An Introduction to the Relational Hylomorphism Calculus

José N. Oliveira
Dept. Informatica
Universidade do Minho, 4700 Braga, Portugal
jno@di.uminho.pt

January 6, 2003

Part I
Rudiments of the Relation Calculus

Inclusion and composition

Composition is associative:

$$R \cdot (S \cdot T) = (R \cdot S) \cdot T \tag{1}$$

Composition is monotonic:

$$\frac{\begin{array}{c} R \subseteq S \\ T \subseteq U \end{array}}{(R \cdot T) \subseteq (S \cdot U)} \tag{2}$$

Identity

$$R \cdot id = id \cdot R = R \tag{3}$$

Equality

"Ping-pong" rule:

$$R = S \quad \equiv \quad R \subseteq S \wedge S \subseteq R \tag{4}$$

Indirect proof:

$$R = S \quad \equiv \quad \forall X.(X \subseteq R \equiv X \subseteq S) \tag{5}$$

Meet and converse

Meet-universal

$$X \subseteq (R \cap S) \quad \equiv \quad (X \subseteq R) \wedge (X \subseteq S) \tag{6}$$

Converse

$$\begin{array}{lll} \textit{Involution :} & (R^\circ)^\circ = R & (7) \\ \textit{Order-preserving :} & R \subseteq S \equiv R^\circ \subseteq S^\circ & (8) \\ \textit{Contravariance :} & (R \cdot S)^\circ = S^\circ \cdot R^\circ & (9) \end{array}$$

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

$$(R \cap S)^\circ = R^\circ \cap S^\circ \tag{10}$$

Elegant (indirect) proofs

$$\begin{array}{ll} & X \subseteq R^\circ \cap S^\circ \\ \equiv & \quad \{ \cap\text{-universal} \} \\ & (X \subseteq R^\circ) \wedge (X \subseteq S^\circ) \\ \equiv & \quad \{ \text{involution} \} \\ & (X^\circ \subseteq R) \wedge (X^\circ \subseteq S) \\ \equiv & \quad \{ \cap\text{-universal} \} \\ & X^\circ \subseteq (R \cap S) \\ \equiv & \quad \{ \text{involution} \} \\ & X \subseteq (R \cap S)^\circ \\ thus & \quad \{ \text{indirection} \} \\ & R^\circ \cap S^\circ = (R \cap S)^\circ \end{array}$$

Dedekind's rule

also known as the **modular law**:

$$(R \cdot S) \cap T \quad \subseteq \quad R \cdot (S \cap (R^\circ \cdot T)) \tag{11}$$

Dually (apply converses and rename):

$$(R \cdot S) \cap T \quad \subseteq \quad (R \cap (T \cdot S^\circ)) \cdot S \tag{12}$$

Symmetrical equivalent statement:

$$(R \cdot S) \cap T \quad \subseteq \quad (R \cap (T \cdot S^\circ)) \cdot (S \cap (R^\circ \cdot T)) \tag{13}$$

= "weak right-distribution of meet over composition".

Properties (A)

- $\cap$-cancellation — from $X = R \cap S$ in (6) infer:

$$R \cap S \subseteq R \quad \wedge \quad R \cap S \subseteq S \tag{14}$$

- $\cap$-abbreviation:

$$R \subseteq S \quad \equiv \quad R = R \cap S \tag{15}$$

- $\cap$-idempotency:

$$R \cap R \quad = \quad R \tag{16}$$

Proof of (15):

$$\begin{array}{ll}
 & R \subseteq S \\
\equiv & \qquad \{ \text{ inclusion is reflexive} \} \\
 & R \subseteq R \wedge R \subseteq S \\
\equiv & \qquad \{ \text{ meet-universal (6) } \} \\
 & R \subseteq (R \cap S) \\
\equiv & \qquad \{ \text{ cancellation (14) } \} \\
 & R \subseteq (R \cap S) \wedge (R \cap S) \subseteq R \\
\equiv & \qquad \{ \text{ ping-pong} \} \\
 & R = (R \cap S)
\end{array}$$

Proof of (11):

$$\begin{tikzcd}
C & B \arrow[l, "R"'] & A \arrow[l, "S"'] \arrow[ll, bend left, "T"]
\end{tikzcd}$$

$$\begin{array}{ll}
 & (\exists b . c R b \wedge b S a) \wedge c T a \\
\equiv & \qquad \{ \text{ predicate calculus } \} \\
 & (\exists b . c R b \wedge b S a \wedge c T a) \\
\equiv & \qquad \{ \text{ converse and trivia } \} \\
 & (\exists b . c R b \wedge b S a \wedge b R^\circ c \wedge c T a) \\
\Rightarrow & \qquad \{ \text{ relational composition } \} \\
 & (\exists b . c R b \wedge b S a \wedge b (R^\circ \cdot T) a) \\
\equiv & \qquad \{ \text{ meet in predicate calculus } \} \\
 & (\exists b . c R b \wedge b (S \cap (R^\circ \cdot T) a))
\end{array}$$

Properties (B)

$\cap$ is commutative:

$$R \cap S \quad = \quad S \cap R \tag{17}$$

$\cap$ is associative:

$$R \cap (S \cap T) \quad = \quad (R \cap S) \cap T \tag{18}$$

$\cap$-fusion:

$$T \cdot (R \cap S) \quad \subseteq \quad (T \cdot R) \cap (T \cdot S) \tag{19}$$

$$(R \cap S) \cdot T \quad \subseteq \quad (R \cdot T) \cap (S \cdot T) \tag{20}$$

Orders and their taxonomy (A)

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

reflexive:	iff $id_A \subseteq R$	(21)
coreflexive:	iff $R \subseteq id_A$	(22)
transitive:	iff $R \cdot R \subseteq R$	(23)
anti-symmetric:	iff $R \cap R^\circ \subseteq id_A$	(24)
symmetric:	iff $R \subseteq R^\circ (\equiv R = R^\circ)$	(25)
connected:	iff $R \cup R^\circ = \top$	(26)

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

Proof of (16):

$$\begin{array}{ll} & X \subseteq (R \cap R) \\ \equiv & \quad \{ \text{ meet-universal} \} \\ & (X \subseteq R) \wedge (X \subseteq R) \\ \equiv & \quad \{ \text{ logic} \} \\ & (X \subseteq R) \\ \equiv & \quad \{ \text{ indirection} \} \\ & R \cap R = R \end{array}$$

Proof of (17):

$$\begin{array}{ll} & X \subseteq (R \cap S) \\ \equiv & \quad \{ \text{ universal} \} \\ & (X \subseteq R) \wedge (X \subseteq S) \\ \equiv & \quad \{ \text{ logic} \} \\ & (X \subseteq S) \wedge (X \subseteq R) \\ \equiv & \quad \{ \text{ universal} \} \\ & X \subseteq (S \cap R) \\ \equiv & \quad \{ \text{ indirection} \} \\ & R \cap S = S \cap R \end{array}$$

Proof of (19):

$$\begin{array}{ll} & T \cdot (R \cap S) \subseteq (T \cdot R) \cap (T \cdot S) \\ \equiv & \quad \{ \text{ meet-universal (6) } \} \\ & T \cdot (R \cap S) \subseteq T \cdot R \wedge T \cdot (R \cap S) \subseteq T \cdot S \\ \Leftarrow & \quad \{ \text{ monotonicity} \} \\ & R \cap S \subseteq R \wedge R \cap S \subseteq S \\ \equiv & \quad \{ \text{ cancellation} \} \\ & \text{T} \end{array}$$

A connected order (26) is such that

$$\forall a, b. aRb \vee bRa$$

Proof of (25):

$$\begin{array}{ll} & R \subseteq R^\circ \\ \equiv & \quad \{ \wedge\text{-idempotency} \} \\ & R \subseteq R^\circ \wedge R \subseteq R^\circ \\ \equiv & \quad \{ \text{ converse is } \subseteq\text{-monotone and involutive} \} \\ & R \subseteq R^\circ \wedge R^\circ \subseteq R \\ \equiv & \quad \{ \text{ ping-pong} \} \\ & R = R^\circ \end{array}$$

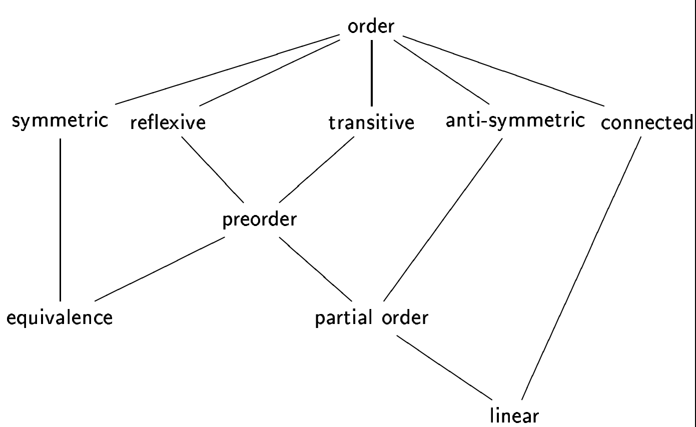
Order taxonomy (B)

- **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 $[\![\phi]\!]$ such that

$$\phi\, a \quad \equiv \quad a[\![\phi]\!]a$$

i.e., it maps every a which validates ϕ onto itself.

Order taxonomy (C)



Kernel and image

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

$$ker\,R \stackrel{\rm def}{=} R^\circ \cdot R \qquad (27)$$

Image of $B \xleftarrow{R} A$ is $B \xleftarrow{img\,R} B$ defined by

$$img\,R \stackrel{\rm def}{=} R \cdot R^\circ \qquad (28)$$

Duality:

$$ker\,(R^\circ) = img\,R \qquad (29)$$
$$img\,(R^\circ) = ker\,R \qquad (30)$$

Proof of (29):

$$
\begin{array}{cl}
& ker\,(R^\circ) \\
= & \quad \{ \text{ definition (27) } \} \\
& (R^\circ)^\circ \cdot R^\circ \\
= & \quad \{ \text{ involution (7) } \} \\
& R \cdot R^\circ \\
= & \quad \{ \text{ definition (30) } \} \\
& img\,R
\end{array}
$$

Using kernel in specifications

Implict specification of *sorting* in VDM notation:

```
ImplSort(l: seq of real) r: seq of real
post IsPermutation(r,l) and IsOrdered(r);
```

where

```
IsPermutation:  seq of real * seq of real -> 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};
```

abbreviates to

Using kernel in specifications

$$ImplSort \stackrel{\rm def}{=} IsOrdered \cdot (ker\;seq2bag)$$

where

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

Properties of kernel and image

Order-preservation:

$$R \subseteq S \quad \Rightarrow \quad \mathit{ker}\, R \subseteq \mathit{ker}\, S \tag{31}$$

$$R \subseteq S \quad \Rightarrow \quad \mathit{img}\, R \subseteq \mathit{img}\, S \tag{32}$$

Symmetry:

$$(\mathit{ker}\, R)^\circ \quad = \quad \mathit{ker}\, R \tag{33}$$

$$(\mathit{img}\, R)^\circ \quad = \quad \mathit{img}\, R \tag{34}$$

Also:

$$R \subseteq R \cdot \mathit{ker}\, R \qquad (= \mathit{img}\, R \cdot R) \tag{35}$$

Entireness and simplicity

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

$$R \text{ is entire} \quad \equiv \quad id \subseteq \mathit{ker}\, R \tag{36}$$

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

$$R \text{ is simple} \quad \equiv \quad \mathit{img}\, R \subseteq id \tag{37}$$

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:

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

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"* — *cf.* (31,32).

Proof of (31) and (32) : From (8) and (2) we get $R^\circ \cdot R \subseteq S^\circ \cdot$ $R \cdot R^\circ \subseteq S \cdot S^\circ$, respectively.

Proof of (33):

$$\begin{array}{cl} & (\mathit{ker}\, R)^\circ \\ = & \quad \{\ \text{definition (27)}\ \} \\ & (R^\circ \cdot R)^\circ \\ = & \quad \{\ \text{contravariance (9)}\ \} \\ & R^\circ \cdot (R^\circ)^\circ \\ = & \quad \{\ \text{involution (7)}\ \} \\ & R^\circ \cdot R \\ = & \quad \{\ \text{definition (27)}\ \} \\ & \mathit{ker}\, R \end{array}$$

Proof of (35):

$$\begin{array}{cl} & R \\ = & \quad \{\ (16)\ \} \\ & R \cap R \\ \subseteq & \quad \{\text{modular law}\} \\ & R \cdot (id \cap R^\circ \cdot R) \\ \subseteq & \quad \{\text{monotonicity}\} \\ & R \cdot R^\circ \cdot R \end{array}$$

Surjectiveness and injectiveness

More taxonomy:

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

Facts:

$$R \text{ is entire and injective} \equiv \mathit{ker}\, R = id \tag{38}$$

$$R \text{ is simple and surjective} \equiv \mathit{img}\, R = id \tag{39}$$

Bijections

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

$$B \xleftarrow{f} A \text{ bijective} \equiv \mathit{ker}\, f = id \wedge \mathit{img}\, f = id \tag{40}$$

In this case

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

More about kernel

Kernel of composition:

$$\mathit{ker}\,(R \cdot S) = S^\circ \cdot (\mathit{ker}\, R) \cdot S \tag{41}$$

Kernel of meet:

$$R^\circ \cdot S \cap id \subseteq \mathit{ker}\,(R \cap S) \tag{42}$$

Kernel of a partial function is transitive:

$$R \text{ is simple} \Rightarrow \mathit{ker}\, R \cdot \mathit{ker}\, R \subseteq \mathit{ker}\, R \tag{43}$$

Proof of (38):

$$
\begin{array}{cl}
& R \text{ is entire and injective} \\
\equiv & \quad \{ \text{ definitions } \} \\
& id \subseteq \mathit{ker}\, R \wedge \mathit{img}\, R^\circ \subseteq id \\
\equiv & \quad \{ \text{ (30) } \} \\
& id \subseteq \mathit{ker}\, R \wedge \mathit{ker}\, R \subseteq id \\
\equiv & \quad \{ \text{ ping-pong (4) } \} \\
& id = \mathit{ker}\, R
\end{array}
$$

Kernel of a function

Kernel of a total function is an equivalence: it is symmetric (33), reflexive (36) and transitive (43):

$$
\begin{array}{cl}
 & a'(\mathit{ker}\, f)a \\
\equiv & \quad \{ \ \mathit{ker}\, f = f^\circ \cdot f \ \} \\
 & \exists a''.(a' f^\circ a'') \wedge (a'' = f\, a) \\
\equiv & \quad \{ \ \text{converse of a function, pointwise} \ \} \\
 & \exists a''.(a'' = fa') \wedge (a'' = f\, a) \\
\equiv & \quad \{ \ \text{equality is transitive} \ \} \\
 & fa' = fa
\end{array}
$$

Properties of coreflexives

For any T and coreflexive R:

$$R \cdot T \subseteq T \tag{44}$$
$$T \cdot R \subseteq T \tag{45}$$

Coreflexives are symmetric and transitive:

$$R = R^\circ = R \cdot R = R \cap id \tag{46}$$

Meet of two coreflexives is composition:

$$R \cap S = R \cdot S \tag{47}$$

Proof of (47): Ping-pong $\Rightarrow$:

$$
\begin{array}{cl}
 & R \text{ and } S \text{ are coreflexives} \\
\Rightarrow & \quad \{ \text{ by } (44, 45) \} \\
 & R \cdot S \subseteq R \wedge R \cdot S \subseteq S \\
\equiv & \quad \{ \text{ by } (6) \} \\
 & R \cdot S \subseteq (R \cap S)
\end{array}
$$

Ping-pong $\Leftarrow$:

$$
\begin{array}{cl}
 & R \cap S \subseteq R \cdot S \\
\equiv & \quad \{ \text{ identity and } (46) \} \\
 & R \cdot id \cap S \subseteq id \cap R \cdot R^\circ \cdot S \\
\equiv & \quad \{ \ S = id \text{ in } (11) \} \\
 & \mathrm{T}
\end{array}
$$

Proof of (42):

$$
\begin{array}{cl}
 & R^\circ \cdot S \cap id \\
\subseteq & \quad \{ \ (13) \text{ for } T := id \text{ and } R := R^\circ \ \} \\
 & (R^\circ \cap S^\circ) \cdot (S \cap R) \\
= & \quad \{ \ \text{converse of meet and definition} \ \} \\
 & \mathit{ker}\,(R \cap S)
\end{array}
$$

Proof of (43):

$$
\begin{array}{cl}
 & R \text{ is simple} \\
\equiv & \quad \{ \text{ definition} \} \\
 & R \cdot R^\circ \subseteq id \\
\Rightarrow & \quad \{ \text{ by } (2) \} \\
 & R^\circ \cdot (R \cdot R^\circ) \cdot R \subseteq R^\circ \cdot R \\
\equiv & \quad \{ \text{ associative } \cdot \} \\
 & (R^\circ \cdot R) \cdot (R^\circ \cdot R) \subseteq (R^\circ \cdot R) \\
\equiv & \quad \{ \text{ definition of } \mathit{ker} \} \\
 & \mathit{ker}\, R \cdot \mathit{ker}\, R \subseteq \mathit{ker}\, R
\end{array}
$$

Proof of (46):

$$
\begin{array}{cl}
 & R \subseteq id \\
\equiv & \quad \{ \text{ abbreviation} \} \\
 & R = R \cap id
\end{array}
$$

Symmetry:

$$
\begin{array}{cl}
 & R \\
\subseteq & \quad \{ \text{ fact } (35) \} \\
 & R \cdot R^\circ \cdot R \\
\subseteq & \quad \{ \text{ coreflexive } R \} \\
 & id \cdot R^\circ \cdot id \\
= & \quad \{ \text{ identities} \} \\
 & R^\circ
\end{array}
$$

Transitivity:

$$
\begin{array}{cl}
 & R \subseteq id \\
\equiv & \quad \{ \text{ fact } (44) \} \\
 & R \cdot R \subseteq R
\end{array}
$$

Range

rng-universal: for all $X \subseteq id$,

$$rng\, R \subseteq X \quad \equiv \quad R \subseteq X \cdot R \tag{48}$$

rng-reflexion (or $rng\, R$ is coreflexive):

$$rng\, R \subseteq id \tag{49}$$

rng-cancellation:

$$R \subseteq (rng\, R) \cdot R \tag{50}$$

— in fact

$$R = (rng\, R) \cdot R \tag{51}$$

Range (cont.)

because from (49) one gets $(rng\, R) \cdot R \subseteq R$ which ping-pongs with (50).

rng-"fusion":

$$rng\, (R \cdot S) \subseteq rng\, R \tag{52}$$

Explicit definition of range

$$rng\, R \quad = \quad img\, R \cap id \tag{53}$$

Corollary — R replaced by $R \cap S$:

$$rng\, (R \cap S) \quad = \quad id \cap (R \cdot S^\circ) \tag{54}$$

Proof of (52):

$$
\begin{array}{cl}
 & rng\,(R \cdot S) \subseteq rng\, R \\
\equiv & \quad \{ \ (48) \ \} \\
 & R \cdot S \subseteq (rng\, R) \cdot R \cdot S \\
\equiv & \quad \{ \ (51) \ \} \\
 & R \cdot S \subseteq R \cdot S \\
\equiv & \quad \{ \ \text{trivia} \ \} \\
 & \mathrm{T}
\end{array}
$$

Proof of (53): We want to prove, for every coreflexive X,

$$img\,R \cap id \subseteq X \quad \equiv \quad R \subseteq X \cdot R$$

cf. (48) Ping-pong proof:

$$
\begin{array}{ll}
 & img\,R \cap id \subseteq X \\
\Rightarrow & \quad \{ \text{ monotonicity} \} \\
 & (img\,R \cap id) \cdot R \subseteq X \cdot R \\
\Rightarrow & \quad \{ \text{ (12) for } R = id,\ S = T = R \text{ and transitive } \subseteq \} \\
 & (R \cap R) \subseteq X \cdot R \\
\equiv & \quad \{ \text{ trivia} \} \\
 & R \subseteq X \cdot R \\
\Rightarrow & \quad \{ \text{ monotonicity} \} \\
 & R \cdot R^{\circ} \cap id \subseteq X \cdot R \cdot R^{\circ} \cap id \\
\Rightarrow & \quad \{ \text{ (12) for } R = X,\ S = R \cdot R^{\circ},\ T = id \text{ and trivia } \} \\
 & R \cdot R^{\circ} \cap id \subseteq X \cdot (R \cdot R^{\circ} \cap X^{\circ}) \\
\Rightarrow & \quad \{ \text{ (19) } \} \\
 & R \cdot R^{\circ} \cap id \subseteq X \cdot R \cdot R^{\circ} \cap X \cdot X^{\circ} \\
\Rightarrow & \quad \{ \text{ (6) from left to right } \} \\
 & R \cdot R^{\circ} \cap id \subseteq X \cdot X^{\circ} \\
\equiv & \quad \{ X \text{ is coreflexive} \} \\
 & img\,R \cap id \subseteq X
\end{array}
$$

Proof of (54): Ping-pong:

$$
\begin{array}{ll}
 & rng\,(R \cap S) \\
= & \quad \{ \text{ definitions } \} \\
 & (R \cap S) \cdot (R \cap S)^{\circ} \cap id \\
= & \quad \{ \text{ converse of meet } \} \\
 & (R \cap S) \cdot (R^{\circ} \cap S^{\circ}) \cap id \\
\subseteq & \quad \{ \text{ monotonicity } \} \\
 & (R \cdot S^{\circ}) \cap id \\
= & \quad \{ \text{ meet idempotency } \} \\
 & (R \cdot S^{\circ}) \cap id \cap id \\
\subseteq & \quad \{ \text{ (42) } \} \\
 & ker\,(R^{\circ} \cap S^{\circ}) \cap id \\
= & \quad \{ \text{ converse of meet } \} \\
 & ker\,(R \cap S)^{\circ} \cap id \\
= & \quad \{ \text{ kernel-image duality } \} \\
 & img\,(R \cap S) \cap id \\
= & \quad \{ \text{ definition } \} \\
 & rng\,(R \cap S)
\end{array}
$$

Proof of (57):

$$
\begin{array}{ll}
 & dom\,R \\
\equiv & \quad \{ \text{ by definition and above} \} \\
 & img\,R^{\circ} \cap id \\
\equiv & \quad \{ \text{ cf. above} \} \\
 & ker\,R \cap id
\end{array}
$$

Range

Range of composition:

$$rng\,(R \cdot S) \quad = \quad rng\,(R \cdot rng\,S) \tag{55}$$

NB:

- *rng*-universal (48) is a Galois connection:

$$\underbrace{rng\,R}_{\substack{f\,R \\ \text{(“lower adjoint”)}}} \subseteq X \quad \equiv \quad R \subseteq \underbrace{X \cdot R}_{\substack{g\,X \\ \text{(“upper adjoint”)}}}$$

- more Galois connections to come.
- Galois connections are mathematically very rich.

Proof of (55): Ping-pong $\subseteq$:

$$
\begin{array}{ll}
 & rng\,(R \cdot S) \\
\subseteq & \quad \{\ (51)\ \} \\
 & rng\,(R \cdot rng\,S \cdot S) \\
\subseteq & \quad \{\ (52)\ \} \\
 & rng\,(R \cdot rng\,S)
\end{array}
$$

Ping-pong $\supseteq$:

$$
\begin{array}{ll}
 & rng\,(R \cdot rng\,S) \subseteq rng\,(R \cdot S) \\
\equiv & \quad \{\ \text{explicitation (53) and simplification} \} \\
 & R \cdot rng\,S \cdot R^\circ \cap id \subseteq R \cdot img\,S \cdot R^\circ \cap id \\
\Leftarrow & \quad \{\ \text{monotonicity} \} \\
 & rng\,S \subseteq img\,S \\
\equiv & \quad \{\ (53)\ \} \\
 & \mathrm{T}
\end{array}
$$

Domain

Definition:

$$dom\,R = rng\,R^\circ \tag{56}$$

that is:

$$dom\,R = img\,R^\circ \cap id = ker\,R \cap id \tag{57}$$

dom-universal: for all $X \subseteq id$,

$$dom\,R \subseteq X \quad \equiv \quad R \subseteq R \cdot X \tag{58}$$

Dual of (51):

$$R = R \cdot (dom\,R) \tag{59}$$

Proof of (58) :

$$
\begin{array}{ll}
 & dom\,R \subseteq X \\
\equiv & \quad \{\ \} \\
 & rng\,R^\circ \subseteq X \\
\equiv & \quad \{\ \} \\
 & R^\circ \subseteq X \cdot R^\circ \\
\equiv & \quad \{\ \text{converses}\ \} \\
 & R \subseteq R \cdot X^\circ \\
\equiv & \quad \{\ \text{coreflexive } X\ \} \\
 & R \subseteq R \cdot X
\end{array}
$$

Kernel and domain

Kernel of injective relation is its domain:

$$R \text{ is injective} \quad \equiv \quad dom\,R = ker\,R \tag{60}$$

Domain of entire relation is the identity:

$$R \text{ is entire} \quad \equiv \quad dom\,R = id \tag{61}$$

Proof of (60):

$$
\begin{array}{ll}
 & R \text{ is injective, } i.e.\ R^\circ \text{ is simple} \\
\equiv & \quad \{\ \} \\
 & img\,R^\circ \subseteq id \\
\equiv & \quad \{\ \} \\
 & ker\,R \subseteq id \\
\equiv & \quad \{\ \} \\
 & ker\,R \cap id = ker\,R \\
\equiv & \quad \{\ \} \\
 & dom\,R = ker\,R
\end{array}
$$

Proof of (61):

$$
\begin{array}{ll}
& R \text{ is entire} \\
\equiv & \qquad \{ \ (36) \ \} \\
& id \subseteq \mathit{ker}\, R \\
\equiv & \qquad \{ \ (15) \ \} \\
& id \cap \mathit{ker}\, R = id \\
\equiv & \qquad \{ \ (57) \ \} \\
& \mathit{dom}\, R = id
\end{array}
$$

Simple/entire shunting

If T is simple, then

$$T \cdot R \subseteq S \quad \equiv \quad (\mathit{ker}\, T) \cdot R \subseteq T^\circ \cdot S \tag{62}$$

$$R \cdot T^\circ \subseteq S \quad \equiv \quad R \cdot \mathit{ker}\, T \subseteq S \cdot T \tag{63}$$

The following version of (62) turns up in [MB02]:

$$T \cdot R \subseteq S \quad \equiv \quad (\mathit{dom}\, T) \cdot R \subseteq T^\circ \cdot S \tag{64}$$

The equivalent version of (63) is:

$$R \cdot \mathit{dom}\, T \subseteq S \cdot T \quad \equiv \quad R \cdot T^\circ \subseteq S \tag{65}$$

Proof of (63):

$$
\begin{array}{ll}
& R \cdot \mathit{ker}\, T \subseteq S \cdot T \\
\equiv & \qquad \{ \text{ taking converses} \} \\
& (\mathit{ker}\, T)^\circ \cdot R^\circ \subseteq T^\circ \cdot S^\circ \\
\equiv & \qquad \{ \ \text{kernel symmetry (33)} \ \} \\
& (\mathit{ker}\, T) \cdot R^\circ \subseteq T^\circ \cdot S^\circ \\
\equiv & \qquad \{ \ \text{fact (62)} \ \} \\
& T \cdot R^\circ \subseteq S^\circ \\
\equiv & \qquad \{ \ \text{taking converses again} \ \} \\
& R \cdot T^\circ \subseteq S
\end{array}
$$

Proof of (62): Ping-pong:

$$
\begin{array}{ll}
& T \cdot R \subseteq S \\
\Rightarrow & \qquad \{ \ \text{monotonicity of } (T^\circ \cdot) \ \} \\
& (\mathit{ker}\, T) \cdot R \subseteq T^\circ \cdot S \\
\Rightarrow & \qquad \{ \ \text{monotonicity of } (T \cdot) \ \} \\
& T \cdot (\mathit{ker}\, T) \cdot R \subseteq T \cdot (T^\circ \cdot S) \\
\Rightarrow & \qquad \{ \ T \subseteq T \cdot \mathit{ker}\, T \text{ by (35)} \ \} \\
& T \cdot R \subseteq (T \cdot T^\circ) \cdot S \\
\Rightarrow & \qquad \{ \ \text{simplicity} \} \\
& T \cdot R \subseteq S
\end{array}
$$

Proof of (64): Ping-pong:

$$
\begin{array}{ll}
& T \cdot R \subseteq S \\
\Rightarrow & \qquad \{ \ \text{monotonicity of } (T^\circ \cdot) \ \} \\
& (\mathit{ker}\, T) \cdot R \subseteq T^\circ \cdot S \\
\Rightarrow & \qquad \{ \ \mathit{dom}\, T \subseteq \mathit{ker}\, T \ \} \\
& (\mathit{dom}\, T) \cdot R \subseteq T^\circ \cdot S \\
\Rightarrow & \qquad \{ \ \text{monotonicity of } (T \cdot) \ \} \\
& T \cdot (\mathit{dom}\, T) \cdot R \subseteq T \cdot T^\circ \cdot S \\
\Rightarrow & \qquad \{ \ \text{fact (59) and simplicity} \} \\
& T \cdot R \subseteq S
\end{array}
$$

Reasoning about functions

Shunting rules:

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \tag{66}$$

$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{67}$$

Equality:

$$f \subseteq g \equiv f = g \equiv f \supseteq g \tag{68}$$

Ping-pong proof of (68) follows.

Proof of (66) and (67): Resort respectively to (64) and (65) for *dom* — because f is entire — and simplify.

Example of a ping-pong proof

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

Relators

A **relator** is a functor on relations

$$\begin{tikzcd} A \arrow[r, dotted, no head] \arrow[d, "R"'] & \mathsf{F}\,A \arrow[d, "\mathsf{F}\,R"] \\ B \arrow[r, dotted, no head] & \mathsf{F}\,B \end{tikzcd}$$

which is monotonic and commutes with converse:

$$\begin{array}{lcl} R \subseteq S & \Rightarrow & (\mathsf{F}\,R) \subseteq (\mathsf{F}\,S) \\ \mathsf{F}\,(R^\circ) & = & (\mathsf{F}\,R)^\circ \end{array}$$

(Recall that F will commute with *composition* and *identity* too.)

Properties of relators

- Relators preserve simplicity and entireness
- Relators commute with kernel and image:

$$\begin{array}{rcll} \mathit{ker}\,(\mathsf{F}\,R) & = & \mathsf{F}\,(\mathit{ker}\,R) & (69) \\ \mathit{img}\,(\mathsf{F}\,R) & = & \mathsf{F}\,(\mathit{img}\,R) & (70) \end{array}$$

- Relators preserve coreflexivity, since $R \subseteq id$ implies $\mathsf{F}\,R \subseteq \mathsf{F}\,id = id$
- (More to come here...)

Proof of (69) :

$$\begin{array}{cl} & \mathsf{F}\,(R^\circ \cdot R) \\ = & \quad \{\ \} \\ & (\mathsf{F}\,R^\circ) \cdot (\mathsf{F}\,R) \\ = & \quad \{\ \} \\ & (\mathsf{F}\,R)^\circ \cdot (\mathsf{F}\,R) \\ = & \quad \{\ \} \\ & \mathit{ker}\,(\mathsf{F}\,R) \end{array}$$

References

[ABH+92] Chritiene Aarts, Roland Backhouse, Paul Hoogendijk, Ed Voermans, and Jaap van der Woude. A relational theory of datatypes, December 1992.

[Blo76] S.L. Bloom. Varieties of ordered algebras. *JCSS*, 13:200–212, 1976.

[MB02] Shin-Cheng Mu and Richard Bird. Inverting functions as folds. In *MPC'02: Mathematics of Program Construction*, Lecture Notes in Computer Science. Springer, 2002. (forthcoming).

[Oli92] J. N. Oliveira. *Software Reification using the SETS Calculus* . In *Proc. of the BCS FACS 5th Refinement Workshop, Theory and Practice of Formal Software*

Development, London, UK, pages 140–171. Springer-Verlag, 8–10 January 1992. (Invited paper).