Formal Software Engineering
(génie logiciel avec l'approche formelle)

J. Christian Attiogbé

Master Alma, Septembre 2015
Two parts course, shared with Pr. Claude Jard and M. Benoît Delahaye

Sets and typing

- Predefined Sets (work as types)
  BOOL, CHAR,
  INTEGER ($\mathbb{Z}$), NAT ($\mathbb{N}$), NAT1 ($\mathbb{N}$*) ,
  STRING
- Cartesian Product E $\times$ F
- The set of subsets (powerset) of E $\mathcal{P}(E)$
  written POW(E)

Set Theory Language

The standard set operators

E, F and T are sets, x an member of F

Description	Notation	Ascii
union	$E \cup F$	`E \/ F`
intersection	$E \cap F$	`E /\ F`
membership	$x \in F$	`x : F`
difference	$E \setminus F$	`E - F`
inclusion	$E \subseteq F$	`E <: F`

+ generalised Union and intersection
+ quantified Union et intersection

Set Theory Language

In ascii notation, the negation is written with /.

Description	Notation	Ascii
not member	$x \notin F$	`x /: F`
non inclusion	$E \not\subseteq F$	`E /<: F`
non equality	$E \neq F$	`E /= F`

Generalised Union (à la B)

an operator to achieve the generalised union of well-formed *set expressions*.

$S \in \mathcal{P}(\mathcal{P}(T))$
$\Rightarrow$
$union(S) = \{x \mid x \in T \wedge \exists\, u.(u \in S \wedge x \in u)\}$

Example

$$union(\{\{aa, ee, ff\}, \{bb, cc, gg\}, \{dd, ee, uu, cc\}\})$$
$$= \{aa, ee, ff, bb, cc, gg, dd, uu\}$$

Sets and Relations

Quantified Union

an operator to achieve the quantified union of well-formed *set expressions*.

$\forall\, x.(x \in S \Rightarrow E \subseteq T)$
$\Rightarrow$

$$\bigcup x.(x \in S \mid E) = \{y \mid y \in T \wedge \exists\, x.(x \in S \wedge y \in E)\}$$

Exemple

$$UNION(x).(x \in \{1, 2, 3\} \mid \{y \mid y \in NAT \wedge y = x * x\})$$
$$= \{1\} \cup \{4\} \cup \{9\} = \{1, 4, 9\}$$

Sets and Relations

Generalised Intersection (à la B)

an operator to achieve the generalised intersection of of well-formed *set expressions*.

$S \in \mathcal{P}(\mathcal{P}(T))$
$\Rightarrow$
$inter(S) = \{x \mid x \in T \wedge \forall\, u.(u \in S \Rightarrow x \in u)\}$

Example

$inter(\{\{aa, ee, ff, cc\}, \{bb, cc, gg\}, \{dd, ee, uu, cc\}\} = \{cc\}$

Sets and Relations

Quantified Intersection (à la B)

an operator to achieve the quantified intersection of of well-formed *set expressions*.

$\forall\, x.(x \in S \Rightarrow E \subseteq T)$
$\Rightarrow$
$\bigcap x.(x \in S \mid E)$
$= \{y \mid y \in T \wedge \forall\, x.(x \in S \Rightarrow y \in E)\}$

Example

$INTER(x).(x \in \{1, 2, 3, 4\} \mid \{y \mid y \in \{1, 2, 3, 4, 5\} \wedge y > x$

$$= inter(\{\{1, 2, 3, 4, 5\}, \{2, 3, 4, 5\}, \{3, 4, 5\}, \{4, 5\}\})$$

Relations

Description	Notation	Ascii
relation	$r : S \leftrightarrow T$	r : S <-> T
domain	$dom(r) \subseteq S$	dom(r) <: S
range	$ran(r) \subseteq T$	ran(r) <: T
composition	$r;s$	r;s
composition r(s)	$r \circ s$	r(s)
identity	$id(S)$	id(S)

Relations (continued)

Description	Notation	Ascii
domain restrictition	$S \lhd r$	S <| r
range restriction	$r \rhd T$	r |> T
domain antirestriction	$S ⩤ r$	S <<| r
range antirestriction	$r ⩥ T$	r |>> T
inverse	$r^{\sim}$	r ~
relationnelle image	$r[S]$	r[S]
overiding	$r1 \oplus r2$	r1 <+ r2
direct product of rel.	$r1 \otimes r2$	r1 >< r2
closure	$closure(r)$	closure(r)
reflexive trans. closure	$closure1(r)$	closure1(r)

Functions

Description	Notation	Ascii
partial function	$S \nrightarrow T$	S +-> T
total function	$S \rightarrow T$	S --> T
partial injection	$S \rightarrowtail\!\!\!+ T$	S >+-> T
total injection	$S \rightarrowtail T$	S >-> T
partial surjection	$S +\!\!\twoheadrightarrow T$	S +->> T
total surjection	$S \twoheadrightarrow T$	S -->> T
total bijection	$S ⤖ T$	S >->> T
lambda abstraction	$\%x.(P \mid E)$	