envolve *componentes* individuais obtidos externamente (*eg.* comprados a um fornecedor);
- cada componente individual tem um *custo* e está armazenado em determinada *quantidade*, verificada em relação a um dado valor mínimo de *alarme*;
- cada componente é, segundo uma quantidade determinada, *parte de* pelo menos um *equipmento* (*eg.* o circuito ref. X tem $n$ circuitos integrados de ref. Y);
- os equipmentos podem conter, segundo uma quantidade determinada, outros equipmentos como *sub-blocos* (*eg.* o computador pessoal ref. Z tem $m$ 'PC boards' de ref. T).

Em resumo, é possível reconstituir a árvore de produção de cada equipmento, árvore essa que pode envolver componentes individuais e/ou outras (sub-)árvores de produção.

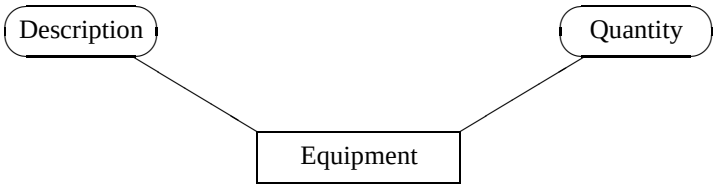
O significado relacional deste diagrama pode ser obtida de acordo com as regras acima descritas. O diagrama envolve apenas duas entidades, $Component$ e $Equipment$. A partir da regra (53) obtém-se:




— i.é,

$$\#Component \rightharpoonup Alarm \times Cost \times Quantity$$

— e




— i.é,

$$\#Equipment \rightharpoonup Description \times Quantity$$

O relacionamento *parte de* ('Part of') pode ser tido em conta adicionando, via regra (54), uma função parcial finita extra:

$$\begin{array}{l}(\#Component \times \#Equipment \rightharpoonup Quantity) \times \\ (\#Component \rightharpoonup Alarm \times Cost \times Quantity) \times \\ (\#Equipment \rightharpoonup Description \times Quantity)\end{array}$$

Finalmente, o relacionamento *sub-bloco-de* ('Sub-block-of') é incorporado segundo a regra (54):

$$\begin{array}{ll}( & (\#Equipment \times \#Equipment \rightharpoonup Quantity) \times \\ & (\#Component \times \#Equipment \rightharpoonup Quantity) \times \\ & (\#Component \rightharpoonup Alarm \times Cost \times Quantity) \times \\ & (\#Equipment \rightharpoonup Description \times Quantity) \\ )_{\phi} & \end{array} \quad (60)$$

**Exercício 9.** Deduza o invariante $\phi$ associado a (60) .
□

## D.6 Preservação da integridade referencial por cálculo

Queremos agora investigar a gama de operações que preserva os invariantes de integridade referencial, isto é, das transacções tais que, por exemplo

$$\Psi_{M:M} \xleftarrow{U} \Psi_{M:M}$$

se verifica. Por exemplo, seja $U$ a classe de transações que aumentam entidades e preservam o relacionamento, isto é

$$\text{post-}U((R',S',T'),(R,S,T)) \quad \equiv \quad R = R' \ \wedge \ S \subseteq S' \ \wedge \ R \subseteq R'$$

A obrigação de prova será, então

$$\langle \forall\ R,S,T,R',S',T' \ :\ R = R' \ \wedge \ S \subseteq S' \ \wedge \ R \subseteq R' :\ \psi_{M:M}(R,S,T) \quad \Rightarrow \quad \psi_{M:M}(R',S',T') \rangle$$

Cálculo:

$$\begin{array}{ll}
 & \psi_{M:M}(R',S',T') \\
\equiv & \qquad \{\ (55)\ \} \\
 & R' \preceq S' \cdot \pi_1 \ \wedge \ R' \preceq T' \cdot \pi_2 \\
\Leftarrow & \qquad \{\ \text{post-}U\text{; } \preceq\text{-monotonia do adjunto superior de (50)}\ \} \\
 & R \preceq S \cdot \pi_1 \ \wedge \ R \preceq T \cdot \pi_2 \\
\equiv & \qquad \{\ (55)\ \} \\
 & \psi_{M:M}(R,S,T)
\end{array}$$

Mais interessante é o mesmo exercício para transacções $U = (\ \dagger R') \times id \times id$ que preservam as entidades e aumentam o relacionamento:

$$\begin{array}{ll}
 & \psi_{M:M}(R \dagger R',S,T) \\
\equiv & \qquad \{\ (55)\ \} \\
 & R \dagger R' \preceq S \cdot \pi_1 \ \wedge \ R \dagger R' \preceq T \cdot \pi_2 \\
\equiv & \qquad \{\ (59) \text{ duas vezes}\ \} \\
 & R \preceq S \cdot \pi_1 \ \wedge \ R' \preceq S \cdot \pi_1 \ \wedge \ R \preceq T \cdot \pi_2 \ \wedge \ R' \preceq T \cdot \pi_2 \\
\equiv & \qquad \{\ (55)\ \} \\
 & \psi_{M:M}(R,S,T) \ \wedge \ \psi_{M:M}(R',S,T) \\
\equiv & \qquad \{\ \text{assumindo a pre-condição } \psi_{M:M}(R',S,T)\ \} \\
 & \psi_{M:M}(R,S,T)
\end{array}$$

**Exercício 10.** Considere o operador de "actualização selectiva" de uma função finita, em notação VDM-SL:

```
selUp[@A,@B]: set of @A * (@B -> @B) * map @A to @B -> map @A to @B
selUp(s,f,x) == x ++ ffmap[@A,@B](f)(s <: x);
```

que por sua vez se baseia no operador genérico

```
ffmap[@A,@B]: (@B -> @B) -> map @A to @B -> map @A to @B
ffmap(f)(x) == { k |-> f(x(k)) | k in set dom x };
```

Partindo a semântica relacional

$$selUp\ \phi\ f\ R \quad \stackrel{\text{def}}{=} \quad R \dagger (f \cdot R \cdot \Phi) \tag{61}$$

analise o impacto na integridade referencial de se fazerem actualizações selectivas de entidades e relacionamentos.
□

---

# E Soluções de alguns exercícios

**Resolução 1**: Por implicação mútua:

1. $f$ é inteira e simples $\Rightarrow$ (17)

$$\begin{array}{ll} & f \cdot R \subseteq S \\ \Rightarrow & \quad \{ \text{ monotonia da composição } \} \\ & f^\circ \cdot f \cdot R \subseteq f^\circ \cdot S \\ \Rightarrow & \quad \{ \ f \text{ é inteira } \} \\ & R \subseteq f^\circ \cdot S \\ \Rightarrow & \quad \{ \text{ monotonia da composição } \} \\ & f \cdot R \subseteq f \cdot f^\circ \cdot S \\ \Rightarrow & \quad \{ \ f \text{ é simples } \} \\ & f \cdot R \subseteq S \end{array}$$

2. (17) $\Rightarrow$ $f$ é inteira e simples

   Que (17) *implica* que $f$ é inteira e simples pode ser observado instanciando $R, S := id, f$ e $S, R := id, f^\circ$, respectivamente.

□

**Resolução 2**:

$$\begin{array}{ll} & f \subseteq g \\ \equiv & \quad \{ \text{ identity } \} \\ & f \cdot id \subseteq g \\ \equiv & \quad \{ \text{ shunting on } f \ \} \\ & id \subseteq f^\circ \cdot g \\ \equiv & \quad \{ \text{ shunting on } g \ \} \\ & id \cdot g^\circ \subseteq f^\circ \\ \equiv & \quad \{ \text{ converses } \} \\ & g \subseteq f \end{array}$$

□

**Resolução 3**:

$$
\begin{array}{ll}
 & \mathsf{ker}\,\underline{k} \;=\; \top \\
\equiv & \quad \{ \text{ indirect equality } \} \\
 & X \subseteq \mathsf{ker}\,\underline{k} \;\equiv\; X \subseteq \top \\
\equiv & \quad \{ \text{ kernel of a function ; every relation is at most } \top \} \\
 & X \subseteq \underline{k}^{\circ} \cdot \underline{k} \;\equiv\; \text{TRUE} \\
\equiv & \quad \{ \text{ GC } (f\cdot), (f^{\circ}\cdot) \} \\
 & \underline{k} \cdot X \subseteq \underline{k} \\
\equiv & \quad \{ \text{ (22) } \} \\
 & \text{TRUE}
\end{array}
$$

□

**Resolução 6**: Prova de (47):

$$
\begin{array}{ll}
 & \Phi \subseteq R \backslash\!\bullet\, \Phi \;\wedge\; \Psi \subseteq R \backslash\!\bullet\, \Psi \\
\Rightarrow & \quad \{ \text{ monotonicity } \} \\
 & (\Phi \cdot \Psi) \subseteq (R \backslash\!\bullet\, \Phi) \cdot (R \backslash\!\bullet\, \Psi) \\
\equiv & \quad \{ \text{ cf. (35) and (36) } \} \\
 & (\Phi \cap \Psi) \subseteq R \backslash\!\bullet\, (\Phi \cap \Psi)
\end{array}
$$

□

**Resolução 7**: Resolução por cálculo:

$$
\begin{array}{ll}
 & \Psi \xleftarrow{R} \mathsf{dom}\,(\Psi \cdot R) \\
\equiv & \quad \{ \text{ (37) } \} \\
 & \mathsf{dom}\,(\Psi \cdot R) \subseteq R \backslash\!\bullet\, \Psi \\
\equiv & \quad \{ \text{ (34) } \} \\
 & \mathsf{rng}\,(R \cdot (\mathsf{dom}\,(\Psi \cdot R))) \subseteq \Psi \\
\equiv & \quad \{ \text{ GCs: rng , conversos } \} \\
 & (\mathsf{dom}\,(\Psi \cdot R)) \cdot R^{\circ} \subseteq \top \cdot \Psi \\
\equiv & \quad \{ \text{ } \top = !^{\circ} \cdot ! \text{ (21) ; shunting (GC) } \} \\
 & ! \cdot (\mathsf{dom}\,(\Psi \cdot R)) \cdot R^{\circ} \subseteq ! \cdot \Psi \\
\equiv & \quad \{ \text{ (25) } \} \\
 & ! \cdot \Psi \cdot R \cdot R^{\circ} \subseteq ! \cdot \Psi \\
\Leftarrow & \quad \{ \text{ (25) } \} \\
 & R \text{ é simples}
\end{array}
$$

Em suma, o facto acima só é válido para especificações simples.
□

**Resolução 8**: Dedução de (50):

$$
\begin{array}{ll}
 & R \cdot f^\circ \preceq S \\
\equiv & \quad \{\ (48)\ \} \\
 & ! \cdot R \cdot f^\circ \subseteq ! \cdot S \\
\equiv & \quad \{\ \text{shunting}\ \} \\
 & ! \cdot R \subseteq ! \cdot S \cdot f \\
\equiv & \quad \{\ (48)\ \} \\
 & R \preceq S \cdot f
\end{array}
$$

□

# Referências


[1] R. Barker. *CASE*METHOD — Entity Relationship Modelling*. Addison-Wesley Publishing Company, Great Britain, 1992.