

An Introduction to Relational Formal Modelling

J.N. Oliveira

DI/UM, 2003-05

December 18, 2005

Functions are not enough

Partiality (in Haskell):

```
Mpi> (split head tail)(tail [1])
(
Program error: {head []}

Mpi> 2/0

Program error: {primDivDouble 2.0 0.0}
```

Functions such as `tail`, `/`, `head` (and many others!) are **partial**

Functions are not enough

VDM-SL notation:

```
vdm> p t1 [ ]
1. 1, c. 4:
    Run-Time Error 77: The sequence was empty
vdm> p 2/0
1. 1, c. 3:
    Run-Time Error 76: Division with zero
vdm>
```

Functions such as `t1`, `/`, `hd` (and many others!) are **partial**

Functions are not enough

```
gets : set of nat -> nat * set of nat
gets(s) == let a in set s
           in mk_(a,s \ {a}) ;
```

is not only partial

```
vdm> p gets({})
/home/jno/work/x.vdm, 1. 4, c. 25:
Run-Time Error 53: The binding environment was empty
vdm>
```

but also **non-deterministic**:

$$gets\{a, b\} = \langle a, \{b\} \rangle \vee gets\{a, b\} = \langle b, \{a\} \rangle$$

Specifications as “properties”

- Specification of **square root**:

$$(sqrt\ x)^2 = x$$

that is

$$sq \cdot sqrt = id$$

(= *sqrt* has left inverse *sq*)

- Specification of *sort*:

$$l' = sort\ l \Leftrightarrow (IsOrdered\ l') \wedge IsPermutation(l', l)$$

Relational approach

Need to model

- total/**partial** functions
- **non-determinism**
- **properties**, datatype **invariants** and loop-invariants
- orders and **inductive** structures
- vagueness or **under-specification**...

⇒ adoption of **binary relations**, which have a long tradition in the...

Pre/post specification style

```
Sort(l: seq of int) r: seq of int
post IsPermutation(r,l) and IsOrdered(r);

IsPermutation: seq of int * seq of int -> bool
IsPermutation(l1,l2) == .....

IsOrdered: seq of int -> bool
IsOrdered(l) == .....

gets(s: set of nat) r: nat * set of nat
pre  card s > 0
post r.#1 in set s and r.#2 = s \ {r.#1} ;
```

Pre/post specification layout

```
Spec(a: A) r: B
pre Precond(a)
post Postcond(r,a);
```

where

$$\begin{aligned} Precond &: A \longrightarrow 2 \\ Postcond &: B \times A \longrightarrow 2 \end{aligned}$$

leads to the **binary relation** approach:

$$Postcond \in 2^{B \times A} \quad \Leftrightarrow \quad Postcond \subseteq B \times A$$

From predicates to relations

- **Predicate logic** connectives such as eg. \wedge are “overloaded” operators
- They can be regarded as models of a more structured logic — that of **binary relations**
- **Functions** generalize to **binary relations** in a very natural way.
- Predicates, sets, functions and relations can **all** be combined in a **single relational calculus**
- Usual infix notation, e.g. $a < b$, can be generalized to any relation R , e.g. aRb

Sets / functions made relational

Strategy: identify every

- **function** $f : A \longrightarrow B$ with the binary relation relating a and b iff $b = f a$. So, bfa literally means $b = f a$.
- binary **predicate** $A \times B \xrightarrow{p} \text{bool}$ with binary relation $\llbracket p \rrbracket$ such that $a \llbracket p \rrbracket b \equiv p(a, b)$.
- unary **predicate** $A \xrightarrow{q} \text{bool}$ with binary relation $\llbracket q \rrbracket$ such that $a \llbracket q \rrbracket b \equiv a = b \wedge (q a)$.
- **set** $S \subseteq A$ with $\llbracket \lambda a. a \in S \rrbracket$. So,

$$a \llbracket S \rrbracket b \equiv a = b \wedge a \in S$$

Arrows “are” binary relations

- “**Type**” relations in a way consistent with functions: $B \xleftarrow{R} A$ wherever bRa involves $b \in B$ and $a \in A$.
- From now on, an arrow

$$B \xleftarrow{R} A$$

means a **binary relation** from A (source) to B (target) and write bRa to denote that pair $\langle b, a \rangle$ is in R .

Relations as Arrows

- **Ordering** on relations:

$$R \subseteq S \equiv bRa \Rightarrow bSa$$

$R \subseteq S$ means that R is either **less defined** or **more deterministic** than S .

- Extend **composition** $f \cdot g$ to $R \cdot S$ in the obvious way

$$b(R \cdot S)c \equiv \exists a \in A. bRa \wedge aSc$$

- Introduce **converse** R°

$$a(R^\circ)b \equiv bRa$$

Relational Equality

Pointwise equality:

$$R = S \equiv (bRa \equiv bSa)$$

Pointfree equality:

- **Cyclic implication** ("ping-pong") rule:

$$R = S \equiv R \subseteq S \wedge S \subseteq R$$

- **Indirect equality** rules:

$$\begin{aligned} R = S &\equiv \forall X. (X \subseteq R \equiv X \subseteq S) \\ &\equiv \forall X. (R \subseteq X \equiv S \subseteq X) \end{aligned}$$

Basic relational combinators

Given $C \xleftarrow{S} B$ and $B \xleftarrow{R} A$

- **Composition** $S \cdot R$ is s.t.

$$c(S \cdot R)a$$

holds wherever there exists some $b \in B$ such that $cSb \wedge bRa$.

- **Converse** $A \xleftarrow{R^\circ} B$ of $B \xleftarrow{R} A$

$$a(R^\circ)b \equiv bRa$$

- **Meet** $R \cap S$ — recall set-theoretical intersection

Basic Relation Calculus (I)

Composition is associative:

$$R \cdot (S \cdot T) = (R \cdot S) \cdot T$$

Identity

$$R \cdot id = id \cdot R = R$$

Empty relation

$$R \cdot \perp = \perp \cdot R = \perp$$

where $B \xleftarrow{\perp} A$ is the smallest relation of its type.

Basic Relation Calculus (II)

Composition is monotonic:

$$\frac{R \subseteq S \quad T \subseteq U}{(R \cdot T) \subseteq (S \cdot U)}$$

Bottom and top relations:

$$\perp \subseteq R \subseteq \top$$

where $B \overset{\top}{\leftarrow} A$ is the largest relation of its type.

Pointwise descriptions:

$$b \top a \equiv \text{true} \quad , \quad b \perp a \equiv \text{false}$$

Converse

$^\circ$ -universal

$$X^\circ \subseteq Y \quad \equiv \quad X \subseteq Y^\circ$$

$^\circ$ -monotonicity:

$$R \subseteq S \equiv R^\circ \subseteq S^\circ$$

Then:

$$\text{Involution :} \quad (R^\circ)^\circ = R$$

$$\text{Contravariance :} \quad (R \cdot S)^\circ = S^\circ \cdot R^\circ$$

These can be proved from $^\circ$ -**universal** by (elegant) indirect proofs (example in next slide):

Indirect proof of involution

$$\begin{aligned}
 & (R^\circ)^\circ \subseteq Y \\
 \equiv & \quad \{ \text{ }^\circ\text{-universal } X^\circ \subseteq Y \equiv X \subseteq Y^\circ \text{ for } X := R^\circ \} \\
 & R^\circ \subseteq Y^\circ \\
 \equiv & \quad \{ \text{ }^\circ\text{-monotonicity} \} \\
 & R \subseteq Y \\
 \therefore & \quad \{ \text{indirection} \} \\
 & (R^\circ)^\circ = R
 \end{aligned}$$

Meet and converse

\cap -universal

$$X \subseteq (R \cap S) \equiv (X \subseteq R) \wedge (X \subseteq S)$$

Converse distributes over \cap (proof in next slide):

$$(R \cap S)^\circ = R^\circ \cap S^\circ$$

Another indirect proof

$$\begin{aligned}
 & X \subseteq R^\circ \cap S^\circ \\
 \equiv & \quad \{ \cap\text{-universal} \} \\
 & (X \subseteq R^\circ) \wedge (X \subseteq S^\circ) \\
 \equiv & \quad \{ \text{monotonicity and involution} \} \\
 & (X^\circ \subseteq R) \wedge (X^\circ \subseteq S) \\
 \equiv & \quad \{ \cap\text{-universal} \} \\
 & X^\circ \subseteq (R \cap S) \\
 \equiv & \quad \{ \text{monotonicity and involution} \} \\
 & X \subseteq (R \cap S)^\circ \\
 \therefore & \quad \{ \text{indirection} \} \\
 & R^\circ \cap S^\circ = (R \cap S)^\circ
 \end{aligned}$$

Converses of functions

Function converses f°, g° etc. always exist (as **relations**) enjoying the following property:

$$(f \ b)R(g \ a) \equiv b(f^\circ \cdot R \cdot g)a$$

which unfolds to

$$\begin{aligned} bR(g \ a) &\equiv b(R \cdot g)a & (f := \text{id}) \\ (f \ b)Ra &\equiv b(f^\circ \cdot R)a & (g := \text{id}) \end{aligned}$$

Pointwise vs pointfree notation

Function

$$\begin{aligned} fac \ 0 &= 1 \\ fac(n+1) &= (n+1) * fac \ n \end{aligned}$$

in pointfree notation:

$$fac \cdot [\underline{0}, suc] = * \cdot [suc, fac]$$

Property

$$fac \ n = fac \ m \Rightarrow n = m$$

($\equiv fac$ is injective) in pointfree notation?

Properties in pointfree style (I)

fac is injective:

$$\begin{aligned} & fac \ n = fac \ m \Rightarrow n = m \\ \equiv & \quad \{ \text{identity function / relation} \} \\ & (fac \ n) \ id \ (fac \ m) \Rightarrow n \ id \ m \\ \equiv & \quad \{ \text{rule } (f \ b)R(g \ a) \equiv b(f^\circ \cdot R \cdot g)a \} \\ & n(fac^\circ \cdot id \cdot fac)m \Rightarrow n \ id \ m \\ \equiv & \quad \{ \text{dropping variables } n \text{ and } m ; \text{ natural-id} \} \\ & fac^\circ \cdot fac \subseteq id \end{aligned}$$

Properties in pointfree style (II)

Example property of integer arithmetics:

$$\begin{aligned}
 & \frac{n}{r} \mid \frac{d}{q} \quad d \times q \leq n \equiv q \leq n/d \\
 \equiv & \quad \{ \text{ using "Haskell section notation" } \} \\
 & (d \times) q \leq n \equiv q \leq n(/d) \\
 \equiv & \quad \{ \text{ rule } (f \ b)Ra \equiv b(f^\circ \cdot R)a \} \\
 & q((d \times)^\circ \cdot \leq) n \equiv q(\leq \cdot (/d)) n \\
 \equiv & \quad \{ \text{ pointwise equality } \} \\
 & (d \times)^\circ \cdot \leq = \leq \cdot (/d)
 \end{aligned}$$

Reasoning:

$$\begin{aligned}
 & q \leq (n/m)/d \\
 \equiv & \quad \{ \text{ "universal" property } \} \\
 & d \times q \leq n/m
 \end{aligned}$$

Orders and their taxonomy (A)

An order (or endo-relation) $A \xleftarrow{R} A$ is

reflexive:	iff $id_A \subseteq R$
coreflexive:	iff $R \subseteq id_A$
transitive:	iff $R \cdot R \subseteq R$
anti-symmetric:	iff $R \cap R^\circ \subseteq id_A$
symmetric:	iff $R \subseteq R^\circ (\equiv R = R^\circ)$
connected:	iff $R \cup R^\circ = \top$

where $A \xleftarrow{\top} A$ is the largest relation of its type.

Order taxonomy (B)

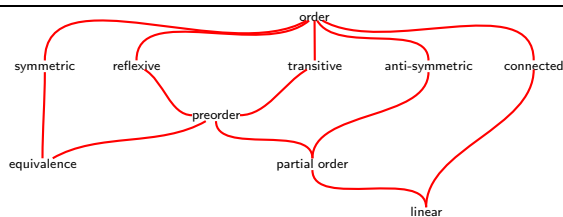
- **Preorders** are reflexive and transitive orders.
- **Partial** orders are anti-symmetric preorders
- **Linear** orders are connected partial orders
- **Equivalences** are symmetric preorders
- **Predicates** are coreflexive orders: the “meaning” of a predicate

$Bool \xleftarrow{\phi} A$ is a coreflexive relation $\llbracket \phi \rrbracket$ such that

$$\phi a \equiv a \llbracket \phi \rrbracket a$$

mapping every a which validates ϕ onto itself.

Order taxonomy (C)



Properties (A)

Dedekind's rule (also known as the **modular law**):

$$(R \cdot S) \cap T \subseteq R \cdot (S \cap (R^\circ \cdot T))$$

Dually (apply converses and rename):

$$(R \cdot S) \cap T \subseteq (R \cap (T \cdot S^\circ)) \cdot S$$

Symmetrical equivalent statement:

$$(R \cdot S) \cap T \subseteq (R \cap (T \cdot S^\circ)) \cdot (S \cap (R^\circ \cdot T))$$

= “weak right-distribution of meet over composition”.

Derived combinators

- **Kernel** of $B \xleftarrow{R} A$ is $A \xleftarrow{\ker R} A$ defined by

$$\ker R \stackrel{\text{def}}{=} R^\circ \cdot R$$

- **Image** of $B \xleftarrow{R} A$ is $B \xleftarrow{\text{img } R} B$ defined by

$$\text{img } R \stackrel{\text{def}}{=} R \cdot R^\circ$$

- Duality:

$$\ker(R^\circ) = \text{img } R$$

$$\text{img}(R^\circ) = \ker R$$

Properties of kernel and image

Order-preservation:

$$R \subseteq S \Rightarrow \ker R \subseteq \ker S$$

$$R \subseteq S \Rightarrow \text{img } R \subseteq \text{img } S$$

Symmetry:

$$(\ker R)^\circ = \ker R$$

$$(\text{img } R)^\circ = \text{img } R$$

Also:

$$R \subseteq R \cdot \ker R \quad (= \text{img } R \cdot R)$$

Entireness and simplicity

An **entire** (or total) relation is such that its kernel is reflexive:

$$R \text{ is entire} \equiv id \subseteq \ker R$$

A **simple** (or functional) relation is such that its image is coreflexive:

$$R \text{ is simple} \equiv \text{img } R \subseteq id$$

Simplicity is the dual of entireness. Simple relations are also called **partial functions**.

(Total) functions

Functions are both simple and entire relations, usually denoted by lowercase letters f :

$$\underbrace{id \subseteq f^\circ \cdot f}_{\text{entire}} \wedge \underbrace{f \cdot f^\circ \subseteq id}_{\text{simple}}$$

Thus:

$$f \subseteq R \Rightarrow R \text{ is entire}$$

$$R \subseteq f \Rightarrow R \text{ is simple}$$

In general, “larger than entire means entire” and “smaller than simple means simple”

Surjectiveness and injectiveness

More taxonomy:

- R is **surjective** iff R° is entire
- R is **injective** iff R° is simple

Facts:

$$\begin{aligned} R \text{ is entire and injective} &\equiv \ker R = id \\ R \text{ is simple and surjective} &\equiv \text{img } R = id \end{aligned}$$

Summary:

	Reflexive	Coreflexive
$\ker R$	entire R	injective R
$\text{img } R$	surjective R	simple R

Bijections

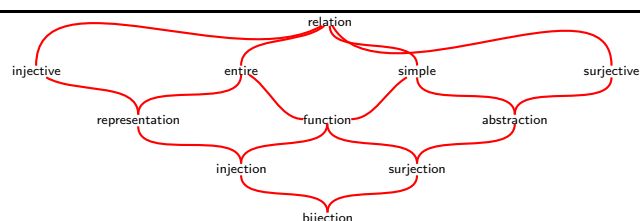
f is **bijjective** iff it is an injective and surjective function (thus simple and entire)

$$B \xleftarrow{f} A \text{ bijective} \equiv \ker f = id \wedge \text{img } f = id$$

In this case

$$id = f^\circ \cdot f \quad \wedge \quad f \cdot f^\circ = id$$

Binary relation taxonomy



Reasoning about functions

Shunting rules:

$$\begin{aligned} f \cdot R \subseteq S &\equiv R \subseteq f^\circ \cdot S \\ R \cdot f^\circ \subseteq S &\equiv R \subseteq S \cdot f \end{aligned}$$

Equality:

$$f \subseteq g \equiv f = g \equiv f \supseteq g$$

Ping-pong proof of the equality rule follows.

Proof of functional equality

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

Adding structure to the calculus

Note a recurrent **pattern** in several laws above:

$$\begin{array}{lcl} \underbrace{X^\circ}_{f \ X} \subseteq Y & \equiv & X \subseteq \underbrace{Y^\circ}_{g \ Y} \\ \underbrace{(h \cdot) X}_{f \ X} \subseteq Y & \equiv & X \subseteq \underbrace{(h^\circ \cdot) Y}_{g \ Y} \\ \underbrace{X(\cdot h^\circ)}_{f \ X} \subseteq Y & \equiv & X \subseteq \underbrace{Y(\cdot h)}_{g \ Y} \end{array}$$

as well as in

$$\underbrace{(d \times) q}_{f \ q} \leq n \quad \equiv \quad q \leq \underbrace{n(/d)}_{g \ n}$$

Back to the primary school desk

The **integral division** algorithm

$$\begin{array}{r|l} 7 & 2 \\ 1 & 3 \end{array} \quad 2 \times 3 + 1 = 7 \quad , \text{ "ie." } \quad 3 = 7/2$$

However

$$\begin{array}{r|l} 7 & 2 \\ 3 & 2 \end{array} \quad 2 \times 2 + 3 = 7 \quad \wedge \quad 2 \neq 7/2$$

$$\begin{array}{r|l} 7 & 2 \\ 5 & 1 \end{array} \quad 2 \times 1 + 5 = 7 \quad \wedge \quad 1 \neq 7/2$$

Quotient is a supremum

$$\begin{array}{r} n \\ r \end{array} \overline{) \begin{array}{l} d \\ q \end{array}}$$

$$d \times q + r = n \equiv q = n/d$$

provided q is the
largest such q (r is
smallest)

$$n/d = \bigvee \{q \mid \exists r . d \times q + r = n\}$$

$$= \bigvee \{q \mid d \times q \leq n\}$$

Maths teachers tell: it takes a while before children master the “ \bigvee semantics”!

What about you? Can you easily reason about n/d in this format?
Try and prove $(n/m)/d = n/(d \times m)$.

“Universal” property instead

Alternative:

$$\begin{array}{r} n \\ r \end{array} \overline{) \begin{array}{l} d \\ q \end{array}}$$

$$q \times d \leq n \equiv q \leq n/d$$

“universal” property of
integral division

Reasoning:

$$\begin{aligned} q &\leq (n/m)/d \\ &\equiv \{ \text{“universal” property} \} \\ q \times d &\leq n/m \end{aligned}$$

Reasoning continued

$$\begin{aligned} &\equiv \{ \text{“universal” property again} \} \\ (q \times d) \times m &\leq n \\ &\equiv \{ \times \text{ is associative} \} \\ q \times (d \times m) &\leq n \\ &\equiv \{ \text{“universal” property again} \} \\ q &\leq n/(d \times m) \end{aligned}$$

Indirect equality

So we have

$$q \leq (n/m)/d \equiv q \leq n/(d \times m)$$

that is,

$$(n/m)/d = n/(d \times m)$$

by the **indirect equality** rule:

$$(q \leq x \equiv q \leq y) \equiv (x = y)$$

Also easy to check

$$\begin{aligned} \text{Cancellation law: } & (n/d) \times d \leq n \\ & \equiv \{ \text{universal property } \} \\ & n/d \leq n/d \\ & \equiv \{ \text{reflexive } \leq \} \\ & \text{true} \\ \text{"Reflection": } & 1 \times d \leq n \equiv 1 \leq n/d \\ & \equiv \{ 1 \text{ is the unit of } \times \} \\ & d \leq n \equiv n/d \geq 1 \end{aligned}$$

Galois connections

n/d is a Galois connection:

$$\begin{array}{c} n \\ r \end{array} \Bigg| \begin{array}{c} d \\ q \end{array} \quad \underbrace{q \times d}_{f \ q} \leq n \equiv q \leq \underbrace{n/d}_{g \ n}$$

In general, for **preorders** (A, \leq) and (B, \sqsubseteq) and

$$(A, \leq) \begin{array}{c} \xrightarrow{g} \\ \xleftarrow{f} \end{array} (B, \sqsubseteq)$$

(f, g) are **Galois connected** iff...

Galois adjoints

$$\underbrace{f}_{\text{lower adjoint}} b \leq a \equiv b \sqsubseteq \underbrace{g}_{\text{upper adjoint}} a$$

that is

$$f^\circ \cdot \leq = \sqsubseteq \cdot g$$

Remarks:

- Galois (connected) adjoints enjoy a number of interesting **generic** properties
- **Very elegant** — **calculational** — way of performing **inequational** reasoning (including **logical** deduction)

Basic properties

Cancellation:

$$(f \cdot g)a \leq a \quad \text{and} \quad b \sqsubseteq (g \cdot f)b$$

Distribution (in case of lattice structures):

$$\begin{aligned} f(a \sqcup a') &= (f a) \vee (f a') \\ g(b \wedge b') &= (g b) \sqcap (g b') \end{aligned}$$

Conversely,

- If f distributes over \sqcup then it has an upper adjoint g ($f^\#$)
- If g distributes over \wedge then it has a lower adjoint f (g^\flat)

Other properties

If (f, g) are Galois connected,

- $f(g)$ **uniquely** determines $g(f)$ — thus the $_^\flat, _^\#$ notations
- f and g are **monotonic**
- (g, f) are also Galois connected — **reverse** the orderings
- $f = f \cdot g \cdot f$ and $g = g \cdot f \cdot g$

etc

Summary

$(f b) \leq a \equiv b \sqsubseteq (g a)$		
Description	$f = g^\flat$	$g = f^\#$
Definition	$f b = \bigwedge \{a \mid b \sqsubseteq g a\}$	$g a = \bigsqcup \{b \mid f b \leq a\}$
Cancellation	$f(g a) \leq a$	$b \sqsubseteq g(f b)$
Distribution	$f(b \sqcup b') = (f b) \vee (f b')$	$g(a' \sqcap a) = (g a') \sqcap (g a)$
Monotonicity	$b \sqsubseteq b' \Rightarrow f b \leq f b'$	$a \leq a' \Rightarrow g a \sqsubseteq g a'$

Converse

$(f X) \subseteq Y \equiv X \subseteq (g Y)$			
Description	$f = g^\flat$	$g = f^\sharp$	Obs.
converse	$(_)^\circ$	$(_)^\circ$	$bR^\circ a \equiv aRb$

Thus:

Cancellation	$(R^\circ)^\circ = R$
Monotonicity	$R \subseteq S \equiv R^\circ \subseteq S^\circ$
Distributions	$(R \cap S)^\circ = R^\circ \cap S^\circ, (R \cup S)^\circ = R^\circ \cup S^\circ$

Functions

$(f X) \subseteq Y \equiv X \subseteq (g Y)$			
Description	$f = g^\flat$	$g = f^\sharp$	Obs.
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

Consequences:

Functional equality:	$h \subseteq g \equiv h = k \equiv h \supseteq k$
Functional division:	$h^\circ \cdot R = h \setminus R$

Question: what does $h \setminus R$ mean?

Relational division

$(f X) \subseteq Y \equiv X \subseteq (g Y)$			
Description	$f = g^\flat$	$g = f^\sharp$	Obs.
left-division	$(R \cdot)$	$(R \setminus _)$	left-factor
right-division	$(\cdot R)$	$(_ / R)$	right-factor

Immediate: $(R \cdot)$ and $(\cdot R)$ distribute over union:

$$\begin{aligned} R \cdot (S \cup T) &= (R \cdot S) \cup (R \cdot T) \\ (S \cup T) \cdot R &= (S \cdot R) \cup (T \cdot R) \end{aligned}$$

Some intuition about relational division operators follows.

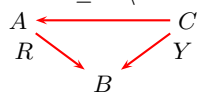
Relational division

The **relational division** operators are upper-adjoints:

$$R \cdot X \subseteq Y \equiv X \subseteq R \setminus Y$$

$$X \cdot R \subseteq Y \equiv X \subseteq Y / R$$

Left division abstracts a (pointwise) universal quantification

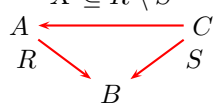
$$X \subseteq R \setminus Y$$


$$a(R \setminus Y)c \equiv (\forall b. bRa \Rightarrow bYc)$$

An example follows.

Example

Recall data division in the **relational model**:

$$X \subseteq R \setminus S$$


$$a(R \setminus S)c \equiv (\forall b. bRa \Rightarrow bSc)$$

$b R a$ = flight b carries passenger a

$b S c$ = flight b belongs to air-company c

$a (R \setminus S) c$ = passenger a is faithful to company c , that is, (s)he only flies company c .

Right division

By taking converses we arrive at $S / R = (R^\circ \setminus S^\circ)^\circ$:

$$\begin{aligned}
 & X \subseteq S / R \\
 \equiv & \quad \{ \text{Galois connection } ((\cdot R), (/R)) \} \\
 & X \cdot R \subseteq S \\
 \equiv & \quad \{ \text{converses} \} \\
 & R^\circ \cdot X^\circ \subseteq S^\circ \\
 \equiv & \quad \{ \text{Galois connection } ((R\cdot), (R\backslash)) \} \\
 & X^\circ \subseteq R^\circ \setminus S^\circ \\
 \equiv & \quad \{ \text{converses} \} \\
 & X \subseteq (R^\circ \setminus S^\circ)^\circ
 \end{aligned}$$

ie. Galois connection

$$X \cdot R \subseteq S \quad \equiv \quad X \subseteq S / R$$

Meet

\cap -universal

$$X \subseteq (R \cap S) \quad \equiv \quad (X \subseteq R) \wedge (X \subseteq S)$$

is a Galois connection

$$(\Delta, \cap)$$

where $\Delta X = (X, X)$, cf.

$$(X, X)(\subseteq \times \subseteq)(R, S) \quad \equiv \quad X \subseteq \cap(R, S)$$

So $\cap = \Delta^\#$ distributes over itself, etc

Properties of \cap

From \cap -universal infer:

- **\cap -cancellation** ($X := R \cap S$)

$$R \cap S \subseteq R \quad \wedge \quad R \cap S \subseteq S$$

- **\cap -abbreviation** ($X := R$)

$$R \subseteq S \quad \equiv \quad R = R \cap S$$

- **\cap -idempotency** ($S := R$)

$$R \cap R = R$$

More properties of \cap

\cap is **commutative**:

$$R \cap S = S \cap R$$

\cap is **associative**:

$$R \cap (S \cap T) = (R \cap S) \cap T$$

\cap -fusion:

$$\begin{aligned} T \cdot (R \cap S) &\subseteq (T \cdot R) \cap (T \cdot S) \\ (R \cap S) \cdot T &\subseteq (R \cdot T) \cap (S \cdot T) \end{aligned}$$

Meet and join

$(f \ X) \leq Y \equiv X \sqsubseteq (g \ Y)$			
Description	$f = g^\flat$	$g = f^\sharp$	Obs.
meet	Δ	\cap	\leq is $(\subseteq \times \subseteq)$
join	\cup	Δ	\sqsubseteq is $(\subseteq \times \subseteq)$

Join:

$$\cup(R, S) \subseteq Y \equiv (R, S)(\subseteq \times \subseteq)(Y, Y)$$

that is,

$$R \cup S \subseteq Y \equiv R \subseteq Y \wedge S \subseteq Y$$

Relational split

Functions:

$$x = \langle f, g \rangle \equiv \pi_1 \cdot x = f \wedge \pi_2 \cdot x = g$$

Relations:

$$X \subseteq \langle R, S \rangle \equiv \pi_1 \cdot X \subseteq R \wedge \pi_2 \cdot X \subseteq S$$

$\langle \rightarrow, \rightarrow \rangle$

$((\pi_1 \cdot) \times (\pi_2 \cdot)) \cdot \Delta$

Properties

$\langle \rightarrow, \rightarrow \rangle$ is an **upper-adjoint**, so it distributes over meet

$$\langle R, S \cap T \rangle = \langle R, S \rangle \cap \langle R, T \rangle$$

$$\langle S \cap T, R \rangle = \langle S, R \rangle \cap \langle T, R \rangle$$

etc. Moreover:

$$\langle R, S \rangle = (\pi_1^\circ \cdot R) \cap (\pi_2^\circ \cdot S) \quad (1)$$

Why? Again Galois at work:

Calculation

$$\begin{aligned}
X \subseteq \langle R, S \rangle &\equiv \pi_1 \cdot X \subseteq R \wedge \pi_2 \cdot X \subseteq S \\
&\equiv \{ \text{Galois connected } ((f \cdot), (f^\circ \cdot)) \} \\
&\quad X \subseteq \pi_1^\circ \cdot R \wedge X \subseteq \pi_2^\circ \cdot S \\
&\equiv \{ \text{Galois connected } (\cap^b, \cap) \} \\
&\quad X \subseteq (\pi_1^\circ \cdot R \cap \pi_2^\circ \cdot S) \\
&\because \{ \text{indirect equality} \} \\
&\quad \langle R, S \rangle = \pi_1^\circ \cdot R \cap \pi_2^\circ \cdot S
\end{aligned}$$

Pointwise $\langle R, S \rangle$

$$\begin{aligned}
(a, b) \langle R, S \rangle c &\equiv (a, b) (\pi_1^\circ \cdot R \cap \pi_2^\circ \cdot S) c \\
&\equiv \{ \text{pointwise } \cap \} \\
&\quad (a, b) (\pi_1^\circ \cdot R) c \wedge (a, b) (\pi_2^\circ \cdot S) c \\
&= \{ \text{rule } (f \cdot b) R a \equiv b (f^\circ \cdot R) a \} \\
&\quad \pi_1(a, b) R c \wedge \pi_2(a, b) S c \\
&= \{ \text{projections} \} \\
&\quad a R c \wedge b S c
\end{aligned}$$

Relational either

Functions:

$$[f, g] = x \equiv f = x \cdot i_1 \wedge g = x \cdot i_2$$

Relations:

$$[R, S] \subseteq X \equiv R \subseteq X \cdot i_1 \wedge S \subseteq X \cdot i_2 \quad (2)$$

Thus $[-, -]$ is a **lower-adjoint**, it distributes over \cup , etc. Moreover,

$$[R, S] = (R \cdot i_1^\circ) \cup (S \cdot i_2^\circ) \quad (3)$$

Domain and range

$(f \ X) \subseteq Y \equiv X \subseteq (g \ Y)$			
Description	$f = g^\flat$	$g = f^\sharp$	Obs.
domain	dom	$(\top \cdot)$	lower \subseteq restricted to coreflexives
range	rng	$(\cdot \top)$	lower \subseteq restricted to coreflexives

cf.



Domain and range

Dualization:

$$\text{dom } R = \text{rng } R^\circ$$

Explicit definitions:

$$\begin{aligned} \text{rng } R &= \text{img } R \cap id \\ \text{dom } R &= \text{img } R^\circ \cap id = \text{ker } R \cap id \end{aligned}$$

Facts:

$$\begin{aligned} R &= R \cdot (\text{dom } R) \\ R &= (\text{rng } R) \cdot R \end{aligned}$$

Domain and split

The following fact holds:

$$\langle R, S \rangle^\circ \cdot \langle X, Y \rangle = (R^\circ \cdot X) \cap (S^\circ \cdot Y)$$

Corollary:

$$\text{dom } R = \ker \langle \text{id}, R \rangle$$

Another consequence of the fact above:

$$\ker R \subseteq \ker (S \cdot R) \iff S \text{ entire}$$

Corollary:

$$\ker R \subseteq \ker (f \cdot R)$$

Comprehending relations

For each $B \xleftarrow{R} A$ define its **graph** or **comprehension** by

$$\mathcal{G} R = \{(b, a) \mid bRa\}$$

Clearly, $R = \llbracket \mathcal{G} R \rrbracket$ and so we often abbreviate $\mathcal{G} R$ to R .

The graph of every **coreflexive** S is made simpler for obvious reasons:

$$\mathcal{G} S = \{a \mid aSa\}$$

Finite relations

R is said to be **finite** wherever $\mathcal{G} R$ is a finite set.

- Finite relations, which can be enumerated, browsed and stored in a computer, are the subject of **relational database** design.
- Every finite, **simple** relation expresses a **functional dependency**.
- The graphs of finite and simple relations are called **mappings** in VDM-SL terminology.
- We will use Greek literals (σ, τ etc) to denote (finite) mappings

VDM-SL mapping notation

- Datatype: $\text{map } A \text{ to } B$
- Pointwise VDM-SL concrete syntax

$$\{a \mapsto b \mid b \sigma a\}$$

replaces $\{(b, a) \mid b \sigma a\}$.

- In VDM-SL notation, $b \sigma a$ is furthermore rephrased as $a \in \text{dom } \sigma \wedge b = \sigma(a)$ — cf. $\sigma = \sigma \cdot \text{dom } \sigma$ — that is, we have

$$\sigma = \{a \mapsto \sigma(a) \mid a \in \text{dom } \sigma\}$$

Meaning of VDM-SL specs

```
Spec(a: A) r: B
pre precondition(a)
post postcond(r, a);
```

where $\text{precond} : \text{bool} \leftarrow A$ and $\text{postcond} : \text{bool} \leftarrow B \times A$ are predicates means $\text{Spec} : B \leftarrow A$ defined by

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

$$\text{Pre} = \llbracket \text{precond} \rrbracket$$

$$\text{Post} = \llbracket \text{postcond} \rrbracket$$

where $A \leftarrow A$ is coreflexive and $B \leftarrow A$ is such that $b \text{ Post } a \equiv \text{postcond}(b, a)$.

VDM-SL *Sqrt* spec

```
Sqrt(x: real) r: real
pre true
post sq(r) = x ;
```

means

$$\begin{aligned} Sqrt &= \llbracket \lambda(r, x).sq\ r = x \rrbracket \cdot id \\ \equiv &\quad \{ \text{meaning of a binary predicate} \} \\ r\ Sqrt\ x &\equiv (sq\ r)\ id\ x \\ \equiv &\quad \{ (f\ b)R(g\ a) \equiv b(f^\circ \cdot R \cdot g)a ; \text{natural-id} \} \\ Sqrt &= sq^\circ \end{aligned}$$

Turning implicit specifications...

Sorting in VDM-SL notation:

```
Sort(l: seq of int) r: seq of int
post IsOrdered(r) and IsPermutation(r,l);
```

where

```
IsPermutation: seq of int * seq of int -> bool
IsPermutation(l1,l2) ==
  forall e in set (elems l1 union elems l2) &
    card {i | i in set inds l1 & l1(i) = e} =
    card {i | i in set inds l2 & l2(i) = e};
```


...into relational models

... abbreviates to

$$Sort \stackrel{\text{def}}{=} \llbracket IsOrdered \rrbracket \cdot IsPermutation(\text{ker } seq2bag)$$

assuming

```
seq2bag: seq of int -> map int to nat1
seq2bag(l) ==
  { e |-> card { i | i in set inds l & l(i) = e } |
    e in set elems l };
```



IsPermutation is an **equivalence** because $\text{ker } f$ always is reflexive, symmetric and transitive.

Relational semantics of VDM-SL

From the VDM-SL on-line manual:

Operator	Name	Semantics description
$s <: m$	Domain restrict to	Creates the map consisting of the elements in m whose key is in s . s need not be a subset of $\text{dom } m$.

Formal **semantics**:

$$\llbracket s <: m \rrbracket = \llbracket m \rrbracket \cdot \llbracket s \rrbracket$$

where $\llbracket s \rrbracket$ is correflexive and $\llbracket m \rrbracket$ is simple.

Relational semantics of VDM-SL

From the VDM-SL on-line manual:

Operator	Name	Semantics description
$m1 \mathrel{++} m2$	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 $m1$.)

Formal **semantics**:

$$\llbracket m1 \mathrel{++} m2 \rrbracket = \llbracket m2 \rrbracket \rightarrow \llbracket m2 \rrbracket, \llbracket m1 \rrbracket$$

cf. relational **McCarthy** conditional:

Relational McCarthy conditional

It is defined by

$$R \rightarrow S, T \stackrel{\text{def}}{=} (S \cdot \text{dom } R) \cup T \cdot (id - \text{dom } R)$$

where

$(f \ X) \subseteq Y \equiv X \subseteq (g \ Y)$			
Description	$f = g^b$	$g = f^\sharp$	Obs.
difference	$(_ - R)$	$(R \cup _)$	

that is,

$$\begin{aligned} X - R \subseteq Y &\equiv X \subseteq R \cup Y \\ X - R &= \bigcap \{Y \mid X \subseteq R \cup Y\} \end{aligned}$$

Reasoning about VDM-SL

We want to prove VDM-SL properties such as

$$\begin{aligned}X <: (Y <: \sigma) &= (X \cap Y) <: \sigma \\ \{\} <: \sigma &= \{\mapsto\} \\ X <: (\sigma_1 ++ \sigma_2) &= (X <: \sigma_1) ++ (X <: \sigma_2)\end{aligned}$$

First, some properties of coreflexives:

- Coreflexives are **symmetric** and **transitive**:

$$R = R^\circ = R \cdot R = R \cap id$$

- **Meet** of two coreflexives is composition:

$$R \cap S = R \cdot S$$

Example of proof

$$\begin{aligned}& \llbracket X <: (Y <: \sigma) \rrbracket \\= & \{ \text{relational meaning of } <: \} \\& \llbracket Y <: \sigma \rrbracket \cdot \llbracket X \rrbracket \\= & \{ \text{relational meaning of } <: \} \\& (\llbracket \sigma \rrbracket \cdot \llbracket Y \rrbracket) \cdot \llbracket X \rrbracket \\= & \{ \text{associativity of } \cdot \text{ and coreflexives } \} \\& \llbracket \sigma \rrbracket \cdot (\llbracket X \rrbracket \cdot \llbracket Y \rrbracket) \\= & \{ \text{meet of two coreflexives is composition } \} \\& \llbracket \sigma \rrbracket \cdot (\llbracket X \rrbracket \cap \llbracket Y \rrbracket)\end{aligned}$$

Proof continued

$$\begin{aligned}
 & \llbracket \sigma \rrbracket \cdot (\llbracket X \rrbracket \cap \llbracket Y \rrbracket) \\
 = & \quad \{ \text{meaning of set intersection} \} \\
 & \llbracket \sigma \rrbracket \cdot \llbracket X \cap Y \rrbracket \\
 = & \quad \{ \text{relational meaning of } <: \} \\
 & \llbracket (X \cap Y) <: \sigma \rrbracket
 \end{aligned}$$

Another proof

$$\begin{aligned}
 & \llbracket X <: (\sigma_1 ++ \sigma_2) \rrbracket \\
 = & \quad \{ \text{relational meaning of } <: \text{ and } ++ \} \\
 & (\llbracket \sigma_2 \rrbracket \rightarrow \llbracket \sigma_2 \rrbracket, \llbracket \sigma_1 \rrbracket) \cdot \llbracket X \rrbracket \\
 = & \quad \{ \text{McCarthy fusion law} \} \\
 & \llbracket \sigma_2 \rrbracket \cdot \llbracket X \rrbracket \rightarrow \llbracket \sigma_2 \rrbracket \cdot \llbracket X \rrbracket, \llbracket \sigma_1 \rrbracket \cdot \llbracket X \rrbracket \\
 = & \quad \{ \text{relational meaning of } <: \} \\
 & \llbracket X <: \sigma_2 \rrbracket \rightarrow \llbracket X <: \sigma_2 \rrbracket, \llbracket X <: \sigma_1 \rrbracket \\
 = & \quad \{ \text{relational meaning of } ++ \} \\
 & \llbracket (X <: \sigma_1) ++ (X <: \sigma_2) \rrbracket
 \end{aligned}$$

Etc.

Home work: define the relational semantics of *e.g.*.

Operator	Name	Semantics description
$m <-: s$	Domain restricted by	Creates the map consisting of the elements in m whose key is not in s . s need not be a subset of $\text{dom } m$.

and prove similar properties.

Override pointwise

Since

$$\text{dom}(\sigma_1 ++ \sigma_2) = \text{dom} \sigma_1 \cup \text{dom} \sigma_2$$

we have, after expansion of the relational definition:

```
s1 ++ s2 ==  
  { k |-> if k in set dom s2  
         then s2(k)  
         else s1(k)  
    | k in set dom s1 union dom s2 }
```

Performing the above proof over this definition would have been far less compact.

Inductive override

Another version of map override:

```
s1 ++ s2 ==  
  if s1 = { |-> }  
  then s2  
  else let k in set dom s1  
       in { k |-> if k in set dom s2  
                 then s2(k)  
                 else s1(k) } munion { k } <-: s1 ++ s2
```

How do we arrive at this recursive scheme?

See next set of slides.

Bibliografia

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