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 ____________

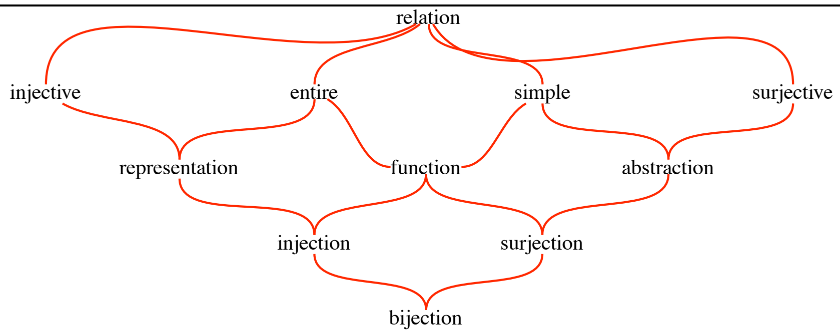
AULA	SUMÁRIO
Teórica 06.09.21 5.ª-feira, 09h00–11h00 Sala DI-A2	Introdução à especificação formal como método de *controlo de qualidade* em 'software'. Motivação: especificação formal — porquê e para quê? Introdução ao binómio *especificação /implementação*. Especificação formal construtiva. Modelação 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*: $$\mathsf{ker}\, R \stackrel{\mathrm{def}}{=} R^{\circ} \cdot R \qquad (7)$$ $$\mathsf{img}\, R \stackrel{\mathrm{def}}{=} R \cdot R^{\circ} \qquad (8)$$ 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

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \qquad (10)$$

$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \qquad (11)$$

O DOCENTE ______________________

AULA	SUMÁRIO
Teórica 06.10.12 5.ª-feira, 09h00–11h00 Sala DI-A2	Representação de predicados unários (conjuntos) por relações coreflexivas.

$$R \text{ é correflexiva} \quad \equiv \quad R \subseteq id$$

Propriedades das relações coreflexivas: simetria e transitividade

$$R = R^\circ = R \cdot R = R \cap id \qquad (12)$$

e intersecção via composição:

$$R \cap S = R \cdot S \qquad (13)$$

Duas coreflexivas úteis: domínio

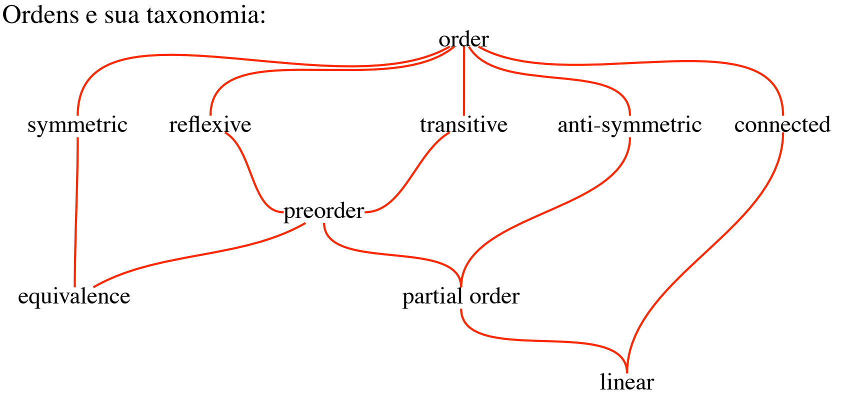
$$\delta\, R \quad = \quad \mathsf{ker}\, R \cap id$$

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-**:

$$Spec \stackrel{\mathrm{def}}{=} Post \cdot Pre$$

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):

$$\langle \forall\, a\ ::\ \phi\, a \Rightarrow \psi(f\ a) \rangle \tag{14}$$

Cálculo da transformada-PF de (14), onde $\Phi = \lceil \phi \rceil$ e $\Psi = \lceil \psi \rceil$,

$$f \cdot \Phi \subseteq \Psi \cdot f \tag{15}$$

(v.s.f.f.)

(cont.)	equivalente a $$\rho\,(f \cdot \Phi) \ \subseteq \ \Psi \tag{16}$$ 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. $$\frac{R \subseteq S \quad T \subseteq U}{(R \cdot T) \subseteq (S \cdot U)} \tag{17}$$ e $$R \subseteq S \equiv R^\circ \subseteq S^\circ \tag{18}$$ Propriedades universais, eg. $^\circ$-universal: $$X^\circ \subseteq Y \quad \equiv \quad X \subseteq Y^\circ \tag{19}$$ *Cálculo de igualdade* de relações — "pointwise" $$R = S \quad \equiv \quad \langle \forall\, a, b \ :: \ bRa \equiv bSa \rangle \tag{20}$$ e "pointfree": -inclusão cíclica (vulg "ping-pong"): $$R = S \quad \equiv \quad R \subseteq S \wedge S \subseteq R \tag{21}$$ -igualdade indirecta: $$R = S \quad \equiv \quad \forall X.(X \subseteq R \equiv X \subseteq S) \tag{22}$$ $$\equiv \quad \forall X.(R \subseteq X \equiv S \subseteq X) \tag{23}$$ Exemplo: cálculo da propriedade de $^\circ$-involução $$(R^\circ)^\circ = R \tag{24}$$ 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): $$\underbrace{f}_{\text{função adjunta inferior}}\ b \leq a \quad\equiv\quad b \sqsubseteq \overbrace{g}^{\text{função adjunta superior}}\ a$$ onde $\leq, \sqsubseteq$ são preordens. As regras de "shunting" como exemplos de CGs. Cálculo da equivalência $$f \subseteq g \equiv f = g \equiv f \supseteq g \qquad (25)$$ 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, $$b \sqsubseteq g(f\ a) \qquad (26)$$ *cancelamento* à direita, $$f(g\ a) \leq a \qquad (27)$$ e monotonia de qualquer adjunto, por exemplo $$x \leq y \quad\Rightarrow\quad (g\ x) \sqsubseteq (g\ y) \qquad (28)$$ Prova de (28) como exemplo de simplicidade de cálculo baseado em GCs: $$\begin{array}{ll} & (g\ x) \sqsubseteq (g\ y) \\ \equiv & \quad \{\ \text{"}gs\text{ à direita passam a }fs\text{ à esquerda" (25)}\ \} \\ & f(g\ x) \leq y \\ \Leftarrow & \quad \{\ \textit{cancelamento}\text{ à direita (27) ; transitividade}\ \} \\ & x \leq y \end{array}$$ Alternativamente: $$\begin{array}{ll} & x \leq y \\ \equiv & \quad \{\ \textit{cancelamento}\text{ à direita (27)}\ \} \\ & f(g\ x) \leq x\ \wedge\ x \leq y \\ \Rightarrow & \quad \{\ \text{transitividade}\ \} \\ & f(g\ x) \leq y \\ \equiv & \quad \{\ \text{"}gs\text{ à direita passam a }fs\text{ à esquerda" (25)}\ \} \\ & (g\ x) \sqsubseteq (g\ y) \end{array}$$ *(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

$$M \dagger N \quad \stackrel{\mathrm{def}}{=} \quad N \rightarrow N\ ,\ M \tag{34}$$

onde se recorre à versão relacional do condicional de McCarthy:

$$R \rightarrow S\ ,\ T \quad \stackrel{\mathrm{def}}{=} \quad (S \cdot \delta\, R) \cup T \cdot (id - \delta\, R) \tag{35}$$

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 pré-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 ____________