Specification et Verification Formelle

Chapter 02: Logical Notations and Set Theory basics

Dr. Hichem Debbi

hichem.debbi@gmail.com

March 20, 2022

Basic logical notations

Symbole	Signification	Définition
$\wedge$	et logique	
$\neg$	négation	
$\vee$	ou logique	$a \vee b \stackrel{def}{=} \neg(\neg a \wedge \neg b)$
$\Rightarrow$	implication	$a \Rightarrow b \stackrel{def}{=} \neg a \vee b$
$\Leftrightarrow$	équivalence	$a \Leftrightarrow b \stackrel{def}{=} (a \Rightarrow b) \wedge (b \Rightarrow a)$

Quantifiers

Symbole	Signification	Syntaxe	Définition
$\forall$	pour tout	$\forall\, Id\_liste \cdot (Prédicat)$	
$\exists$	il existe	$\exists\, Id\_liste \cdot (Prédicat)$	$\exists\, x \cdot (P) \stackrel{def}{=\!=} \neg \forall\, x \cdot (\neg\, P)$

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Sets Predicates

Symbole	Signification	Définition
$\in$	appartient à	
$\notin$	n'appartient pas à	$x \notin s \stackrel{def}{=\!=} \neg(x \in s)$
$\subseteq$	est inclus dans	$s \subseteq t \stackrel{def}{=\!=} s \in \mathbb{P}(t)$
$\not\subseteq$	n'est pas inclus dans	$s \not\subseteq t \stackrel{def}{=\!=} \neg(s \subseteq t)$
$\subset$	est strictement inclus dans	$s \subset t \stackrel{def}{=\!=} (s \subseteq t \land s \neq t)$
$\not\subset$	n'est pas strictement inclus dans	$s \not\subset t \stackrel{def}{=\!=} \neg(s \subset t)$

Expressions d'ensembles

	Signification	Définition
$\cup$	union	$s_1 \cup s_2 \stackrel{def}{=} \{x \mid x \in t \ \wedge \ (x \in s_1 \ \vee \ x \in s_2)\}$
$\cap$	intersection	$s_1 \cap s_2 \stackrel{def}{=} \{x \mid x \in t \ \wedge \ (x \in s_1 \ \wedge \ x \in s_2)\}$
$-$	différence d'ensembles	$s_1 - s_2 \stackrel{def}{=} \{x \mid x \in t \ \wedge \ (x \in s_1 \ \wedge \ x \notin s_2)\}$

1985
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Properties

$$s \subseteq s \qquad \text{(réflexivité)}$$

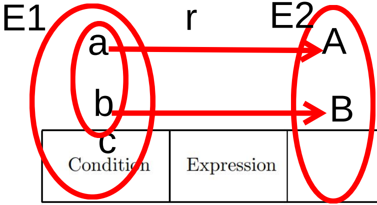
$$s \subseteq t \;\wedge\; t \subseteq u \Rightarrow s \subseteq u \qquad \text{(transitivité)}$$

$$s \subseteq t \;\wedge\; t \subseteq s \Rightarrow s = t \qquad \text{(anti-symétrie)}$$

- they represent a set of couples
- Relations are useful in specifying invariants, properties...

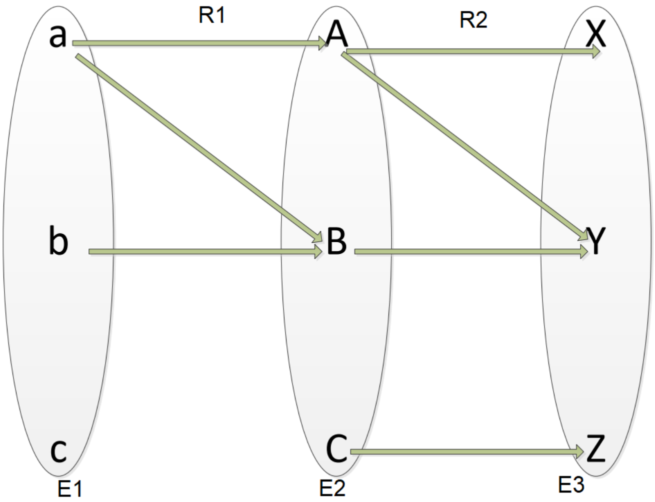
Symbole	Signification	Définition
$\leftrightarrow$	relation entre deux ensembles	$E_1 \leftrightarrow E_2 \stackrel{def}{=\!=} \mathbb{P}(E_1 \times E_2)$

Relations



Condition	Expression	Définition
$r \in E_1 \leftrightarrow E_2$	$\mathsf{dom}(r)$	$\{x \mid x \in E_1 \ \wedge \ \exists y \cdot (y \in E_2 \ \wedge \ (x \mapsto y) \in r)\}$
$r \in E_1 \leftrightarrow E_2$	$\mathsf{ran}(r)$	$\{y \mid y \in E_2 \ \wedge \ \exists x \cdot (x \in E_1 \ \wedge \ (x \mapsto y) \in r)\}$
$r \in E_1 \leftrightarrow E_2$ et $F \subseteq E_1$	$r[F]$	$\{y \mid y \in E_2 \ \wedge \ \exists x \cdot (x \in F \ \wedge \ (x \mapsto y) \in r)\}$

Relations - Example



Relations - Example

- $R1 : E1 \leftrightarrow E2 \qquad R1 = \{(a, A), (a, B), (b, B)\} = \{a \mapsto A, a \mapsto B, b \mapsto B\}$
- $R2 : E2 \leftrightarrow \qquad E3 R2 = \{(A, x), (A, y), (B, y), (C, z)\}$
- $dom(R1) = \{a, b\} \quad ran(R1) = \{A, B\} codomain(R1) = \{A, B, C\} \quad R1[b, c] = \{B\}$
- $R1; R2 = \{(a, x), (a, y), (b, y)\}$
- $R1^{-1} = \{(A, a), (B, a), (B, b)\}$

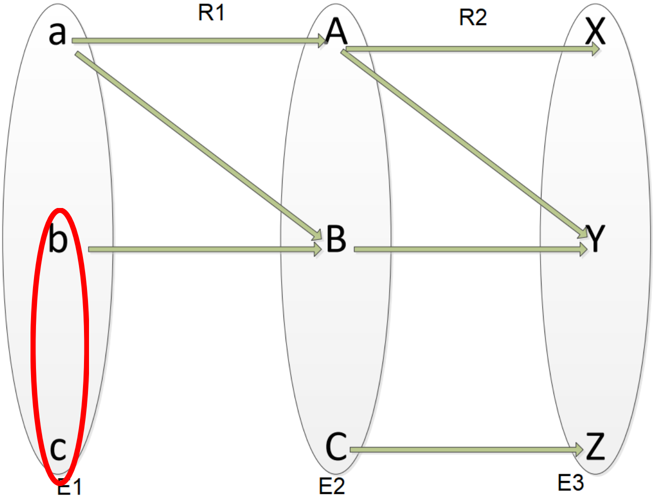
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Operations on Relations

Condition	Expression	Définition
	$\mathsf{id}(E)$	$\{x, y \mid (x \mapsto y) \in E \times E \ \wedge \ x = y\}$
$r \in s \leftrightarrow t$	r^{-1}	$\{y, x \mid (y \mapsto x) \in t \times s \ \wedge \ (x \mapsto y) \in r\}$
$r_1 \in t \leftrightarrow u$ et $r_2 \in u \leftrightarrow v$	$r_1 \ ; \ r_2$	$\{x, z \mid x, z \in t \times v \ \wedge \ \exists y \cdot (y \in u \ \wedge \ (x \mapsto y) \in r_1 \ \wedge \ (y \mapsto z) \in r_2)\}$
$r_1 \in t \leftrightarrow u$ et $r_2 \in t \leftrightarrow v$	$r_1 \otimes r_2$	$\{x, (y, z) \mid x, (y, z) \in t \times (u \times v) \ \wedge \ (x \mapsto y) \in r_1 \ \wedge \ (x \mapsto z) \in r_2\}$
$r_1 \in t \leftrightarrow u$ et $r_2 \in v \leftrightarrow w$	$r_1 \parallel r_2$	$\{(x, z), (y, a) \mid (x, z), (y, a) \in (t \times v) \times (u \times w) \ \wedge \ (x \mapsto y) \in r_1 \ \wedge \ (z \mapsto a) \in r_2\}$
	$\mathsf{prj}_1(E, F)$	$\{x, y, z \mid x, y, z \in E \times F \times E \ \wedge \ z = x\}$
	$\mathsf{prj}_2(E, F)$	$\{x, y, z \mid x, y, z \in E \times F \times F \ \wedge \ z = y\}$

1985
جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

Relations - Example

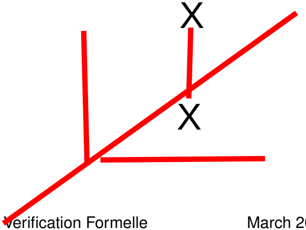


Restrictions - Example

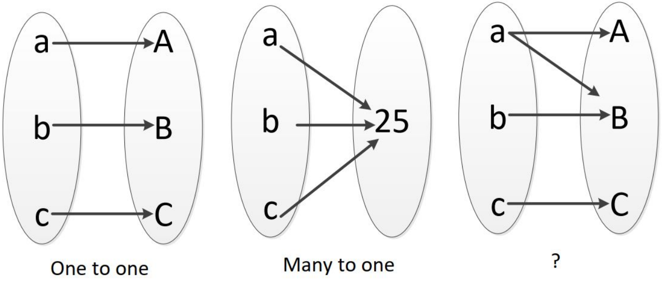
- $E \lhd R$ Restriction of R to domain E
  Example: $\{b, c\} \lhd R1 = \{b \mapsto B\}$
- $E \rhd R$ Restriction of R to co-domain E
  Example: $R1 \rhd \{B, C\} = \{a \mapsto B, b \mapsto B\}$
- $E \lhd\!\lhd R$ Anti-restriction of R to domain E
  Example: $\{b, c\} \lhd\!\lhd R1 = \{a \mapsto A, a \mapsto B\}$
- $E \rhd\!\rhd R$ Anti-restriction of R to co-domain E
  Example: $\{b, c\} \rhd\!\rhd R1 = \{a \mapsto A, a \mapsto B\}$

Fonctions

- Functions are relations, in which each element of the domain is associated to one and only one element of the co-domain.
- Let A and B be two sets. A function F from A to B has the following notation: $F \rightarrow B$
- F affect exactly one element of B, denoted $F(a) \in B$, to $a \in A$, and this for every $a \in A$.
- A is called the domain, and B is the co-domain.
- b is the image of a by F
- a is the pre-image of b



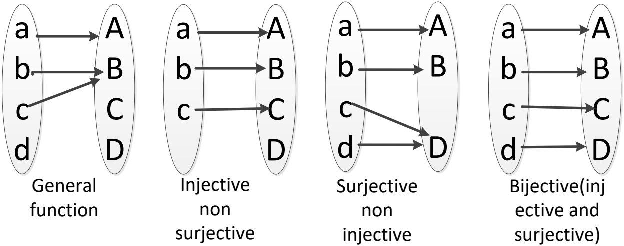
Fonctions Examples



Fonctions types

Signification	Expression	Définition
fonctions partielles	$s \pfun t$	$\{r \mid r \in s \leftrightarrow t \wedge \forall x, y, z \cdot (x, y \in r \ \wedge \ x, z \in r \Rightarrow y = z)\}$
fonctions totales	$s \rightarrow t$	$\{f \mid f \in s \pfun t \ \wedge \ \mathsf{dom}(f) = s\}$
injectives partielles	$s \pinj t$	$\{f \mid f \in s \pfun t \ \wedge \ f^{-1} \in t \pfun s\}$
injectives totales	$s \rightarrowtail t$	$s \pinj t \ \cap \ s \rightarrow t$
surjectives partielles	$s \psurj t$	$\{f \mid f \in s \pfun t \ \wedge \ \mathsf{ran}(f) = t\}$
surjectives totales	$s \twoheadrightarrow t$	$s \psurj t \ \cap \ s \rightarrow t$
bijectives partielles	$s \pbij t$	$s \pinj t \ \cap \ s \psurj t$
bijectives totales	$s \bij t$	$s \rightarrowtail t \ \cap \ s \twoheadrightarrow t$

Fonctions types



Fonctions

- **Injective:** Every member of A has its unique matching member in B
- **Surjective:** Every member of B has at least on matching member in A or The range of function is equal to co-domain.
- **Bijective:** Every member of B has exactly on matching member in A

References

- The B-Book: Assigning Programs to Meanings, J. R. Abrial
- Specification en B Support de cours Ecole des Jeunes Chercheurs en Programmation EJCP 2007