Universidade do Minho

2006/07	1.º Semestre ☒	2.º Semestre ☐	Anual ☐
DISCIPLINAS Métodos Formais de Programação I (7007N2) + Opção I — Métodos Formais de Programação I (5307P6) CURSOS LMCC + LESI	DOCENTES J.N. Oliveira - 406006 L.S. Barbosa - 406023		

AULA	SUMÁRIO
Teórica 06.09.14 5.ª-feira, 09h00–11h00 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. O DOCENTE _____

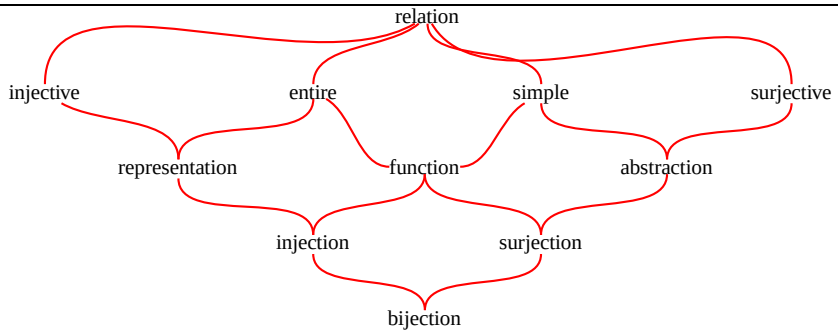
AULA	SUMÁRIO
Teórica 06.09.21 5.ª-feira, 09h00–11h00 Sala DI-A2	Introdução à especificação formal como método de *controlo de qualidade* em 'software'. Motivação: especificação formal — porquê e para quê? Introdução ao binómio *especificação /implementação*. Especificação formal construtiva. Modelação de requisitos e sua ambiguidade. Ambiguidades e certezas. Adopção do 'standard' ISO/IEC 13817-1 (VDM-SL). Apresentação da ferramenta VDMTools para desenvolvimento formal em VDM-SL. O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.09.28 5.ª-feira, 09h00–11h00 Sala DI-A2	Ciclo de vida de Balzer para desenvolvimento formal de 'software'. Prototipagem e animação. Validação por teste. Importância da verificação formal das propriedades de um modelo. Não-determinismo e parcialidade. Necessidade de especificar pré/pós-condições em VDM-SL. Exemplos: acesso a conjuntos finitos; especificação da operação de ordenação de sequências ($Sort$). Tolerância à especificação incompleta em VDM-SL. Sintaxe de operações via pré/pós-condições em VDM-SL e a a sua correspondência com relações binárias. Introdução ao cálculo de relações binárias. Tipo de uma relação. Diagramas envolvendo setas. *(v.s.f.f.)*

(cont.)	Composição de relações: $$b(R \cdot S)c \quad \equiv \quad \langle \exists\, a \;::\; bRa \;\wedge\; aSc \rangle \qquad (1)$$ Ordem de inclusão de relações: $$R \subseteq S \quad \equiv \quad \langle \forall\, b, a \;::\; bRa \Rightarrow bSa \rangle \qquad (2)$$ Conversa de uma relação $$a(R^\circ)b \equiv bRa \qquad (3)$$ As funções vistas como casos particulares de relações, $$b\ f\ a \quad \equiv \quad b = f\ a \qquad (4)$$ cf. a regra $$b(f^\circ \cdot R \cdot g)a \quad \equiv \quad (f\ b)R(g\ a) \qquad (5)$$ O DOCENTE _____

AULA	SUMÁRIO
Teórica 2006.09.28 5.ª feira, 14h00-16h00 (Aula suplementar)	Introdução à *transformada-PF* e formulação de propriedades em notação "point-free". Exemplo — monotonia de uma função f: $$\leq \quad \subseteq \quad f^\circ \cdot \leq \cdot f \qquad (6)$$ Os operadores *ker* e *img*: $$\mathsf{ker}\ R \stackrel{\text{def}}{=} R^\circ \cdot R \qquad (7)$$ $$\mathsf{img}\ R \stackrel{\text{def}}{=} R \cdot R^\circ \qquad (8)$$ Relações inteiras (totais), sobrejectivas e simples (funcionais). Taxonomia de relações binárias: *(v.s.f.f.)*

(cont.)



Funções como casos particulares de relações: estudo do quadro

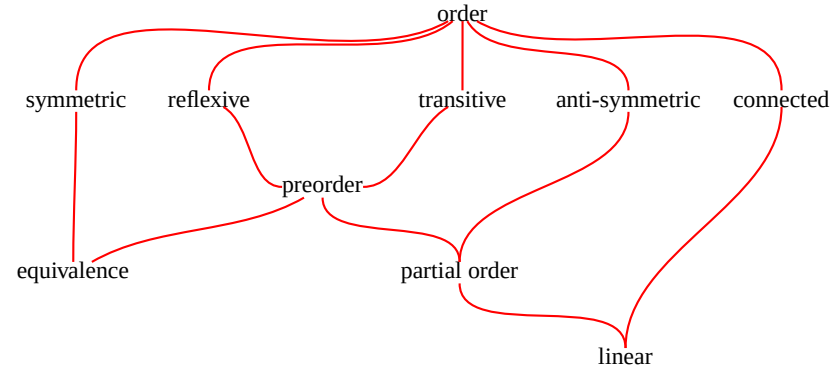
Pointwise	Pointfree	
"Left" Uniqueness		
$b\ f\ a\ \wedge\ b'\ f\ a \quad \Rightarrow \quad b = b'$	$\mathsf{img}\ f \quad \subseteq \quad id$	(f is simple) (9)
Leibniz principle		
$a = a' \quad \Rightarrow \quad f\ a = f\ a'$	$id \quad \subseteq \quad \mathsf{ker}\ f$	(f is entire)

e sua equivalência a qualquer uma das propriedades

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \tag{10}$$
$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{11}$$

O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.10.12 5.ª-feira, 09h00–11h00 Sala DI-A2	Representação de predicados unários (conjuntos) por relações coreflexivas. R é correflexiva $\quad \equiv \quad R \subseteq id$ Propriedades das relações coreflexivas: simetria e transitividade $R = R^\circ = R \cdot R = R \cap id$ (12) e intersecção via composição: $R \cap S = R \cdot S$ (13) Duas coreflexivas úteis: domínio $\delta\ R \quad = \quad \mathsf{ker}\ R \cap id$ e contradomínio: $\rho\ R \quad = \quad \mathsf{img}\ R \cap id$ *(v.s.f.f.)*

(cont.)	Ordens e sua taxonomia:  Exemplos. O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.10.19 5.ª-feira, 09h00–11h00 Sala DI-A2	Significado da especificação de uma operação via pré/pós-condições em VDM-SL. Semântica relacional de um par **pre-** / **post-**: $$Spec \stackrel{\text{def}}{=} Post \cdot Pre$$ Exemplo: $Sqrt = sq^{\circ}$. Papel da pre-condição. Breve introdução aos invariantes de tipos de dados. O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.10.26 5.ª-feira, 09h00–11h00 Sala DI-A2	Invariantes de tipos de dados. Sintaxe VDM-SL para invariantes. Exemplos de invariantes e sua relação com as *regras de negócio* dos sistemas de informação. Obrigações de prova associadas à formulação de invariantes. Caso de uma função $B \xleftarrow{f} A$ onde ϕ é o invariante associado à entrada (A) e ψ é o invariante da saída (B): $$\langle \forall\ a\ ::\ \phi\ a \Rightarrow \psi(f\ a) \rangle \quad (14)$$ Cálculo da transformada-PF de (14), onde $\Phi = \lceil \phi \rceil$ e $\Psi = \lceil \psi \rceil$, $$f \cdot \Phi\ \subseteq\ \Psi \cdot f \quad (15)$$ *(v.s.f.f.)*

(cont.)	equivalente a $$\rho\,(f \cdot \Phi) \;\subseteq\; \Psi \qquad (16)$$ As obrigações de prova da tmetodologia VDM standard: a *satisfabilidade* (101) e sua versão-PF (**??**); a preservação de invariantes (103) e sua transformada-PF (105). Necessidade de leis de cálculo-PF para realizar estas provas. O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.11.02 5.ª-feira, 09h00–11h00 Sala DI-A2	*Leis de cálculo relacional:* monotonia dos principais operadores, eg. $$\frac{\begin{array}{c} R \subseteq S \\ T \subseteq U \end{array}}{(R \cdot T) \subseteq (S \cdot U)} \qquad (17)$$ e $$R \subseteq S \equiv R^\circ \subseteq S^\circ \qquad (18)$$ Propriedades universais, eg. $^\circ$-universal: $$X^\circ \subseteq Y \quad \equiv \quad X \subseteq Y^\circ \qquad (19)$$ *Cálculo de igualdade* de relações — "pointwise" $$R = S \quad \equiv \quad \langle \forall\, a, b \;::\; bRa \equiv bSa \rangle \qquad (20)$$ e "pointfree": -inclusão cíclica (vulg "ping-pong"): $$R = S \quad \equiv \quad R \subseteq S \wedge S \subseteq R \qquad (21)$$ -igualdade indirecta: $$R = S \quad \equiv \quad \forall X.(X \subseteq R \equiv X \subseteq S) \qquad (22)$$ $$\equiv \quad \forall X.(R \subseteq X \equiv S \subseteq X) \qquad (23)$$ Exemplo: cálculo da propriedade de $^\circ$-involução $$(R^\circ)^\circ = R \qquad (24)$$ O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.11.09 5.ª-feira, 09h00–11h00 Sala DI-A2	Introdução à estruturação do cálculo relacional com base em conecções de Galois (CG): função adjunta superior $\underbrace{f}\ b \leq a \quad \equiv \quad b \sqsubseteq \overbrace{g}\ a$ função adjunta inferior onde $\leq, \sqsubseteq$ são preordens. As regras de "shunting" como exemplos de CGs. Cálculo da equivalência $$f \subseteq g \equiv f = g \equiv f \supseteq g \tag{25}$$ a partir dessas regras, como exemplo de cálculo de igualdade por inclusão cíclica (vulg "ping-pong"). Quadro das principais CG do cálculo relacional (ver pág. 113). As propriedades básicas de uma CG (25): *cancelamento* à esquerda, $$b \sqsubseteq g(f\ a) \tag{26}$$ *cancelamento* à direita, $$f(g\ a) \leq a \tag{27}$$ e monotonia de qualquer adjunto, por exemplo $$x \leq y \quad \Rightarrow \quad (g\ x) \sqsubseteq (g\ y) \tag{28}$$ Prova de (28) como exemplo de simplicidade de cálculo baseado em GCs: $(g\ x) \sqsubseteq (g\ y)$ $\equiv$ { "gs à direita passam a fs à esquerda" (25) } $f(g\ x) \leq y$ $\Leftarrow$ { *cancelamento* à direita (27) ; transitividade } $x \leq y$ Alternativamente: $x \leq y$ $\equiv$ { *cancelamento* à direita (27) } $f(g\ x) \leq x\ \wedge\ x \leq y$ $\Rightarrow$ { transitividade } $f(g\ x) \leq y$ $\equiv$ { "gs à direita passam a fs à esquerda" (25) } $(g\ x) \sqsubseteq (g\ y)$ *(v.s.f.f.)*

(cont.)

Quadro resumo dessas propriedades:

$(f\ b) \leq a \equiv b \sqsubseteq (g\ a)$		
Descrição	$f = g^\flat$	$g = f^\sharp$
Definição	$f\ b = \bigwedge\{a \mid b \sqsubseteq g\ a\}$	$g\ a = \bigsqcup\{b \mid f\ b \leq a\}$
Cancelamentos	$f(g\ a) \leq a$	$b \sqsubseteq g(f\ b)$
Distributividade	$f(b \sqcup b') = (f\ b) \vee (f\ b')$	$g(a' \sqcap a) = (g\ a') \sqcap (g\ a)$
Monotonia	$b \sqsubseteq b' \Rightarrow f\ b \leq f\ b'$	$a \leq a' \Rightarrow g\ a \sqsubseteq g\ a'$

Dedução *imediata* de propriedades como, por exemplo

$$(R \cup S)^\circ = R^\circ \cup S^\circ \tag{29}$$
$$(R \cap S)^\circ = R^\circ \cap S^\circ \tag{30}$$

(converso é adjunto superior e inferior, logo tem as duas distributividades).
Intuição da generalidade do conceito de CG e suas propriedades a partir da GC que define a divisão inteira de números naturais:

$$q \times d \leq n \equiv q \leq n/d \tag{31}$$

incluindo cálculo de propriedades mais elaboradas como por exemplo $(n/m)/d = n/(d \times m)$.

O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.11.16 5.ª-feira, 09h00–11h00 Sala DI-A2	Relação entre propriedades universais e CGs. Exemplos: a intersecção, $$X \subseteq (R \cap S) \quad \equiv \quad (X \subseteq R) \wedge (X \subseteq S) \tag{32}$$ a união $$R \cup S \subseteq X \quad \equiv \quad (R \subseteq X) \wedge (S \subseteq X) \tag{33}$$ e as versões relacionais de $\langle R, S\rangle$ e $[R\ , S]$: $$X \subseteq \langle R, S\rangle \quad \equiv \quad \pi_1 \cdot X \subseteq R \ \wedge \ \pi_2 \cdot X \subseteq S$$ $$X = [R\ , S] \quad \equiv \quad X \cdot i_1 = R \quad \wedge \quad X \cdot i_2 = S$$ *(v.s.f.f.)*

(cont.)	Semântica relacional dos operadores de VDM-SL. Comparação entre descrições semânticas informais como, por exemplo | Operator	Name	Semantics description
---	---	---
`m1 ++ m2`	Override	overrides and merges `m1` with `m2`, i.e. it is like a merge except that `m1` and `m2` need not be compatible; any common elements are as by `m2` (so `m2` overrides `m1`.)	 e definições semânticas formais, neste caso $$M \dagger N \quad \stackrel{\text{def}}{=} \quad N \rightarrow N \, , \, M \tag{34}$$ onde se recorre à versão relacional do condicional de McCarthy: $$R \rightarrow S \, , \, T \quad \stackrel{\text{def}}{=} \quad (S \cdot \delta \, R) \cup T \cdot (id - \delta \, R) \tag{35}$$ Equivalência entre (34) e $$M \dagger N \quad = \quad N \cup M \cdot (\neg \delta \, N) \tag{36}$$ O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.11.23 5.ª-feira, 09h00–11h00 Sala DI-A2	Apresentação dos principais padrões de desenho (recorrentes em modelos VDM) que se baseiam em funções parciais finitas e seus invariantes: *classificação, quantificação, identificação* e *"heaps"*. Uso do cálculo relacional para descarregar as obrigações de prova associadas à modelação de dados com funções parciais finitas. Referência às pré-ordens de *definição* (107) e de *injectividade* (119). O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.11.30 5.ª-feira, 09h00–11h00 Sala DI-A2	Cálculo de invariantes usando a transformada-PF. Exemplo: preservação do invariante $$\langle \forall \, a \in rng \, M \, :: \, \psi \, a \rangle \tag{37}$$ (*"todos os elementos do contradomínio satifiazem* ϕ*"*) no padrão de identificação. O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.12.07 5.ª-feira, 09h00–11h00 Sala DI-A2	A *integridade-referencial* como uma classe de invariantes sobre relações simples e finitas em bases de dados. Diagramas Entidades-Relações (ER) e sua semântica *pointfree* baseada na pre-ordem de definição de relações. Exemplos: relacionamentos M:M (114) e M:1 (116). Relacionamentos 1:1 (118). O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.12.14 5.ª-feira, 09h00–11h00 Sala DI-A2	*Não houve aula devido à participação do docente em reunião científica internacional* O DOCENTE _____

AULA	SUMÁRIO
Teórica 06.12.21 5.ª-feira, 09h00–11h00 Sala DI-A2	A preservação de integridade referencial como caso particular de preservação de invariantes. Exemplos: preservação de um relacionamento M:M por um operador que apenas acrescenta entidades; preservação do mesmo invariante por uma função que acrescenta (apenas) ao relacionamento. Necessidade de reforço de pré-condições. *Objectificação* de modelos. Modelos com estado interno. Invariante do estado. Sintaxe VDM para modelos com estado interno: cláusulas `ext rd` e `ext wr`. Síntese final. Revisão dos sumários. Articulação da disciplina com outras que se lhe seguem no plano de estudos. Questões em aberto: como calcular *propriedades* de especificações que são recursivas? E como derivar código imperativo executável a partir de modelos abstractos? Preenchimento do questionário de avaliação. Encerramento da disciplina. O DOCENTE _____

Adenda aos sumários de MFP-I/0607

A Obrigações de prova em VDM e sua realização por cálculo

A.1 Obrigações de prova em VDM ao nível da especificação de operações

A metodologia VDM establece duas obrigações de prova sobre um dado par *pre/post*:

- *Satisfabilidade* (*satisfiability*):

$$\langle \forall\ a\ ::\ pre(a) \Rightarrow \langle \exists\ b\ ::\ post(b,a) \rangle \rangle \tag{101}$$

  No caso de existir um invariante:

$$\langle \forall\ a\ ::\ pre(a) \Rightarrow \langle \exists\ b\ ::\ inv(b)\ \wedge\ post(b,a) \rangle \rangle \tag{102}$$

- *Preservação de invariantes*:

$$\langle \forall\ r, a\ ::\ post(r,a)\ \wedge\ pre\ a\ \wedge\ inv\ a \Rightarrow inv\ r \rangle \tag{103}$$

Na sua versão sem variáveis, (101) converte-se em

$$Pre \quad \subseteq \quad \delta\, Post \tag{104}$$

equivalente a

$$Pre \quad \subseteq \quad \top \cdot Post$$

e (103) em

$$\rho\,(Spec \cdot Inv) \subseteq Inv \tag{105}$$

equivalente a:

$$Spec \cdot Inv\ \subseteq\ Inv \cdot Spec \tag{106}$$

onde $Spec = \lceil post \rceil \cdot \lceil pre \rceil$ e $Inv = \lceil inv \rceil$.

A.2 Descarga de obrigações de prova por cálculo

B Abordagem relacional à integridade referencial

A *integridade-referencial* dos dados em bases de dados 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

$$R \preceq S \quad \equiv \quad \delta\, R \subseteq \delta\, S \tag{107}$$

isto é

$$R \preceq S \quad \equiv \quad ! \cdot R \subseteq ! \cdot S \tag{108}$$

Exercício 1. Deduzir as CGs

$$R \cdot f^{\circ} \preceq S \quad \equiv \quad R \preceq S \cdot f \tag{109}$$
$$R \cup S \preceq T \quad \equiv \quad R \preceq T \ \wedge \ S \preceq T \tag{110}$$
$$(R \dagger S) \preceq T \quad \equiv \quad R \preceq T \ \wedge \ S \preceq T \tag{111}$$

□

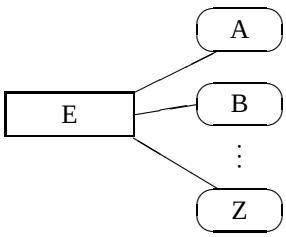
B.1 Entidades e atributos

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.

B.1.1 Entidades



$$= \quad \#E \rightharpoonup A \times B \times \cdots \times Z \tag{112}$$

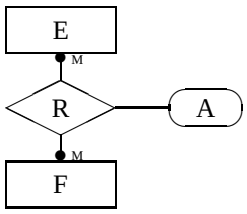
onde se usa a notação $A \rightharpoonup B$ para designar o espaço de relações simples finitas de A para B.

B.1.2 Relacionamentos

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

[1] Usam-se nestes diagramas as convenções gráficas propostas em [2].

B.2 Relacionamentos M:M



$$= \quad ((\#E \times \#F \rightharpoonup A)\times \\ (\#E \rightharpoonup \cdots)\times \\ (\#F \rightharpoonup \cdots))_{\psi_{M:M}} \tag{113}$$

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

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

Diagrama de tipos:

$$E \xleftarrow{S} \#E \xleftarrow{\pi_1} \#E \times \#F \xrightarrow{\pi_2} \#F \xrightarrow{T} F$$
$$\#E \times \#F \xrightarrow{R} A$$

Integridade referencial (pointfree):

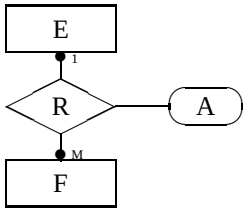
$$R \cdot \pi_1^\circ \preceq S \;\wedge\; R \cdot \pi_2^\circ \preceq T$$

isto é

$$R \preceq S \cdot \pi_1 \;\wedge\; R \preceq T \cdot \pi_2 \tag{114}$$

graças a (109).

B.3 Relacionamentos M:1



$$= \quad ((\#F \rightharpoonup \#E \times A)\times \\ (\#E \rightharpoonup \cdots)\times \\ (\#F \rightharpoonup \cdots))_{\psi_{M:1}} \tag{115}$$

Integridade referencial (pointfree):

$$\psi_{M:1}(R,S,T) \quad \equiv \quad \delta\, R \subseteq \delta\, T \;\wedge\; \rho\,(\pi_1 \cdot R) \subseteq \delta\, S$$

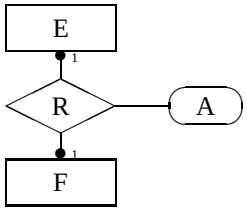
isto é

$$\begin{aligned} \psi_{M:1}(R,S,T) \quad &\equiv \quad R \preceq T \;\wedge\; R^\circ \cdot \pi_1^\circ \preceq S \\ &\equiv \quad R \preceq T \;\wedge\; R^\circ \preceq S \cdot \pi_1 \end{aligned} \tag{116}$$

Diagrama de tipos:

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

B.4 Relacionamentos 1:1



$$= \quad ((\#F \rightharpoonup \#E \times A)\times \\ (\#E \rightharpoonup \cdots)\times \\ (\#F \rightharpoonup \cdots))_{\psi_{1:1}} \tag{117}$$

Integridade referencial (pointfree):

$$\psi_{1:1}(R,S,T) \quad \stackrel{\text{def}}{=} \quad \psi_{M:1}(R,S,T) \ \wedge \ id \sqsubseteq \pi_1 \cdot R \tag{118}$$

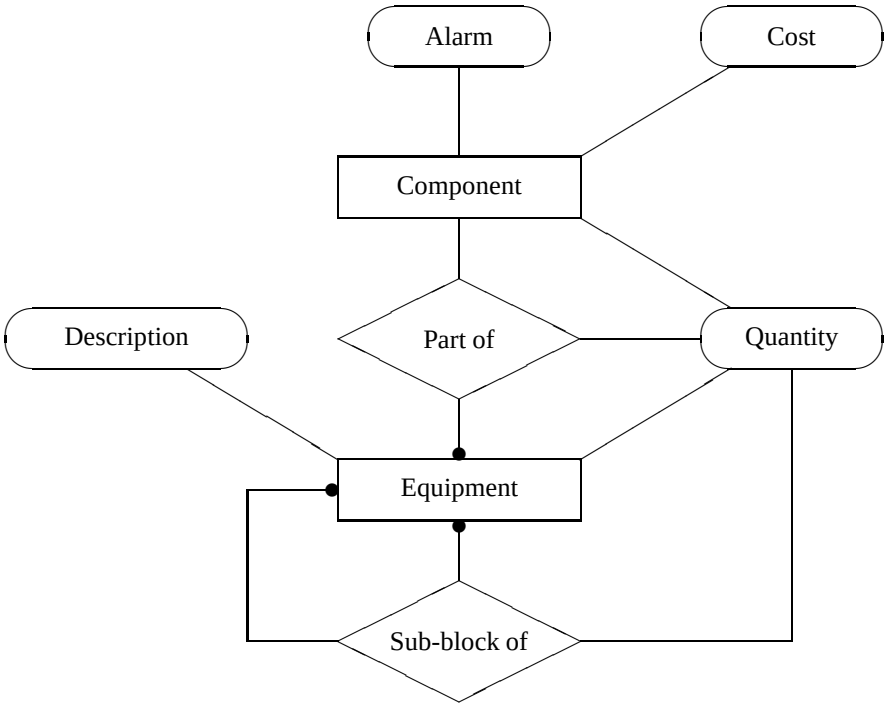
onde

$$R \sqsubseteq S \quad \equiv \quad \ker S \subseteq \ker R \tag{119}$$

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

B.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.



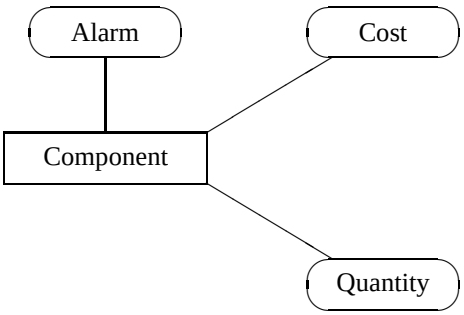
Este diagrama pretende registar as seguintes intuições sobre o problema:

- 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.

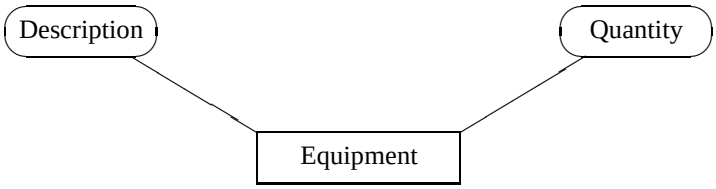
O significado relacional deste diagrama pode ser obtida de acordo com as regras acima descritas. O diagrama envolve apenas duas entidades, $Component$ e $Equipment$. A partir da regra (112) obtém-se:



— 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 (113), 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 (113):

$$\begin{array}{ll}(& (\#Equipment \times \#Equipment \rightharpoonup Quantity) \times \\ & (\#Component \times \#Equipment \rightharpoonup Quantity) \times \\ & (\#Component \rightharpoonup Alarm \times Cost \times Quantity) \times \\ & (\#Equipment \rightharpoonup Description \times Quantity) \\ )_\phi & \end{array} \tag{120}$$

Exercício 2. Deduza o invariante ϕ associado a (120) .
□

B.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 uma transação que aumenta entidades e preserva o relacionamento, isto é

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

Instanciando a obrigação de prova que teremos de efectuar (103), ter-se-á:

$$\langle \forall\, r, a \ :\ \text{post-}U(r,a) :\ \text{pre-}U\ a \ \wedge \ \psi_{M:M}\ a \Rightarrow \psi_{M:M}\ r \rangle$$

que se converte em

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

O raciocínio típico nestas provas é calcular o antecendente da implicação a partir do consequente, introduzindo uma pré-condição se necessário:

$$\begin{array}{ll} & \psi_{M:M}(R',S',T') \\ \equiv & \qquad \{\ (114)\ \} \\ & R' \preceq S' \cdot \pi_1 \ \wedge \ R' \preceq T' \cdot \pi_2 \\ \Leftarrow & \qquad \{\ \text{post-}U\text{; } \preceq\text{-monotonia do adjunto superior de (109)}\ \} \\ & R \preceq S \cdot \pi_1 \ \wedge \ R \preceq T \cdot \pi_2 \\ \equiv & \qquad \{\ (114)\ \} \\ & \psi_{M:M}(R,S,T) \end{array}$$

Mais interessante é o mesmo exercício para transacções funcionais $u = (\ \dagger\ R') \times id \times id$ que preservam as entidades e aumentam o relacionamento, sobrepondo-lhe R'. Como u é uma função, aplica-se-lhe

$$\langle \forall\, x \ ::\ \psi_{M:M}\ x \Rightarrow \psi_{M:M}(u\ x) \rangle \tag{121}$$

que é um caso particular de (14). De novo se parte do consequente para o antecedente da implicação (121):

$$\begin{array}{ll} & \psi_{M:M}(R \dagger R', S, T) \\ \equiv & \qquad \{\ (114)\ \} \\ & R \dagger R' \preceq S \cdot \pi_1 \ \wedge \ R \dagger R' \preceq T \cdot \pi_2 \\ \equiv & \qquad \{\ (111) \text{ duas vezes}\ \} \\ & R \preceq S \cdot \pi_1 \ \wedge \ R' \preceq S \cdot \pi_1 \ \wedge \ R \preceq T \cdot \pi_2 \ \wedge \ R' \preceq T \cdot \pi_2 \\ \equiv & \qquad \{\ (114)\ \} \\ & \psi_{M:M}(R,S,T) \ \wedge \ \psi_{M:M}(R',S,T) \end{array}$$

Verifica-se assim que o antecedente de (121) tem de ser reforçado com a pre-condição $\psi_{M:M}(R', S, T)$, sem a qual (notar a equivalência) não é possível garantir o invariante. Este caso ilustra, pois, a situação em que uma função (inteira) tem de ser transformada em função parcial (por introdução de uma pré-condição) em face da existência de invariantes.

Exercício 3. Escreva em sintaxe VDM-SL a operação que se acaba de estudar acima.
□

C Alguns exercícios

C.1 Relações binárias

Exercício 4. Provar a equivalência

$$f \text{ é inteira e simples } \equiv (10)$$

□

Exercício 5. Demonstrar a implicação

$$f \cdot r = id \quad \Rightarrow \quad f \text{ é sobrejectiva e } r \text{ é injectiva} \tag{122}$$

Sugestão: começar por $r \subseteq f^\circ$

□

Exercício 6. Provar (25).
□

Exercício 7. Mostrar que o núcleo de uma função constante é $\top$

$$\ker \underline{k} = \top \tag{123}$$

a partir da propriedade natural

$$\underline{k} \cdot R \subseteq \underline{k} \tag{124}$$

□

Exercício 8. Converter a CG associada a δ em

$$\delta\, R \subseteq Y \quad \equiv \quad !\cdot R \subseteq\, !\cdot Y \tag{125}$$

a partir de

$$\top \quad = \quad \mathsf{ker}\, ! \tag{126}$$

□

Exercício 9. Demonstrar

$$!\cdot \delta\, R \quad = \quad !\cdot R \tag{127}$$

por igualdade indirecta.
□

C.2 Mappings e relações simples

Exercício 10. Partindo de (212) e de (213), complete o cálculo seguinte da versão (mais simples) da regra de "ping-pong" (21) para relações simples M e N:

$$M = N \quad \equiv \quad M \subseteq N \ \wedge\ \delta\, N \subseteq \delta\, M \tag{128}$$

$$\begin{array}{cl}
 & M = N \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ N \subseteq M \ \wedge\ \delta\, N = \delta\, M \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ \delta\, N \subseteq N^\circ \cdot M \ \wedge\ \delta\, N = \delta\, M \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ \delta\, M \subseteq N^\circ \cdot M \ \wedge\ \delta\, N = \delta\, M \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ M^\circ \subseteq N^\circ \ \wedge\ \delta\, N = \delta\, M \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ M \subseteq N \ \wedge\ \delta\, N \subseteq \delta\, M \ \wedge\ \delta\, M \subseteq \delta\, N \\
\equiv & \qquad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
 & M \subseteq N \ \wedge\ \delta\, N \subseteq \delta\, M
\end{array}$$

□

Exercício 11. Mostrar que as equivalências

$$N \subseteq M \quad \equiv \quad M \dagger N = M \tag{129}$$
$$\delta\, M \subseteq \delta\, N \quad \equiv \quad M \dagger N = N \tag{130}$$

decorrem de (128).
□

Exercício 12. Demonstrar que, para quaisquer relações R e S, se tem

$$R \dagger S = R \cup S \quad \equiv \quad R \subseteq R \dagger S \tag{131}$$

Mostrar também que, no caso de R e S serem duas relações simples M e N, respectivamente, então (131) dá lugar a

$$M \dagger N = M \cup N \quad \equiv \quad M \cdot N^\circ \subseteq id \tag{132}$$

Mostrar ainda que $M \cdot N^\circ \subseteq id$ é quivalente à formulação da relação de compatibilidade entre duas relações simple:

$$M \simeq N \quad \stackrel{\text{def}}{=} \quad M \cdot \delta\, N = N \cdot \delta\, M \tag{133}$$

Com base em

$$M \simeq N \quad = \quad M \cdot N^\circ \subseteq id \tag{134}$$

mostar que $\simeq$ é uma relação simétrica e reflexiva.
□

Exercício 13. Apresente justificações para a prova que se segue de que a sobreposição de relações é associativa:

$$R \dagger (S \dagger P) \quad = \quad (R \dagger N) \dagger P \tag{135}$$

Cálculo a completar:

$$\begin{array}{ll} & (R \dagger S) \dagger P \\ = & \quad \{\ \text{(34) twice}\ \} \\ & P \rightarrow P\ ,\ (S \rightarrow N\ ,\ R) \\ = & \quad \{\ \ldots\ \} \\ & P \cup (S \cup R \cdot (\neg \delta\, N)) \cdot (\neg \delta\, P) \\ = & \quad \{\ \ldots\ \} \end{array}$$

$$\begin{array}{ll} & P \cup S \cdot (\neg\delta\, P) \cup R \cdot (\neg(\delta\, N \cup \delta\, P)) \\ = & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & (S \dagger P) \cup R \cdot (\neg\delta\,(N \dagger P)) \\ = & \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\ & R \dagger (S \dagger P) \end{array}$$

□

C.3 Diagramas E-R

Exercício 14. 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

$$selUp\ \phi\ f\ R \quad \stackrel{\mathrm{def}}{=} \quad R \dagger (f \cdot R \cdot \Phi) \tag{136}$$

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

Exercício 15. Perante o seguinte fragmento da formulação dos requisitos de uma aplicação de gestão pedagógica,

> *No sistema académico de uma dada universidade toda a disciplina é fornecida por um e um só departamento, que a entrega a um seu docente responsável (regente). Departamentos e disciplinas são entidades caracterizadas, entre outros atributos, pelo seu nome.*

dois programadores discutem sobre qual dos seguintes diagramas de Entidades-Relações (a) e (b), que se seguem, devem adoptar:

(a)

(b)

1. Dê-lhes a sua ajuda, comparando (a) e (b) com base na semântica-PF que estudou para diagramas deste tipo.
2. Escreva a função que, em notação SETS, converte a informação relacional de um dos formatos (a) ou (b) para o outro, se é que tal função pode ser definida.

□

D PF-transform Reference Manual

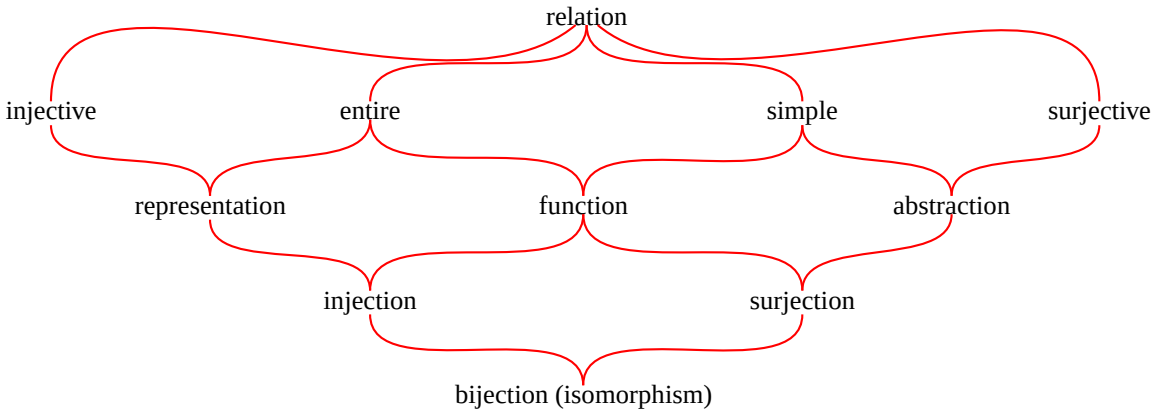
D.1 Relational taxonomy

Classification criteria:

	Reflexive	*Coreflexive*
ker R	entire R	injective R
img R	surjective R	simple R

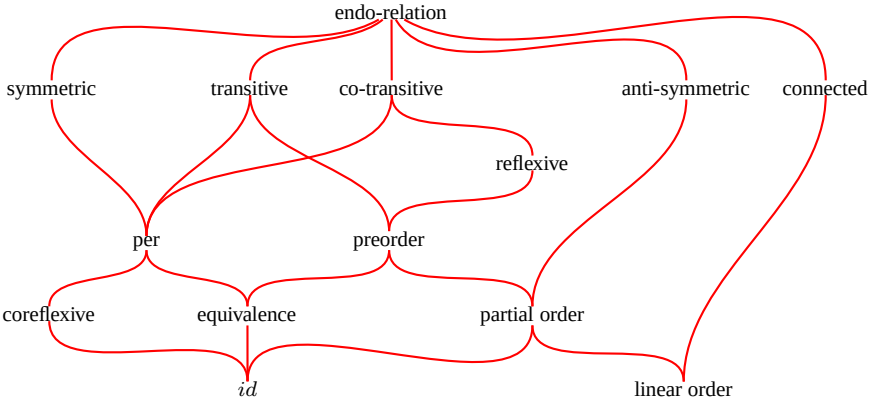
(201)

Binary relations:



(202)

Orders:



(203)

D.2 PF-transformation rules

"Guardanapo":

$$b(f^\circ \cdot R \cdot g)a \quad \equiv \quad (f\ b)R(g\ a) \tag{204}$$

Left-division:

$$b\ (R \setminus Y)\ a \quad \equiv \quad \langle \forall\ c\ :\ c\ R\ b :\ c\ Y\ a \rangle \tag{205}$$

Pointwise ordering on functions:

$$f\ \dot{\sqsubseteq}\ g \quad \equiv \quad f \subseteq \sqsubseteq \cdot g \quad \equiv \quad \langle \forall\ a\ ::\ (f\ a) \sqsubseteq (g\ a) \rangle \tag{206}$$

D.3 Table of useful Galois connections

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	$(h\cdot)$	$(h^\circ\cdot)$	NB: h is a function
"converse" shunting rule	$(\cdot h^\circ)$	$(\cdot h)$	NB: h is a function
left-division	$(R\cdot)$	$(R \setminus\ )$	R under ...
right-division	$(\cdot R)$	$(\ /R)$	... over R
range	ρ	$(\cdot \top)$	lower $\subseteq$ restricted to coreflexives
domain	δ	$(\top \cdot)$	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	$f(X \cup Y) = (f\ X) \cup (f\ Y)$	$g(X \cap Y) = (g\ X) \cap (g\ Y)$	$f(\bigcup_i X_i) = \bigcup_i (f\ X_i)$ $g(\bigcap_i X_i) = \bigcap_i (g\ X_i)$

(207)

D.4 Other Galois connections

Meet-universal

$$X \subseteq (R \cap S) \quad \equiv \quad (X \subseteq R) \wedge (X \subseteq S) \tag{208}$$

Join-universal

$$(R \cup S) \subseteq X \quad \equiv \quad (R \subseteq X) \wedge (S \subseteq X) \tag{209}$$

Split-universal

$$X \subseteq \langle R, S \rangle \quad \equiv \quad \pi_1 \cdot X \subseteq R \ \wedge \ \pi_2 \cdot X \subseteq S \tag{210}$$

Either-universal

$$X = [R\,,S] \quad \equiv \quad X \cdot i_1 = R \quad \wedge \quad X \cdot i_2 = S \tag{211}$$

D.5 "Almost" Galois connections

"Shunting" rules for S a simple relation:

$$S \cdot R \subseteq T \quad \equiv \quad (\delta\, S) \cdot R \quad \subseteq \quad S^\circ \cdot T \tag{212}$$
$$R \cdot S^\circ \subseteq T \quad \equiv \quad R \cdot \delta\, S \quad \subseteq \quad T \cdot S \tag{213}$$

Variants concerning domain and range:

$$\delta\, R \subseteq X \quad \equiv \quad R \subseteq R \cdot X \tag{214}$$
$$\rho\, R \subseteq X \quad \equiv \quad R \subseteq X \cdot R \tag{215}$$

D.6 Converses

$$(R \cdot S)^\circ = S^\circ \cdot R^\circ \tag{216}$$

D.7 Coreflexives

Since coreflexives are simple, the following follow from (212,213):

$$\Phi \cdot R \subseteq S \quad \equiv \quad \Phi \cdot R \subseteq \Phi \cdot S \tag{217}$$
$$R \cdot \Phi \subseteq S \quad \equiv \quad R \cdot \Phi \subseteq S \cdot \Phi \tag{218}$$

D.8 Relational divisions

$$(R \setminus S) \cdot f = R \setminus (S \cdot f) \tag{219}$$

D.9 Meets

$$(S \cap T) \cdot R = (S \cdot R) \cap (T \cdot R) \quad \Leftarrow \quad T \cdot \mathsf{img}\, R \subseteq T \vee S \cdot \mathsf{img}\, R \subseteq S \tag{220}$$

Therefore, for f a function,

$$(S \cap T) \cdot f = (S \cdot f) \cap (T \cdot f) \tag{221}$$

$$R \cdot (S \cap T) = (R \cdot S) \cap (R \cdot T) \quad \Leftarrow \quad (\mathsf{ker}\, R) \cdot T \subseteq T \vee (\mathsf{ker}\, R) \cdot S \subseteq S \tag{222}$$

D.10 Splits

Definition equivalent to (210)

$$\langle R, S\rangle \quad = \quad \pi_1^\circ \cdot R \cap \pi_2^\circ \cdot S \tag{223}$$

The same definition pointwise: for all a, b, c

$$(a, b)\langle R, S\rangle c \quad \equiv \quad a\ R\ c\ \wedge\ b\ S\ c \tag{224}$$

Split cancellation

$$\pi_1 \cdot \langle R, S\rangle = R \cdot \delta\, S \quad \wedge \quad \pi_2 \cdot \langle R, S\rangle = S \cdot \delta\, R \tag{225}$$

Split (conditional) fusion [2]:

$$\langle R, S\rangle \cdot T = \langle R \cdot T, S \cdot T\rangle \quad \Leftarrow \quad R \cdot (\mathsf{img}\, T) \subseteq R \vee S \cdot (\mathsf{img}\, T) \subseteq S \tag{226}$$

Split absorption

$$\langle R \cdot T, S \cdot U\rangle \quad = \quad (R \times S) \cdot \langle T, U\rangle \tag{227}$$

Splits and converses:

$$\langle R, S\rangle^\circ \cdot \langle X, Y\rangle \quad = \quad (R^\circ \cdot X) \cap (S^\circ \cdot Y) \tag{228}$$

Therefore:

$$\mathsf{ker}\, \langle R, S\rangle \quad = \quad \mathsf{ker}\, R \cap \mathsf{ker}\, S \tag{229}$$

D.11 Eithers

Definition:

$$[R\,, S] \quad = \quad (R \cdot i_1^\circ) \cup (S \cdot i_2^\circ) \tag{230}$$

From (211), all coproduct properties extend to relations, in particular: $+$-reflexion:

$$id = [i_1\,, i_2] \tag{231}$$

etc. Eithers and converses:

$$[R\,, S] \cdot [T\,, U]^\circ \quad = \quad (R \cdot T^\circ) \cup (S \cdot U^\circ) \tag{232}$$

D.12 Relational projection

Definition

$$\pi_{g,f} R \quad \stackrel{\text{def}}{=} \quad g \cdot R \cdot f^\circ \tag{233}$$

Property

$$\pi_{g,f} R \subseteq S \quad \equiv \quad g(S \leftarrow R)f \tag{234}$$

References

[1] Chritiene Aarts, Roland Backhouse, Paul Hoogendijk, Ed Voermans, and Jaap van der Woude. A relational theory of datatypes, December 1992. Available from `www.cs.nott.ac.uk/~rcb/papers`.

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

[2] Theorem 12.30 in [1].