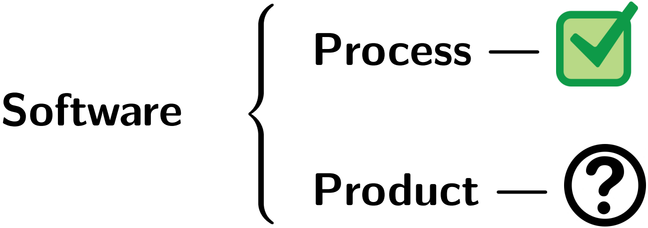
CSI - A Calculus for Information Systems (2023/24)

Class 1 — About FM

Global picture

Concerning software ‘engineering’:



Software

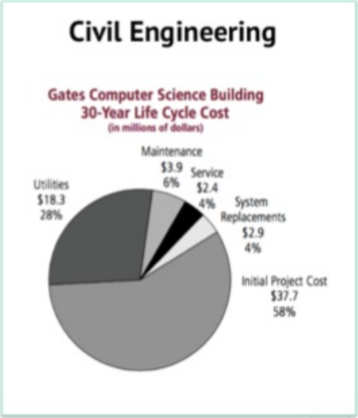
Process — ☑

Product — ?

Formal methods provide an answer to the question mark above.

Global picture

Concerning software ‘engineering’:



Credits: Zhenjiang Hu, NII, Tokyop JP

Have you ever used a FM?

Of course you have! Check this:

A problem

> *My three children*
> *were born at a 3 year*
> *interval rate.*
> *Altogether, they are*
> *as old as me. I am 48.*
> *How old are they?*

A model

$$x + (x+3) + (x+6) = 48$$

— maths description of the problem.

Some calculations

$$\begin{array}{cl} & 3x + 9 = 48 \\ \equiv & \{ \text{"al-djabr" rule} \} \\ & 3x = 48 - 9 \\ \equiv & \{ \text{"al-hatt" rule} \} \\ & x = 16 - 3 \end{array}$$

The solution

$$\begin{array}{rcl} x & = & 13 \\ x+3 & = & 16 \\ x+6 & = & 19 \end{array}$$

Have you ever used a FM?

Of course you have! Check this:

A problem

> *My three children*
> *were born at a 3 year*
> *interval rate.*
> *Altogether, they are*
> *as old as me. I am 48.*
> *How old are they?*

A model

$$x + (x+3) + (x+6) = 48$$

— maths description of the problem.

Some calculations

$$\begin{array}{cl} & 3x + 9 = 48 \\ \equiv & \{ \text{"al-djabr" rule} \} \\ & 3x = 48 - 9 \\ \equiv & \{ \text{"al-hatt" rule} \} \\ & x = 16 - 3 \end{array}$$

The solution

$$\begin{array}{rcl} x & = & 13 \\ x+3 & = & 16 \\ x+6 & = & 19 \end{array}$$

Have you ever used a FM?

Of course you have! Check this:

A problem

My three children were born at a 3 year interval rate. Altogether, they are as old as me. I am 48. How old are they?

A model

$$x + (x + 3) + (x + 6) = 48$$

— maths description of the problem.

Some calculations

$$\begin{array}{ll} & 3x + 9 = 48 \\ \equiv & \{ \text{"al-djabr" rule} \} \\ & 3x = 48 - 9 \\ \equiv & \{ \text{"al-hatt" rule} \} \\ & x = 16 - 3 \end{array}$$

The solution

$$\begin{array}{rcl} x & = & 13 \\ x + 3 & = & 16 \\ x + 6 & = & 19 \end{array}$$

Have you ever used a FM?

Of course you have! Check this:

A problem

My three children
were born at a 3 year
interval rate.
Altogether, they are
as old as me. I am 48.
How old are they?

A model

$$x + (x + 3) + (x + 6) = 48$$

— maths description of the problem.

Some calculations

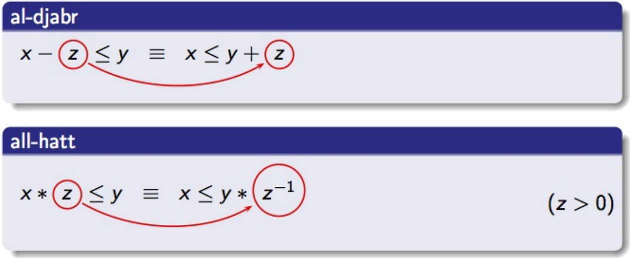
$$\begin{array}{ll} & 3x + 9 = 48 \\ \equiv & \{ \text{"al-djabr" rule} \} \\ & 3x = 48 - 9 \\ \equiv & \{ \text{"al-hatt" rule} \} \\ & x = 16 - 3 \end{array}$$

The solution

$$\begin{array}{rcl} x & = & 13 \\ x + 3 & = & 16 \\ x + 6 & = & 19 \end{array}$$

Have you ever used a FM?

"Al-djabr" rule ? "al-hatt" rule ?



al-djabr

$$x - \textcircled{z} \leq y \;\equiv\; x \leq y + \textcircled{z}$$

all-hatt

$$x * \textcircled{z} \leq y \;\equiv\; x \leq y * \textcircled{z^{-1}} \qquad (z > 0)$$

These rules that you have used so many times were discovered by Persian mathematicians, notably by Al-Huwarizmi (9c AD).

NB: "**algebra**" stems from "**al-djabr**" and "**algarismo**" from **Al-Huwarizmi**.

Software problems

Now, suppose the **problem** was

> *Please write a program to list the students of my class ordered by their marks.*

Is there a mathematical **model** for this problem?

Yes, of course there is — see aside:

$$sort \subseteq \frac{bag}{bag} \cap \frac{true}{sorted}$$

where

$$sorted = \ldots marks \ldots$$

$$bag = \ldots.$$

But,

- what do $X \cap Y$, $\frac{f}{g}$ ... mean here?
- Is there an "**algebra**" for such symbols?

Yes — Wait and see :-)

Software problems

Now, suppose the **problem** was

Please write a program to list the students of my class ordered by their marks.

Is there a mathematical **model** for this problem?

Yes, of course there is — see aside:

$$sort \subseteq \frac{bag}{bag} \cap \frac{true}{sorted}$$

where

$sorted = \ldots marks \ldots$

$bag = \ldots.$

But,

- what do $X \cap Y$, $\frac{f}{g}$ … mean here?
- Is there an "**algebra**" for such symbols?

Yes — Wait and see :-)

Software problems

Now, suppose the **problem** was

Please write a program to list the students of my class ordered by their marks.

Is there a mathematical **model** for this problem?

Yes, of course there is — see aside:

$$sort \subseteq \frac{bag}{bag} \cap \frac{true}{sorted}$$

where

$sorted = \ldots marks \ldots$

$bag = \ldots.$

But,

- what do $X \cap Y$, $\frac{f}{g}$ ... mean here?
- Is there an "**algebra**" for such symbols?

Yes — Wait and see :-)

Software problems

Now, suppose the **problem** was

> *Please write a program to list the students of my class ordered by their marks.*

Is there a mathematical **model** for this problem?

Yes, of course there is — see aside:

$$\mathit{sort} \subseteq \frac{\mathit{bag}}{\mathit{bag}} \cap \frac{\mathit{true}}{\mathit{sorted}}$$

where

$\mathit{sorted} = \ldots \mathit{marks} \ldots$

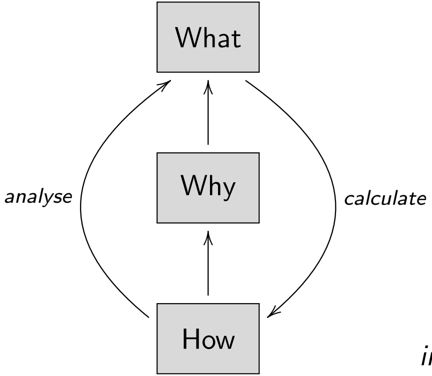
$\mathit{bag} = \ldots.$

But,

- what do $X \cap Y$, $\frac{f}{g}$ ... mean here?
- Is there an "**algebra**" for such symbols?

Yes — Wait and see :-)

FM — scientific software design

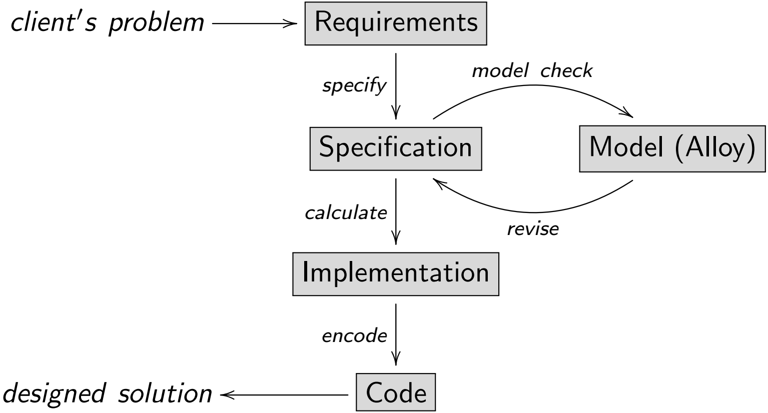


specification (*model*)

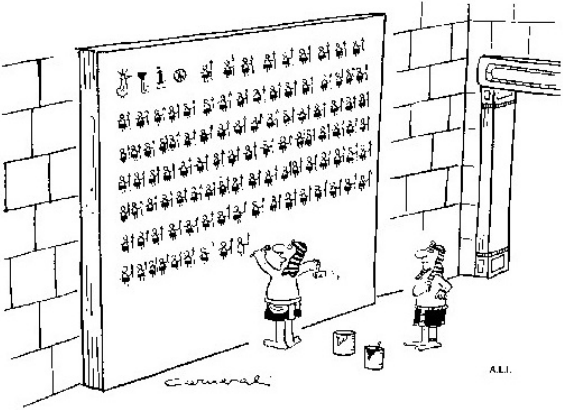
justification

implementation (*program*)

FM — simplified life-cycle



Notation matters!



Are you sure there isn't a simpler means of writing 'The Pharaoh had 10,000 soldiers?'

Credits: Cliff B. Jones 1980 [2]

Well-known FM notations / tools / resources

Just a sample, as there are many — follow the links (in alphabetic order):

Notations:

- Alloy
- B-Method
- JML
- mCRL2
- SPARK-Ada
- TLA+
- VDM
- Z

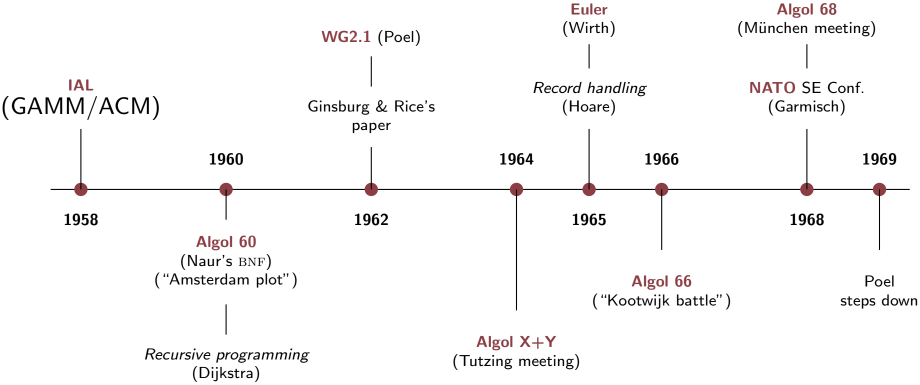
Tools:

- Alloy 4
- Coq
- Frama-C
- NuSMV
- Overture

Resources:

- Formal Methods Europe
- Formal Methods wiki (Oxford)

60+ years ago (1958-)



IAL
(GAMM/ACM)

1958

1960

Algol 60
(Naur's BNF)
("Amsterdam plot")

Recursive programming
(Dijkstra)

WG2.1 (Poel)

Ginsburg & Rice's
paper

1962

1964

Algol X+Y
(Tutzing meeting)

Euler
(Wirth)

Record handling
(Hoare)

1965

1966

Algol 66
("Kootwijk battle")

Algol 68
(München meeting)

NATO SE Conf.
(Garmisch)

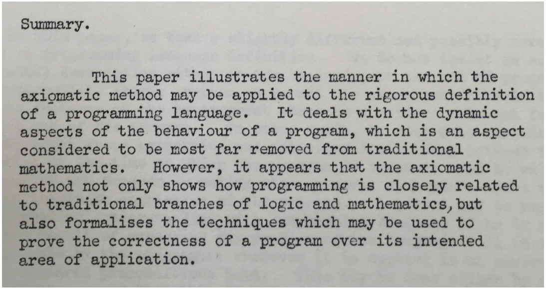
1968

1969

Poel
steps down

Hoare Logic — "turning point" (1968)

Floyd-Hoare logic for **program correctness** dates back to 1968:



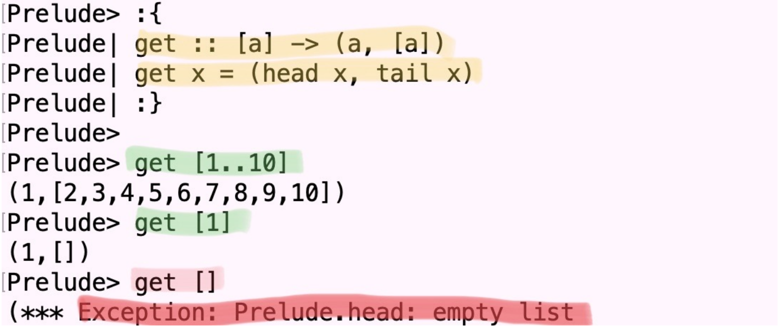
Summary.

This paper illustrates the manner in which the axiomatic method may be applied to the rigorous definition of a programming language. It deals with the dynamic aspects of the behaviour of a program, which is an aspect considered to be most far removed from traditional mathematics. However, it appears that the axiomatic method not only shows how programming is closely related to traditional branches of logic and mathematics, but also formalises the techniques which may be used to prove the correctness of a program over its intended area of application.

(ADB/IFIP/1164;1456)

Inv/pre/post

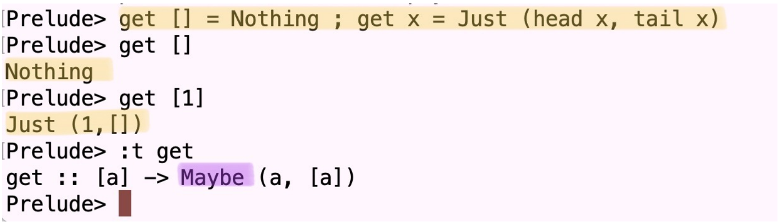
Starting where (pure) **functions** stop:



```
[Prelude> :{
[Prelude| get :: [a] -> (a, [a])
[Prelude| get x = (head x, tail x)
[Prelude| :}
[Prelude>
[Prelude> get [1..10]
(1,[2,3,4,5,6,7,8,9,10])
[Prelude> get [1]
(1,[])
[Prelude> get []
(*** Exception: Prelude.head: empty list
```

Inv/pre/post

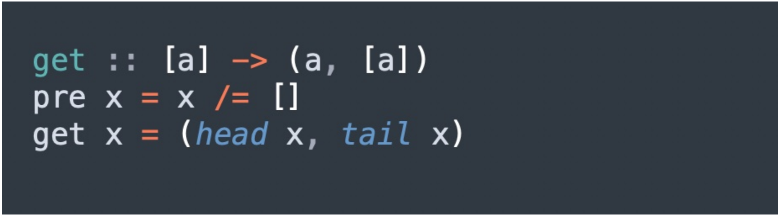
Error handling...



```
Prelude> get [] = Nothing ; get x = Just (head x, tail x)
Prelude> get []
Nothing
Prelude> get [1]
Just (1,[])
Prelude> :t get
get :: [a] -> Maybe (a, [a])
Prelude> 
```

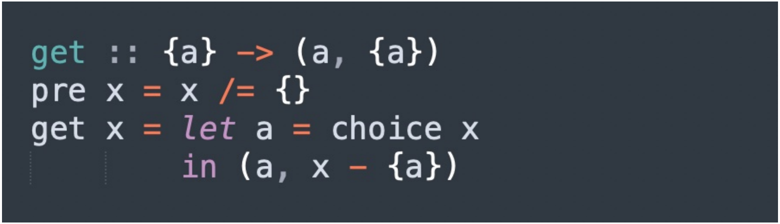
Inv/pre/post

Pre-conditions?



```
get :: [a] -> (a, [a])
pre x = x /= []
get x = (head x, tail x)
```

Not everything is a **list**, a **tree** or a **stream**...



```
get :: {a} -> (a, {a})
pre x = x /= {}
get x = let a = choice x
        in (a, x - {a})
```

Inv/pre/post

`pre`**...?** `choice`**...?**

- Non-determinism
- Parallelism
- Abstraction

Inv/pre/post

`pre`...? `choice`...?

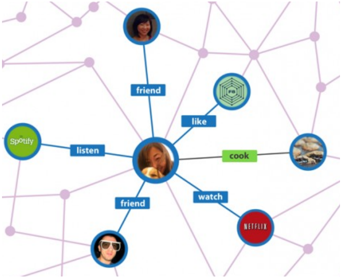
- Non-determinism
- Parallelism
- Abstraction

Functions not enough!

Solution?

Relations *(which extend functions)*

Is “everything” a relation?



How to “dematerialize“ them?

Software is pre-science — **formal** but not fully **calculational**

Software is too diverse — many approaches, lack of unity

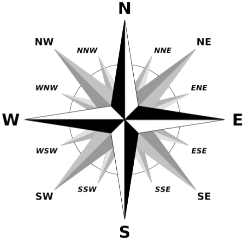
Software is too wide a concept — from assembly to quantum programming

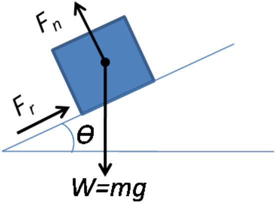
Can you think of a **unified** theory able to express and reason about software *in general*?

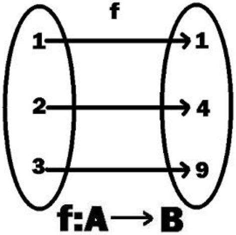
Put in another way:

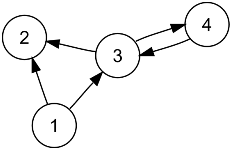
> *Is there a “lingua franca” for the software sciences?*

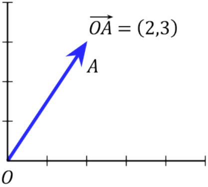
Check the pictures...



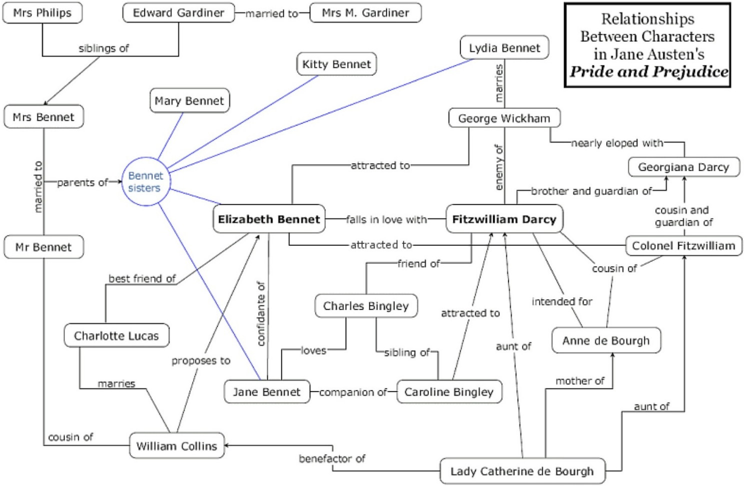






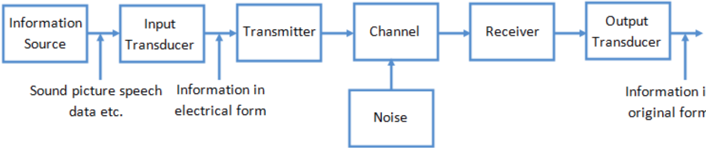


Check the pictures

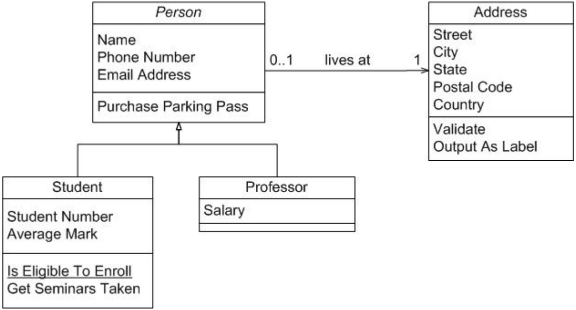


(Wikipedia: **Pride and Prejudice**, by Jane Austin, 1813.)

Check the pictures



Information Source
Input Transducer
Transmitter
Channel
Receiver
Output Transducer
Noise
Sound picture speech data etc.
Information in electrical form
Information in original form



Person
Name
Phone Number
Email Address
Purchase Parking Pass

0..1 lives at 1

Address
Street
City
State
Postal Code
Country
Validate
Output As Label

Student
Student Number
Average Mark
Is Eligible To Enroll
Get Seminars Taken

Professor
Salary

Check the pictures

Which **graphical** device have you found **common** to **all** pictures?

Arrows everywhere

Arrows! Thus we identify a (graphical) ingredient **common** to describing (several) **different** fields of human activity.

For this ingredient to be able to support a **generic** theory of systems, mind the remarks:

- We need a **generic** notation able to cope with very distinct problem domains, e.g. **process** theory versus **database** theory, for instance.
- Notation is not enough — we need to **reason** and **calculate** about software.
- Semantics-rich **diagram** representations are welcome.
- System description may have a **quantitative** side too.

Class 2 — Going Relational

Relation algebra

In previous courses you may have used **predicate logic**, **finite automata**, **grammars** etc to capture the meaning of real-life problems.

Question:

Is there a unified formalism for **formal modelling***?*

Relation algebra

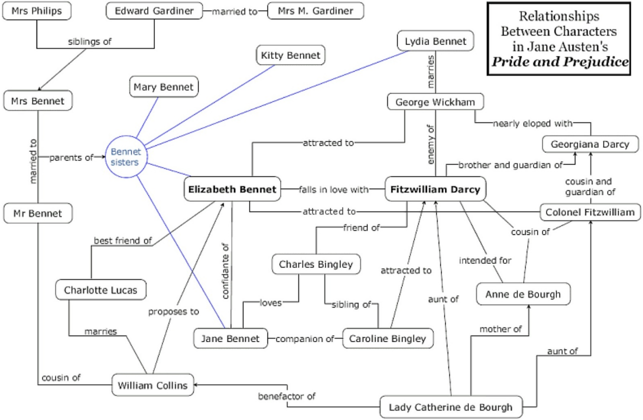
Historically, predicate logic was **not** the first to be proposed:

- Augustus de Morgan (1806-71) — recall *de Morgan* laws — proposed a **Logic of Relations** as early as 1867.
- Predicate logic appeared later.

Perhaps de Morgan was right in the first place: in real life, "everything is a **relation**"...

Everything is a relation...

... as diagram



shows. (Wikipedia: **Pride and Prejudice**, by Jane Austin, 1813.)

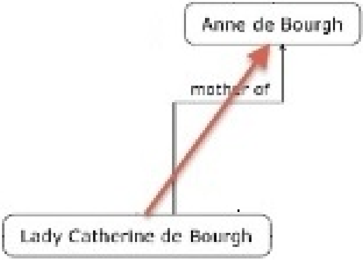
Arrow notation for relations

The picture is a collection of **relations** — vulg. a **semantic network** — elsewhere known as a (binary) **relational system**.

However, in spite of the use of **arrows** in the picture (aside) not many people would write

$$mother\_of : People \to People$$

as the **type** of **relation** $mother\_of$.



Pairs

Consider assertions

$$\begin{array}{ccc} 0 & \leqslant & \pi \\ \texttt{Catherine} & \textit{isMotherOf} & \texttt{Anne} \\ 3 & =(1+) & 2 \end{array}$$

They are statements of fact concerning various kinds of object — real numbers, people, natural numbers, etc

They involve **two** such objects, that is, **pairs**

$$\begin{array}{c} (0, \pi) \\ (\texttt{Catherine}, \texttt{Anne}) \\ (3, 2) \end{array}$$

respectively.

Sets of pairs

So, we might have written instead:

$$\begin{array}{rcl} (0, \pi) & \in & \leqslant \\ (\texttt{Catherine}, \texttt{Anne}) & \in & \mathit{isMotherOf} \\ (3, 2) & \in & (1+) \end{array}$$

What are $(\leqslant)$, $\mathit{isMotherOf}$, $(1+)$?

- they could be regarded as **sets of pairs**
- better: they should be regarded as **binary relations**.

Therefore,

- **orders** — eg. $(\leqslant)$ — are special cases of relations
- **functions** — eg. $\mathit{succ} = (1+)$ — are special cases of relations.

Binary Relations

Binary relations are typed:

Arrow notation. *Arrow* $A \xrightarrow{R} B$ *denotes a binary relation from* A *(source) to* B *(target).*

A, B are types.

Writing

$$B \xleftarrow{R} A$$

means the same as

$$A \xrightarrow{R} B\ .$$

Notation

Infix notation

The usual infix notation used in natural language — eg. Catherine isMotherOf Anne — and in maths — eg. $0 \leqslant \pi$ — extends to arbitrary $B \xleftarrow{R} A$: we write

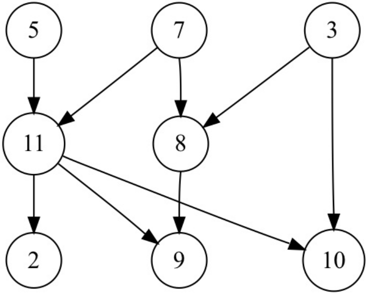
$$b \; R \; a$$

to denote that $(b, a) \in R$.

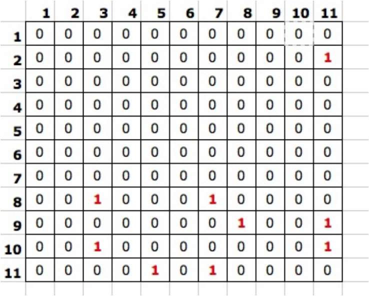
Binary relations are matrices

Binary relations can be regarded as Boolean **matrices**, eg.

Relation R:



Matrix M:



	1	2	3	4	5	6	7	8	9	10	11
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	1	0	0	0	1	0	0	0	0
9	0	0	0	0	0	0	0	1	0	0	1
10	0	0	1	0	0	0	0	0	0	0	1
11	0	0	0	0	1	0	1	0	0	0	0

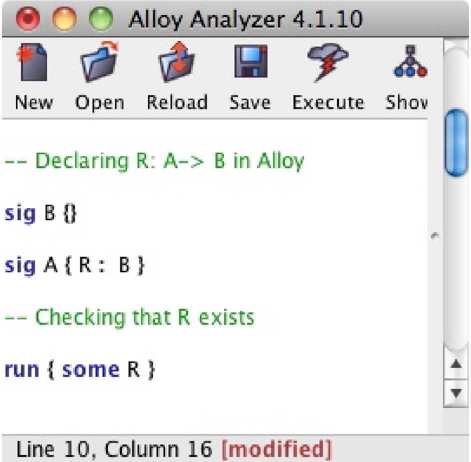
In this case $A = B = \{1..11\}$. Relations $A \xleftarrow{R} A$ over a single type are also referred to as (directed) **graphs**.

Alloy: where "everything is a relation"

Declaring binary relation $A \xrightarrow{R} B$ is **Alloy** (aside).

Alloy is a tool designed at MIT (`http://alloy.mit.edu/alloy`)

We shall be using **Alloy** [1] in this course.



```
-- Declaring R: A-> B in Alloy

sig B {}

sig A { R : B }

-- Checking that R exists

run { some R }
```

Line 10, Column 16 [modified]

Functions are relations

Lowercase letters (or identifiers starting by one such letter) will denote special relations known as **functions**, eg. f, g, $succ$, etc.

We regard **function** $f : A \longrightarrow B$ as the binary relation which relates b to a iff $b = f\ a$. So,

$$b\ f\ a \ \text{ literally means } \ b = f\ a \tag{1}$$

Therefore, we generalize

$$\boxed{\begin{array}{c} B \xleftarrow{\ f\ } A \\ b = f\ a \end{array}} \quad \text{to} \quad \boxed{\begin{array}{c} B \xleftarrow{\ R\ } A \\ b\ R\ a \end{array}}$$

Exercise

Taken from Propositiones ad acuendos iuuenes (“Problems to Sharpen the Young”), by abbot Alcuin of York († 804):

> XVIII. Propositio de homine et capra et lvpo.
> *Homo quidam debebat ultra fluuium transferre lupum, capram, et fasciculum cauli. Et non potuit aliam nauem inuenire, nisi quae duos tantum ex ipsis ferre ualebat. Praeceptum itaque ei fuerat, ut omnia haec ultra illaesa omnino transferret. Dicat, qui potest, quomodo eis illaesis transire potuit?*

Exercise

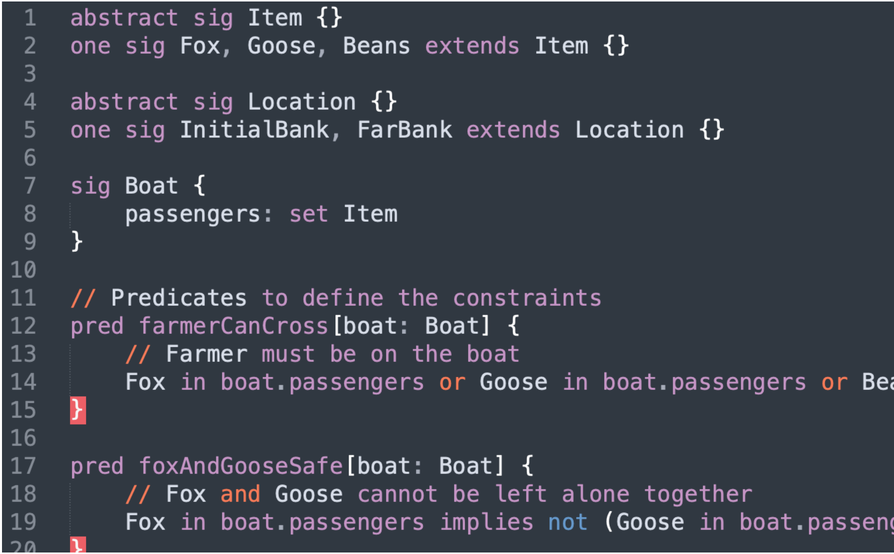
> XVIII. FOX, GOOSE AND BAG OF BEANS PUZZLE. *A farmer goes to market and purchases a fox, a goose, and a bag of beans. On his way home, the farmer comes to a river bank and hires a boat. But in crossing the river by boat, the farmer could carry only himself and a single one of his purchases - the fox, the goose or the bag of beans. (If left alone, the fox would eat the goose, and the goose would eat the beans.) Can the farmer carry himself and his purchases to the far bank of the river, leaving each purchase intact?*

Identify the main **types** and **relations** involved in the puzzle and draw them in a diagram.

Home work

- How would you address this problem?
- Try an write an Alloy for it (sig's only)

NB: You can seek help from ChatGPT — but please be critical...



```
abstract sig Item {}
one sig Fox, Goose, Beans extends Item {}

abstract sig Location {}
one sig InitialBank, FarBank extends Location {}

sig Boat {
    passengers: set Item
}

// Predicates to define the constraints
pred farmerCanCross[boat: Boat] {
    // Farmer must be on the boat
    Fox in boat.passengers or Goose in boat.passengers or Bea
}

pred foxAndGooseSafe[boat: Boat] {
    // Fox and Goose cannot be left alone together
    Fox in boat.passengers implies not (Goose in boat.passeng
}
```

Propositio de homine et capra et lvpo

Data types:

$$\mathit{Being} = \{\mathit{Farmer}, \mathit{Fox}, \mathit{Goose}, \mathit{Beans}\} \tag{2}$$

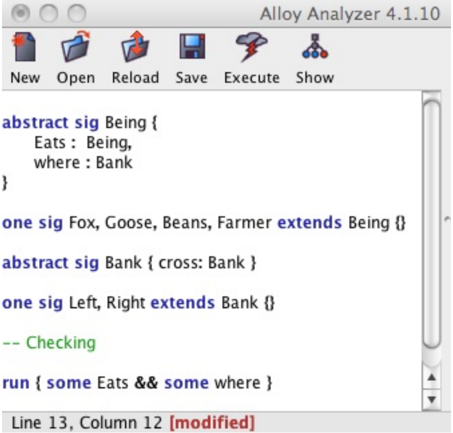
$$\mathit{Bank} = \{\mathit{Left}, \mathit{Right}\} \tag{3}$$

Relations:

$$\begin{tikzcd}
\mathit{Being} \arrow[r, "\mathit{Eats}"] & \mathit{Being} \arrow[d, "\mathit{where}"'] & \\
& \mathit{Bank} \arrow[r, "\mathit{cross}"] & \mathit{Bank}
\end{tikzcd} \tag{4}$$

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Specification source written in Alloy:

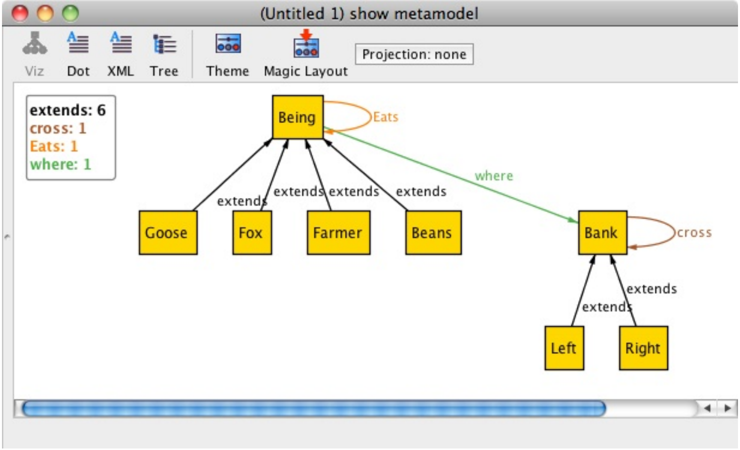


```
abstract sig Being {
    Eats :  Being,
    where : Bank
}

one sig Fox, Goose, Beans, Farmer extends Being {}

abstract sig Bank { cross: Bank }

one sig Left, Right extends Bank {}

-- Checking

run { some Eats && some where }
```

Line 13, Column 12 [modified]

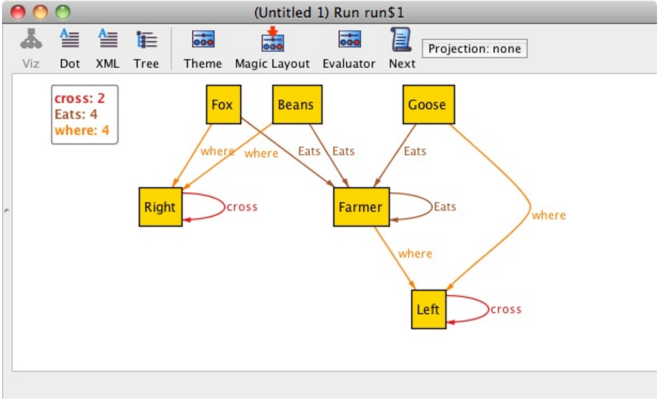
PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Diagram of specification (model) given by Alloy:



PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Diagram of instance of the model given by Alloy:



Silly instance, why? — specification too **loose**...

Composition

Recall **function composition** (aside).

$$\begin{tikzcd} B & A \arrow[l, "f"'] & C \arrow[l, "g"'] \arrow[ll, bend left, "f \cdot g"] \end{tikzcd} \qquad (5)$$

$$b = f(g\ c)$$

We extend $f \cdot g$ to relational composition $R \cdot S$ in the obvious way:

$$b(R \cdot S)c \quad \equiv \quad \langle \exists\ a\ ::\ b\ R\ a\ \wedge\ a\ S\ c \rangle$$

Composition

That is:

$$\begin{tikzcd}
B & A \arrow[l, "R"'] & C \arrow[l, "S"'] \arrow[ll, bend left, "R\cdot S"]
\end{tikzcd}$$

$$b(R \cdot S)c \quad \equiv \quad \langle \exists\ a \ :: \ b\ R\ a \ \wedge \ a\ S\ c \rangle \tag{6}$$

Example: $Uncle = Brother \cdot Parent$, *that expands to*

$$u\ Uncle\ c \quad \equiv \quad \langle \exists\ p \ :: \ u\ Brother\ p \wedge p\ Parent\ c \rangle$$

Note how this rule *removes* $\exists$ when applied from right to left.

Notation $R \cdot S$ is said to be **point-free** (no variables, or points).

Check generalization

Back to functions, (6) becomes[1]

$$
\begin{array}{cl}
& b(f\cdot g)c \\
\equiv & \langle \exists\ a\ ::\ b\ f\ a \wedge a\ g\ c \rangle \\
\equiv & \qquad \{\ a\ g\ c \text{ means } a = g\ c\ (1)\ \} \\
& \langle \exists\ a\ ::\ b\ f\ a \wedge a = g\ c \rangle \\
\equiv & \qquad \{\ \exists\text{-trading (143) ; } b\ f\ a \text{ means } b = f\ a\ (1)\ \} \\
& \langle \exists\ a\ :\ a = g\ c\ :\ b = f\ a \rangle \\
\equiv & \qquad \{\ \exists\text{-one point rule (147)}\ \} \\
& b = f(g\ c)
\end{array}
$$

So, we easily recover what we had before (5).

---

[1] Check the appendix on predicate calculus.

Relation inclusion

Relation inclusion generalizes function equality:

Equality *on functions*

$$f = g \quad \equiv \quad \langle \forall\ a\ ::\ f\ a = g\ a \rangle \tag{7}$$

generalizes to **inclusion** *on relations:*

$$R \subseteq S \quad \equiv \quad \langle \forall\ b, a\ :\ b\ R\ a :\ b\ S\ a \rangle \tag{8}$$

(read $R \subseteq S$ as "R is at most S").

Inclusion is **typed**:

For $R \subseteq S$ to hold both R and S need to be of the same **type**, *say* $B \xleftarrow{R,S} A$.

Relation inclusion

$R \subseteq S$ is a partial order, that is, it is

reflexive,

$$id \ \subseteq \ R \tag{9}$$

transitive

$$R \ \subseteq \ S \wedge S \ \subseteq \ Q \Rightarrow R \ \subseteq \ Q \tag{10}$$

and **antisymmetric**:

$$R \subseteq S \ \wedge \ S \subseteq R \quad \equiv \quad R = S \tag{11}$$

Therefore:

$$R = S \ \equiv \ \langle \forall\ b, a \ :: \ b\ R\ a \ \equiv \ b\ S\ a \rangle \tag{12}$$

Special relations

Every type $B \longleftarrow A$ has its

- **bottom** relation $B \xleftarrow{\perp} A$, which is such that, for all b, a, $b \perp a \equiv \textsc{False}$
- **topmost** relation $B \xleftarrow{\top} A$, which is such that, for all b, a, $b \top a \equiv \textsc{True}$

Every type $A \longleftarrow A$ has the

- **identity** relation $A \xleftarrow{id} A$ which is nothing but function
$$id\ a = a \tag{13}$$

Clearly, for every R,

$$\perp \subseteq R \subseteq \top \tag{14}$$

Relational equality

Both (12) and (11) establish **relation equality**, resp. in PW/PF fashion.

Rule (11) is also called “ping-pong” or **cyclic inclusion**, often taking the format

$$\begin{array}{ll}
 & R \\
\subseteq & \qquad \{ \; .... \; \} \\
 & S \\
\subseteq & \qquad \{ \; .... \; \} \\
 & R \\
:: & \qquad \{ \;\; \text{“ping-pong” (11)} \;\; \} \\
 & R = S
\end{array}$$

Indirect relation equality

Most often we prefer an *indirect* way of proving relation equality:

Indirect equality *rules:*

$$R = S \quad \equiv \quad \langle \forall\ X \ :: \ (X \subseteq R \equiv X \subseteq S) \rangle \tag{15}$$

$$\equiv \quad \langle \forall\ X \ :: \ (R \subseteq X \equiv S \subseteq X) \rangle \tag{16}$$

Compare with eg. equality of sets in discrete maths:

$$A = B \quad \equiv \quad \langle \forall\ a \ :: \ a \in A \ \equiv \ b \in B \rangle$$

Indirect relation equality

$$\text{The typical layout is e.g.} \quad \left\{ \begin{array}{ll} & X \subseteq R \\ \equiv & \qquad \{ \ \dots \ \} \\ & X \subseteq \ldots \\ \equiv & \qquad \{ \ \dots \ \} \\ & X \subseteq S \\ :: & \qquad \{ \ \text{indirect equality (15)} \ \} \\ & R = S \\ \Box & \end{array} \right.$$

Diagrams

Assertions of the form $X \subseteq Y$ where X and Y are relation compositions can be represented graphically by square-shaped diagrams, see the following exercise.

Exercise 1: Let $a \; S \; n$ mean: *"student a is assigned number n"*. Using (6) and (8), check that assertion

$S \cdot \geqslant \; \subseteq \; \top \cdot S$ depicted by diagram

$$\begin{tikzcd}
\mathbb{N} \arrow[d, "s"'] & \mathbb{N} \arrow[l, "\geqslant"'] \arrow[d, "s"] \arrow[dl, phantom, "\subseteq"] \\
A & A \arrow[l, "\top"]
\end{tikzcd}$$

means that numbers are assigned to students sequentially. □

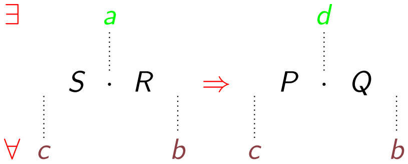
Diagrams ("magic squares")

Pointfree:

$$\begin{tikzcd}
A \arrow[d, "S"'] \arrow[dr, phantom, "\subseteq"] & B \arrow[l, "R"'] \arrow[d, "Q"] \\
C & D \arrow[l, "P"]
\end{tikzcd}$$

$S \cdot R \subseteq P \cdot Q$

Pointwise:



Exercises

Exercise 2: Use (6) and (8) and predicate calculus to show that

$$R \cdot id \;=\; R \;=\; id \cdot R \tag{17}$$

$$R \cdot \bot \;=\; \bot \;=\; \bot \cdot R \tag{18}$$

hold and that composition is associative:

$$R \cdot (S \cdot T) = (R \cdot S) \cdot T \tag{19}$$

□

Exercise 3: Use (7), (8) and predicate calculus to show that

$$f \subseteq g \quad \equiv \quad f = g$$

holds (moral: for functions, inclusion and equality coincide). □

(**NB**: see the appendix for a compact set of rules of the predicate calculus.)

Converses

Every relation $B \xleftarrow{R} A$ has a **converse** $B \xrightarrow{R^\circ} A$ which is such that, for all a, b,

$$a(R^\circ)b \quad \equiv \quad b\ R\ a \tag{20}$$

Note that converse commutes with composition

$$(R \cdot S)^\circ = S^\circ \cdot R^\circ \tag{21}$$

and with itself:

$$(R^\circ)^\circ = R \tag{22}$$

Converse captures the **passive voice**: *Catherine eats the apple* — $R = (eats)$ — is the same as *the apple is eaten by Catherine* — $R^\circ = (is\ eaten\ by)$.

Function converses

Function converses f°, g° etc. always exist (as **relations**) and enjoy the following (very useful!) property,

$$(f\ b)R(g\ a) \quad \equiv \quad b(f^\circ \cdot R \cdot g)a \tag{23}$$

cf. diagram:

$$\begin{tikzcd} C & D \arrow[l, "R"'] \\ B \arrow[u, "f"] & A \arrow[l, "f^\circ \cdot R \cdot g"] \arrow[u, "g"'] \end{tikzcd}$$

Therefore (tell why):

$$b(f^\circ \cdot g)a \quad \equiv \quad f\ b = g\ a \tag{24}$$

Let us see an example of using these rules.

Class 3 — The “Zoo” of Binary Relations

PF-transform at work

Transforming a well-known PW-formula into PF notation:

f is **injective**

$\equiv \quad \{$ recall definition from discrete maths $\}$

$\langle \forall\, y, x \;:\; (f\ y) = (f\ x) :\; y = x \rangle$

$\equiv \quad \{\ (24)$ for $f = g\ \}$

$\langle \forall\, y, x \;:\; y(f^{\circ} \cdot f)x :\; y = x \rangle$

$\equiv \quad \{\ (23)$ for $R = f = g = id\ \}$

$\langle \forall\, y, x \;:\; y(f^{\circ} \cdot f)x :\; y(id)x \rangle$

$\equiv \quad \{$ go pointfree (8) i.e. drop $y, x\ \}$

$f^{\circ} \cdot f \subseteq id$

The other way round

Now check what $id \subseteq f \cdot f^\circ$ means:

$$
\begin{array}{ll}
 & id \subseteq f \cdot f^\circ \\
\equiv & \qquad \{ \text{ relational inclusion (8) } \} \\
 & \langle \forall\ y, x \ :\ y(id)x :\ y(f \cdot f^\circ)x \rangle \\
\equiv & \qquad \{ \text{ identity relation ; composition (6) } \} \\
 & \langle \forall\ y, x \ :\ y = x :\ \langle \exists\ z\ ::\ y\ f\ z \wedge z\ f^\circ x \rangle \rangle \\
\equiv & \qquad \{ \text{ } \forall\text{-one point (146) ; converse (20) } \} \\
 & \langle \forall\ x\ ::\ \langle \exists\ z\ ::\ x\ f\ z \wedge x\ f\ z \rangle \rangle \\
\equiv & \qquad \{ \text{ trivia ; function } f \text{ } \} \\
 & \langle \forall\ x\ ::\ \langle \exists\ z\ ::\ x = f\ z \rangle \rangle \\
\equiv & \qquad \{ \text{ recalling definition from maths } \} \\
 & f \text{ is } \textbf{surjective}
\end{array}
$$

Why *id* (really) matters

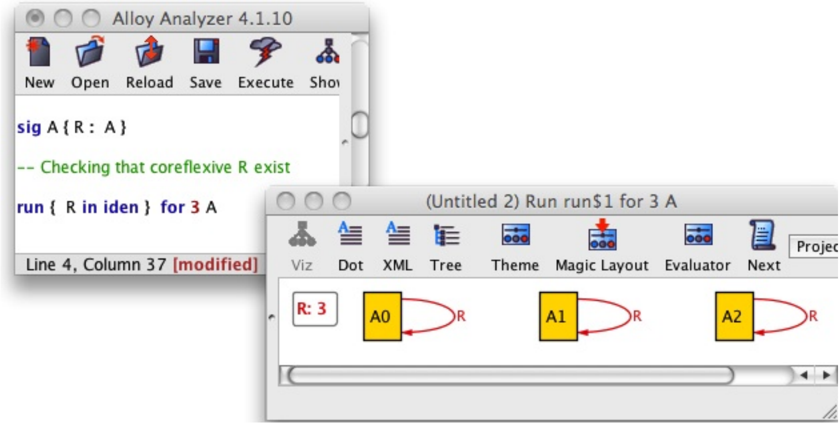
Terminology:

- Say R *is reflexive* iff $id \subseteq R$
  pointwise: $\langle \forall\ a\ ::\ a\ R\ a \rangle$ (check as homework);
- Say R *is coreflexive* (or *diagonal*) iff $R \subseteq id$
  pointwise: $\langle \forall\ b, a\ :\ b\ R\ a :\ b = a \rangle$ (check as homework).

Define, for $B \xleftarrow{R} A$:

Kernel of R	**Image** of R
$A \xleftarrow{\ker R} A$ $\ker R \overset{\mathrm{def}}{=} R^\circ \cdot R$	$B \xleftarrow{\mathrm{img}\ R} B$ $\mathrm{img}\ R \overset{\mathrm{def}}{=} R \cdot R^\circ$

Alloy: checking for coreflexive relations



```
sig A { R : A }

-- Checking that coreflexive R exist

run { R in iden } for 3 A
```

Line 4, Column 37 [modified]

Kernels of functions

Meaning of $\ker f$:

$$\begin{array}{cl} & a'(\ker f)a \\ \equiv & \{\ \text{substitution}\ \} \\ & a'(f^\circ \cdot f)a \\ \equiv & \{\ \text{rule (24)}\ \} \\ & f\ a' = f\ a \end{array}$$

In words: $a'(\ker f)a$ means a' *and* a *"have the same* f*-image"*.

Exercise 4: Let K be a nonempty data domain, $k \in K$ and $\underline{k}$ be the *"everywhere* k*"* function:

$$\begin{array}{rcl} \underline{k} & : & A \longrightarrow K \\ \underline{k}\,a & = & k \end{array} \tag{25}$$

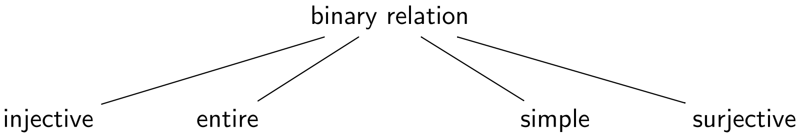
Compute which relations are defined by the following expressions:

$$\ker \underline{k}, \quad \underline{b} \cdot \underline{c}^\circ, \quad \mathrm{img}\ \underline{k} \tag{26}$$

□

Binary relation taxonomy

Topmost criteria:



binary relation

injective entire simple surjective

Definitions:

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

(27)

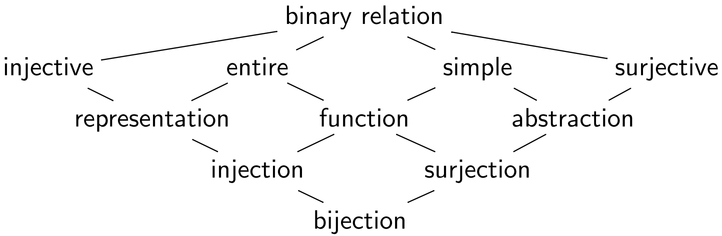
Facts:

$$\ker (R^\circ) = \mathrm{img}\ R \tag{28}$$

$$\mathrm{img}\ (R^\circ) = \ker R \tag{29}$$

Binary relation taxonomy

The whole picture:



binary relation (30)

injective entire simple surjective

representation function abstraction

injection surjection

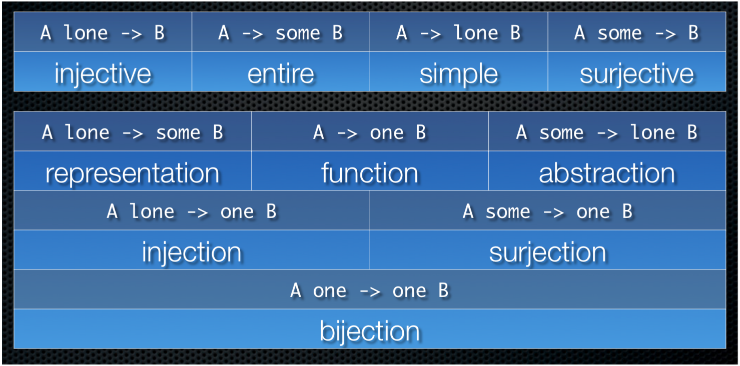
bijection

Exercise 5: Resort to (28,29) and (27) to prove the following rules of thumb:

- converse of **injective** is **simple** (and vice-versa)
- converse of **entire** is **surjective** (and vice-versa)

□

The same in Alloy

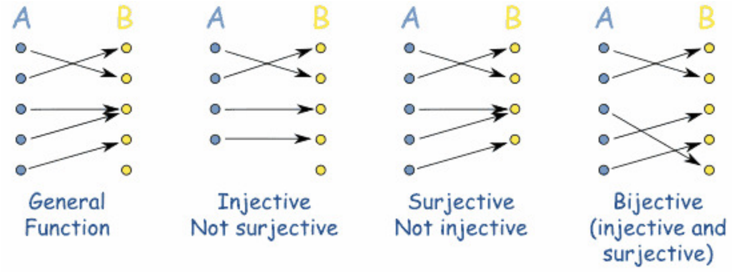


`A lone -> B`	injective
`A -> some B`	entire
`A -> lone B`	simple
`A some -> B`	surjective
`A lone -> some B`	representation
`A -> one B`	function
`A some -> lone B`	abstraction
`A lone -> one B`	injection
`A some -> one B`	surjection
`A one -> one B`	bijection

(Courtesy of Alcino Cunha.)

Exercises

Exercise 6: Label the items (uniquely) in these drawings[2]



and compute, in each case, the **kernel** and the **image** of each relation. Why are all these relations **functions**? □

---

[2] Credits: `http://www.matematikaria.com/unit/injective-surjective-bijective.html`.

Exercises

Exercise 7: Prove the following fact

$$\textit{A relation } f \textit{ is a bijection } \textbf{iff} \textit{ its converse } f^\circ \textit{ is a function} \tag{31}$$

by completing:

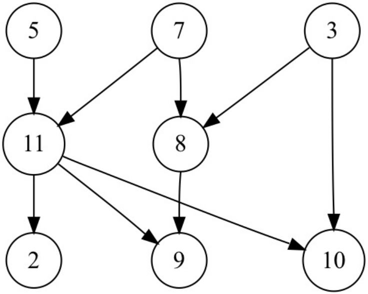
$$\begin{array}{cl}
 & f \text{ and } f^\circ \text{ are functions} \\
\equiv & \qquad \{ \ \dots \ \} \\
 & (id \subseteq \ker f \wedge \mathrm{img}\, f \subseteq id) \wedge (id \subseteq \ker (f^\circ) \wedge \mathrm{img}\, (f^\circ) \subseteq id) \\
\equiv & \qquad \{ \ \dots \ \} \\
 & \vdots \\
\equiv & \qquad \{ \ \dots \ \} \\
 & f \text{ is a bijection}
\end{array}$$

□

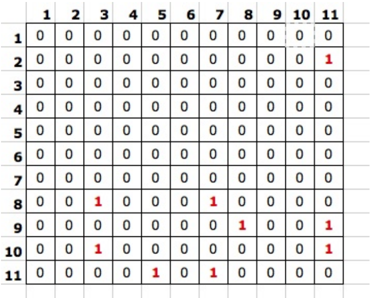
Taxonomy using matrices

Recall that binary relations can be regarded as Boolean **matrices**, eg.

Relation *R*:



Matrix *M*:



	1	2	3	4	5	6	7	8	9	10	11
1	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0
8	0	0	1	0	0	0	1	0	0	0	0
9	0	0	0	0	0	0	0	1	0	0	1
10	0	0	1	0	0	0	0	0	0	0	1
11	0	0	0	0	1	0	1	0	0	0	0

Taxonomy using matrices

- **entire** — at least one 1 in every column (32)
- **surjective** — at least one 1 in every row (33)
- **simple** — at most one 1 in every column (34)
- **injective** — at most one 1 in every row (35)
- **bijective** — exactly one 1 in evey column and every row. (36)

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Exercise 8: Let relation $Bank \xrightarrow{cross} Bank$ (4) be defined by:

$$\begin{array}{rcl} Left & cross & Right \\ Right & cross & Left \end{array}$$

It therefore is a bijection. Why? □

Exercise 9: Check which of the following properties,

simple, *entire*,
injective,
surjective,
reflexive,
coreflexive

Eats	Fox	Goose	Beans	Farmer
Fox	0	1	0	0
Goose	0	0	1	0
Beans	0	0	0	0
Farmer	0	0	0	0

hold for relation *Eats* (4) above ("food chain" $Fox > Goose > Beans$).

□

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Exercise 10: Relation $where : Being \to Bank$ should obey the following constraints:

- *everyone is somewhere in a bank*
- *no one can be in both banks at the same time.*

Express such constraints in relational terms. Conclude that $where$ should be a **function**. ☐

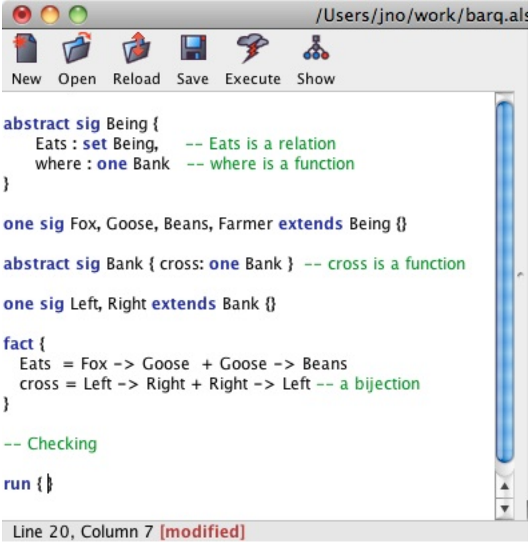
Exercise 11: There are only two **constant** functions (25) in the type $Being \longrightarrow Bank$ of $where$. Identify them and explain their role in the puzzle. ☐

Exercise 12: Two functions f and g are bijections iff $f^\circ = g$, recall (31). Convert $f^\circ = g$ to point-wise notation and check its meaning. ☐

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Adding detail to the previous **Alloy** model (aside)

(More about Alloy syntax and semantics later.)



```
abstract sig Being {
    Eats : set Being,       -- Eats is a relation
    where : one Bank        -- where is a function
}

one sig Fox, Goose, Beans, Farmer extends Being {}

abstract sig Bank { cross: one Bank }  -- cross is a function

one sig Left, Right extends Bank {}

fact {
  Eats  = Fox -> Goose  + Goose -> Beans
  cross = Left -> Right + Right -> Left -- a bijection
}

-- Checking

run {}
```

Line 20, Column 7 [modified]

Functions in one slide

Recapitulating: a **function** f is a binary relation such that

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

NB: Following a widespread convention, functions will be denoted by lowercase characters (eg. f, g, ϕ) or identifiers starting with lowercase characters, and function application will be denoted by juxtaposition, eg. $f\ a$ instead of $f(a)$.

Functions, relationally

(The following properties of any function f are **extremely** useful.)

Shunting rules:

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \tag{37}$$

$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{38}$$

Equality rule:

$$f \subseteq g \quad \equiv \quad f = g \quad \equiv \quad f \supseteq g \tag{39}$$

Rule (39) follows from (37,38) by “cyclic inclusion” (next slide).

Proof of functional equality rule (39)

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

Then:

$$
\begin{array}{ll}
 & f = g \\
\equiv & \qquad \{ \text{ cyclic inclusion (11) } \} \\
 & f \subseteq g \wedge g \subseteq f \\
\equiv & \qquad \{ \text{ aside } \} \\
 & f \subseteq g \\
\equiv & \qquad \{ \text{ aside } \} \\
 & g \subseteq f \\
\Box &
\end{array}
$$

Dividing functions

$$\frac{f}{g} = g^{\circ} \cdot f \qquad cf. \quad \begin{tikzcd} B \arrow[dr, "g"'] & & A \arrow[ll, "\frac{f}{g}"'] \arrow[dl, "f"] \\ & C & \end{tikzcd} \tag{40}$$

Exercise 13: Check the properties:

$$\frac{f}{id} = f \tag{41}$$

$$\frac{f \cdot h}{g \cdot k} = k^{\circ} \cdot \frac{f}{g} \cdot h \tag{42}$$

$$\frac{f}{f} = \ker f \tag{43}$$

$$\left(\frac{f}{g}\right)^{\circ} = \frac{g}{f} \tag{44}$$

□

Exercise 14: Infer $id \subseteq \ker f$ (f is total) and $\mathrm{img}\ f \subseteq id$ (f is simple) from the shunting rules (37) or (38). □

Dividing functions

By (23) we have:

$$b \,\frac{f}{g}\, a \quad \equiv \quad g\ b = f\ a \tag{45}$$

How useful is this? Think of the following sentence:

Mary lives where John was born.

By (45), this can be expressed by a division:

$$Mary\ \frac{birthplace}{residence}\ John \ \equiv\ residence\ Mary = birthplace\ John$$

In general,

$b\,\frac{f}{g}\,a$ *means "the* g *of* b *is the* f *of* a*".*

Endo-relations

A relation $A \xrightarrow{R} A$ whose input and output types coincide is called an

---

endo-relation.

This special case of relation is gifted with an extra **taxonomy** and many **applications**.

We have already seen them: $\ker R$ and $\mathrm{img}\ R$ are **endo-relations**.

Graphs, orders, the identity, equivalences and so on are all **endo-relations** as well.

Taxonomy of endo-relations

Besides

reflexive: iff $id \subseteq R$ (46)

coreflexive: iff $R \subseteq id$ (47)

an endo-relation $A \xleftarrow{R} A$ can be

transitive: iff $R \cdot R \subseteq R$ (48)

symmetric: iff $R \subseteq R^\circ (\equiv R = R^\circ)$ (49)

anti-symmetric: iff $R \cap R^\circ \subseteq id$ (50)

irreflexive: iff $R \cap id = \bot$

connected: iff $R \cup R^\circ = \top$ (51)

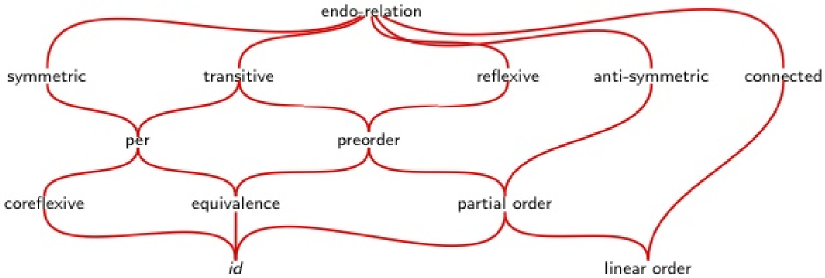
where, in general, for R, S of the same type:

$$b\ (R \cap S)\ a \quad \equiv \quad b\ R\ a \wedge b\ S\ a \tag{52}$$

$$b\ (R \cup S)\ a \quad \equiv \quad b\ R\ a \vee b\ S\ a \tag{53}$$

Taxonomy of endo-relations

Combining these criteria, endo-relations $A \xleftarrow{R} A$ can further be classified as



Taxonomy of endo-relations

In summary:

- **Preorders** are reflexive and transitive orders.
  Example: $\mathit{age}\ y \leqslant \mathit{age}\ x$.
- **Partial** orders are anti-symmetric preorders
  Example: $y \subseteq x$ where x and y are sets.
- **Linear** orders are connected partial orders
  Example: $y \leqslant x$ in $\mathbb{N}$
- **Equivalences** are symmetric preorders
  Example: $\mathit{age}\ y = \mathit{age}\ x$. [3]
- **Pers** are partial equivalences
  Example: $y\ \mathit{IsBrotherOf}\ x$.

---

[3] Kernels of functions are always equivalence relations, see exercise 21.

Exercises

Exercise 15: Consider the relation

$$b \; R \; a \;\equiv\; \textit{team } b \textit{ is playing against team } a \textit{ at the moment}$$

Is this relation: reflexive? irreflexive? transitive? anti-symmetric? symmetric? connected? □

Exercise 16: Check which of the following properties,

transitive, symmetric, anti-symmetric, connected

hold for the relation *Eats* of exercise 9. □

Exercises

Exercise 17: A relation R is said to be **co-transitive** or **dense** iff the following holds:

$$\langle \forall\ b, a\ :\ b\ R\ a :\ \langle \exists\ c\ :\ b\ R\ c :\ c\ R\ a \rangle \rangle \tag{54}$$

Write the formula above in PF notation. Find a relation (eg. over numbers) which is co-transitive and another which is not. □

Exercise 18: Expand criteria (48) to (51) to pointwise notation. □

Exercises

Exercise 19: The teams (T) of a football league play games (G) at home or away, and every game takes place in some date:

$$\begin{tikzcd}
T & G \arrow[l, "home"'] \arrow[r, "away"] \arrow[d, "date"'] & T \\
 & D &
\end{tikzcd}$$

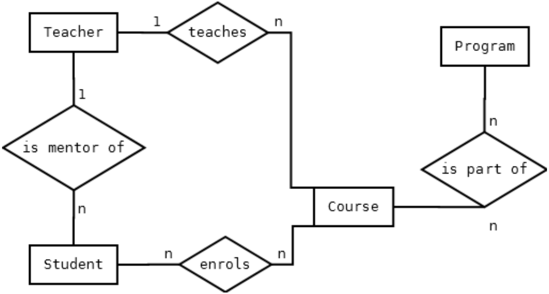
Moreover, *(a) No team can play two games on the same date; (b) All teams play against each other but not against themselves; (c) For each home game there is another game away involving the same two teams.* Show that

$$id \subseteq \frac{away}{home} \cdot \frac{away}{home} \tag{55}$$

captures one of the requirements above (which?) and that (55) amounts to forcing $home \cdot away^\circ$ to be symmetric. □

Formalizing ER diagrams

So-called "**Entity-Relationship**" (ER) diagrams are commonly used to capture relational information, e.g.[4]



ER-diagrams can be **formalized** in $A \xrightarrow{R} B$ notation, see e.g. the following relational algebra (RA) diagram.

---

[4] Credits: `https://dba.stackexchange.com/questions`.

Exercise

$$\begin{tikzcd}
\mathit{Teacher} & \mathit{Program} \arrow[d, "\mathit{IsPartOf}"] \\
\mathit{Student} \arrow[u, "\mathit{isMentorOf}"] & \mathit{Course} \arrow[l, "\mathit{Enrols}"'] \arrow[ul, "\mathit{teaches}"']
\end{tikzcd} \tag{56}$$

Exercise 20: Looking at diagram (56),

- Specify the property: *mentors of students necessarily are among their teachers.*
- Specify the relation R between students and teachers such that $t\ R\ s$ means: t *is the mentor of* s *and also teaches one of her/his courses.*

☐

Class 4 — Meet and Join

Meet and join

Recall **meet** (intersection) and **join** (union), introduced by (52) and (53), respectively.

They lift pointwise conjunction and disjunction, respectively, to the pointfree level.

Their meaning is nicely captured by the following **universal** properties:

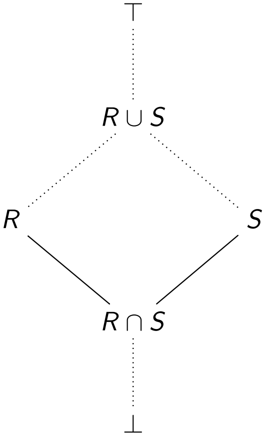
$$X \subseteq R \cap S \equiv X \subseteq R \wedge X \subseteq S \quad (57)$$

$$R \cup S \subseteq X \equiv R \subseteq X \wedge S \subseteq X \quad (58)$$

NB: recall the generic notions of **greatest lower bound** and **least upper bound**, respectively.

In summary

Type $B \longleftarrow A$ forms a lattice:



“top”

join, lub (“least upper bound”)

meet, glb (“greatest lower bound”)

“bottom”

How universal properties help

Using (57) i.e.

$$X \subseteq R \cap S \equiv \left\{ \begin{array}{lcl} X & \subseteq & R \\ X & \subseteq & S \end{array} \right.$$

as example, similarly for (58).

Cancellation

$(X := R \cap S)$:

$$\left\{ \begin{array}{lcl} R \cap S & \subseteq & R \\ R \cap S & \subseteq & S \end{array} \right. \quad (59)$$

$R \cap \top = R$ why? Use indirect equality

$$\begin{array}{ll} & X \subseteq R \cap \top \\ \equiv & \quad \{ \text{ universal property } \} \\ & \left\{ \begin{array}{lcl} X & \subseteq & R \\ X & \subseteq & \top \end{array} \right. \\ \equiv & \quad \{ \ \top \text{ is above anything } \} \\ & X \subseteq R \\ :: & \quad \{ \text{ indirect equality } \} \\ & R \cap \top = R \end{array}$$

How universal properties help

Meet and join have other expected properties, e.g. **associativity**

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

again proved aside by indirect equality.

$$
\begin{array}{cl}
 & X \subseteq (R \cap S) \cap Q \\
\equiv & \qquad \{ \text{ $\cap$-universal (57) twice } \} \\
 & (X \subseteq R \wedge X \subseteq S) \wedge X \subseteq Q \\
\equiv & \qquad \{ \text{ $\wedge$ is associative } \} \\
 & X \subseteq R \wedge (X \subseteq S \wedge X \subseteq Q) \\
\equiv & \qquad \{ \text{ $\cap$-universal (57) twice } \} \\
 & X \subseteq R \cap (S \cap Q) \\
:: & \qquad \{ \text{ indirection (15) } \} \\
 & (R \cap S) \cap Q = R \cap (S \cap Q) \\
\square &
\end{array}
$$

Distributivity

As we will prove later, **composition** distributes over **union**

$$R \cdot (S \cup Q) = (R \cdot S) \cup (R \cdot Q) \tag{60}$$

$$(S \cup Q) \cdot R = (S \cdot R) \cup (Q \cdot R) \tag{61}$$

while distributivity over **intersection** is side-conditioned:

$$(S \cap Q) \cdot R = (S \cdot R) \cap (Q \cdot R) \quad \Leftarrow \quad \left\{ \begin{array}{c} Q \cdot \mathrm{img}\ R \subseteq Q \\ \vee \\ S \cdot \mathrm{img}\ R \subseteq S \end{array} \right. \tag{62}$$

$$R \cdot (Q \cap S) = (R \cdot Q) \cap (R \cdot S) \quad \Leftarrow \quad \left\{ \begin{array}{c} (\ker R) \cdot Q \subseteq Q \\ \vee \\ (\ker R) \cdot S \subseteq S \end{array} \right. \tag{63}$$

Propositio de homine et capra et lvpo

Back to our running example, we specify:

Being at the same bank:

$$\mathit{SameBank} = \ker \mathit{where} = \frac{\mathit{where}}{\mathit{where}}$$

Risk of somebody eating somebody else:

$$\mathit{CanEat} = \mathit{SameBank} \cap \mathit{Eats}$$

Then

"Starvation" is ensured by Farmer *present at the same bank:*

$$\mathit{CanEat} \subseteq \mathit{SameBank} \cdot \underline{\mathit{Farmer}} \tag{64}$$

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

By (37), “starvation” property (64) converts to:

$$\mathit{where} \cdot \mathit{CanEat} \quad \subseteq \quad \mathit{where} \cdot \underline{\mathit{Farmer}}$$

In this version, (64) can be depicted as a ‘magic square’:

$$\begin{tikzcd}
\mathit{Being} \arrow[d, "\mathit{where}"'] & & \mathit{Being} \arrow[ll, "\mathit{CanEat}"'] \arrow[d, "\underline{\mathit{Farmer}}"] \arrow[dll, phantom, "\subseteq"] \\
\mathit{Bank} & & \mathit{Being} \arrow[ll, "\mathit{where}"]
\end{tikzcd} \qquad (65)$$

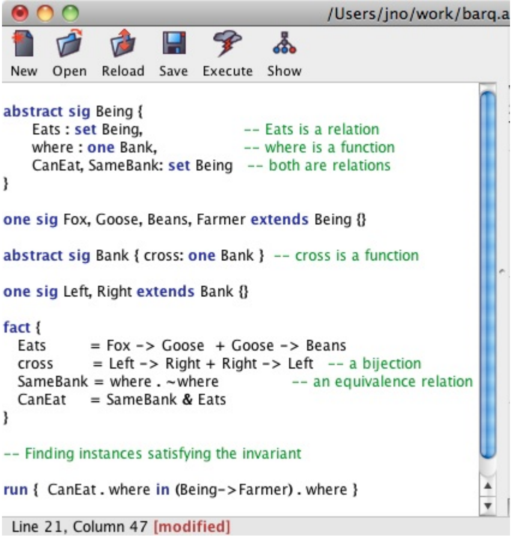
This “reads” in a nice way:

where (somebody) *CanEat* (somebody else) (that’s)
where (the) *Farmer* (is).

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Properties which — such as (65) — are desirable and must **always hold** are called **invariants**.

See aside the ‘starvation’ invariant (65) written in **Alloy**.



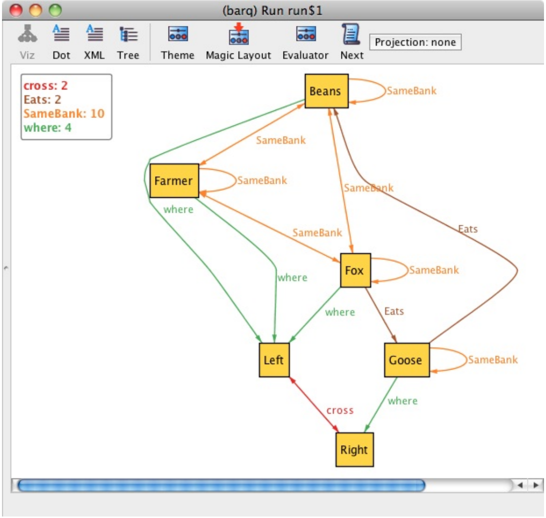
```
abstract sig Being {
    Eats : set Being,                 -- Eats is a relation
    where : one Bank,                 -- where is a function
    CanEat, SameBank: set Being       -- both are relations
}

one sig Fox, Goose, Beans, Farmer extends Being {}

abstract sig Bank { cross: one Bank }  -- cross is a function

one sig Left, Right extends Bank {}

fact {
  Eats       = Fox -> Goose  + Goose -> Beans
  cross      = Left -> Right + Right -> Left   -- a bijection
  SameBank = where . ~where                 -- an equivalence relation
  CanEat     = SameBank & Eats
}

-- Finding instances satisfying the invariant

run {  CanEat . where in (Being->Farmer) . where }
```

Line 21, Column 47 [modified]

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Carefully observe instance of such an invariant (aside):

- *SameBank* is an **equivalence** — exactly the **kernel** of *where*
- *Eats* is simple but not transitive
- *cross* is a **bijection**
- *CanEat* is empty
- etc



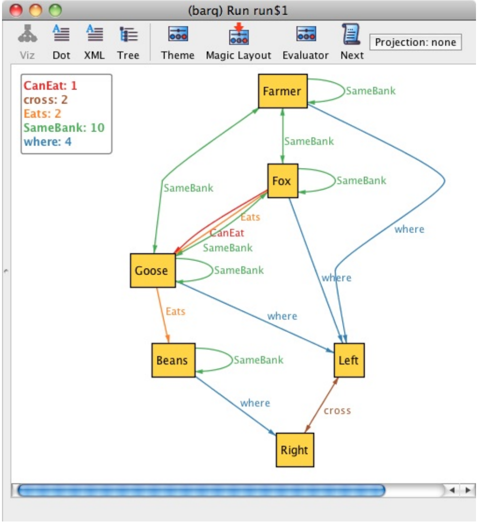
(barq) Run run$1

cross: 2
Eats: 2
SameBank: 10
where: 4

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Another instance of the same invariant, in which:

- *CanEat* is **not** empty (*Fox* can eat *Goose*!)
- but *Farmer* is on the same bank :-)



CanEat: 1
cross: 2
Eats: 2
SameBank: 10
where: 4

Why is *SameBank* an equivalence?

Recall that $SameBank = \ker\ where$. Then *SameBank* is an **equivalence relation** by the exercise below.

Exercise 21: Knowing that property

$$f \cdot f^{\circ} \cdot f = f \tag{66}$$

holds for every function f, prove that $\ker f = \frac{f}{f}$ (43) is an **equivalence** relation. ☐

Equivalence relations expressed in this way are captured in natural language by the textual pattern

---

$a(\ker\ f)b$ *means* *"a and b have the same f"*

---

which is very common in requirements.

Class 5a – Exploring “magic squares”

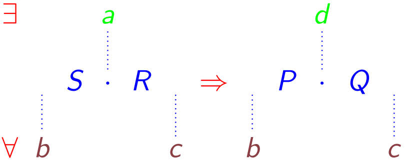
‘Magic square’ patterns

Recall

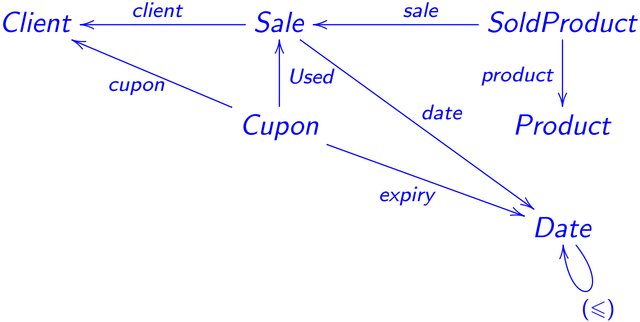
$$\begin{tikzcd}
A \arrow[d, "S"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q"] \\
B & D \arrow[l, "P"]
\end{tikzcd}$$

$$S \cdot R \subseteq P \cdot Q$$

… i.e. the pointwise:



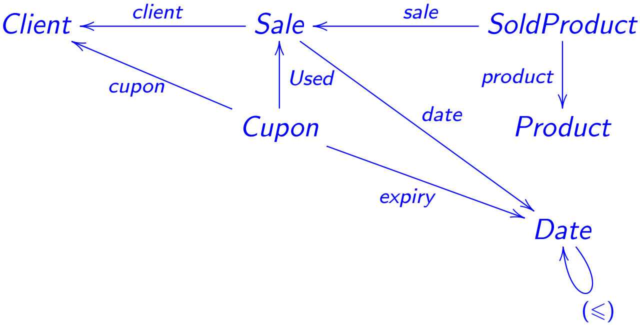
"D. Acácia grocery"



Find "magic square" for property:

Coupons cannot be used beyond their expiry date.

“D. Acácia grocery”



Find “magic square” for property:

Coupons can only be used by clients who own them.

‘Magic square’ patterns

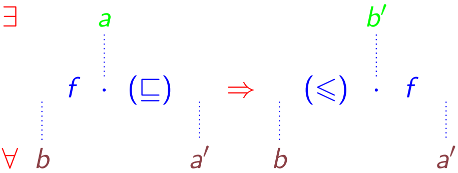
Now consider the special case

$$\begin{tikzcd}
A \arrow[d, "f"'] & A \arrow[l, "(\sqsubseteq)"'] \arrow[d, "f"] \arrow[dl, phantom, "\subseteq"] \\
B & B \arrow[l, "(\leqslant)"]
\end{tikzcd}
\qquad\qquad
f \cdot (\sqsubseteq) \subseteq (\leqslant) \cdot f$$

where $(\sqsubseteq)$ and $(\leqslant)$ are preorders.

‘Magic square’ patterns

Do we need…



$$f \cdot (\sqsubseteq) \Rightarrow (\leqslant) \cdot f$$

as before?

'Magic square' patterns

No — for **functions** things are much easier:

$$\begin{array}{cl}
 & f \cdot (\sqsubseteq) \ \subseteq \ (\leqslant) \cdot f \\
\equiv & \qquad \{ \ (37) \ \} \\
 & (\sqsubseteq) \ \subseteq \ f^\circ \cdot (\leqslant) \cdot f \\
\equiv & \qquad \{ \ (23) \ \} \\
 & \langle \forall \ a, a' \ : \ a \sqsubseteq a' : \ f \ a \leqslant f \ a' \rangle
\end{array}$$

In summary,

$$f \cdot (\sqsubseteq) \ \subseteq \ (\leqslant) \cdot f \qquad (67)$$

states that f is a **monotonic** function.

‘Magic square’ patterns

Now consider yet another special case:

$$\begin{tikzcd}
A \arrow[d, "f"'] \arrow[dr, phantom, "\subseteq"] & A \arrow[l, "id"'] \arrow[d, "g"] \\
B & B \arrow[l, "(\leqslant)"]
\end{tikzcd}$$

$$f \subseteq (\leqslant) \cdot g$$

Likewise, $f \subseteq (\leqslant) \cdot g$ will unfold to

$$\langle \forall\ a\ ::\ f\ a \leqslant g\ a \rangle$$

meaning that

> f *is* **pointwise-smaller** *than* g *wrt.* $(\leqslant)$.

‘Magic square’ patterns

Now consider yet another special case:

$$\begin{tikzcd}
A \arrow[d, "f"'] & A \arrow[l, "id"'] \arrow[d, "g"] \arrow[dl, phantom, "\subseteq"] \\
B & B \arrow[l, "(\leqslant)"]
\end{tikzcd}$$

$$f \subseteq (\leqslant) \cdot g$$

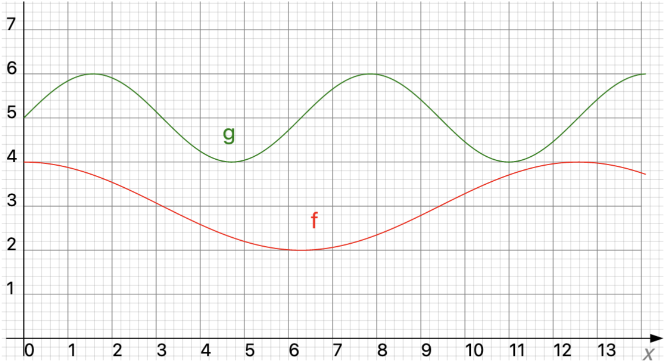
Likewise, $f \subseteq (\leqslant) \cdot g$ will unfold to

$$\langle \forall\ a\ ::\ f\ a \leqslant g\ a \rangle$$

meaning that

f *is* **pointwise-smaller** *than* g *wrt.* $(\leqslant)$.

$f \overset{.}{\leqslant} g$



Usual abbreviation: $f \overset{.}{\leqslant} g \equiv f \subseteq (\leqslant) \cdot g$.

Relational patterns: the pre-order $f^\circ \cdot (\leqslant) \cdot f$

Given a **preorder** $(\leqslant)$, a function f function taking values on the carrier set of $(\leqslant)$, define

$$(\leqslant_f) = f^\circ \cdot (\leqslant) \cdot f$$

It is easy to show that:

$$b \ \leqslant_f \ a \ \equiv \ (f \ b) \leqslant (f \ a)$$

That is, we compare **objects** a and b with respect to their **attribute** f.

Exercise 22:

1. Show that $(\leqslant_f)$ is a **preorder.**
2. Show that $(\leqslant_f)$ is not (in general) a total order even in the case $(\leqslant)$ is so.

□

Exercises

Exercise 23: As generalization of exercise 1, draw the most general "magic square" that accommodates relational assertion:

$$M \cdot R^\circ \subseteq \top \cdot M \tag{68}$$

$\square$

Exercise 24: Type the following relational assertions

$$M \cdot N^\circ \subseteq \bot \tag{69}$$

$$M \cdot N^\circ \subseteq id \tag{70}$$

$$M^\circ \cdot \top \cdot N \subseteq > \tag{71}$$

and check their pointwise meaning. Confirm your intuitions by repeating this exercise in Alloy. $\square$

Exercises

Exercise 25: Let $bag : A^* \to \mathbb{N}^A$ be the function that, given a finite sequence (list) indicates the number of occurrences of its elements, for instance,

$$\begin{array}{l} bag\ [a, b, a, c]\ a = 2 \\ bag\ [a, b, a, c]\ b = 1 \\ bag\ [a, b, a, c]\ c = 1 \end{array}$$

Let $ordered : A^* \to \mathbb{B}$ be the obvious predicate assuming a **total** order predefined in A. Finally, let $true = \underline{\mathrm{True}}$. Having defined

$$S = \frac{bag}{bag} \cap \frac{true}{ordered} \tag{72}$$

identify the type of S and, going pointwise and simplifying, tell which operation is specified by S. ☐

Exercises

Exercise 26: Prove the **union simplicity** rule:

$$M \cup N \text{ is simple} \quad \equiv \quad M,\ N \text{ are simple and } M \cdot N^{\circ} \subseteq id \tag{73}$$

$\square$

Exercise 27: Derive from (73) the corresponding rule for **injective** relations. $\square$

Exercise 28: Explain in your own words the following equalities:

$$1 \xleftarrow{\top} 1 \;=\; 1 \xleftarrow{!} 1 \;=\; id \tag{74}$$

$\square$

Class 5b – Monotone reasoning

Monotonicity

All relational combinators studied so far are $\subseteq$-**monotonic**, namely:

$$R \subseteq S \quad \Rightarrow \quad R^\circ \subseteq S^\circ \tag{75}$$

$$R \subseteq S \wedge U \subseteq V \quad \Rightarrow \quad R \cdot U \subseteq S \cdot V \tag{76}$$

$$R \subseteq S \wedge U \subseteq V \quad \Rightarrow \quad R \cap U \subseteq S \cap V \tag{77}$$

$$R \subseteq S \wedge U \subseteq V \quad \Rightarrow \quad R \cup U \subseteq S \cup V \tag{78}$$

etc hold.

Transitivity, recall:

$$R \ \subseteq \ S \wedge S \ \subseteq \ Q \Rightarrow R \ \subseteq \ Q$$

Proofs by $\subseteq$-transitivity

Wishing to prove $R \subseteq S$, the following rules are of help by relying on a "mid-point" M (analogy with interval arithmetics):

- Rule A: **lowering the upper side**

$$\begin{array}{ll} & R \subseteq S \\ \Leftarrow & \quad \{ \ M \subseteq S \text{ is known ; transitivity of } \subseteq (10) \ \} \\ & R \subseteq M \end{array}$$

  and then proceed with $R \subseteq M$.

Proofs by $\subseteq$-transitivity

- Rule B: **raising the lower side**

$$\begin{array}{ll} & R \subseteq S \\ \Leftarrow & \{ \ R \subseteq M \text{ is known; transitivity of } \subseteq \ \} \\ & M \subseteq S \end{array}$$

  and then proceed with $M \subseteq S$.

Example

Composition of simple $A \xrightarrow{S} B$ and $B \xrightarrow{R} C$ is simple:

$$
\begin{array}{ll}
& \mathrm{img}\,(R \cdot S) \subseteq id \\
\equiv & \qquad \{\ \} \\
& R \cdot S \cdot S^\circ \cdot R^\circ \subseteq id \\
\Leftarrow & \qquad \{\ S \text{ is simple, } S \cdot S^\circ \subseteq id\text{; rule B }\} \\
& R \cdot R^\circ \subseteq id \\
\Leftarrow & \qquad \{\ R \text{ is simple, } R \cdot R^\circ \subseteq id\text{; rule B }\} \\
& id \subseteq id \\
\equiv & \qquad \{\ R \subseteq R \text{ always holds }\} \\
& true
\end{array}
$$

Example

Proof of shunting rule (37):

$$
\begin{array}{ll}
 & R \subseteq f^{\circ} \cdot S \\
\Leftarrow & \qquad \{ \; id \subseteq f^{\circ} \cdot f \text{ ; raising the lower-side } \} \\
 & f^{\circ} \cdot f \cdot R \subseteq f^{\circ} \cdot S \\
\Leftarrow & \qquad \{ \text{ monotonicity of } (f^{\circ} \cdot) \; \} \\
 & f \cdot R \subseteq S \\
\Leftarrow & \qquad \{ \; f \cdot f^{\circ} \subseteq id \text{ ; lowering the upper-side } \} \\
 & f \cdot R \subseteq f \cdot f^{\circ} \cdot S \\
\Leftarrow & \qquad \{ \text{ monotonicity of } (f \cdot) \; \} \\
 & R \subseteq f^{\circ} \cdot S
\end{array}
$$

Thus the equivalence in (37) is established by circular implication.

Exercises (monotonicity and transitivity)

Exercise 29: Prove the following rules of thumb:

- **smaller** than injective (simple) is injective (simple)
- **larger** than entire (surjective) is entire (surjective)
- $R \cap S$ is injective (simple) provided one of R or S is so
- $R \cup S$ is entire (surjective) provided one of R or S is so.

□

Exercise 30: Prove that relational **composition** preserves **all** relational classes in the taxonomy of (30). □

Meaning of $f \cdot r = id$

On the one hand,

$$
\begin{array}{ll}
 & f \cdot r = id \\
\equiv & \qquad \{ \text{ equality of functions } \} \\
 & f \cdot r \subseteq id \\
\equiv & \qquad \{ \text{ shunting } \} \\
 & r \subseteq f^{\circ}
\end{array}
$$

Since f is simple:

- f° is injective
- and so is r, because “smaller than injective is injective”.

Meaning of $f \cdot r = id$

On the other hand,

$$
\begin{array}{ll}
 & f \cdot r = id \\
\equiv & \quad \{ \text{ equality of functions } \} \\
 & id \subseteq f \cdot r \\
\equiv & \quad \{ \text{ shunting } \} \\
 & r^\circ \subseteq f
\end{array}
$$

Since r is entire:

- r° is surjective
- and so is f because “larger that surjective is surjective”.

Meaning of $f \cdot r = id$

We conclude that

f is **surjective** *and r is* **injective** *wherever $f \cdot r = id$ holds.*

Since both are functions, we furthermore conclude that

f is an **abstraction** *and r is a* **representation**

Exercise 31: Why are π_1 and π_2 **surjective** and i_1 and i_2 **injective**? Why are isomorphisms **bijections**? $\square$

Converse magic squares

$$\begin{tikzcd} A \arrow[d, "P"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q"] \\ B & D \arrow[l, "S"] \end{tikzcd} \equiv \begin{tikzcd} A \arrow[d, "R^\circ"'] \arrow[dr, phantom, "\subseteq"] & B \arrow[l, "P^\circ"'] \arrow[d, "S^\circ"] \\ C & D \arrow[l, "Q^\circ"] \end{tikzcd} \qquad (79)$$

Magic square compositionality

Magic squares compose, not only **horizontally**

$$\begin{tikzcd}
A \arrow[d, "P"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q"] \arrow[dr, phantom, "\subseteq"] & C' \arrow[l, "R'"'] \arrow[d, "Q'"] & \Rightarrow & A \arrow[d, "P"'] \arrow[dr, phantom, "\subseteq"] & C' \arrow[l, "R \cdot R'"'] \arrow[d, "Q'"] \\
B & D \arrow[l, "S"] & D' \arrow[l, "S'"] & & B' & D' \arrow[l, "S \cdot S'"]
\end{tikzcd} \tag{80}$$

Magic square compositionality

... but also **vertically**:

$$\begin{tikzcd}
A \arrow[d, "P"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q"] \\
B \arrow[d, "P'"'] \arrow[dr, phantom, "\subseteq"] & D \arrow[l, "S"] \arrow[d, "Q'"] \\
B' & D' \arrow[l, "S'"]
\end{tikzcd}
\quad \Rightarrow \quad
\begin{tikzcd}
A \arrow[d, "P' \cdot P"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q' \cdot Q"] \\
B' & D' \arrow[l, "S'"]
\end{tikzcd}
\tag{81}$$

Exercise 32: Prove (80) and (81). □

Exercise 33: Use (81) to prove that the compostion of monotonic functions is a monotonic function. □

Class 6 — Pairs and sums

Relational pairing

Recall:

$$\begin{tikzcd} A & A \times B \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & B \\ & C \arrow[ul, "f"] \arrow[u, "\langle f,g\rangle"] \arrow[ur, "g"'] & \end{tikzcd}$$

$$\langle f,g\rangle\, c = (f\ c, g\ c) \tag{82}$$

Clearly:

$$(a,b) = \langle f,g\rangle\ c$$

$$\equiv \qquad \{\ \langle f,g\rangle\ c = (f\ c, g\ c)\ (82)\ ;\ \text{equality of pairs}\ \}$$

$$\left\{ \begin{array}{l} a = f\ c \\ b = g\ c \end{array} \right.$$

$$\equiv \qquad \{\ y = f\ x\ \equiv\ y\, f\, x\ \}$$

$$\left\{ \begin{array}{l} a\ f\ c \\ b\ g\ c \end{array} \right.$$

Relational pairing

That is:

$$(a,b)\ \langle f,g\rangle\ c \;\equiv\; a\ f\ c \wedge b\ g\ c$$

This suggests the generalization

$$(a,b)\ \langle R,S\rangle\ c \;\equiv\; a\ R\ c \wedge b\ S\ c \tag{83}$$

from which one immediately derives the ('Kronecker') **product**:

$$R \times S = \langle R \cdot \pi_1, S \cdot \pi_2\rangle \tag{84}$$

(84) unfolds to the pointwise:

$$(b,d)(R \times S)(a,c) \quad \equiv \quad b\ R\ a \wedge d\ S\ c \tag{85}$$

Relational pairing example (in matrix layout)

Example — given relations

$$where^\circ = \begin{array}{r|cc} & Left & Right \\ \hline Fox & 1 & 0 \\ Goose & 0 & 1 \\ Beans & 0 & 1 \end{array} \quad and \quad cross = \begin{array}{r|cc} & Left & Right \\ \hline Left & 0 & 1 \\ Right & 1 & 0 \end{array}$$

pairing them up evaluates to:

$$\langle where^\circ, cross \rangle = \begin{array}{r|cc} & Left & Right \\ \hline (Fox, Left) & 0 & 0 \\ (Fox, Right) & 1 & 0 \\ (Goose, Left) & 0 & 1 \\ (Goose, Right) & 0 & 0 \\ (Beans, Left) & 0 & 1 \\ (Beans, Right) & 0 & 0 \end{array}$$

Exercises

Exercise 34: Show that

$$(b,c)\langle R,S\rangle a \quad\equiv\quad b\ R\ a \wedge c\ S\ a$$

PF-transforms to:

$$\langle R,S\rangle \;=\; \pi_1^\circ \cdot R \cap \pi_2^\circ \cdot S \tag{86}$$

Then infer universal property

$$X \subseteq \langle R,S\rangle \quad\equiv\quad \pi_1 \cdot X \subseteq R \;\wedge\; \pi_2 \cdot X \subseteq S \tag{87}$$

from (86) via indirect equality (15). □

Exercise 35: What can you say about (87) in case X, R and S are functions? □

Exercises

Exercise 36: Unconditional distribution laws

$$\begin{array}{rcl}(P \cap Q) \cdot S & = & (P \cdot S) \cap (Q \cdot S) \\ R \cdot (P \cap Q) & = & (R \cdot P) \cap (R \cdot Q)\end{array}$$

will hold provide one of R or S is simple and the other injective. Tell which (justifying). $\square$

Exercise 37: Derive from

$$\langle R, S \rangle^\circ \cdot \langle X, Y \rangle \quad = \quad (R^\circ \cdot X) \cap (S^\circ \cdot Y) \tag{88}$$

the following properties:

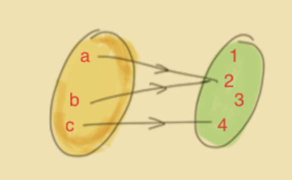
$\square$
$$\ker \langle R, S \rangle \; = \; \ker R \cap \ker S \tag{89}$$

Injectivity preorder

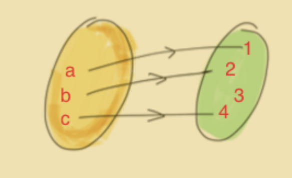
$\ker R = R^\circ \cdot R$ *measures* the level of **injectivity** of R according to the preorder $(\leqslant)$ defined by

$$R \leqslant S \quad \equiv \quad \ker S \subseteq \ker R \tag{90}$$

telling that R is *less injective* or *more defined* (entire) than S — for instance:



$\leqslant$



Injectivity preorder

Restricted to *functions*, $(\leqslant)$ is *universally* bounded by

$$! \leqslant f \leqslant id$$

Also easy to show:

$$id \leqslant f \quad \equiv \quad f \text{ is injective} \tag{91}$$

Exercise 38: Let f and g be the two functions depicted on the right.

Check the assertions:

1. $f \leqslant g$
2. $g \leqslant f$
3. Both hold
4. None holds.

$$\begin{tikzcd}
C & W \arrow[l, "f"'] \arrow[r, "g"] & \mathbb{N}_0 \\
& \texttt{"Armstrong"} \arrow[dl, mapsto] \arrow[r, mapsto] & 9 \\
\texttt{'A'} & \texttt{"Albert"} \arrow[l, mapsto] \arrow[r, mapsto] & 6 \\
\texttt{'M'} & \texttt{"Minho"} \arrow[l, mapsto] \arrow[r, mapsto] & 5 \\
\texttt{'B'} & \texttt{"Braga"} \arrow[l, mapsto] \arrow[ur, mapsto] &
\end{tikzcd}$$

□

The specification pattern $h \leqslant \langle f, g \rangle$

As illustration of the use of this ordering in **formal specification**, suppose one writes

$$room \leqslant \langle lect, slot \rangle$$

in the context of the data model

$$\begin{tikzcd}
Teacher & Class \arrow[l, "lect"'] \arrow[r, "room"] \arrow[d, "slot"'] & Room \\
& TD &
\end{tikzcd}$$

where TD abbreviates time and date.

The specification pattern $h \leqslant \langle f, g \rangle$

What are we telling about this model by writing

$$room \leqslant \langle lect, slot \rangle\,?$$

Unfolding it:

$$\begin{array}{cl} & room \leqslant \langle lect, slot \rangle \\ \equiv & \quad \{\ (90)\ \} \\ & \ker \langle lect, slot \rangle \ \subseteq\ \ker room \\ \equiv & \quad \{\ (89)\ ;\ (43)\ \} \\ & \frac{lect}{lect} \cap \frac{slot}{slot} \ \subseteq\ \frac{room}{room} \\ \equiv & \quad \{\ \text{going pointwise, for all } c_1, c_2 \in Class\ \} \\ & \left\{ \begin{array}{l} lect\ c_1 = lect\ c_2 \\ slot\ c_1 = slot\ c_2 \end{array} \right. \Rightarrow room\ c_1 = room\ c_2 \end{array}$$

The specification pattern $h \leqslant \langle f, g \rangle$

That is, $room \leqslant \langle lect, slot \rangle$ imposes that

> *a given lecturer cannot be in two different rooms at the same time.*

(Think of c_1 and c_2 as classes shared by different courses, possibly of different degrees.)

In the standard terminology of database theory this is called a **functional dependency**, meaning that:

- $room$ is **dependent** on $lect$ and $slot$, i.e.
- $lect$ and $slot$ **determine** $room$.

Generalization: the “agenda design pattern”

Nobody can be in different places at the same time

$$\mathit{where} \leqslant \langle \mathit{who}, \mathit{when} \rangle$$

in the context of the generic data model:

$$\begin{tikzcd}
\mathit{Who} & \mathit{Meeting} \arrow[l, "\mathit{who}"'] \arrow[r, "\mathit{where}"] \arrow[d, "\mathit{when}"'] & \mathit{Where} \\
 & \mathit{When} &
\end{tikzcd}$$

Exercise 39: Do $\mathit{who} \leqslant \langle \mathit{where}, \mathit{when} \rangle$ and $\mathit{when} \leqslant \langle \mathit{who}, \mathit{where} \rangle$ express reasonable facts? □

The specification pattern $h \leqslant \langle f, g \rangle$

Let $h := id$ in this pattern:

Two functions f and g are said to be **complementary** *wherever $id \leqslant \langle f, g \rangle$.*

For instance:

> π_1 *and* π_2 *are complementary since* $\langle \pi_1, \pi_2 \rangle = id$ *by* $\times$*-reflection.*

Informal interpretation:

> **Non-injective** f *and* g *compensate each other's lack of injectivity so that their pairing is* **injective***.*

Universal property

$$\langle R, S\rangle \leqslant X \quad \equiv \quad R \leqslant X \wedge S \leqslant X \tag{92}$$

Cancellation of (92) means that *pairing* always *increases injectivity*:

$$R \leqslant \langle R, S\rangle \quad \text{and} \quad S \leqslant \langle R, S\rangle . \tag{93}$$

(93) unfolds to $\ker \langle R, S\rangle \ \subseteq \ (\ker R) \cap (\ker S)$, confirming (89).

Injectivity **shunting law**:

$$R \cdot g \leqslant S \quad \equiv \quad R \leqslant S \cdot g^{\circ} \tag{94}$$

Exercise 40: $\langle R, id\rangle$ is always *injective* — why? □

Relation pairing continued

The **fusion**-law of relation pairing requires a side condition:

$$\begin{aligned} &\langle R, S\rangle \cdot T = \langle R \cdot T, S \cdot T\rangle \\ &\qquad \Leftarrow \; R \cdot (\mathrm{img}\ T) \subseteq R \vee S \cdot (\mathrm{img}\ T) \subseteq S \end{aligned} \tag{95}$$

The **absorption** law

$$(R \times S) \cdot \langle P, Q\rangle = \langle R \cdot P, S \cdot Q\rangle \tag{96}$$

holds unconditionally.

Exercises

Exercise 41: Recalling (31), prove that

$$swap = \langle \pi_2, \pi_1 \rangle \tag{97}$$

is a bijection. (Assume property $(R \cap S)^\circ = R^\circ \cap S^\circ$.) □

Exercise 42: Derive from the laws of pairing studied thus far the following facts about relational product:

$$id \times id = id \tag{98}$$

$$(R \times S) \cdot (P \times Q) = (R \cdot P) \times (S \cdot Q) \tag{99}$$

□

Exercise 43: Show that (95) holds. Suggestion: recall (62). From this infer that no side-condition is required for T simple. □

Relational sums

Example (Haskell):

```
data X = Boo Bool | Err String
```

PF-transforms to

$$\begin{tikzcd}
Bool \arrow[r, "i_1"] \arrow[dr, "Boo"'] & Bool + String \arrow[d, "{[Boo\ ,Err]}"] & String \arrow[l, "i_2"'] \arrow[dl, "Err"] \\
& X &
\end{tikzcd} \tag{100}$$

where

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

cf.

$$\begin{tikzcd}
A \arrow[r, "i_1"] \arrow[dr, "R"'] & A + B \arrow[d, "{[R\ ,S]}"] & B \arrow[l, "i_2"'] \arrow[dl, "S"] \\
& C &
\end{tikzcd}$$

Dually: $R + S = [i_1 \cdot R\ , i_2 \cdot S]$

Relational sums

From $[R\ ,S] = (R \cdot i_1^\circ) \cup (S \cdot i_2^\circ)$ above one easily infers, by indirect equality,

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

(check this).

It turns out that inclusion can be strengthened to equality, and therefore **relational coproducts** have exactly the same properties as functional ones, stemming from the universal property:

$$[R\ ,S] = X \quad \equiv \quad R = X \cdot i_1 \ \wedge \ S = X \cdot i_2 \tag{101}$$

Thus $[i_1\ ,i_2] = id$ — solve (101) for R and S when $X = id$, etc etc.

Divide and conquer

The property for sums (coproducts) corresponding to (88) for products is:

$$[R\ ,S] \cdot [T\ ,U]^\circ \quad = \quad (R \cdot T^\circ) \cup (S \cdot U^\circ) \tag{102}$$

NB: This *divide-and-conquer* rule is essential to **parallelizing** relation composition by **block** decomposition.

Exercise 44: Show that:

$$\mathrm{img}\ [R\ ,S] \quad = \quad \mathrm{img}\ R \cup \mathrm{img}\ S \tag{103}$$

$$\mathrm{img}\ i_1 \cup \mathrm{img}\ i_2 \quad = \quad id \tag{104}$$

□

Exercises

Exercise 45: The type declaration

$$\textbf{data}\ \mathit{Maybe}\ a = \mathsf{Nothing} \mid \mathsf{Just}\ a$$

in Haskell corresponds, as is known, to the declaration of the isomorphism:

$$\begin{array}{l} \mathsf{in} : 1 + A \to \mathit{Maybe}\ A \\ \mathsf{in} = [\underline{\mathsf{Nothing}}\ , \mathsf{Just}] \end{array}$$

Show that the relation

$$R = i_1 \cdot \underline{\mathsf{Nothing}}^{\circ} \cup i_2 \cdot \mathsf{Just}^{\circ}$$

is a function. $\square$

Exercises

Exercise 46: Consider the following definition of a relation $A \xleftarrow{R} A^*$,

$$R \cdot \mathsf{in} = [\bot \ , \pi_1 \cup R \cdot \pi_2]$$

where

$$\mathsf{in} = [\mathsf{nil} \ , \mathsf{cons}] \tag{105}$$

$$\mathsf{nil} \ \_ = [\,] \tag{106}$$

$$\mathsf{cons}\ (h, t) = h : t \tag{107}$$

(a) Rely on the co-product laws to derive (formally) the *pointwise* definition of R.

(b) Based on this, spell out the meaning of $a \ R \ x$ in you own words. $\square$

$+$ meets $\times$

The **exchange law**

$$[\langle R,S\rangle\ ,\langle T,V\rangle] \;=\; \langle [R\ ,\ T],[S\ ,\ V]\rangle \tag{108}$$

holds for all relations as in diagram

$$\begin{tikzcd}
A \arrow[r, "i_1"] \arrow[d, "R"'] \arrow[drr, "S"' near start] & A+B & B \arrow[l, "i_2"'] \arrow[d, "V"] \arrow[dll, "T"' near start] \\
C & C\times D \arrow[l, "\pi_1"] \arrow[r, "\pi_2"'] & D
\end{tikzcd}$$

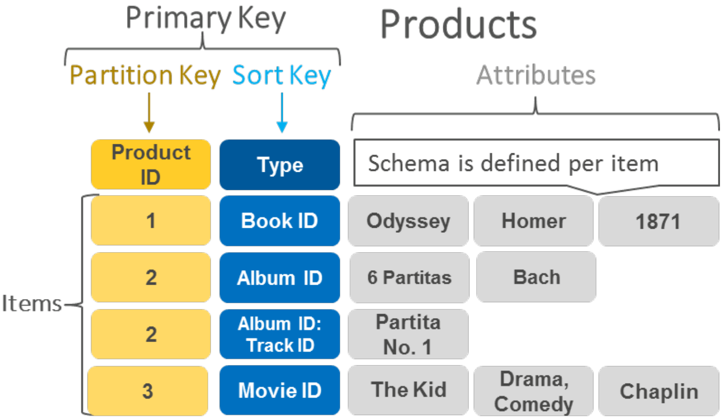
and the **fusion** law

$$\langle R,S\rangle \cdot f \;=\; \langle R\cdot f, S\cdot f\rangle \tag{109}$$

also holds, where f is a function. (Why?)

Exercise 47: Relying on both (101) and (109) prove (108). ☐

On key-value (KV) data models



Primary Key

Products

Partition Key Sort Key

Attributes

Items

Product ID	Type	Schema is defined per item		
1	Book ID	Odyssey	Homer	1871
2	Album ID	6 Partitas	Bach	
2	Album ID: Track ID	Partita No. 1		
3	Movie ID	The Kid	Drama, Comedy	Chaplin

On key-value data models

Simple relations abstract what is currently known as the **key-value-pair** (**KV**) data model in modern databases

E.g. Hbase, Amazon DynamoDB etc

In each such relation $K \xrightarrow{S} V$, K is said to be the **key** and V the **value**.

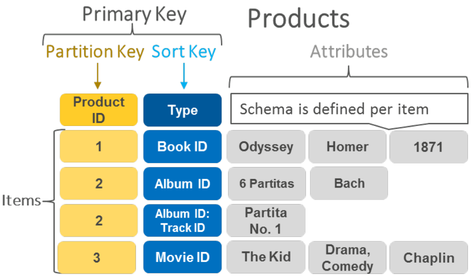
No-SQL, **columnar** *database trend.*

Example above:

$$\underbrace{PartitionKey \times SortKey}_{K} \to \underbrace{Type \times \ldots}_{V}$$

On key-value data models

“Schema is defined per item”…



Primary Key

Products

Partition Key Sort Key

Attributes

Items

Product ID	Type	Schema is defined per item		
1	Book ID	Odyssey	Homer	1871
2	Album ID	6 Partitas	Bach	
2	Album ID: Track ID	Partita No. 1		
3	Movie ID	The Kid	Drama, Comedy	Chaplin

In this example:

$$V = \mathit{Title} \times (1 + \mathit{Author} \times (1 + \mathit{Date} \times \ldots))$$

This shows the expressiveness of **products** and **coproducts** in data modelling.

Magic square sums

Exercise 48: Prove (110) below.

$$\begin{tikzcd}
A & & C \arrow[ll, "R"'] \arrow[dd, "Q"] & & & & \\
 & \subseteq & & & & & \\
B & & D \arrow[ll, "S"] & & A+A' & & C+C' \arrow[ll, "R+R'"'] \arrow[dd, "Q+Q'"] \\
 & + & & = & & \subseteq & \\
A' & & C' \arrow[ll, "R'"'] \arrow[dd, "Q'"] & & B+B' & & D+D' \arrow[ll, "S+S'"] \\
 & \subseteq & & & & & \\
B' & & D' \arrow[ll, "S"] & & & &
\arrow[from=1-1, to=3-1, "P"']
\arrow[from=3-5, to=5-5, "P+P'"']
\arrow[from=5-1, to=7-1, "P'"']
\end{tikzcd} \tag{110}$$

□

Class 7 — Relational division

Relational division

In the same way

$$z \times y \leqslant x \;\equiv\; z \leqslant x \div y$$

means that $x \div y$ is the largest **number** which multiplied by y approximates x,

$$Z \cdot Y \subseteq X \;\equiv\; Z \subseteq X / Y \tag{111}$$

means that X/Y is the largest **relation** which pre-composed with Y approximates X.

What is the pointwise meaning of X/Y?

We reason:

First, the types of

$$Z \cdot Y \subseteq X \;\equiv\; Z \subseteq X/Y$$

$$\begin{tikzcd}
& A \arrow[dl, "X/Y"'] \\
C & B \arrow[l, "X"] \arrow[u, "Y"']
\end{tikzcd}$$

Next, the calculation:

$$\begin{array}{cl}
& c\ (X/Y)\ a \\
\equiv & \qquad \{ \text{ introduce points } C \xleftarrow{\underline{c}} 1 \text{ and } A \xleftarrow{\underline{a}} 1 \ \} \\
& x(\underline{c}^{\circ} \cdot (X/Y) \cdot \underline{a})x \\
\equiv & \qquad \{ \text{ one-point } (146) \ \} \\
& x' = x \;\Rightarrow\; x'(\underline{c}^{\circ} \cdot (X/Y) \cdot \underline{a})x
\end{array}$$

Proceed by going pointfree:

We reason

$$
\begin{array}{ll}
 & id \subseteq \underline{c}^\circ \cdot (X/Y) \cdot \underline{a} \\
\equiv & \qquad \{ \text{ shunting rules } \} \\
 & \underline{c} \cdot \underline{a}^\circ \subseteq X/Y \\
\equiv & \qquad \{ \text{ universal property (111) } \} \\
 & \underline{c} \cdot \underline{a}^\circ \cdot Y \subseteq X \\
\equiv & \qquad \{ \text{ now shunt } \underline{c} \text{ back to the right } \} \\
 & \underline{a}^\circ \cdot Y \subseteq \underline{c}^\circ \cdot X \\
\equiv & \qquad \{ \text{ back to points via (23) } \} \\
 & \langle \forall\, b \;:\; a\, Y\, b : \; c\, X\, b \rangle
\end{array}
$$

Outcome

In summary:

$$c\ (X/Y)\ a\ \equiv\ \langle \forall\ b\ :\ a\ Y\ b :\ c\ X\ b \rangle$$

$$\begin{tikzcd}
& a \arrow[dl, maps to, "X/Y"'] \\
c & b \arrow[l, maps to, "X"] \arrow[u, maps to, "Y"']
\end{tikzcd} \tag{112}$$

Example:

$a\ Y\ b$ = passenger a chooses flight b

$c\ X\ b$ = company c operates flight b

$c\ (X/Y)\ a$ = company c is the only one trusted by passenger a, that is, a **only flies** c.

Pattern $X\ /\ Y$

Informally, $c\ (X\ /\ Y)\ a$ captures the linguistic pattern

---

a **only** Y *those* b*'s* **such that** $c\ X\ b$.

$$\begin{tikzcd}
 & a \arrow[dl, mapsto, "X/Y"'] \\
c & b \arrow[l, mapsto, "X"] \arrow[u, mapsto, "Y"']
\end{tikzcd}$$

For instance,

Students *enrolled*
in **courses** *only*
dealing with
particular **subjects**

$$\begin{tikzcd}
 & \mathit{student} \arrow[dl, mapsto, "\mathit{Dealt\_in}/\mathit{Enrolled}"'] \\
\mathit{subject} & \mathit{course} \arrow[l, mapsto, "\mathit{Dealt\_in}"] \arrow[u, mapsto, "\mathit{Enrolled}"']
\end{tikzcd}$$

Pointwise meaning in full

The full pointwise encoding of

$$Z \cdot Y \subseteq X \;\equiv\; Z \subseteq X/Y$$

is:

$$\begin{array}{ll} & \langle \forall\, c, b \;:\; \langle \exists\, a \;:\; cZa : \; aYb \rangle : \; cXb \rangle \\ \equiv & \\ & \langle \forall\, c, a \;:\; cZa : \; \langle \forall\, b \;:\; aYb : \; cXb \rangle \rangle \end{array}$$

If we drop variables and regard the uppercase letters as denoting Boolean terms dealing without variable c, this becomes

$$\langle \forall\, b \;:\; \langle \exists\, a \;:\; Z : \; Y \rangle : \; X \rangle \;\equiv\; \langle \forall\, a \;:\; Z : \; \langle \forall\, b \;:\; Y : \; X \rangle \rangle$$

recognizable as the **splitting** rule (154) of the Eindhoven calculus.

Put in other words: **existential** quantification is **lower** adjoint to **universal** quantification.

Exercises

Exercise 49: Prove the equalities

$$X \cdot f = X / f^\circ \tag{113}$$
$$X / \bot = \top \tag{114}$$
$$X / id = X \tag{115}$$

and check their pointwise meaning. □

Exercise 50: Define

$$X \setminus Y = (Y^\circ / X^\circ)^\circ \tag{116}$$

and infer:

$$a(R \setminus S)c \equiv \langle \forall\ b\ :\ b\ R\ a :\ b\ S\ c \rangle \tag{117}$$
$$R \cdot X \subseteq Y \equiv X \subseteq R \setminus Y \tag{118}$$

□

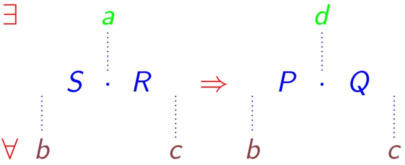
Patterns in diagrams (again!)

Back to our good old "rectangle":

$$\begin{tikzcd}
A \arrow[d, "S"'] \arrow[dr, phantom, "\subseteq"] & C \arrow[l, "R"'] \arrow[d, "Q"] \\
B & D \arrow[l, "P"]
\end{tikzcd}$$

$$S \cdot R \subseteq P \cdot Q$$

... i.e. the pointwise:



Patterns in diagrams - very special case

Again assuming two preorders $(\sqsubseteq)$ and $(\leqslant)$:

$$\begin{tikzcd}
A \arrow[d, "f^\circ"'] \arrow[dr, phantom, "="] & A \arrow[l, "(\sqsubseteq)"'] \arrow[d, "g"] \\
B & B \arrow[l, "(\leqslant)"]
\end{tikzcd}$$

$$f^\circ \cdot (\sqsubseteq) = (\leqslant) \cdot g$$

$$f\ b \sqsubseteq a \ \equiv\ b \leqslant g\ a \qquad (119)$$

In this very special situation, f and g in

$$\begin{tikzcd}
(A, \sqsubseteq) \arrow[r, bend left, "g"] & (B, \leqslant) \arrow[l, bend left, "f"]
\end{tikzcd}$$

are said to be **Galois connected** (GC) and we write

$$f \vdash g \qquad (120)$$

Patterns in diagrams - very special case

Again assuming two preorders $(\sqsubseteq)$ and $(\leqslant)$:

$$\begin{tikzcd}
A \arrow[d, "f^\circ"'] \arrow[dr, phantom, "="] & A \arrow[l, "(\sqsubseteq)"'] \arrow[d, "g"] \\
B & B \arrow[l, "(\leqslant)"]
\end{tikzcd}$$

$$f^\circ \cdot (\sqsubseteq) = (\leqslant) \cdot g$$

$$f\ b \sqsubseteq a \ \equiv\ b \leqslant g\ a \qquad (119)$$

In this very special situation, f and g in

$$\begin{tikzcd}
(A, \sqsubseteq) \arrow[r, bend left, "g"] & (B, \leqslant) \arrow[l, bend left, "f"]
\end{tikzcd}$$

are said to be **Galois connected** (GC) and we write

$$f \vdash g \qquad (120)$$

Patterns in diagrams - even more special case

Preorders $(\sqsubseteq)$ and $(\leqslant)$ are the **identity**:

$$\begin{tikzcd}
A \arrow[d, "f^\circ"'] \arrow[dr, phantom, "="] & A \arrow[l, "id"'] \arrow[d, "g"] \\
B & B \arrow[l, "id"]
\end{tikzcd}$$

$$f^\circ = g$$

$$f\ b = a \ \equiv\ b = g\ a \qquad (121)$$

That is to say,

$$\begin{tikzcd}
A \arrow[r, bend left, "g"] \arrow[r, phantom, "\cong"] & B \arrow[l, bend left, "f"]
\end{tikzcd}$$

Isomorphisms *are special cases of* **Galois connections**.

Patterns in diagrams - even more special case

Preorders $(\sqsubseteq)$ and $(\leqslant)$ are the **identity**:

$$\begin{tikzcd}
A \arrow[d, "f^\circ"'] & A \arrow[l, "id"'] \arrow[d, "g"] \arrow[dl, phantom, "="] \\
B & B \arrow[l, "id"]
\end{tikzcd}$$

$$f^\circ = g$$

$$f\ b = a \ \equiv\ b = g\ a \tag{121}$$

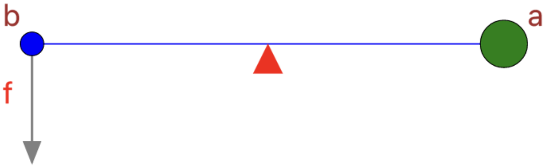
That is to say,

$$\begin{tikzcd}
A \arrow[r, bend left, "g"] \arrow[r, phantom, "\cong"] & B \arrow[l, bend left, "f"]
\end{tikzcd}$$

Isomorphisms *are special cases of* **Galois connections**.

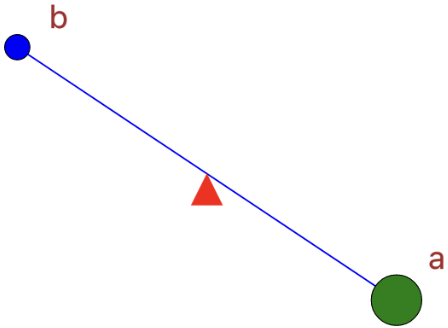
GC — mechanics analogy

Stability:



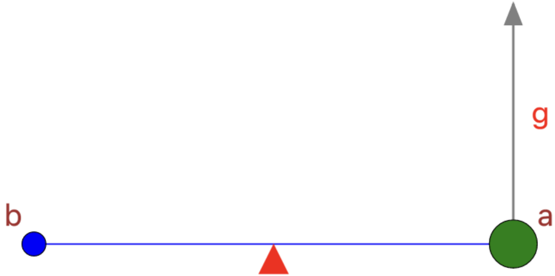
GC — mechanics analogy

Instability:



GC — mechanics analogy

Stability restored:



"Restauratio" rule (Middle Ages).

Example of GC

Integer division:

$$z \times y \leqslant x \ \equiv\ z \leqslant x \div y$$

that is:

$$z \ \underbrace{\times y}_{f} \leqslant x \ \equiv\ z \leqslant x \ \underbrace{\div y}_{g}$$

So:

$$(\times y) \vdash (\div y)$$

Principle:

Difficult $(\div y)$ *explained by* **easy** $(\times y)$.

GCs

Interpreting:

$$f^\circ \cdot (\sqsubseteq) = (\leqslant) \cdot g, \textit{ ie.}$$
$$f\ b \sqsubseteq a \ \equiv\ b \leqslant g\ a, \textit{ ie.}$$
$$f \vdash g$$

- $f\ b$ is the **smallest** a such that $b \leqslant g\ a$ holds.
- $g\ a$ is the **largest** b such that $f\ b \sqsubseteq a$ holds.

Thus $z \times y \leqslant x \ \equiv\ z \leqslant x \div y$ reads like this:

$x \div y$ *is the largest* z *such that* $z \times y \leqslant x$.

Yes! (back to the primary school desk)

The **whole division** algorithm

$$\begin{array}{r|l} 7 & 2 \\ \cline{2-2} 1 & 3 \end{array} \qquad 2 \times 3 + 1 = 7 \quad , \text{“i.e.“} \qquad 3 = 7 \div 2$$

However

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

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

That is:

$$\begin{array}{r|c} x & y \\ \cline{2-2} \ldots & x \div y \end{array} \qquad z \times y \leqslant x \Rightarrow z \leqslant x \div y$$

$x \div y$ **largest** z
such that
$z \times y \leqslant x$.

GCs as specifications

Thus:

$z \times y \leqslant x \;\equiv\; z \leqslant x \div y$ *is a* **specification** *of* $x \div y$

How does it relate to its **implementation**, e.g.

$$\begin{array}{l} x \div y = \\ \quad \textbf{if } x < y \textbf{ then } 0 \\ \quad \textbf{else } 1 + (x - y) \div y \end{array}$$

?

It's a long story. For the moment, let us appreciate the power of the GC concept.

GCs as specifications

Consider the following **requirements** about the take function in Haskell:

---

take *n xs should yield the* **longest** *possible* **prefix** *of xs not exceeding n in* **length**.

Warming up examples:

$$\text{take } 2\ [10,20,30] = [10,20]$$
$$\text{take } 20\ [10,20,30] = [10,20,30]$$
$$\ldots$$

How do we write a formal **specification** for these requirements?

Specifying functions on lists

Clearly,

- $\mathsf{take}\ n\ xs$ is a **prefix** of xs — specify this as e.g.

  $\mathsf{take}\ n\ xs\ \preceq\ xs$

  where $\preceq$ denotes the **prefix** partial order.
- the length of $\mathsf{take}\ n\ xs$ cannot exceed n — easy to specify:

  $\mathsf{length}\ (\mathsf{take}\ n\ xs) \leqslant n$

Altogether:

$$\mathsf{length}\ (\mathsf{take}\ n\ xs) \leqslant n\ \wedge\ \mathsf{take}\ n\ xs\ \preceq\ xs \tag{122}$$

But this is not **enough** — (silly) implementation $\mathsf{take}\ n\ xs = [\,]$ meets (122)!

Superlatives...

The crux is how to formally specify the **superlative** in

...take n xs should yield the **longest possible** *prefix...*

This is the **hard** part but there is a standard method to follow:

- think of an arbitrary list ys also satisfying (122)

$$\mathsf{length}\ ys \leqslant n \ \wedge\ ys \preceq xs$$

- Then (from above) ys should be a prefix of $\mathsf{take}\ n\ xs$:

$$\mathsf{length}\ ys \leqslant n \wedge ys \preceq xs \Rightarrow ys \preceq \mathsf{take}\ n\ xs \tag{123}$$

Final touch

So we have two clauses,

a **easy** *one (122)*

and

a **hard** *one (123).*

Interestingly, (122) can be derived from (123) itself,

$$\mathsf{length}\ ys \leqslant n \wedge ys \preceq xs \Leftarrow ys \preceq \mathsf{take}\ n\ xs$$

by letting $ys := \mathsf{take}\ n\ xs$ and simplifying.

So a single line is enough to **formally specify** *take*:

$$length\ ys \leqslant n \ \wedge\ ys \preceq xs \quad \equiv \quad ys \preceq \mathsf{take}\ n\ xs \tag{124}$$

— a **GC**.

Reasoning about specifications (GCs)

One of the advantages of **formal specification** is that one may **quest** the specification (aka **model**) to derive useful properties of the design **before the implementation phase**.

GCs + **indirect equality** (on partial orders) yield much in this process — see the following exercise.

Exercise 51: Solely relying on specification (124) use indirect equality to prove that

$$take\ (length\ xs)\ xs = xs \tag{125}$$

$$take\ 0\ xs = [\,] \tag{126}$$

$$take\ n\ [\,] = [\,] \tag{127}$$

hold. □

GCs: many properties for free

$$(f\ b) \leqslant a \equiv b \sqsubseteq (g\ a)$$

Description	$f = g^\flat$	$g = f^\sharp$
Definition	$f\ b = \bigwedge\{a : b \sqsubseteq g\ a\}$	$g\ a = \bigsqcup\{b : f\ b \leqslant a\}$
Cancellation	$f(g\ a) \leqslant a$	$b \sqsubseteq g(f\ b)$
Distribution	$f(b \sqcup b') = (f\ b) \vee (f\ b')$	$g(a' \wedge a) = (g\ a') \sqcap (g\ a)$
Monotonicity	$b \sqsubseteq b' \Rightarrow f\ b \leqslant f\ b'$	$a \leqslant a' \Rightarrow g\ a \sqsubseteq g\ a'$

Exercise 52: Derive from (119) that both f and g are monotonic. $\Box$

Remark on GCs

Galois connections originate from the work of the French mathematician Evariste Galois (1811-1832). Their main advantages,

> *simple, generic and highly calculational*

are welcome in proofs in computing, due to their size and complexity, recall E. Dijkstra:

> *elegant* $\equiv$ *simple and remarkably effective.*

In the sequel we will re-interpret the **relational operators** we've seen so far as Galois adjoints.

Examples

Not only

$$\underbrace{z\ {\color{red}(\times y)}}_{{\color{red}f}\ z} \leqslant x \quad \equiv \quad z \leqslant \underbrace{x\ {\color{red}(\div y)}}_{{\color{red}g}\ n}$$

but also the two **shunting rules**,

$$\underbrace{{\color{red}(h\cdot)}X}_{{\color{red}f}\ X} \subseteq Y \quad \equiv \quad X \subseteq \underbrace{{\color{red}(h^\circ\cdot)}Y}_{{\color{red}g}\ Y}$$

$$\underbrace{X{\color{red}(\cdot h^\circ)}}_{{\color{red}f}\ X} \subseteq Y \quad \equiv \quad X \subseteq \underbrace{Y{\color{red}(\cdot h)}}_{{\color{red}g}\ Y}$$

as well as **converse**,

$$\underbrace{X^{\color{red}\circ}}_{{\color{red}f}\ X} \subseteq Y \quad \equiv \quad X \subseteq \underbrace{Y^{\color{red}\circ}}_{{\color{red}g}\ Y}$$

and so and so forth — are **adjoints** of GCs: see the next slides.

Converse

$$(f\ X) \subseteq Y \equiv X \subseteq (g\ Y)$$

Description	$f = g^\flat$	$g = f^\sharp$	**Obs.**
converse	$(\_)^\circ$	$(\_)^\circ$	$b\ R^\circ\ a \equiv a\ R\ b$

Thus:

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

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

Distributions $(R \cap S)^\circ = R^\circ \cap S^\circ, (R \cup S)^\circ = R^\circ \cup S^\circ$

Exercise 53: Why is it that converse-monotonicity can be strengthened to an equivalence? $\square$

Example of calculation from the GC

Converse involution (cancellation):

$$(R^\circ)^\circ \;=\; R \tag{128}$$

Proof of (128):

$$
\begin{array}{ll}
 & (R^\circ)^\circ = R \\
\equiv & \qquad \{ \text{ antisymmetry ("ping-pong") } \} \\
 & (R^\circ)^\circ \;\subseteq\; R \wedge R \;\subseteq\; (R^\circ)^\circ \\
\equiv & \qquad \{ \text{ }^\circ\text{-universal } \; X^\circ \;\subseteq\; Y \;\;\equiv\;\; X \subseteq Y^\circ \;\; \text{twice } \} \\
 & R^\circ \;\subseteq\; R^\circ \wedge R^\circ \;\subseteq\; R^\circ \\
\equiv & \qquad \{ \text{ reflexivity (twice) } \} \\
 & \textsc{True}
\end{array}
$$

Relational division

$(f\ X) \subseteq Y \equiv X \subseteq (g\ Y)$

Description	$f = g^\flat$	$g = f^\sharp$	**Obs.**
right-division	$(\cdot R)$	$(\ /\ R)$	right-factor
left-division	$(R \cdot)$	$(R \setminus\ )$	left-factor

that is,

$$X \cdot R \subseteq Y \equiv X \subseteq Y \,/\, R \tag{129}$$

$$R \cdot X \subseteq Y \equiv X \subseteq R \setminus Y \tag{130}$$

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

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

$(\setminus R)$ and $(/R)$ are monotonic and distribute over $\cap$.

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: $h \subseteq g \equiv \quad h = k \quad \equiv h \supseteq k$

Functional division: $R \cdot h = R / h^\circ$

Other operators

<table>
<tr><td colspan="4">$(f\ X) \subseteq Y \equiv X \subseteq (g\ Y)$</td></tr>
<tr><th>Description</th><th>$f = g^\flat$</th><th>$g = f^\sharp$</th><th>Obs.</th></tr>
<tr><td>implication</td><td>$(R \cap\ )$</td><td>$(R \Rightarrow\ )$</td><td>$b(R \Rightarrow X)a \equiv bRa \Rightarrow bXa$</td></tr>
<tr><td>difference</td><td>$(\_ - R)$</td><td>$(R \cup\ )$</td><td>$b\ (X - R)\ a \equiv \begin{cases} b\ X\ a \\ \neg\ (b\ R\ a) \end{cases}$</td></tr>
</table>

Thus the universal properties of implication and difference,

$$R \cap X \subseteq Y \quad \equiv \quad X \subseteq R \Rightarrow Y \tag{131}$$

$$X - R \subseteq Y \quad \equiv \quad X \subseteq R \cup Y \tag{132}$$

are GCs — etc, etc

Exercise 54: Show that $R \cap (R \Rightarrow Y) \subseteq Y$ ("modus ponens") holds and that $R - R = \bot - R = \bot$. □

Relation shrinking

Given relations $R : A \leftarrow B$ and $S : A \leftarrow A$, define $R \upharpoonright S : A \leftarrow B$, pronounced "$R$ shrunk by S", by

$$X \subseteq R \upharpoonright S \quad \equiv \quad X \subseteq R \;\wedge\; X \cdot R^\circ \subseteq S \tag{133}$$

cf. diagram:

$$\begin{tikzcd}
 & B \arrow[dl, "R \upharpoonright S"'] \arrow[d, "R"] \\
A & A \arrow[l, "S"]
\end{tikzcd}$$

Property (133) states that $R \upharpoonright S$ is the largest part of R such that, if it yields an output for an input x, this must be a 'maximum, with respect to S, among all possible outputs of x by R.

Exercise 55: Show, by indirect equality, that (133) is equivalent to:

$$R \upharpoonright S \;=\; R \cap S / R^\circ \tag{134}$$

□

Relation shrinking

Given relations $R : A \leftarrow B$ and $S : A \leftarrow A$, define $R \upharpoonright S : A \leftarrow B$, pronounced “$R$ shrunk by S”, by

$$X \subseteq R \upharpoonright S \;\equiv\; X \subseteq R \,\wedge\, X \cdot R^{\circ} \subseteq S \tag{133}$$

cf. diagram:

$$\begin{tikzcd}
 & B \arrow[dl, "R\upharpoonright S"'] \arrow[d, "R"] \\
A & A \arrow[l, "S"]
\end{tikzcd}$$

Property (133) states that $R \upharpoonright S$ is the largest part of R such that, if it yields an output for an input x, this must be a ‘maximum, with respect to S, among all possible outputs of x by R.

Exercise 56: Show, by indirect equality, that (133) is equivalent to:

$$R \upharpoonright S \;=\; R \cap S / R^{\circ} \tag{134}$$

□

Relation shrinking

Example Given

$$Examiner \times Mark \xleftarrow{R} Student \quad = \left(\begin{array}{c|c|c} Examiner & Mark & Student \\ \hline Smith & 10 & John \\ Smith & 11 & Mary \\ Smith & 15 & Arthur \\ Wood & 12 & John \\ Wood & 11 & Mary \\ Wood & 15 & Arthur \end{array}\right)$$

suppose we wish to choose the best mark for each student.

Relation shrinking

Then $S = \pi_1 \cdot R$ is the relation

$$Mark \xleftarrow{\pi_1 \cdot R} Student \;=\; \left(\begin{array}{c|c} Mark & Student \\ \hline 10 & John \\ 11 & Mary \\ 12 & John \\ 15 & Arthur \end{array}\right)$$

and

$$Mark \xleftarrow{S \upharpoonright (\geqslant)} Student \;=\; \left(\begin{array}{c|c} Mark & Student \\ \hline 11 & Mary \\ 12 & John \\ 15 & Arthur \end{array}\right)$$

Properties of shrinking

Two *fusion* rules:

$$(S \cdot f) \upharpoonright R = (S \upharpoonright R) \cdot f \qquad (135)$$

$$(f \cdot S) \upharpoonright R = f \cdot (S \upharpoonright (f^{\circ} \cdot R \cdot f)) \qquad (136)$$

"Chaotic optimization":

$$R \upharpoonright \top = R \qquad (137)$$

"Impossible optimization":

$$R \upharpoonright \bot = \bot \qquad (138)$$

"Brute force" determinization:

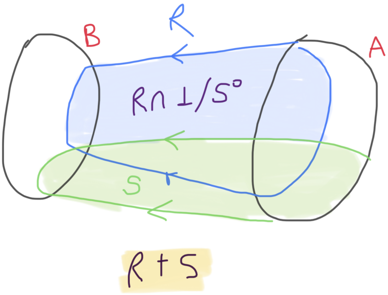
$$R \upharpoonright id = \text{largest simple fragment of } R \qquad (139)$$

Relation overriding

The relational **overriding** combinator

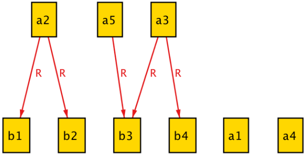
$$R \dagger S \;=\; S \cup R \cap \bot / S^{\circ} \tag{140}$$

yields the relation which contains the **whole** of S and that **part** of R where S is undefined — read $R \dagger S$ as "R overridden by S".



Exercise on relation overriding

Let $R : A \to B$ be given as in the picture, where $A = \{ a_1, a_2, a_3, a_4, a_5 \}$ and $B = \{ b_1, b_2, b_3, b_4 \}$:



Represent as a Boolean matrix the following relation overriding:

$$P = \top \dagger R = \begin{array}{c|c|c|c|c|c|} & a_1 & a_2 & a_3 & a_4 & a_5 \\ \hline b_1 & 0 & 0 & 0 & 0 & 0 \\ \hline b_2 & 0 & 0 & 0 & 0 & 0 \\ \hline b_3 & 0 & 0 & 0 & 0 & 0 \\ \hline b_4 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}$$

Exercise on relation overriding

And now this other one:

$$Q = R \dagger (\underline{b_4} \cdot \underline{a_2}^\circ) = \begin{array}{c|c|c|c|c|c|} & a_1 & a_2 & a_3 & a_4 & a_5 \\ \hline \hline b_1 & 0 & 0 & 0 & 0 & 0 \\ \hline b_2 & 0 & 0 & 0 & 0 & 0 \\ \hline b_3 & 0 & 0 & 0 & 0 & 0 \\ \hline b_4 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}$$

$\square$

Exercise 57: (a) Show that $\bot \dagger S = S$, $R \dagger \bot = R$ and $R \dagger R = R$ hold. (b) Infer the universal property:

$$X \subseteq R \dagger S \quad \equiv \quad X - S \subseteq R \wedge (X - S) \cdot S^\circ = \bot \tag{141}$$

$\square$

Background — Eindhoven quantifier calculus

Trading:

$$\langle \forall\, k : R \wedge S : T \rangle = \langle \forall\, k : R : S \Rightarrow T \rangle \tag{142}$$

$$\langle \exists\, k : R \wedge S : T \rangle = \langle \exists\, k : R : S \wedge T \rangle \tag{143}$$

de Morgan:

$$\neg\langle \forall\, k : R : T \rangle = \langle \exists\, k : R : \neg T \rangle \tag{144}$$

$$\neg\langle \exists\, k : R : T \rangle = \langle \forall\, k : R : \neg T \rangle \tag{145}$$

One-point:

$$\langle \forall\, k : k = e : T \rangle = T[k := e] \tag{146}$$

$$\langle \exists\, k : k = e : T \rangle = T[k := e] \tag{147}$$

Background — Eindhoven quantifier calculus

Nesting:

$$\langle \forall\, a, b : R \wedge S : T \rangle = \langle \forall\, a : R : \langle \forall\, b : S : T \rangle\rangle \tag{148}$$

$$\langle \exists\, a, b : R \wedge S : T \rangle = \langle \exists\, a : R : \langle \exists\, b : S : T \rangle\rangle \tag{149}$$

Rearranging-∀:

$$\langle \forall\, k : R \vee S : T \rangle = \langle \forall\, k : R : T \rangle \wedge \langle \forall\, k : S : T \rangle \tag{150}$$

$$\langle \forall\, k : R : T \wedge S \rangle = \langle \forall\, k : R : T \rangle \wedge \langle \forall\, k : R : S \rangle \tag{151}$$

Rearranging-∃:

$$\langle \exists\, k : R : T \vee S \rangle = \langle \exists\, k : R : T \rangle \vee \langle \exists\, k : R : S \rangle \tag{152}$$

$$\langle \exists\, k : R \vee S : T \rangle = \langle \exists\, k : R : T \rangle \vee \langle \exists\, k : S : T \rangle \tag{153}$$

Splitting:

$$\langle \forall\, j : R : \langle \forall\, k : S : T \rangle\rangle = \langle \forall\, k : \langle \exists\, j : R : S \rangle : T \rangle \tag{154}$$

$$\langle \exists\, j : R : \langle \exists\, k : S : T \rangle\rangle = \langle \exists\, k : \langle \exists\, j : R : S \rangle : T \rangle \tag{155}$$

References

D. Jackson.
Software Abstractions: Logic, Language, and Analysis.
The MIT Press, Cambridge Mass., 2012.
Revised edition, ISBN 0-262-01715-2.

C.B. Jones.
Software Development — A Rigorous Approach.
Prentice-Hall, 1980.