Event-B Course

6. Summary of Mathematical Notation and Proofs

Jean-Raymond Abrial

September-October-November 2011

Purpose of this Presentation

- Foundation for deductive and formal proofs

- A quick review of Propositional Calculus

- A quick review of First Order Predicate Calculus

- Refresher on Set Theory

- Formalising Data Structures (list, tree, graph)

- 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 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

Foundation for Deductive (and formal) Proofs

- Concepts of Sequent and Inference Rule

- Backward and Forward Reasoning

- Basic Inference Rules

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

- We are given:
  - a collection $\mathcal{T}$ of inference rules of the form $\frac{A}{C}$
  - a sequent container K, containining 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 $\dfrac{}{S2}$ **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 $S1$

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

$$\begin{tikzcd}[column sep=small]
 & \begin{array}{c} S1 \\ \textbf{r3} \end{array} \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{array}{c} S2 \\ \textbf{?} \end{array} & \begin{array}{c} S3 \\ \textbf{?} \end{array} & \begin{array}{c} S4 \\ \textbf{?} \end{array}
\end{tikzcd}$$

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

$$\swarrow \quad \downarrow \quad \searrow$$

$S2$ **r1** $\quad$ $S3$ **?** $\quad$ $S4$ **?**

Proof of $S1$

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

$$\begin{tikzcd}
 & \begin{matrix} S1 \\ \mathbf{r3} \end{matrix} \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{matrix} S2 \\ \mathbf{r1} \end{matrix} & \begin{matrix} S3 \\ \mathbf{r5} \end{matrix} \arrow[dl] \arrow[d] & \begin{matrix} S4 \\ \mathbf{?} \end{matrix} \\
\begin{matrix} S5 \\ \mathbf{?} \end{matrix} & \begin{matrix} S6 \\ \mathbf{?} \end{matrix} &
\end{tikzcd}$$

Proof of $S1$

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

$$\begin{tikzcd} & \begin{array}{c} S1 \\ \mathbf{r3} \end{array} \arrow[dl] \arrow[d] \arrow[dr] & \\ \begin{array}{c} S2 \\ \mathbf{r1} \end{array} & \begin{array}{c} S3 \\ \mathbf{r5} \end{array} \arrow[dl] \arrow[d] & \begin{array}{c} S4 \\ \mathbf{?} \end{array} \\ \begin{array}{c} S5 \\ \mathbf{r4} \end{array} & \begin{array}{c} S6 \\ \mathbf{?} \end{array} & \end{tikzcd}$$

Proof of $S1$

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

$$\begin{tikzcd}
 & \begin{array}{c} S1 \\ \textbf{r3} \end{array} \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{array}{c} S2 \\ \textbf{r1} \end{array} & \begin{array}{c} S3 \\ \textbf{r5} \end{array} \arrow[dl] \arrow[d] & \begin{array}{c} S4 \\ \textbf{?} \end{array} \\
\begin{array}{c} S5 \\ \textbf{r4} \end{array} & \begin{array}{c} S6 \\ \textbf{r6} \end{array} &
\end{tikzcd}$$

Proof of $S1$

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

$$\begin{tikzcd}
 & \begin{array}{c} S1 \\ \textbf{r3} \end{array} \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{array}{c} S2 \\ \textbf{r1} \end{array} & \begin{array}{c} S3 \\ \textbf{r5} \end{array} \arrow[dl] \arrow[d] & \begin{array}{c} S4 \\ \textbf{r2} \end{array} \arrow[d] \\
\begin{array}{c} S5 \\ \textbf{r4} \end{array} & \begin{array}{c} S6 \\ \textbf{r6} \end{array} & \begin{array}{c} S7 \\ \textbf{?} \end{array}
\end{tikzcd}$$

Proof of $S1$

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

$$\begin{tikzcd}
 & S1 \atop \mathbf{r3} \arrow[dl] \arrow[d] \arrow[dr] & \\
S2 \atop \mathbf{r1} & S3 \atop \mathbf{r5} \arrow[dl] \arrow[d] & S4 \atop \mathbf{r2} \arrow[d] \\
S5 \atop \mathbf{r4} & S6 \atop \mathbf{r6} & S7 \atop \mathbf{r7}
\end{tikzcd}$$

Recording the Proof of Sequent $S1$

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

$$\begin{tikzcd}[column sep=small]
& & \begin{array}{c} S1 \\ \textbf{r3} \end{array} \arrow[dll] \arrow[d] \arrow[drr] & & \\
\begin{array}{c} S2 \\ \textbf{r1} \end{array} & & \begin{array}{c} S3 \\ \textbf{r5} \end{array} \arrow[dll] \arrow[d] & & \begin{array}{c} S4 \\ \textbf{r2} \end{array} \arrow[d] \\
\begin{array}{c} S5 \\ \textbf{r4} \end{array} & & \begin{array}{c} S6 \\ \textbf{r6} \end{array} & & \begin{array}{c} S7 \\ \textbf{r7} \end{array}
\end{tikzcd}$$

- 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:

$$
\begin{tikzcd}
 & \begin{array}{c} S1 \\ \mathbf{r3} \end{array} \arrow[dl] \arrow[d] \arrow[dr] & \\
\begin{array}{c} S2 \\ \mathbf{r1} \end{array} & \begin{array}{c} S3 \\ \mathbf{r5} \end{array} \arrow[dl] \arrow[d] & \begin{array}{c} S4 \\ \mathbf{r2} \end{array} \arrow[d] \\
\begin{array}{c} S5 \\ \mathbf{r4} \end{array} & \begin{array}{c} S6 \\ \mathbf{r6} \end{array} & \begin{array}{c} S7 \\ \mathbf{r7} \end{array}
\end{tikzcd}
$$

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

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 $\dfrac{}{S2}$ **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**
		$S5$	**?**
		$S6$	**?**
	$S4$		**?**

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**
		$S6$		**?**
	$S4$			**?**

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 $\dfrac{}{S2}$ **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** $\dfrac{}{S7}$

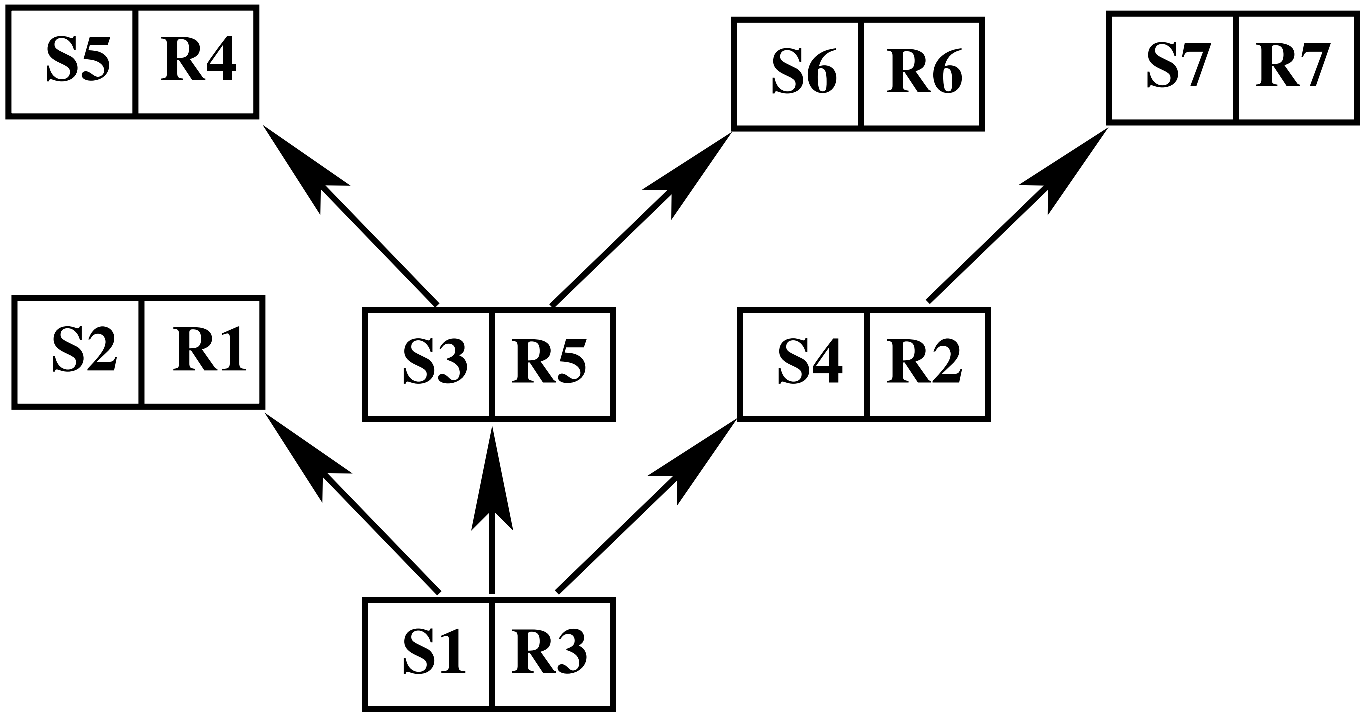
$S1$			**r3**
	$S2$		**r1**
	$S3$		**r5**
		$S5$	**r4**
		$S6$	**r6**
	$S4$		**r2**
		$S7$	**?**

Proof of $S1$

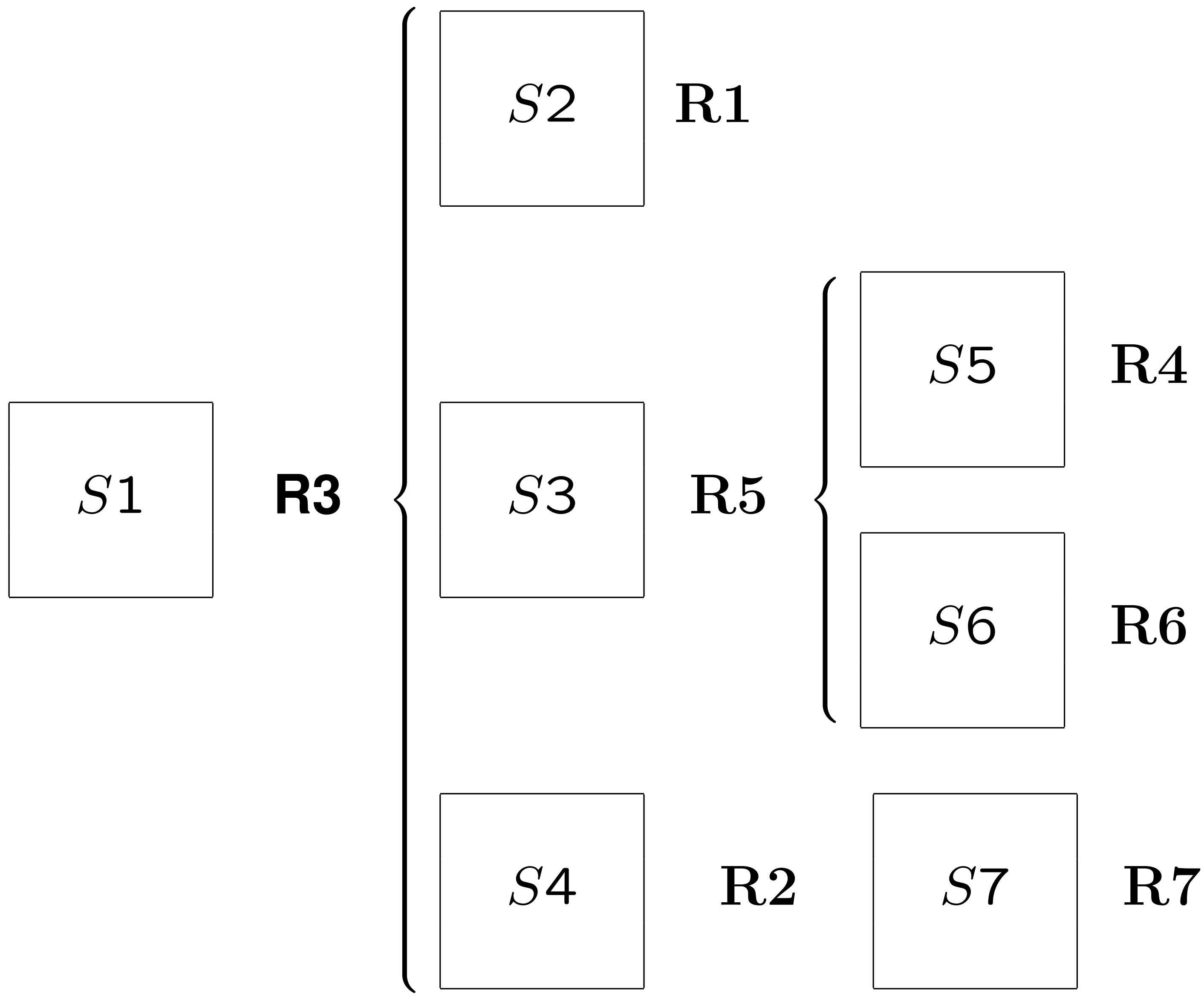
r1 $\dfrac{}{S2}$ **r2** $\dfrac{S7}{S4}$ **r3** $\dfrac{S2 \quad S3 \quad S4}{S1}$ **r4** $\dfrac{}{S5}$ **r5** $\dfrac{S5 \quad S6}{S3}$ **r6** $\dfrac{}{S6}$ **r7** $\dfrac{}{S7}$

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

Other Representations of the Proof(1)



Other Representations of the Proof (2)



Foundation for Deductive (and formal) Proofs

- Concepts of Sequent and Inference Rule

- Backward and Forward Reasoning

- Basic Inference Rules

More on Sequent

- We supposedly have a Predicate Language (not defined yet)

- A sequent is denoted by:

$$\boxed{\text{H} \vdash G}$$

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

- G is a predicate: the goal

$$\boxed{\text{Under the hypotheses of collection H, prove the goal } G}$$

- 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

$$\frac{}{\mathbf{H},\ P \ \vdash \ P}\ \text{HYP}$$

$$\frac{\mathbf{H} \ \vdash \ Q}{\mathbf{H},\ P \ \vdash \ Q}\ \text{MON}$$

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

Purpose of this Presentation

- Foundation for deductive and formal proofs

- A quick review of Propositional Calculus

- A quick review of First Order Predicate Calculus

- Refresher on Set Theory

- Formalising Data Structures (list, tree, graph)

- Given predicates P and Q, we can construct:

- CONJUNCTION: $P \wedge Q$

- IMPLICATION: $P \Rightarrow Q$

- NEGATION: $\neg P$

$$
\begin{array}{lll}
Predicate & ::= & Predicate \ \wedge \ Predicate \\
 & & Predicate \ \Rightarrow \ Predicate \\
 & & \neg \ Predicate
\end{array}
$$

- This syntax is ambiguous

- Pairs of matching parentheses can be added freely.

- Operator $\wedge$ is left associative.

- So, $\boldsymbol{P} \wedge \boldsymbol{Q} \wedge \boldsymbol{R}$ is to be read $(\boldsymbol{P} \wedge \boldsymbol{Q}) \wedge \boldsymbol{R}$.

- Operator $\Rightarrow$ is not associative: $\boldsymbol{P} \Rightarrow \boldsymbol{Q} \Rightarrow \boldsymbol{R}$ is not allowed.

- Write explicitly $(\boldsymbol{P} \Rightarrow \boldsymbol{Q}) \Rightarrow \boldsymbol{R}$ or $\boldsymbol{P} \Rightarrow (\boldsymbol{Q} \Rightarrow \boldsymbol{R})$.

- Operators have precedence in this decreasing order: $\neg$, $\wedge$, $\Rightarrow$.

Extensions: Truth, Falsity, Disjunction and Equivalence

- TRUTH: $\top$

- FALSITY: $\bot$

- DISJUNCTION: $\boldsymbol{P} \vee \boldsymbol{Q}$

- EQUIVALENCE: $\boldsymbol{P} \Leftrightarrow \boldsymbol{Q}$

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

- Pairs of matching parentheses can be added freely.

- Operators $\wedge$ and $\vee$ are left 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

$$\frac{}{\mathsf{H},\ \bot\ \vdash\ P}\ \textbf{FALSE\_L}$$

$$\frac{\mathsf{H}\ \vdash\ P \qquad \mathsf{H}\ \vdash\ \neg P}{\mathsf{H}\ \vdash\ \bot}\ \textbf{FALSE\_R}$$

$$\frac{\mathsf{H},\ \neg Q\ \vdash\ P}{\mathsf{H},\ \neg P\ \vdash\ Q}\ \textbf{NOT\_L}$$

$$\frac{\mathsf{H},\ P\ \vdash\ \bot}{\mathsf{H}\ \vdash\ \neg P}\ \textbf{NOT\_R}$$

$$\frac{\mathsf{H},\ P,\ Q\ \vdash\ R}{\mathsf{H},\ P \wedge Q\ \vdash\ R}\ \textbf{AND\_L}$$

$$\frac{\mathsf{H}\ \vdash\ P \qquad \mathsf{H}\ \vdash\ Q}{\mathsf{H}\ \vdash\ P \wedge Q}\ \textbf{AND\_R}$$

$$\frac{\mathsf{H},\ P\ \vdash\ R \qquad \mathsf{H},\ Q\ \vdash\ R}{\mathsf{H},\ P \vee Q\ \vdash\ R}\ \textbf{OR\_L}$$

$$\frac{\mathsf{H},\ \neg P\ \vdash\ Q}{\mathsf{H}\ \vdash\ P \vee Q}\ \textbf{OR\_R}$$

$$\frac{\mathsf{H},\ P,\ Q\ \vdash\ R}{\mathsf{H},\ P,\ P \Rightarrow Q\ \vdash\ R}\ \textbf{IMP\_L}$$

$$\frac{\mathsf{H},\ P\ \vdash\ Q}{\mathsf{H}\ \vdash\ P \Rightarrow Q}\ \textbf{IMP\_R}$$

Derived Rule: Proof by Cases

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

We assume the antecedents (if any) and prove the consequent.

- $\mathsf{H} \ \vdash\ P$ **CUT**
  - $\mathsf{H} \ \vdash\ Q \lor \neg Q$ **OR_R**
    - $\mathsf{H}, \neg Q \ \vdash\ \neg Q$ **HYP**
  - $\mathsf{H}, Q \lor \neg Q \ \vdash\ P$ **OR_L**
    - $\mathsf{H}, Q \ \vdash\ P$ **ant.**
    - $\mathsf{H}, \neg Q \ \vdash\ P$ **ant.**

Derived Rule: Proof by Contradiction (1)

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

Proof of rule **CT_L**:

$$\boxed{\mathsf{H},\ P \vdash Q}\ \mathbf{CASE}\ \begin{cases} \boxed{\mathsf{H},\ P,\ Q \ \vdash\ Q}\ \mathbf{HYP} \\[2ex] \boxed{\mathsf{H},\ P,\ \neg\, Q \ \vdash\ Q}\ \mathbf{CUT}\ \begin{cases} \boxed{\mathsf{H}, P, \neg\, Q \ \vdash\ \neg\, P}\ \mathbf{MON}\ \ \ldots \\[1ex] \boxed{\mathsf{H}, P, \neg\, Q, \neg\, P \ \vdash\ Q}\ \mathbf{NOT\_L}\ \ \ldots \end{cases} \end{cases}$$

$$\ldots\ \boxed{\mathsf{H}, \neg\, Q \ \vdash\ \neg\, P}\ \textbf{antecedent}$$

$$\ldots\ \boxed{\mathsf{H}, P, \neg\, Q, \neg\, Q \ \vdash\ P}\ \mathbf{HYP}$$

Derived Rule: Proof by Contradiction (2)

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

Proof of rule **CT_R**:

$$\boxed{\mathsf{H}\ \vdash\ P}\ \ \mathbf{CASE}\ \begin{cases} \boxed{\mathsf{H},\ P\ \vdash\ P}\ \ \mathbf{HYP} \\[2ex] \boxed{\mathsf{H},\ \neg P\ \vdash\ P}\ \ \mathbf{CUT}\ \begin{cases} \boxed{\mathsf{H}, \neg P\ \vdash\ \bot}\ \ \textbf{antecedent} \\[1ex] \boxed{\mathsf{H}, \neg P, \bot\ \vdash\ P}\ \ \mathbf{FALSE\_L} \end{cases} \end{cases}$$

Rewriting Rules

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

commutativity	$P \vee Q \Leftrightarrow Q \vee P$ $P \wedge Q \Leftrightarrow Q \wedge P$ $(P \Leftrightarrow Q) \Leftrightarrow (Q \Leftrightarrow P)$
associativity	$(P \vee Q) \vee R \Leftrightarrow P \vee (Q \vee R)$ $(P \wedge Q) \wedge R \Leftrightarrow P \wedge (Q \wedge R)$ $((P \Leftrightarrow Q) \Leftrightarrow R) \Leftrightarrow (P \Leftrightarrow (Q \Leftrightarrow R))$
distributivity	$R \wedge (P \vee Q) \Leftrightarrow (R \wedge P) \vee (R \wedge Q)$ $R \vee (P \wedge Q) \Leftrightarrow (R \vee P) \wedge (R \vee Q)$ $R \Rightarrow (P \wedge Q) \Leftrightarrow (R \Rightarrow P) \wedge (R \Rightarrow Q)$ $(P \vee Q) \Rightarrow R \Leftrightarrow (P \Rightarrow R) \wedge (Q \Rightarrow R)$

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

de Morgan	$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$ $\neg(P \wedge Q) \Leftrightarrow (P \Rightarrow \neg Q)$ $\neg(P \Rightarrow Q) \Leftrightarrow (P \wedge \neg Q)$
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	$(P \Leftrightarrow Q) \Rightarrow ((P \wedge R) \Leftrightarrow (Q \wedge R))$ $(P \Leftrightarrow Q) \Rightarrow ((P \vee R) \Leftrightarrow (Q \vee R))$ $(P \Leftrightarrow Q) \Rightarrow ((R \Rightarrow P) \Leftrightarrow (R \Rightarrow Q))$ $(P \Leftrightarrow Q) \Rightarrow ((P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R))$ $(P \Leftrightarrow Q) \Rightarrow (\neg P \Leftrightarrow \neg Q)$

Purpose of this Presentation

- Foundation for deductive and formal proofs

- A quick review of Propositional Calculus

- A quick review of First Order Predicate Calculus

- Refresher on Set Theory

- Formalising Data Structures (list, tree, graph)

Syntax of our Predicate Language so far

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

- The letter P, Q, etc. we have used are generic variables

- Each of them stands for a $\mathit{predicate}$

- All our proofs were thus also generic (able to be instantiated)

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

- 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.

$$\frac{\mathbf{H},\ \forall \mathbf{x} \cdot \mathbf{P(x)},\ \mathbf{P(E)} \quad \vdash \quad \mathbf{Q}}{\mathbf{H},\ \forall \mathbf{x} \cdot \mathbf{P(x)} \quad \vdash \quad \mathbf{Q}} \qquad \text{ALL\_L}$$

where **E** is an expression

$$\frac{\mathbf{H} \quad \vdash \quad \mathbf{P(x)}}{\mathbf{H} \quad \vdash \quad \forall \mathbf{x} \cdot \mathbf{P(x)}} \qquad \text{ALL\_R}$$

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

Extending the language: Existential Quantification

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

Rules of Inference for Existential Quantification

$$\frac{\mathbf{H},\ \mathbf{P(x)} \ \vdash \ \mathbf{Q}}{\mathbf{H},\ \exists \mathbf{x} \cdot \mathbf{P(x)} \ \vdash \ \mathbf{Q}} \quad \text{XST\_L}$$

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

$$\frac{\mathbf{H} \ \vdash \ \mathbf{P(E)}}{\mathbf{H} \ \vdash \ \exists \mathbf{x} \cdot \mathbf{P(x)}} \quad \text{XST\_R}$$

where **E** is an expression

Comparing the Quantification Rules

$$\frac{\mathbf{H},\ \forall \mathbf{x} \cdot \mathbf{P(x)},\ \mathbf{P(E)} \ \vdash \ \mathbf{Q}}{\mathbf{H},\ \forall \mathbf{x} \cdot \mathbf{P(x)} \ \vdash \ \mathbf{Q}} \quad \text{ALL\_L}$$

$$\frac{\mathbf{H} \ \vdash \ \mathbf{P(E)}}{\mathbf{H} \ \vdash \ \exists \mathbf{x} \cdot \mathbf{P(x)}} \quad \text{XST\_R}$$

$$\frac{\mathbf{H} \ \vdash \ \mathbf{P(x)}}{\mathbf{H} \ \vdash \ \forall \mathbf{x} \cdot \mathbf{P(x)}} \quad \text{ALL\_R}$$

$$\frac{\mathbf{H},\ \mathbf{P(x)} \ \vdash \ \mathbf{Q}}{\mathbf{H},\ \exists \mathbf{x} \cdot \mathbf{P(x)} \ \vdash \ \mathbf{Q}} \quad \text{XST\_L}$$

$$\forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \quad \vdash \quad \forall x \cdot (\forall y \cdot P_{x,y} \;\Rightarrow\; Q_x)$$

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \vdash \\ \quad \forall x \cdot (\forall y \cdot P_{x,y} \;\Rightarrow\; Q_x) \end{array}$$

ALL_R
ALL_R
IMP_R

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \quad P_{x,y} \\ \vdash \\ \quad Q_x \end{array}$$

CUT . . .

. . .

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \quad P_{x,y} \\ \vdash \\ \quad \exists y \cdot P_{x,y} \end{array}$$

XST_R

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \quad P_{x,y} \\ \vdash \\ \quad P_{x,y} \end{array}$$

HYP

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \quad P_{x,y} \\ \quad \exists y \cdot P_{x,y} \\ \vdash \\ \quad Q_x \end{array}$$

ALL_L
IMP_L

$$\begin{array}{l} \quad \forall x \cdot (\exists y \cdot P_{x,y}) \;\Rightarrow\; Q_x \\ \quad Q_x \\ \quad P_{x,y} \\ \quad \exists y \cdot P_{x,y} \\ \vdash \\ \quad Q_x \end{array}$$

HYP

An Interesting Derived Rule

- Replacing an existential goal by a simpler one

$$\frac{\mathsf{H} \;\vdash\; \exists x \cdot Q \qquad \mathsf{H},\; Q \;\vdash\; P}{\mathsf{H} \;\vdash\; \exists x \cdot P} \quad \textbf{CUT\_XST} \;(\mathsf{x}\ \underline{\mathsf{nfin}}\ \mathsf{H})$$

Proof of **CUT_XST**

$$\boxed{\mathsf{H} \vdash \exists x \cdot P} \quad \textbf{CUT} \begin{cases} \boxed{\mathsf{H} \vdash \exists x \cdot Q} \quad \textbf{antecedent} \\[2ex] \boxed{\mathsf{H},\ \exists x \cdot Q \vdash \exists x \cdot P} \quad \begin{matrix}\textbf{XST\_L} \\ \textbf{XST\_R}\end{matrix} \quad \boxed{\mathsf{H},\ Q \vdash P} \end{cases}$$

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 $P \;\vee\; \forall x \cdot Q \quad \Leftrightarrow \quad \forall x \cdot (P \vee Q)$ $P \;\wedge\; \exists x \cdot Q \quad \Leftrightarrow \quad \exists x \cdot (P \wedge Q)$ $P \;\Rightarrow\; \forall x \cdot Q \quad \Leftrightarrow \quad \forall x \cdot (P \Rightarrow Q)$

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

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

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

Equality Rules of Inference

$$\frac{\mathbf{H(F)},\ \mathbf{E} = \mathbf{F} \ \vdash\ \mathbf{P(F)}}{\mathbf{H(E)},\ \mathbf{E} = \mathbf{F} \ \vdash\ \mathbf{P(E)}} \quad \text{EQ\_LR}$$

$$\frac{\mathbf{H(E)},\ \mathbf{E} = \mathbf{F} \ \vdash\ \mathbf{P(E)}}{\mathbf{H(F)},\ \mathbf{E} = \mathbf{F} \ \vdash\ \mathbf{P(F)}} \quad \text{EQ\_RL}$$

$$\frac{}{\vdash\ \mathbf{E} = \mathbf{E}} \quad \text{EQL}$$

$$\frac{\mathbf{H} \ \vdash\ \mathbf{E} = \mathbf{G} \ \wedge\ \mathbf{F} = \mathbf{I}}{\mathbf{H} \ \vdash\ \mathbf{E} \mapsto \mathbf{F} = \mathbf{G} \mapsto \mathbf{I}} \quad \text{PAIR}$$

Classical Results for Equality

symmetry	$E = F \quad \Leftrightarrow \quad F = E$
transitivity	$E = F \wedge F = G \quad \Rightarrow \quad E = G$
pair	$E \mapsto F = G \mapsto H \quad \Rightarrow \quad E = G \wedge F = H$
One-point rules	if x not free in E $(\forall x \cdot x = E \Rightarrow P(x)) \quad \Leftrightarrow \quad P(E)$ $(\exists x \cdot x = E \wedge P(x)) \quad \Leftrightarrow \quad P(E)$

Purpose of this Presentation

- Foundation for deductive and formal proofs

- A quick review of Propositional Calculus

- A quick review of First Order Predicate Calculus

- A refresher on Set Theory

- Formalising Data Structures (list, tree, graph)

$$
\begin{array}{lll}
predicate & ::= & \bot \\
& & \top \\
& & \neg\, predicate \\
& & predicate \;\land\; predicate \\
& & predicate \;\lor\; predicate \\
& & predicate \;\Rightarrow\; predicate \\
& & predicate \;\Leftrightarrow\; predicate \\
& & \forall\, var\_list \cdot predicate \\
& & \exists\, var\_list \cdot predicate \\
& & expression \;=\; expression \\
& & expression \;\in\; expression
\end{array}
$$

$$
\begin{array}{lll}
expression & ::= & variable \\
 & & expression \mapsto expression \\
 & & \\
variable & ::= & identifier \\
 & & \\
var\_list & ::= & variable \\
 & & variable, var\_list \\
 & & \\
set & ::= & set \times set \\
 & & \mathbb{P}(set) \\
 & & \{\, var\_list \cdot predicate \mid expression \,\}
\end{array}
$$

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

- Basis
  - Basic operators

- 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

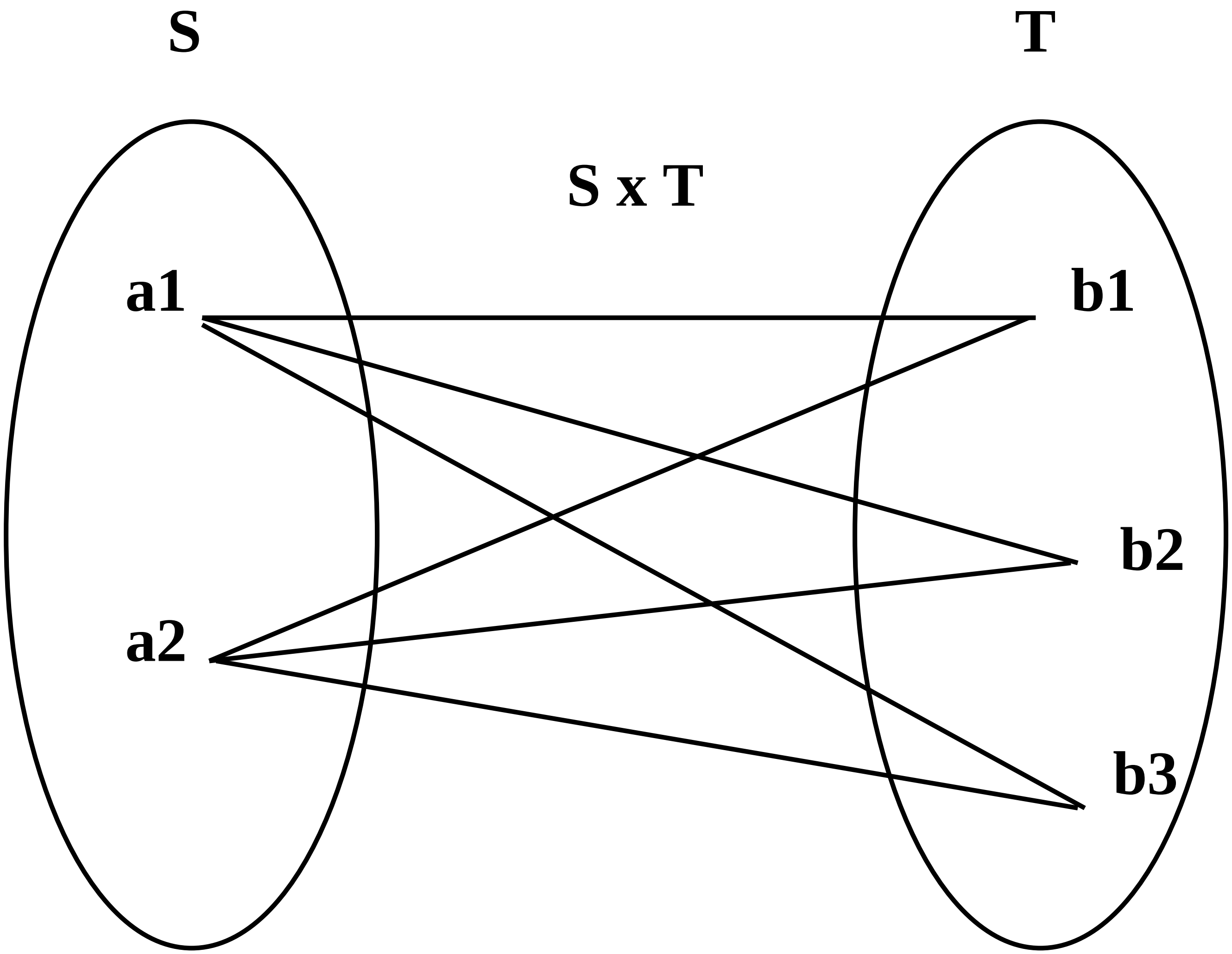
$$\boldsymbol{E} \in \boldsymbol{S}$$

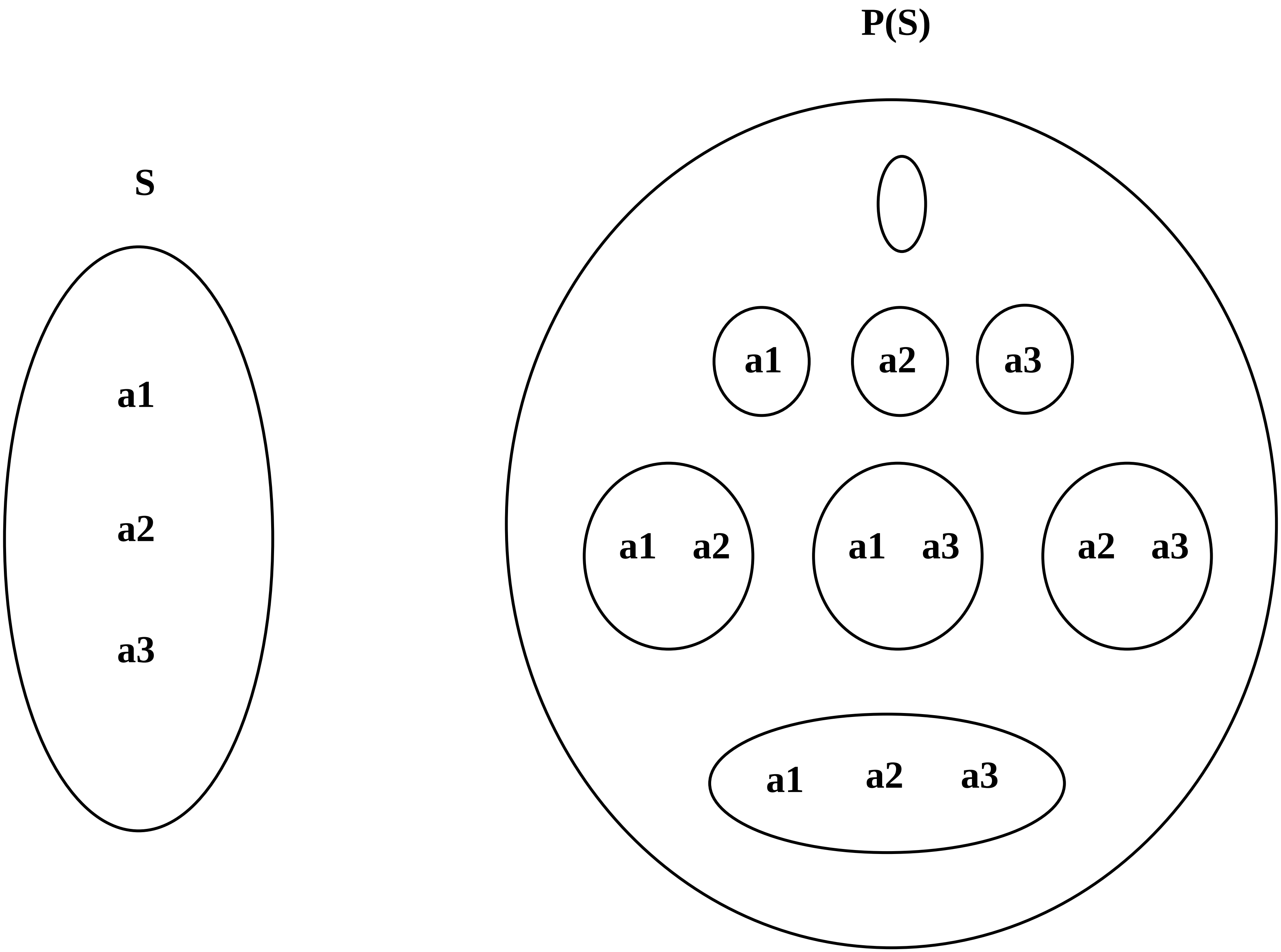
- where $\boldsymbol{E}$ is an expression and $\boldsymbol{S}$ is a set

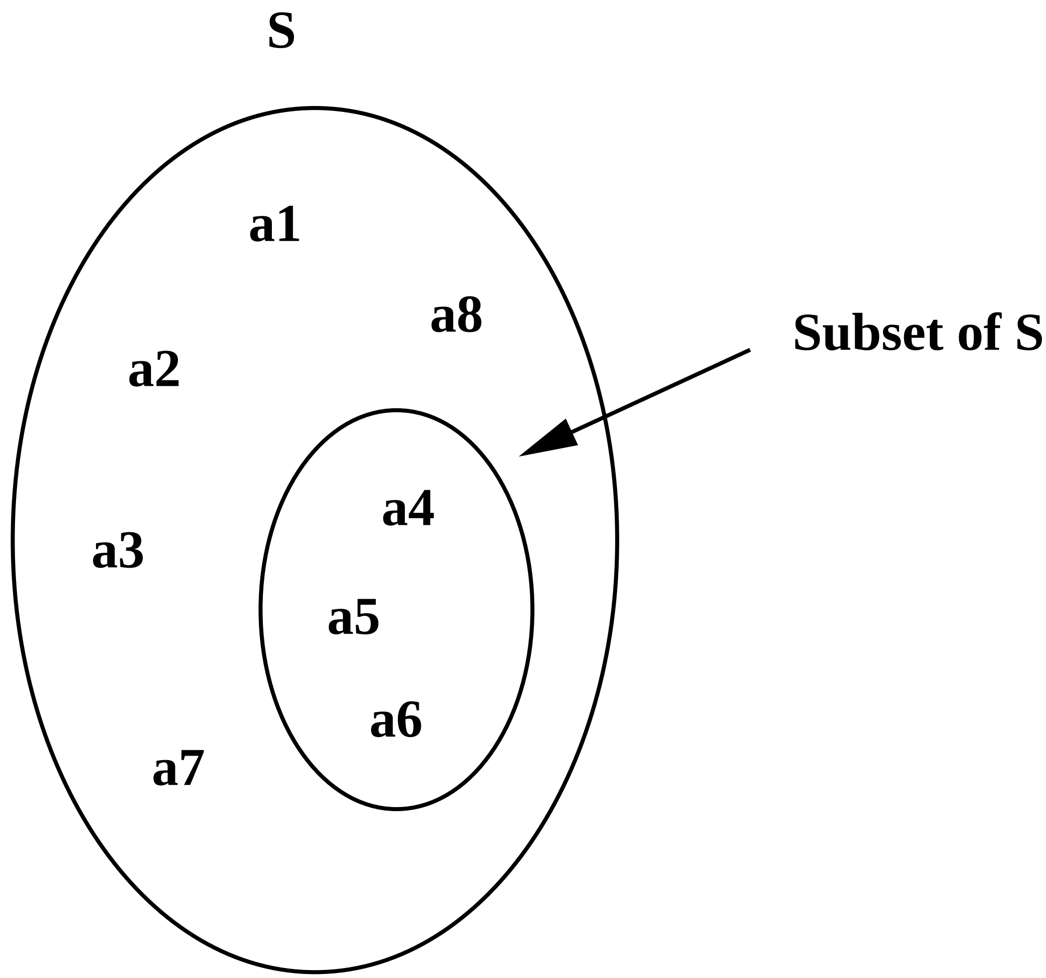
There are three basic constructs in set theory:

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

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


S
T
S x T
a1
a2
b1
b2
b3


S
a1
a2
a3
P(S)
a1
a2
a3
a1 a2
a1 a3
a2 a3
a1 a2 a3


S
a1
a8
Subset of S
a2
a4
a3
a5
a6
a7

Basic Set Operator Memberships (Axioms)

These axioms are defined by equivalences.

Left Part	Right Part
$\boldsymbol{E} \mapsto \boldsymbol{F} \in \boldsymbol{S} \times \boldsymbol{T}$	$\boldsymbol{E} \in \boldsymbol{S} \;\; \wedge \;\; \boldsymbol{F} \in \boldsymbol{T}$
$\boldsymbol{S} \in \mathbb{P}(\boldsymbol{T})$	$\forall \boldsymbol{x} \cdot (\, \boldsymbol{x} \in \boldsymbol{S} \Rightarrow \boldsymbol{x} \in \boldsymbol{T} \,)$
$\boldsymbol{E} \in \{\boldsymbol{x} \cdot \boldsymbol{x} \in \boldsymbol{S} \;\; \wedge \;\; \boldsymbol{P} \mid \boldsymbol{F}\}$	$\exists \boldsymbol{x} \cdot \boldsymbol{x} \in \boldsymbol{S} \;\; \wedge \;\; \boldsymbol{P} \;\; \wedge \;\; \boldsymbol{E} = \boldsymbol{F}$
$\boldsymbol{E} \in \{\boldsymbol{x} \mid \boldsymbol{x} \in \boldsymbol{S} \;\; \wedge \;\; \boldsymbol{P}(\boldsymbol{x})\}$	$\boldsymbol{E} \in \boldsymbol{S} \;\; \wedge \;\; \boldsymbol{P}(\boldsymbol{E})$

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

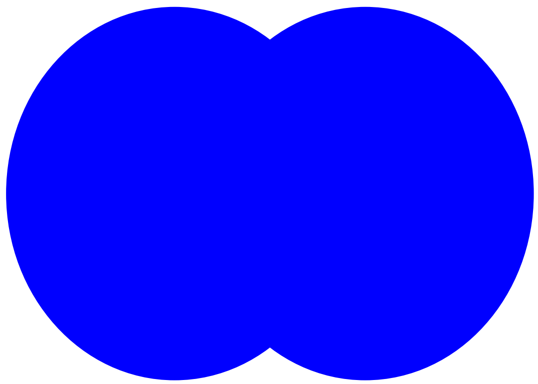
The first rule is just a syntactic extension

The second rule is the Extensionality Axiom

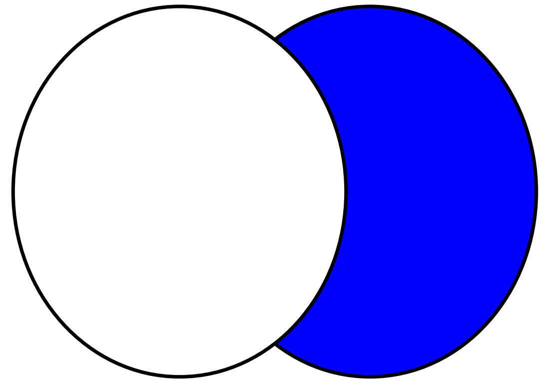
Union	$\boldsymbol{S} \cup \boldsymbol{T}$
Intersection	$\boldsymbol{S} \cap \boldsymbol{T}$
Difference	$\boldsymbol{S} \setminus \boldsymbol{T}$
Extension	$\{\boldsymbol{a}, \ldots, \boldsymbol{b}\}$
Empty set	$\varnothing$

Union, Difference, Intersection

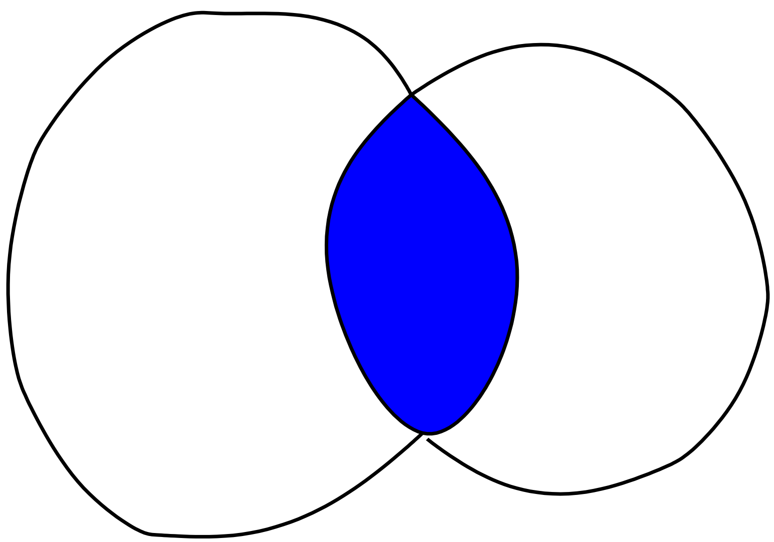
Union



Difference



Intersection



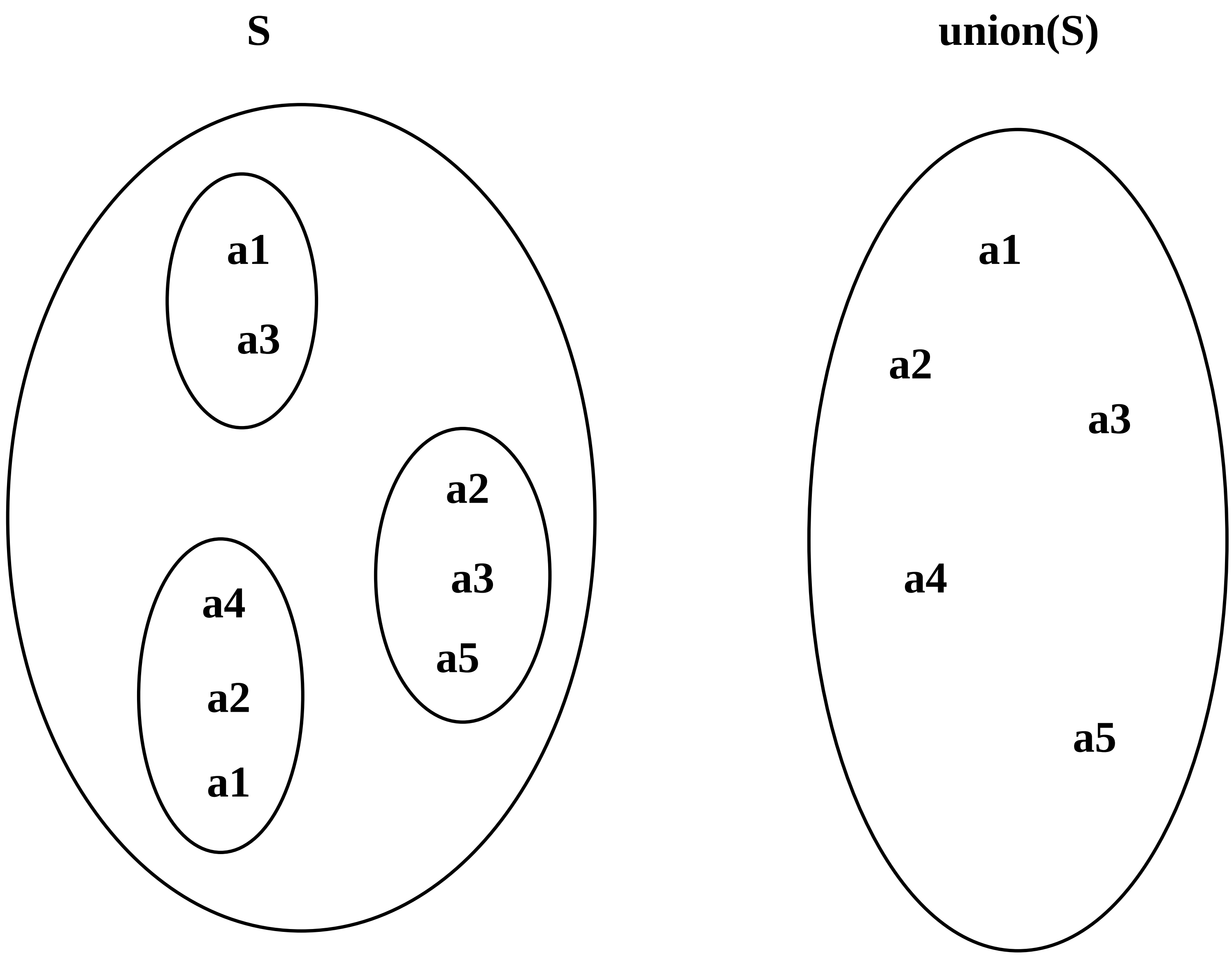
$\boldsymbol{E} \in \boldsymbol{S} \cup \boldsymbol{T}$	$\boldsymbol{E} \in \boldsymbol{S} \quad \vee \quad \boldsymbol{E} \in \boldsymbol{T}$
$\boldsymbol{E} \in \boldsymbol{S} \cap \boldsymbol{T}$	$\boldsymbol{E} \in \boldsymbol{S} \quad \wedge \quad \boldsymbol{E} \in \boldsymbol{T}$
$\boldsymbol{E}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

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

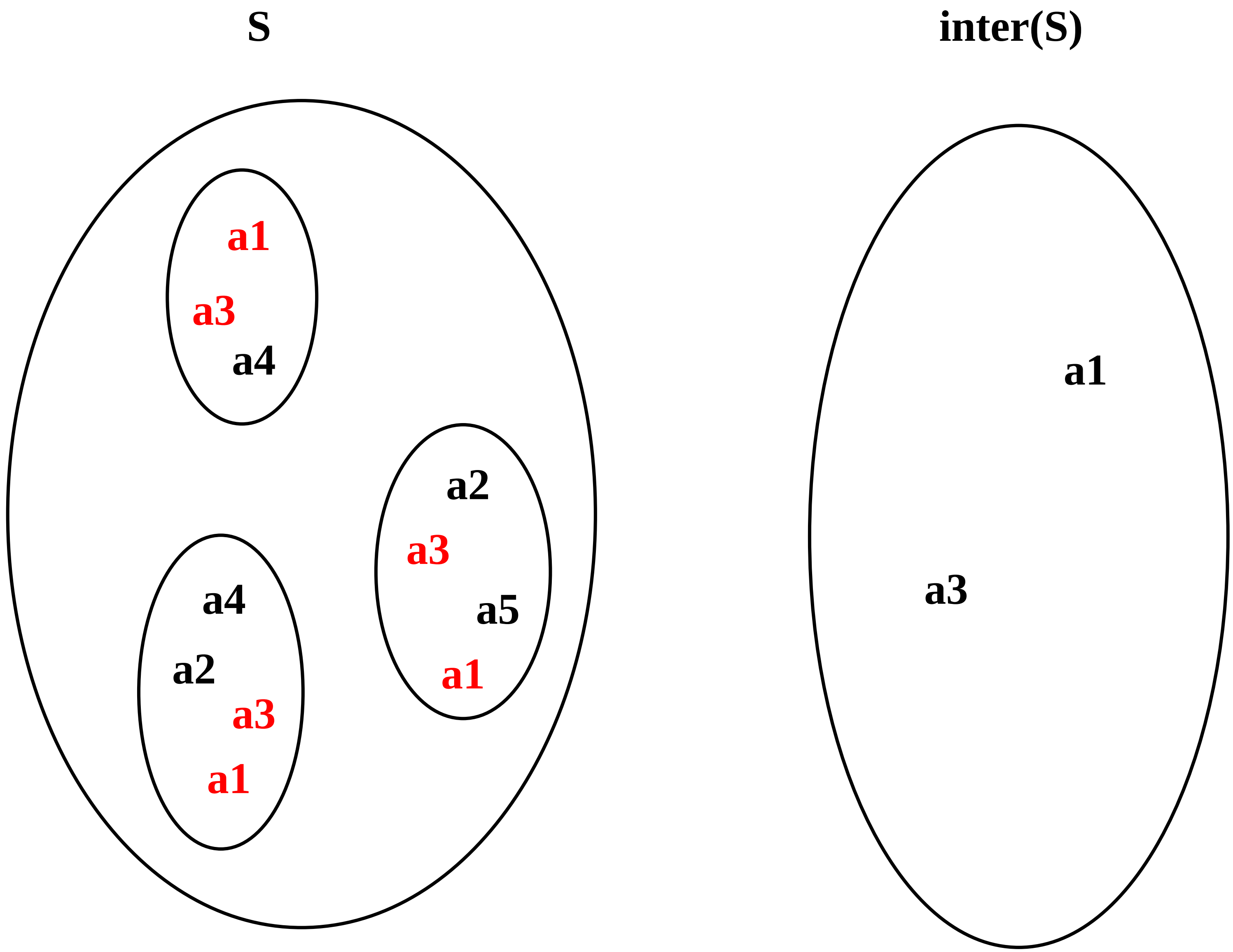
Generalizations of Elementary Operators

Generalized Union	union (S)
Union Quantifier	$\bigcup\, x \cdot (x \in S \ \wedge\ P \mid T)$
Generalized Intersection	inter (S)
Intersection Quantifier	$\bigcap\, x \cdot (x \in S \ \wedge\ P \mid T)$

Generalized Union



Generalized Intersection



$E \in \text{union}(S)$	$\exists s \cdot (s \in S \land E \in s)$
$E \in \bigcup x \cdot (x \in S \land P \mid T)$	$\exists x \cdot (x \in S \land P \land E \in T)$
$E \in \text{inter}(S)$	$\forall s \cdot (s \in S \Rightarrow E \in s)$
$E \in \bigcap x \cdot (x \in S \land P \mid T)$	$\forall x \cdot (x \in S \land P \Rightarrow E \in T)$

Well-definedness condition for case 3: $S \neq \varnothing$

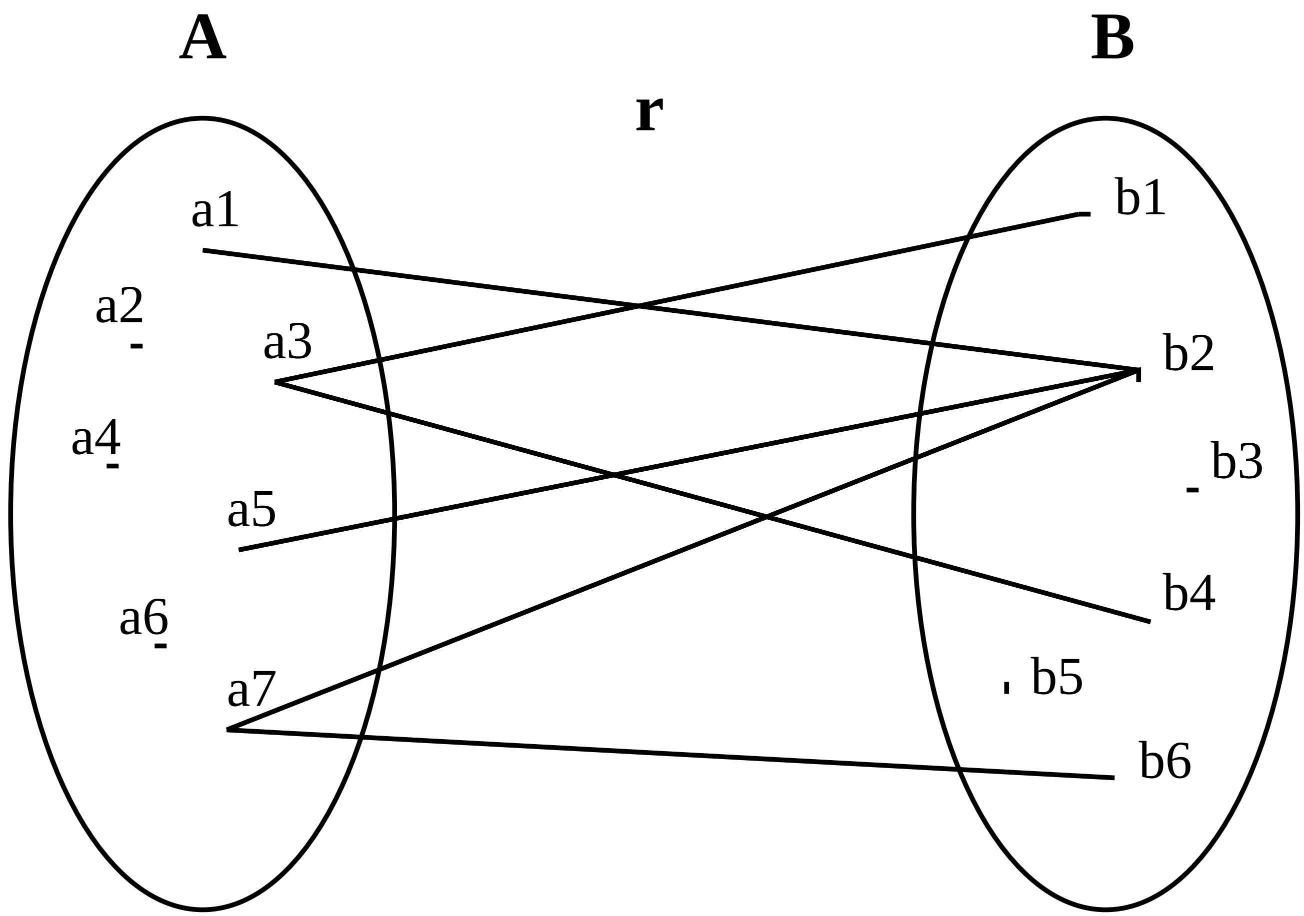
Well-definedness condition for case 4: $\exists x \cdot (x \in S \land P)$

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

Binary Relation Operators (1)

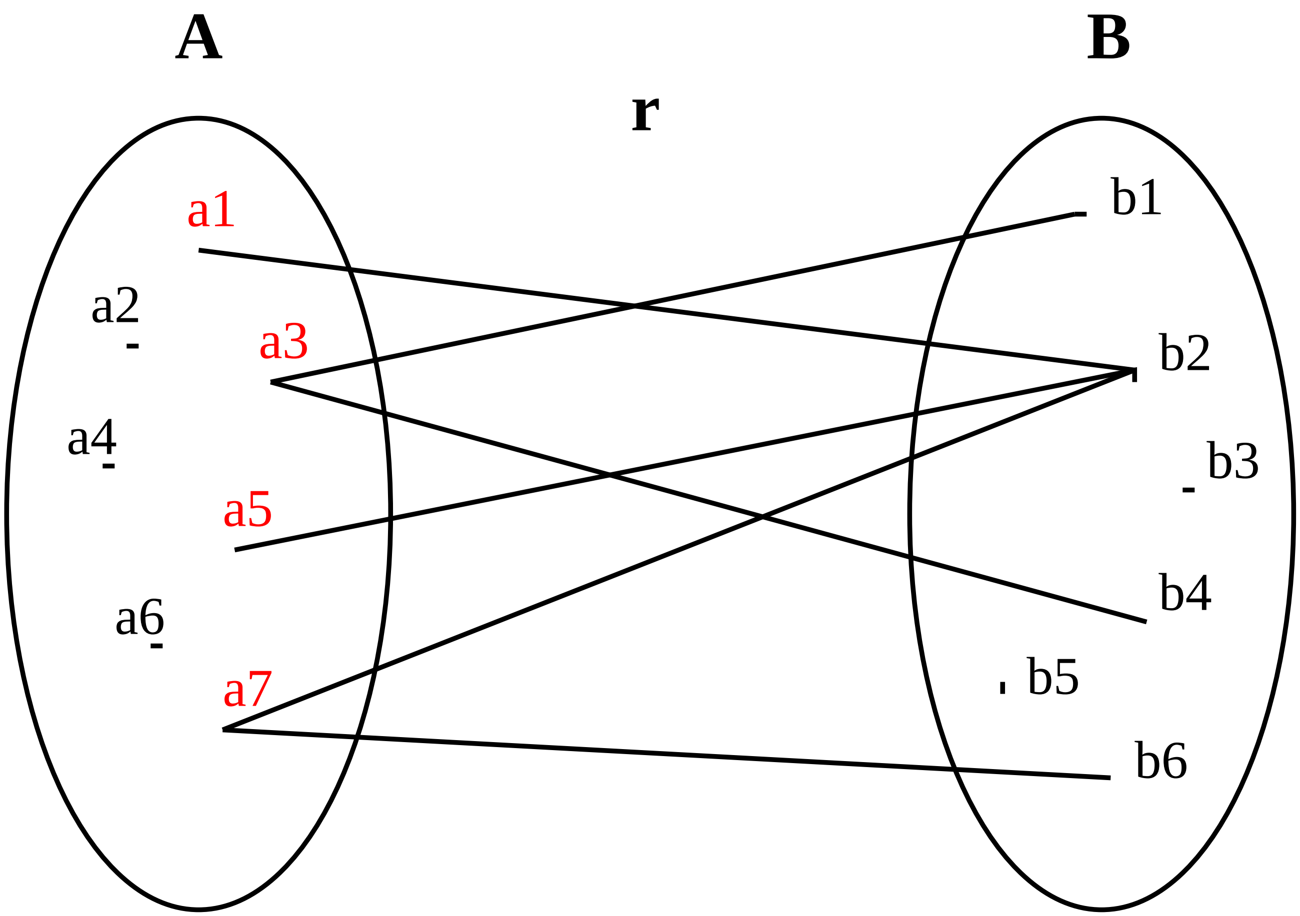
Binary relations	$S \leftrightarrow T$
Domain	$\mathsf{dom}\,(r)$
Range	$\mathsf{ran}\,(r)$
Converse	r^{-1}

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



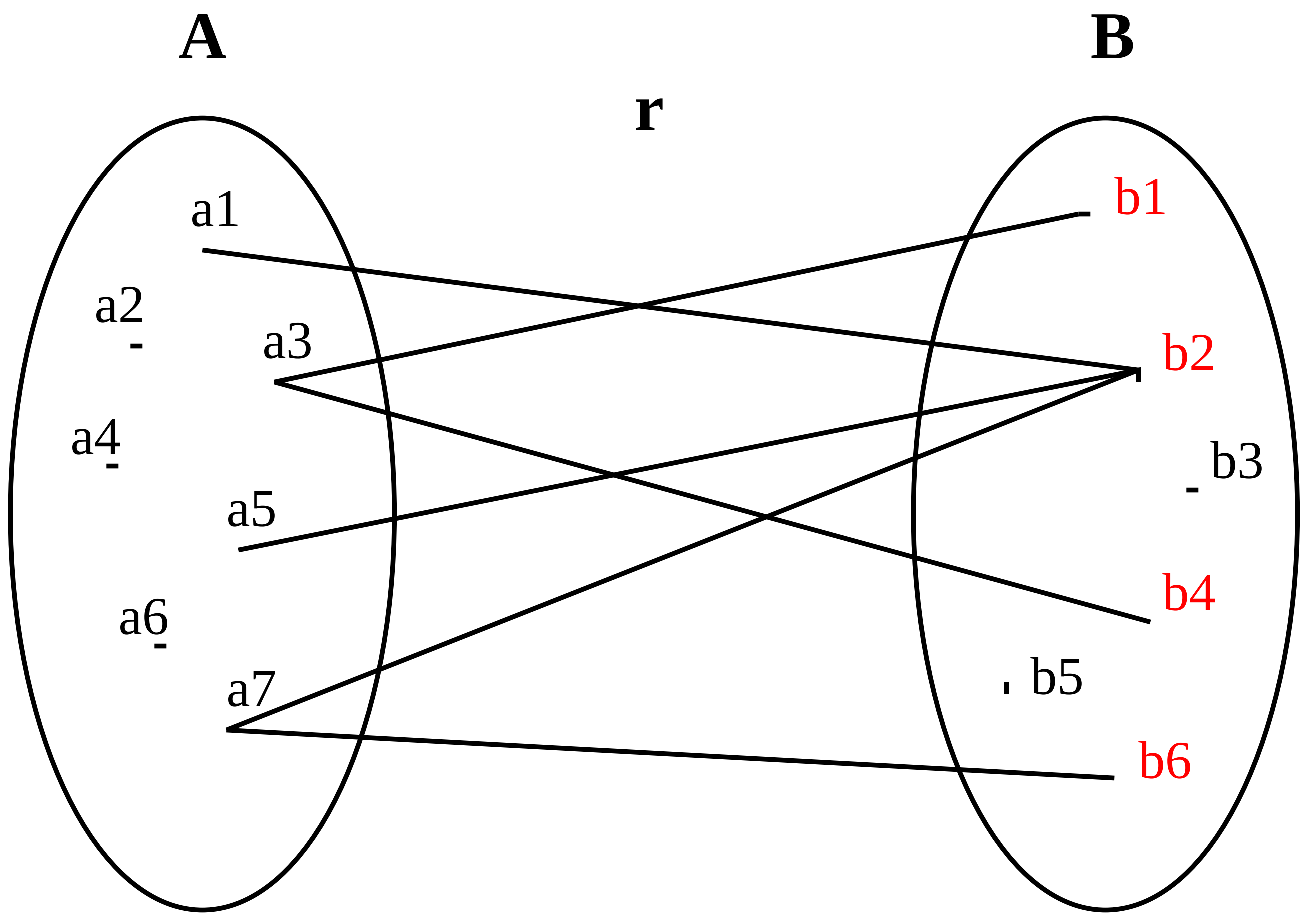
$$r \in A \leftrightarrow B$$

Domain of Binary Relation r

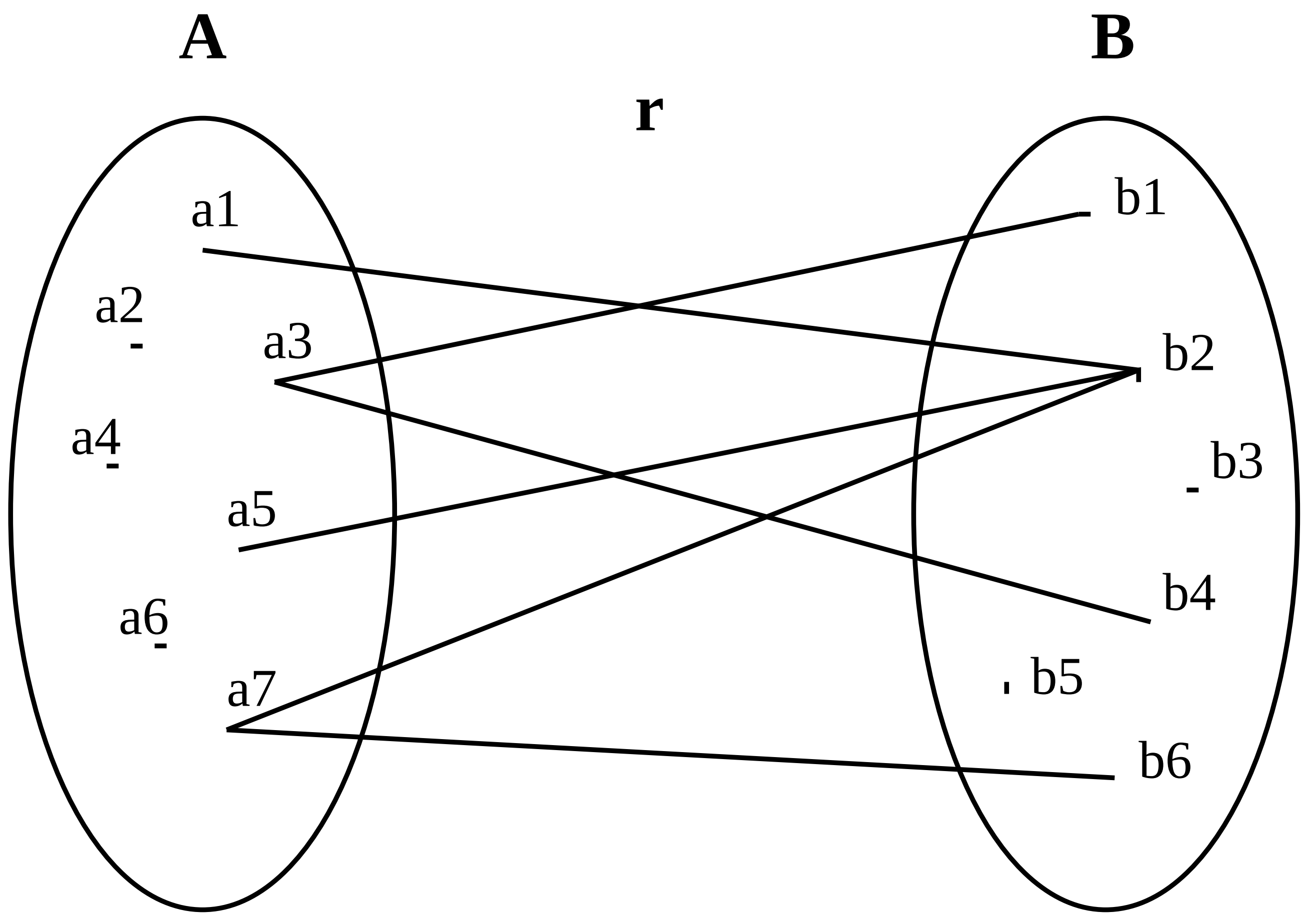


$$\text{dom}(r) = \{a1, a3, a5, a7\}$$

Range of Binary Relation r



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



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

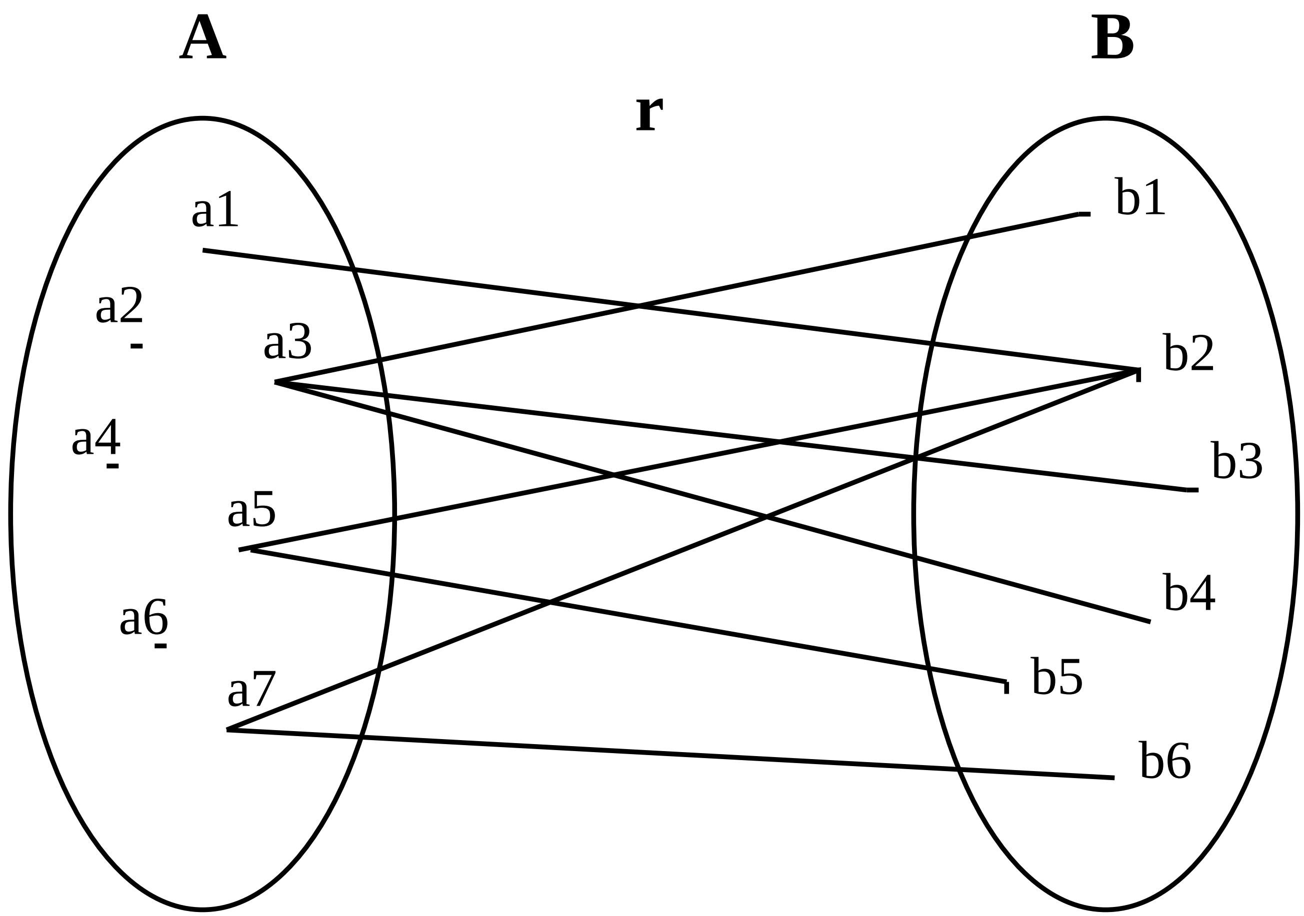
Binary Relation Operator Memberships (1)

Left Part	Right Part
$r \in S \leftrightarrow T$	$r \subseteq S \times T$
$E \in \text{dom}\,(r)$	$\exists y \cdot (E \mapsto y \;\in\; r)$
$F \in \text{ran}\,(r)$	$\exists x \cdot (x \mapsto F \;\in\; r)$
$E \mapsto F \in r^{-1}$	$F \mapsto E \in r$

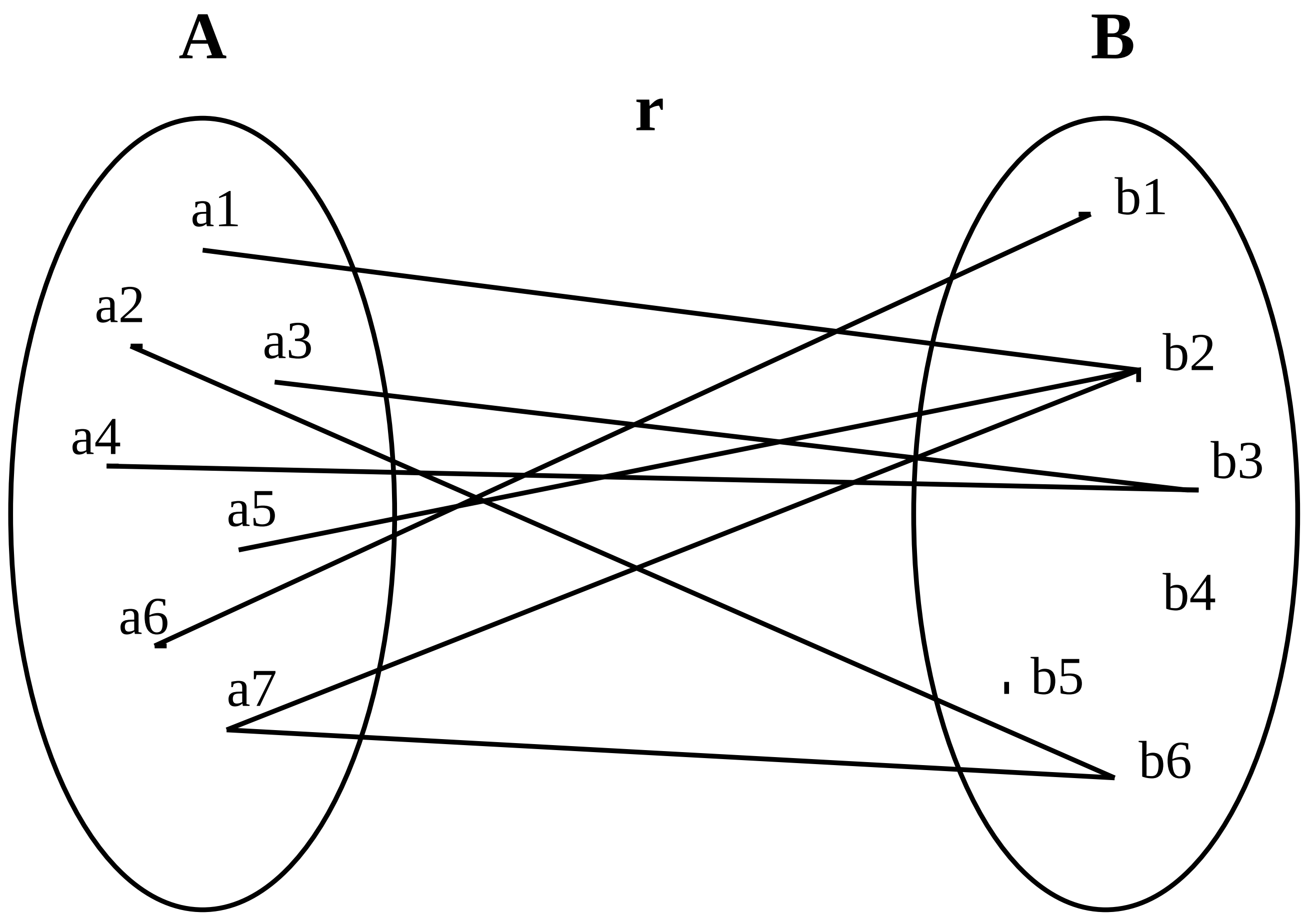
Binary Relation Operators (2)

Partial surjective binary relations	$S \srel T$
Total binary relations	$S \trel T$
Total surjective binary relations	$S \strel T$

A Partial Surjective Relation

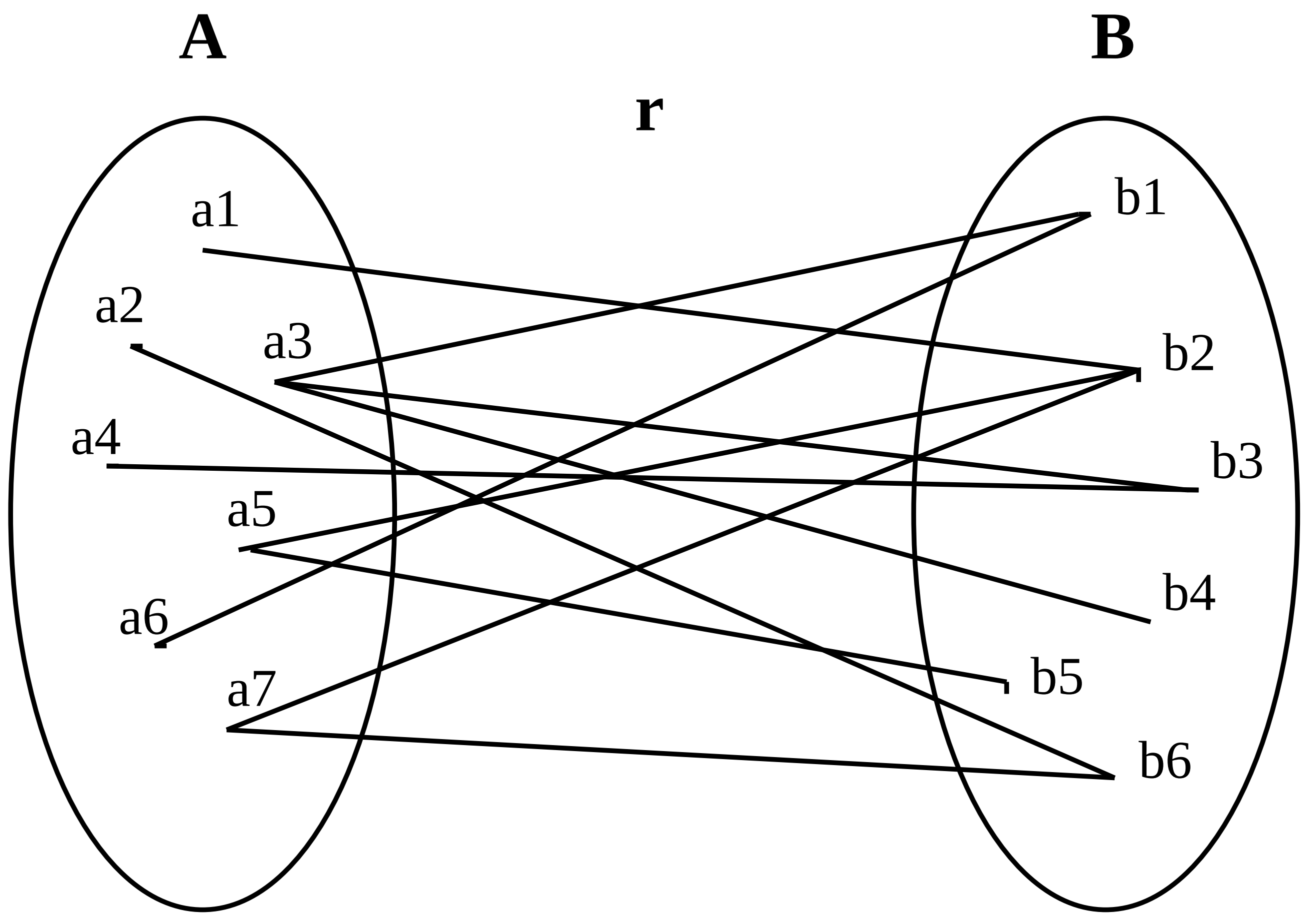


$$r \in A \leftrightarrow\!\!\!\!\twoheadrightarrow B$$



$$r \in A \twoheadleftrightarrow B$$

A Total Surjective Relation



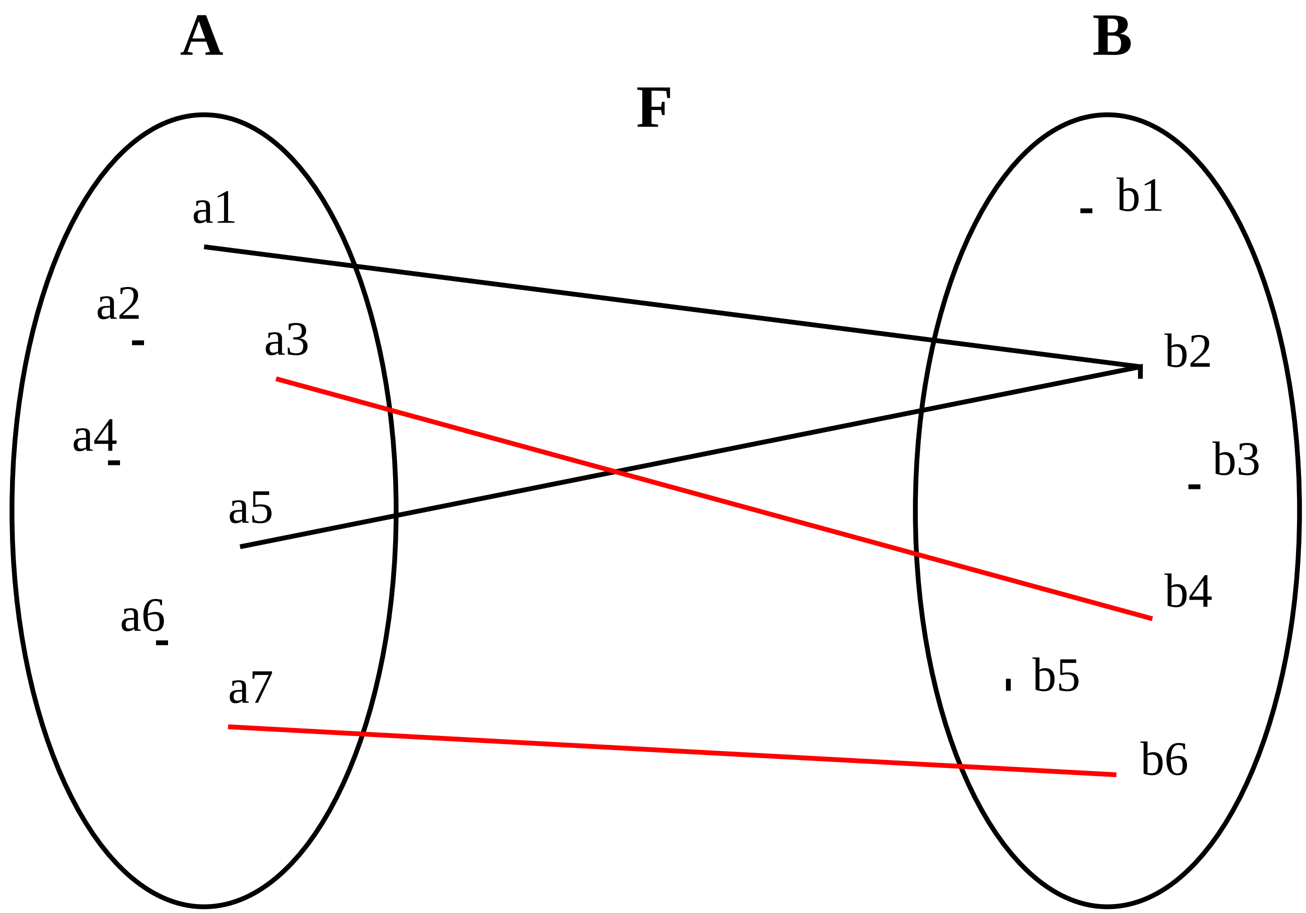
$$r \in A \twoheadleftrightarrow B$$

Binary Relation Operator Memberships (2)

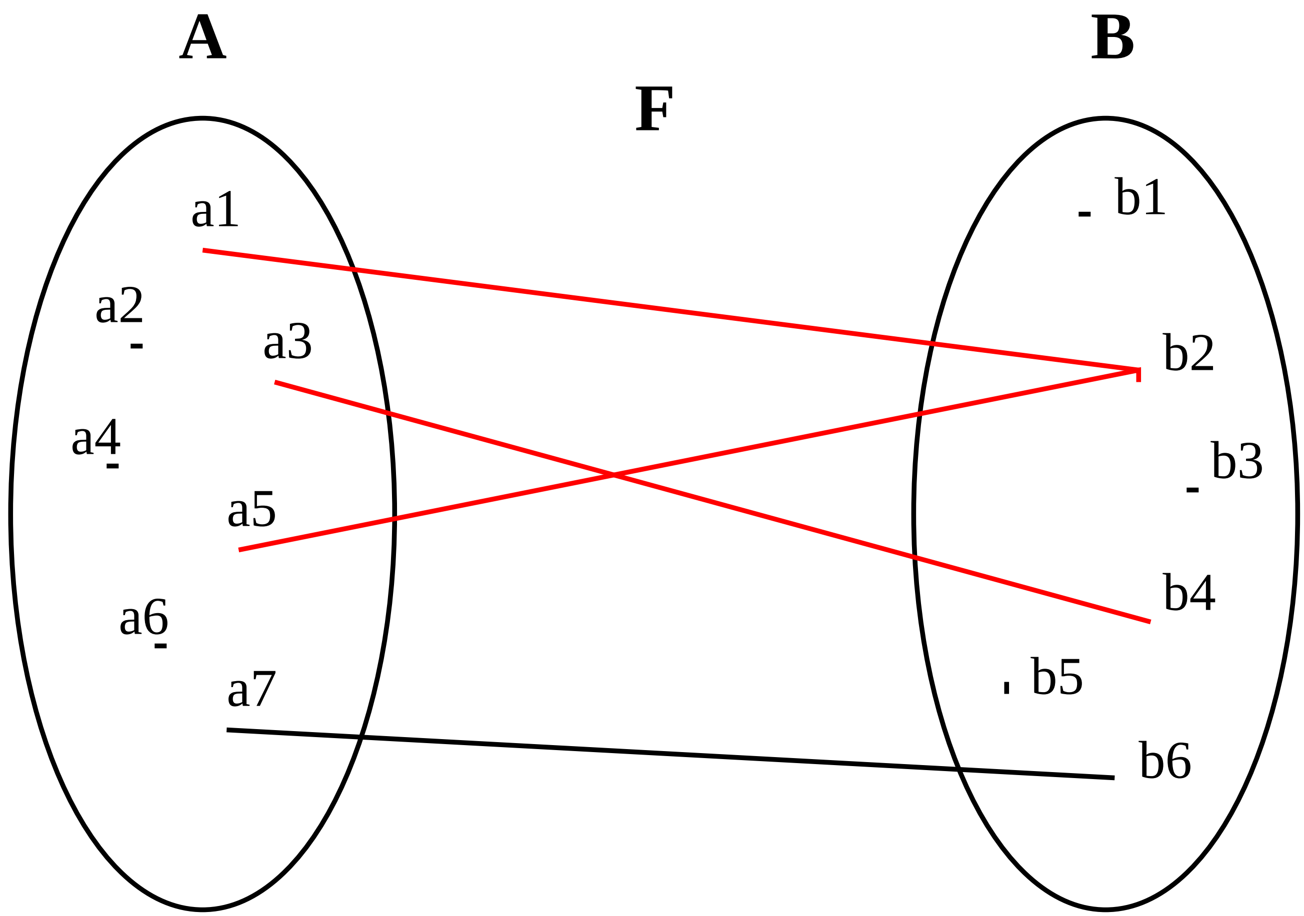
Left Part	Right Part
$r \in S \leftarrow\mkern-14mu\twoheadrightarrow T$	$r \in S \leftrightarrow T \ \land\ \mathsf{ran}(r) = T$
$r \in S \twoheadleftarrow\mkern-14mu\rightarrow T$	$r \in S \leftrightarrow T \ \land\ \mathsf{dom}(r) = T$
$r \in S \twoheadleftarrow\mkern-14mu\twoheadrightarrow T$	$r \in S \leftarrow\mkern-14mu\twoheadrightarrow T \ \land\ r \in S \twoheadleftarrow\mkern-14mu\rightarrow T$

Binary Relation Operators (3)

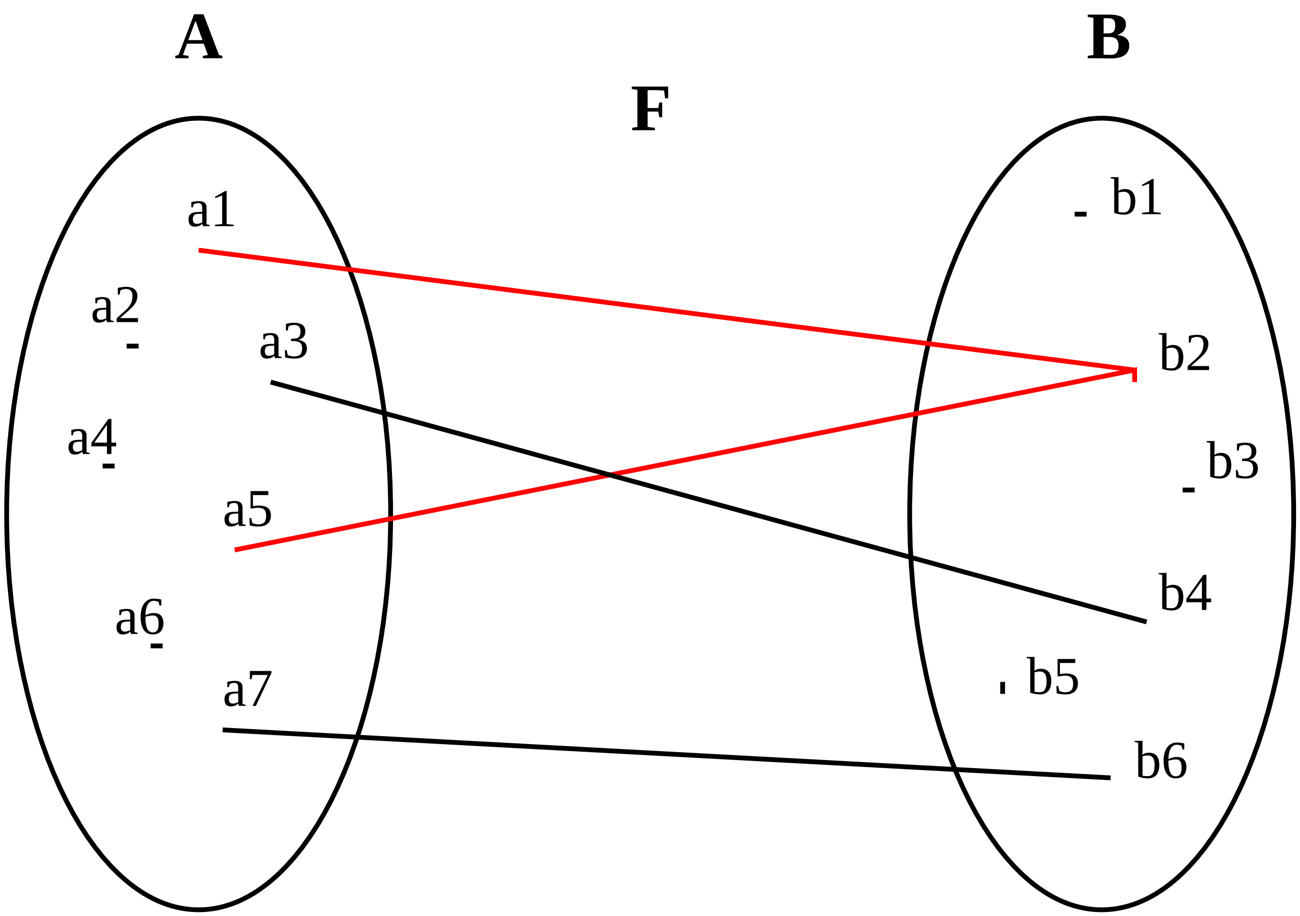
Domain restriction	$S \lhd r$
Range restriction	$r \rhd T$
Domain subtraction	$S \unlhd r$
Range subtraction	$r \unrhd T$



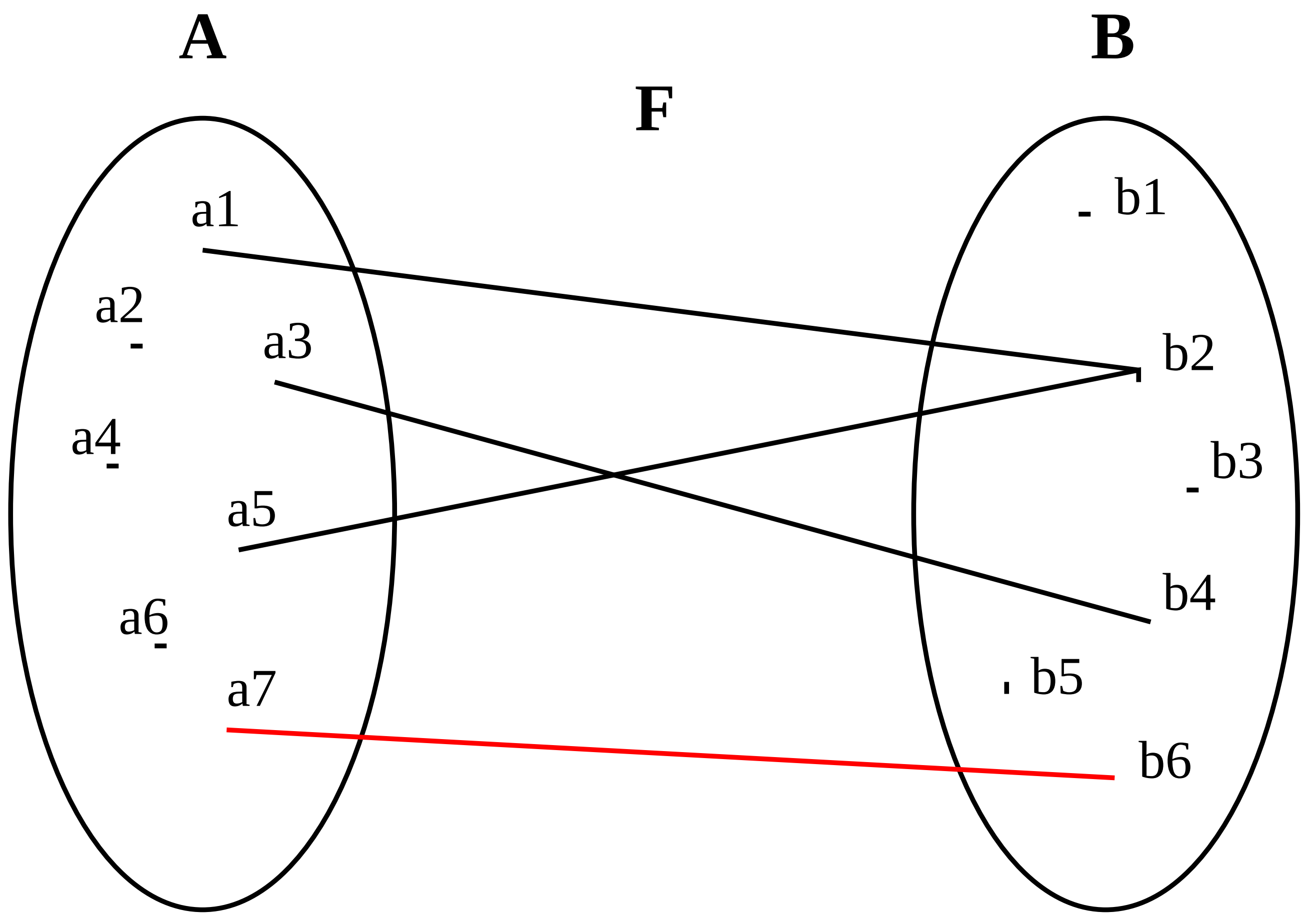
$$\{a3,\ a7\} \lhd F$$



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



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



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

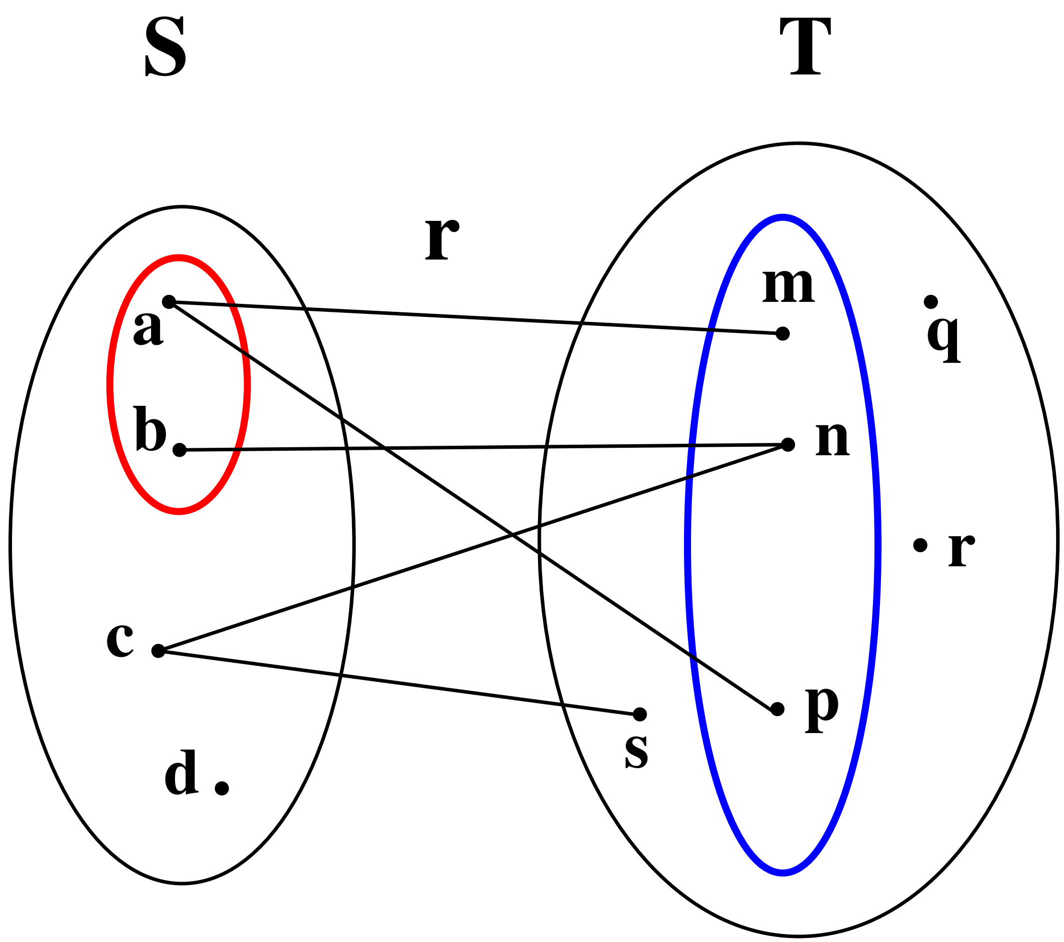
Binary Relation Operator Memberships (3)

Left Part	Right Part
$E \mapsto F \;\in\; S \lhd r$	$E \in S \;\;\wedge\;\; E \mapsto F \in r$
$E \mapsto F \;\in\; r \rhd T$	$E \mapsto F \in r \;\;\wedge\;\; F \in T$
$E \mapsto F \;\in\; S \mathbin{\lhd\!\!\!-} r$	$E \notin S \;\;\wedge\;\; E \mapsto F \in r$
$E \mapsto F \;\in\; r \mathbin{\rhd\!\!\!\!-} T$	$E \mapsto F \in r \;\;\wedge\;\; F \notin T$

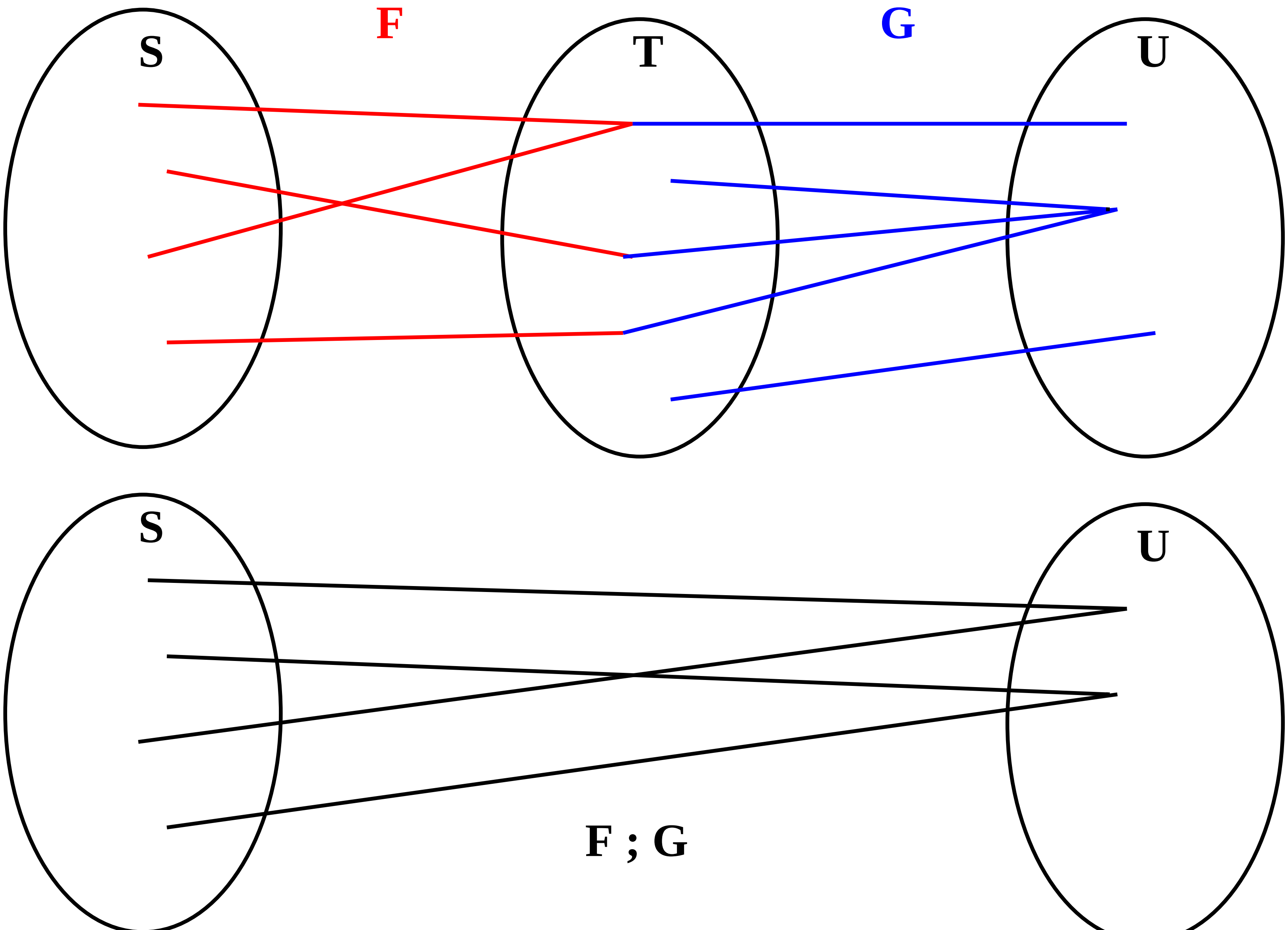
Binary Relation Operators (4)

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

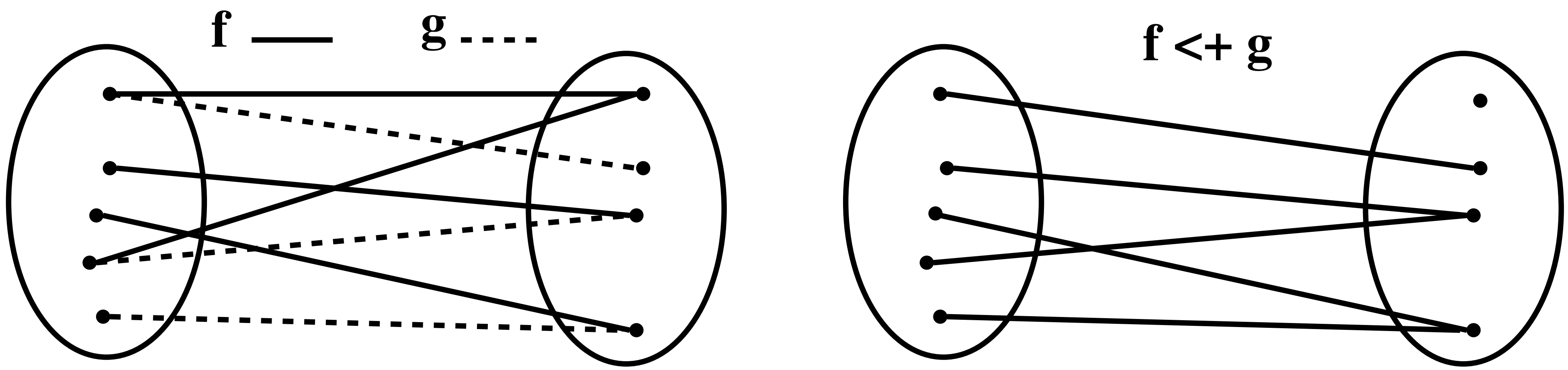
Image of $\{a, b\}$ under r



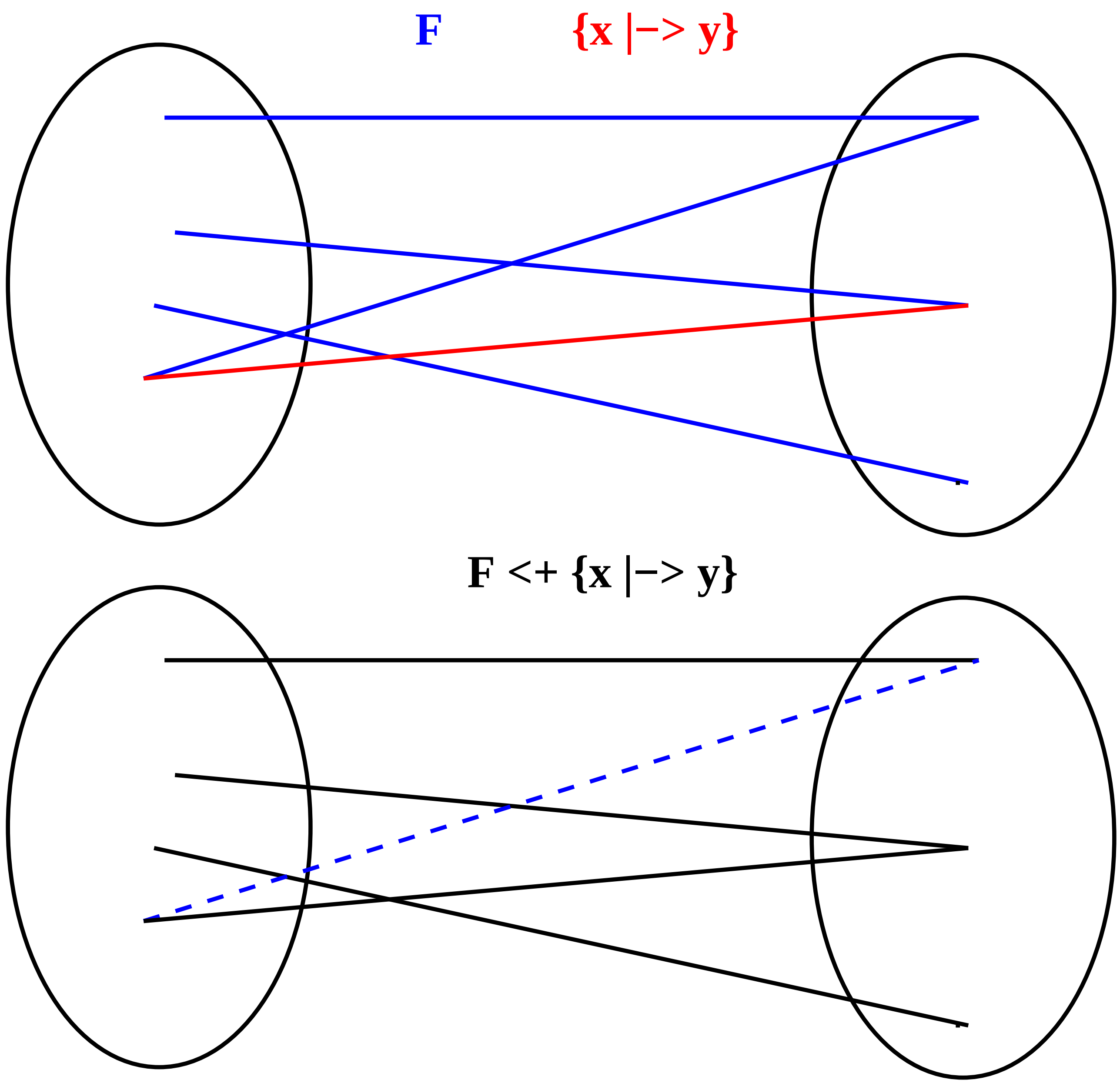
$$r[\{a, b\}] = \{m, n, p\}$$


F
G
S
T
U
S
U
F ; G

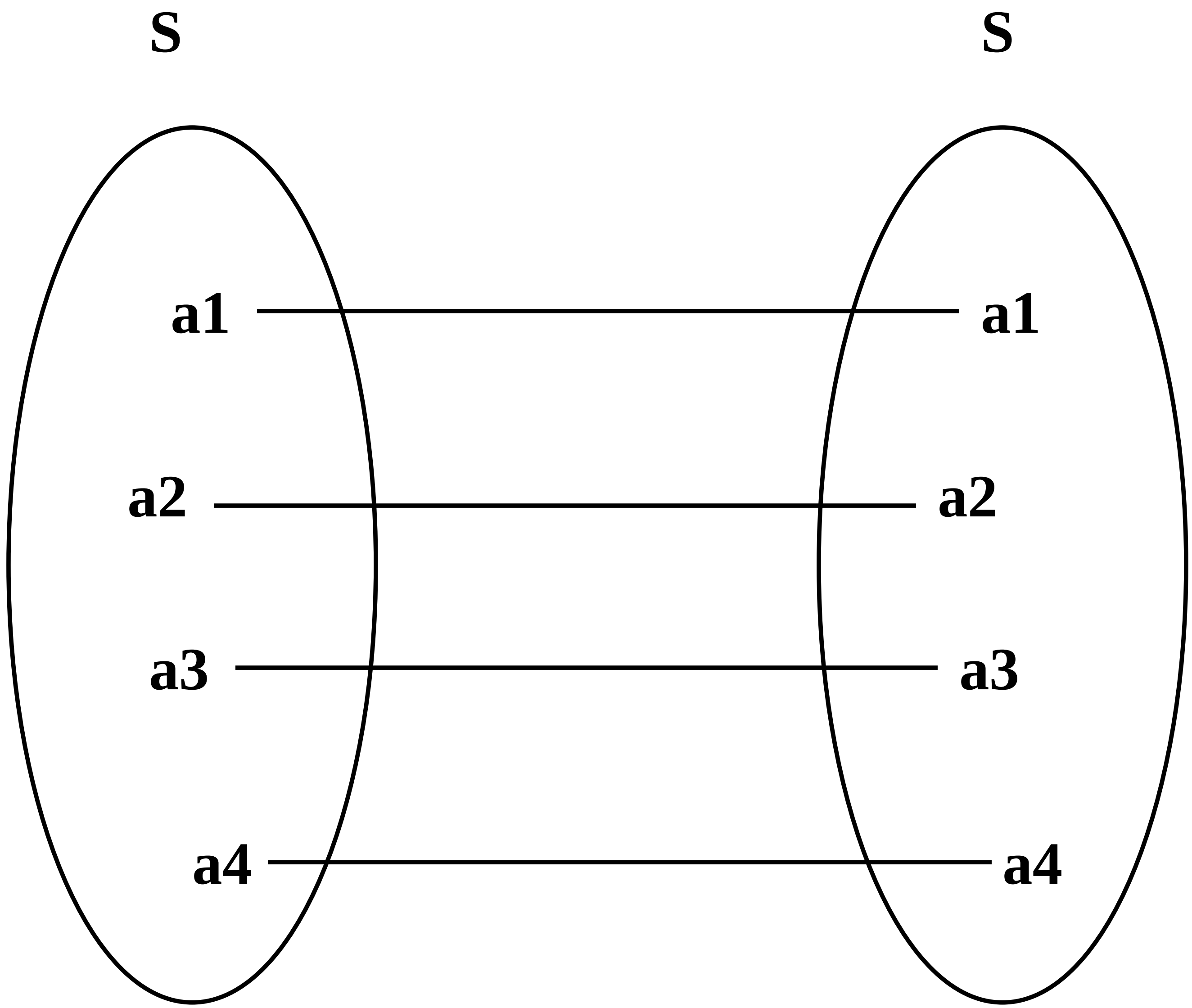
The Overriding Operator



Special Case



The Identity Relation



Binary Relation Operator Memberships (4)

$F \in r[w]$	$\exists x \cdot (\, x \in w \;\; \wedge \;\; x \mapsto F \in r \,)$
$E \mapsto F \in (p \,;\, q)$	$\exists x \cdot (\, E \mapsto x \in p \;\; \wedge \;\; x \mapsto F \in q \,)$
$E \mapsto F \in p \mathbin{\lhd\!\!\!+} q$	$(\mathrm{dom}\,(q) \mathbin{\lhd\!\!\!-} p) \;\cup\; q$
$E \mapsto F \in \mathrm{id}$	$F = E$

Binary Relation Operators (5)

Direct Product	$p \otimes q$
First Projection	prj_1
Second Projection	prj_2
Parallel Product	$p \parallel q$

Binary Relation Operator Memberships (5)

$E \mapsto (F \mapsto G) \in p \otimes q$	$E \mapsto F \in p \quad \wedge \quad E \mapsto G \in q$
$(E \mapsto F) \mapsto G \in \mathsf{prj}_1$	$G = E$
$(E \mapsto F) \mapsto G \in \mathsf{prj}_2$	$G = F$
$(E \mapsto G) \mapsto (F \mapsto H) \in p \parallel q$	$E \mapsto F \in p \quad \wedge \quad G \mapsto H \in q$

Summary of Binary Relation Operators

$S \leftrightarrow T$	$S \lhd r$	$r[w]$	prj_1
$\mathsf{dom}\,(r)$	$r \rhd T$	$p\,;\,q$	prj_2
$\mathsf{ran}\,(r)$	$S \trianglelefteq r$	$p \mathbin{\lhd\!\!\!+} q$	$\mathsf{id}\,(S)$
r^{-1}	$r \trianglerighteq T$	$p \otimes q$	$p \parallel q$

Classical Results with Relation Operators

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

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

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

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

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

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

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

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

$$\ldots$$

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

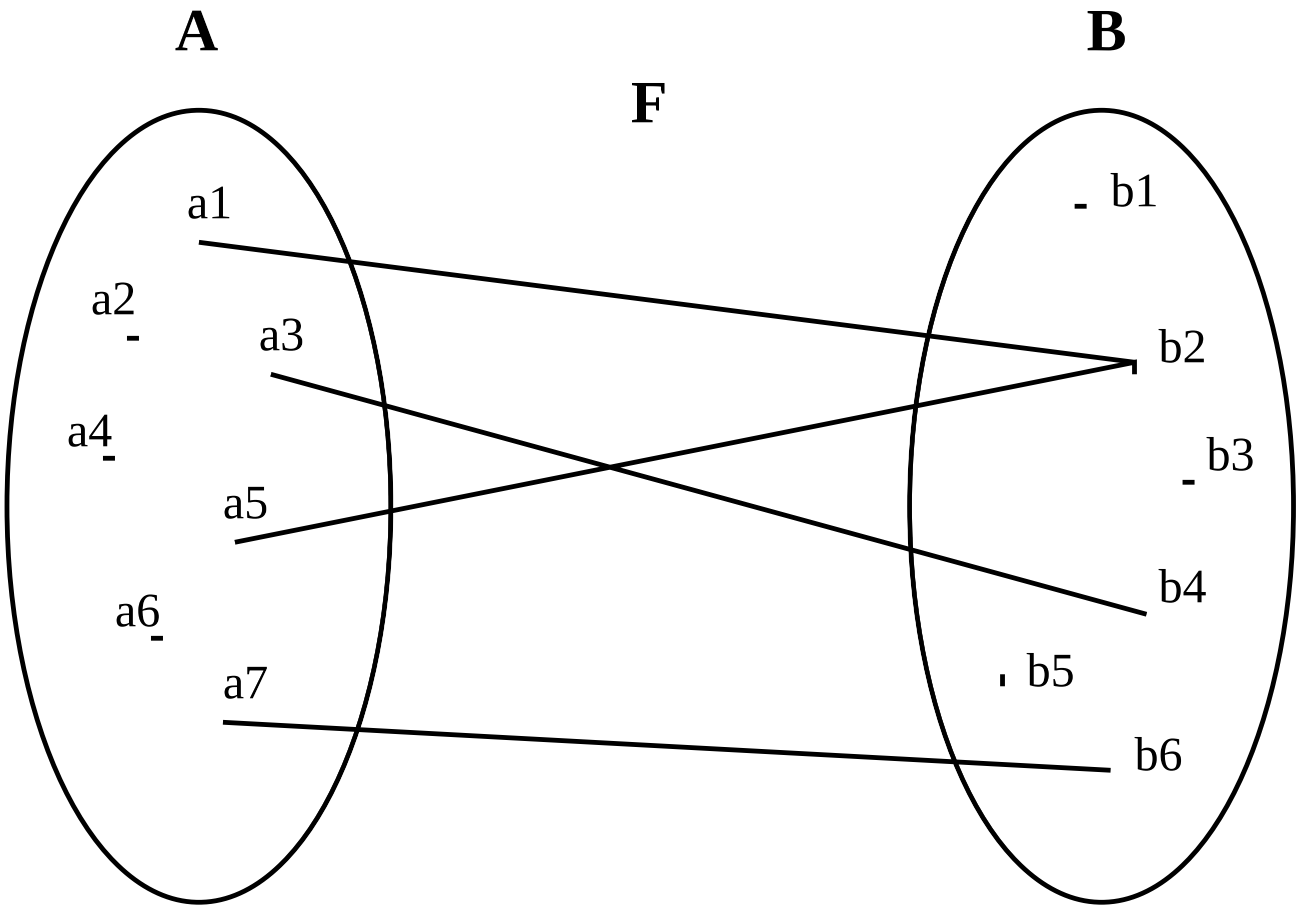
Given a relation r such that $r \in S \leftrightarrow S$

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

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

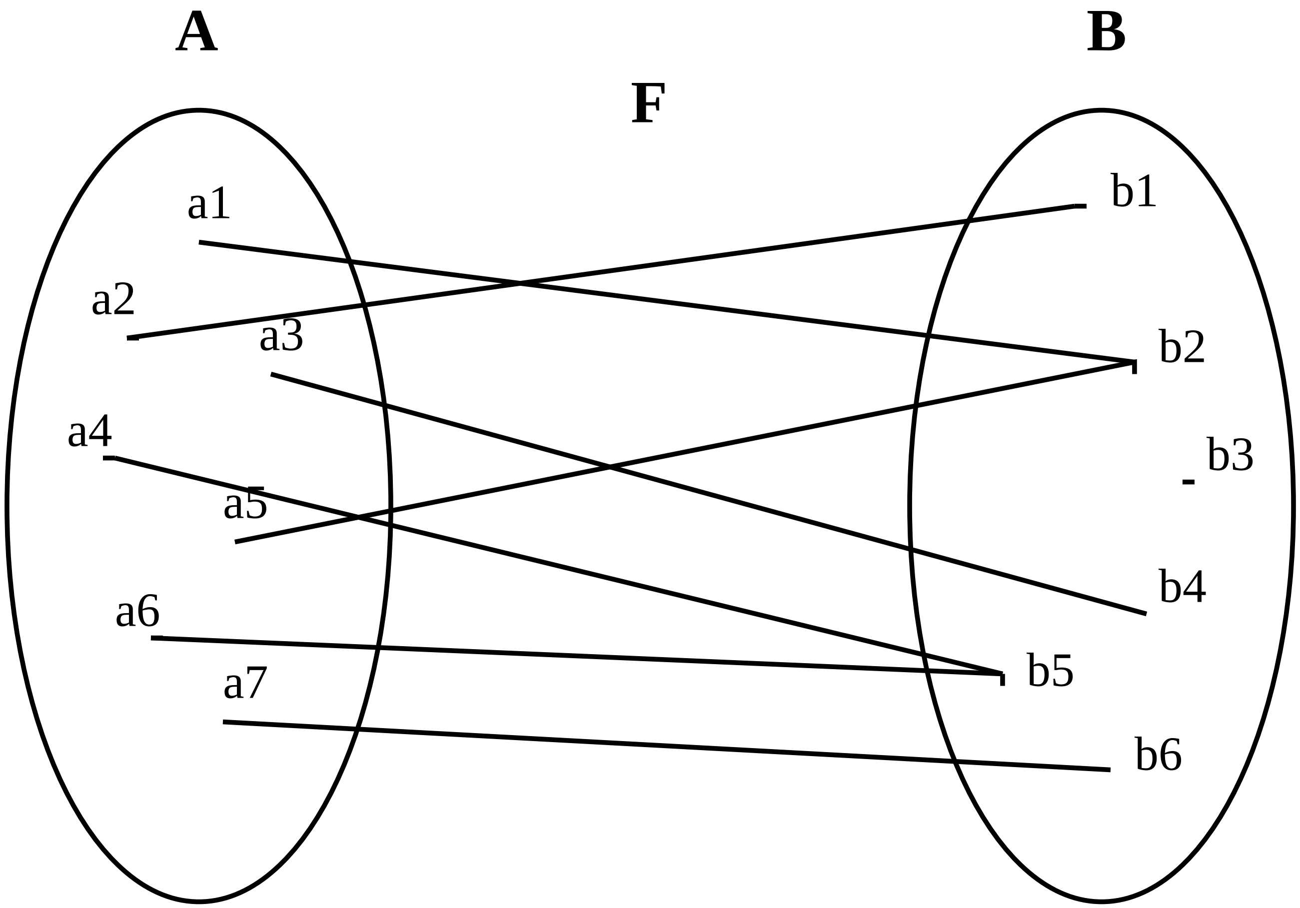
Partial functions	$S \nrightarrow T$
Total functions	$S \rightarrow T$
Partial injections	$S \rightarrowtail\!\!\!\!\!\!+\;\; T$
Total injections	$S \rightarrowtail T$

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



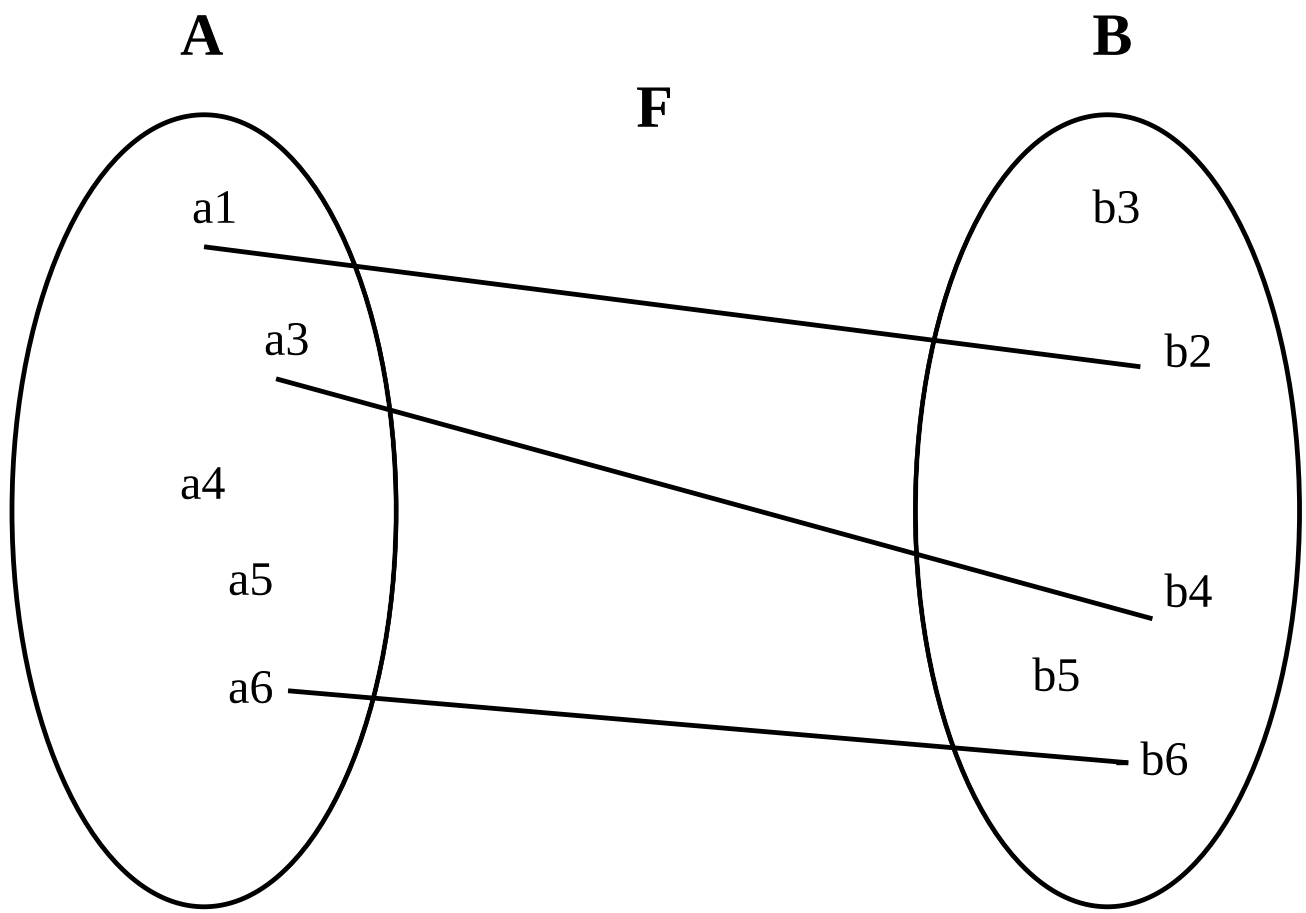
$$F \in A \nrightarrow B$$

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



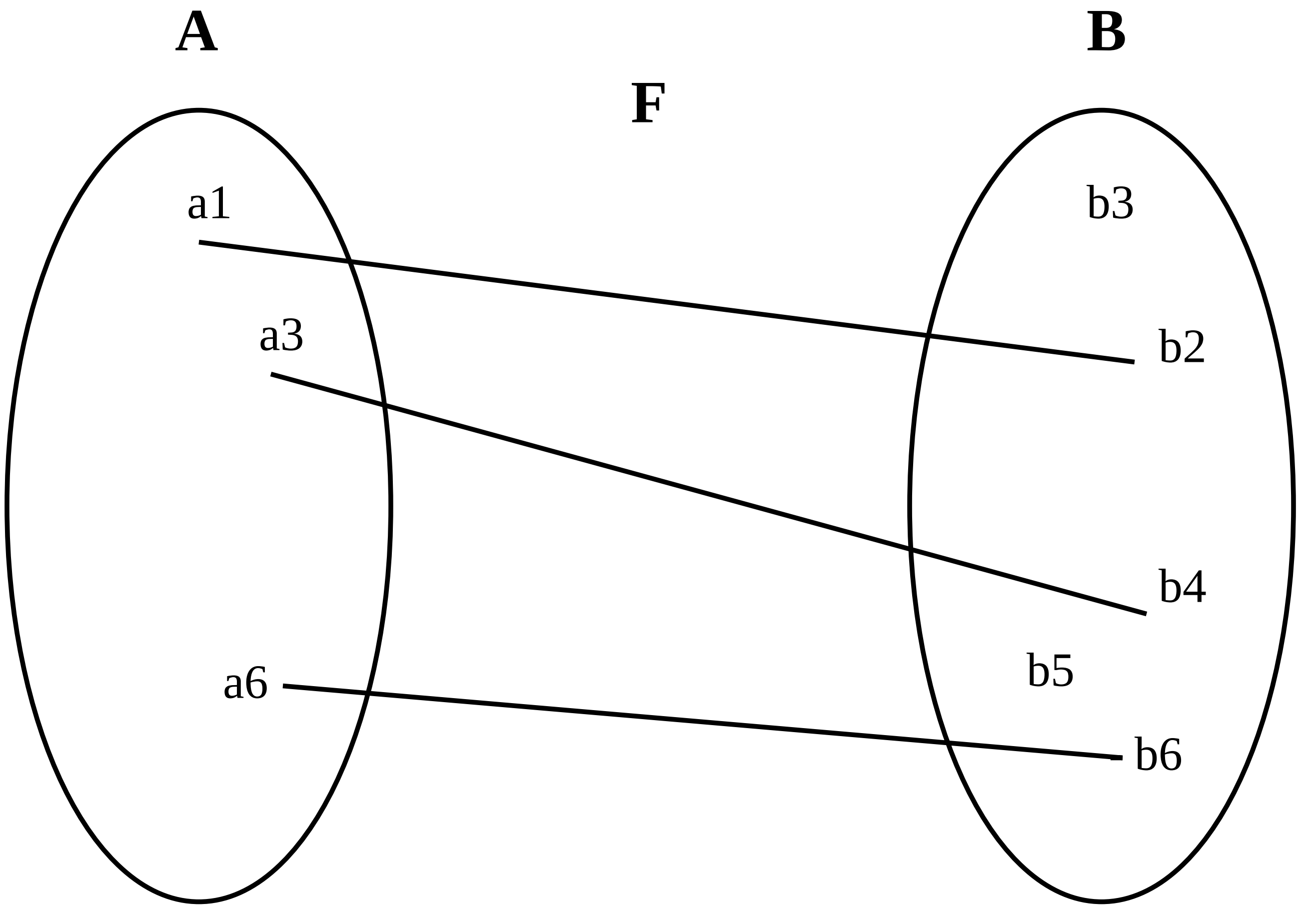
$$F \in A \rightarrow B$$

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



$$\boldsymbol{F} \in \boldsymbol{A} \rightarrowtail\!\!\!\!\!\!+\;\, \boldsymbol{B}$$

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



$$\boldsymbol{F \in A \rightarrowtail B}$$

Function Operator Memberships (1)

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

- The predicate:

$$f^{-1}\,;f \subseteq \mathrm{id}$$

- can be successively translated to:

$$\forall\, x, y, z \cdot x \mapsto y \in f \;\wedge\; x \mapsto z \in f \;\Rightarrow\; y = z$$

- This is done as follows by applying various rewriting rules:

$$f^{-1}\,;f \subseteq \mathrm{id}$$

$$\forall\, y, z \cdot y \mapsto z \in (f^{-1}\,;f) \;\Rightarrow\; y \mapsto z \in \mathrm{id}$$

$$\forall\, y, z \cdot y \mapsto z \in (f^{-1}\,;f) \;\Rightarrow\; y = z$$

$$\forall\, y, z \cdot (\exists\, x \cdot y \mapsto x \in f^{-1} \;\wedge\; x \mapsto z \in f) \;\Rightarrow\; y = z$$

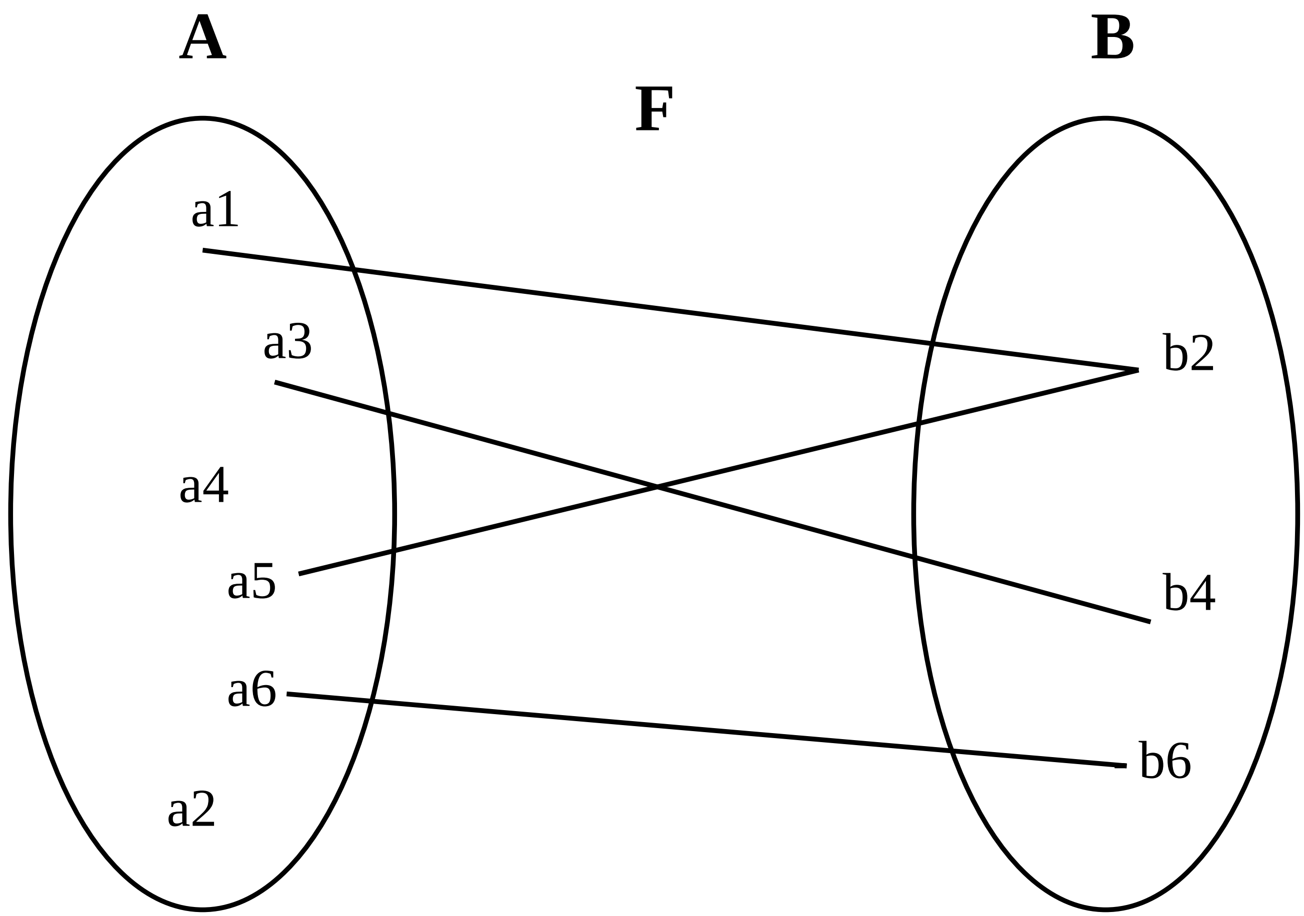
$$\forall\, y, z \cdot (\exists\, x \cdot x \mapsto y \in f \;\wedge\; x \mapsto z \in f) \;\Rightarrow\; y = z$$

$$\forall\, x, y, z \cdot x \mapsto y \in f \;\wedge\; x \mapsto z \in f \;\Rightarrow\; y = z$$

Function Operators (2)

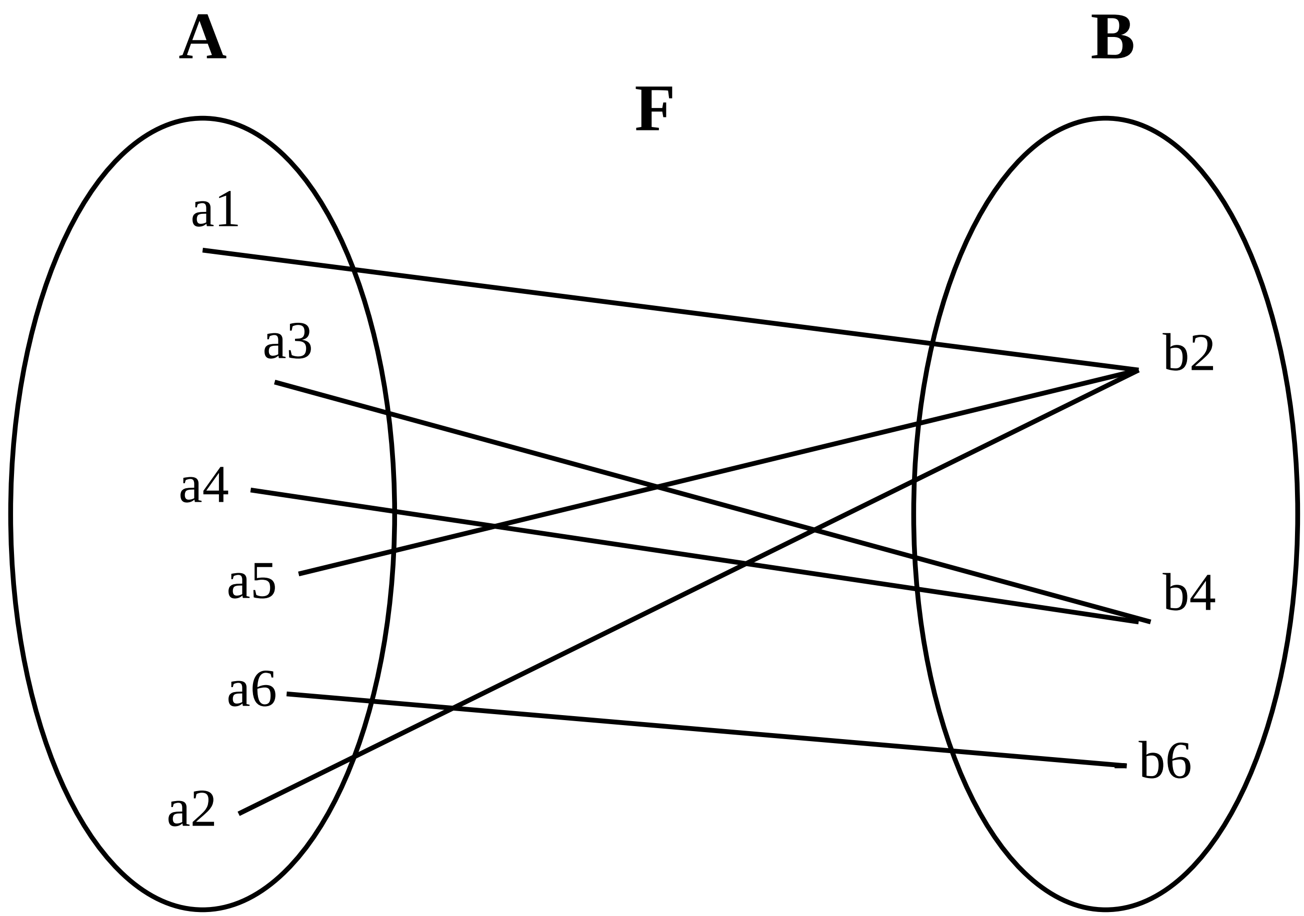
Partial surjections	$S \twoheadrightarrow\!\!\!\!\!\!+\; T$
Total surjections	$S \twoheadrightarrow T$
Bijections	$S \rightarrowtail\!\!\!\!\!\twoheadrightarrow T$

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



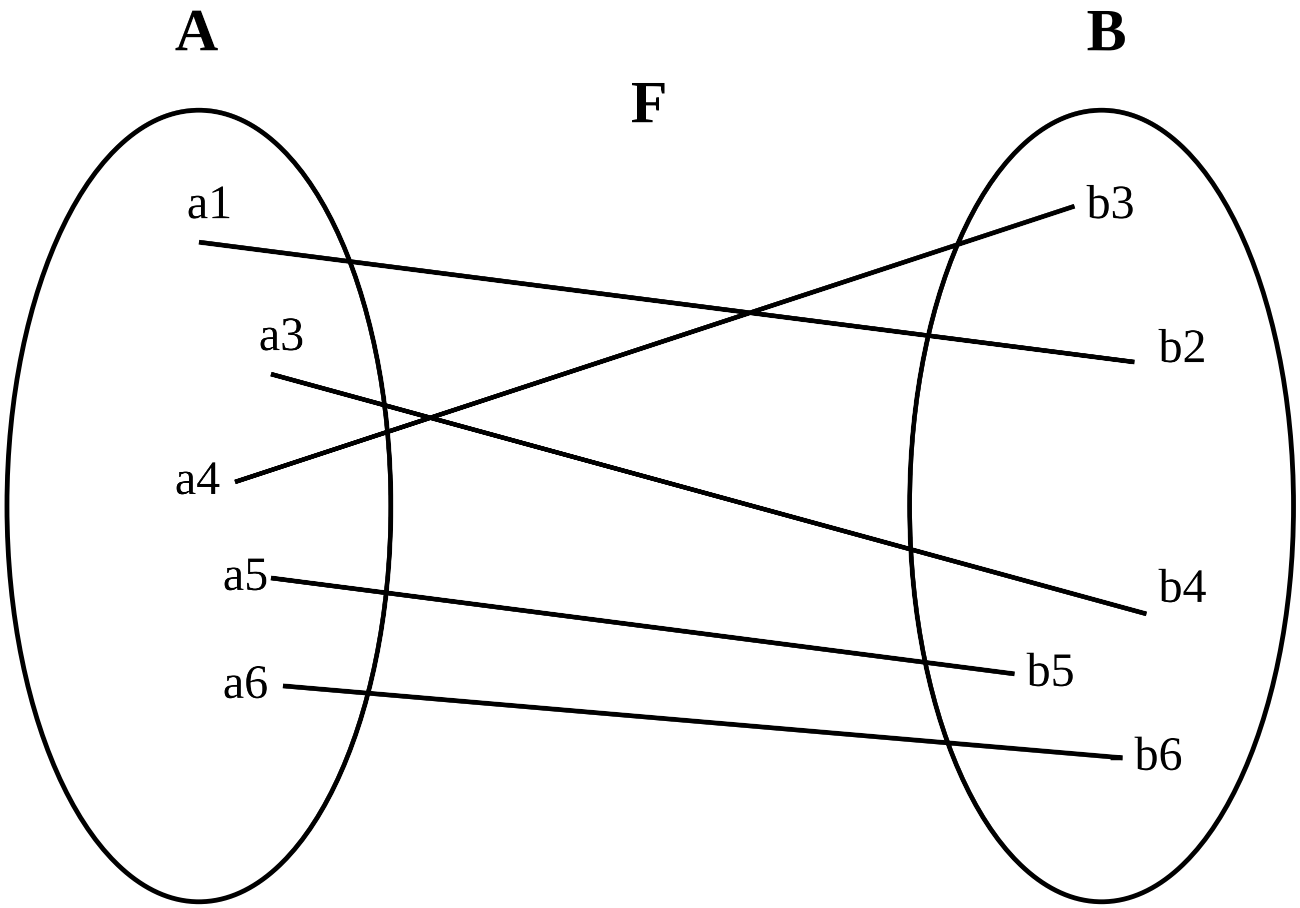
$$F \in A \twoheadrightarrow B$$

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



$$\boldsymbol{F \in A \twoheadrightarrow B}$$

A Bijection F from a Set A to a Set B



$$\boldsymbol{F} \in \boldsymbol{A} \rightarrowtail\!\!\!\!\twoheadrightarrow \boldsymbol{B}$$

Function Operator Memberships (2)

Left Part	Right Part
$f \in S \mathrel{+\mkern-18mu\twoheadrightarrow} T$	$f \in S \mathrel{+\mkern-18mu\rightarrow} T \quad \wedge \quad T = \mathrm{ran}(f)$
$f \in S \twoheadrightarrow T$	$f \in S \rightarrow T \quad \wedge \quad T = \mathrm{ran}(f)$
$f \in S \mathrel{\rightarrowtail\mkern-18mu\twoheadrightarrow} T$	$f \in S \rightarrowtail T \quad \wedge \quad f \in S \twoheadrightarrow T$

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

$S \times T$	$S \setminus T$	r^{-1}	$r[w]$	**id**	$\{x \mid x \in S \wedge P\}$
$\mathbb{P}(S)$	$S \leftrightarrow T$ $S \twoheadleftrightarrow T$	$S \lhd r$ $S \ntriangleleft r$	$p ; q$	$S \nrightarrow T$ $S \rightarrow T$	$\{x \cdot x \in S \wedge P \mid E\}$
$S \subseteq T$	$S \leftrightarrow\!\!\!\!\rightarrow T$ $S \twoheadleftrightarrow T$	$r \rhd T$ $r \ntriangleright T$	$p \Leftarrow q$	$S \rightarrowtail\!\!\!\!\!\nrightarrow T$ $S \rightarrowtail T$	$\{a, b, \ldots, n\}$
$S \cup T$	**dom** (r) **ran** (r)	$\mathbf{prj_1}$	$p \otimes q$	$S \nrightarrow\!\!\!\!\twoheadrightarrow T$ $S \twoheadrightarrow T$	union $\bigcup$
$S \cap T$	$\varnothing$	$\mathbf{prj_2}$	$p \parallel q$	$S \rightarrowtail\!\!\!\!\twoheadrightarrow T$	inter $\bigcap$

$$\lambda x \cdot x \in S \mid E(x)$$

Left Part	Right Part
$a \mapsto b \;\in\; \lambda x \cdot x \in S \mid E(x)$	$E(a) = b$

Side Condition: $a \in S$

Given a partial function $\boldsymbol{f}$, we have

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

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

Purpose of this Presentation

- Foundation for deductive and formal proofs

- A quick review of Propositional Calculus

- A quick review of First Order Predicate Calculus

- A refresher on Set Theory

- Formalising Data Structures (list, tree, graph)

Infinite List (1)

- Defining an infinite list built on a set V

- We have a point f of V (the beginning of the list)

- We have a bijective function n from V to $V \setminus \{f\}$.

This can be formalized as follows:

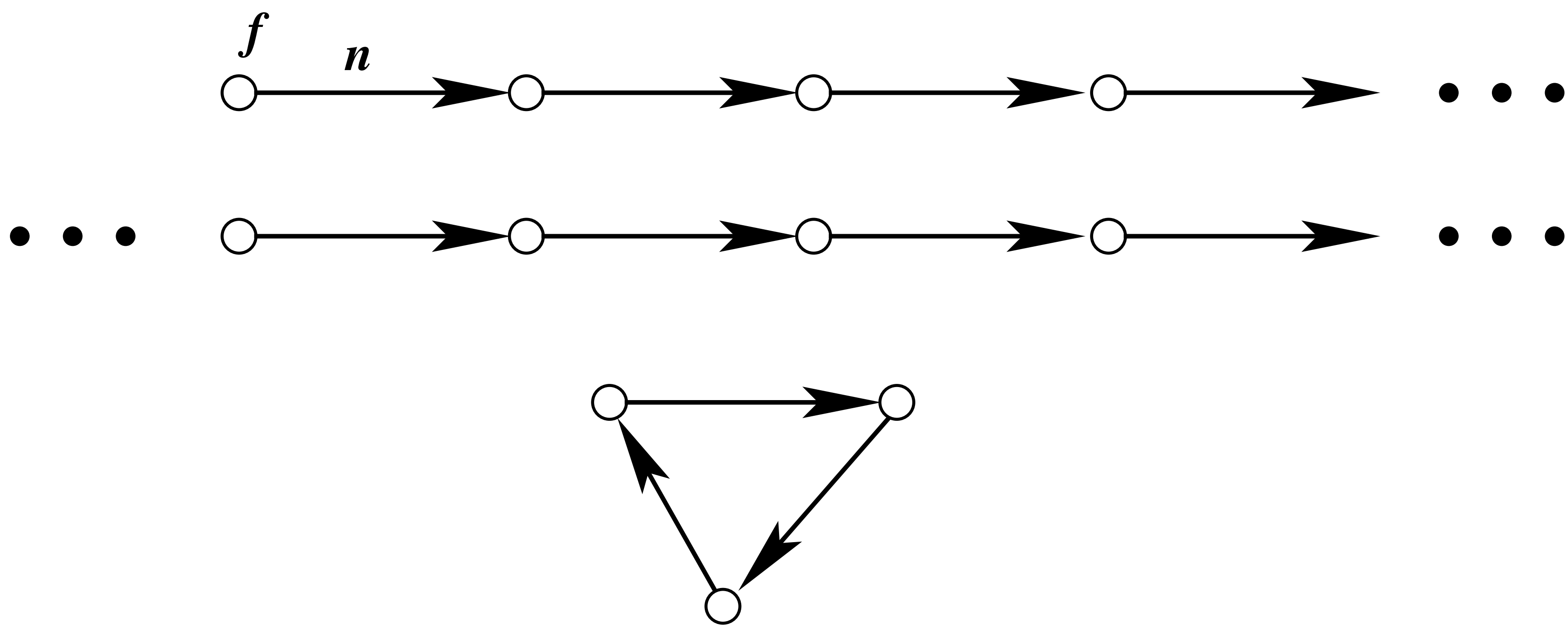
$$\mathbf{axm\_1:} \quad f \in V$$

$$\mathbf{axm\_2:} \quad n \in V \rightarrowtail\!\!\!\!\twoheadrightarrow V \setminus \{f\}$$

Infinite List (2)

- However, **axm_1** and **axm_2** are not sufficient

- We must say that there are:
    - no cycles
    - no backward infinite chains



Infinite List (3): Cycles and Backward Infinite Chains

- Suppose a set S is made of a cycle or an infinite BACKWARD chain

- Each point x in S is related to a point y in S by the relation n^{-1}.

$$y \xleftarrow{\quad n^{-1} \quad} x$$

$$\forall x \cdot x \in S \Rightarrow (\exists y \cdot y \in S \wedge x \mapsto y \in n^{-1})$$

$$S \subseteq n[S]$$

- But as the empty set enjoys this property, we have thus:

$$\boxed{\textbf{axm\_3}: \quad \forall S \cdot S \subseteq n[S] \Rightarrow S = \varnothing}$$

Summary of Axioms for infinite List

$$\textbf{axm\_1}: \quad f \in V$$

$$\textbf{axm\_2}: \quad n \in V \rightarrowtail\!\!\!\!\!\twoheadrightarrow V \setminus \{f\}$$

$$\textbf{axm\_3}: \quad \forall S \cdot S \subseteq n[S] \;\Rightarrow\; S = \varnothing$$

- From axm_3

$$\boxed{\mathbf{axm\_3:} \quad \forall S \cdot S \subseteq n[S] \;\Rightarrow\; S = \varnothing}$$

- We can deduce the following theorem (hint: instantiate S with $V \setminus T$)

$$\boxed{\mathbf{thm1:} \quad \forall T \cdot f \in T \;\wedge\; n[T] \subseteq T \;\Rightarrow\; V = T}$$

- By unfolding $n[T] \subseteq T$, we obtain:

$$\boxed{\mathbf{thm\_2:} \quad \forall T \cdot f \in T \;\wedge\; (\forall x \cdot x \in T \Rightarrow n(x) \in T) \;\Rightarrow\; V = T}$$

- Proving that each element x in the list has a property $P(x)$.

$$\forall\, x \cdot x \in V \Rightarrow P(x)$$

- The same as proving: $V = \{\, x \mid x \in V \land P(x)\}$

- For this, we instantiate T with $\{\, x \mid x \in V \land P(x)\}$ in **thm_2**:

$$\boxed{\mathbf{thm\_2:} \quad \forall T \cdot f \in T \;\land\; (\forall x \cdot x \in T \Rightarrow n(x) \in T) \;\Rightarrow\; V = T}$$

- This requires proving successively:

$$P(f)$$

$$\forall x \cdot x \in V \land P(x) \Rightarrow n(x) \in V \land P(n(x))$$

Example: the Natural Numbers (1)

$$\begin{array}{ll} \mathbf{axm\_1:} & \boldsymbol{f} \in \boldsymbol{V} \\ \mathbf{axm\_2:} & \boldsymbol{n} \in \boldsymbol{V} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \boldsymbol{V} \setminus \{\boldsymbol{f}\} \end{array}$$

Translating these axioms to the set of Natural Numbers, $\mathbb{N}$, we obtain:

$$\begin{array}{ll} \mathbf{axm\_1:} & \mathbf{0} \in \mathbb{N} \\ \mathbf{axm\_2:} & \boldsymbol{succ} \in \mathbb{N} \rightarrowtail\!\!\!\!\!\twoheadrightarrow \mathbb{N} \setminus \{0\} \end{array}$$

This corresponds to the four first Peano Axioms

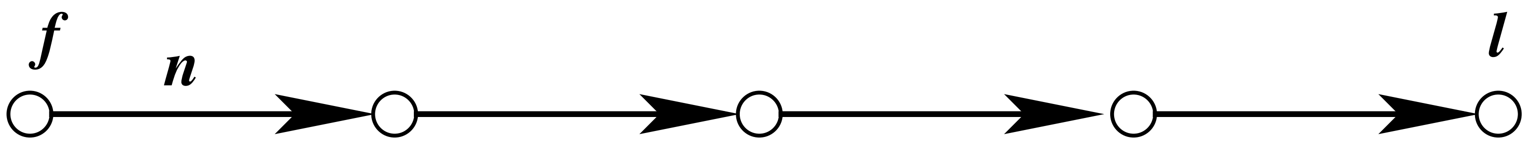
Example: the Natural Numbers (2)

$$\mathbf{thm\_2:} \quad \forall T \cdot f \in T \ \wedge \ (\forall x \cdot x \in T \Rightarrow n(x) \in T) \ \Rightarrow \ V = T$$

Translating this to the natural numbers, we obtain the fifth Peano axiom.

$$\forall T \cdot 0 \in T \ \wedge \ (\forall x \cdot x \in T \Rightarrow x + 1 \in T) \ \Rightarrow \ \mathbb{N} = T$$

Finite List



- Here are the axioms of finite lists

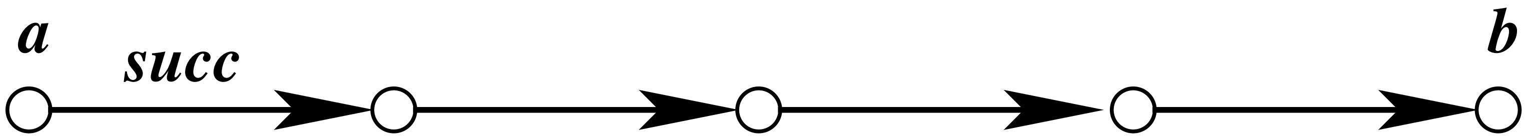
$$
\begin{array}{ll}
\mathbf{axm\_1:} & f \in V \\
\mathbf{axm\_2:} & l \in V \\
\mathbf{axm\_3:} & n \in V \setminus \{l\} \rightarrowtail\!\!\!\!\rightarrow V \setminus \{f\} \\
\mathbf{axm\_4:} & \forall S \cdot S \subseteq n[S] \;\Rightarrow\; S = \varnothing
\end{array}
$$

- Notice that axiom **axm_4** is not symmetric with regard to both directions on the list.

- But this can be proved in a systematic manner.

Example of Finite List: Interval

A classical example is a numerical interval $a\,..\,b$ (with $a \leq b$).



It is easy to prove the following:

$$a \in a\,..\,b$$

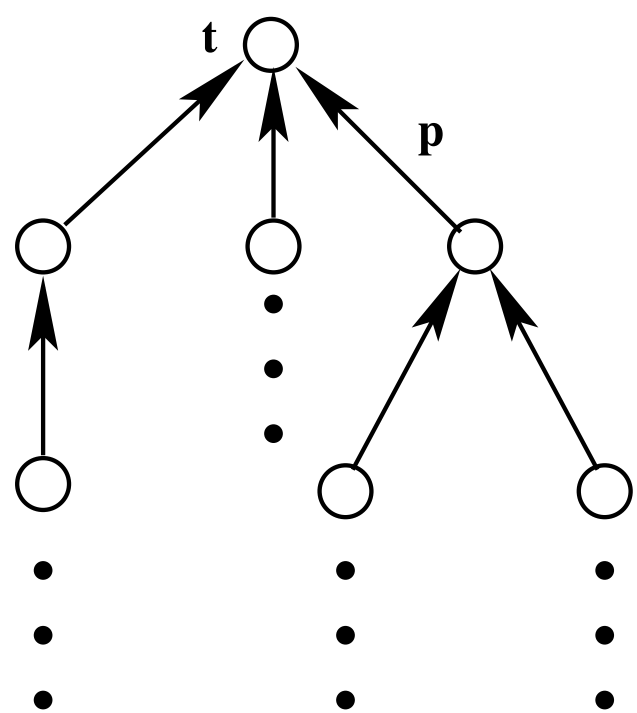
$$b \in a\,..\,b$$

$$(a\,..\,b-1) \lhd succ \;\in\; (a\,..\,b) \setminus \{b\} \rightarrowtail\!\!\!\!\twoheadrightarrow (a\,..\,b) \setminus \{a\}$$

- Infinite trees generalise infinite lists.

-The beginning f of the list is replaced by the top t of the tree.

-The function p replaces n^{-1} of the infinite list



$$\mathbf{axm\_1:} \quad t \in V$$

$$\mathbf{axm\_2:} \quad p \in V \setminus \{t\} \twoheadrightarrow V$$

$$\mathbf{axm\_3:} \quad \forall S \cdot S \subseteq p^{-1}[S] \;\Rightarrow\; S = \varnothing$$

We define an induction rule which generalise that of infinite lists.

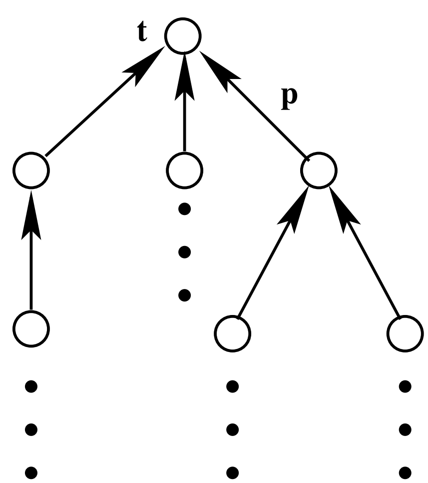
$$\mathbf{thm\_1:} \quad \forall T \cdot t \in T \;\wedge\; p^{-1}[T] \subseteq T \;\Rightarrow\; V = T$$

Induction Rule for Infinite Trees

thm_1: $\forall T \cdot t \in T \;\wedge\; p^{-1}[T] \subseteq T \;\Rightarrow\; V = T$

thm_1 can be further unfolded to the following equivalent one:

thm_2: $\forall T \cdot$ $t \in T$
$\forall x \cdot x \in V \setminus \{t\} \;\wedge\; p(x) \in T \;\Rightarrow\; x \in T$
$\Rightarrow$
$V = T$



Proof of Unfolding

$$p^{-1}[T] \;\subseteq\; T$$

$$\Leftrightarrow$$

$$\forall x \cdot x \in p^{-1}[T] \;\Rightarrow\; x \in T$$

$$\Leftrightarrow$$

$$\forall x \cdot (\, \exists y \cdot y \in T \;\wedge\; x \mapsto y \in p \,) \;\Rightarrow\; x \in T$$

$$\Leftrightarrow$$

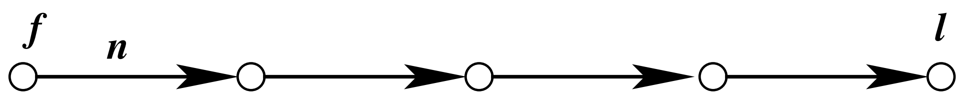
$$\forall x \cdot (\, \exists y \cdot y \in T \;\wedge\; x \in \mathrm{dom}(p) \;\wedge\; y = p(x) \,) \;\Rightarrow\; x \in T$$

$$\Leftrightarrow$$

$$\forall x \cdot x \in V \setminus \{t\} \;\wedge\; p(x) \in T \;\Rightarrow\; x \in T$$

$$\boxed{\mathbf{axm\_2:} \quad p \in V \setminus \{t\} \twoheadrightarrow V}$$

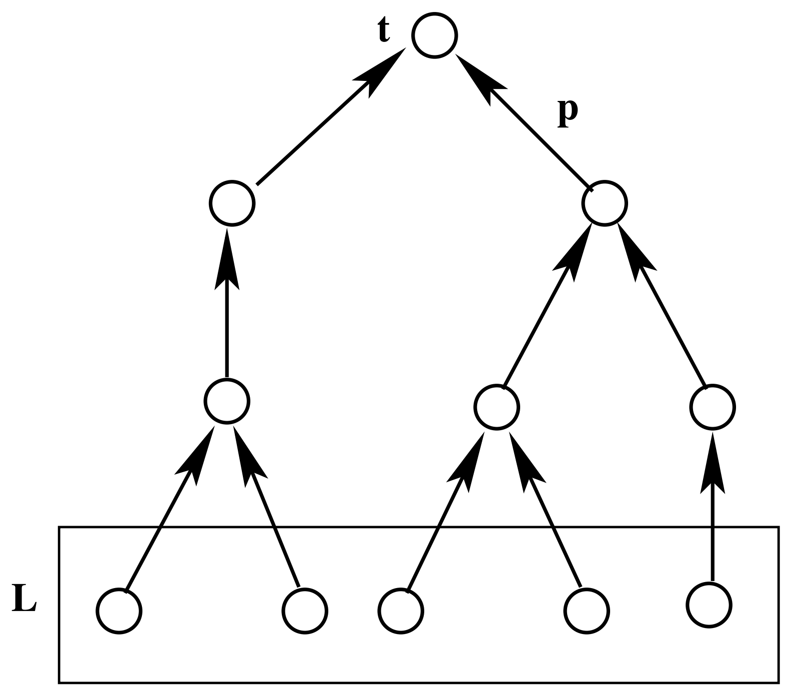
- Finite depth trees generalise finite lists.



- We still have a top point t which was f in the list.

- But the last element l of the list is now replaced by a set L.

- These are the so-called leafs of the tree.

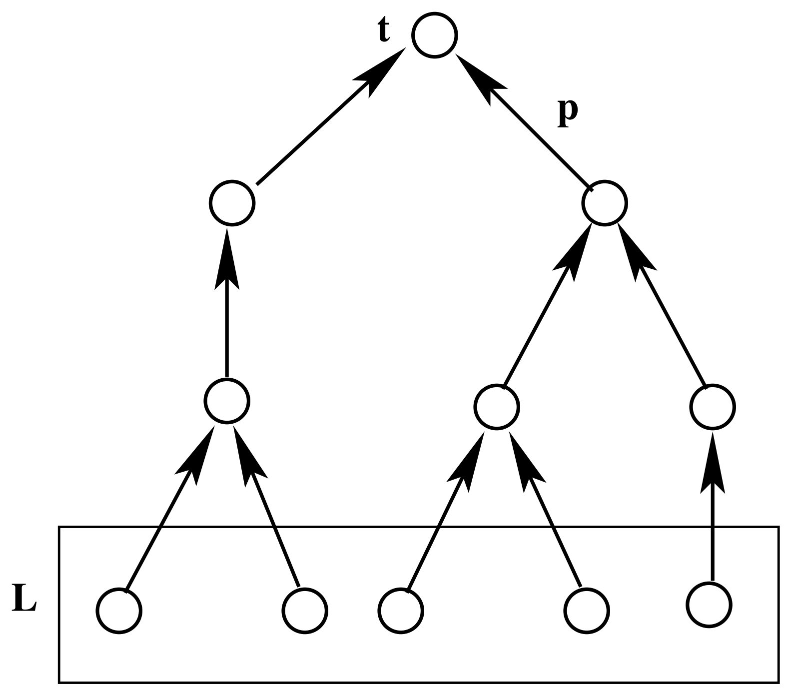


$$\mathbf{axm\_1:} \quad t \in V$$

$$\mathbf{axm\_2:} \quad L \subseteq V$$

$$\mathbf{axm\_3:} \quad p \in V \setminus \{t\} \twoheadrightarrow V \setminus L$$

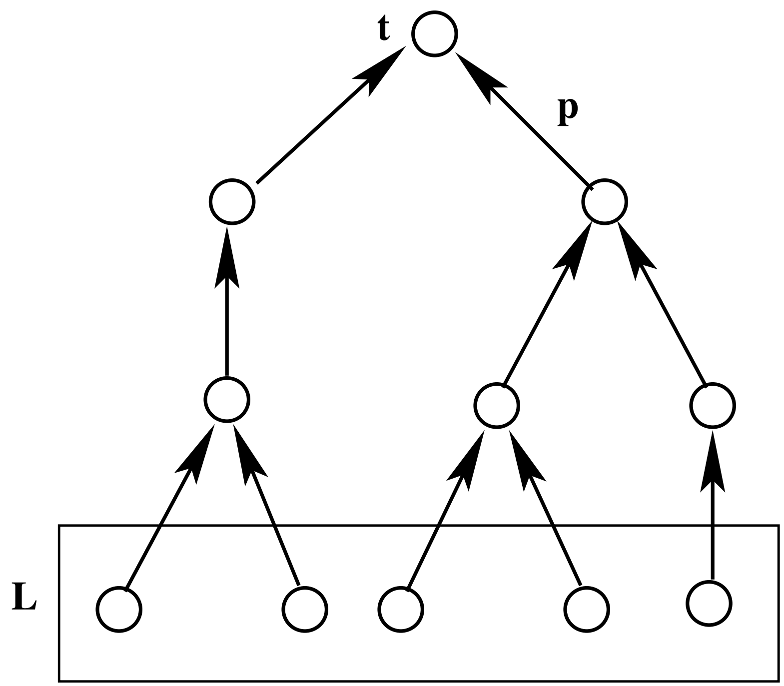
$$\mathbf{axm\_4:} \quad \forall S \cdot S \subseteq p^{-1}[S] \;\Rightarrow\; S = \varnothing$$



- As for finite lists, we have possible inductions in both directions.

$$\textbf{thm\_1}: \quad \forall T \cdot t \in T \;\wedge\; p^{-1}[T] \subseteq T \;\Rightarrow\; V = T$$

$$\textbf{thm\_4}: \quad \forall T \cdot L \subseteq T \;\wedge\; p[T] \subseteq T \;\Rightarrow\; V = T$$



Let a, b and c be three binary relations:

$$a \in S \leftrightarrow T$$

$$b \in T \leftrightarrow U$$

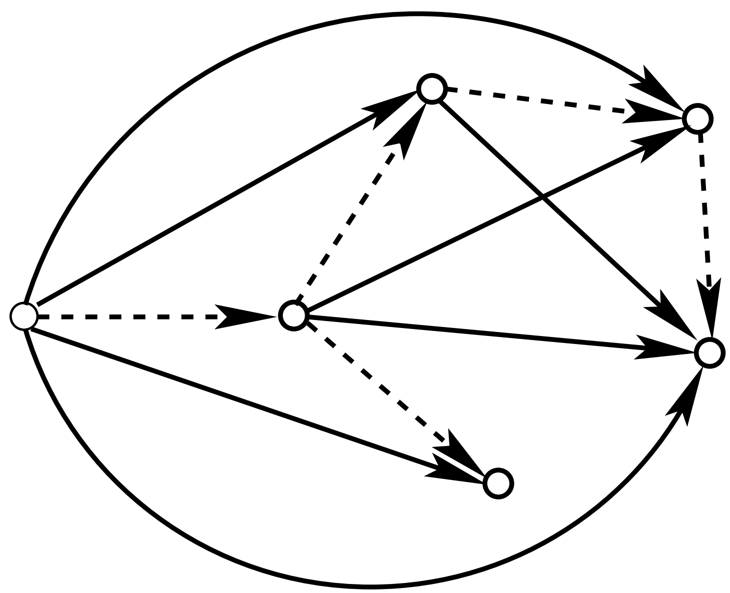
$$c \in S \leftrightarrow U$$

We have then the following theorem:

$$a\,;b \subseteq c \;\Leftrightarrow\; a \subseteq \overline{(b\,;\overline{c^{-1}})^{-1}}$$

Irreflexive Transitive Closure

- We are given a relation r from a set S to itself
- The irreflexive transitive closure of r is denoted by cl(r).
- cl(r) is also a relation from S to S.
- The characteristic properties of cl(r) are the following:
    1. Relation r is included in cl(r)
    2. The forward composition of cl(r) with r is included in cl(r)
    3. Relation cl(r) is the smallest relation dealing with 1 and 2



Axioms for Irreflexive Transitive Closure

$$\mathbf{axm\_1:} \quad r \;\in\; S \leftrightarrow S$$

$$\mathbf{axm\_2:} \quad \mathsf{cl}(r) \;\in\; S \leftrightarrow S$$

$$\mathbf{axm\_3:} \quad r \;\subseteq\; \mathsf{cl}(r)$$

$$\mathbf{axm\_4:} \quad \mathsf{cl}(r)\,;r \;\subseteq\; \mathsf{cl}(r)$$

$$\mathbf{axm\_5:} \quad \forall p \cdot \; r \subseteq p \;\;\land\;\; p\,;r \subseteq p \;\;\Rightarrow\;\; \mathsf{cl}(r) \subseteq p$$

Properties of the Irreflexive Transitive Closure

$$\mathbf{thm\_1:} \quad \mathsf{cl}(r) \mathbin{;} \mathsf{cl}(r) \subseteq \mathsf{cl}(r)$$

$$\mathbf{thm\_2:} \quad \mathsf{cl}(r) = r \cup r \mathbin{;} \mathsf{cl}(r)$$

$$\mathbf{thm\_3:} \quad \mathsf{cl}(r) = r \cup \mathsf{cl}(r) \mathbin{;} r$$

$$\mathbf{thm\_4:} \quad \forall s \cdot r[s] \subseteq s \;\Rightarrow\; \mathsf{cl}(r)[s] \subseteq s$$

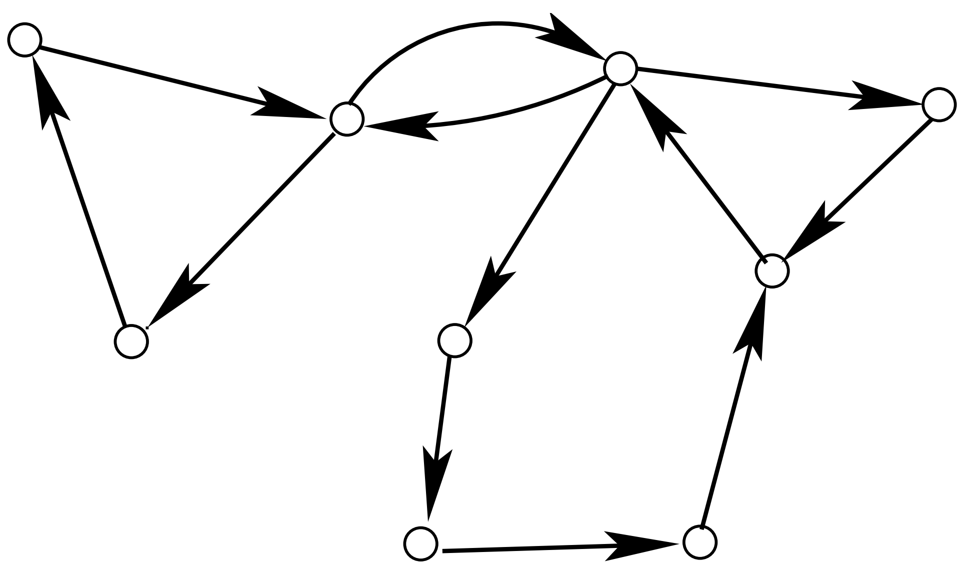
$$\mathbf{thm\_5:} \quad \mathsf{cl}(r^{-1}) = \mathsf{cl}(r)^{-1}$$

Strongly Connected Graph

- We are given a set V and a non-empty binary relation r from V to itself

- The graph representing this relation is strongly connected

- if any two distinct points in V are connected by a path built on r



Axioms for Strongly Connected Graph

$$\mathbf{axm\_1:} \quad \boldsymbol{r} \in \boldsymbol{V} \leftrightarrow \boldsymbol{V}$$

$$\mathbf{axm\_2:} \quad \boldsymbol{V} \times \boldsymbol{V} \subseteq \mathrm{cl}(\boldsymbol{r})$$

- Basic property

$$\mathbf{thm\_1:} \quad \forall \boldsymbol{S} \cdot \boldsymbol{S} \neq \varnothing \ \wedge \ \boldsymbol{r}[\boldsymbol{S}] \subseteq \boldsymbol{S} \ \Rightarrow \ \boldsymbol{V} = \boldsymbol{S}$$

- This is an induction rule