Summary of the Mathematical Notation

Jean-Raymond Abrial
(edited by Thai Son Hoang)

Department of Computer Science
Swiss Federal Institute of Technology Zürich (ETH Zürich)

Bucharest DEPLOY 2-day course, 14-16/07/10, ETH Zurich

Outline

Foundation for Deductive and Formal Proofs

- Reason: We want to understand how proofs can be mechanized.
- Topics:
  - Concepts of Sequent and Inference Rule.
  - Backward and Forward reasoning
  - Basic Inference Rules.

Sequent

- Sequent is the generic name for "something we want to prove"
- We shall be more precise later

Inference Rule

- An inference rule is a tool to perform a formal proof
- It is denoted by:

$$\frac{A}{C}$$

- A is a (possibly empty) collection of sequents: the antecedents
- C is a sequent: the consequent

> The proofs of each sequent of A
> —— together give you ——
> a proof of sequent C

Backward and Forward Reasoning

Given an inference rule $\frac{A}{C}$ with antecedents A and consequent C

- Forward reasoning: $\frac{A}{C}\downarrow$
  Proofs of each sequent in A give you a proof of the consequent C
- Backward reasoning: $\frac{A}{C}\uparrow$
  In order to get a proof of C, it is sufficient to have proofs of each sequent in A

Proofs are usually done using backward reasoning

"Executing" the Proof of a Sequent S (backward reasoning)

We are given:

- a collection $\mathcal{T}$ of inference rules of the form $\frac{A}{C}$
- a sequent container K, containing S initially

> while K is not empty
>
> choose a rule $\frac{A}{C}$ in $\mathcal{T}$ whose consequent C is in K;
>
> replace C in K by the antecedents A (if any)

This proof method is said to be goal oriented.

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

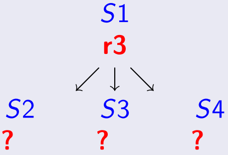
$S1$

?

- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$



- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

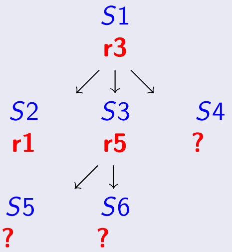
r1 $\dfrac{}{S2}$ **r2** $\dfrac{S7}{S4}$ **r3** $\dfrac{S2 \quad S3 \quad S4}{S1}$ **r4** $\dfrac{}{S5}$ **r5** $\dfrac{S5 \quad S6}{S3}$ **r6** $\dfrac{}{S6}$ **r7** $\dfrac{}{S7}$

$S1$
r3
↙ ↓ ↘
$S2$ $S3$ $S4$
r1 **?** **?**

- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

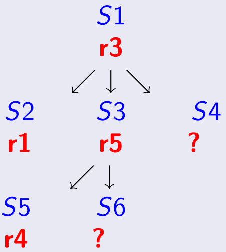
r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$



- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

$$\textbf{r1}\ \frac{}{S2} \qquad \textbf{r2}\ \frac{S7}{S4} \qquad \textbf{r3}\ \frac{S2 \quad S3 \quad S4}{S1} \qquad \textbf{r4}\ \frac{}{S5} \qquad \textbf{r5}\ \frac{S5 \quad S6}{S3} \qquad \textbf{r6}\ \frac{}{S6} \qquad \textbf{r7}\ \frac{}{S7}$$



- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

$\textbf{r1}\ \frac{}{S2} \qquad \textbf{r2}\ \frac{S7}{S4} \qquad \textbf{r3}\ \frac{S2 \quad S3 \quad S4}{S1} \qquad \textbf{r4}\ \frac{}{S5} \qquad \textbf{r5}\ \frac{S5 \quad S6}{S3} \qquad \textbf{r6}\ \frac{}{S6} \qquad \textbf{r7}\ \frac{}{S7}$

$S1$
r3
↙ ↓ ↘
$S2$ **r1** — $S3$ **r5** — $S4$ **?**
$S3$ **r5**: ↙ ↓
$S5$ **r4** — $S6$ **r6**

- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

$$\textbf{r1}\ \frac{}{S2} \qquad \textbf{r2}\ \frac{S7}{S4} \qquad \textbf{r3}\ \frac{S2 \quad S3 \quad S4}{S1} \qquad \textbf{r4}\ \frac{}{S5} \qquad \textbf{r5}\ \frac{S5 \quad S6}{S3} \qquad \textbf{r6}\ \frac{}{S6} \qquad \textbf{r7}\ \frac{}{S7}$$

S1
r3
↙ ↓ ↘

S2	S3	S4
r1	**r5**	**r2**
	↙ ↓	↓
S5	S6	S7
r4	**r6**	**?**

- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

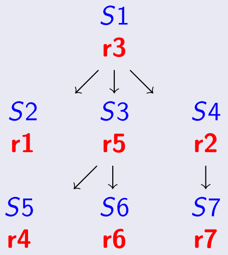
$S1$
r3
↙ ↓ ↘

$S2$	$S3$	$S4$
r1	**r5**	**r2**
	↙ ↓	↓
$S5$	$S6$	$S7$
r4	**r6**	**r7**

- The proof is a tree
- We have shown here a depth-first strategy

Proof of S1

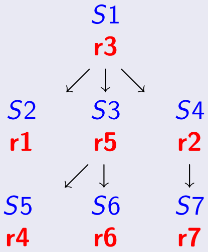
$$\mathbf{r1}\ \frac{}{S2} \qquad \mathbf{r2}\ \frac{S7}{S4} \qquad \mathbf{r3}\ \frac{S2 \quad S3 \quad S4}{S1} \qquad \mathbf{r4}\ \frac{}{S5} \qquad \mathbf{r5}\ \frac{S5 \quad S6}{S3} \qquad \mathbf{r6}\ \frac{}{S6} \qquad \mathbf{r7}\ \frac{}{S7}$$



- The proof is a tree
- We have shown here a depth-first strategy

Alternate Representation of the Proof Tree

A vertical representation of the proof tree:



S1	**r3**
S2	**r1**
S3	**r5**
S5	**r4**
S6	**r6**
S4	**r2**
S7	**r7**

Proof of S1

r1 $\dfrac{}{S2}$ **r2** $\dfrac{S7}{S4}$ **r3** $\dfrac{S2 \quad S3 \quad S4}{S1}$ **r4** $\dfrac{}{S5}$ **r5** $\dfrac{S5 \quad S6}{S3}$ **r6** $\dfrac{}{S6}$ **r7** $\dfrac{}{S7}$

$S1$ **?**

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

$S1$	**r3**
$S2$	**?**
$S3$	**?**
$S4$	**?**

Proof of S1

r1 $\dfrac{}{S2}$ **r2** $\dfrac{S7}{S4}$ **r3** $\dfrac{S2 \quad S3 \quad S4}{S1}$ **r4** $\dfrac{}{S5}$ **r5** $\dfrac{S5 \quad S6}{S3}$ **r6** $\dfrac{}{S6}$ **r7** $\dfrac{}{S7}$

$S1$	**r3**
$S2$	**r1**
$S3$	**?**
$S4$	**?**

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

$S1$			**r3**
	$S2$		**r1**
	$S3$		**r5**
		$S5$	**?**
		$S6$	**?**
	$S4$		**?**

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

$S1$	**r3**
$S2$	**r1**
$S3$	**r5**
$S5$	**r4**
$S6$	**?**
$S4$	**?**

Proof of S1

r1 $\dfrac{}{S2}$ **r2** $\dfrac{S7}{S4}$ **r3** $\dfrac{S2 \quad S3 \quad S4}{S1}$ **r4** $\dfrac{}{S5}$ **r5** $\dfrac{S5 \quad S6}{S3}$ **r6** $\dfrac{}{S6}$ **r7** $\dfrac{}{S7}$

S1			**r3**
	S2		**r1**
	S3		**r5**
		S5	**r4**
		S6	**r6**
	S4		**?**

Proof of S1

r1 $\frac{}{S2}$ **r2** $\frac{S7}{S4}$ **r3** $\frac{S2 \quad S3 \quad S4}{S1}$ **r4** $\frac{}{S5}$ **r5** $\frac{S5 \quad S6}{S3}$ **r6** $\frac{}{S6}$ **r7** $\frac{}{S7}$

$S1$			**r3**
	$S2$		**r1**
	$S3$		**r5**
		$S5$	**r4**
		$S6$	**r6**
	$S4$		**r2**
		$S7$	**?**

Proof of $S1$

$$\mathbf{r1}\ \frac{}{S2} \qquad \mathbf{r2}\ \frac{S7}{S4} \qquad \mathbf{r3}\ \frac{S2 \quad S3 \quad S4}{S1} \qquad \mathbf{r4}\ \frac{}{S5} \qquad \mathbf{r5}\ \frac{S5 \quad S6}{S3} \qquad \mathbf{r6}\ \frac{}{S6} \qquad \mathbf{r7}\ \frac{}{S7}$$

$S1$			**r3**
	$S2$		**r1**
	$S3$		**r5**
		$S5$	**r4**
		$S6$	**r6**
	$S4$		**r2**
		$S7$	**r7**

More on Sequent

- We supposedly have a Predicate Language (not defined yet)
- A sequent is denoted by:

$$H \ \vdash \ G$$

- H is a (possibly empty) collection of predicates: the hypotheses
- G is a predicate: the goal

Meaning ...

Under the hypotheses of collection H, prove the goal G

Basic Inference Rules of Mathematical Reasoning

- HYPOTHESIS: If the goal belongs to the hypotheses of a sequent, then the sequent is proved,
- MONOTONICITY: Once a sequent is proved, any sequent with the same goal and more hypotheses is also proved,
- CUT: If you succeed in proving P under H, then P can be added to the collection H for proving a goal G.

Basic Inference Rules of Mathematical Reasoning

- HYPOTHESIS: If the goal belongs to the hypotheses of a sequent, then the sequent is proved,
- MONOTONICITY: Once a sequent is proved, any sequent with the same goal and more hypotheses is also proved,
- CUT: If you succeed in proving P under H, then P can be added to the collection H for proving a goal G.

Basic Inference Rules of Mathematical Reasoning

- HYPOTHESIS: If the goal belongs to the hypotheses of a sequent, then the sequent is proved,
- MONOTONICITY: Once a sequent is proved, any sequent with the same goal and more hypotheses is also proved,
- CUT: If you succeed in proving P under H, then P can be added to the collection H for proving a goal G.

Basic Inference Rules

$$\frac{}{\mathsf{H},\ P \ \vdash\ P} \qquad \mathsf{HYP}$$

$$\frac{\mathsf{H} \ \vdash\ Q}{\mathsf{H},\ P \ \vdash\ Q} \qquad \mathsf{MON}$$

$$\frac{\mathsf{H} \ \vdash\ P \qquad \mathsf{H},\ P \ \vdash\ Q}{\mathsf{H} \ \vdash\ Q} \qquad \mathsf{CUT}$$

Basic Constructs of Propositional Calculus

Given predicates P and Q, we can construct:

- CONJUNCTION: $P \wedge Q$
- IMPLICATION: $P \Rightarrow Q$
- NEGATION: $\neg P$

Syntax

$$
\begin{array}{lcl}
\mathit{Predicate} & ::= & \mathit{Predicate} \;\wedge\; \mathit{Predicate} \\
 & & \mathit{Predicate} \;\Rightarrow\; \mathit{Predicate} \\
 & & \neg\; \mathit{Predicate}
\end{array}
$$

- This syntax is ambiguous.

More on Syntax

- Pairs of matching parentheses can be added freely.
- Operator $\wedge$ is associative.
- Operator $\Rightarrow$ is not associative: $P \Rightarrow Q \Rightarrow R$ is not allowed.
- Write explicitly $(P \Rightarrow Q) \Rightarrow R$ or $P \Rightarrow (Q \Rightarrow R)$.
- Operators have precedence in this decreasing order: $\neg$, $\wedge$, $\Rightarrow$.

Extensions: Truth, Falsity, Disjunction and Equivalence

- TRUTH: $\top$
- FALSITY: $\bot$
- DISJUNCTION: $P \lor Q$
- EQUIVALENCE: $P \Leftrightarrow Q$

Syntax

$$
\begin{array}{lcl}
\mathit{Predicate} & ::= & \mathit{Predicate} \;\wedge\; \mathit{Predicate} \\
 & & \mathit{Predicate} \;\Rightarrow\; \mathit{Predicate} \\
 & & \neg\; \mathit{Predicate} \\
 & & \bot \\
 & & \top \\
 & & \mathit{Predicate} \;\vee\; \mathit{Predicate} \\
 & & \mathit{Predicate} \;\Leftrightarrow\; \mathit{Predicate}
\end{array}
$$

More on Syntax

- Pairs of matching parentheses can be added freely.
- Operators $\wedge$ and $\vee$ are associative.
- Operator $\Rightarrow$ and $\Leftrightarrow$ are not associative.
- Precedence decreasing order: $\neg$, $\wedge$ and $\vee$, $\Rightarrow$ and $\Leftrightarrow$.

More on Syntax (cont'd)

- The mixing of $\wedge$ and $\vee$ without parentheses is not allowed.
- You have to write either $P \wedge (Q \vee R)$ or $(P \wedge Q) \vee R$
- The mixing of $\Rightarrow$ and $\Leftrightarrow$ without parentheses is not allowed.
- You have to write either $P \Rightarrow (Q \Leftrightarrow R)$ or $(P \Rightarrow Q) \Leftrightarrow R$

Propositional Calculus Rules of Inference (1)

- Rules about conjunction

$$\begin{array}{c} \mathbf{H}, \mathbf{P}, \mathbf{Q} \;\vdash\; \mathbf{R} \\ \hline\hline \mathbf{H},\; \mathbf{P} \wedge \mathbf{Q} \;\vdash\; \mathbf{R} \end{array} \quad \text{AND\_L}$$

$$\begin{array}{c} \mathbf{H} \;\vdash\; \mathbf{P} \qquad \mathbf{H} \;\vdash\; \mathbf{Q} \\ \hline \mathbf{H} \;\vdash\; \mathbf{P} \wedge \mathbf{Q} \end{array} \quad \text{AND\_R}$$

- Rules about implication

$$\begin{array}{c} \mathbf{H}, \mathbf{P}, \mathbf{Q} \;\vdash\; \mathbf{R} \\ \hline \mathbf{H},\; \mathbf{P},\; \mathbf{P} \Rightarrow \mathbf{Q} \;\vdash\; \mathbf{R} \end{array} \quad \text{IMP\_L}$$

$$\begin{array}{c} \mathbf{H}, \mathbf{P} \;\vdash\; \mathbf{Q} \\ \hline\hline \mathbf{H} \;\vdash\; \mathbf{P} \Rightarrow \mathbf{Q} \end{array} \quad \text{IMP\_R}$$

Note

Rules with a double horizontal line can be applied in both directions.

Propositional Calculus Rules of Inference (2)

- Rules about disjunction

$$\frac{\mathbf{H}, \mathbf{P} \;\vdash\; \mathbf{R} \qquad\qquad \mathbf{H}, \mathbf{Q} \;\vdash\; \mathbf{R}}{\mathbf{H},\; \mathbf{P} \vee \mathbf{Q} \;\vdash\; \mathbf{R}} \qquad \text{OR\_L}$$

$$\frac{\mathbf{H}, \neg P \;\vdash\; \mathbf{Q}}{\mathbf{H} \;\vdash\; \mathbf{P} \vee \mathbf{Q}} \qquad \text{OR\_R}$$

Propositional Calculus Rules of Inference (3)

- Rules about negation

$$\frac{\mathbf{H},\ \neg\mathbf{Q}\ \vdash\ \mathbf{P}}{\mathbf{H},\ \neg\mathbf{P}\ \vdash\ \mathbf{Q}}\quad \text{NOT\_L}$$

$$\frac{\mathbf{H},\mathbf{P}\ \vdash\ \bot}{\mathbf{H}\ \vdash\ \neg\mathbf{P}}\quad \text{NOT\_R}$$

$$\frac{}{\mathbf{H},\bot\ \vdash\ \mathbf{P}}\quad \text{FALSE\_L}$$

$$\frac{\mathbf{H}\ \vdash\ \mathbf{P}\qquad \mathbf{H}\ \vdash\ \neg\mathbf{P}}{\mathbf{H}\ \vdash\ \bot}\quad \text{FALSE\_R}$$

Propositional Calculus Rules of Inference (4)

- Deriving rules:

$$\frac{\mathsf{H},\ Q \ \vdash\ P \qquad \mathsf{H},\ \neg Q \ \vdash\ P}{\mathsf{H} \ \vdash\ P} \quad \textbf{CASE}$$

$$\frac{\mathsf{H}.\ \neg Q \ \vdash\ \neg P}{\mathsf{H},\ P \ \vdash\ Q} \quad \textbf{CT\_L}$$

$$\frac{\mathsf{H}.\ \neg P \ \vdash\ \bot}{\mathsf{H} \ \vdash\ P} \quad \textbf{CT\_R}$$

$$\frac{\mathsf{H} \ \vdash\ P}{\mathsf{H} \ \vdash\ P \lor Q} \quad \textbf{OR\_R1}$$

$$\frac{\mathsf{H} \ \vdash\ Q}{\mathsf{H} \ \vdash\ P \lor Q} \quad \textbf{OR\_R2}$$

Propositional Calculus Rules of Inference (4)

- Rewriting rules:

Predicate	Rewritten
$\top$	$\neg \bot$
$P \Leftrightarrow Q$	$(P \Rightarrow Q) \wedge (Q \Rightarrow P)$

- More derived rules:

$$\frac{}{\mathsf{H} \ \vdash \ \top} \quad \mathbf{TRUE\_R}$$

$$\frac{\mathsf{H} \ \vdash \ P}{\mathsf{H}, \top \ \vdash \ P} \quad \mathbf{TRUE\_L}$$

CLASSICAL RESULTS (1)

commutativity	$P \lor Q$	$\Leftrightarrow$	$Q \lor P$
	$P \land Q$	$\Leftrightarrow$	$Q \land P$
	$(P \Leftrightarrow Q)$	$\Leftrightarrow$	$(Q \Leftrightarrow P)$
associativity	$(P \lor Q) \lor R$	$\Leftrightarrow$	$P \lor (Q \lor R)$
	$(P \land Q) \land R$	$\Leftrightarrow$	$P \land (Q \land R)$
	$((P \Leftrightarrow Q) \Leftrightarrow R)$	$\Leftrightarrow$	$(P \Leftrightarrow (Q \Leftrightarrow R))$
distributivity	$R \land (P \lor Q)$	$\Leftrightarrow$	$(R \land P) \lor (R \land Q)$
	$R \lor (P \land Q)$	$\Leftrightarrow$	$(R \lor P) \land (R \lor Q)$
	$R \Rightarrow (P \land Q)$	$\Leftrightarrow$	$(R \Rightarrow P) \land (R \Rightarrow Q)$
	$(P \lor Q) \Rightarrow R$	$\Leftrightarrow$	$(P \Rightarrow R) \land (Q \Rightarrow R)$

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

CLASSICAL RESULTS (2)

excluded middle	$P \lor \neg P$
idempotence	$P \lor P \Leftrightarrow P$ $P \land P \Leftrightarrow P$
absorbtion	$(P \lor Q) \land P \Leftrightarrow P$ $(P \land Q) \lor P \Leftrightarrow P$
truth	$(P \Leftrightarrow \top) \Leftrightarrow P$
falsity	$(P \Leftrightarrow \bot) \Leftrightarrow \neg P$

CLASSICAL RESULTS (3)

de Morgan	$\neg(P \lor Q) \Leftrightarrow (\neg P \land \neg Q)$ $\neg(P \land Q) \Leftrightarrow (\neg P \lor \neg Q)$ $\neg(P \land Q) \Leftrightarrow (P \Rightarrow \neg Q)$ $\neg(P \Rightarrow Q) \Leftrightarrow (P \land \neg Q)$
contraposition	$(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$ $(\neg P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow P)$ $(P \Rightarrow \neg Q) \Leftrightarrow (Q \Rightarrow \neg P)$
double negation	$P \Leftrightarrow \neg\neg P$

CLASSICAL RESULTS (4)

transitivity	$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \;\Rightarrow\; (P \Rightarrow R)$
monotonicity	$(P \Rightarrow Q) \Rightarrow ((P \wedge R) \Rightarrow (Q \wedge R))$ $(P \Rightarrow Q) \Rightarrow ((P \vee R) \Rightarrow (Q \vee R))$ $(P \Rightarrow Q) \Rightarrow ((R \Rightarrow P) \Rightarrow (R \Rightarrow Q))$ $(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$ $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$
equivalence	$(P \Leftrightarrow Q) \Rightarrow ((P \wedge R) \Leftrightarrow (Q \wedge R))$ $(P \Leftrightarrow Q) \Rightarrow ((P \vee R) \Leftrightarrow (Q \vee R))$ $(P \Leftrightarrow Q) \Rightarrow ((R \Rightarrow P) \Leftrightarrow (R \Rightarrow Q))$ $(P \Leftrightarrow Q) \Rightarrow ((P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R))$ $(P \Leftrightarrow Q) \Rightarrow (\neg P \Leftrightarrow \neg Q)$

Syntax of our Predicate Language so far

$$
\begin{array}{lll}
\textit{predicate} & ::= & \bot \\
 & & \top \\
 & & \neg\, \textit{predicate} \\
 & & \textit{predicate} \;\wedge\; \textit{predicate} \\
 & & \textit{predicate} \;\vee\; \textit{predicate} \\
 & & \textit{predicate} \;\Rightarrow\; \textit{predicate} \\
 & & \textit{predicate} \;\Leftrightarrow\; \textit{predicate}
\end{array}
$$

- The letter P, Q, etc. we have used are generic variables.
- Each of them stands for a *predicate*.
- All our proofs were thus also generic (able to be instantiated).

Refining our Language: Predicate Calculus

$$
\begin{array}{lll}
\mathit{predicate} & ::= & \bot \\
 & & \top \\
 & & \neg\, \mathit{predicate} \\
 & & \mathit{predicate} \;\wedge\; \mathit{predicate} \\
 & & \mathit{predicate} \;\vee\; \mathit{predicate} \\
 & & \mathit{predicate} \;\Rightarrow\; \mathit{predicate} \\
 & & \mathit{predicate} \;\Leftrightarrow\; \mathit{predicate} \\
 & & \forall \mathit{var\_list} \cdot \mathit{predicate} \\
 & & [\mathit{var\_list} := \mathit{exp\_list}]\; \mathit{predicate} \\
 & & \\
\mathit{expression} & ::= & \mathit{variable} \\
 & & [\mathit{var\_list} := \mathit{exp\_list}]\; \mathit{expression} \\
 & & \mathit{expression} \mapsto \mathit{expression} \\
 & & \\
\mathit{variable} & ::= & \mathit{identifier}
\end{array}
$$

On Predicates and Expressions

- A Predicate is a formal text that can be PROVED
- An Expression DENOTES AN OBJECT.
- A Predicate denotes NOTHING.
- An Expression CANNOT BE PROVED
- Predicates and Expressions are INCOMPATIBLE.

Predicate Calculus: Linguistic Concepts.

- Substitution and Universal Quantification.
- Free/Bound Occurrences.
- Inference rules.
- Extension

VARIABLES, PROPOSITIONS AND PREDICATES

- A Proposition: $8 \in \mathbb{N} \Rightarrow 8 \geq 0$
- A Predicate (n is a variable): $n \in \mathbb{N} \Rightarrow n \geq 0$

WHAT CAN WE DO WITH A PREDICATE ?

- Specialize it: Substitution

$$[n := 8]\,(n \in \mathbb{N} \;\Rightarrow\; n \geq 0)$$

$$\downarrow$$

$$8 \in \mathbb{N} \;\Rightarrow\; 8 \geq 0$$

- Generalize it: Universal Quantification

$$\forall n \cdot (\, n \in \mathbb{N} \;\Rightarrow\; n \geq 0\,)$$

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

SUBSTITUTION

Simple Substitution

$$[x := E]\,P$$

- x is a VARIABLE,
- E is an EXPRESSION,
- P is a PREDICATE,
- Denotes the predicate obtained by replacing all FREE OCCURRENCES of x by E in P.

UNIVERSAL QUANTIFICATION

Universal Quantification

$$\forall x \cdot P$$

- x is said to be the QUANTIFIED VARIABLE
- P forms the SCOPE of x
- To say that such a predicate is proved, is the same as saying that all predicates of the following form are proved:

$$[x := E]P$$

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Free and Bound Occurrences

- Occurrences of the variable n are FREE (substitutable) in:

$$n \in \mathbb{N} \;\Rightarrow\; n \geq 0$$

- Occurrences of the variable n are BOUND (not substitutable) in:

$$[n := 8]\,(n \in \mathbb{N} \;\Rightarrow\; n \geq 0)$$

$$\forall n \cdot (\, n \in \mathbb{N} \;\Rightarrow\; n \geq 0\,)$$

Inference Rules for Predicate Calculus

$$\frac{\mathrm{H},\ \forall x \cdot P,\ [x := E]P \ \vdash\ Q}{\mathrm{H},\ \forall x \cdot P \ \vdash\ Q} \qquad \textbf{ALL\_L}$$

where **E** is an expression

$$\frac{\mathbf{H} \ \vdash\ \mathbf{P}}{\mathbf{H} \ \vdash\ \forall \mathbf{x} \cdot \mathbf{P}} \qquad \textbf{ALL\_R}$$

- In rule ALL_R, variable **x** is not free in H

Extending the language: Existential Quantification

$$
\begin{array}{lcl}
\mathit{predicate} & ::= & \bot \\
 & & \top \\
 & & \neg\, \mathit{predicate} \\
 & & \mathit{predicate} \wedge \mathit{predicate} \\
 & & \mathit{predicate} \vee \mathit{predicate} \\
 & & \mathit{predicate} \Rightarrow \mathit{predicate} \\
 & & \mathit{predicate} \Leftrightarrow \mathit{predicate} \\
 & & \forall \mathit{var\_list} \cdot \mathit{predicate} \\
 & & \exists \mathit{var\_list} \cdot \mathit{predicate} \\
 & & [\mathit{var\_list} := \mathit{exp\_list}]\, \mathit{predicate} \\
 & & \\
\mathit{expression} & ::= & \mathit{variable} \\
 & & [\mathit{var\_list} := \mathit{exp\_list}]\, \mathit{expression} \\
 & & \mathit{expression} \mapsto \mathit{expression} \\
 & & \\
\mathit{variable} & ::= & \mathit{identifier}
\end{array}
$$

Rules of Inference for Existential Quantification

$$\frac{\mathrm{H},\ P\ \vdash\ Q}{\mathrm{H},\ \exists x \cdot P\ \vdash\ Q} \qquad \textbf{XST\_L}$$

- In rule XST_L, variable **x** is not free in **H** and **Q**

$$\frac{\mathrm{H}\ \vdash\ [x := E]P}{\mathrm{H}\ \vdash\ \exists x \cdot P} \qquad \textbf{XST\_R}$$

where **E** is an expression

Comparing the Quantification Rules

$$\frac{\mathsf{H},\ \forall x \cdot P,\ [x := E]P \ \vdash\ Q}{\mathsf{H},\ \forall x \cdot P \ \vdash\ Q} \quad \textbf{ALL\_L}$$

$$\frac{\mathsf{H} \ \vdash\ [x := E]P}{\mathsf{H} \ \vdash\ \exists x \cdot P} \quad \textbf{XST\_R}$$

$$\frac{\mathbf{H} \ \vdash\ \mathbf{P}}{\mathbf{H} \ \vdash\ \forall \mathbf{x} \cdot \mathbf{P}} \quad \textbf{ALL\_R}$$

$$\frac{\mathsf{H},\ P \ \vdash\ Q}{\mathsf{H},\ \exists x \cdot P \ \vdash\ Q} \quad \textbf{XST\_L}$$

CLASSICAL RESULTS (1)

commutativity	$\forall x \cdot \forall y \cdot P \quad \Leftrightarrow \quad \forall y \cdot \forall x \cdot P$ $\exists x \cdot \exists y \cdot P \quad \Leftrightarrow \quad \exists y \cdot \exists x \cdot P$
distributivity	$\forall x \cdot (P \wedge Q) \quad \Leftrightarrow \quad \forall x \cdot P \;\wedge\; \forall x \cdot Q$ $\exists x \cdot (P \vee Q) \quad \Leftrightarrow \quad \exists x \cdot P \;\vee\; \exists x \cdot Q$
associativity	if x not free in P $P \;\vee\; \forall x \cdot Q \quad \Leftrightarrow \quad \forall x \cdot (P \vee Q)$ $P \;\wedge\; \exists x \cdot Q \quad \Leftrightarrow \quad \exists x \cdot (P \wedge Q)$ $P \;\Rightarrow\; \forall x \cdot Q \quad \Leftrightarrow \quad \forall x \cdot (P \Rightarrow Q)$

CLASSICAL RESULTS (2)

de Morgan laws	$\neg\,\forall x\cdot P \;\Leftrightarrow\; \exists x\cdot\neg\,P$ $\neg\,\exists x\cdot P \;\Leftrightarrow\; \forall x\cdot\neg\,P$ $\neg\,\forall x\cdot(P \Rightarrow Q) \;\Leftrightarrow\; \exists x\cdot(P \wedge \neg\,Q)$ $\neg\,\exists x\cdot(P \wedge Q) \;\Leftrightarrow\; \forall x\cdot(P \Rightarrow \neg\,Q)$
monotonicity	$\forall x\cdot(P \Rightarrow Q) \;\Rightarrow\; (\forall x\cdot P \;\Rightarrow\; \forall x\cdot Q)$ $\forall x\cdot(P \Rightarrow Q) \;\Rightarrow\; (\exists x\cdot P \;\Rightarrow\; \exists x\cdot Q)$
equivalence	$\forall x\cdot(P \Leftrightarrow Q) \;\Rightarrow\; (\forall x\cdot P \;\Leftrightarrow\; \forall x\cdot Q)$ $\forall x\cdot(P \Leftrightarrow Q) \;\Rightarrow\; (\exists x\cdot P \;\Leftrightarrow\; \exists x\cdot Q)$

Summary of Logical Operators

$P \wedge Q$	$\neg\, P$
$P \;\vee\; Q$	$\forall x \cdot P$
$P \Rightarrow Q$	$\exists x \cdot P$

Refining our Language: Equality

$$
\begin{array}{lll}
\textit{predicate} & ::= & \bot \\
 & & \top \\
 & & \neg\, \textit{predicate} \\
 & & \textit{predicate} \;\wedge\; \textit{predicate} \\
 & & \textit{predicate} \;\vee\; \textit{predicate} \\
 & & \textit{predicate} \;\Rightarrow\; \textit{predicate} \\
 & & \textit{predicate} \;\Leftrightarrow\; \textit{predicate} \\
 & & \forall \textit{variable} \cdot \textit{predicate} \\
 & & \exists \textit{variable} \cdot \textit{predicate} \\
 & & [\textit{variable} := \textit{expression}]\; \textit{predicate} \\
 & & \textit{expression} = \textit{expression} \\
 & & \\
\textit{expression} & ::= & \cdots \\
 & & \\
\textit{variable} & ::= & \cdots
\end{array}
$$

Equality Rules of Inference

$$\frac{[x := F]H,\ E = F \ \vdash\ [x := F]P}{[x := E]H,\ E = F \ \vdash\ [x := E]P} \qquad \textbf{EQ\_LR}$$

$$\frac{[x := E]H,\ E = F \ \vdash\ [x := E]P}{[x := F]H,\ E = F \ \vdash\ [x := F]P} \qquad \textbf{EQ\_RL}$$

- Rewriting rules:

Operator	Predicate	Rewritten
Equality	$E = E$	$\top$
Equality of pairs	$E \mapsto F \ = \ G \mapsto H$	$E = G \ \wedge \ F = H$

Classical Results for Equality

symmetry transitivity	$E = F \;\Leftrightarrow\; F = E$ $E = F \;\wedge\; F = G \;\Rightarrow\; E = G$
One-point rules	if ***x*** not free in ***E*** $\forall x \cdot (x = E \;\Rightarrow\; P) \;\Leftrightarrow\; [x := E]P$ $\exists x \cdot (x = E \;\wedge\; P) \;\Leftrightarrow\; [x := E]P$

Refining our Language: Set Theory (1)

$$
\begin{array}{lll}
\textit{predicate} & ::= & \bot \\
& & \top \\
& & \neg\, \textit{predicate} \\
& & \textit{predicate} \;\wedge\; \textit{predicate} \\
& & \textit{predicate} \;\vee\; \textit{predicate} \\
& & \textit{predicate} \;\Rightarrow\; \textit{predicate} \\
& & \textit{predicate} \;\Leftrightarrow\; \textit{predicate} \\
& & \forall\, \textit{var\_list} \cdot \textit{predicate} \\
& & \exists\, \textit{var\_list} \cdot \textit{predicate} \\
& & [\textit{var\_list} := \textit{exp\_list}]\, \textit{predicate} \\
& & \textit{expression} \;=\; \textit{expression} \\
& & \textit{expression} \;\in\; \textit{set}
\end{array}
$$

Refining our Language: Set Theory (2)

$$
\begin{array}{lcl}
\mathit{expression} & ::= & \mathit{variable} \\
 & & [\mathit{var\_list} := \mathit{exp\_list}]\ \mathit{expression} \\
 & & \mathit{expression} \mapsto \mathit{expression} \\
 & & \mathit{set} \\
 & & \\
\mathit{variable} & ::= & \mathit{identifier} \\
 & & \\
\mathit{set} & ::= & \mathit{set} \times \mathit{set} \\
 & & \mathbb{P}(\mathit{set}) \\
 & & \{\ \mathit{var\_list} \cdot \mathit{predicate} \mid \mathit{expression}\ \}
\end{array}
$$

- When *expression* is the same as *var_list*, the last construct can be written $\{\ \mathit{var\_list} \mid \mathit{predicate}\ \}$

Set Theory

1. Basis
   - Basic operators
2. Extensions
   - Elementary operators
   - Generalization of elementary operators
   - Binary relation operators
   - Function operators

Set Theory: Membership

- Set theory deals with a new predicate: the membership predicate

$$E \in S$$

where E is an expression and S is a set

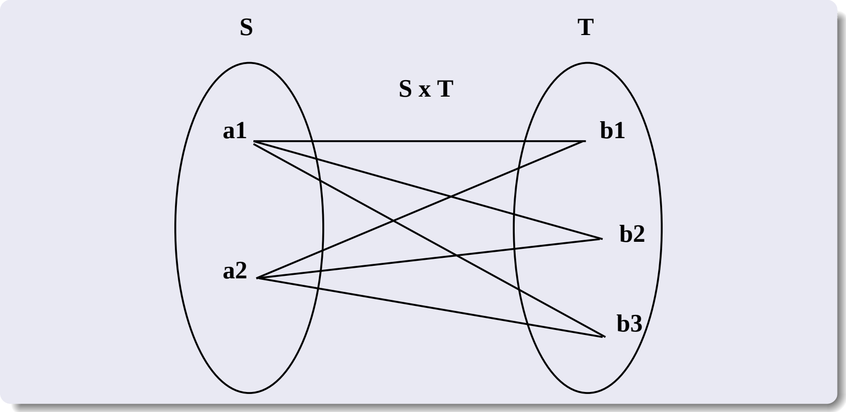
Set Theory: Basic Constructs

There are three basic constructs in set theory:

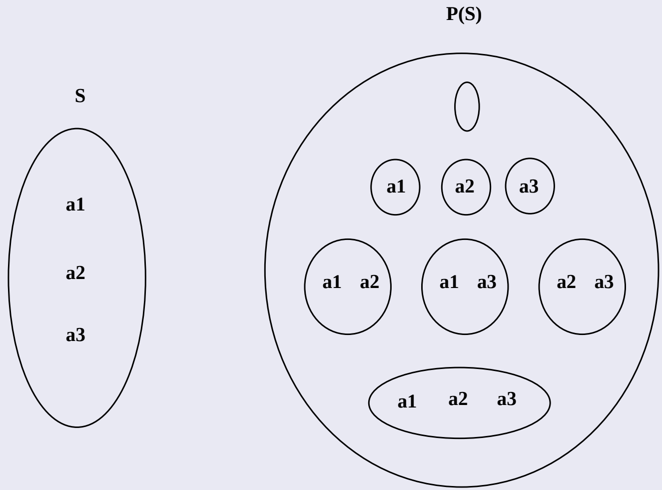
Cartesian product	$S \times T$
Power set	$\mathbb{P}(S)$
Comprehension 1	$\{x \cdot P \mid F\}$
Comprehension 2	$\{x \mid P\}$

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

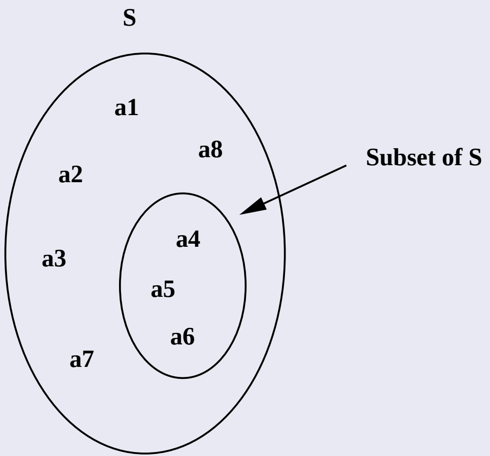
Cartesian Product



Power Set



Set Comprehension



Basic Set Operator Memberships (Axioms)

These axioms are defined by equivalences.

Left Part	Right Part
$E \mapsto F \in S \times T$	$E \in S \;\; \land \;\; F \in T$
$S \in \mathbb{P}(T)$	$\forall x \cdot (\, x \in S \;\Rightarrow\; x \in T \,)$ (x is not free in S and T)
$E \in \{x \cdot P \mid F\}$	$\exists x \cdot P \;\land\; E = F$ (x is not free in E)
$E \in \{x \mid P\}$	$[x := E]P$ (x is not free in E)

Hochschule Zürich
Technology Zurich

Set Inclusion and Extensionality Axiom

Left Part	Right Part
$S \subseteq T$	$S \in \mathbb{P}(T)$
$S = T$	$S \subseteq T \quad \wedge \quad T \subseteq S$

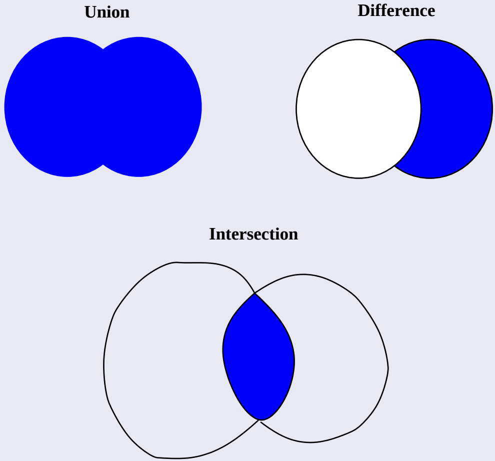
The first rule is just a syntactic extension

The second rule is the Extensionality Axiom

Elementary Set Operators

Union	$S \cup T$
Intersection	$S \cap T$
Difference	$S \setminus T$
Extension	$\{a, \ldots, b\}$
Empty set	$\varnothing$

Union, Difference, Intersection



Elementary Set Operator Memberships

$E \in S \cup T$	$E \in S \ \vee \ E \in T$
$E \in S \cap T$	$E \in S \ \wedge \ E \in T$
$E \in S \setminus T$	$E \in S \ \wedge \ E \notin T$
$E \in \{a, \ldots, b\}$	$E = a \ \vee \ \ldots \ \vee \ E = b$
$E \in \varnothing$	$\bot$

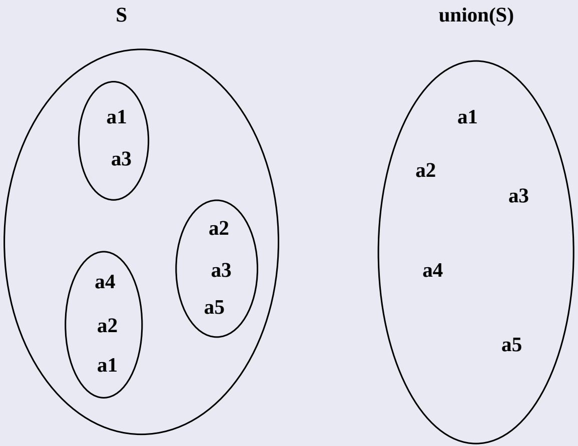
Summary of Basic and Elementary Operators

$S \times T$	$S \cup T$
$\mathbb{P}(S)$	$S \cap T$
$\{\, x \cdot P \mid F \,\}$	$S \setminus T$
$S \subseteq T$	$\{a, \ldots, b\}$
$S = T$	$\varnothing$

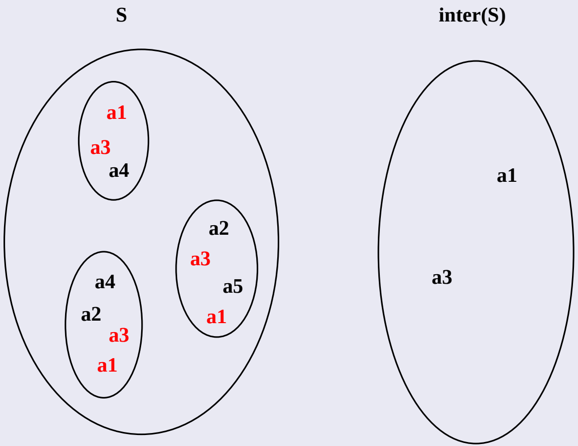
Generalizations of Elementary Operators

Generalized Union	$\mathrm{union}\,(S)$
Union Quantifier	$\bigcup x \cdot (P \mid T)$
Generalized Intersection	$\mathrm{inter}\,(S)$
Intersection Quantifier	$\bigcap x \cdot (P \mid T)$

Generalized Union



Generalized Intersection



Generalizations of Elementary Operator Memberships

$E \in \mathrm{union}(S)$	$\exists s \cdot s \in S \wedge E \in s$ (s is not free in S and E)
$E \in (\bigcup x \cdot P \mid T)$	$\exists x \cdot P \wedge E \in T$ (x is not free in E)
$E \in \mathrm{inter}(S)$	$\forall s \cdot s \in S \Rightarrow E \in s$ (s is not free in S and E)
$E \in (\bigcap x \cdot P \mid T)$	$\forall x \cdot P \Rightarrow E \in T$ (x is not free in E)

Well-definedness condition for case 3: $S \neq \varnothing$
Well-definedness condition for case 4: $\exists x \cdot P$

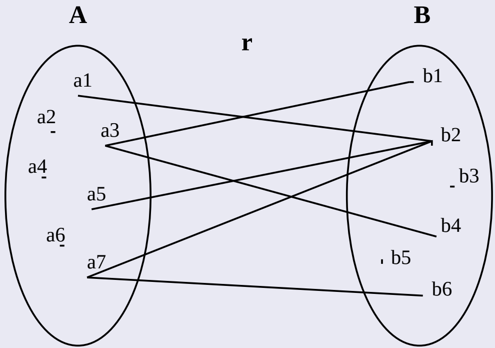
Summary of Generalizations of Elementary Operators

$\mathrm{union}\,(S)$
$\bigcup x \cdot P \mid T$
$\mathrm{inter}\,(S)$
$\bigcap x \cdot P \mid T$

Binary Relation Operators (1)

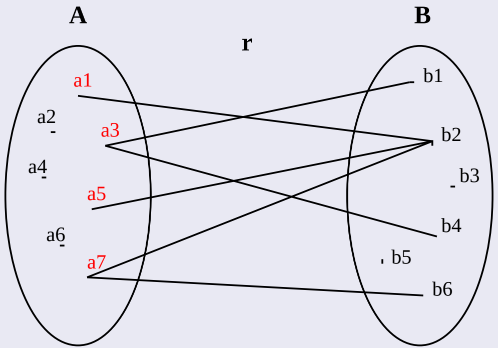
Binary relations	$S \leftrightarrow T$
Domain	$\mathrm{dom}\,(r)$
Range	$\mathrm{ran}\,(r)$
Converse	r^{-1}

A Binary Relation r from a Set A to a Set B



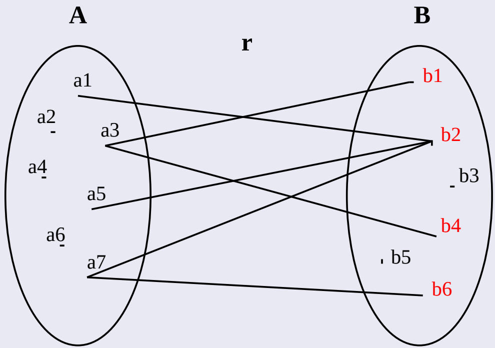
$$r \in A \leftrightarrow B$$

Domain of Binary Relation r



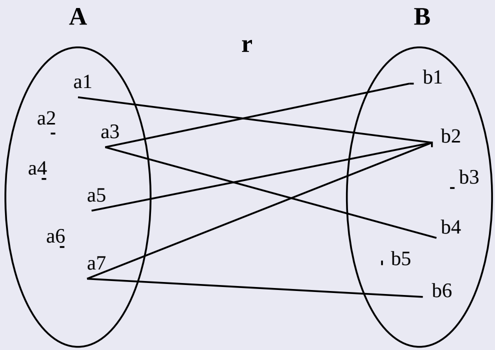
$$\mathrm{dom}(r) = \{a1, a3, a5, a7\}$$

Range of Binary Relation r



$$\mathrm{ran}(r) \;=\; \{b1, b2, b4, b6\}$$

Converse of Binary Relation r



$$r^{-1} = \{b1 \mapsto a3, b2 \mapsto a1, b2 \mapsto a5, b2 \mapsto a7, b4 \mapsto a3, b6 \mapsto a7\}$$

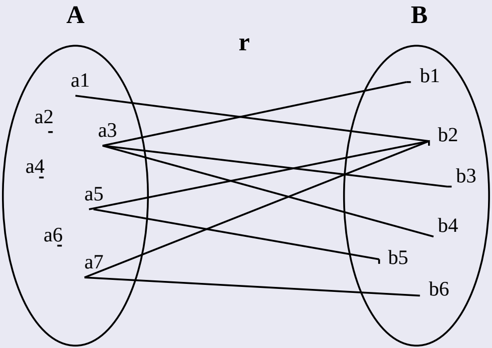
Binary Relation Operator Memberships (1)

Left Part	Right Part
$r \in S \leftrightarrow T$	$r \subseteq S \times T$
$E \in \mathrm{dom}\,(r)$	$\exists y \cdot E \mapsto y \;\in\; r$ (y is not free in E and r)
$F \in \mathrm{ran}\,(r)$	$\exists x \cdot x \mapsto F \;\in\; r$ (x is not free in F and r)
$E \mapsto F \in r^{-1}$	$F \mapsto E \in r$

Binary Relation Operators (2)

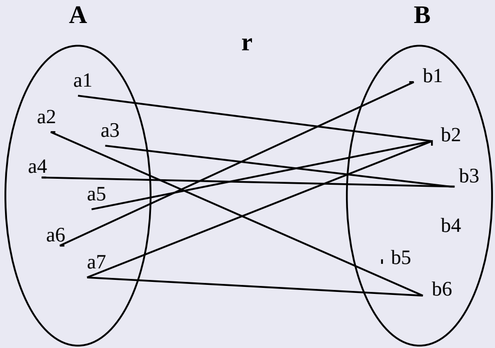
Partial surjective binary relations	$S \mathbin{\leftarrow\!\!\!\twoheadrightarrow} T$
Total binary relations	$S \mathbin{\twoheadleftarrow\!\!\!\rightarrow} T$
Total surjective binary relations	$S \mathbin{\twoheadleftarrow\!\!\!\twoheadrightarrow} T$

A Partial Surjective Relation



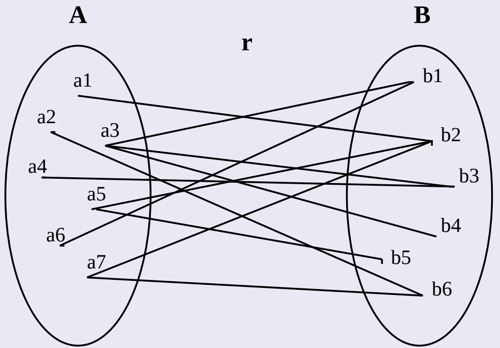
$$r \in A \leftrightarrow\!\!\!\!\rightarrow B$$

A Total Relation



$$r \in A \leftrightarrow\!\!\!\!\rightarrow B$$

A Total Surjective Relation



$$r \in A \twoheadleftrightarrow B$$

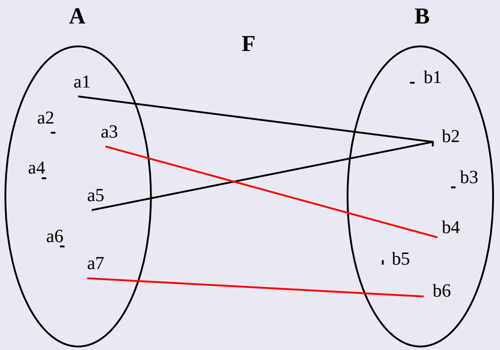
Binary Relation Operator Memberships (2)

Left Part	Right Part
$r \in S \mathrel{\leftarrow\!\!\twoheadrightarrow} T$	$r \in S \leftrightarrow T \;\land\; \mathrm{ran}(r) = T$
$r \in S \mathrel{\twoheadleftarrow\!\!\rightarrow} T$	$r \in S \leftrightarrow T \;\land\; \mathrm{dom}(r) = S$
$r \in S \mathrel{\twoheadleftarrow\!\!\twoheadrightarrow} T$	$r \in S \mathrel{\leftarrow\!\!\twoheadrightarrow} T \;\land\; r \in S \mathrel{\twoheadleftarrow\!\!\rightarrow} T$

Binary Relation Operators (3)

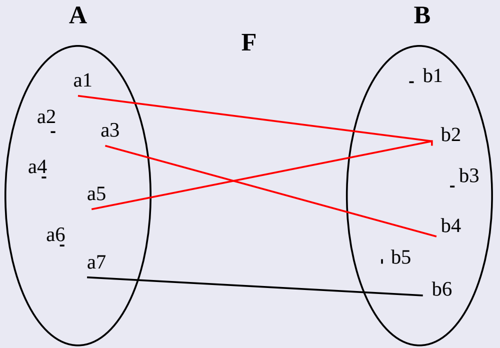
Domain restriction	$S \lhd r$
Range restriction	$r \rhd T$
Domain subtraction	$S \lhd\!\!- r$
Range subtraction	$r \rhd\!\!- T$

The Domain Restriction Operator



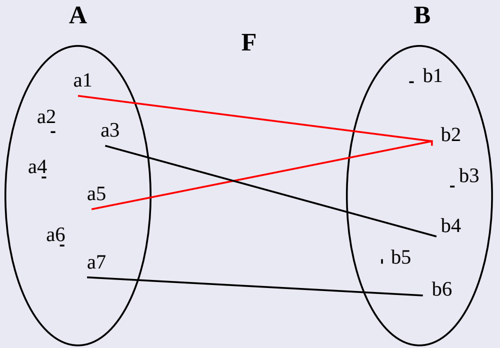
$\{a3,\ a7\} \lhd F$

The Range Restriction Operator



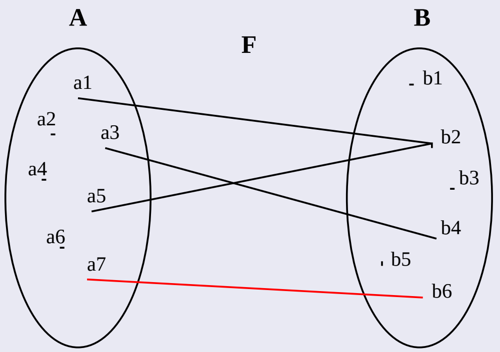
$F \rhd \{b2, b4\}$

The Domain Substraction Operator



$$\{a3,\ a7\} \lhd F$$

The Range Substraction Operator



$F \rhd \{b2, b4\}$

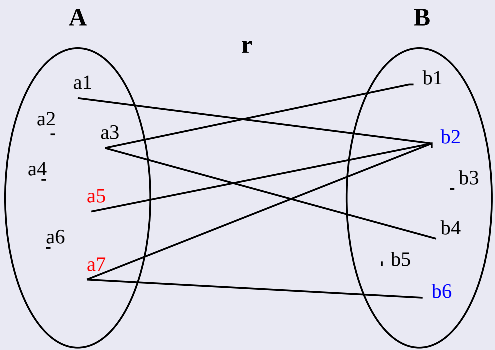
Binary Relation Operator Memberships (3)

Left Part	Right Part
$E \mapsto F \in S \lhd r$	$E \in S \;\wedge\; E \mapsto F \in r$
$E \mapsto F \in r \rhd T$	$E \mapsto F \in r \;\wedge\; F \in T$
$E \mapsto F \in S ⩤ r$	$E \notin S \;\wedge\; E \mapsto F \in r$
$E \mapsto F \in r ⩥ T$	$E \mapsto F \in r \;\wedge\; F \notin T$

Binary Relation Operators (4)

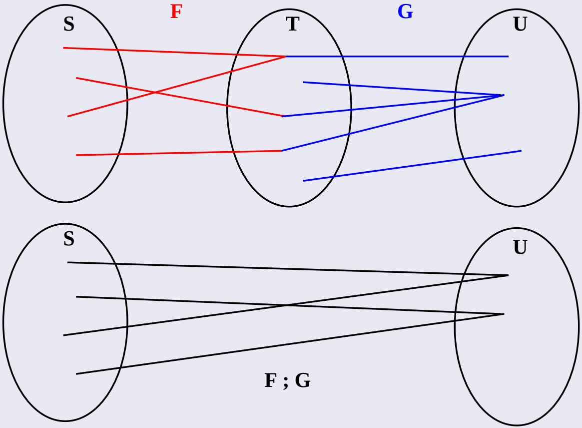
Image	$r[w]$
Composition	$p\,;\,q$
Overriding	$p \Leftarrow q$
Identity	$\mathrm{id}\,(S)$

Image of $\{a5, a7\}$ under r

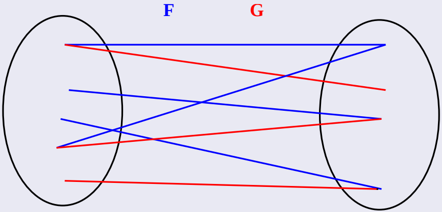


$$r[\{a5, a7\}] = \{b2, b6\}$$

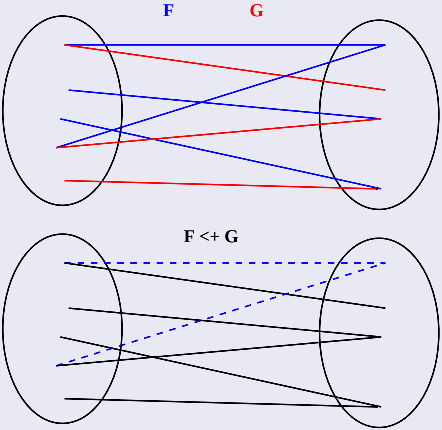
Forward Composition



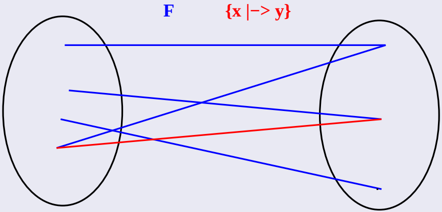
The Overriding Operator



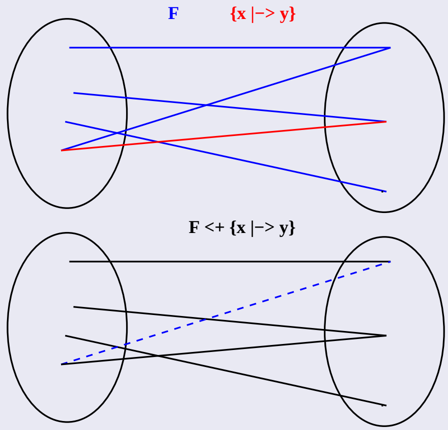
The Overriding Operator



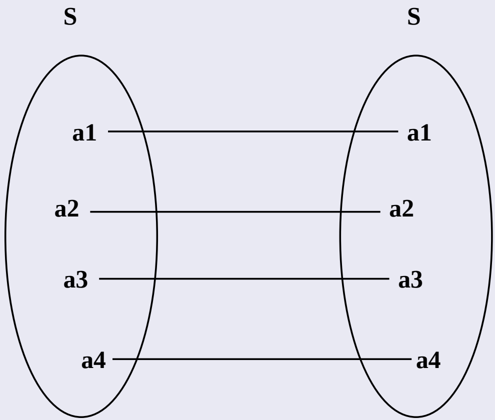
Special Case



Special Case



The Identity Relation



Binary Relation Operator Memberships (4)

$F \in r[w]$	$\exists x \cdot x \in w \;\wedge\; x \mapsto F \in r$ (x is not free in F, r and w)
$E \mapsto F \in (p\,;q)$	$\exists x \cdot E \mapsto x \in p \;\wedge\; x \mapsto F \in q$ (x is not free in E, F, p and q)
$E \mapsto F \in p \Leftarrow q$	$E \mapsto F \in (\mathrm{dom}\,(q) \lhd p) \;\cup\; q$
$E \mapsto F \in \mathrm{id}\,(S)$	$E \in S \;\wedge\; F = E$

Binary Relation Operators (5)

Direct Product	$p \otimes q$
First Projection	$\text{prj}_1(S, T)$
Second Projection	$\text{prj}_2(S, T)$
Parallel Product	$p \parallel q$

Binary Relation Operator Memberships (5)

$E \mapsto (F \mapsto G) \in p \otimes q$	$E \mapsto F \in p \;\wedge\; E \mapsto G \in q$
$(E \mapsto F) \mapsto G \in \mathrm{prj}_1(S,T)$	$E \in S \;\wedge\; F \in T \;\wedge\; G = E$
$(E \mapsto F) \mapsto G \in \mathrm{prj}_2(S,T)$	$E \in S \;\wedge\; F \in T \;\wedge\; G = F$
$(E \mapsto G) \mapsto (F \mapsto H) \in p \parallel q$	$E \mapsto F \in p \;\wedge\; G \mapsto H \in q$

Summary of Binary Relation Operators

$S \leftrightarrow T$	$S \lhd r$	$r[w]$	$\mathrm{prj}_1\,(S, T)$
$\mathrm{dom}\,(r)$	$r \rhd T$	$p\,;q$	$\mathrm{prj}_2\,(S, T)$
$\mathrm{ran}\,(r)$	$S \mathbin{⩤} r$	$p \mathbin{<\!\!+} q$	$\mathrm{id}\,(S)$
r^{-1}	$r \mathbin{⩥} T$	$p \otimes q$	$p \parallel q$

Classical Results with Relation Operators

$$r^{-1-1} = r$$

$$\mathrm{dom}(r^{-1}) \;=\; \mathrm{ran}(r)$$

$$(S \lhd r)^{-1} \;=\; r^{-1} \rhd S$$

$$(p\,;q)^{-1} \;=\; q^{-1}\,;p^{-1}$$

$$(p\,;q)\,;r \;=\; q\,;(p\,;r)$$

$$(p\,;q)[w] \;=\; q[p[w]]$$

$$p\,;(q \cup r) \;=\; (p\,;q) \;\cup\; (p\,;r)$$

$$r[a \cup b] \;=\; r[a] \cup r[b]$$

$$\ldots$$

Hochschule Zürich
echnology Zurich

More classical Results

Given a relation r such that $r \in S \leftrightarrow S$

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

Translations into First Order Predicates

Given a relation r such that $r \in S \leftrightarrow S$

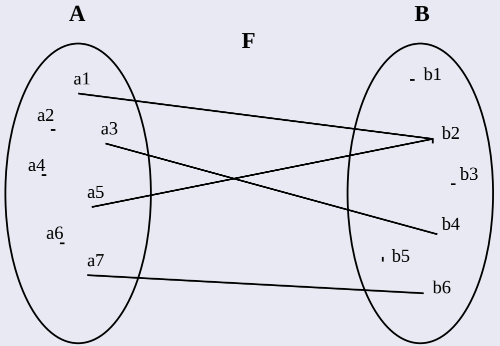
$r = r^{-1}$	$\forall x, y \cdot x \in S \land y \in S \Rightarrow (x \mapsto y \in r \Leftrightarrow y \mapsto x \in r)$
$r \cap r^{-1} = \varnothing$	$\forall x, y \cdot x \mapsto y \in r \Rightarrow y \mapsto x \notin r$
$r \cap r^{-1} \subseteq \mathrm{id}(S)$	$\forall x, y \cdot x \mapsto y \in r \land y \mapsto x \in r \Rightarrow x = y$
$\mathrm{id}(S) \subseteq r$	$\forall x \cdot x \in S \Rightarrow x \mapsto x \in r$
$r \cap \mathrm{id}(S) = \varnothing$	$\forall x, y \cdot x \mapsto y \in r \Rightarrow x \neq y$
$r ; r \subseteq r$	$\forall x, y, z \cdot x \mapsto y \in r \land y \mapsto z \in r \Rightarrow x \mapsto z \in r$

Set-theoretic statements are far more readable than predicate calculus statements

Function Operators (1)

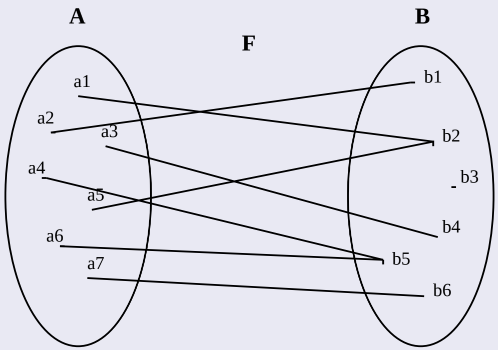
Partial functions	$S \mathrel{+\!\!\!\rightarrow} T$
Total functions	$S \rightarrow T$
Partial injections	$S \mathrel{\rightarrowtail\!\!\!\!\!\!+} T$
Total injections	$S \rightarrowtail T$

A Partial Function F from a Set A to a Set B



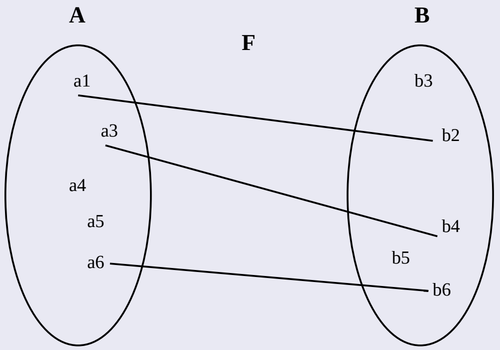
$$F \in A \mathrel{+\!\!\!\rightarrow} B$$

A Total Function F from a Set A to a Set B



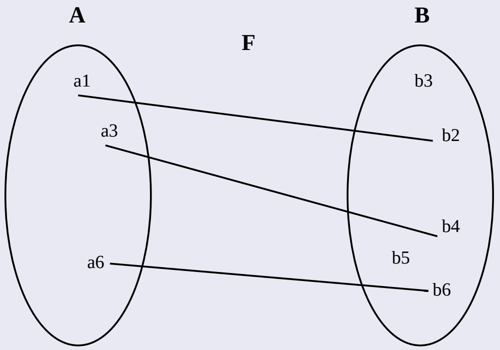
$$F \in A \rightarrow B$$

A Partial Injection F from a Set A to a Set B



$$F \in A \rightarrowtail\!\!\!\!\!\!\!+\, B$$

A Total Injection F from a Set A to a Set B



$F \in A \rightarrowtail B$

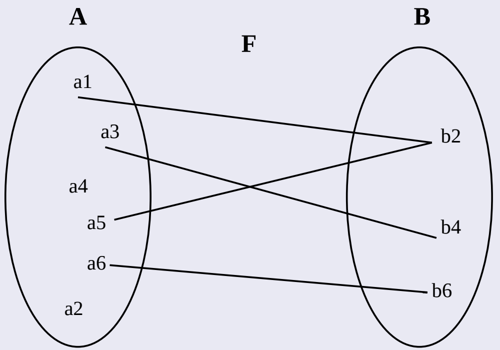
Function Operator Memberships (1)

Left Part	Right Part
$f \in S \mathrel{+\!\!\!\rightarrow} T$	$f \in S \leftrightarrow T \;\; \wedge \;\; (f^{-1} \,;\, f) = \mathrm{id}(\mathrm{ran}(f))$
$f \in S \rightarrow T$	$f \in S \mathrel{+\!\!\!\rightarrow} T \;\; \wedge \;\; s = \mathrm{dom}(f)$
$f \in S \mathrel{\rightarrowtail\!\!\!\!\!+} T$	$f \in S \mathrel{+\!\!\!\rightarrow} T \;\; \wedge \;\; f^{-1} \in T \mathrel{+\!\!\!\rightarrow} S$
$f \in S \rightarrowtail T$	$f \in S \rightarrow T \;\; \wedge \;\; f^{-1} \in T \mathrel{+\!\!\!\rightarrow} S$

Function Operators (2)

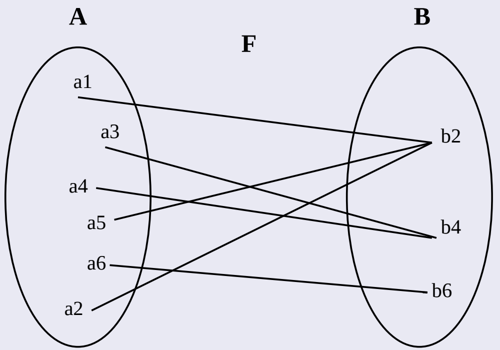
Partial surjections	$S \twoheadrightarrow\!\!\!\!\!\!\!+\;\; T$
Total surjections	$S \twoheadrightarrow T$
Bijections	$S \rightarrowtail\!\!\!\!\!\twoheadrightarrow T$

A Partial Surjection F from a Set A to a Set B



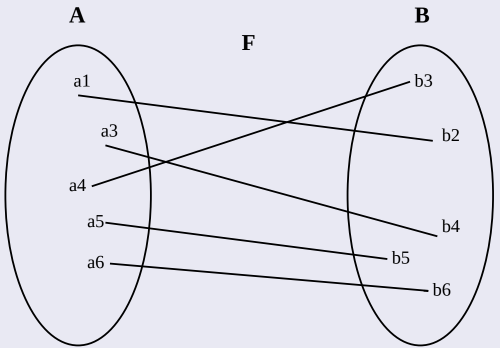
$$F \in A \twoheadrightarrow\!\!\!\!\!+ \; B$$

A Total Surjection F from a Set A to a Set B



$F \in A \twoheadrightarrow B$

A Bijection F from a Set A to a Set B



$$F \in A \rightarrowtail\!\!\!\!\twoheadrightarrow B$$

Function Operator Memberships (2)

Left Part	Right Part
$f \in S \twoheadrightarrow\!\!\!\!\!\!\shortmid\;\; T$	$f \in S \nrightarrow T \quad \wedge \quad T = \mathrm{ran}(f)$
$f \in S \twoheadrightarrow T$	$f \in S \rightarrow T \quad \wedge \quad T = \mathrm{ran}(f)$
$f \in S \rightarrowtail\!\!\!\!\!\twoheadrightarrow T$	$f \in S \rightarrowtail T \quad \wedge \quad f \in S \twoheadrightarrow T$

Summary of Function Operators

$S ⇸ T$	$S ⤀ T$
$S \rightarrow T$	$S \twoheadrightarrow T$
$S ⤔ T$	$S ⤖ T$
$S \rightarrowtail T$	

Summary of all Set-theoretic Operators (40)

$S \times T$	$S \setminus T$	r^{-1}	$r[w]$	$\mathrm{id}\,(S)$	$\{\,x \mid x \in S \;\land\; P\,\}$
$\mathbb{P}(S)$	$S \leftrightarrow T$ $S \trel T$	$S \lhd r$ $S \domsub r$	$p \,;\, q$	$S \pfun T$ $S \rightarrow T$	$\{\,x \cdot x \in S \;\land\; P \mid E\}$
$S \subseteq T$	$S \srel T$ $S \strel T$	$r \rhd T$ $r \ransub T$	$p \ovl q$	$S \pinj T$ $S \tinj T$	$\{\,a,\; b,\; \ldots,\; n\,\}$
$S \cup T$	$\mathrm{dom}\,(r)$ $\mathrm{ran}\,(r)$	prj_1	$p \otimes q$	$S \psur T$ $S \twoheadrightarrow T$	union $\bigcup$
$S \cap T$	$\varnothing$	prj_2	$p \parallel q$	$S \tbij T$	inter $\bigcap$

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Applying a Function

Given a partial function f, we have

Left Part	Right Part
$F = f(E)$	$E \mapsto F \in f$

Well-definedness condition: $E \in \mathrm{dom}\,(f)$

Example: a Very Strict Society

- Every person is either a man or a woman
- But no person can be a man and a woman at the same time
- Only women have husbands, who must be a man
- Woman have at most one husband
- Likewise, men have at most one wife
- Moreover, mother are married women

Formal Representation

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\!\!\!\;\shortmid\;\; men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

- Every person is either a man or a woman.
- But no person can be a man and a woman at the same time.
- Only women have husbands, who must be a man.
- Woman have at most one husband.
- Likewise, men have at most one wife.
- Moreover, mother are married women.

Formal Representation

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\!\!\!+\; men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

- Every person is either a man or a woman.
- But no person can be a man and a woman at the same time.
- Only women have husbands, who must be a man.
- Woman have at most one husband.
- Likewise, men have at most one wife.
- Moreover, mother are married women.

Formal Representation

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\!\!\!+\; men$$

$$mother \in PERSON \to \mathrm{dom}(husband)$$

- Every person is either a man or a woman.
- But no person can be a man and a woman at the same time.
- Only women have husbands, who must be a man.
- Woman have at most one husband.
- Likewise, men have at most one wife.
- Moreover, mother are married women.

Defining New Concepts

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\!\rightarrow men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

$$wife = husband^{-1}$$

$$spouse = husband \cup wife$$

$$father = mother \; ; \; husband$$

Defining New Concepts

$$
\begin{aligned}
men &\subseteq PERSON \\
women &= PERSON \setminus men \\
husband &\in women \rightarrowtail\!\!\!\!\!\twoheadrightarrow men \\
mother &\in PERSON \rightarrow \mathrm{dom}(husband)
\end{aligned}
$$

$$
\begin{aligned}
wife &= husband^{-1} \\
spouse &= husband \cup wife \\
father &= mother \; ; \; husband
\end{aligned}
$$

Defining New Concepts

$$
\begin{aligned}
men &\subseteq PERSON \\
women &= PERSON \setminus men \\
husband &\in women \mathrel{\mkern 6mu\mapstochar\mkern -6mu\rightarrowtail} men \\
mother &\in PERSON \rightarrow \mathrm{dom}(husband)
\end{aligned}
$$

$$
\begin{aligned}
wife &= husband^{-1} \\
spouse &= husband \cup wife \\
father &= mother \; ; \; husband
\end{aligned}
$$

Defining New Concepts

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\twoheadrightarrow men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

$$wife = husband^{-1}$$

$$spouse = husband \cup wife$$

$$father = mother\ ;\ husband$$

Defining New Concepts

$$
\begin{aligned}
men &\subseteq PERSON \\
women &= PERSON \setminus men \\
husband &\in women \rightarrowtail\!\!\!\!\!\twoheadrightarrow men \\
mother &\in PERSON \rightarrow \mathrm{dom}(husband)
\end{aligned}
$$

$$
\begin{aligned}
father &= mother \,;\, husband \\
children &= (mother \cup father)^{-1} \\
daughter &= children \rhd women \\
sibling &= (children^{-1} \,;\, children) \setminus \mathrm{id}(PERSON)
\end{aligned}
$$

Defining New Concepts

$$\mathit{men} \subseteq \mathit{PERSON}$$

$$\mathit{women} = \mathit{PERSON} \setminus \mathit{men}$$

$$\mathit{husband} \in \mathit{women} \rightarrowtail\!\!\!\!\twoheadrightarrow \mathit{men}$$

$$\mathit{mother} \in \mathit{PERSON} \rightarrow \mathrm{dom}(\mathit{husband})$$

$$\mathit{father} = \mathit{mother} \,;\, \mathit{husband}$$

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

$$\mathit{daughter} = \mathit{children} \rhd \mathit{women}$$

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

Defining New Concepts

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women ⤔ men$$

$$mother \in PERSON \to \mathrm{dom}(husband)$$

$$father = mother \,;\, husband$$

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

$$daughter = children \rhd women$$

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

Defining New Concepts

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

$$husband \in women \rightarrowtail\!\!\!\!\!\!\twoheadrightarrow men$$

$$mother \in PERSON \rightarrow \mathrm{dom}(husband)$$

$$father = mother \,;\, husband$$

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

$$daughter = children \rhd women$$

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

Exercises. To be defined

$$brother \;=\; ?$$

$$sibling - in - law \;=\; ?$$

$$nephew - or - niece \;=\; ?$$

$$uncle - or - aunt \;=\; ?$$

$$cousin \;=\; ?$$

Exercises. To be proved

$$mother = father \; ; \; wife$$

$$spouse = spouse^{-1}$$

$$sibling = sibling^{-1}$$

$$cousin = cousin^{-1}$$

$$father \; ; \; father^{-1} = mother \; ; \; mother^{-1}$$

$$father \; ; \; mother^{-1} = \varnothing$$

$$mother \; ; \; father^{-1} = \varnothing$$

$$father \; ; \; children = mother \; ; \; children$$

For Further Reading I

J-R. Abrial.
Modeling in Event-B: System and Software Engineering, Chapter 9 — Mathematical Language.
CUP, 2010.