Summary of Mathematical Notation

Jean-Raymond Abrial (ETHZ)

March 2008

Purpose of this Presentation

- Topics:
  - Foundation for deductive and formal proofs
  - A quick review of Propositional Calculus
  - A quick review of First Order Predicate Calculus
  - A quick review of Set Theory
  - A quick review of Arithmetic

- WARNING: This presentation does not contain an exhaustive treatment of proof, first order logic, set theory, and arithmetic

- It is a REMINDER of notions supposedly already encountered

- 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

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

$$\frac{\mathbf{A}}{\mathbf{C}} \quad \mathbf{R}$$

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

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

Most steps done in a proof are backward steps

“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, 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

Example of a Proof

- We are given the following set of inference rules

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

- We have 7 rules **r1** to **r7**

- S1 to S7 are supposed to denote some sequents

- Notice that rules **r1**, **r4**, **r6**, and **r7** have no antecedents

- Our intention is to prove sequent $S1$ using backward reasoning

Proof of sequent $S1$

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

$$S1$$

?

Proof of Sequent $S1$

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

$$\begin{tikzcd}
 & \begin{array}{c} S1 \\ \mathbf{r3} \end{array} & \\
\begin{array}{c} S2 \\ \mathbf{?} \end{array} \arrow[ur] & \begin{array}{c} S3 \\ \mathbf{?} \end{array} \arrow[u] & \begin{array}{c} S4 \\ \mathbf{?} \end{array} \arrow[ul]
\end{tikzcd}$$

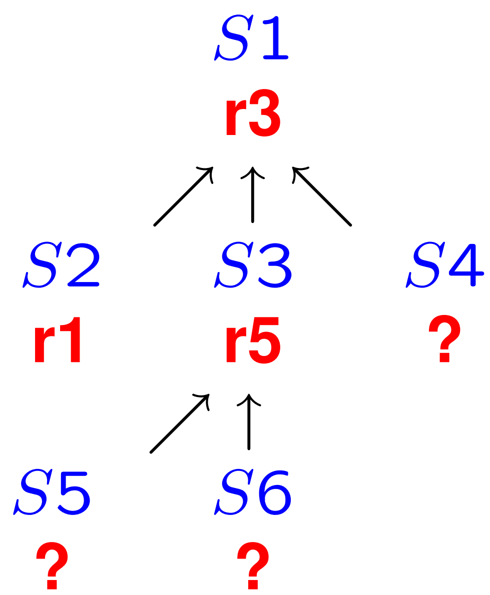
Proof of Sequent $S1$

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

$$\begin{tikzcd} & \begin{array}{c} S1 \\ \mathbf{r3} \end{array} & \\ \begin{array}{c} S2 \\ \mathbf{r1} \end{array} \arrow[ur] & \begin{array}{c} S3 \\ \mathbf{?} \end{array} \arrow[u] & \begin{array}{c} S4 \\ \mathbf{?} \end{array} \arrow[ul] \end{tikzcd}$$

Proof of Sequent $S1$

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



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

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

Proof of Sequent $S1$

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

$$\begin{array}{ccc}
 & S1 & \\
 & \textbf{r3} & \\
\nearrow & \uparrow & \nwarrow \\
S2 & S3 & S4 \\
\textbf{r1} & \textbf{r5} & \textbf{?} \\
\nearrow & \uparrow & \\
S5 & S6 & \\
\textbf{r4} & \textbf{r6} &
\end{array}$$

Proof of Sequent $S1$

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

$$\begin{tikzcd}
 & \substack{S1 \\ \mathbf{r3}} & \\
\substack{S2 \\ \mathbf{r1}} \arrow[ur] & \substack{S3 \\ \mathbf{r5}} \arrow[u] & \substack{S4 \\ \mathbf{r2}} \arrow[ul] \\
\substack{S5 \\ \mathbf{r4}} \arrow[ur] & \substack{S6 \\ \mathbf{r6}} \arrow[u] & \substack{S7 \\ \mathbf{?}} \arrow[u]
\end{tikzcd}$$

Proof of Sequent $S1$

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

$$\begin{tikzcd}
 & \begin{array}{c} S1 \\ \textbf{r3} \end{array} & \\
\begin{array}{c} S2 \\ \textbf{r1} \end{array} \arrow[ur] & \begin{array}{c} S3 \\ \textbf{r5} \end{array} \arrow[u] & \begin{array}{c} S4 \\ \textbf{r2} \end{array} \arrow[ul] \\
\begin{array}{c} S5 \\ \textbf{r4} \end{array} \arrow[ur] & \begin{array}{c} S6 \\ \textbf{r6} \end{array} \arrow[u] & \begin{array}{c} S7 \\ \textbf{r7} \end{array} \arrow[u]
\end{tikzcd}$$

Recording the Proof of Sequent $S1$

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

$$\begin{tikzcd}
 & \begin{array}{c} S1 \\ \textbf{r3} \end{array} & \\
\begin{array}{c} S2 \\ \textbf{r1} \end{array} \arrow[ur] & \begin{array}{c} S3 \\ \textbf{r5} \end{array} \arrow[u] & \begin{array}{c} S4 \\ \textbf{r2} \end{array} \arrow[ul] \\
\begin{array}{c} S5 \\ \textbf{r4} \end{array} \arrow[ur] & \begin{array}{c} S6 \\ \textbf{r6} \end{array} \arrow[u] & \begin{array}{c} S7 \\ \textbf{r7} \end{array} \arrow[u]
\end{tikzcd}$$

- The proof is a tree

Alternate Representation of the Proof Tree

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

- A vertical representation of the proof tree:

$$\begin{array}{ccc}
 & S1 & \\
 & \mathbf{r3} & \\
\nearrow & \uparrow & \nwarrow \\
S2 & S3 & S4 \\
\mathbf{r1} & \mathbf{r5} & \mathbf{r2} \\
\nearrow & \uparrow & \uparrow \\
S5 & S6 & S7 \\
\mathbf{r4} & \mathbf{r6} & \mathbf{r7}
\end{array}$$

$$\begin{array}{lll}
S1 & & \mathbf{r3} \\
\quad S2 & & \mathbf{r1} \\
\quad S3 & & \mathbf{r5} \\
\qquad S5 & & \mathbf{r4} \\
\qquad S6 & & \mathbf{r6} \\
\quad S4 & & \mathbf{r2} \\
\qquad S7 & & \mathbf{r7}
\end{array}$$

Foundation for Deductive (and formal) Proofs

- Concepts of Sequent and Inference Rule

- Backward and Forward Reasoning

- <u>Basic Inference Rules</u>

Being (a Little) more Precise About Sequents

- We supposedly have a PREDICATE Language (NOT DEFINED YET)

- A sequent is denoted by the following construct: $\boxed{\mathbf{H} \vdash \mathbf{G}}$

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

- **G** is a predicate: the goal

Under the hypotheses of collection **H**, prove the goal **G**

- There are three basic inference rules

- These rules are independent of our future Predicate Language

- **HYP**: If the goal belongs to the hypotheses of a sequent,

  then the sequent is proved,

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

- **MON**: Once a sequent is proved, any sequent with the same goal and more hypotheses is also proved,

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

- **CUT**: If you succeed in proving **P** under **H**, then **P** can be added to the collection **H** for proving a goal **Q**.

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

- It will be done by successive refinements:

  (1) Propositional Language

  (2) First Order Predicate Language

  (3) Equality and Pairs

  (4) Set theory

  (5) Arithmetic

- Each additional language is built on top of the previous ones

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 quick review of Set Theory

- A quick review of Arithmetic

- Given predicates P and Q, we can construct:

- NEGATION: $\neg P$

- CONJUNCTION: $P \wedge Q$

- IMPLICATION: $P \Rightarrow Q$

$$
\begin{aligned}
\mathit{Predicate} \ ::= \ & \neg \ \mathit{Predicate} \\
& \mathit{Predicate} \ \wedge \ \mathit{Predicate} \\
& \mathit{Predicate} \ \Rightarrow \ \mathit{Predicate}
\end{aligned}
$$

- This syntax is ambiguous

- Pairs of matching parentheses can be added freely.

- Operator $\wedge$ is associative: $P \wedge Q \wedge R$ is allowed.

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

- Write explicitely either $(P \Rightarrow Q) \Rightarrow R$ or $P \Rightarrow (Q \Rightarrow R)$.

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

- Example:

$\neg P \Rightarrow Q \wedge R$ is to be read as $(\neg P) \Rightarrow (Q \wedge R)$

Propositional Calculus Rules of Inference (1)

- Rules about conjunction

$$\frac{\mathbf{H, P, Q} \;\vdash\; \mathbf{R}}{\mathbf{H,\ P \wedge Q} \;\vdash\; \mathbf{R}} \quad \textbf{AND\_L}$$

$$\frac{\mathbf{H} \;\vdash\; \mathbf{P} \qquad \mathbf{H} \;\vdash\; \mathbf{Q}}{\mathbf{H} \;\vdash\; \mathbf{P \wedge Q}} \quad \textbf{AND\_R}$$

- Rules about implication

$$\frac{\mathbf{H, P, Q} \;\vdash\; \mathbf{R}}{\mathbf{H,\ P,\ P \Rightarrow Q} \;\vdash\; \mathbf{R}} \quad \textbf{IMP\_L}$$

$$\frac{\mathbf{H, P} \;\vdash\; \mathbf{Q}}{\mathbf{H} \;\vdash\; \mathbf{P \Rightarrow Q}} \quad \textbf{IMP\_R}$$

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

Propositional Calculus Rules of Inference (2)

- Rules about negation

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

$$\frac{H, P \ \vdash\ Q \qquad H, P \ \vdash\ \neg Q}{H \ \vdash\ \neg P}\ \textbf{NOT\_R}$$

$$\frac{H, \neg P \ \vdash\ Q \qquad H, \neg P \ \vdash\ \neg Q}{H \ \vdash\ P}\ \textbf{NOT\_R}$$

- FALSITY: $\perp$

- TRUTH: $\top$

- DISJUNCTION: $P \lor Q$

- EQUIVALENCE: $P \Leftrightarrow Q$

Definitions of the New Constructs

$$
\begin{array}{lcl}
\bot & == & P \land \neg P \\
\top & == & \neg \ \bot \\
P \lor Q & == & \neg P \Rightarrow Q \\
P \Leftrightarrow Q & == & (P \Rightarrow Q) \ \land \ (Q \Rightarrow P)
\end{array}
$$

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

- 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 $(P \Rightarrow Q) \Leftrightarrow R$

- Example:

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

More Rules

- Rules about disjunction

$$\frac{\mathbf{H}, \mathbf{P} \ \vdash \ \mathbf{R} \qquad \mathbf{H}, \mathbf{Q} \ \vdash \ \mathbf{R}}{\mathbf{H},\ \mathbf{P} \lor \mathbf{Q} \ \vdash \ \mathbf{R}} \ \textbf{OR\_L}$$

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

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

More Rules

- Rule about negation

$$\frac{}{\bot \;\vdash\; \mathbf{P}} \quad \textbf{CNTR}$$

- Transforming a disjunctive goal

$$\frac{\mathbf{H}, \neg \mathbf{P} \;\vdash\; \mathbf{Q}}{\mathbf{H} \;\vdash\; \mathbf{P} \vee \mathbf{Q}} \quad \textbf{NEG}$$

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 quick review of Set Theory

- A quick review of Arithmetic

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

- The letter $\boldsymbol{P}$, $\boldsymbol{Q}$, etc. we have used are generic variables

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

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

On Predicates and Expressions

- A Predicate is a formal text that can be proved

- An Expression is a formal text denoting an object.

- A Predicate denotes nothing.

- An Expression cannot be proved.

- Predicates and Expressions are incompatible.

- Expressions will be considerably extended in the set-theoretic and arithmetic notations.

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

where **E** is an expression

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

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

Extending the language: Existential Quantification

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

Definition of Existential Quantification

$$\exists\, x \cdot P \quad == \quad \neg\, \forall\, x \cdot \neg\, P$$

Rules of Inference for Existential Quantification

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

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

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

where **E** is an expression

Comparing the Quantification Rules

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

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

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

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

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

Refining our Language: Equality and Pairs

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

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

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

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

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

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 quick review of Set Theory

- A quick review of Arithmetic

Refining our Language: Set Theory (1)

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

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

- 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 deals with a new predicate, the membership predicate:

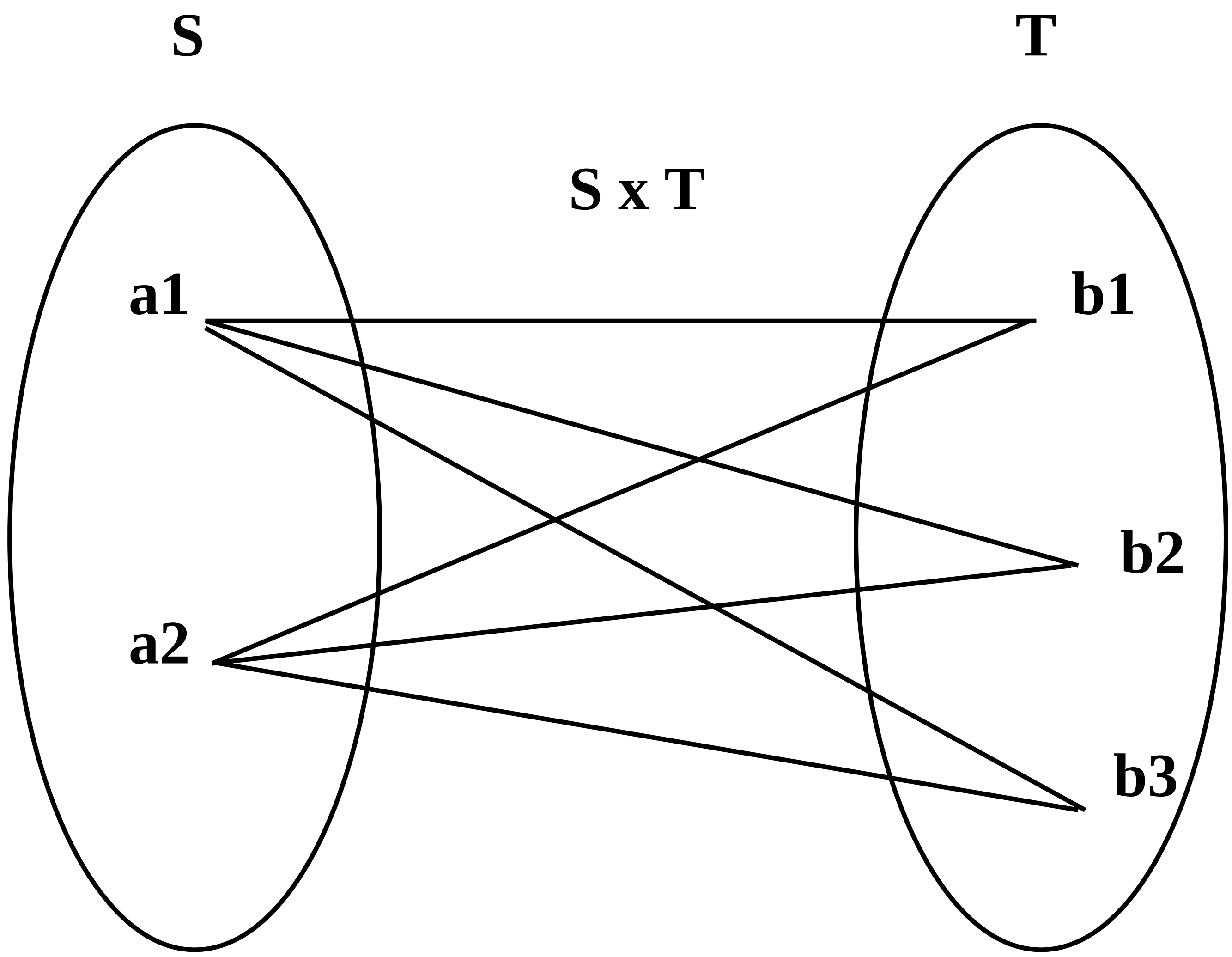
$$\boldsymbol{E} \in \boldsymbol{S}$$

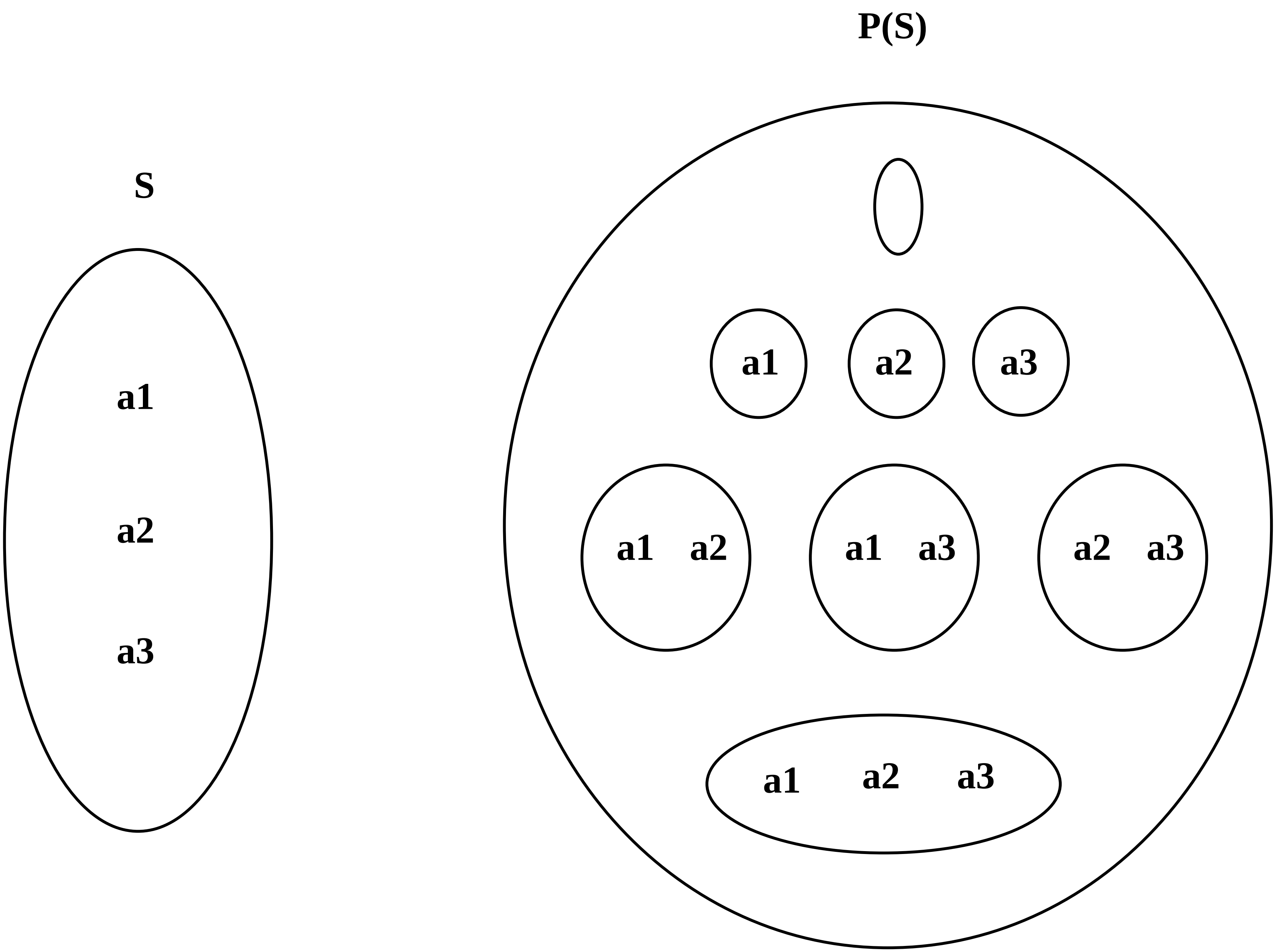
- where $\boldsymbol{E}$ is an expression and $\boldsymbol{S}$ is a set

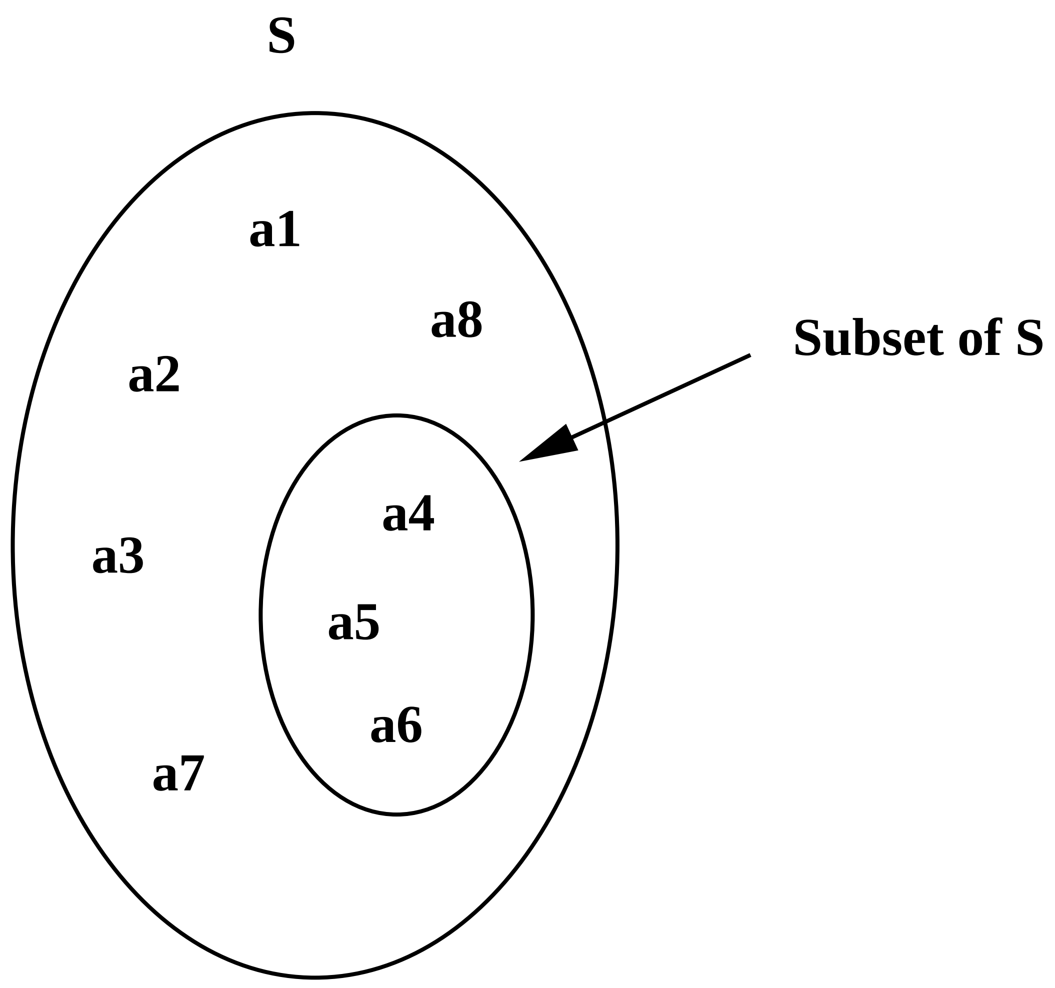
There are three basic constructs in set theory:

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

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
a2
a4
a3
a5
a6
a7
Subset of S

Basic Set Operator Memberships (Axioms)

These axioms are defined by equivalences.

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

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

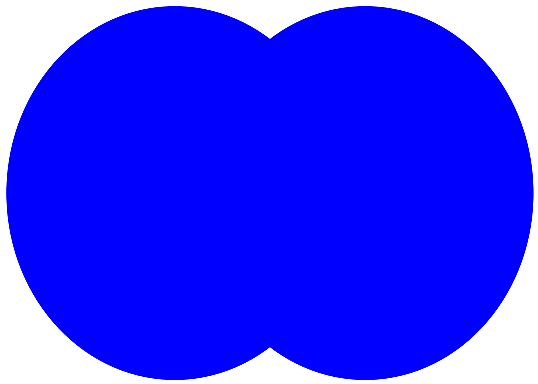
The first rule is just a syntactic extension

The second rule is the Extensionality Axiom

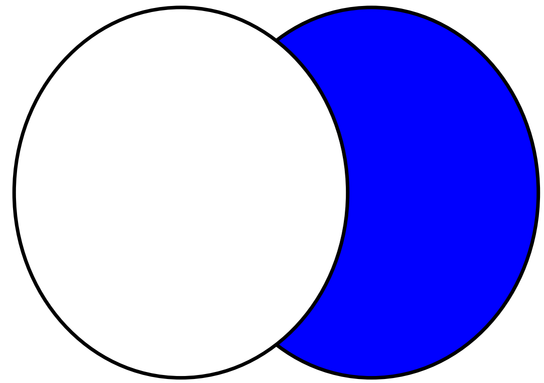
Union	$S \cup T$
Intersection	$S \cap T$
Difference	$S \setminus T$
Extension	$\{a, \ldots, b\}$
Empty set	$\varnothing$

Union, Difference, Intersection

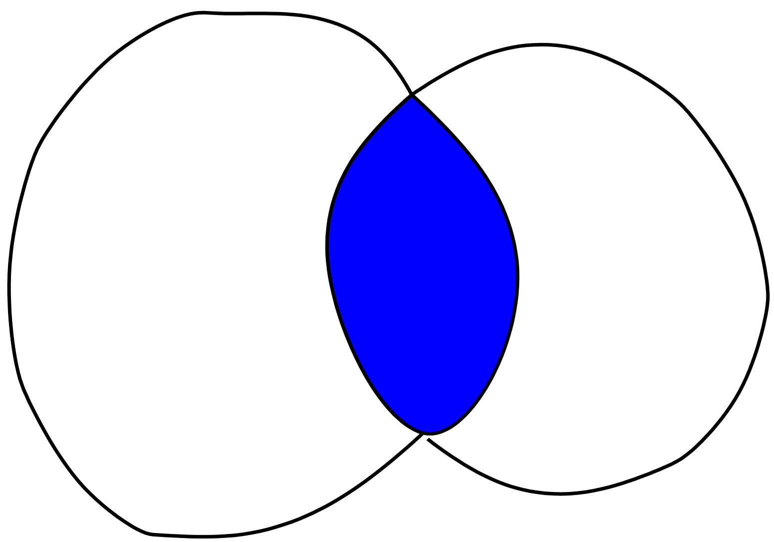
Union



Difference



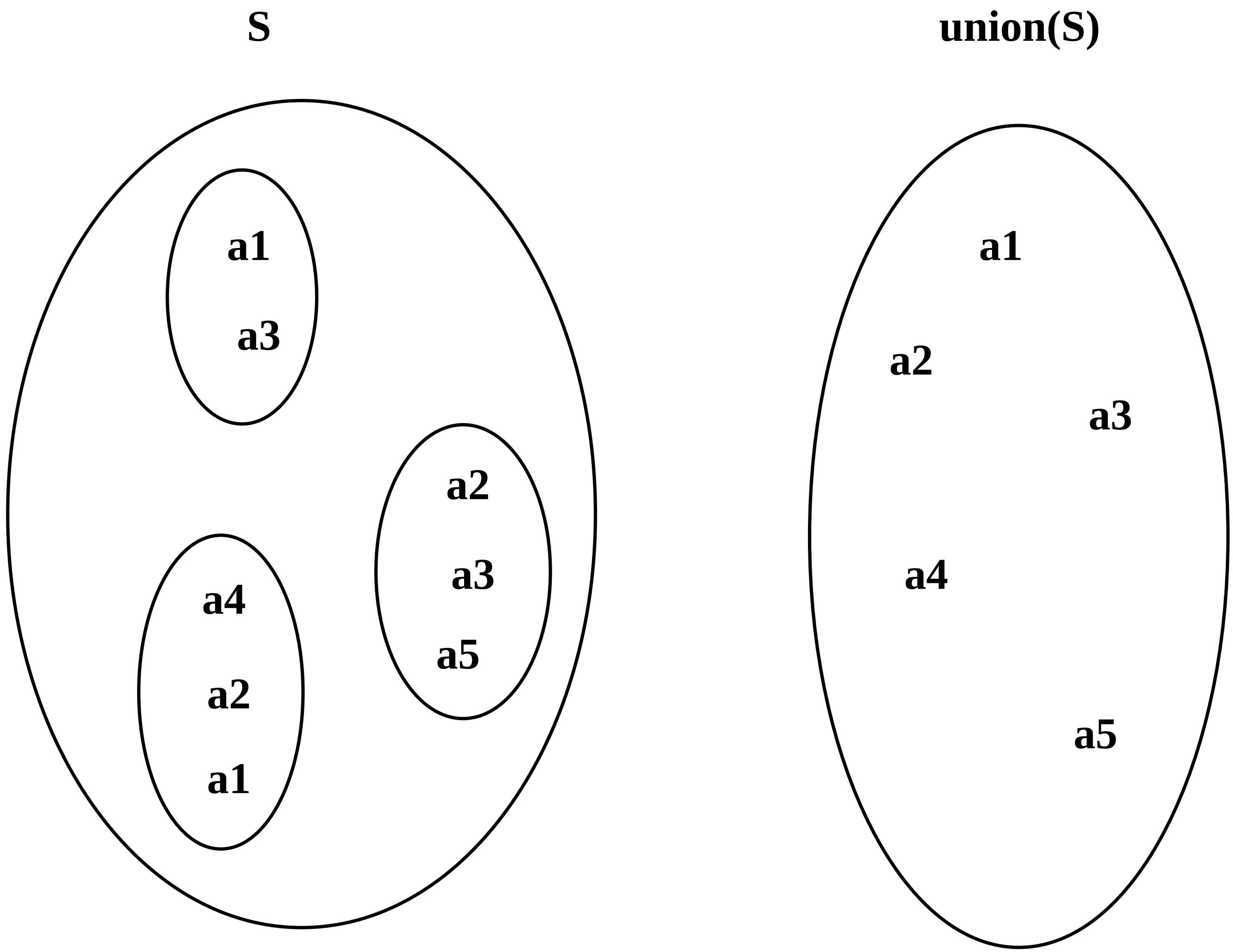
Intersection



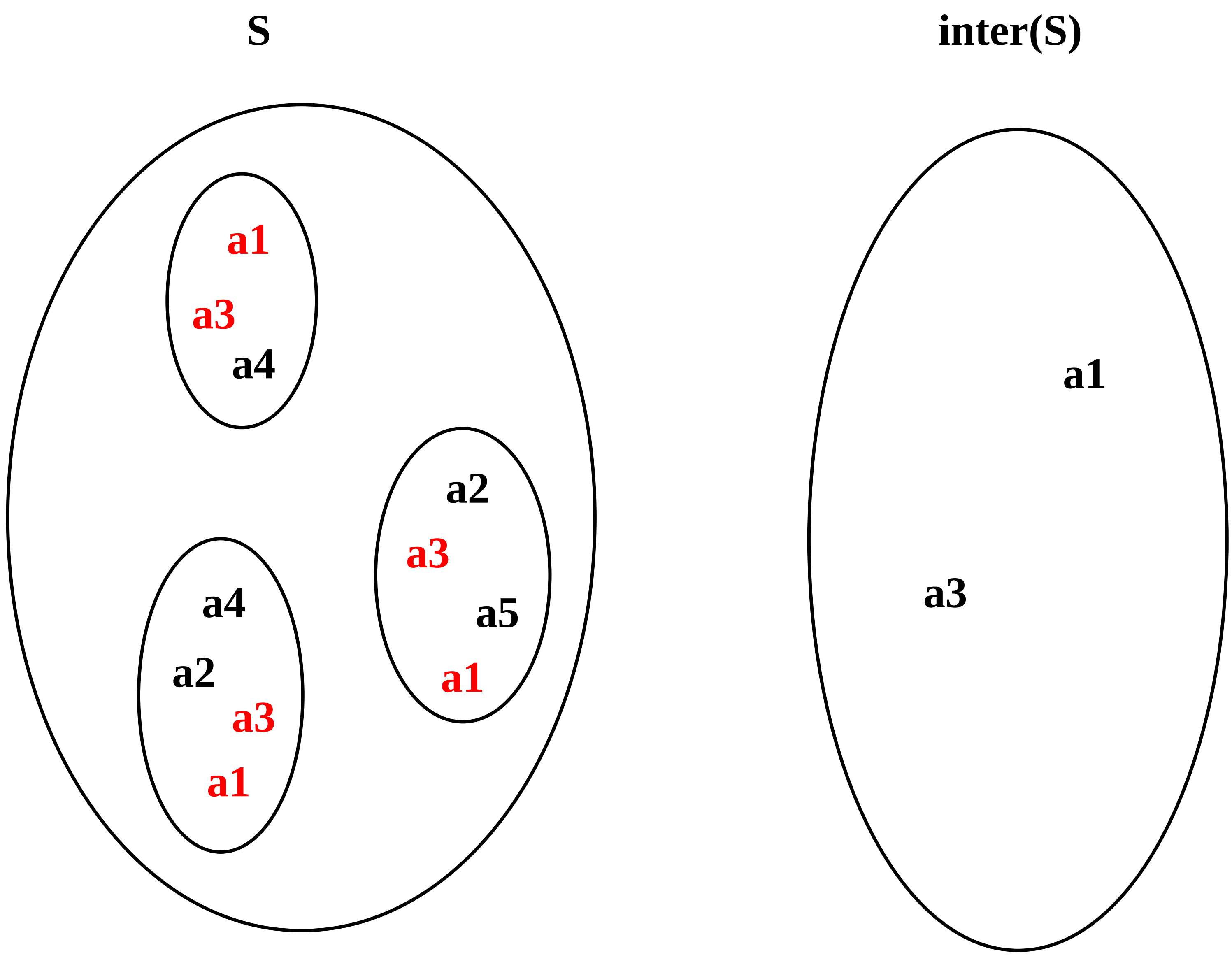
$\boldsymbol{E} \in \boldsymbol{S} \cup \boldsymbol{T}$	$\boldsymbol{E} \in \boldsymbol{S} \quad \vee \quad \boldsymbol{E} \in \boldsymbol{T}$
$\boldsymbol{E} \in \boldsymbol{S} \cap \boldsymbol{T}$	$\boldsymbol{E} \in \boldsymbol{S} \quad \wedge \quad \boldsymbol{E} \in \boldsymbol{T}$
$\boldsymbol{E}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

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

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


S
union(S)
a1
a3
a2
a3
a5
a4
a2
a1
a1
a2
a3
a4
a5

Generalized Intersection



$E \;\in\;$ union (S)	$\exists s \cdot s \in S \;\wedge\; E \in s$
$E \;\in\; \bigcup\, x \cdot x \in S \;\wedge\; P(x) \mid T(x)$	$\exists x \cdot x \in S \;\wedge\; P(x) \;\wedge\; E \in T(x)$
$E \;\in\;$ inter (S)	$\forall s \cdot s \in S \;\Rightarrow\; E \in s$
$E \;\in\; \bigcap\, x \cdot x \in S \;\wedge\; P(x) \mid T(x)$	$\forall x \cdot x \in S \;\wedge\; P(x) \;\Rightarrow\; E \in T(x)$

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

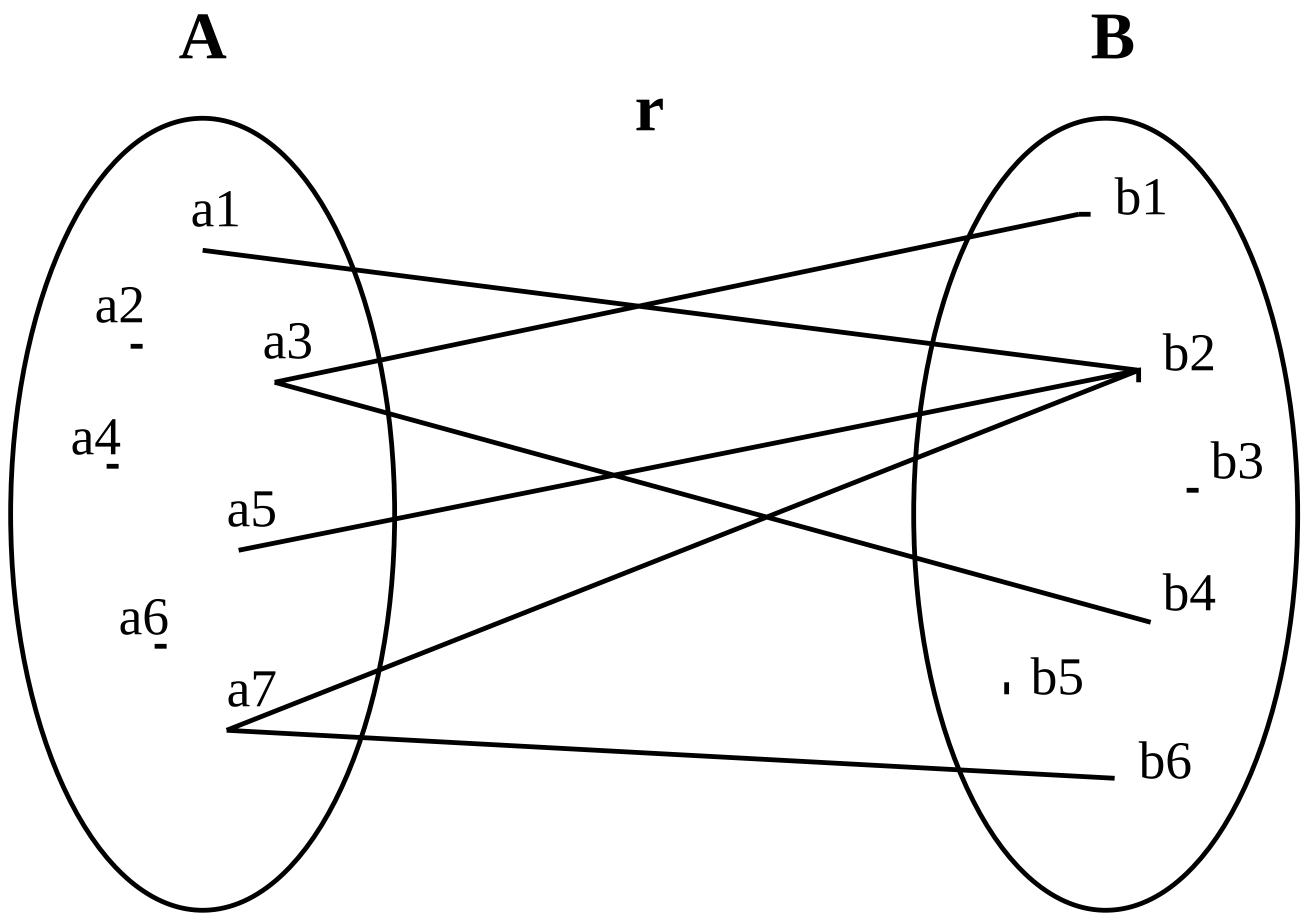
Well-definedness condition for case 4: $\exists\, x \cdot x \in S \;\wedge P(x)$

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

Binary Relation Operators (1)

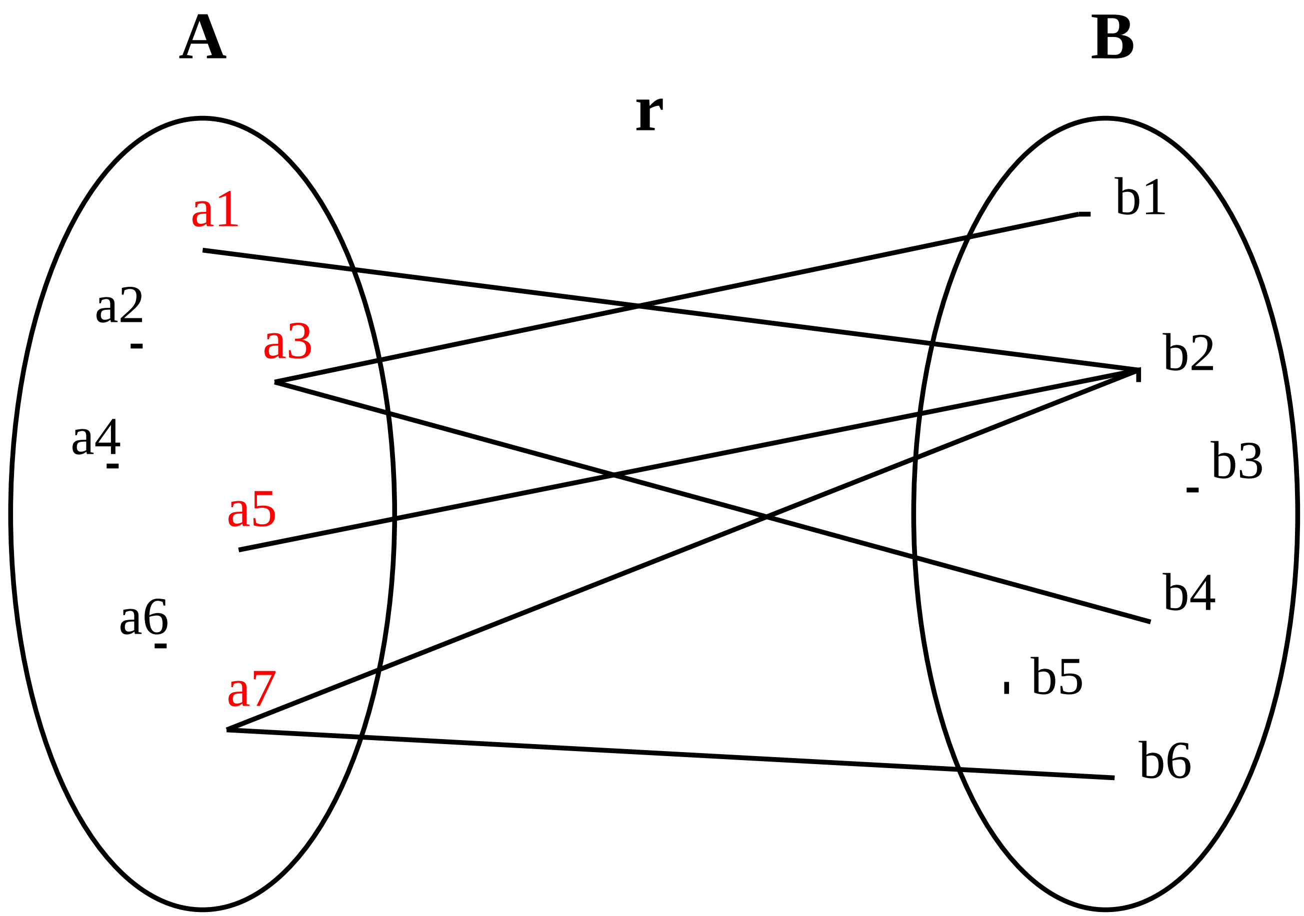
Binary relations	$S \leftrightarrow T$
Domain	$\mathrm{dom}\,(r)$
Range	$\mathrm{ran}\,(r)$
Converse	r^{-1}

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



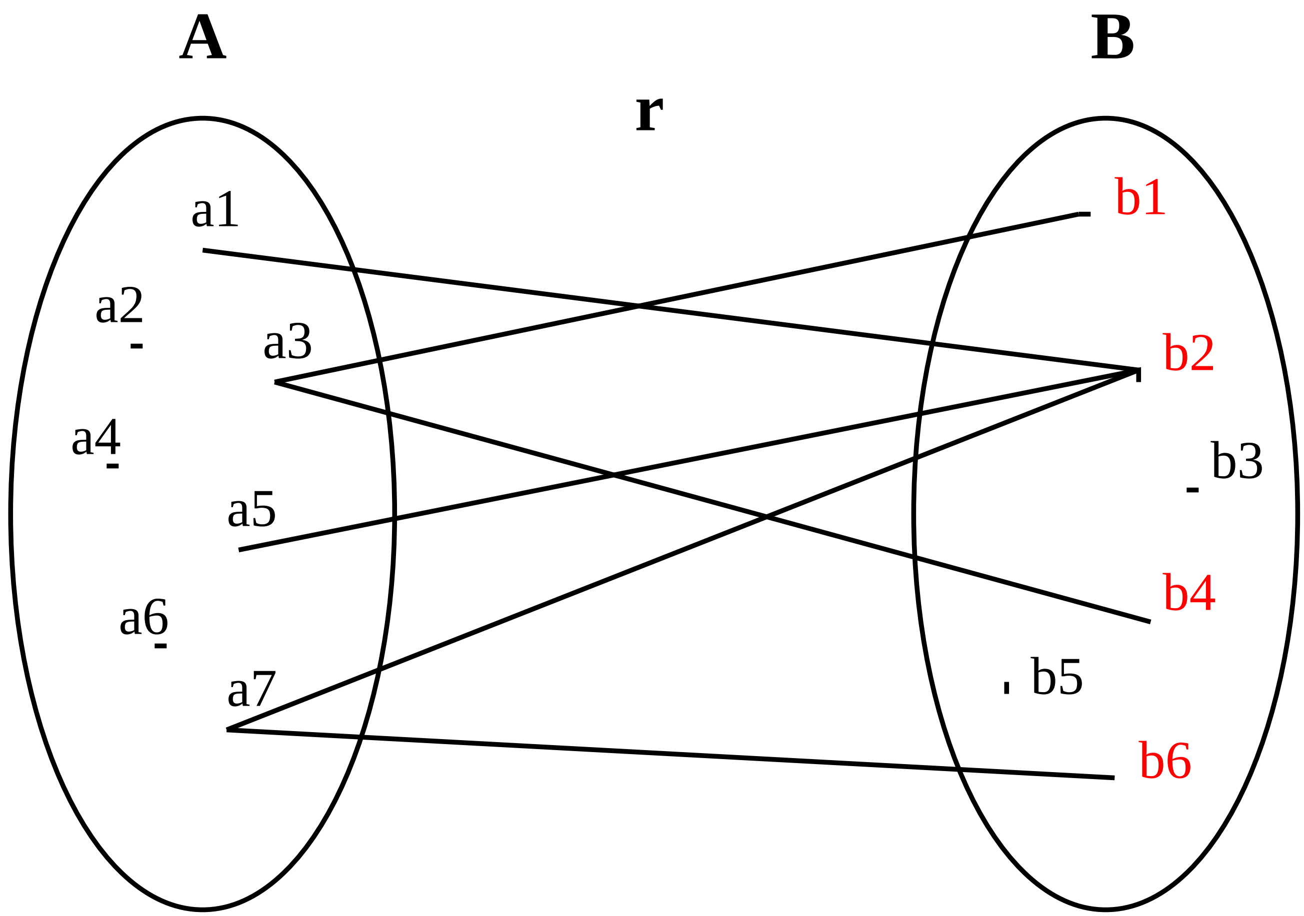
$$r \in A \leftrightarrow B$$

Domain of Binary Relation r



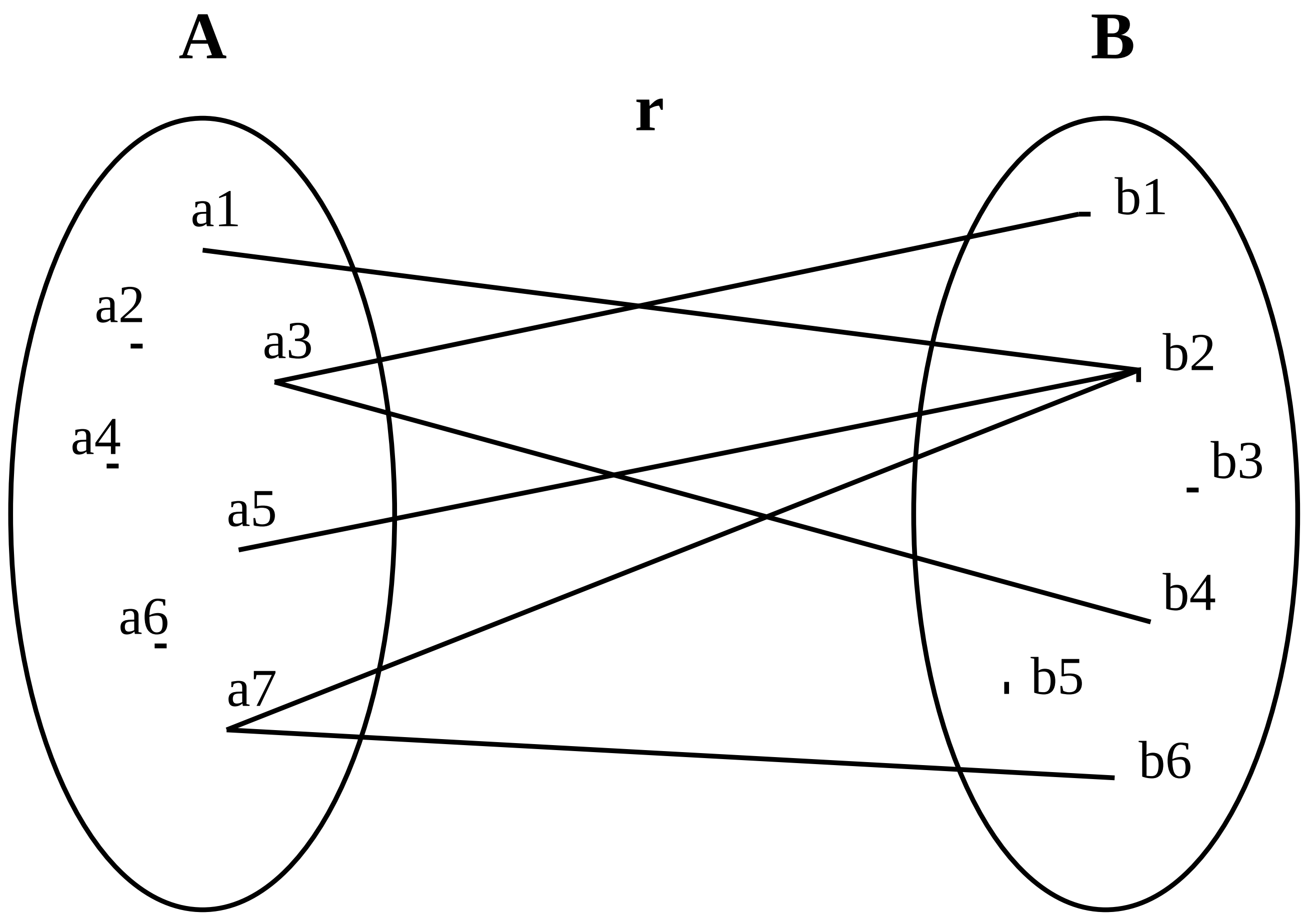
$$\mathsf{dom}(r) = \{a1, a3, a5, a7\}$$

Range of Binary Relation r



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

Converse of Binary Relation r



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

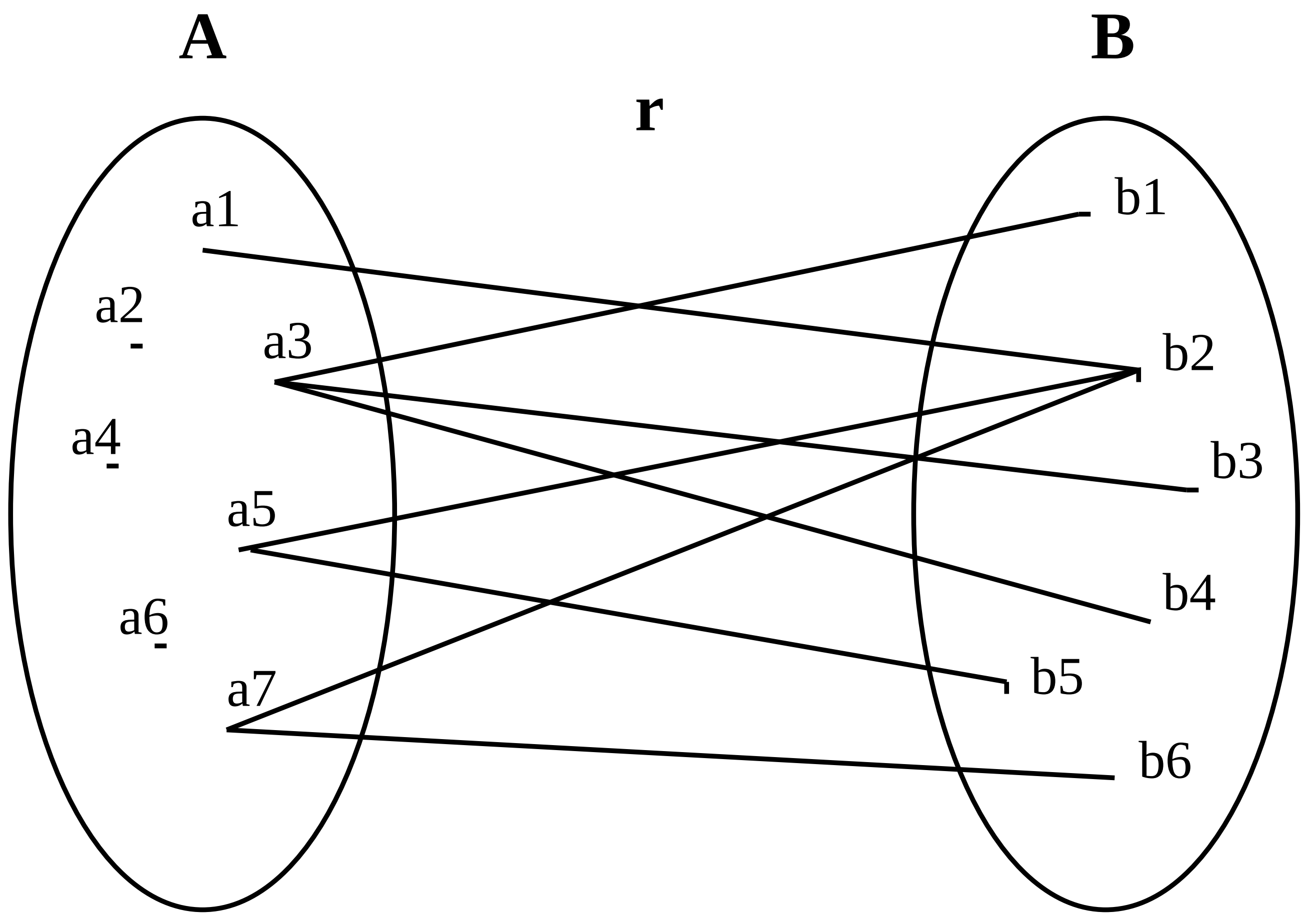
Binary Relation Operator Memberships (1)

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

Binary Relation Operators (2)

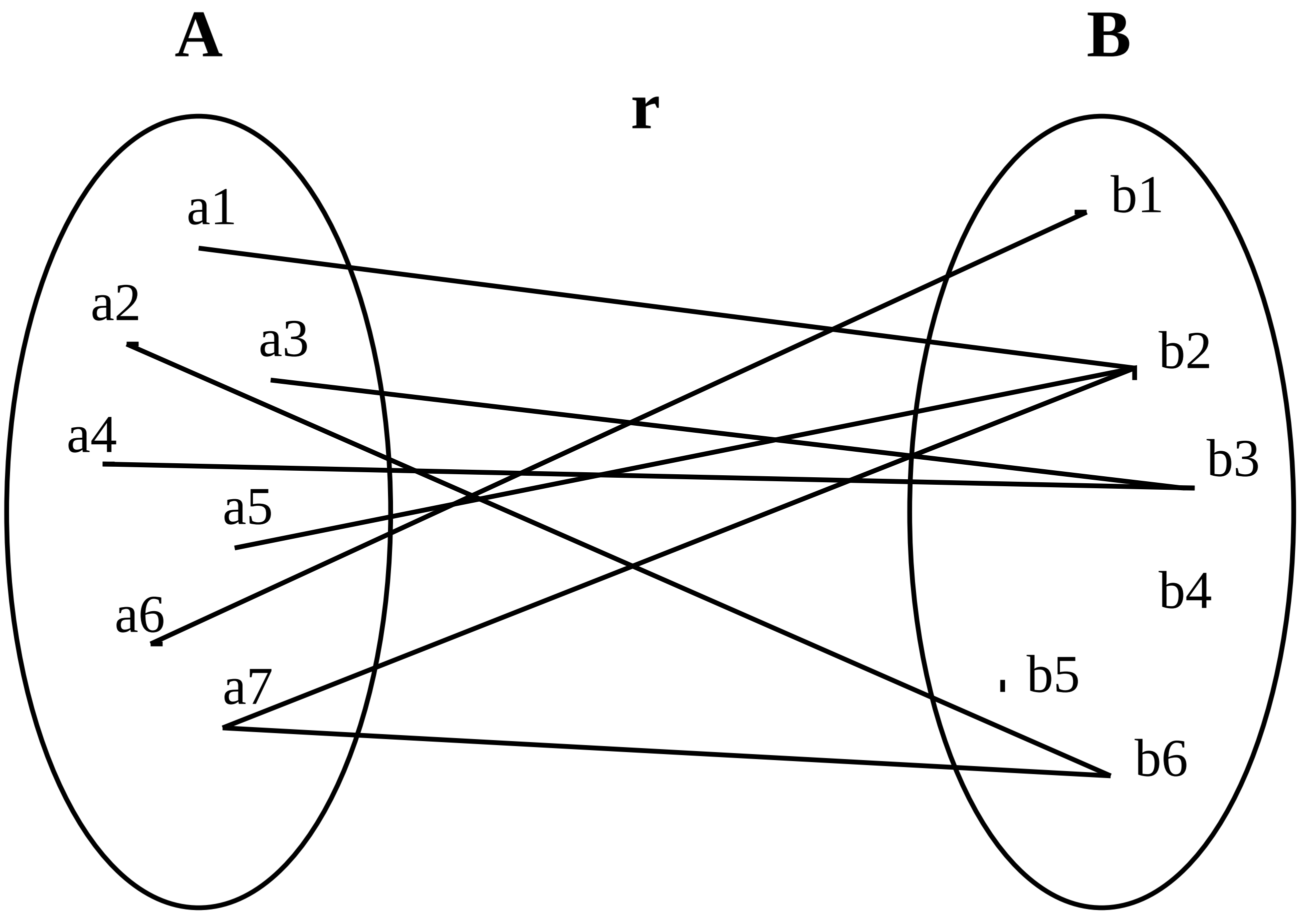
Partial surjective binary relations	$S \mathrel{\leftarrow\!\!\!\twoheadrightarrow} T$
Total binary relations	$S \mathrel{\twoheadleftarrow\!\!\!\rightarrow} T$
Total surjective binary relations	$S \mathrel{\twoheadleftarrow\!\!\!\twoheadrightarrow} T$

A Partial Surjective Relation



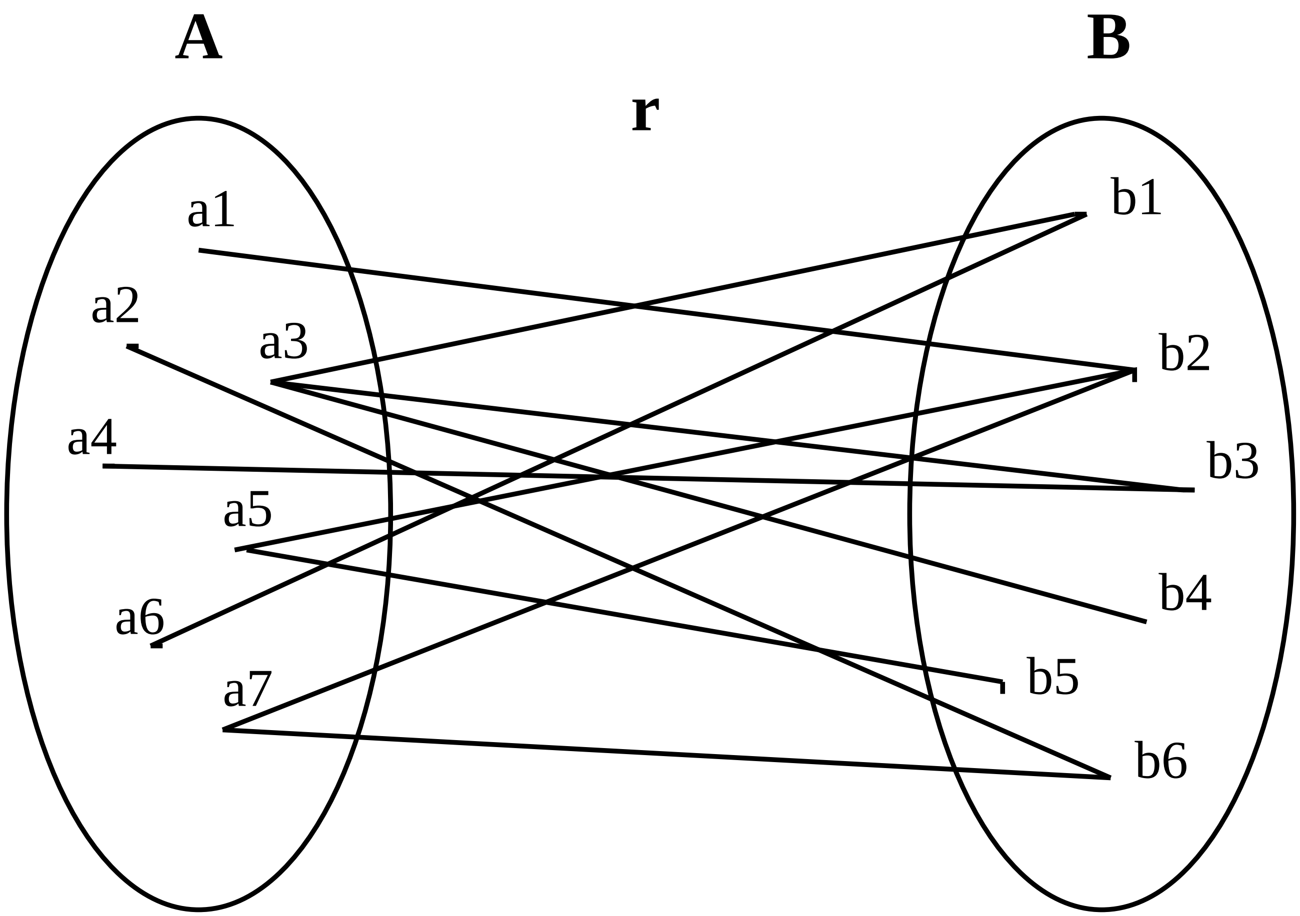
$$r \in A \leftrightarrow\!\!\!\!\rightarrow B$$

A Total Relation



$$r \in A \leftrightarrow B$$

A Total Surjective Relation



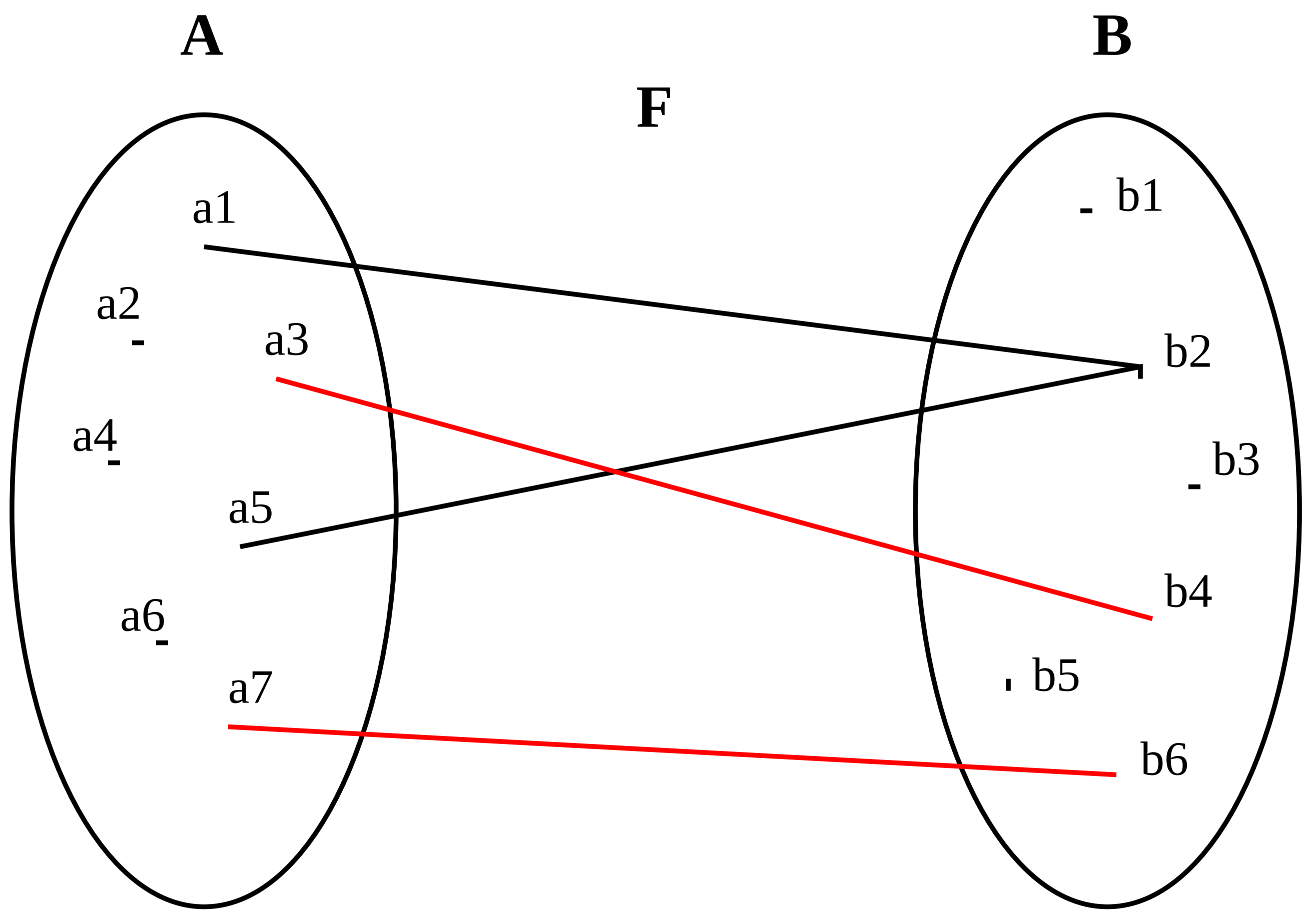
$$r \in A \leftrightarrow\!\!\!\!\twoheadrightarrow B$$

Binary Relation Operator Memberships (2)

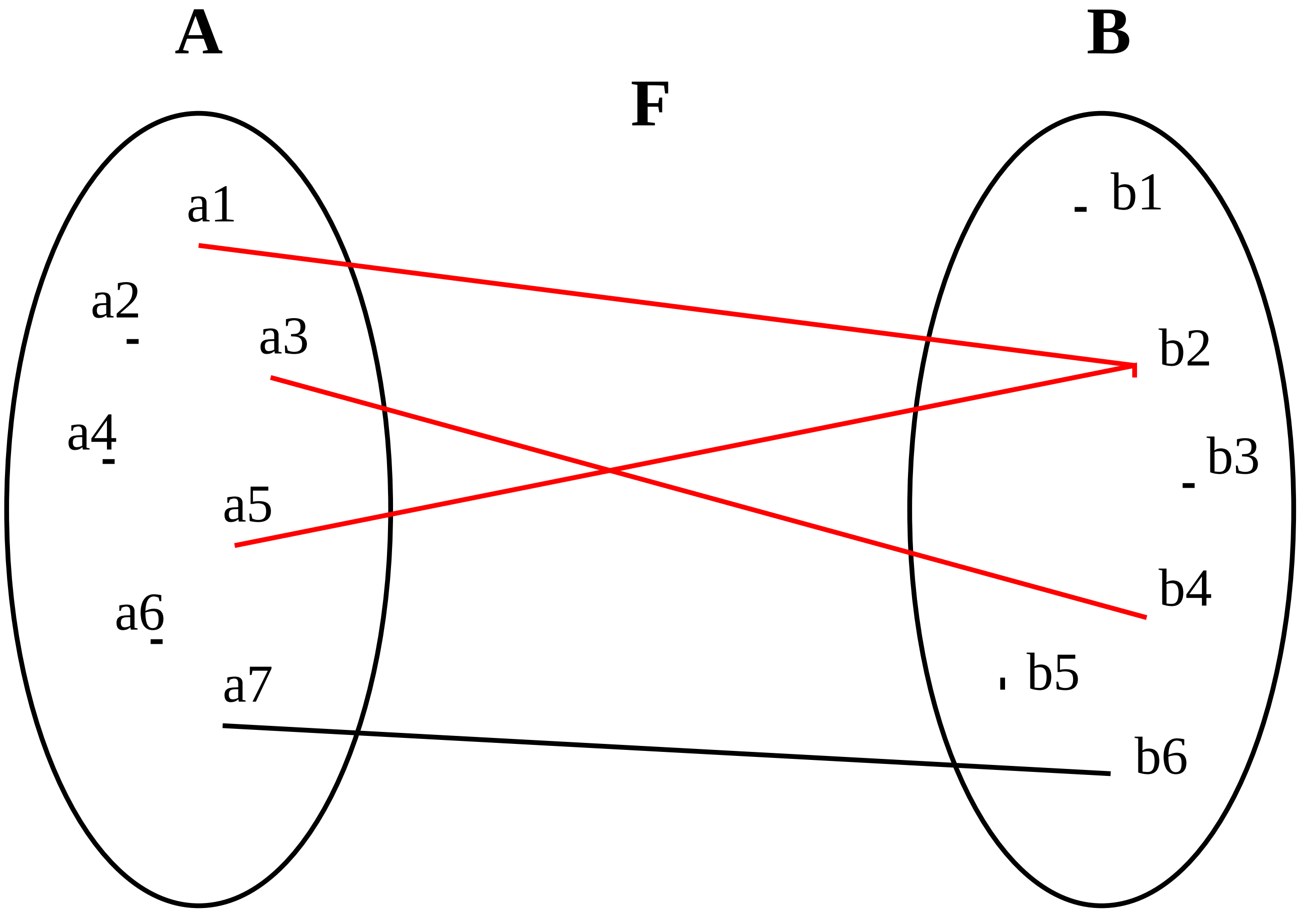
Left Part	Right Part
$r \in S \mathrel{\leftarrow\!\!\!\twoheadrightarrow} T$	$r \in S \leftrightarrow T \ \wedge\ \mathsf{ran}(r) = T$
$r \in S \mathrel{\twoheadleftarrow\!\!\!\rightarrow} T$	$r \in S \leftrightarrow T \ \wedge\ \mathsf{dom}(r) = T$
$r \in S \mathrel{\twoheadleftarrow\!\!\!\twoheadrightarrow}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

Binary Relation Operators (3)

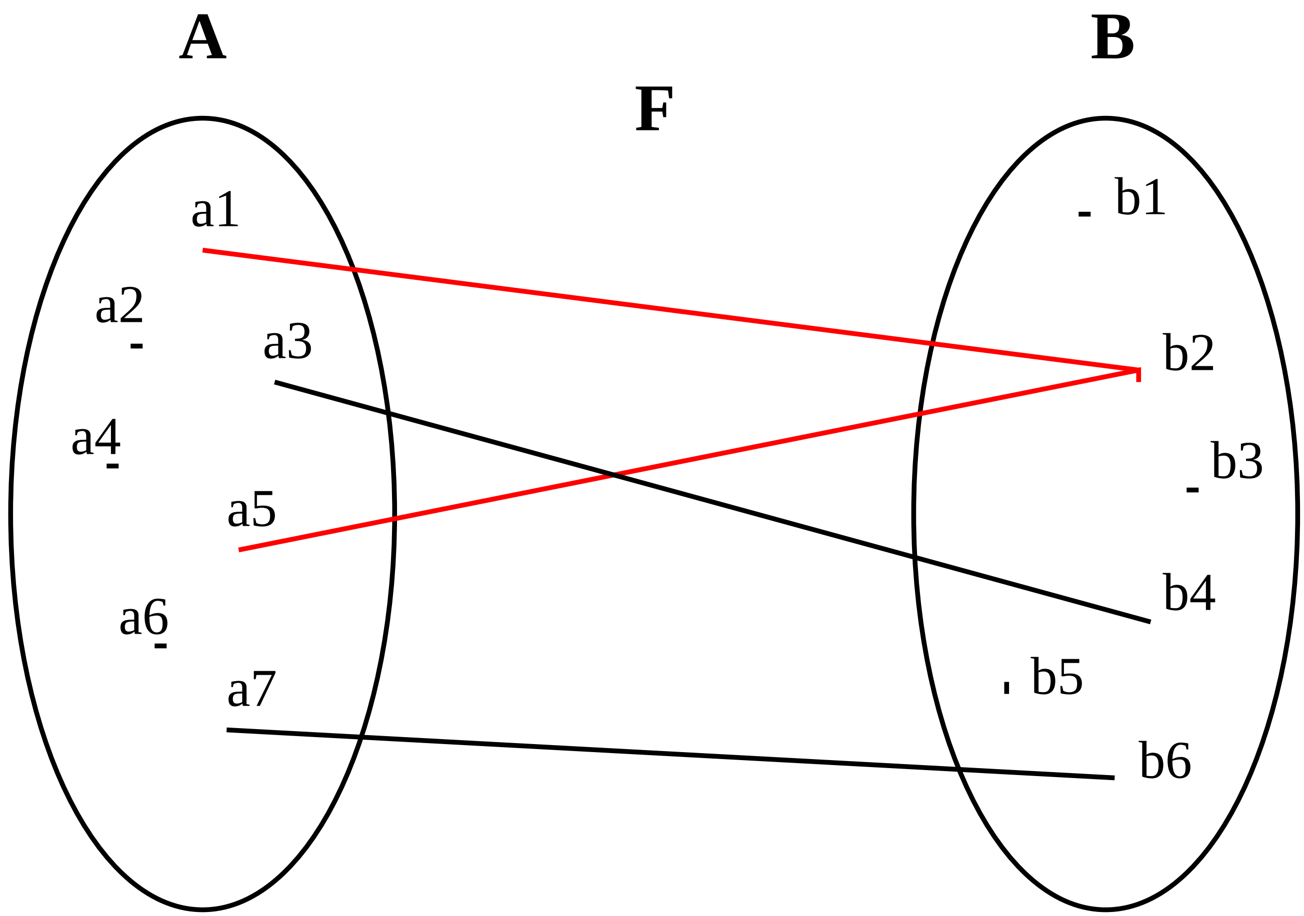
Domain restriction	$S \lhd r$
Range restriction	$r \rhd T$
Domain subtraction	$S \mathbin{\ooalign{$\lhd$\cr$-$}} r$
Range subtraction	$r \mathbin{\ooalign{$\rhd$\cr$-$}} T$



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

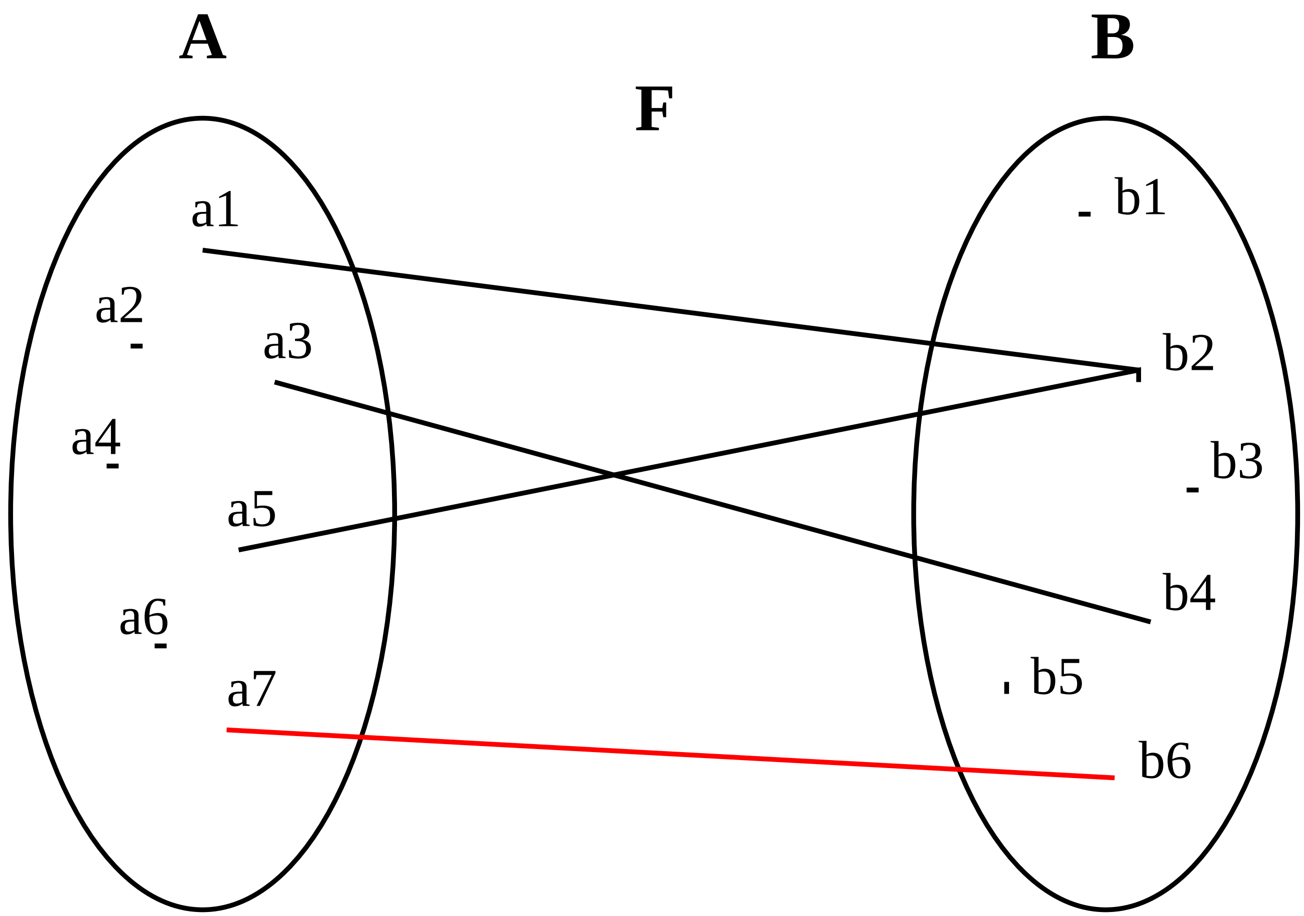


$$F \rhd \{b2, b4\}$$



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

The Range Restriction Operator



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

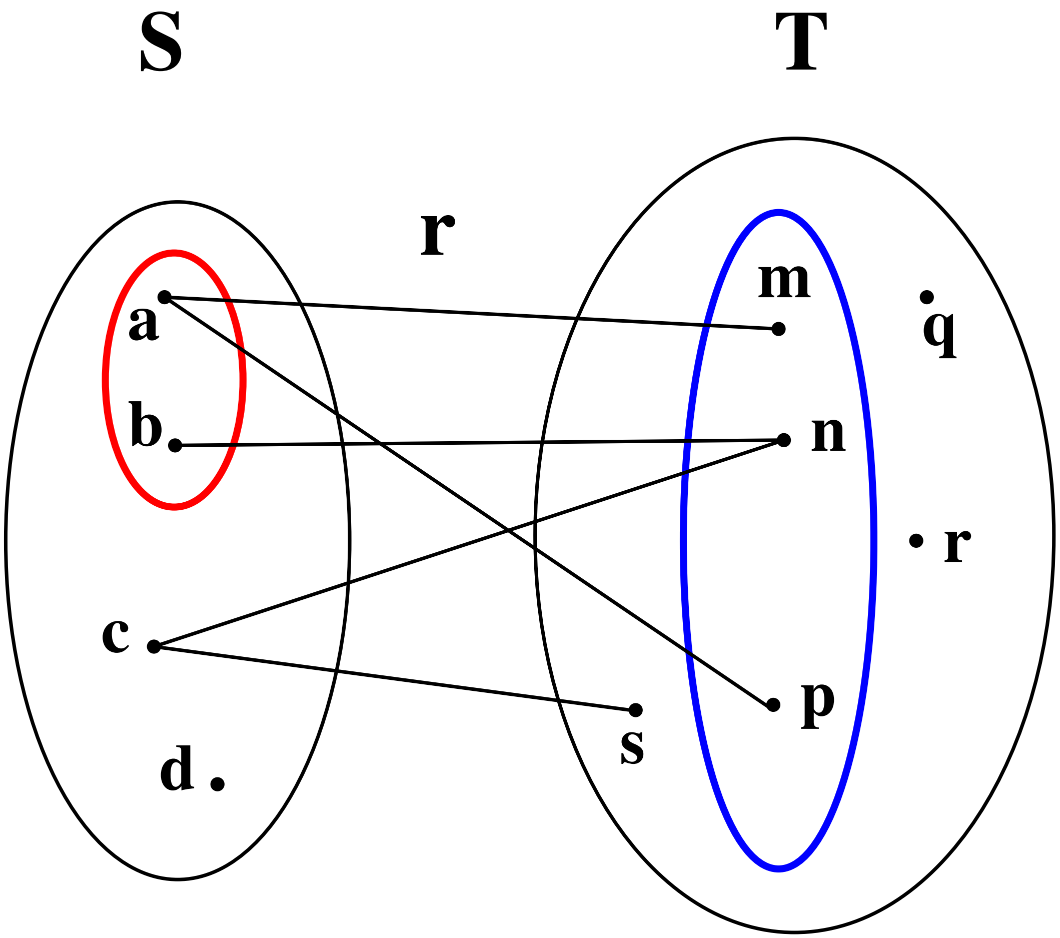
Binary Relation Operator Memberships (3)

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

Binary Relation Operators (4)

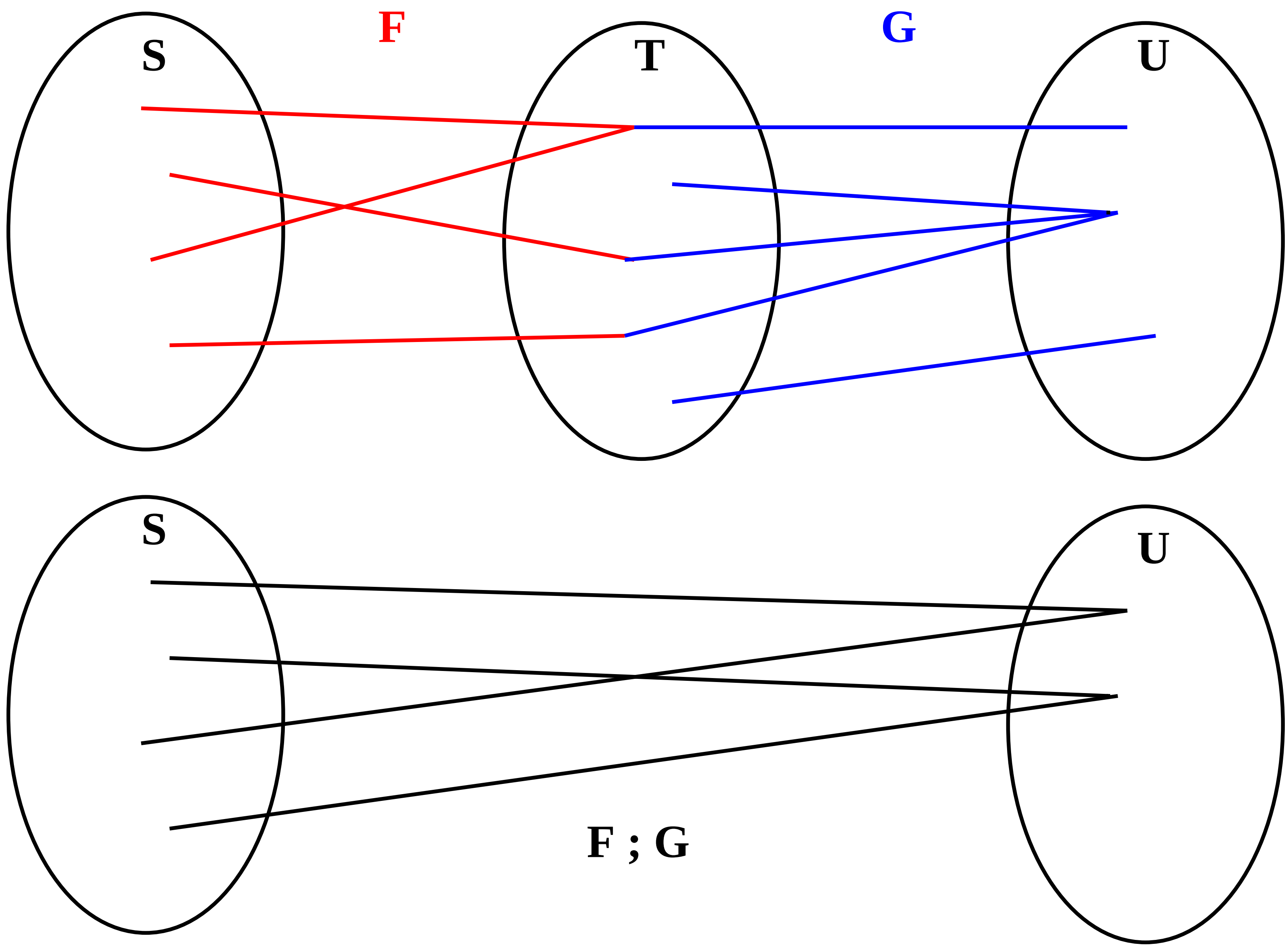
Image	$r[w]$
Composition	$p \,;\, q$
Overriding	$p \mathbin{\triangleleft\!\!\!+} q$
Identity	$\mathrm{id}\,(S)$

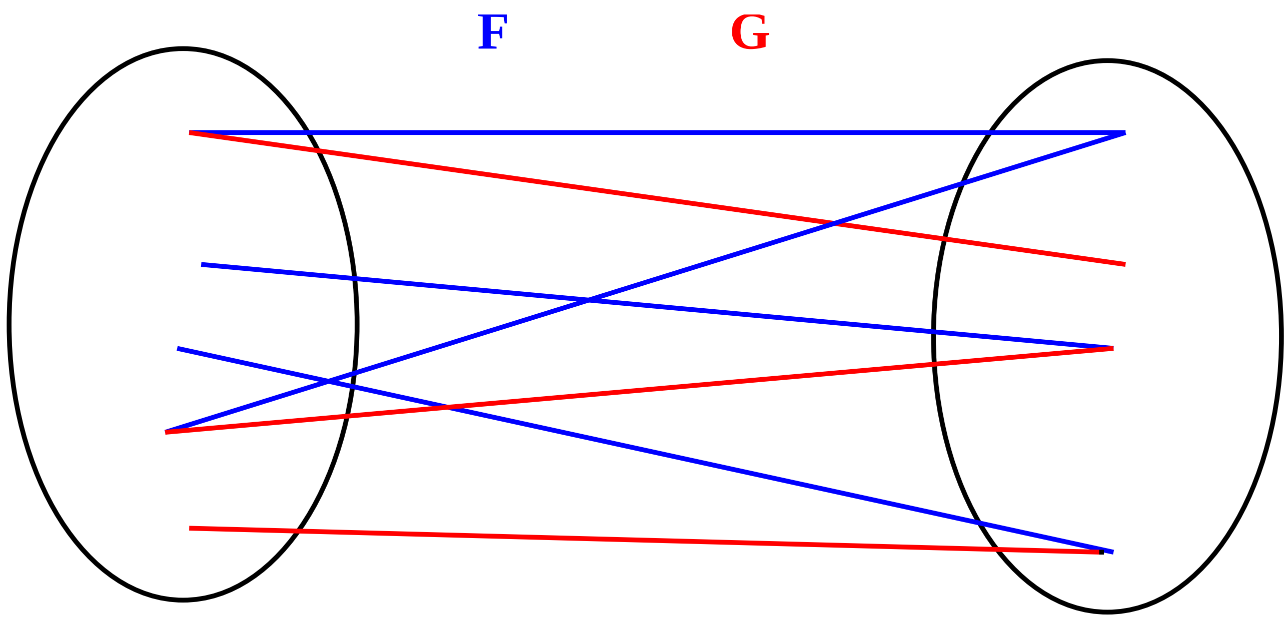
Image of $\{a, b\}$ under r



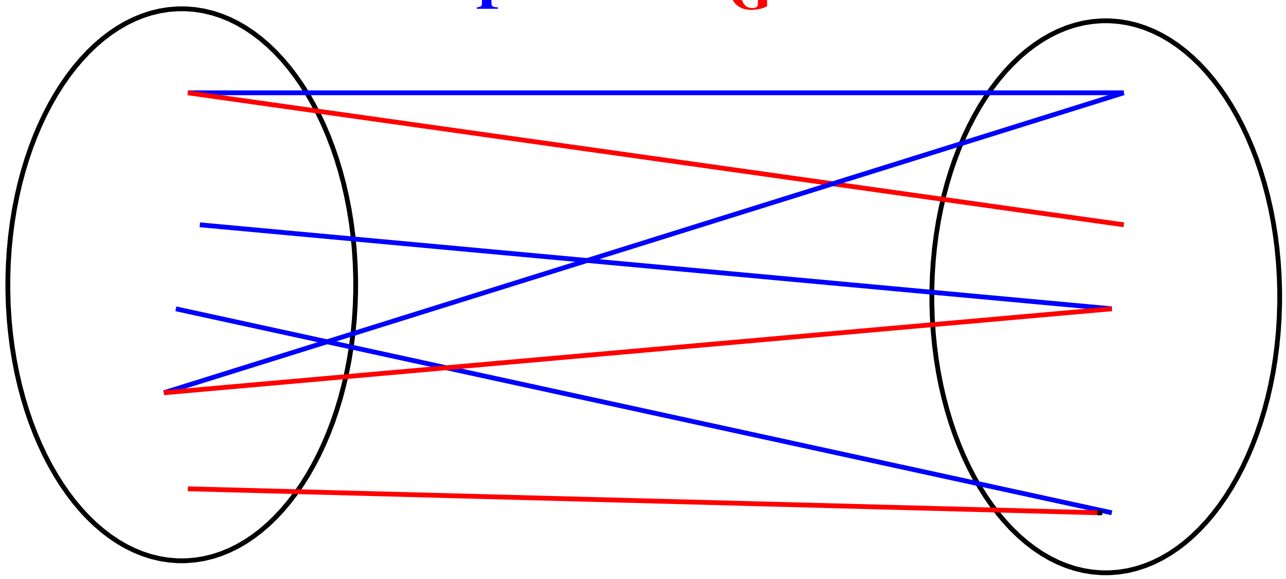
$$r[\{a,b\}] = \{m,n,p\}$$

Forward Composition

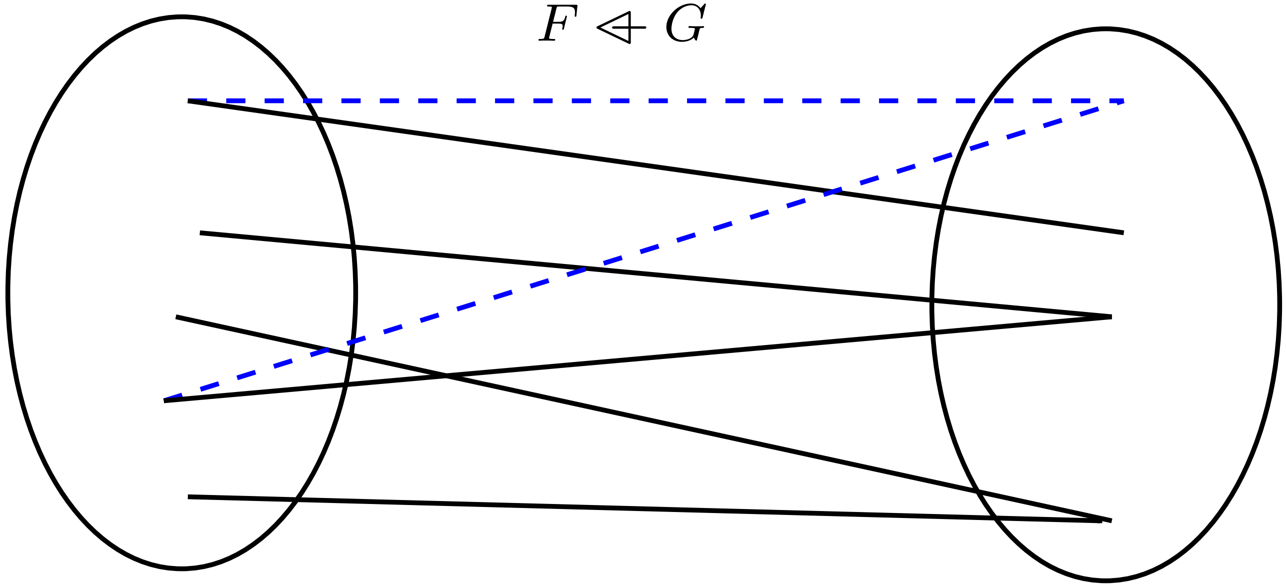



F
G

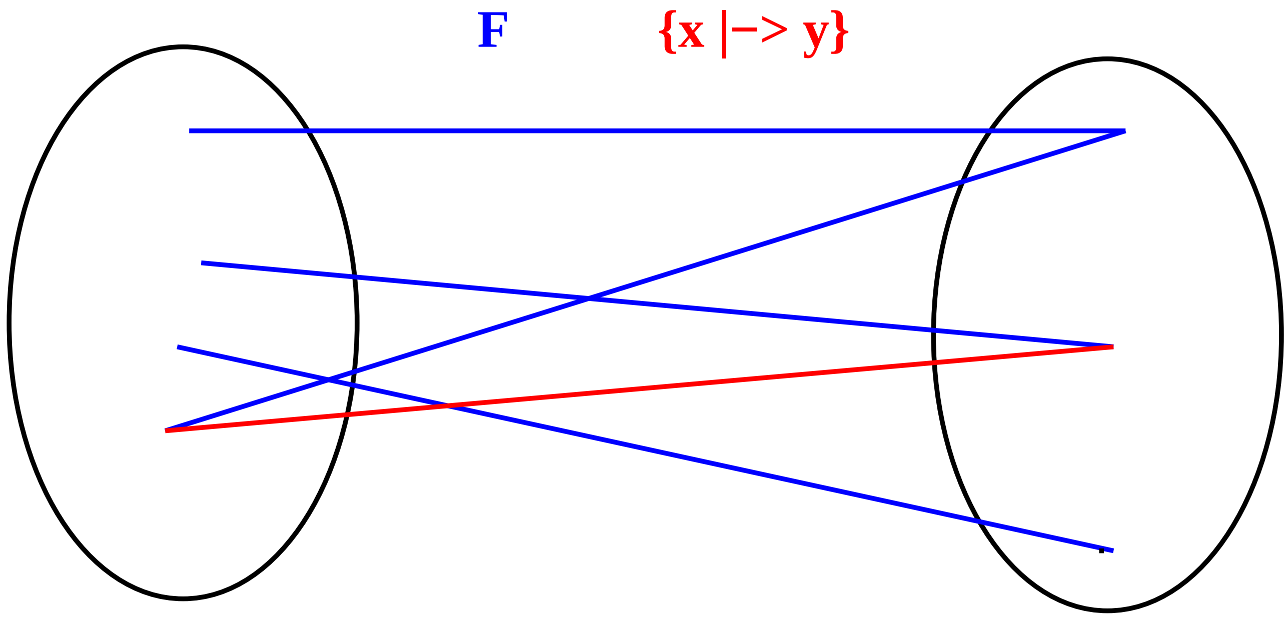
F **G**



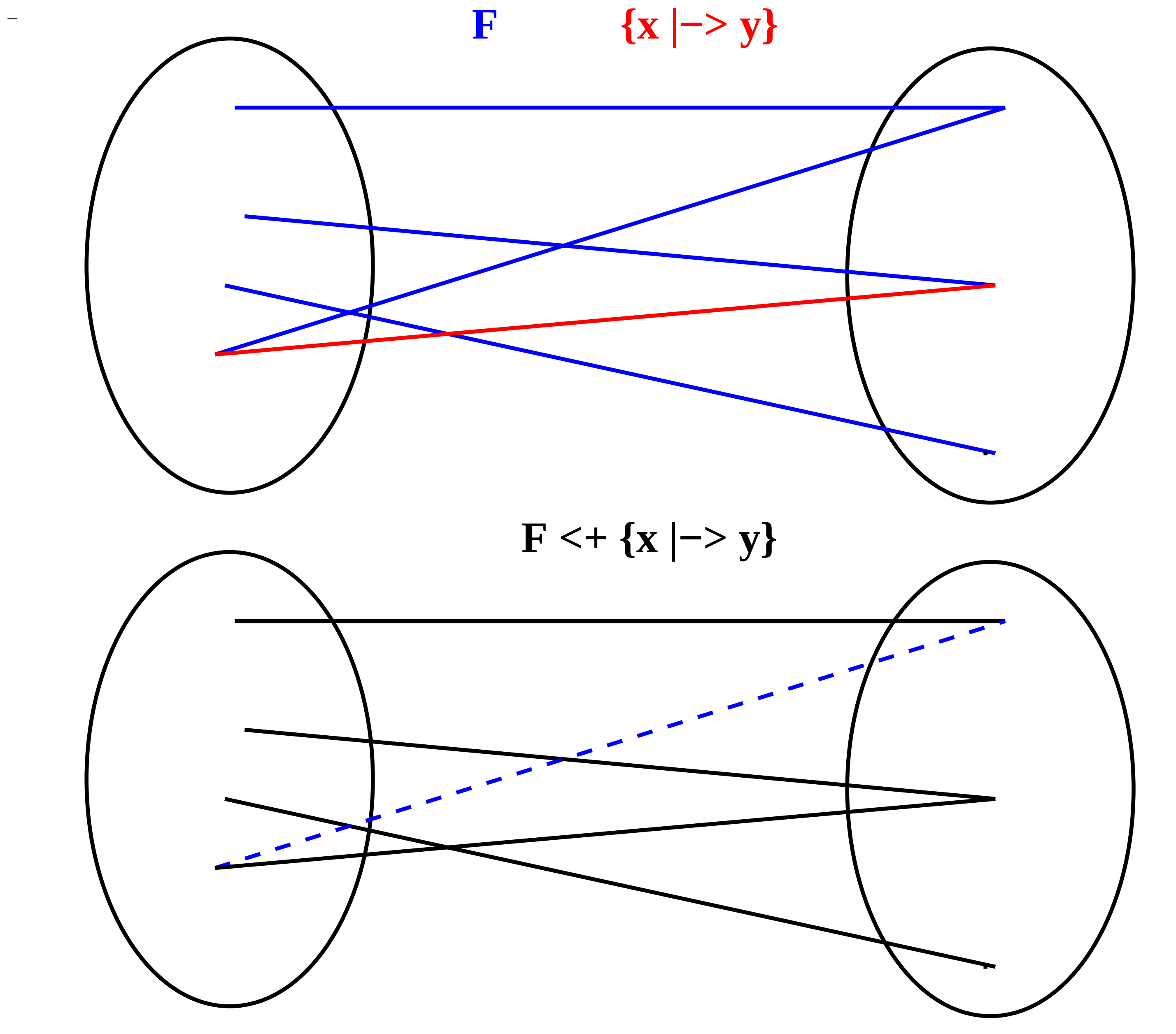
$F \mathbin{\lhd\!\!-} G$

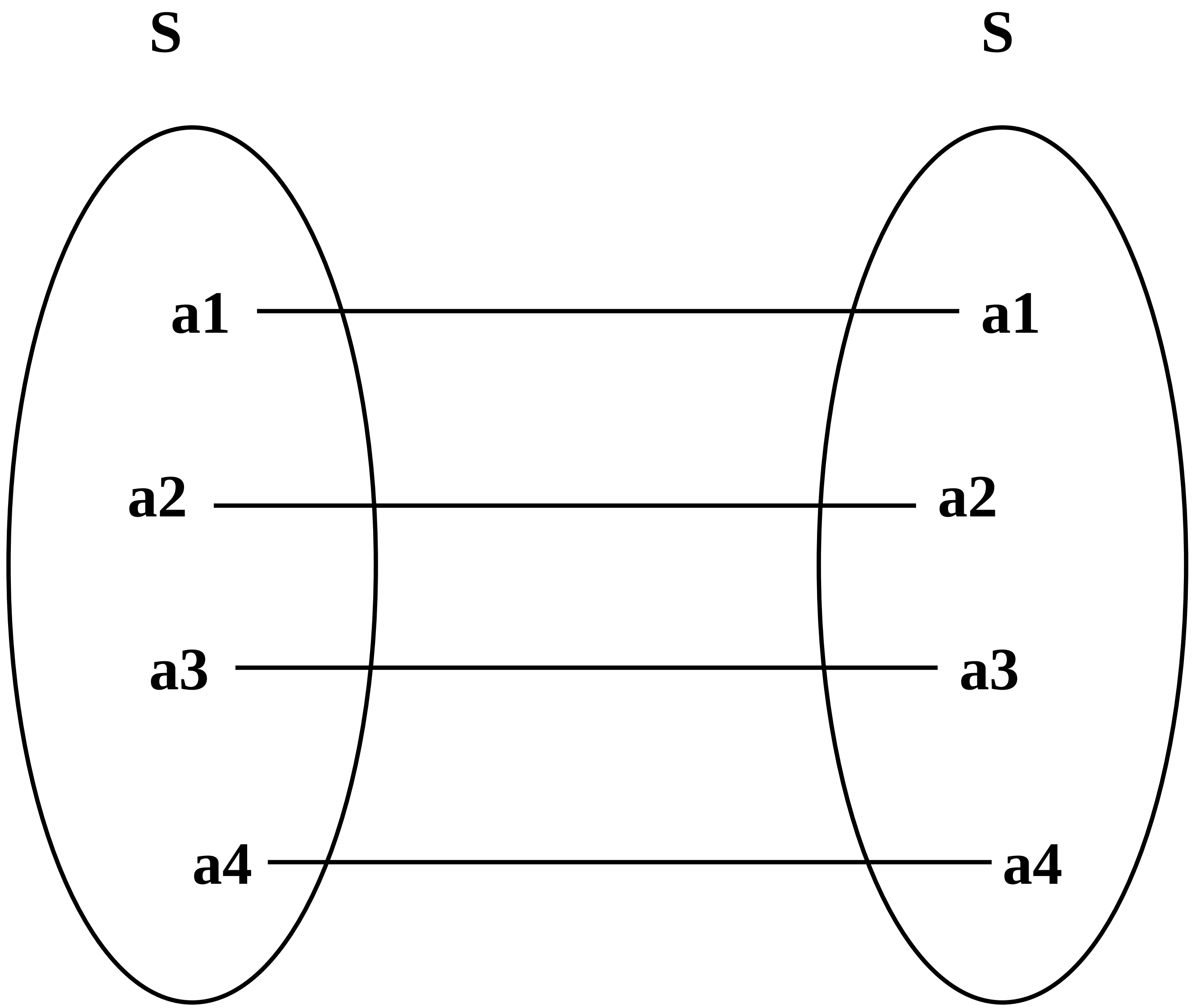


Special Case



Special Case




S
S
a1
a1
a2
a2
a3
a3
a4
a4

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

Binary Relation Operators (5)

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

Binary Relation Operator Memberships (5)

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

Summary of Binary Relation Operators

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

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

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

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

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

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

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

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

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

$$\ldots$$

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
$r \cap r^{-1} \subseteq \mathrm{id}(S)$	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

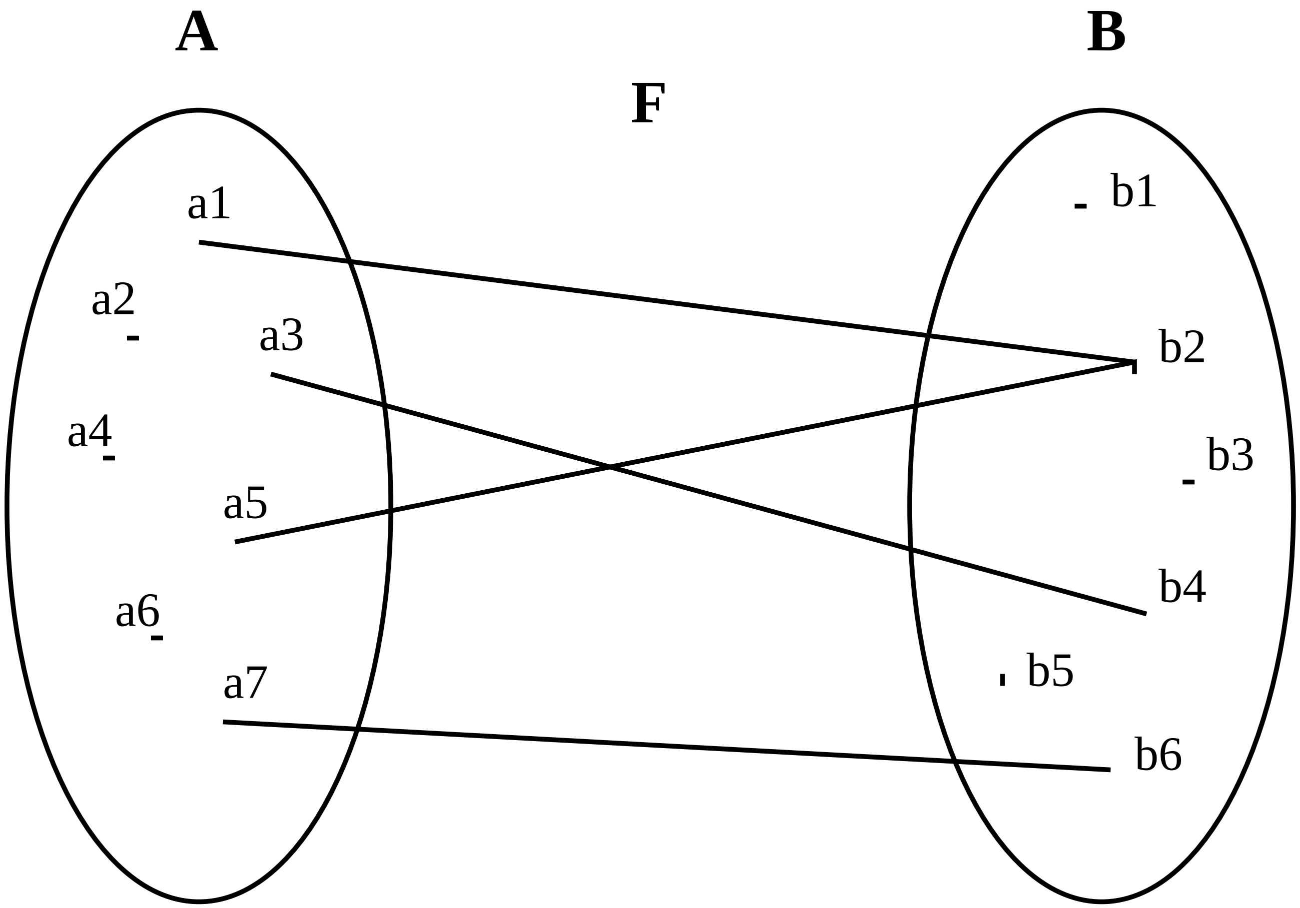
Given a relation r such that $r \in S \leftrightarrow S$

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

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

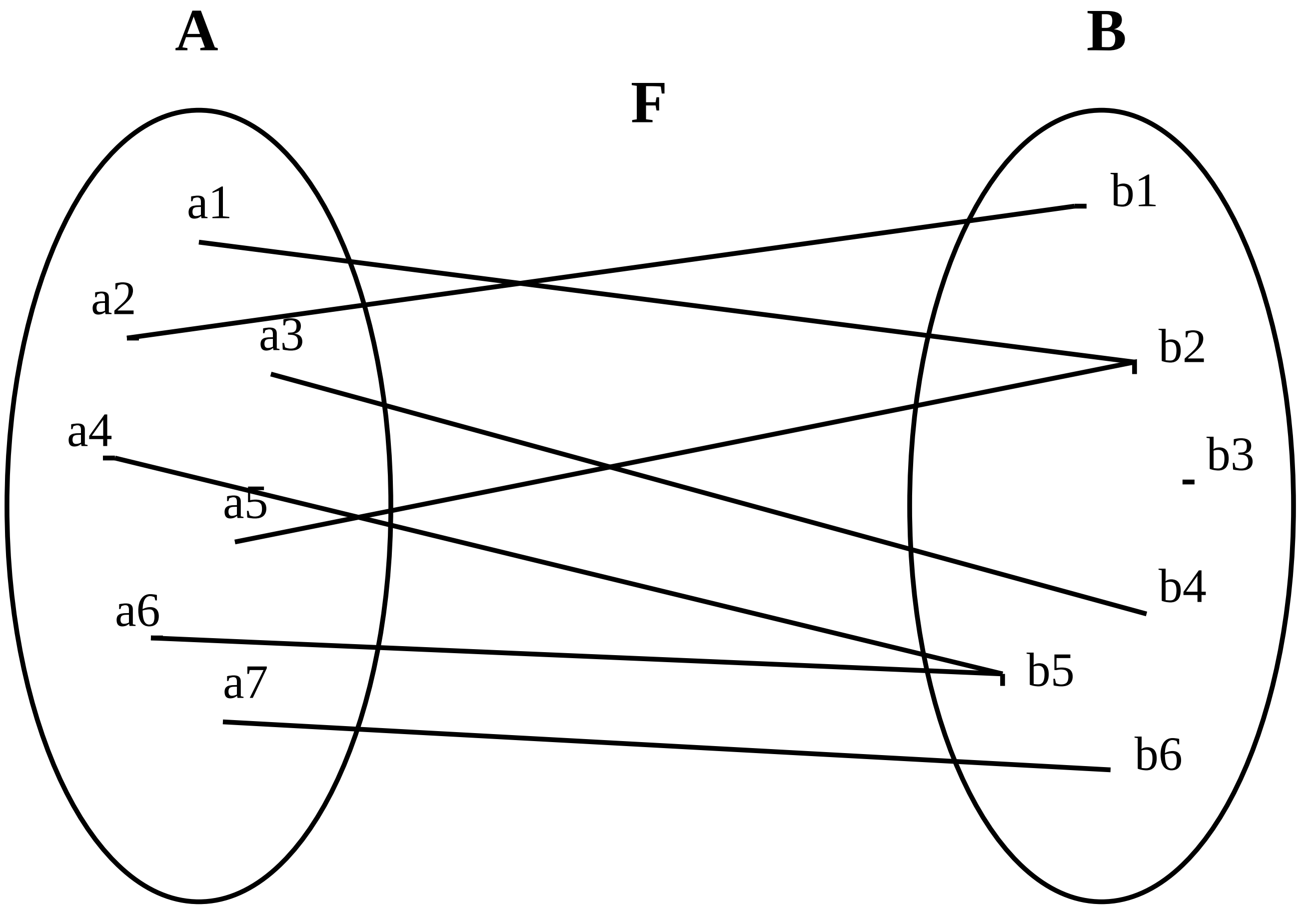
Partial functions	$S \nrightarrow T$
Total functions	$S \longrightarrow T$
Partial injections	$S \rightarrowtail\!\!\!\!+ \, T$
Total injections	$S \rightarrowtail T$

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



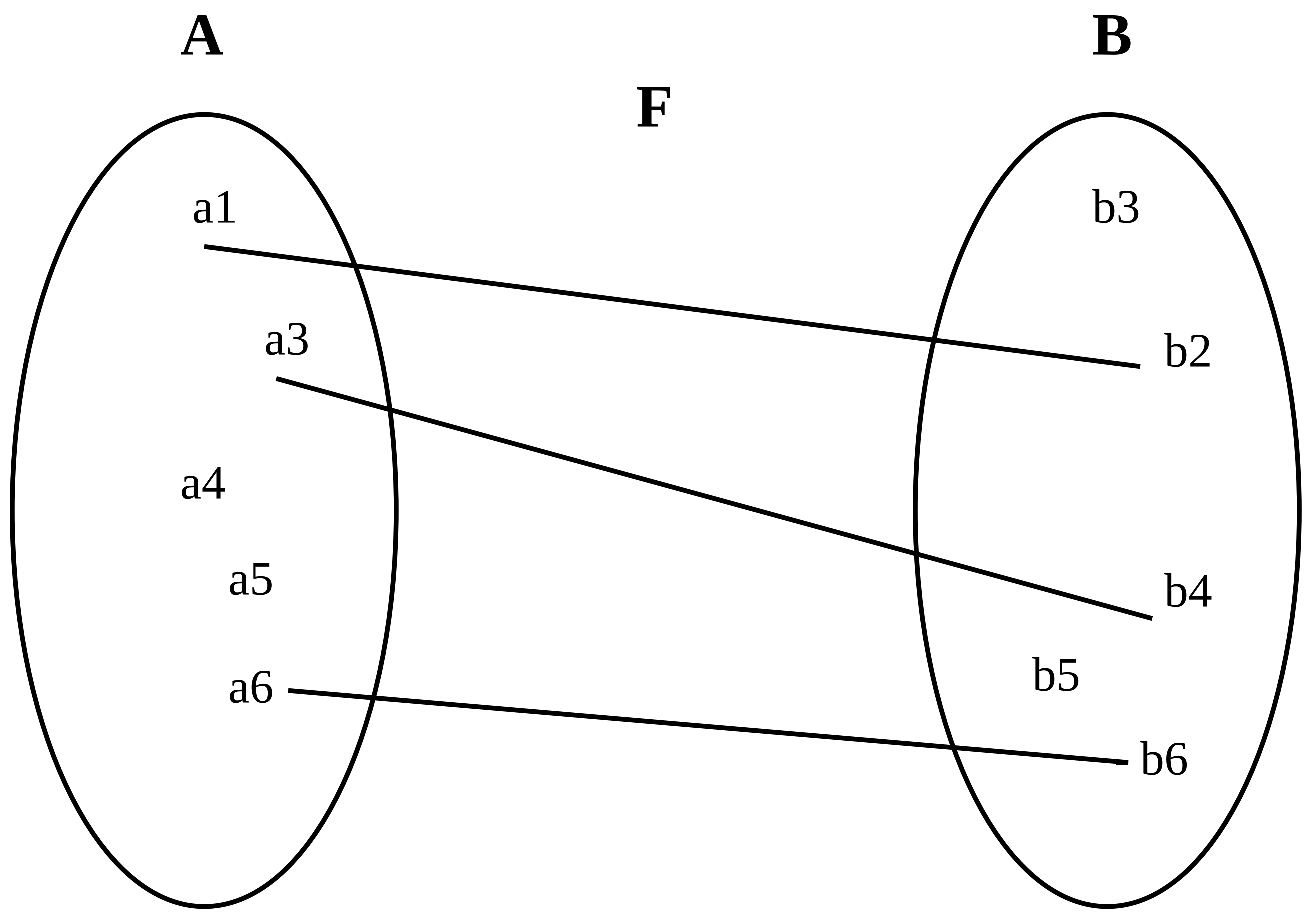
$$F \in A \mapsto B$$

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



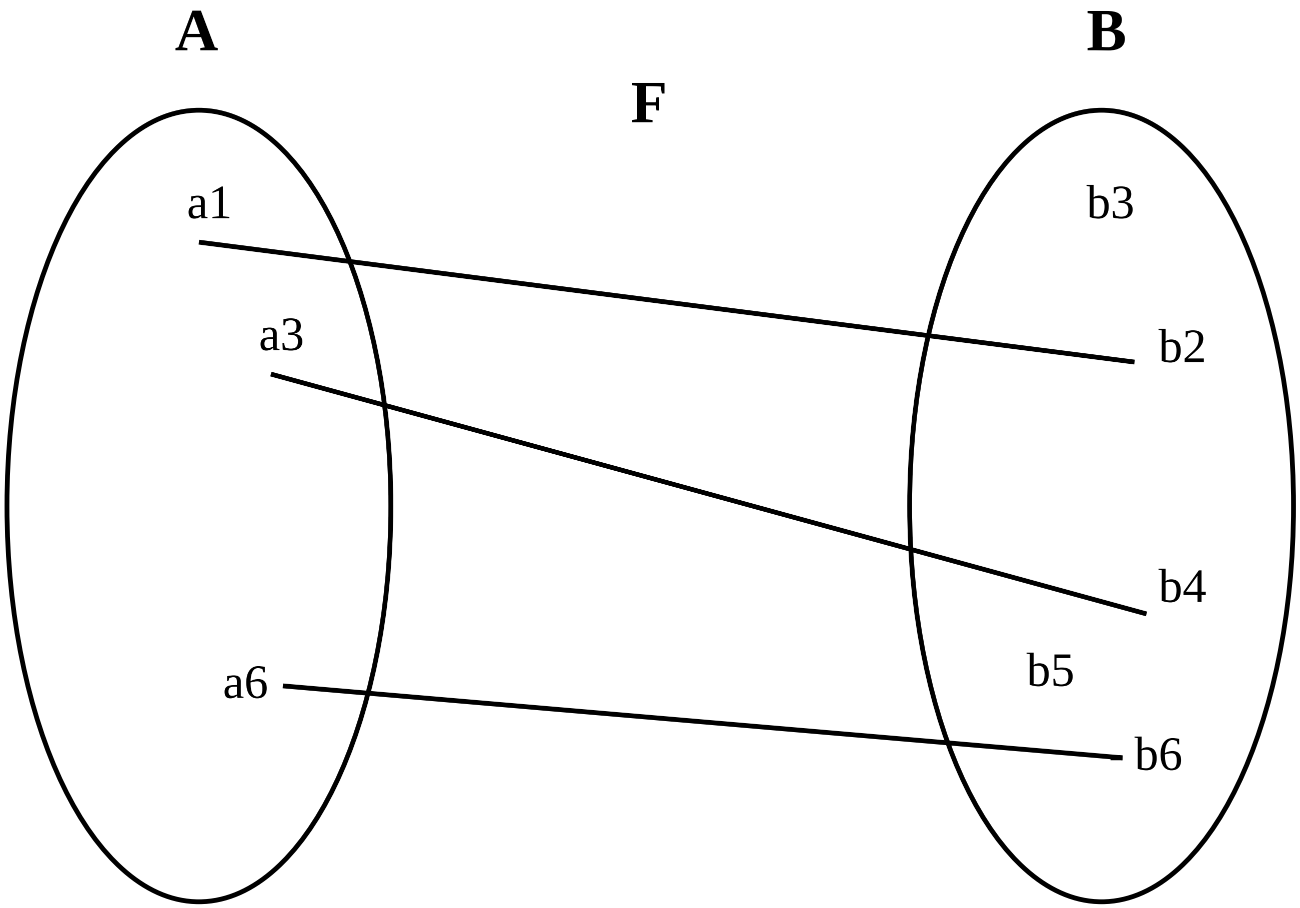
$$F \in A \rightarrow B$$

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



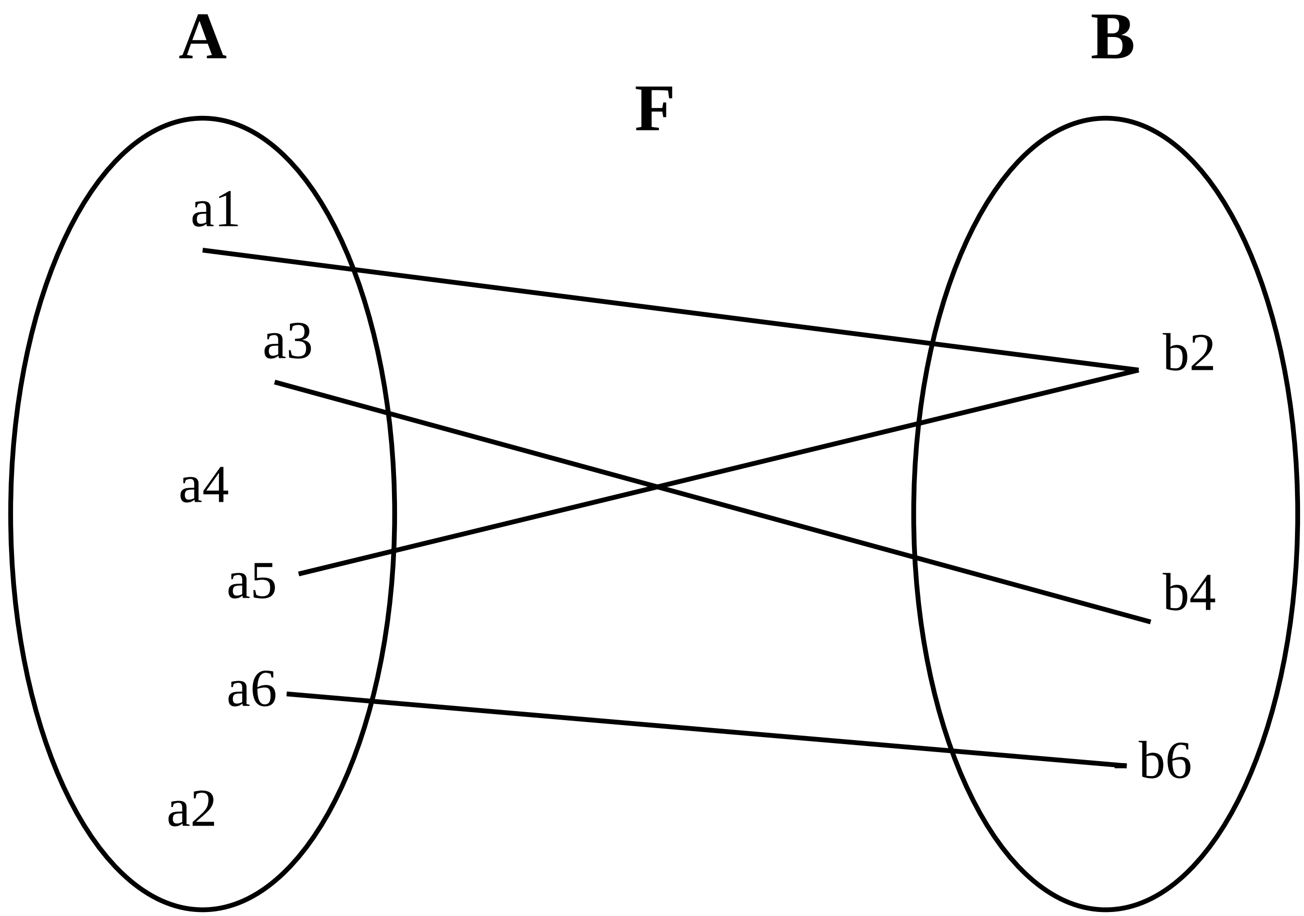
$$F \in A \rightarrowtail B$$

Left Part	Right Part
$f \in S \pfun T$	$f \in S \leftrightarrow T \quad \land \quad (f^{-1} \,;\, f) = \mathrm{id}(\mathrm{ran}(f))$
$f \in S \rightarrow T$	$f \in S \pfun T \quad \land \quad S = \mathrm{dom}(f)$
$f \in S \pinj T$	$f \in S \pfun T \quad \land \quad f^{-1} \in T \pfun S$
$f \in S \rightarrowtail T$	$f \in S \rightarrow T \quad \land \quad f^{-1} \in T \pfun S$

Function Operators (2)

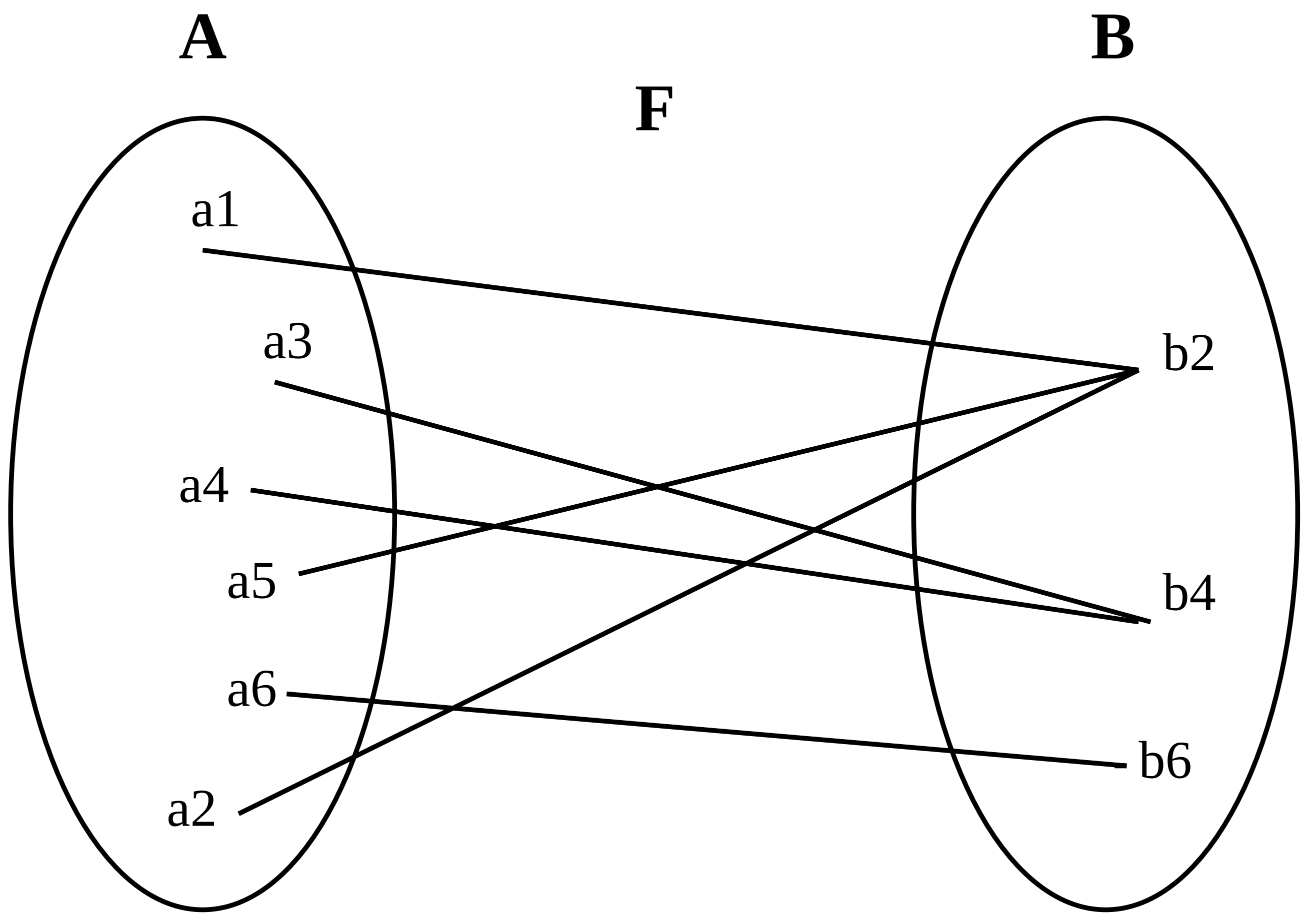
Partial surjections	$S \mathrel{+\!\!\!\twoheadrightarrow} T$
Total surjections	$S \twoheadrightarrow T$
Bijections	$S \rightarrowtail\!\!\!\!\twoheadrightarrow T$

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



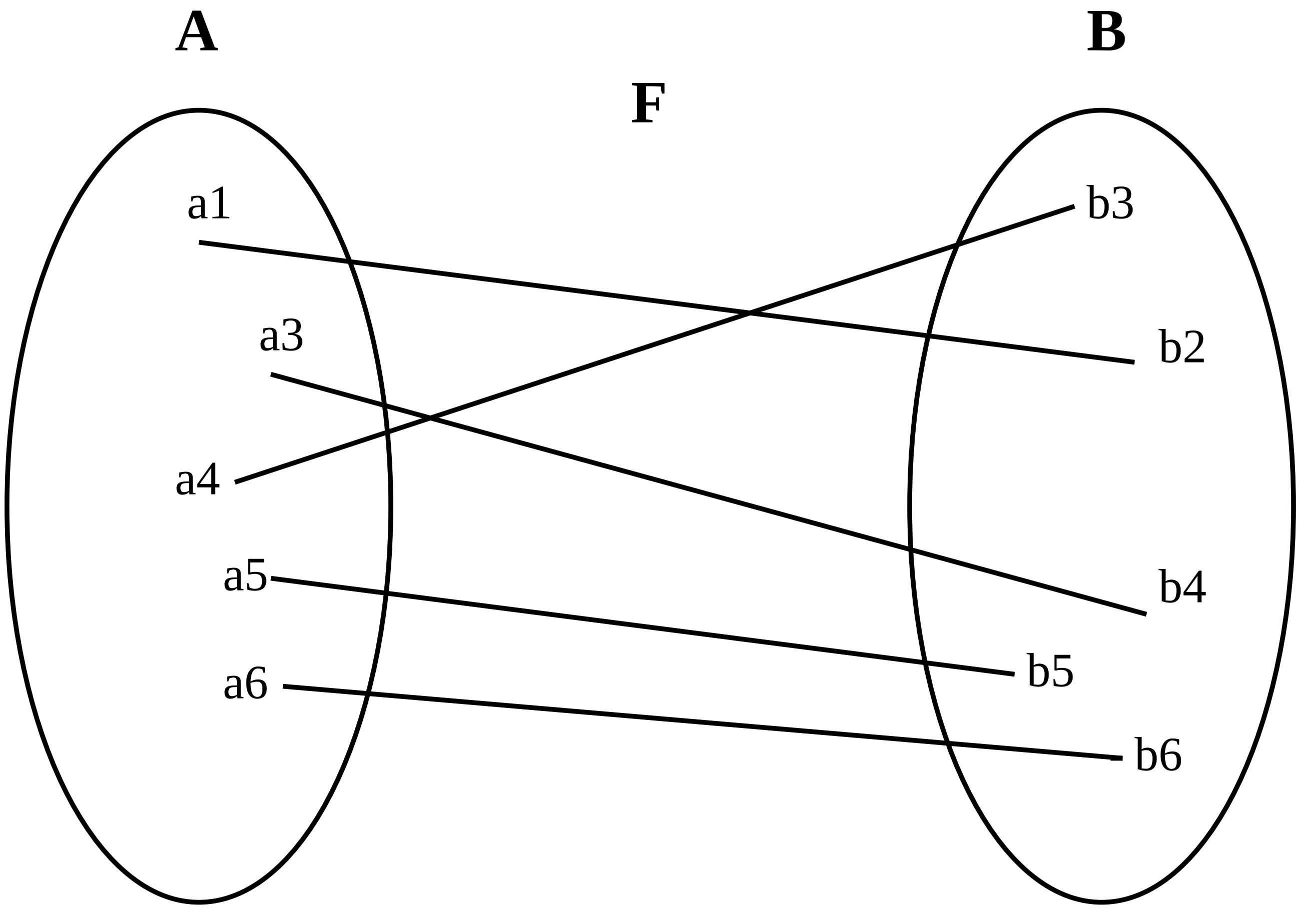
$$F \in A \twoheadrightarrow\!\!\!\!\!\!+\; B$$

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



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

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

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

Summary of all Set-theoretic Operators (40)

$S \times T$	$S \setminus T$	r^{-1}	$r[w]$	$\mathrm{id}\,(S)$	$\{\, x \mid x \in S \;\wedge\; P \,\}$
$\mathbb{P}(S)$	$S \leftrightarrow T$ $S \twoheadleftarrow\!\!\twoheadrightarrow T$	$S \lhd r$ $S ⩤ r$	$p\,;q$	$S ⇸ T$ $S \longrightarrow T$	$\{\, x \cdot x \in S \;\wedge\; P \mid E \}$
$S \subseteq T$	$S \leftarrow\!\!\twoheadrightarrow T$ $S \twoheadleftarrow\!\!\rightarrow T$	$r \rhd T$ $r ⩥ T$	$p \mathbin{<\!\!+} q$	$S ⤔ T$ $S \rightarrowtail T$	$\{\, a,\, b,\, \ldots,\, n \,\}$
$S \cup T$	$\mathrm{dom}\,(r)$ $\mathrm{ran}\,(r)$	prj_1	$p \otimes q$	$S ⤀ T$ $S \twoheadrightarrow T$	union $\quad \bigcup$
$S \cap T$	$\varnothing$	prj_2	$p \parallel q$	$S ⤖ T$	inter $\quad \bigcap$

Given a partial function f, we have

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

Well-definedness conditions: f is a partial function

$E \ \in \ \mathbf{dom}\,(f)$

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

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

- 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

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

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

- 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

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

- 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

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

$$
\begin{aligned}
wife &= \\
spouse &= \\
father &=
\end{aligned}
$$

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

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

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

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

$$spouse =$$

$$father =$$

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

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

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

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

$$spouse = husband \cup wife$$

$$father =$$

$$men \subseteq PERSON$$

$$women = PERSON \setminus men$$

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

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

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

$$spouse = husband \cup wife$$

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

$$
\begin{aligned}
\boldsymbol{men} &\subseteq \boldsymbol{PERSON} \\
\boldsymbol{women} &= \boldsymbol{PERSON} \setminus \boldsymbol{men} \\
\boldsymbol{husband} &\in \boldsymbol{women} \rightarrowtail\!\!\!\!\!\!\!+\;\; \boldsymbol{men} \\
\boldsymbol{mother} &\in \boldsymbol{PERSON} \longrightarrow \mathrm{dom}(\boldsymbol{husband})
\end{aligned}
$$

$$
\begin{aligned}
\boldsymbol{father} &= \boldsymbol{mother} \,;\, \boldsymbol{husband} \\
\boldsymbol{children} &= \\
\boldsymbol{daughter} &= \\
\boldsymbol{sibling} &=
\end{aligned}
$$

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

$$
\begin{aligned}
father &= mother \,;\, husband \\
children &= (mother \cup father)^{-1} \\
daughter &= \\
sibling &=
\end{aligned}
$$

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

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

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

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

$$brother = ?$$

$$sibling-in-law = ?$$

$$nephew-or-niece = ?$$

$$uncle-or-aunt = ?$$

$$cousin = ?$$

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

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 quick review of Set Theory
- A quick review of Arithmetic

$$
\begin{array}{lcl}
predicate & ::= & \bot \\
& & \top \\
& & \neg\, predicate \\
& & predicate \;\wedge\; predicate \\
& & predicate \;\vee\; predicate \\
& & predicate \;\Rightarrow\; predicate \\
& & predicate \;\Leftrightarrow\; predicate \\
& & \forall\, var\_list \cdot predicate \\
& & \exists\, var\_list \cdot predicate \\
& & expression \;=\; expression \\
& & expression \;\in\; set \\
& & number \;<\; number \\
& & number \;\leq\; number \\
& & number \;>\; number \\
& & number \;\geq\; number \\
& & \mathrm{finite}(set)
\end{array}
$$

$$
\begin{array}{lcl}
expression & ::= & variable \\
 & & expression \mapsto expression \\
 & & set \\
 & & number \\
 & & \\
variable & ::= & identifier \\
 & & \\
var\_list & ::= & variable \\
 & & variable, var\_list \\
 & & \\
set & ::= & set \times set \\
 & & \mathbb{P}(set) \\
 & & \{\, var\_list \cdot predicate \mid expression \,\} \\
 & & \mathbb{Z} \\
 & & \mathbb{N} \\
 & & number \mathrel{..} number
\end{array}
$$

$$
\begin{array}{lcl}
number & ::= & 0 \\
 & & 1 \\
 & & \ldots \\
 & & -\,number \\
 & & number + number \\
 & & number - number \\
 & & number * number \\
 & & number / number \\
 & & number \bmod number \\
 & & number\,\hat{}\,number \\
 & & \mathrm{card}(set) \\
 & & \min(set) \\
 & & \max(set)
\end{array}
$$

Summary of the Well-definedness Conditions

$\mathrm{inter}\,(S)$	$S \neq \varnothing$
$\bigcap\, x \cdot x \in S \;\wedge\; P(x) \mid T(x)$	$\exists\, x \cdot x \in S \;\wedge P(x)$
$f(E)$	f is a partial function $E \in \mathrm{dom}(f)$
E/F	$F \neq 0$
$E \bmod F$	$F \neq 0$
$\mathrm{card}(S)$	$\mathrm{finite}(S)$
$\min(S)$	$S \subseteq \mathbb{Z}$ $\exists x \cdot x \in \mathbb{Z} \;\wedge\; (\forall n \cdot n \in S \;\Rightarrow\; x \leq n)$
$\max(S)$	$S \subseteq \mathbb{Z}$ $\exists x \cdot x \in \mathbb{Z} \;\wedge\; (\forall n \cdot n \in S \;\Rightarrow\; x \geq n)$