Event B: Sets, Relations, Functions, Data Structures[1]

Manuel Carro
manuel.carro@upm.es

IMDEA Software Institute &
Universidad Politécnica de Madrid

[1]Many slides borrowed from J. R. Abrial: see http://wiki.event-b.org/index.php/Event-B_Language

First-order predicate calculus: informal

We have a universe of objects. We make statements about these objects. *Sweet Reason* [HGTA11] is a delightful introduction to logic with examples.

$\forall x \cdot P(x)$: For all elements x, P holds. P can be arbitrarily complex.

$\exists x \cdot P(x)$: For some element x, P holds. P can be arbitrarily complex.

First-order predicate calculus: informal

$l(x, y)$ — x loves y

$\forall x \cdot \forall y \cdot l(x, y)$

$\exists x \cdot \exists y \cdot l(x, y)$

$\forall x \cdot \exists y \cdot l(x, y)$

$\exists y \cdot \forall x \cdot l(x, y)$

$\forall y \cdot \exists x \cdot l(x, y)$

$\exists x \cdot \forall y \cdot l(x, y)$

$\forall x \cdot \neg l(x, x)$

$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	
$\forall x \cdot \exists y \cdot l(x, y)$	
$\exists y \cdot \forall x \cdot l(x, y)$	
$\forall y \cdot \exists x \cdot l(x, y)$	
$\exists x \cdot \forall y \cdot l(x, y)$	
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	
$\exists y \cdot \forall x \cdot l(x, y)$	
$\forall y \cdot \exists x \cdot l(x, y)$	
$\exists x \cdot \forall y \cdot l(x, y)$	
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	
$\forall y \cdot \exists x \cdot l(x, y)$	
$\exists x \cdot \forall y \cdot l(x, y)$	
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	there is someone who is loved by everybody
$\forall y \cdot \exists x \cdot l(x, y)$	
$\exists x \cdot \forall y \cdot l(x, y)$	
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	there is someone who is loved by everybody
$\forall y \cdot \exists x \cdot l(x, y)$	everybody is loved by someone
$\exists x \cdot \forall y \cdot l(x, y)$	
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	there is someone who is loved by everybody
$\forall y \cdot \exists x \cdot l(x, y)$	everybody is loved by someone
$\exists x \cdot \forall y \cdot l(x, y)$	there is someone who loves everybody
$\forall x \cdot \neg l(x, x)$	
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	there is someone who is loved by everybody
$\forall y \cdot \exists x \cdot l(x, y)$	everybody is loved by someone
$\exists x \cdot \forall y \cdot l(x, y)$	there is someone who loves everybody
$\forall x \cdot \neg l(x, x)$	no one loves themself
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: informal

$l(x, y)$	x loves y
$\forall x \cdot \forall y \cdot l(x, y)$	everyone loves everyone else (including themself)
$\exists x \cdot \exists y \cdot l(x, y)$	at least a person loves someone (perhaps themself)
$\forall x \cdot \exists y \cdot l(x, y)$	everybody loves someone
$\exists y \cdot \forall x \cdot l(x, y)$	there is someone who is loved by everybody
$\forall y \cdot \exists x \cdot l(x, y)$	everybody is loved by someone
$\exists x \cdot \forall y \cdot l(x, y)$	there is someone who loves everybody
$\forall x \cdot \neg l(x, x)$	no one loves themself
$\forall x \cdot \exists y \cdot l(x, y) \Rightarrow x \neq y$	everybody loves someone else

We usually want to prove these statements true or false. We use inference rules to prove truth or falsehood.

First-order predicate calculus: inference rules

$$\frac{H,\ \forall x \cdot P(x),\ P(E)\ \vdash\ Q}{H,\ \forall x \cdot P(x)\ \vdash\ Q}\ \textbf{ALL\_L} \qquad \frac{H\ \vdash\ P(x)}{H\ \vdash\ \forall x \cdot P(x)}\ \textbf{ALL\_R}$$

$$\frac{H,\ P(x)\ \vdash\ Q}{H,\ \exists x \cdot P(x)\ \vdash\ Q}\ \textbf{XST\_L} \qquad \frac{H\ \vdash\ P(E)}{H\ \vdash\ \exists x \cdot P(x)}\ \textbf{XST\_R}$$

- **E** is an expression. Nobody tells you which one works.
- In **ALL_R**, **x** not free in **H**.
- In **XST_L**, **x** not free in **H** and **Q**.

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg\exists x \cdot \neg P(x)$$

(definition of existential quantifier)

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg\exists x \cdot \neg P(x)$$

(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x,y) \Rightarrow \forall y \cdot \exists x \cdot P(x,y)$$

(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x,y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x,y)$$

(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg\exists x \cdot \neg P(x)$$

(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x,y) \Rightarrow \forall y \cdot \exists x \cdot P(x,y)$$

(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x,y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x,y)$$

(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg \exists x \cdot \neg P(x)$$
(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x, y) \Rightarrow \forall y \cdot \exists x \cdot P(x, y)$$
(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x, y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x, y)$$
(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

When $x \notin vars(B)$:

$$\forall x \cdot (P(x) \Rightarrow B) \equiv (\exists x \cdot P(x)) \Rightarrow B$$
(Prove it!)

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg \exists x \cdot \neg P(x)$$
(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x, y) \Rightarrow \forall y \cdot \exists x \cdot P(x, y)$$
(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x, y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x, y)$$
(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

When $x \notin vars(B)$:

$$\forall x \cdot (P(x) \Rightarrow B) \equiv (\exists x \cdot P(x)) \Rightarrow B$$
(Prove it!)

$$\forall x \cdot P(x) \wedge Q(x) \equiv (\forall x \cdot P(x)) \wedge (\forall x \cdot Q(x))$$

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg \exists x \cdot \neg P(x)$$
(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x, y) \Rightarrow \forall y \cdot \exists x \cdot P(x, y)$$
(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x, y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x, y)$$
(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

When $x \notin vars(B)$:

$$\forall x \cdot (P(x) \Rightarrow B) \equiv (\exists x \cdot P(x)) \Rightarrow B$$
(Prove it!)

$$\forall x \cdot P(x) \wedge Q(x) \equiv (\forall x \cdot P(x)) \wedge (\forall x \cdot Q(x))$$

$$\exists x \cdot P(x) \vee Q(x) \equiv (\exists x \cdot P(x)) \vee (\exists x \cdot Q(x))$$

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg \exists x \cdot \neg P(x)$$
(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x, y) \Rightarrow \forall y \cdot \exists x \cdot P(x, y)$$
(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x, y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x, y)$$
(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

When $x \notin vars(B)$:

$$\forall x \cdot (P(x) \Rightarrow B) \equiv (\exists x \cdot P(x)) \Rightarrow B$$
(Prove it!)

$$\forall x \cdot P(x) \wedge Q(x) \equiv (\forall x \cdot P(x)) \wedge (\forall x \cdot Q(x))$$

$$\exists x \cdot P(x) \vee Q(x) \equiv (\exists x \cdot P(x)) \vee (\exists x \cdot Q(x))$$

$$\forall x \cdot P(x) \vee Q(x) \not\equiv (\forall x \cdot P(x)) \vee (\forall x \cdot Q(x))$$
(example?)

Some deductions and (non) equivalences

$$\forall x \cdot P(x) \equiv \neg\exists x \cdot \neg P(x)$$
(definition of existential quantifier)

$$\exists x \cdot \forall y \cdot P(x,y) \Rightarrow \forall y \cdot \exists x \cdot P(x,y)$$
(If LHS true, there some fixed a s.t. $\forall y \cdot P(a, Y)$)

$$\forall y \cdot \exists x \cdot P(x,y) \not\Rightarrow \exists x \cdot \forall y \cdot P(x,y)$$
(If LHS true, x may depend on each y, i.e., there may **not** be a single a s.t. $\forall y \cdot P(a, Y)$)

$$P(a) \Rightarrow \exists x \cdot P(x)$$

When $x \notin vars(B)$:

$$\forall x \cdot (P(x) \Rightarrow B) \equiv (\exists x \cdot P(x)) \Rightarrow B$$
(Prove it!)

$$\forall x \cdot P(x) \wedge Q(x) \equiv (\forall x \cdot P(x)) \wedge (\forall x \cdot Q(x))$$

$$\exists x \cdot P(x) \vee Q(x) \equiv (\exists x \cdot P(x)) \vee (\exists x \cdot Q(x))$$

$$\forall x \cdot P(x) \vee Q(x) \not\equiv (\forall x \cdot P(x)) \vee (\forall x \cdot Q(x))$$
(example?)

$$\exists x \cdot P(x) \wedge Q(x) \not\equiv (\exists x \cdot P(x)) \wedge (\exists x \cdot Q(x))$$
(example?)

Set theory: membership

- Set: well-defined collection of distinct objects.
- Can be finite or infinite.
- Primary predicate: membership

$$E \in S$$

- E is an expression, S is a set.

Set theory: basic constructs

$S = \{1,2,3,4,5,6\}$ $\quad T = \{a,b,c,d\}$ $\quad R(x) \equiv x \mod 2 = 0$

S and T are sets, R is a predicate, x is a variable.

Basic constructs

Cartesian product	$S \times T$	$\{(a,1),(a,2),\ldots,(a,6),(b,1),\ldots,(d,6)\}$
Power set	$\mathcal{P}(S)$	$\{\varnothing,\{a\},\{a,b\},\ldots,\{a,e\},\ldots,\{a,b,c,d\}\}$
Comprehension	$\{x \mid x \in S \wedge R(x)\}$	$\{2,4,6\}$
Comprehension 2	$\{x \cdot x \in S \wedge R(x) \mid x * x\}$	$\{4,16,36\}$

Notation: tuples $(a,1)$ are written $a \mapsto 1$.

See the reference card for information on how to input these in Rodin.

Set theory: basic constructs
Examples

Shortcut: $m..n \equiv \{x \in \mathbb{Z} \mid m \leq x \wedge x \leq n\}$

- $\{x \mid x \in \mathbb{N} \wedge x < 2\} \times 8..10$
- $\{x \cdot x \in 3..5 \mid x \mapsto x * x\}$
- $\{n \cdot n \in \mathbb{N} \mid (0..n) \mapsto n\}$
- $\{x, y \cdot x \mapsto y \in 1..3 \times 2..4 \mid x + y\}$

Operations on sets

$S \subseteq T$	Inclusion
$S = T$	Equality
$S \subset T$	Strict inclusion
$S \cup T$	Union
$S \cap T$	Intersection
$S \setminus T$	Difference
$E \in \{a, \ldots, z\}$	Membership
$E \in \varnothing$	$\perp$
$\lvert S \rvert$	number of elements

- Operators based on membership and logic operations (see the reference slide).
- $E \notin T \equiv \neg(E \in T)$.
- Also: generalized / conditional union and intersection (see reference cards).

Binay relations

- A binary relation r is a set of tuples:
  $r \subseteq S \times T$
- Notation: $r \in S \leftrightarrow T$
  - $S \leftrightarrow T$: the set of all the possible relationships between S and T.
  - $S \leftrightarrow T \equiv \mathcal{P}(S \times T)$
  - The relation r would be one of these relationships.
- $r \in 1..3 \leftrightarrow 7..11$
  - $r = \{1 \mapsto 10, 2 \mapsto 7, 2 \mapsto 11\}$
  - $4 \mapsto 10 \notin r$
- $dom(r) = \{1, 2\}$ (note $3 \notin dom(r)$)
- $ran(r) = \{10, 7, 11\}$ (note $8, 9 \notin ran(r)$)
- $r^{-1} = \{10 \mapsto 1, 7 \mapsto 2, 11 \mapsto 2\}$

- $r \in \{\text{meat}, \text{fish}, \text{pasta}, \text{bacon}\} \leftrightarrow \{\text{carbs}, \text{protein}, \text{fat}\}$ write one relation.
- Relation of $dom(r)$, $ran(r)$ with S and T
- Given S and T, how many different r may there be?

Types of relations

Total	$S \leftarrow\!\!\!\!\leftrightarrow T$	$r \in S \leftrightarrow T \wedge dom(r) = S$
Surjective	$S \leftrightarrow\!\!\!\!\rightarrow T$	$r \in S \leftrightarrow T \wedge ran(r) = T$
Both	$S \twoheadleftarrow\!\!\!\!\twoheadrightarrow T$	$r \in S \leftrightarrow\!\!\!\!\rightarrow T \wedge r \in S \leftarrow\!\!\!\!\leftrightarrow T$

Sets and relations are very useful modeling tools!

Choosing the right type of relation helps (automatically) capture problem conditions.

Operations on relations

Domain restriction	$S \lhd r$	Tuples in r with first component in S
Domain subtraction	$S \unlhd r$	Tuples in r with first component not in S
Range restriction	$r \rhd T$	Tuples in r with second component in T
Range subtraction	$r \unrhd T$	Tuples in r with second component not in T

Let us study the relation $Prey \in Animal \leftrightarrow Animal$.

Operations on relations

Domain restriction	$S \lhd r$	Tuples in r with first component in S
Domain subtraction	$S \mathbin{⩤} r$	Tuples in r with first component not in S
Range restriction	$r \rhd T$	Tuples in r with second component in T
Range subtraction	$r \mathbin{⩥} T$	Tuples in r with second component not in T

Let us study the relation $Prey \in Animal \leftrightarrow Animal$.

We assume $Prey$ *contains* $hunter \mapsto hunted$.

- $Mammal \lhd Prey$
- $Mammal \mathbin{⩤} Prey$
- $Prey \rhd Spiders$
- $Fish \lhd (Prey \rhd Spiders)$
- $Spiders \mathbin{⩤} (Prey \rhd Spiders)$

Operations on relations

Image	$r[S]$	Set of rhs of tuples with lhs in S
Composition	$p; q$	*Chain* the relations p and q
Overriding	$p \mathbin{\lhd\!\!\!+} q$	Add tuples in q to p, override whose with same lhs
Identity	$id(S)$	Relate every element with itself

$\{1 \mapsto a, 1 \mapsto c, 2 \mapsto b, 2 \mapsto c, 3 \mapsto d\}[\{1,2\}] = \{a, b, c\}$

$\{1 \mapsto a, 1 \mapsto c, 2 \mapsto b\}; \{a \mapsto \alpha, a \mapsto \beta, b \mapsto \delta, b \mapsto \alpha\} = \{1 \mapsto \alpha, 1 \mapsto \beta, 2 \mapsto \delta, 2 \mapsto \alpha\}$

$\{1 \mapsto a, 1 \mapsto c, 2 \mapsto b, 3 \mapsto d\} \mathbin{\lhd\!\!\!+} \{1 \mapsto d, 2 \mapsto e, 4 \mapsto f\} = \{1 \mapsto d, 2 \mapsto e, 3 \mapsto d, 4 \mapsto f\}$

$id(\{a, b, c\}0 = \{a \mapsto a, b \mapsto b, c \mapsto c\}$

Image: $r[S] \equiv ran(S \lhd r)$

Functions

- Functions: one type of relation.
- Function f: set of tuples $x \mapsto y$
- Notation: $f(x) = y$
- *Every element in domain relates only to one element in range.*

$$f(x) = y \wedge f(x) = z \Rightarrow y = z$$

- WD conditions to evaluate $f(x)$:
  - $f \in S \mathbin{⇸} T$
  - $x \in \mathrm{dom}(f)$
- Use right kind of function: captures conditions, makes it possible to use specific inference rules.

Total function ($dom(f) = S$)	$S \to T$
Partial function	$S \mathbin{⇸} T$
Injection: if $f(x) = f(y)$, then $x = y$.	
Partial injection	$S \mathbin{⤔} T$
Total injection	$S \rightarrowtail T$
Surjection: $f \in S \leftrightarrow T$, $ran(f) = T$.	
Partial surjection	$S \mathbin{⤀} T$
Total surjection	$S \twoheadrightarrow T$
Injective and surjective	
Bijection	$S \mathbin{⤖} T$

Defining and using functions

Misc. examples

$f \in 1..5 \mathbin{⇸} \{a, b, c\}$ (partial)
$g \in 1..5 \to \{a, b, c\}$ (total)

- Initialization:
  - $f := \varnothing$ (f is a set!)
  - $f(2) := b$ ($\equiv f = \{2 \mapsto b\}$)
  - $g := 1..5 \times \{a\}$
    $g = \{1 \mapsto a, \ldots, 5 \mapsto a\}$
    $\mathrm{ran}(g) = \{a\}$
- Update:
  - $g(2) := b \quad \equiv$
    $g := (\{2\} \mathbin{⩤} g) \cup \{2 \mapsto b\} \quad \equiv$
    $g := g \mathbin{\lhd\!\!\!+} \{2 \mapsto b\}$
  - $g(2) := g(2) + 1 \quad \equiv$
    $g := (\{2\} \mathbin{⩤} g) \cup \{2 \mapsto g(2) + 1\} \quad \equiv$
    $g := g \mathbin{\lhd\!\!\!+} \{2 \mapsto g(2) + 1\}$

- Computing differences:
  $f \in 1..K \to \mathbb{N}$
  $df \in 1..K - 1 \to \mathbb{Z}$
  $df := \{i \cdot i \in \mathrm{dom}(df) \mid i \mapsto f(i+1) - f(i)\}$
- Characteristic function of a set:
  $s \subseteq T \quad f_s \in T \to 0..1$
  $f_s := (\{i \mid i \in s\} \times \{1\}) \cup$
  $(\{i \mid i \in T \setminus s\} \times \{0\})$
- Higher order:
  $so \in \mathbb{N} \mathbin{⇸} (\mathbb{N} \mathbin{⇸} \mathbb{N})$
  $so := \{1 \mapsto \{10 \mapsto 5, 11 \mapsto 4\},$
  $2 \mapsto \{10 \mapsto 4, 12 \mapsto 3\}\}$
  $so(2) \leadsto \{10 \mapsto 4, 12 \mapsto 3\}$
  $so(2)(10) \leadsto 4$

An example of functions and relations: a strict society

Every person is man or woman $men \subseteq PERSON$

An example of functions and relations: a strict society

Every person is man or woman $men \subseteq PERSON$
No person is man and woman $women = PERSON \setminus men$

An example of functions and relations: a strict society

Every person is man or woman $men \subseteq PERSON$
No person is man and woman $women = PERSON \setminus men$
Women have husbands (men)
At most one husband per woman $husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+\;\,} men$
Men at most one wife

An example of functions and relations: a strict society

Every person is man or woman $men \subseteq PERSON$
No person is man and woman $women = PERSON \setminus men$
Women have husbands (men)
At most one husband per woman $husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+\;\,} men$
Men at most one wife
Mother are married women $mother \in PERSON \mathrel{\rightarrow\!\!\!\!\!+\;} \mathrm{dom}(husband)$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \text{ ⤔ } men$
Men at most one wife	
Mother are married women	$mother \in PERSON \text{ ⇸ } \mathrm{dom}(husband)$

Some derived relations

$wife =$
$spouse =$
$father =$
$children =$
$daughter =$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \text{ ⤔ } men$
Men at most one wife	
Mother are married women	$mother \in PERSON \text{ ⇸ } \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse =$
$father =$
$children =$
$daughter =$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \text{ ⤔ } men$
Men at most one wife	
Mother are married women	$mother \in PERSON \text{ ⇸ } \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father =$
$children =$
$daughter =$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \text{ ⤔ } men$
Men at most one wife	
Mother are married women	$mother \in PERSON \text{ ⇸ } \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father = mother ; husband$
$children =$
$daughter =$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+} men$
Men at most one wife	
Mother are married women	$mother \in PERSON \nrightarrow \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father = mother ; husband$
$children = (mother \cup father)^{-1}$

$daughter =$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+} men$
Men at most one wife	
Mother are married women	$mother \in PERSON \nrightarrow \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father = mother ; husband$
$children = (mother \cup father)^{-1}$

$daughter = women \lhd children$
$sibling =$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+} men$
Men at most one wife	
Mother are married women	$mother \in PERSON \nrightarrow \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father = mother ; husband$
$children = (mother \cup father)^{-1}$

$daughter = women \lhd children$

$sibling = (children^{-1} ; children) \setminus \mathrm{id}(PERSON)$
$brother =$

An example of functions and relations: a strict society

Every person is man or woman	$men \subseteq PERSON$
No person is man and woman	$women = PERSON \setminus men$
Women have husbands (men)	
At most one husband per woman	$husband \in women \mathrel{\rightarrowtail\!\!\!\!\!\!+} men$
Men at most one wife	
Mother are married women	$mother \in PERSON \nrightarrow \mathrm{dom}(husband)$

Some derived relations

$wife = husband^{-1}$
$spouse = husband \cup wife$
$father = mother ; husband$
$children = (mother \cup father)^{-1}$

$daughter = women \lhd children$
$sibling = (children^{-1} ; children) \setminus \mathrm{id}(PERSON)$

$brother = sibling \rhd men$

Arithmetic

- The usual (+, -, *, $\div$) plus: mod, ^ (power).
- card(set), min(set), max(set)

Data structures

- Data structures with pointers: formalized with relations, functions.
- Axioms give *properties* of the functions that model data structures.
- Specific forms of these axioms (capturing induction on the data structures) well-suited to be used in automated proofs.
- We will formalize:
  - (In)Finite lists.
  - (In)Finite trees.
- Others (circular lists, graphs) possible, more involved.

Infinite lists

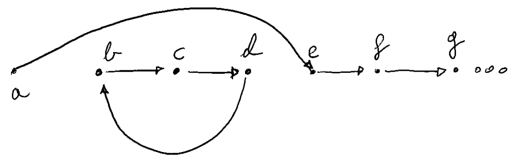
- Set V of list nodes.
- Initial node f.
- Bijective *next* function

axm_1 : $\quad f \in V$

axm_2 : $\quad n \in V \rightarrowtail\!\!\!\!\rightarrow V \setminus \{f\}$

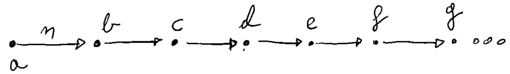
Note: isomorphic to natural numbers with $V = \mathbb{N}$, $f = 0$, $n = succ$.

Avoiding cycles



$S = \{b, c, d\} \quad n[S] = \{b, c, d\}$

$S \subseteq n[S]$



$S = \{b, c, d\} \quad n[S] = \{c, d, e\}$

$S \nsubseteq n[S]$

Avoiding cycles

- If a list has a cycle, then there is a $S \subseteq V$ s.t. $S \subseteq n[S]$.
- On the other hand, it is always the case that $\varnothing \subseteq n[\varnothing]$.
- So we insist that this is the only case:

$$\text{axm\_3} : \forall S \cdot S \subseteq V \land S \subseteq n[S] \Rightarrow S = \varnothing$$

- It can be used to prove properties in infinite lists!
- In particular, to derive an scheme for (strong) induction.

From absence of cycles to induction

$$\forall S \cdot S \subseteq V \land S \subseteq n[S] \Rightarrow S = \varnothing$$

S can be written $S = V \setminus T$ (for some T). Then:

Redundant

$$\forall S \cdot S = V \setminus T \land \boxed{S \subseteq V} \land S \subseteq n[S] \Rightarrow S = \varnothing$$

$$\forall S \cdot S = V \setminus T \land S \subseteq n[S] \Rightarrow \boxed{S = \varnothing}$$

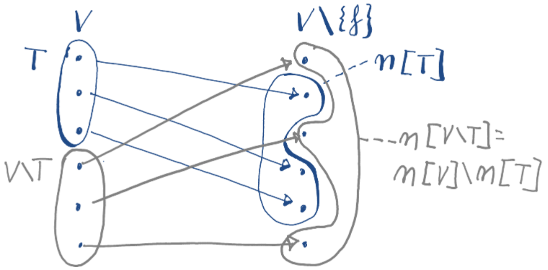
$$V \setminus T = \varnothing \equiv V \subseteq T$$

$$\forall S \cdot S = V \setminus T \land S \subseteq n[S] \Rightarrow V \subseteq T$$

From absence of cycles to induction

$$\forall S \cdot S = V \setminus T \land S \subseteq \boxed{n[S]} \Rightarrow V \subseteq T$$

n bijective: $n[V \setminus T] = n[V] \setminus n[T]$
(because $n[S]$ and $n[T]$ don't intersect)



From absence of cycles to induction

$$S \subseteq n[S] \rightsquigarrow V \setminus T \subseteq n[V \setminus T] = n[V] \setminus n[T]$$

By definition: $f \in V$, $f \notin n[V \setminus T]$

Since $V \setminus T \subseteq n[V \setminus T]$, $f \notin V \setminus T$

Therefore $f \in T$ so that $f \notin V \setminus T$

And $n[V] = V \setminus \{f\}$

From absence of cycles to induction

$V\setminus T \subseteq n[V]\setminus n[T]$

$\boxed{V\setminus T} \subseteq (V\setminus\{f\}) \setminus \boxed{n[T]}$

...we will have no elements here

If we remove too much from here...

Condition: $n[T] \subseteq T$

From absence of cycles to induction

All together:

$\forall S \cdot S = \boxed{V}\setminus\boxed{T} \wedge f \in T \wedge n[T] \subseteq T \Rightarrow V \subseteq T$

Fixed   Variable

$\forall T \cdot f \in T \wedge n[T] \subseteq T \Rightarrow V \subseteq T$

T extension of a predicate:

$x \in T \leftrightarrow P(x)$ or $T = \{x \mid P(x)\}$

From absence of cycles to induction

$$\forall T \cdot f \in T \wedge n[T] \subseteq T \Rightarrow V \subseteq T$$

If we expand $n[T] \subseteq T$:

$$\forall T \cdot f \in T \wedge (\forall x \cdot x \in T \Rightarrow n(x) \in T) \Rightarrow V \subseteq T$$

- T set of elements with some property P: $T = \{x|P(x)\}$
- If:
  - Initial node f has property P ($f \in T$), and
  - For every element with property P ($x \in T$), the next one has property P ($n(x) \in T$), then
  - All elements have property P ($V \subseteq T$).
- Equivalently:
  $\underline{\forall P} \cdot P(f) \wedge (\forall x \cdot P(x) \Rightarrow P(n(x))) \Rightarrow (\forall x \cdot x \in V \Rightarrow P(x))$

Using thm_2 to prove list properties

- We want to prove $P(x)$ for all $x \in V$.
- Elements for which P holds:
  $T = \{x|x \in V \wedge P(X)\}$.
- We want to prove that $T = V$.
- Since clearly $T \subseteq V$, it is enough to prove $V \subseteq T$.
- We do that by instantiating T:
  $T \equiv \{x|x \in V \wedge P(x)\}$.

$$\begin{array}{rl} f \in \{x|x \in V \wedge P(x)\} & \wedge \\ (\forall x \cdot x \in \{x|x \in V \wedge P(x)\} \Rightarrow n(x) \in \{x|x \in V \wedge P(x)\}) & \Rightarrow \\ V \subseteq \{x|x \in V \wedge P(x)\} & \end{array}$$

- $f \in \{x|x \in V \wedge P(x)\} \equiv P(f)$.
- Second part equivalent to
  $\forall x \cdot x \in V \wedge P(x) \Rightarrow P(n(x))$.
- The RHS is equivalent to
  $\forall x \cdot x \in V \Rightarrow P(x)$.

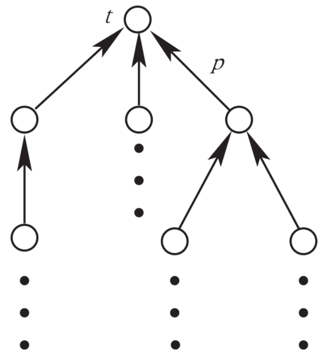
Instantiating thm_2 gives a scheme to prove by induction in infinite lists.

Finite lists

- As infinite lists, but including a last (l) element.
- This needs a different axiom 2:

$$
\begin{aligned}
\text{axm\_4}: &\quad l \in V \\
\text{axm\_5}: &\quad \text{finite}(V) \\
\text{axm\_2}': &\quad n \in V \setminus \{l\} \rightarrowtail\!\!\!\!\twoheadrightarrow V \setminus \{f\}
\end{aligned}
$$

Infinite trees



- t is the root.
- p relates every node with its parent (it is a surjection).

- There should not be cycles.

$$
\begin{aligned}
\text{axm\_1}: &\quad t \in V \\
\text{axm\_2}: &\quad p \in V \setminus \{t\} \twoheadrightarrow V \\
\text{axm\_3}: &\quad \forall S \cdot S \subseteq p^{-1}[S] \Rightarrow S = \varnothing
\end{aligned}
$$

Induction rule:

$$\forall T \cdot t \in T \land p^{-1}[T] \subseteq T \Rightarrow V \subseteq T$$

Instantiation to prove properties:

$$
\begin{aligned}
\forall T \cdot \quad & T \subseteq V \land t \in T \land \\
& (\forall x \cdot x \in V \setminus \{t\} \land p(x) \in T \Rightarrow x \in T) \\
& \Rightarrow V \subseteq T
\end{aligned}
$$

Finite trees

- t is the root.
- p relates every node with its parent.
- L is the set of tree leaves.
- There should not be cycles.

$$
\begin{aligned}
\text{axm\_1}: &\quad t \in V \\
\text{axm\_2}: &\quad L \subseteq V \\
\text{axm\_3}: &\quad p \in V \setminus \{t\} \twoheadrightarrow V \setminus L \\
\text{axm\_4}: &\quad \forall S \cdot S \subseteq p^{-1}[S] \Rightarrow S = \varnothing
\end{aligned}
$$

Set theory: basic constructs

Definitions

Defined by equivalences (included here for reference)

$$
\begin{aligned}
E \mapsto F \in S \times T &\quad\equiv\quad E \in S \land F \in T \\
S \in \mathbb{P}(T) &\quad\equiv\quad \forall x \cdot x \in S \Rightarrow x \in T \\
E \in \{x \cdot x \in S \land P(x) \mid F(x)\} &\quad\equiv\quad \exists x \cdot x \in S \land P(x) \land E = F(x) \\
E \in \{x \mid x \in S \land P(x)\} &\quad\equiv\quad E \in S \land P(E)
\end{aligned}
$$

Operations on sets: definitions

$$
\begin{array}{rcl}
S \subseteq T & \equiv & S \in \mathbb{P}(T) \\
S = T & \equiv & S \subseteq T \wedge T \subseteq S \\
S \subset T & \equiv & S \in \mathbb{P}(T) \wedge \neg(S = T) \\
S \cup T & \equiv & \{x \mid x \in S \vee x \in T\} \\
S \cap T & \equiv & \{x \mid x \in S \wedge x \in T\} \\
S \setminus T & \equiv & \{x \mid x \in S \wedge x \notin T\} \\
E \in \{a, \ldots, z\} & \equiv & E = a \vee \ldots \vee E = z \\
E \in \varnothing & \equiv & \perp
\end{array}
$$

Relations

$$
\begin{array}{rcl}
x \in dom(r) & \equiv & \exists y \cdot x \mapsto y \in r \\
y \in ran(r) & \equiv & \exists x \cdot x \mapsto y \in r \\
r^{-1} & \equiv & \{y \mapsto x \mid x \mapsto y \in r\}
\end{array}
$$

Domain restriction	$S \lhd r$	$\{x \mapsto y \in r \mid x \in S\}$
Domain subtraction	$S ⩤ r$	$\{x \mapsto y \in r \mid x \notin S\}$
Range restriction	$r \rhd T$	$\{x \mapsto y \in r \mid y \in T\}$
Range subtraction	$r ⩥ T$	$\{x \mapsto y \in r \mid y \notin T\}$

Image	$r[S]$	$\{y \mid x \mapsto y \in r \wedge x \in S\}$
Composition	$p; q$	$\{x \mapsto z \mid x \mapsto y \in p \wedge y \mapsto z \in q\}$
Overriding	$p \mathbin{\lhd\!\!\!+} q$	$q \cup (dom(q) ⩤ p)$
Identity	$id(S)$	$\{x \mapsto x \mid x \in S\}$

For reference: some useful results and definitions

$$
\begin{array}{rcl}
(r^{-1})^{-1} & = & r \\
\mathrm{dom}(r^{-1}) & = & \mathrm{ran}(r) \\
(S \lhd r)^{-1} & = & r^{-1} \rhd S \\
(p; q)^{-1} & = & q^{-1}; p^{-1} \\
p; (q; r) & = & (p; q); r \\
p; (q \cup r) & = & (p; q) \cup (p; r) \\
(p; q)[S] & = & q[p[S]] \\
r[S \cup T] & = & r[S] \cup r[T]
\end{array}
$$

$r = r^{-1}$	symmetric
$r \cap r^{-1} = \varnothing$	asymmetric
$\mathrm{id}(S) \subseteq r$	reflexive
$r; r \subseteq r$	transitive

Set-theoretic notation more readable than predicate calculus

$$r = r^{-1} \equiv \forall x, y \cdot x \in S \wedge y \in S \Rightarrow (x \mapsto y \in r \Leftrightarrow y \mapsto x \in r)$$

Properties

$$
\begin{array}{rcl}
mother & = & father; wife \\
spouse & = & spouse^{-1} \\
sibling & = & sibling^{-1} \\
cousin & = & cousin^{-1} \\
father; father^{-1} & = & mother; mother^{-1} \\
father; mother^{-1} & = & \varnothing \\
mother; father^{-1} & = & \varnothing \\
father; children & = & mother; children
\end{array}
$$

James M. Henle, Jay L. Garfield, Thomas Tymoczko, and Emily Altreuter.
Sweet Reason: A Field Guide to Modern Logic.
Wiley-Blackwell, 2nd edition, 211.
ISBN: 978-1-444-33715-0.