Event B: Sets, Relations, Functions, Arithmetic[1]

Manuel Carro
manuel.carro@upm.es

Universidad Politécnica de Madrid &
IMDEA Software Institute

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

Set theory: membership

- Event-B formal reasoning is built based on:
  - First-order logic inference rules (seen).
  - Set theory (to be touched upon).
- Set theory as a foundation for relations, functions (and, therefore, data structures).
  - Proofs often reduced to proving goals on sets.
- We will briefly see how this is intuitively done.

Set theory: membership

- A set is a well-defined collection of distinct objects.
- Set theory is based on the membership predicate

$$E \in S$$

- E is an expression, S is a set.

Definitions

There are three basic constructs in set theory, defined by equivalences.
S and T are sets, x is a variable, P is a predicate, F is an expression.

Cartesian product: $S \times T$

$$E \mapsto F \in S \times T \equiv E \in S \land F \in T$$

Powerset: $\mathbb{P}(T)$

$$S \in \mathbb{P}(T) \equiv \forall x \cdot x \in S \Rightarrow x \in T$$

Comprehension:

Version 1: $\{x \mid x \in S \land P(x)\}$

$$E \in \{x \mid x \in S \land P(x)\} \equiv E \in S \land P(E)$$

Version 2: $\{x \cdot x \in S \land P(x) \mid F(x)\}$

$$E \in \{x \cdot x \in S \land P(x) \mid F(x)\} \equiv \exists x \cdot x \in S \land P(x) \land E = F(x)$$

Set theory: basic constructs

Examples

$$
\begin{aligned}
\{1,2,3\} \times \{a,b\} &= \{1 \mapsto a, 1 \mapsto b, 2 \mapsto a, 2 \mapsto b, 3 \mapsto a, 3 \mapsto b\} \\
\mathbb{P}(\{1,2,3\}) &= \{\{1,2,3\},\{1,2\},\{1,3\},\{2,3\},\{1\},\{2\},\{3\},\varnothing\} \\
\{x \mid x \in \{2,3,4,5\} \wedge x \mod 2 = 0\} &= \{2,4\} \\
\{x \cdot x \in \{2,3,4,5\} \wedge x \mod 2 = 1 \mid x^2\} &= \{25,9\}
\end{aligned}
$$

Reminder: $A \mapsto B$ is a tuple.
It is sometimes written as (A, B) in other formalisms.

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

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

Operations on sets

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

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

Binay relations

- A binary relation $r \in S \leftrightarrow T$ is a subset of their Cartesian product: $r \subseteq S \times T$
- Different syntax to highlight structure.
- $S \leftrightarrow T$: all (= the set of) the possible relations between S and T.
  - r would be one of them.

- $r \in 1..3 \leftrightarrow 7..11$
  - $r = \{1 \mapsto 10, 2 \mapsto 7, 2 \mapsto 11\}$
  - $4 \mapsto 10 \notin r$

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

- $r \in \{\text{meat}, \text{fish}, \text{pasta}, \text{bacon}\} \leftrightarrow \{\text{carbs}, \text{protein}, \text{fat}\}$ – write a couple of relations.
- $dom(r)$, $ran(r)$, relation with S and T
- How many different r may there be?

Types of relations

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

Hint: sets and relations are very useful modeling tools!

Operations on relations

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

Assume $Prey \in Animal \leftrightarrow Animal$.

We mean $hunter \mapsto hunted$*. The syntax of the relation does not reveal its intended semantics.*

- $Mammal \lhd Prey$
- $Mammal \ntriangleleft Prey$
- $Prey \rhd Spiders$
- $Fish \lhd (Prey \rhd Spiders)$
- $Spiders \ntriangleleft (Prey \rhd Spiders)$

Operations on relations

Image	$r[S]$	$\{y \mid x \mapsto y \in r \land x \in S\}$
Composition	$p; q$	$\{x \mapsto z \mid x \mapsto y \in p \land y \mapsto z \in q\}$
Overriding	$p \Leftarrow q$	$q \cup (dom(q) \lhd p)$
Identity	$id(S)$	$\{x \mapsto x \mid x \in S\}$

Overriding:

- Take q, and add the tuples from p whose lhs are not already in q.
- Or, take p and add q, overriding the tuples with the same lhs.

Some useful results, definitions

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

$r = r^{-1}$	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

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

Functions

- Functions: one type of relations.
- Notation: $f(x) = y \equiv x \mapsto y \in f$.
- Every element in domain relates only to one element in range.

$$x \mapsto y \in f \land x \mapsto z \in f \Rightarrow y = z$$

- WD conditions:
  - $f \in S \mathrel{+\!\!\!\!\rightarrow} T$
  - $x \in \mathrm{dom}(f)$
- Using right type of function allows different proofs.

Total function ($dom(f) = S$)	$S \rightarrow T$
Partial function	$S \mathrel{+\!\!\!\!\rightarrow} T$

Injection: if $f(x) = f(y)$, then $x = y$.

Partial injection	$S \mathrel{\rightarrowtail\!\!\!\!\!+} T$
Total injection	$S \rightarrowtail T$

Surjection: $f \in S \leftrightarrow T$, $ran(f) = T$.

Partial surjection	$S \mathrel{+\!\!\!\!\twoheadrightarrow} T$
Total surjection	$S \twoheadrightarrow T$

Bijection	$S \mathrel{\rightarrowtail\!\!\!\!\twoheadrightarrow} T$

An example of functions and relations: a strict society

- Every person is either a man or a woman.
- No person is man and woman at the same time.
- Only women have husbands, who must be men.
- Woman have at most one husband.
- Men have at most one wife.
- Mother are married women.

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	$husband \in women \rightarrowtail\!\!\!\!\!\!\!+\;\; men$
Men at most one wife	
Mother are married women	$mother \in PERSON \nrightarrow \mathrm{dom}(husband)$

Let us derive some relations (Double check with Rodin)

$wife = husband^{-1}$

$spouse = husband \cup wife$

$father = mother ; husband$

$children = (mother \cup father)^{-1}$

$daughter = children \rhd women$

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

$brother = men \rhd sibling$

Properties

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

Arithmetic

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