CSI - A Calculus for Information Systems (2024/25)

Class 1 — About FM

Global picture

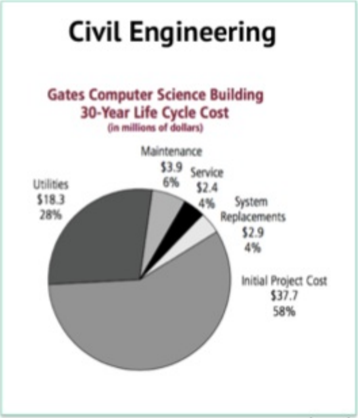
Concerning software 'engineering':

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

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

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

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

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

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

The solution

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

Have you ever used a FM?

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

al-djabr

$$x - z \leq y \;\equiv\; x \leq y + z$$

all-hatt

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

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:

$$
\begin{aligned}
&sort \subseteq \frac{bag}{bag} \cap \frac{true}{sorted}\\
&\quad \textbf{where}\\
&\qquad sorted = \ldots marks \ldots\\
&\qquad bag = \ldots.
\end{aligned}
$$

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 :-)

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

$$sorted = \ldots marks \ldots$$

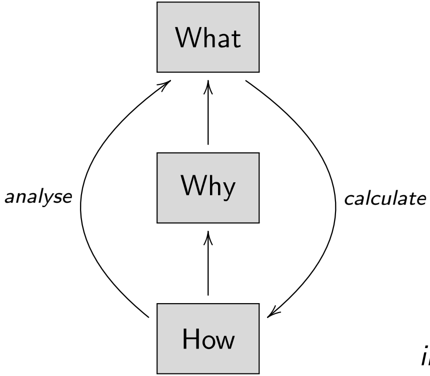
$$bag = \ldots.$$

But,

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

Yes — Wait and see :-)

FM — scientific software design

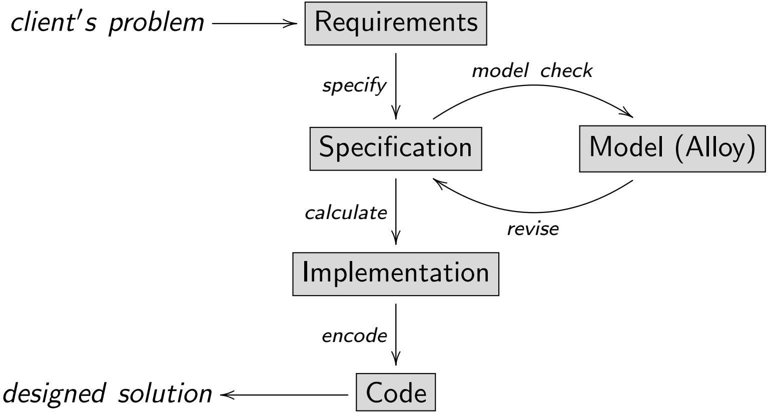


specification (*model*)

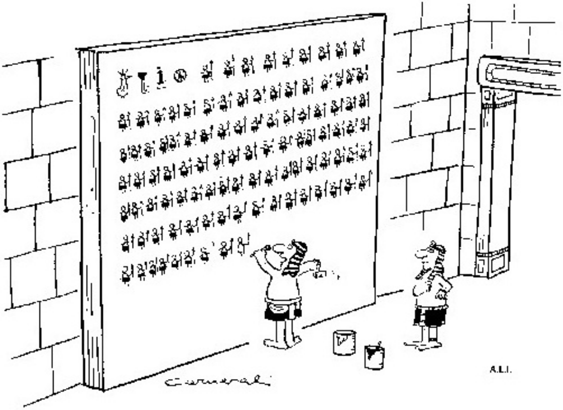
justification

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

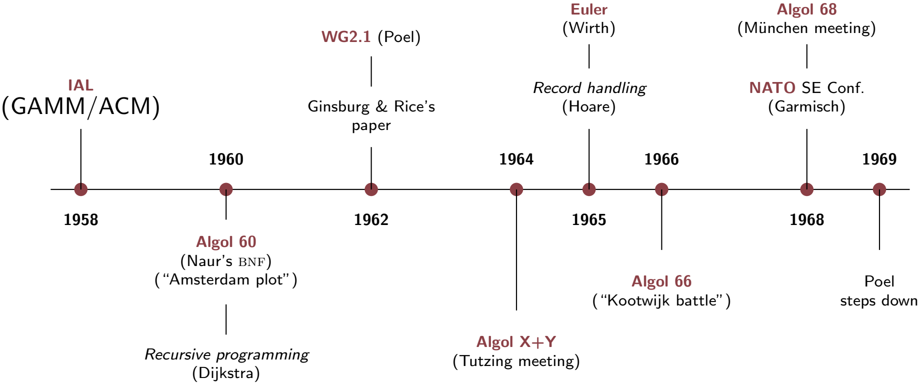
Tools:

- Alloy 6
- Coq
- Frama-C
- NuSMV
- Overture

Resources:

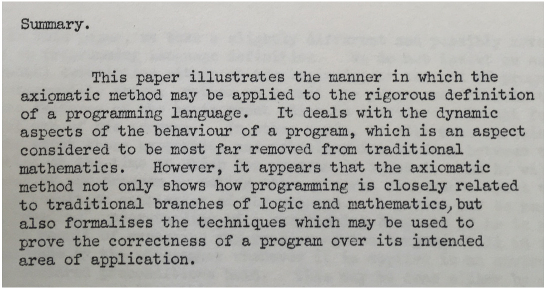
- Formal Methods Europe
- Formal Methods wiki (Oxford)

60+ years ago (1958-)



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

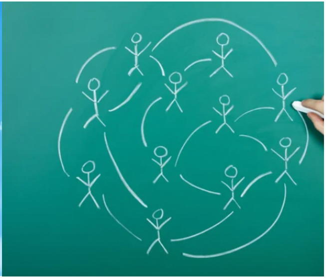
`pre`...? `choice`...?

- Non-determinism
- Parallelism
- Abstraction

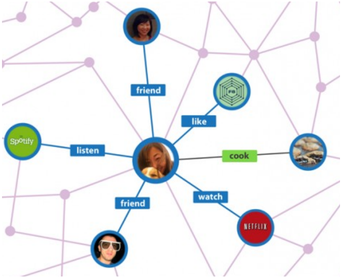
Functions not enough!

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

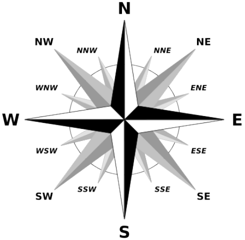
Software is too **wide** — from assembly to quantum programming

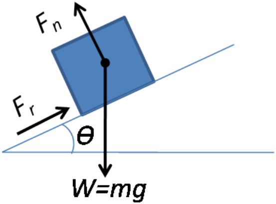
Can you think of a **unified** theory able to express and reason about software **in general**?

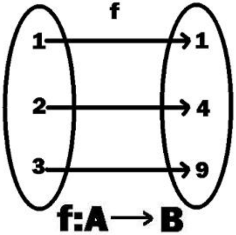
Put in another way:

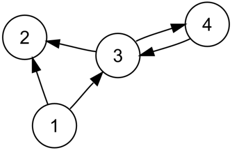
> *Is there a “lingua franca” for the software sciences?*

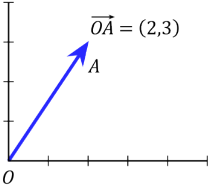
Check the pictures...



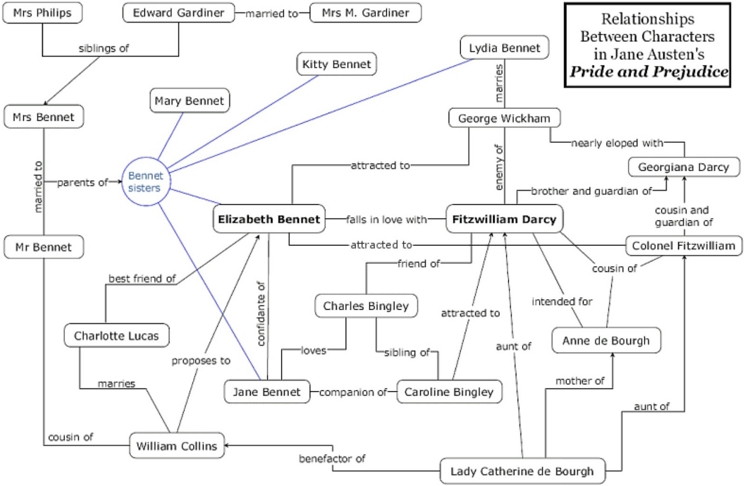






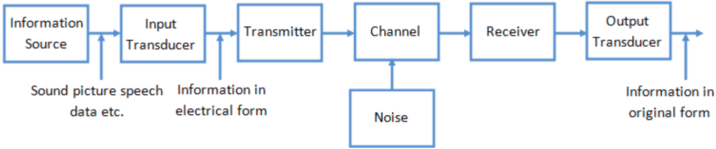


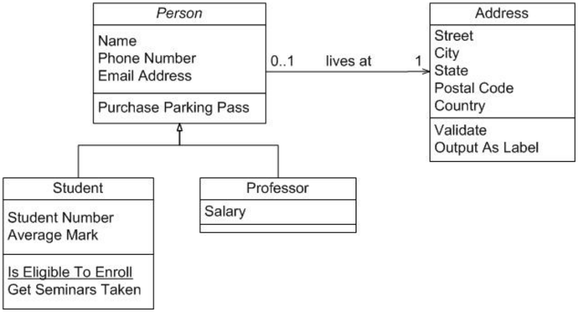
Check the pictures



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

Check the pictures





Check the pictures

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

Arrows everywhere

Arrows! A (graphical) device **common** to describing (many) **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 descriptions may have a **quantitative** side too.

Going Relational

Relation algebra

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

Question:

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

Relation algebra

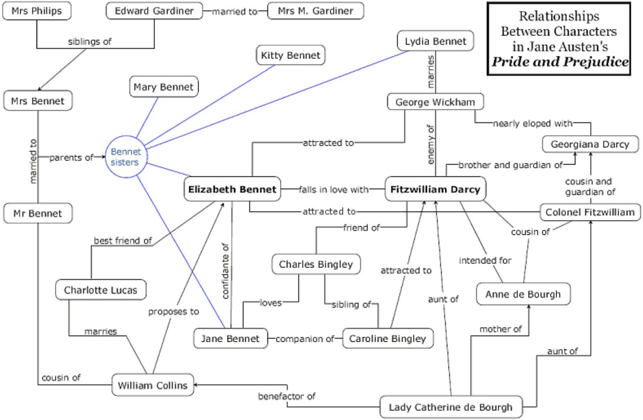
Historically, predicate logic was **not** the first one proposed:

- 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.)

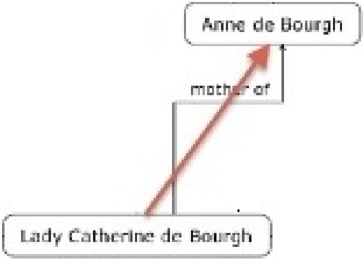
Arrow notation for relations

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

$$mother\_of : People \rightarrow People$$

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



Pairs

Consider assertions

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

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, one 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 can 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. $\mathtt{Catherine}\ \mathit{isMotherOf}\ \mathtt{Anne}$ *— and in maths — eg.* $0 \leqslant \pi$ *— extends to arbitrary* $B \xleftarrow{R} A$ *: we write*

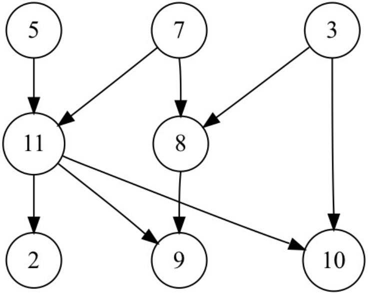
$$b\ R\ a$$

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

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

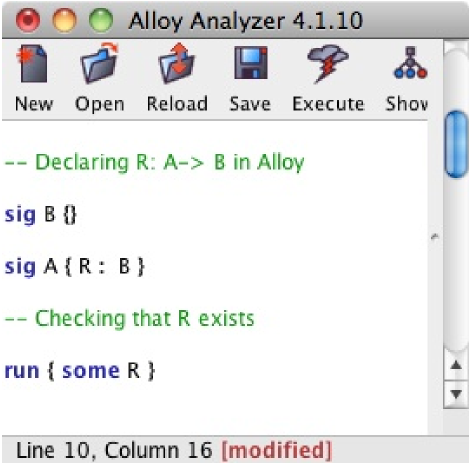
In this case $A = B = \{1..11\}$. Relations $A \xleftarrow{R} A$ over a single type A are also referred to as (directed) **graphs**.

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.



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:

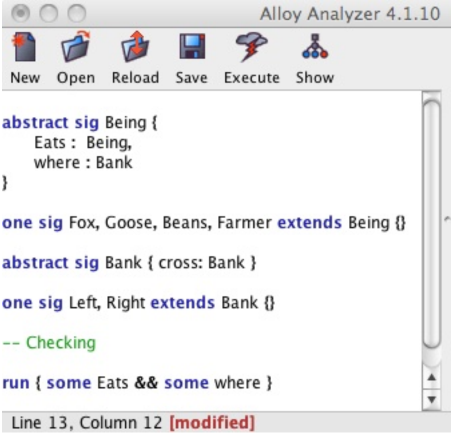
$$\begin{aligned} \mathit{Being} &= \{\mathit{Farmer}, \mathit{Fox}, \mathit{Goose}, \mathit{Beans}\} && (2) \\ \mathit{Bank} &= \{\mathit{Left}, \mathit{Right}\} && (3) \end{aligned}$$

Relations:

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

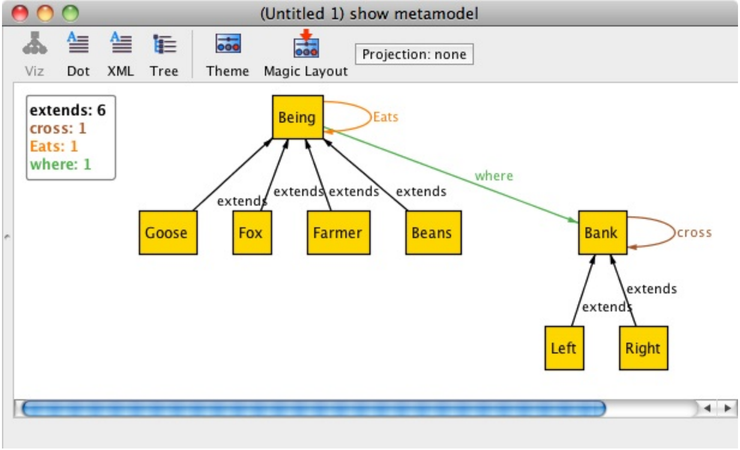
Propositio de homine et capra et lvpo

Specification source written in Alloy:



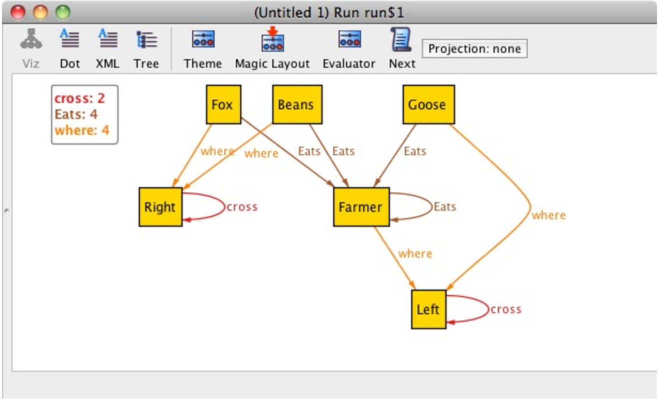
Propositio de homine et capra et lvpo

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:

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

$$b(R \cdot S)c \;\equiv\; \langle \exists\, a \,::\, b\,R\,a \,\wedge\, a\,S\,c \rangle \qquad (6)$$

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

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

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]

$$
\begin{array}{rcl}
b(f \cdot g)c & \equiv & \langle \exists\ a\ ::\ b\ f\ a \wedge a\ g\ c \rangle \\
& \equiv & \qquad \{\ a\ g\ c \text{ means } a = g\ c\ (1)\ \} \\
& & \langle \exists\ a\ ::\ a = g\ c \wedge b\ f\ a \rangle \\
& \equiv & \qquad \{\ \exists\text{-trading } (58)\ ;\ b\ f\ a \text{ means } b = f\ a\ (1)\ \} \\
& & \langle \exists\ a\ :\ a = g\ c :\ b = f\ a \rangle \\
& \equiv & \qquad \{\ \exists\text{-one point rule } (62)\ \} \\
& & b = f(g\ c)
\end{array}
$$

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

[1] Check the appendix on predicate calculus.

Class 2 — The "Zoo" of Binary Relations

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,

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

transitive

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

and **antisymmetric**:

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

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

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

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

$S \cdot \mathsf{succ} \subseteq \top \cdot S$ depicted by diagram

$$\begin{tikzcd} \mathbb{N} \arrow[d, "S"'] \arrow[dr, phantom, "\subseteq"] & \mathbb{N} \arrow[l, "\mathsf{succ}"'] \arrow[d, "S"] \\ A & A \arrow[l, "\top"] \end{tikzcd}$$

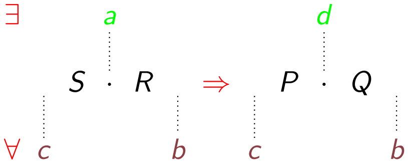
(onde $\mathsf{succ}\ n = n + 1$) means that numbers are assigned to students sequentially. □

Diagrams ("magic squares")

Pointfree:

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

Pointwise:



Exercises

Exercise 2: Consider sports competitions involving teams which have atlets (players) and coaches. Follow the rule of the previous slide and spell out the logical meaning of the following *magic square*:

$$\begin{tikzcd} Team \arrow[d, "the\_coach\_of"'] \arrow[dr, phantom, "\subseteq"] & Competition \arrow[l, "Involved"'] \arrow[d, "Involved"] \\ Atlet & Team \arrow[l, "Player\_of"] \end{tikzcd}$$

Then express this meaning in natural language, avoiding reading completely through the logic obtained in the previous step. □

Exercises

Exercise 3: Use (6) and (8) and predicate calculus to show that

$$R \cdot id \;=\; R \;=\; id \cdot R \tag{15}$$

$$R \cdot \bot \;=\; \bot \;=\; \bot \cdot R \tag{16}$$

hold and that composition is associative:

$$R \cdot (S \cdot T) = (R \cdot S) \cdot T \tag{17}$$

□

Exercise 4: 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,

$$a(R^\circ)b \quad \equiv \quad b\ R\ a \tag{18}$$

Note that converse commutes with composition

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

and with itself:

$$(R^\circ)^\circ = R \tag{20}$$

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,

$$(f\ b)R(g\ a) \ \equiv\ b(f^\circ \cdot R \cdot g)a \tag{21}$$

cf. diagram:

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

Therefore (tell why):

$$b(f^\circ \cdot g)a \ \equiv\ f\ b = g\ a \tag{22}$$

Let us see an example of using these rules.

PF-transform at work

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

$$
\begin{array}{ll}
& f \text{ is } \textbf{injective} \\
\equiv & \qquad \{ \text{ recall definition from discrete maths } \} \\
& \langle \forall\, y, x \;:\; (f\ y) = (f\ x) :\; y = x \rangle \\
\equiv & \qquad \{ \text{ (22) for } f = g \ \} \\
& \langle \forall\, y, x \;:\; y(f^\circ \cdot f)x :\; y = x \rangle \\
\equiv & \qquad \{ \text{ (21) for } R = f = g = id \ \} \\
& \langle \forall\, y, x \;:\; y(f^\circ \cdot f)x :\; y(id)x \rangle \\
\equiv & \qquad \{ \text{ go pointfree (8) i.e. drop } y, x \ \} \\
& f^\circ \cdot f \subseteq id
\end{array}
$$

The other way round

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

$$
\begin{array}{ll}
 & id \subseteq f \cdot f^\circ \\
\equiv & \quad \{ \text{ relational inclusion (8) } \} \\
 & \langle \forall\, y, x \;:\; y(id)x :\; y(f \cdot f^\circ)x \rangle \\
\equiv & \quad \{ \text{ identity relation ; composition (6) } \} \\
 & \langle \forall\, y, x \;:\; y = x :\; \langle \exists\, z \;::\; y\ f\ z \wedge z\ f^\circ x \rangle \rangle \\
\equiv & \quad \{ \text{ $\forall$-one point (61) ; converse (18) } \} \\
 & \langle \forall\, x \;::\; \langle \exists\, z \;::\; x\ f\ z \wedge x\ f\ z \rangle \rangle \\
\equiv & \quad \{ \text{ trivia ; function } f \} \\
 & \langle \forall\, x \;::\; \langle \exists\, z \;::\; x = f\ z \rangle \rangle \\
\equiv & \quad \{ \text{ recalling definition from maths } \} \\
 & f \text{ is } \textbf{surjective}
\end{array}
$$

Why *id* (really) matters

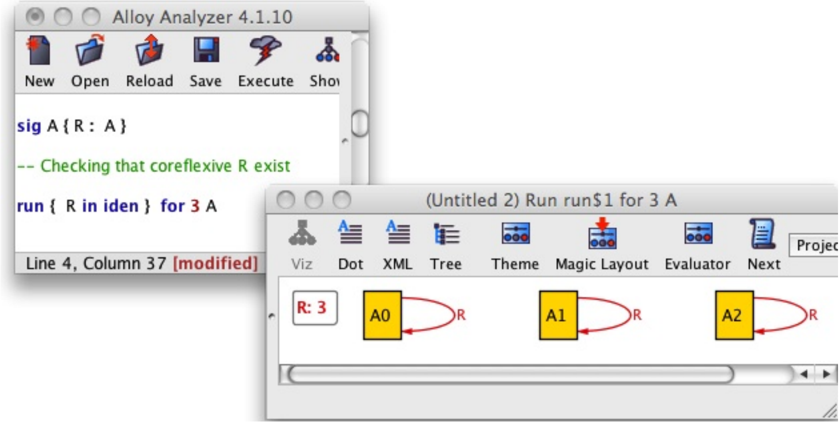
Terminology:

- 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
$A \xleftarrow{\ker R} A$ $\ker R \stackrel{\mathrm{def}}{=} R^\circ \cdot R$	$B \xleftarrow{\mathrm{img}\ R} B$ $\mathrm{img}\ R \stackrel{\mathrm{def}}{=} R \cdot R^\circ$

Alloy: checking for coreflexive relations



Kernels of functions

Meaning of $\ker f$:

$$
\begin{array}{cl}
 & a' (\ker f) a \\
\equiv & \qquad \{ \text{ substitution } \} \\
 & a' (f^{\circ} \cdot f) a \\
\equiv & \qquad \{ \text{ rule (22) } \} \\
 & f\ a' = f\ a
\end{array}
$$

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

Exercise 5: Let K be a nonempty data domain, $k \in K$ and $\underline{k}$ be the *"everywhere* k*"* function:

$$
\begin{array}{rcl}
\underline{k} & : & A \to K \\
\underline{k}\, a & = & k
\end{array}
\tag{23}
$$

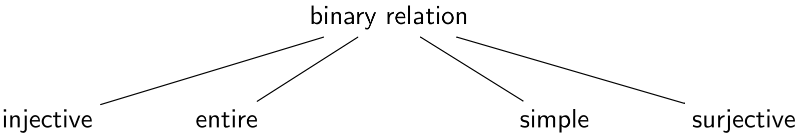
Compute which relations are defined by the following expressions:

$$
\ker \underline{k}, \quad \underline{b} \cdot \underline{c}^{\circ}, \quad \operatorname{img} \underline{k} \tag{24}
$$

□

Binary relation taxonomy

Topmost criteria:



Definitions:

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

(25)

Facts:

$$\ker\,(R^\circ) = \mathrm{img}\ R \tag{26}$$

$$\mathrm{img}\,(R^\circ) = \ker R \tag{27}$$

Binary relation taxonomy

The whole picture:

$$
\begin{tikzcd}[column sep=tiny]
 & & & \text{binary relation} \arrow[dlll, dash] \arrow[dl, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
\text{injective} \arrow[dr, dash] & & \text{entire} \arrow[dl, dash] \arrow[dr, dash] & & \text{simple} \arrow[dl, dash] \arrow[dr, dash] & & \text{surjective} \arrow[dl, dash] \\
 & \text{representation} \arrow[dr, dash] & & \text{function} \arrow[dl, dash] \arrow[dr, dash] & & \text{abstraction} \arrow[dl, dash] & \\
 & & \text{injection} \arrow[dr, dash] & & \text{surjection} \arrow[dl, dash] & & \\
 & & & \text{bijection} & & &
\end{tikzcd}
\tag{28}
$$

Exercise 6: Resort to (26,27) and (25) 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	A -> some B	A -> lone B	A some -> B
injective	entire	simple	surjective

A lone -> some B	A -> one B	A some -> lone B
representation	function	abstraction

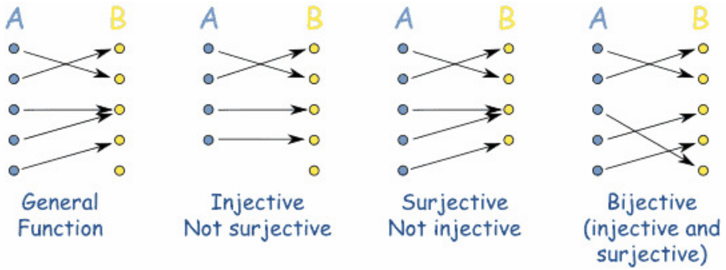
A lone -> one B	A some -> one B
injection	surjection

A one -> one B
bijection

(Courtesy of Alcino Cunha.)

Exercises

Exercise 7: 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 8: Prove the following fact

$$\textit{A function } f \textit{ is a bijection } \textbf{iff} \textit{ its converse } f^\circ \textit{ is a function} \tag{29}$$

by completing:

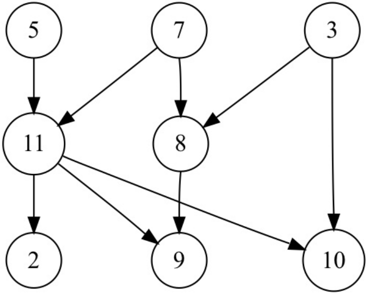
$$
\begin{array}{cl}
 & f \text{ and } f^\circ \text{ are functions} \\
\equiv & \qquad \{ \ \dots \ \} \\
 & (id \subseteq \ker f \wedge \operatorname{img} f \subseteq id) \wedge (id \subseteq \ker (f^\circ) \wedge \operatorname{img} (f^\circ) \subseteq id) \\
\equiv & \qquad \{ \ \dots \ \} \\
 & \vdots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

$\square$

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 (30)
- **surjective** — at least one 1 in every row (31)
- **simple** — at most one 1 in every column (32)
- **injective** — at most one 1 in every row (33)
- **bijective** — exactly one 1 in evey column and every row. (34)

PROPOSITIO DE HOMINE ET CAPRA ET LVPO

Exercise 9: 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 10: 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 11: 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**. □

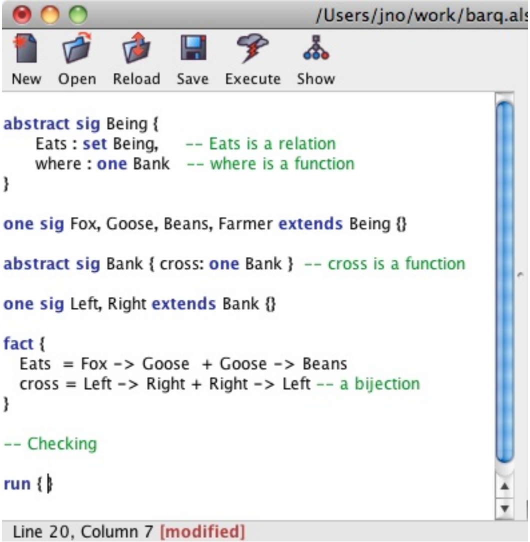
Exercise 12: There are only two **constant** functions (23) in the type $Being \longrightarrow Bank$ of *where*. Identify them and explain their role in the puzzle. □

Exercise 13: Two functions f and g are bijections iff $f^{\circ} = g$, recall (29). 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.)



Class 3 — Functions

Functions in one slide

As seen before, 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:

$$f \cdot R \subseteq S \quad \equiv \quad R \subseteq f^\circ \cdot S \tag{35}$$

$$R \cdot f^\circ \subseteq S \quad \equiv \quad R \subseteq S \cdot f \tag{36}$$

Equality rule:

$$f \subseteq g \quad \equiv \quad f = g \quad \equiv \quad f \supseteq g \tag{37}$$

Rule (37) follows from (35,36) by “cyclic inclusion” (next slide).

Proof of functional equality rule (37)

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

Then:

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

Dividing functions

$$\frac{f}{g} = g^\circ \cdot f \qquad cf. \quad \begin{tikzcd} B \arrow[dr, "g"'] & & A \arrow[ll, "\frac{f}{g}"'] \arrow[dl, "f"] \\ & C & \end{tikzcd} \tag{38}$$

Exercise 14: Check the properties:

$$\frac{f}{id} = f \tag{39}$$

$$\frac{f \cdot h}{g \cdot k} = k^\circ \cdot \frac{f}{g} \cdot h \tag{40}$$

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

$$\left(\frac{f}{g}\right)^\circ = \frac{g}{f} \tag{42}$$

□

Exercise 15: Infer $id \subseteq \ker f$ (f is total) and $\mathrm{img}\ f \subseteq id$ (f is simple) from the shunting rules (35) or (36). □

Dividing functions

By (21) we have:

$$b \, \frac{f}{g} \, a \quad \equiv \quad g \; b = f \; a \tag{43}$$

How useful is this? Think of the following sentence:

Mary lives where John was born.

By (43), this can be expressed by a division:

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

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 some: $\mathrm{ker}\ R$ 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

$$\textbf{reflexive:} \quad \text{iff } id \subseteq R \tag{44}$$

$$\textbf{coreflexive:} \quad \text{iff } R \subseteq id \tag{45}$$

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

$$\textbf{transitive:} \quad \text{iff } R \cdot R \subseteq R \tag{46}$$

$$\textbf{symmetric:} \quad \text{iff } R \subseteq R^\circ (\equiv R = R^\circ) \tag{47}$$

$$\textbf{anti-symmetric:} \quad \text{iff } R \cap R^\circ \subseteq id \tag{48}$$

$$\textbf{irreflexive:} \quad \text{iff } R \cap id = \bot$$

$$\textbf{connected:} \quad \text{iff } R \cup R^\circ = \top \tag{49}$$

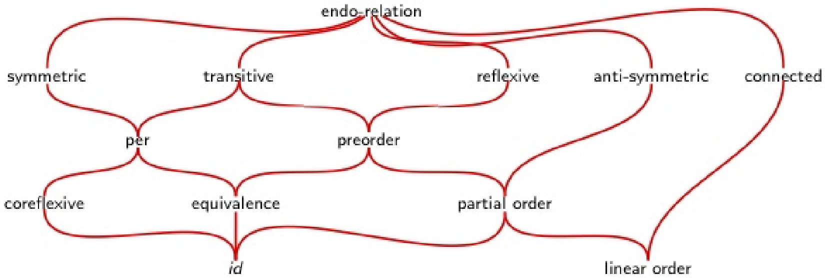
where, in general, for R, S of the same type:

$$b\ (R \cap S)\ a \quad \equiv \quad b\ R\ a \wedge b\ S\ a \tag{50}$$

$$b\ (R \cup S)\ a \quad \equiv \quad b\ R\ a \vee b\ S\ a \tag{51}$$

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: $age\ y \leqslant age\ x$.
- **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: $age\ y = age\ x$. [3]
- **Pers** are partial equivalences
  Example: $y\ \mathit{IsBrotherOf}\ x$.

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

Exercises

Exercise 16: Consider the relation

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

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

Exercise 17: Check which of the following properties,

transitive, symmetric, anti-symmetric, connected

hold for the relation *Eats* of exercise 10. □

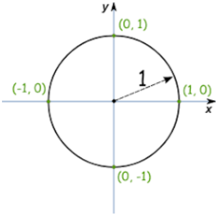
Exercises

Exercise 18: Let $\mathbb{R} \xleftarrow{R} \mathbb{R}$ be the binary relation that defines the unit circunference,

$$y \; R \; x \quad \stackrel{\text{def}}{=} \quad y^2 + x^2 = 1 \qquad (52)$$

that is,

$$R = \frac{(1-) \cdot sq}{sq} \qquad (53)$$



where $sq : \mathbb{R} \to \mathbb{R}$ and $(1-) : \mathbb{R} \to \mathbb{R}$ are the functions $y = x^2$ e $y = 1 - x$, respectively.

Without using (52), show that R is **symmetric**. $\square$

Exercises

Exercise 19: 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 20: Expand criteria (46) to (49) to pointwise notation. □

Exercises

Exercise 21: The teams (T) of a football league play games (G) at home or away, and every game takes place in some date:

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

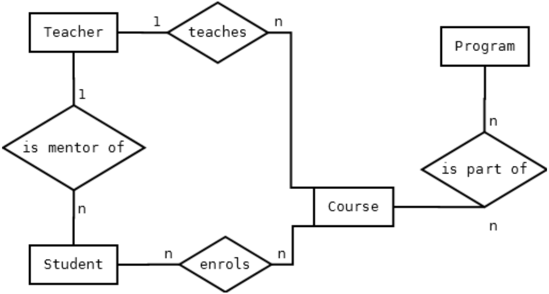
Moreover, *(a) No team can play two games on the same date; (b) All teams play against each other but not against themselves; (c) For each home game there is another game away involving the same two teams.* Show that

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

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

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 22: Looking at diagram (56),

- Specify the property *mentors of students necessarily are among their teachers* in the relational pointfree style.
- Why is

$$\frac{\mathit{teaches}}{\mathit{isMentorOf}} \subseteq \mathit{Enrols}$$

inadequate as answer to the previous question?

$\square$

Class 4 – Meet and Join

Background — Eindhoven quantifier calculus

Trading:

$$\langle \forall\ k : \phi \wedge \varphi : \gamma \rangle = \langle \forall\ k : \phi : \varphi \Rightarrow \gamma \rangle \tag{57}$$
$$\langle \exists\ k : \phi \wedge \varphi : \gamma \rangle = \langle \exists\ k : \phi : \varphi \wedge \gamma \rangle \tag{58}$$

de Morgan:

$$\neg \langle \forall\ k : \phi : \gamma \rangle = \langle \exists\ k : \phi : \neg\, \gamma \rangle \tag{59}$$
$$\neg \langle \exists\ k : \phi : \gamma \rangle = \langle \forall\ k : \phi : \neg\, \gamma \rangle \tag{60}$$

One-point:

$$\langle \forall\ k : k = e : \gamma \rangle = \gamma[k := e] \tag{61}$$
$$\langle \exists\ k : k = e : \gamma \rangle = \gamma[k := e] \tag{62}$$

Background — Eindhoven quantifier calculus

Nesting:

$$\langle\forall\, a, b : \phi \wedge \varphi : \gamma\rangle = \langle\forall\, a : \phi : \langle\forall\, b : \varphi : \gamma\rangle\rangle \tag{63}$$

$$\langle\exists\, a, b : \phi \wedge \varphi : \gamma\rangle = \langle\exists\, a : \phi : \langle\exists\, b : \varphi : \gamma\rangle\rangle \tag{64}$$

Rearranging-∀:

$$\langle\forall\, k : \phi \vee \varphi : \gamma\rangle = \langle\forall\, k : \phi : \gamma\rangle \wedge \langle\forall\, k : \varphi : \gamma\rangle \tag{65}$$

$$\langle\forall\, k : \phi : \gamma \wedge \varphi\rangle = \langle\forall\, k : \phi : \gamma\rangle \wedge \langle\forall\, k : \phi : \varphi\rangle \tag{66}$$

Rearranging-∃:

$$\langle\exists\, k : \phi : \gamma \vee \varphi\rangle = \langle\exists\, k : \phi : \gamma\rangle \vee \langle\exists\, k : \phi : \varphi\rangle \tag{67}$$

$$\langle\exists\, k : \phi \vee \varphi : \gamma\rangle = \langle\exists\, k : \phi : \gamma\rangle \vee \langle\exists\, k : \varphi : \gamma\rangle \tag{68}$$

Splitting:

$$\langle\forall\, j : \phi : \langle\forall\, k : \varphi : \gamma\rangle\rangle = \langle\forall\, k : \langle\exists\, j : \phi : \varphi\rangle : \gamma\rangle \tag{69}$$

$$\langle\exists\, j : \phi : \langle\exists\, k : \varphi : \gamma\rangle\rangle = \langle\exists\, k : \langle\exists\, j : \phi : \varphi\rangle : \gamma\rangle \tag{70}$$

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.
IBSN 0138218846.