

# Event-B Course

## 6. Summary of Mathematical Notation and Proofs

Jean-Raymond Abrial

September-October-November 2011

- 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

- 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  $C$

- 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  $K$ , containing  $S$  initially

WHILE  $K$  is not empty

CHOOSE a rule  $\frac{A}{C}$  in  $\mathcal{T}$  whose consequent  $C$  is in  $K$ ;

REPLACE  $C$  in  $K$  by the antecedents  $A$  (if any)

This proof method is said to be goal oriented

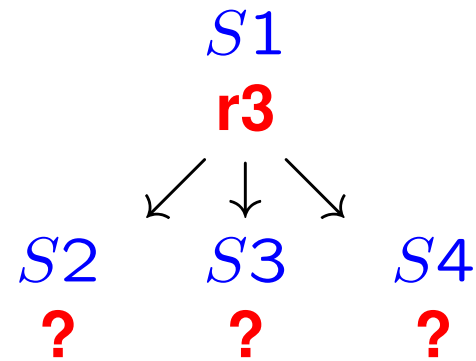


$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

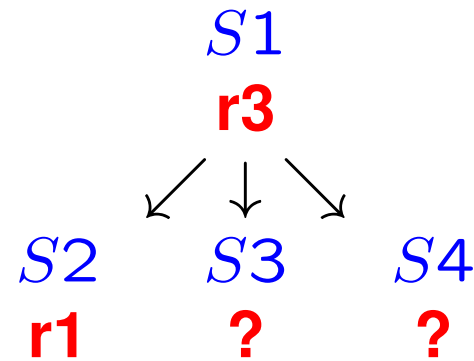
$S1$

?

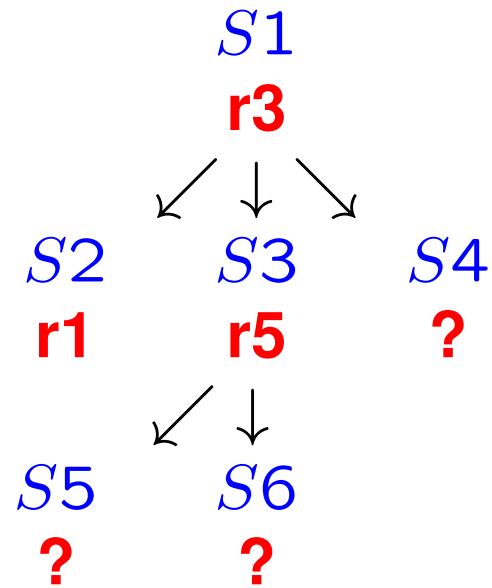
$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



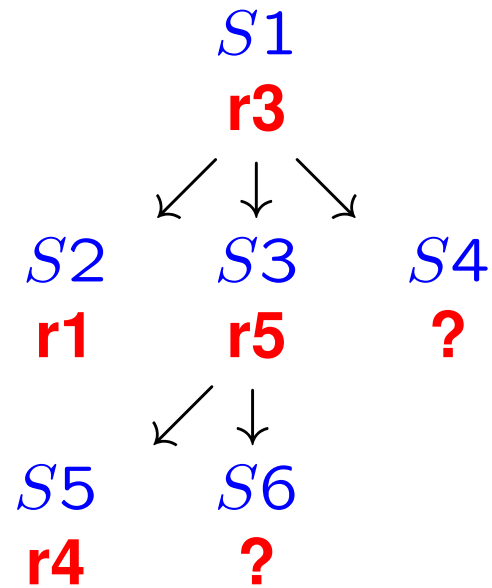
$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



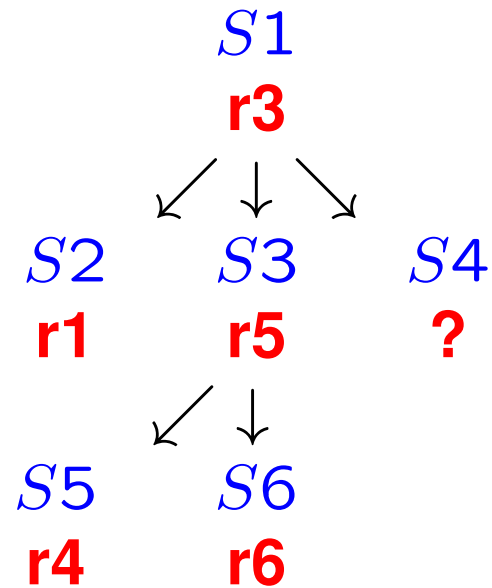
$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



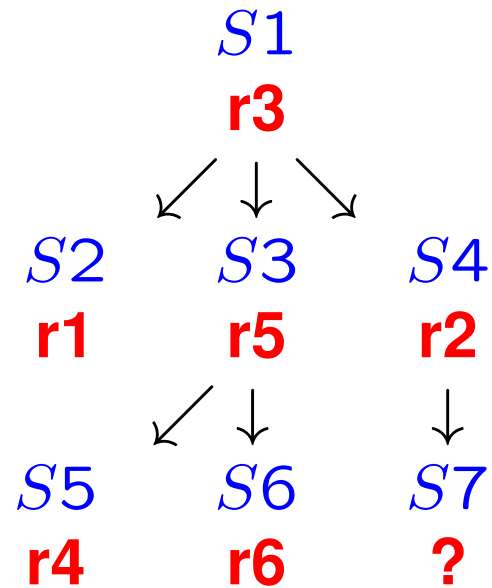
$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



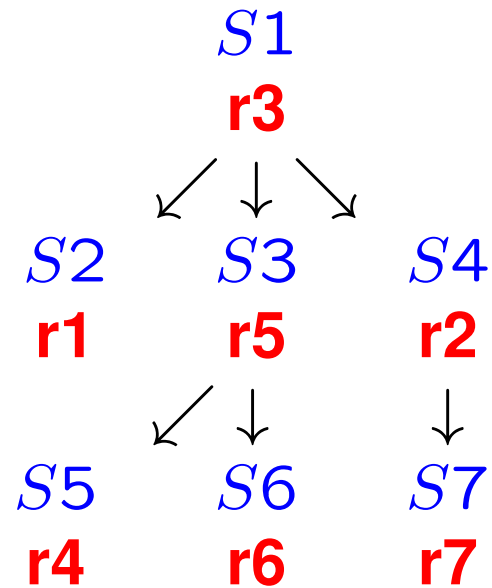
$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



$$r1_{\overline{S2}} \quad r2_{\overline{S4} \overline{S7}} \quad r3_{\overline{S2} \overline{S3} \overline{S4} \overline{S1}} \quad r4_{\overline{S5}} \quad r5_{\overline{S5} \overline{S6} \overline{S3}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

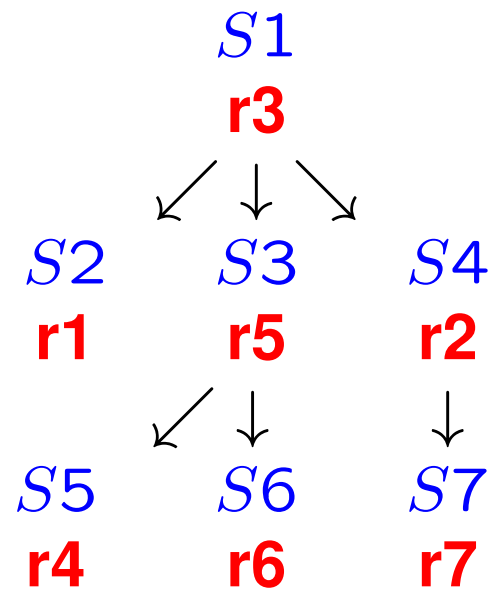


$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$



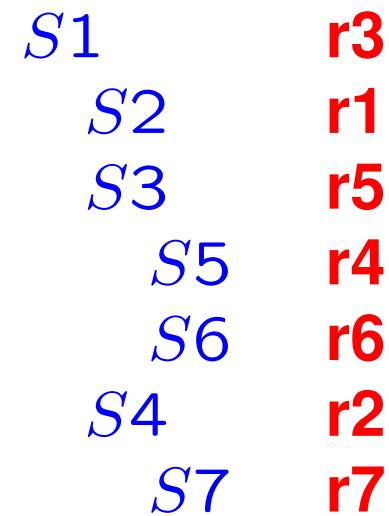
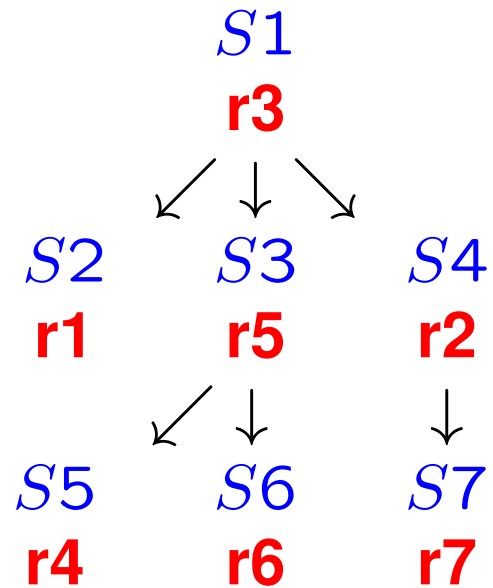


$r1_{\overline{S2}}$     $r2_{\overline{S4} \overline{S7}}$     $r3_{\overline{S1} \overline{S2} \overline{S3} \overline{S4}}$     $r4_{\overline{S5}}$     $r5_{\overline{S3} \overline{S5} \overline{S6}}$     $r6_{\overline{S6}}$     $r7_{\overline{S7}}$



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

- A **vertical representation** of the proof tree:



$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

$S1$

?

$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

$S1$

$r3$

$S2$

$?$

$S3$

$?$

$S4$

$?$

$$r1_{\overline{S2}} \quad r2_{\overline{S4}^{S7}} \quad r3_{\overline{S1}^{S2 \ S3 \ S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3}^{S5 \ S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

$S1$

$S2$

$S3$

$S4$

$r3$

$r1$

?

?

$$r1_{\overline{S2}} \quad r2_{\overline{S4}} \quad r3_{\overline{S2} \overline{S3} \overline{S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S5} \overline{S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

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

$$r1_{\overline{S2}} \quad r2_{\overline{S4}} \quad r3_{\overline{S2} \overline{S3} \overline{S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S5} \overline{S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

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

$$r1_{\overline{S2}} \quad r2_{\overline{S4}} \quad r3_{\overline{S2} \overline{S3} \overline{S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S5} \overline{S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

$$\begin{array}{cc} S1 & r3 \\ S2 & r1 \\ S3 & r5 \\ S5 & r4 \\ S6 & r6 \\ S4 & ? \end{array}$$

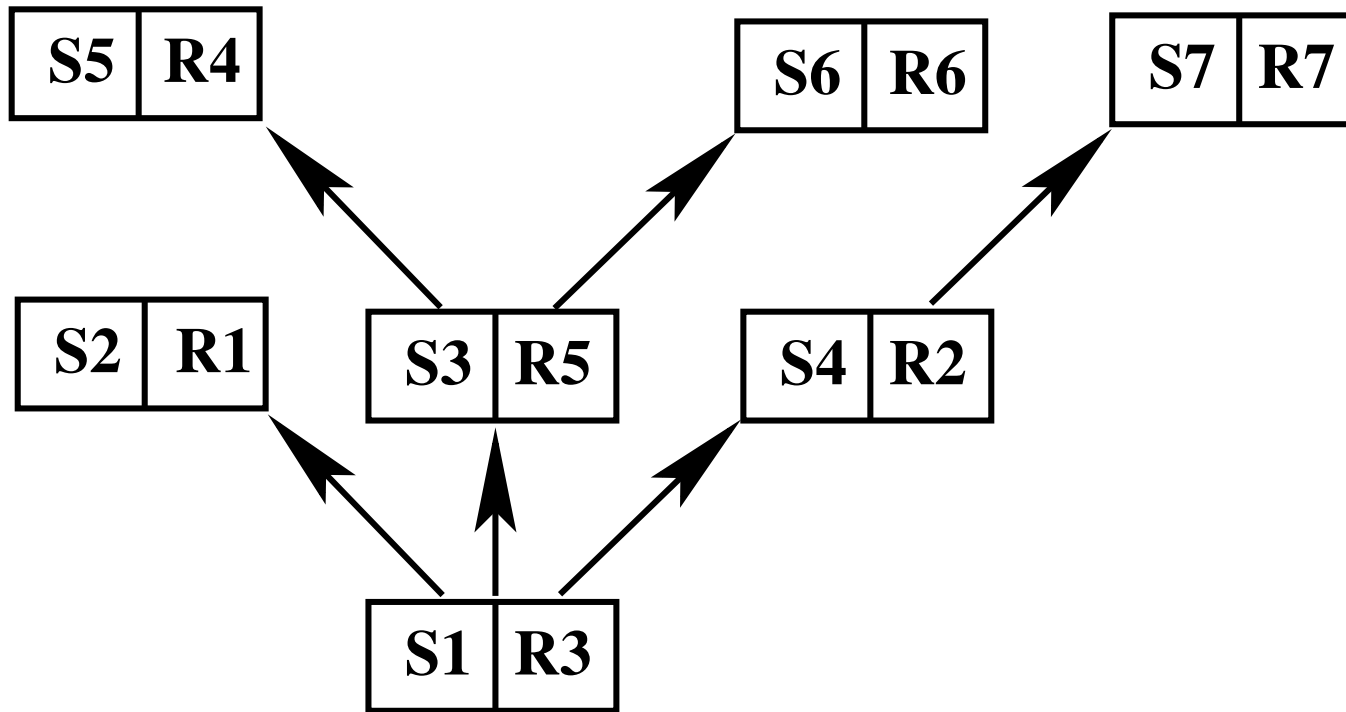


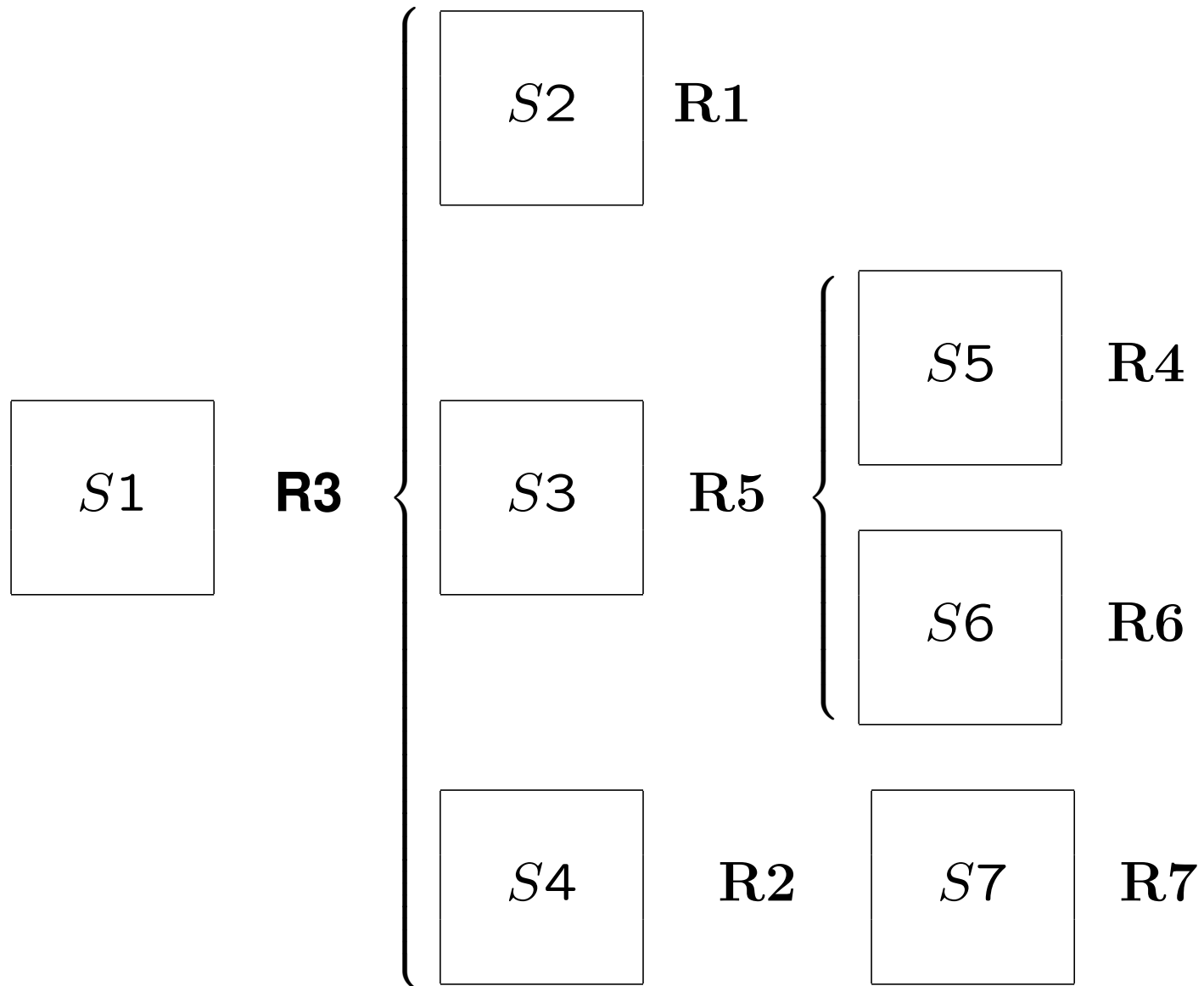
$$r1_{\overline{S2}} \quad r2_{\overline{S4} \overline{S7}} \quad r3_{\overline{S1} \overline{S2} \overline{S3} \overline{S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3} \overline{S5} \overline{S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

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

$$r1_{\overline{S2}} \quad r2_{\overline{S4} \overline{S7}} \quad r3_{\overline{S1} \overline{S2} \overline{S3} \overline{S4}} \quad r4_{\overline{S5}} \quad r5_{\overline{S3} \overline{S5} \overline{S6}} \quad r6_{\overline{S6}} \quad r7_{\overline{S7}}$$

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





- Concepts of **Sequent** and **Inference Rule**
- **Backward** and **Forward** Reasoning
- **Basic** Inference Rules

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

$$H \vdash G$$

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

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  $G$ .

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

HYP

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

MON

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

CUT



- 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:**  $\neg P$

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

- This syntax is ambiguous

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

- TRUTH:  $\top$
- FALSITY:  $\perp$
- DISJUNCTION:  $P \vee Q$
- EQUIVALENCE:  $P \Leftrightarrow Q$

$$\begin{aligned} \textit{Predicate} ::= & \textit{Predicate} \wedge \textit{Predicate} \\ & \textit{Predicate} \Rightarrow \textit{Predicate} \\ & \neg \textit{Predicate} \\ & \perp \\ & \top \\ & \textit{Predicate} \vee \textit{Predicate} \\ & \textit{Predicate} \Leftrightarrow \textit{Predicate} \end{aligned}$$

- 
- 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  $\Leftrightarrow$ .

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



$$\frac{}{H, \perp \vdash P} \text{ FALSE\_L}$$

$$\frac{H \vdash P \quad H \vdash \neg P}{H \vdash \perp} \text{ FALSE\_R}$$

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

$$\frac{H, P \vdash \perp}{H \vdash \neg P} \text{ NOT\_R}$$

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

$$\frac{H \vdash P \quad H \vdash Q}{H \vdash P \wedge Q} \text{ AND\_R}$$

$$\frac{H, P \vdash R \quad H, Q \vdash R}{H, P \vee Q \vdash R} \text{ OR\_L}$$

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

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

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

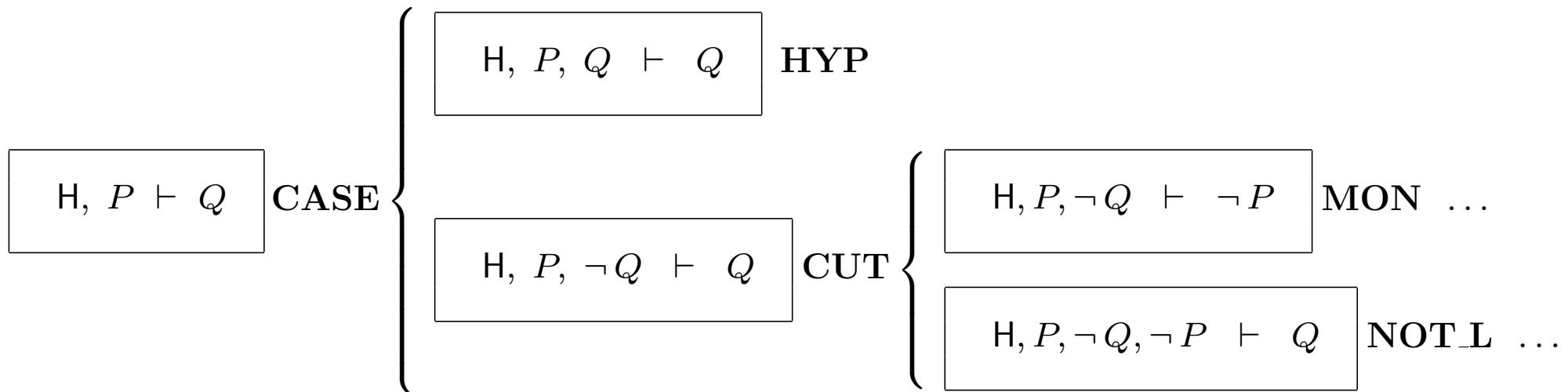
$$\frac{H, Q \vdash P \quad H, \neg Q \vdash P}{H \vdash P} \text{ CASE}$$

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

$$\boxed{H \vdash P} \text{ CUT } \left\{ \begin{array}{l} \boxed{H \vdash Q \vee \neg Q} \text{ OR\_R } \boxed{H, \neg Q \vdash \neg Q} \text{ HYP} \\ \boxed{H, Q \vee \neg Q \vdash P} \text{ OR\_L } \left\{ \begin{array}{l} \boxed{H, Q \vdash P} \text{ ant.} \\ \boxed{H, \neg Q \vdash P} \text{ ant.} \end{array} \right. \end{array} \right.$$

$$\frac{H, \neg Q \vdash \neg P}{H, P \vdash Q} \text{CT\_L}$$

Proof of rule **CT\_L**:



...  $\boxed{H, \neg Q \vdash \neg P}$  antecedent

...  $\boxed{H, P, \neg Q, \neg Q \vdash P}$  HYP

$$\frac{H, \neg P \vdash \perp}{H \vdash P} \text{CT\_R}$$

Proof of rule **CT\_R**:

$$\boxed{H \vdash P} \text{ CASE } \left\{ \begin{array}{l} \boxed{H, P \vdash P} \text{ HYP} \\ \boxed{H, \neg P \vdash P} \text{ CUT } \left\{ \begin{array}{l} \boxed{H, \neg P \vdash \perp} \text{ antecedent} \\ \boxed{H, \neg P, \perp \vdash P} \text{ FALSE\_L} \end{array} \right. \end{array} \right.$$

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

commutativity	$  \begin{aligned}  P \vee Q &\Leftrightarrow Q \vee P \\  P \wedge Q &\Leftrightarrow Q \wedge P \\  (P \Leftrightarrow Q) &\Leftrightarrow (Q \Leftrightarrow P)  \end{aligned}  $
associativity	$  \begin{aligned}  (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))  \end{aligned}  $
distributivity	$  \begin{aligned}  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)  \end{aligned}  $

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	$(P \Leftrightarrow \perp) \Leftrightarrow \neg P$

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	$P \Leftrightarrow \neg \neg P$



transitivity	$(P \Rightarrow Q) \wedge (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$
monotonicity	$\begin{aligned} (P \Rightarrow Q) &\Rightarrow ((P \wedge R) \Rightarrow (Q \wedge R)) \\ (P \Rightarrow Q) &\Rightarrow ((P \vee R) \Rightarrow (Q \vee R)) \\ (P \Rightarrow Q) &\Rightarrow ((R \Rightarrow P) \Rightarrow (R \Rightarrow Q)) \\ (P \Rightarrow Q) &\Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R)) \\ (P \Rightarrow Q) &\Rightarrow (\neg Q \Rightarrow \neg P) \end{aligned}$
equivalence	$\begin{aligned} (P \Leftrightarrow Q) &\Rightarrow ((P \wedge R) \Leftrightarrow (Q \wedge R)) \\ (P \Leftrightarrow Q) &\Rightarrow ((P \vee R) \Leftrightarrow (Q \vee R)) \\ (P \Leftrightarrow Q) &\Rightarrow ((R \Rightarrow P) \Leftrightarrow (R \Rightarrow Q)) \\ (P \Leftrightarrow Q) &\Rightarrow ((P \Rightarrow R) \Leftrightarrow (Q \Rightarrow R)) \\ (P \Leftrightarrow Q) &\Rightarrow (\neg P \Leftrightarrow \neg Q) \end{aligned}$

- 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)

$$\begin{aligned} \textit{predicate} ::= & \perp \\ & \top \\ & \neg \textit{predicate} \\ & \textit{predicate} \wedge \textit{predicate} \\ & \textit{predicate} \vee \textit{predicate} \\ & \textit{predicate} \Rightarrow \textit{predicate} \\ & \textit{predicate} \Leftrightarrow \textit{predicate} \end{aligned}$$

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

*predicate* ::=  $\perp$   
 $\top$   
 $\neg$  *predicate*  
*predicate*  $\wedge$  *predicate*  
*predicate*  $\vee$  *predicate*  
*predicate*  $\Rightarrow$  *predicate*  
*predicate*  $\Leftrightarrow$  *predicate*  
 $\forall$  *var\_list* . *predicate*

*expression* ::= *variable*  
*expression*  $\mapsto$  *expression*

*variable* ::= *identifier*

*var\_list* ::= *variable*  
*variable*, *var\_list*

- 
- 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.

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

where **E** is an expression

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

- In rule ALL\_R, variable **x** is not free in H

*predicate* ::=  $\perp$   
 $\top$   
 $\neg$  *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*

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

- In rule XST\_L, variable **x** is not free in **H**

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

where **E** is an expression



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

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

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

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

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

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

ALL\_R  
ALL\_R  
IMP\_R

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

CUT ...

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

XST\_R

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

HYP

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

ALL\_L  
IMP\_L

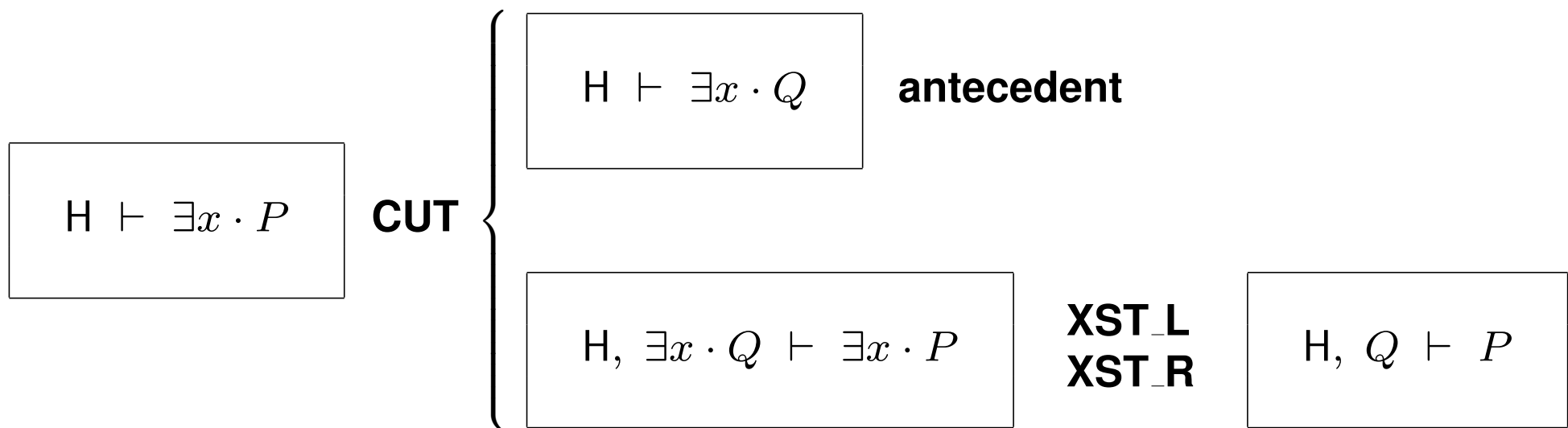
$$\begin{array}{l} \forall x \cdot (\exists y \cdot P_{x,y}) \Rightarrow Q_x \\ Q_x \\ P_{x,y} \\ \exists y \cdot P_{x,y} \\ \vdash \\ Q_x \end{array}$$

HYP

- Replacing an existential goal by a simpler one

$$\frac{H \vdash \exists x \cdot Q \quad H, Q \vdash P}{H \vdash \exists x \cdot P} \quad \text{CUT\_XST} \quad (x \text{ nfin } H)$$

Proof of **CUT\_XST**



commutativity	$\forall x \cdot \forall y \cdot P \Leftrightarrow \forall y \cdot \forall x \cdot P$ $\exists x \cdot \exists y \cdot P \Leftrightarrow \exists y \cdot \exists x \cdot P$
distributivity	$\forall x \cdot (P \wedge Q) \Leftrightarrow \forall x \cdot P \wedge \forall x \cdot Q$ $\exists x \cdot (P \vee Q) \Leftrightarrow \exists x \cdot P \vee \exists x \cdot Q$
associativity	<p><b>if</b> <math>x</math> not free in <math>P</math></p> $P \vee \forall x \cdot Q \Leftrightarrow \forall x \cdot (P \vee Q)$ $P \wedge \exists x \cdot Q \Leftrightarrow \exists x \cdot (P \wedge Q)$ $P \Rightarrow \forall x \cdot Q \Leftrightarrow \forall x \cdot (P \Rightarrow Q)$

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	$\forall x \cdot (P \Leftrightarrow Q) \Rightarrow (\forall x \cdot P \Leftrightarrow \forall x \cdot Q)$ $\forall x \cdot (P \Leftrightarrow Q) \Rightarrow (\exists x \cdot P \Leftrightarrow \exists x \cdot Q)$

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

*predicate* ::=  $\perp$   
 $\top$   
 $\neg$  *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* ::= ...

*variable* ::= ...

*var\_list* ::= ...

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

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

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

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



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

- 
- 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)

*predicate* ::=  $\perp$   
 $\top$   
 $\neg$  *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*  $\in$  *expression*

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

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

- 
- 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

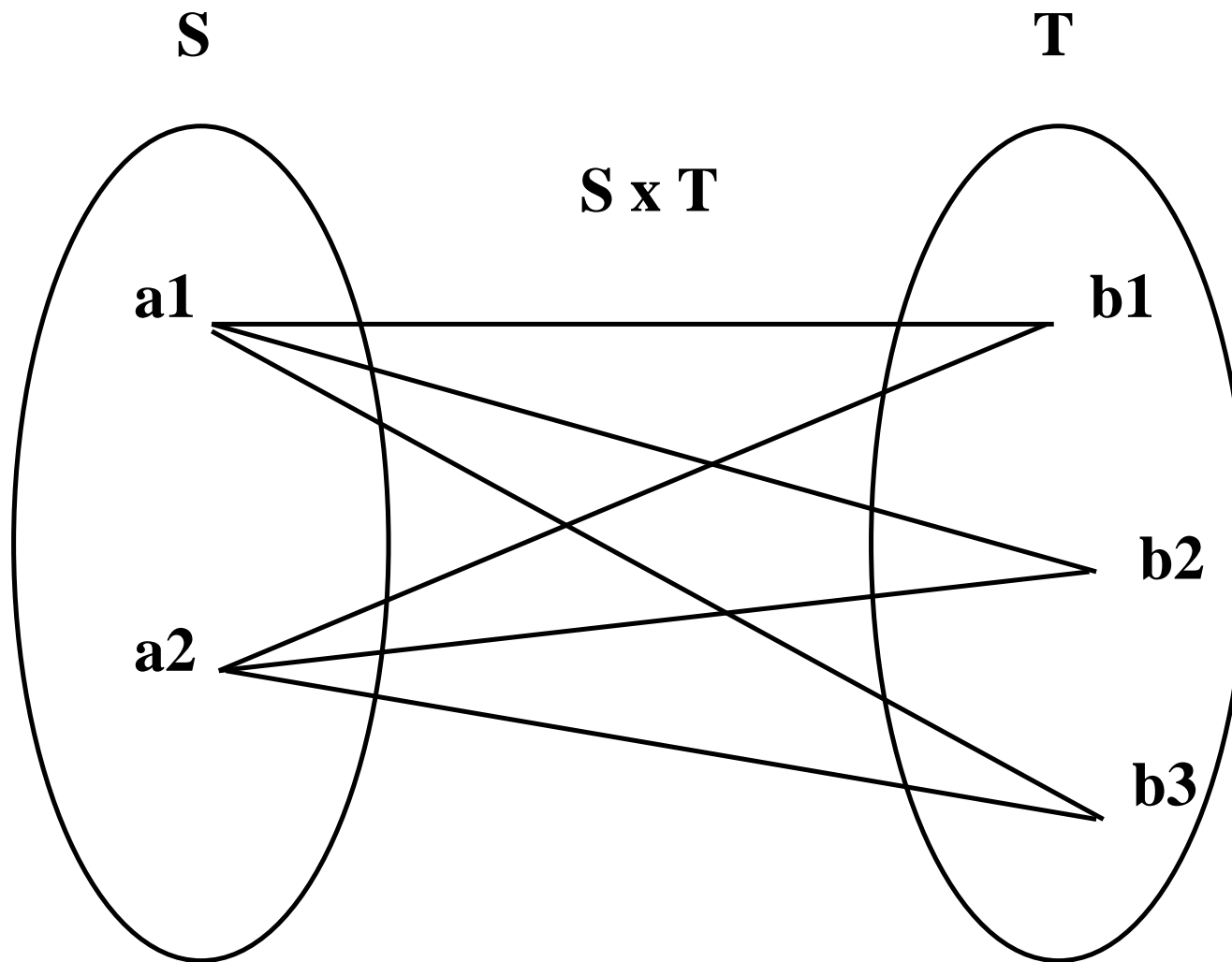
$$E \in S$$

- where  $E$  is an **expression** and  $S$  is a **set**

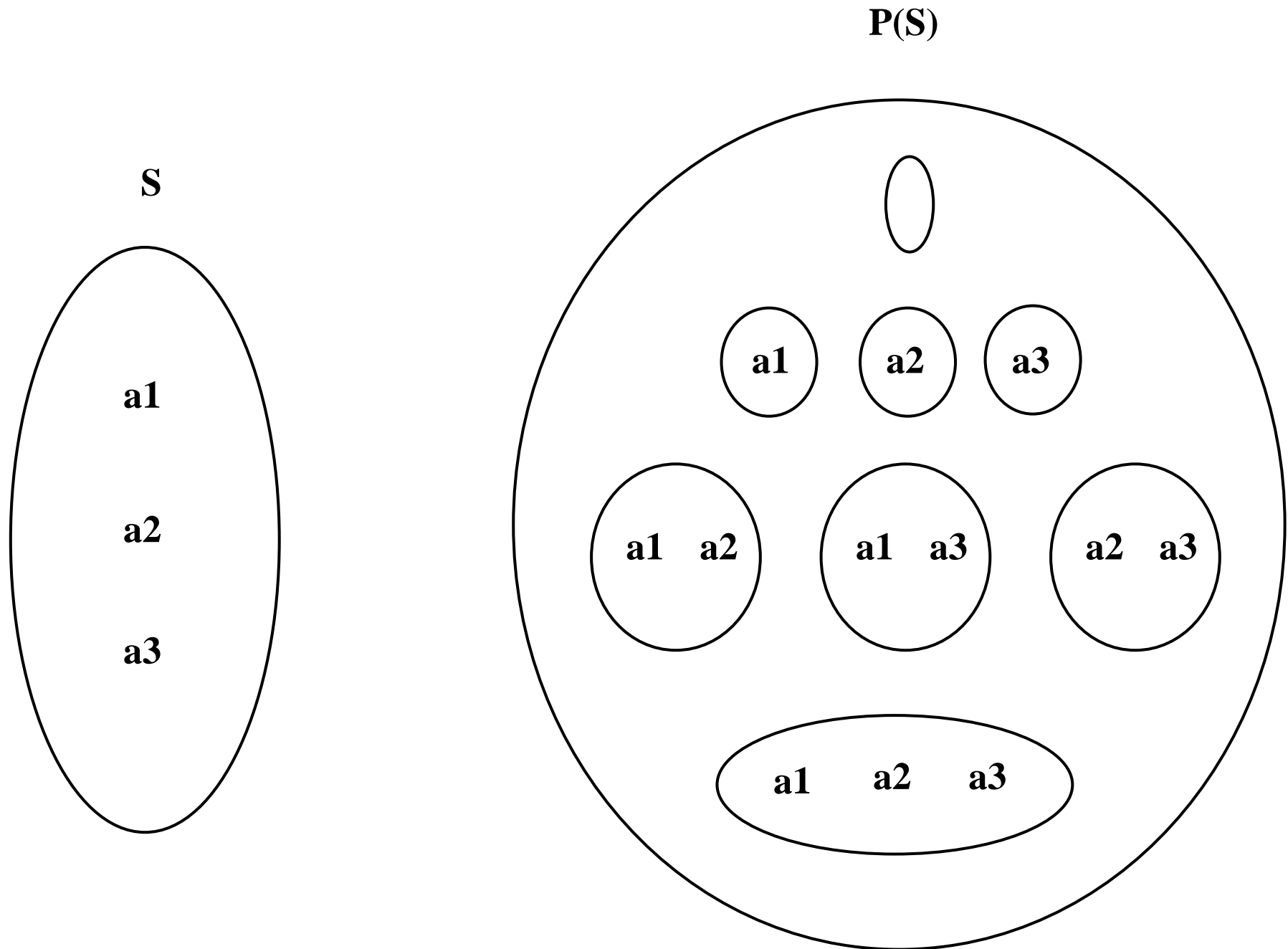
There are **three basic constructs** in set theory:

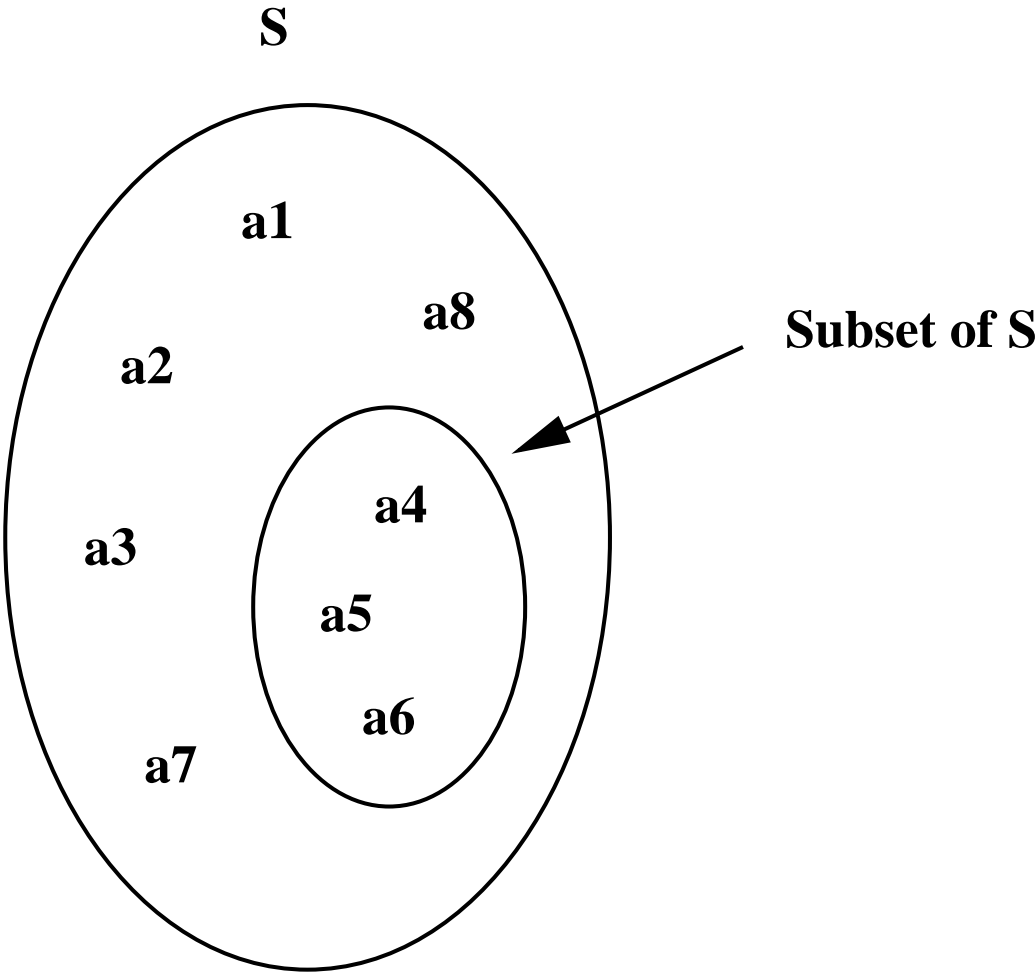
Cartesian product	$S \times T$
Power set	$\mathbb{P}(S)$
Comprehension 1	$\{ x \cdot x \in S \wedge P \mid F \}$
Comprehension 2	$\{ x \mid x \in S \wedge P \}$

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









These axioms are defined by **equivalences**.

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

---

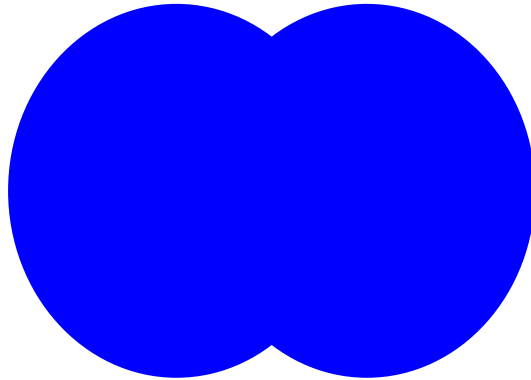
Left Part	Right Part
$S \subseteq T$	$S \in \mathbb{P}(T)$
$S = T$	$S \subseteq T \wedge T \subseteq S$

The first rule is just a **syntactic extension**

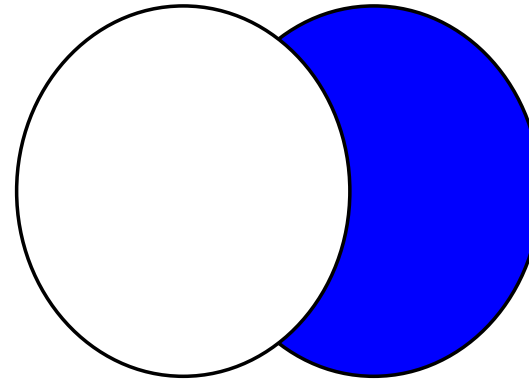
The second rule is the **Extensionality Axiom**

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

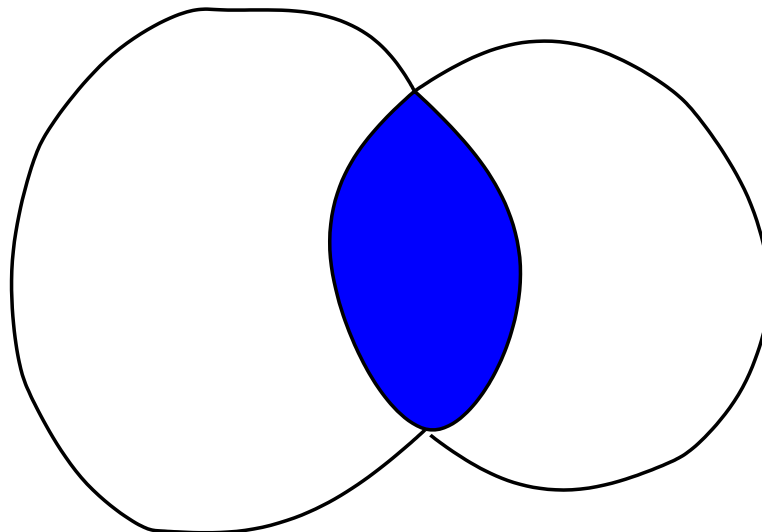
**Union**



**Difference**



**Intersection**



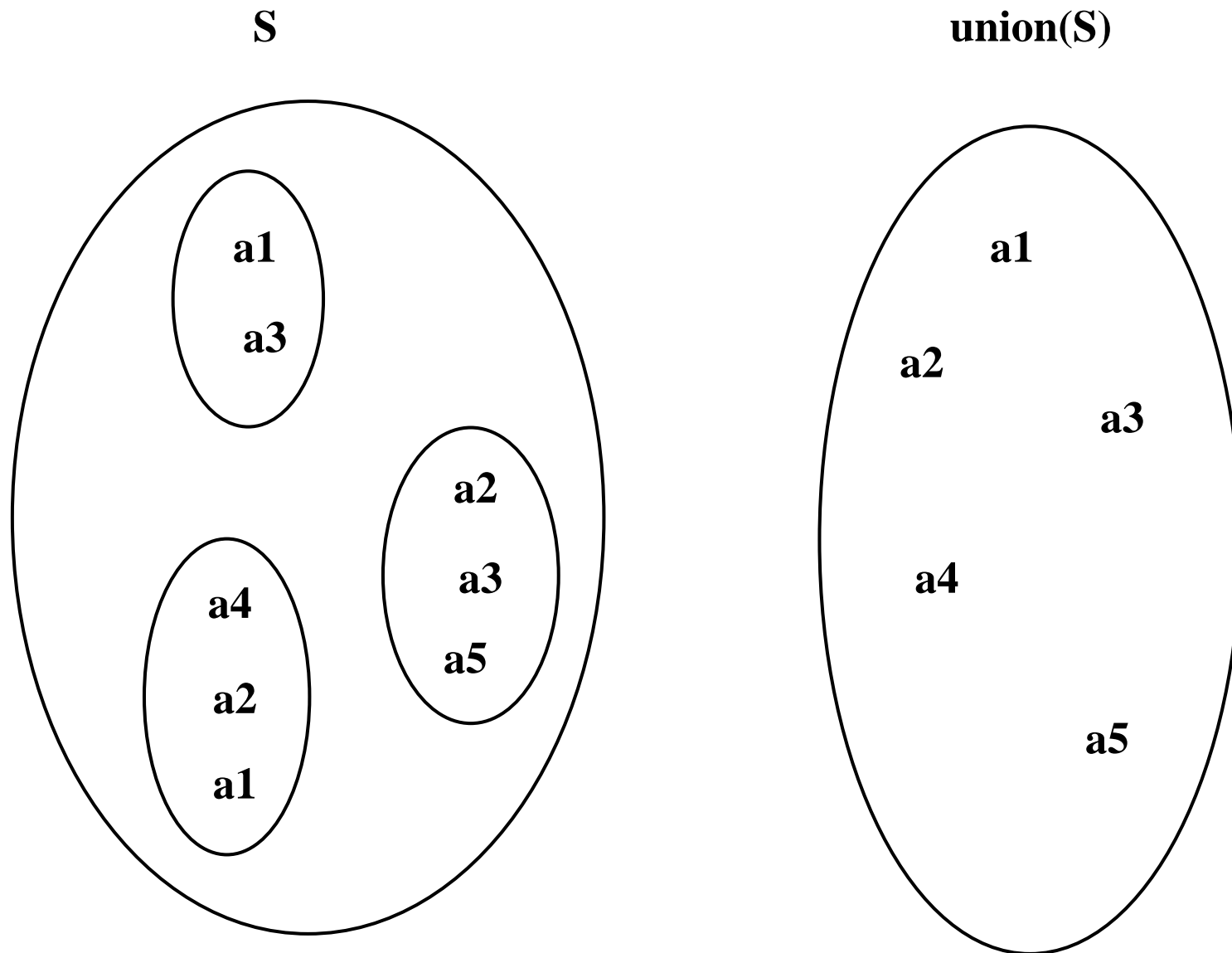
$E \in S \cup T$	$E \in S \vee E \in T$
$E \in S \cap T$	$E \in S \wedge E \in T$
$E \in S \setminus T$	$E \in S \wedge E \notin T$
$E \in \{a, \dots, b\}$	$E = a \vee \dots \vee E = b$
$E \in \emptyset$	$\perp$

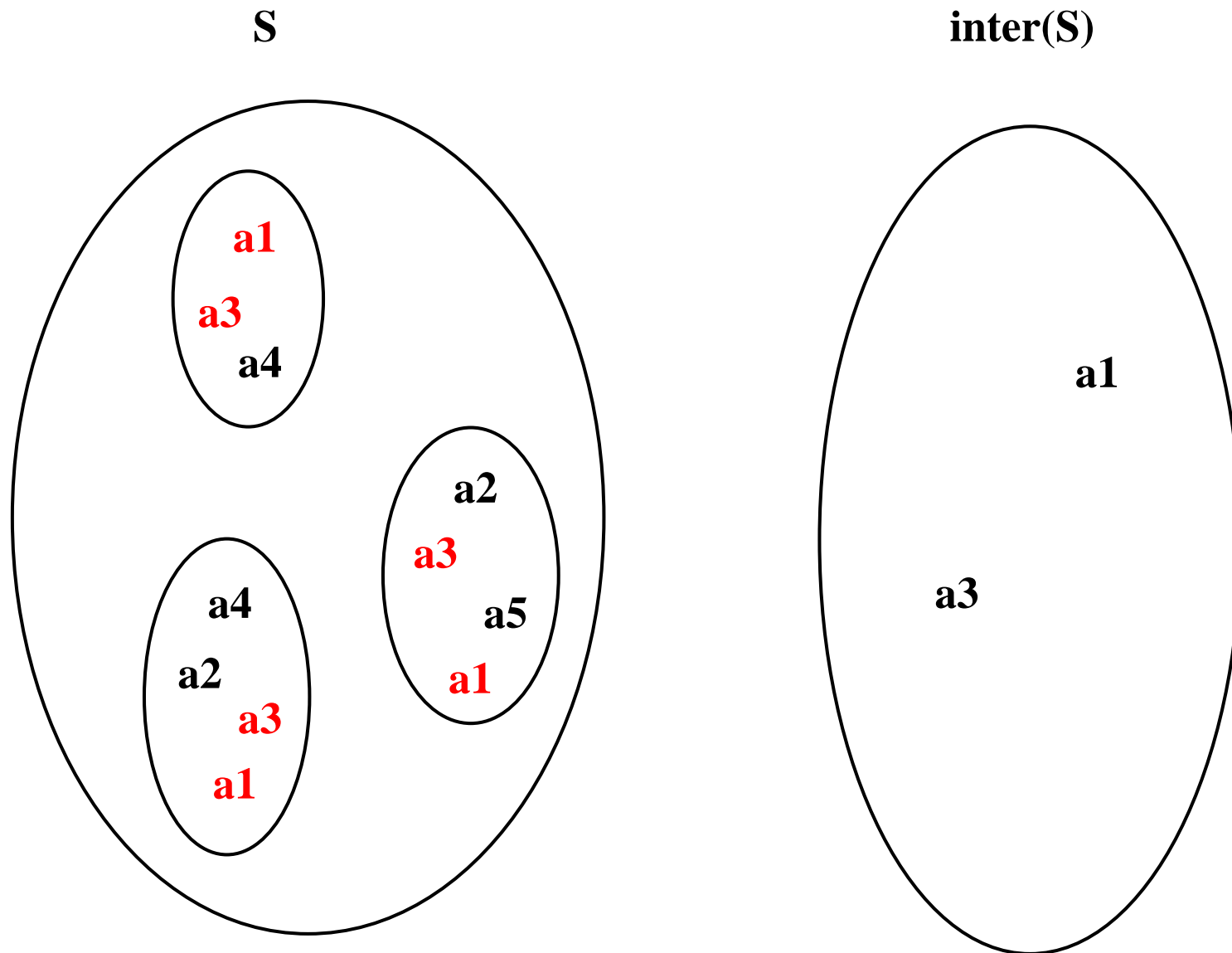
$S \times T$	$S \cup T$
$\mathbb{P}(S)$	$S \cap T$
$\{x \mid x \in S \wedge P\}$	$S \setminus T$
$S \subseteq T$	$\{a, \dots, b\}$
$S = T$	$\emptyset$



---

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





$E \in \text{union}(S)$	$\exists s \cdot (s \in S \wedge E \in s)$
$E \in \cup x \cdot (x \in S \wedge P \mid T)$	$\exists x \cdot (x \in S \wedge P \wedge E \in T)$
$E \in \text{inter}(S)$	$\forall s \cdot (s \in S \Rightarrow E \in s)$
$E \in \cap x \cdot (x \in S \wedge P \mid T)$	$\forall x \cdot (x \in S \wedge P \Rightarrow E \in T)$

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

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

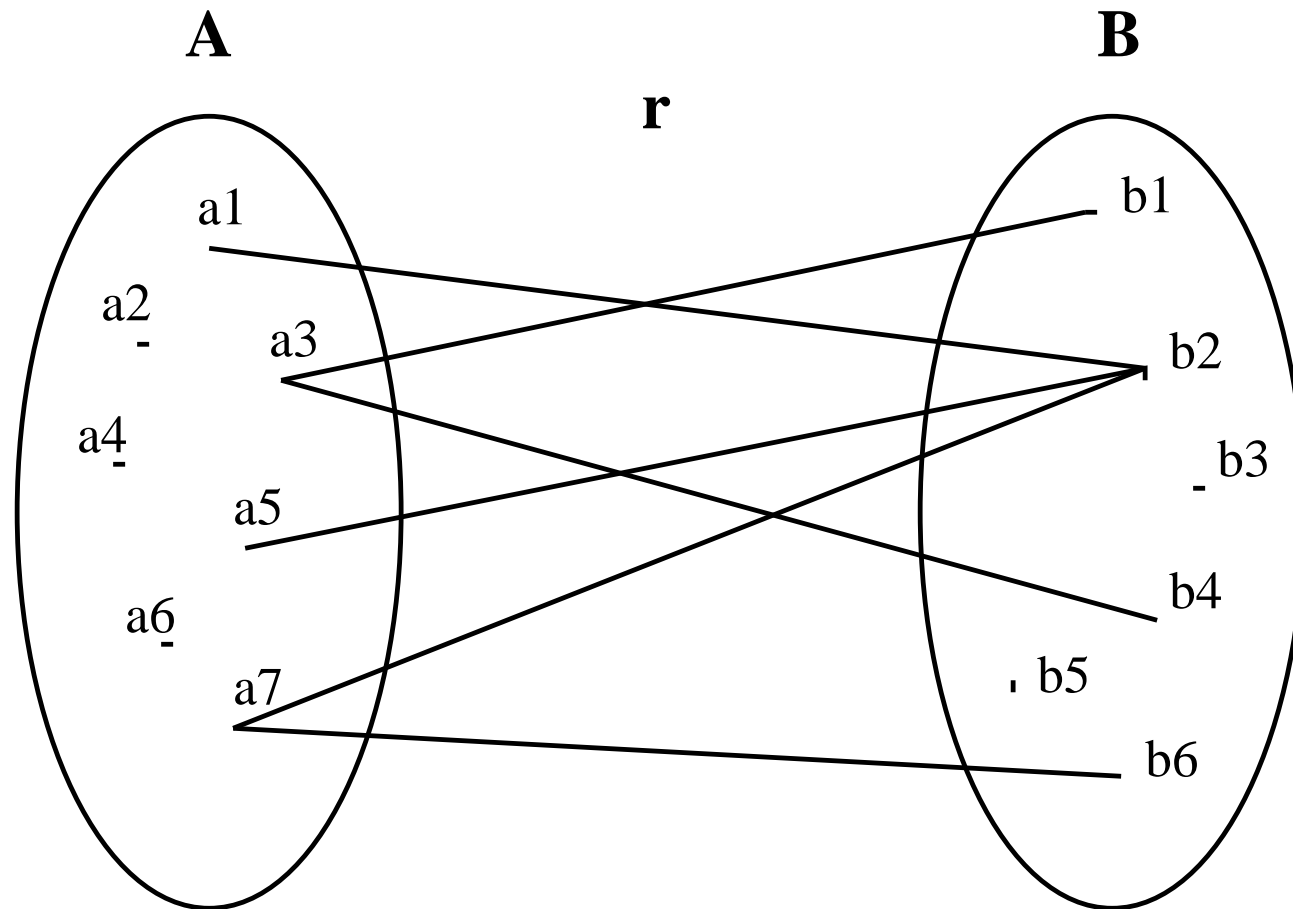
union ( $S$ )

$\cup x \cdot (x \in S \wedge P \mid T)$

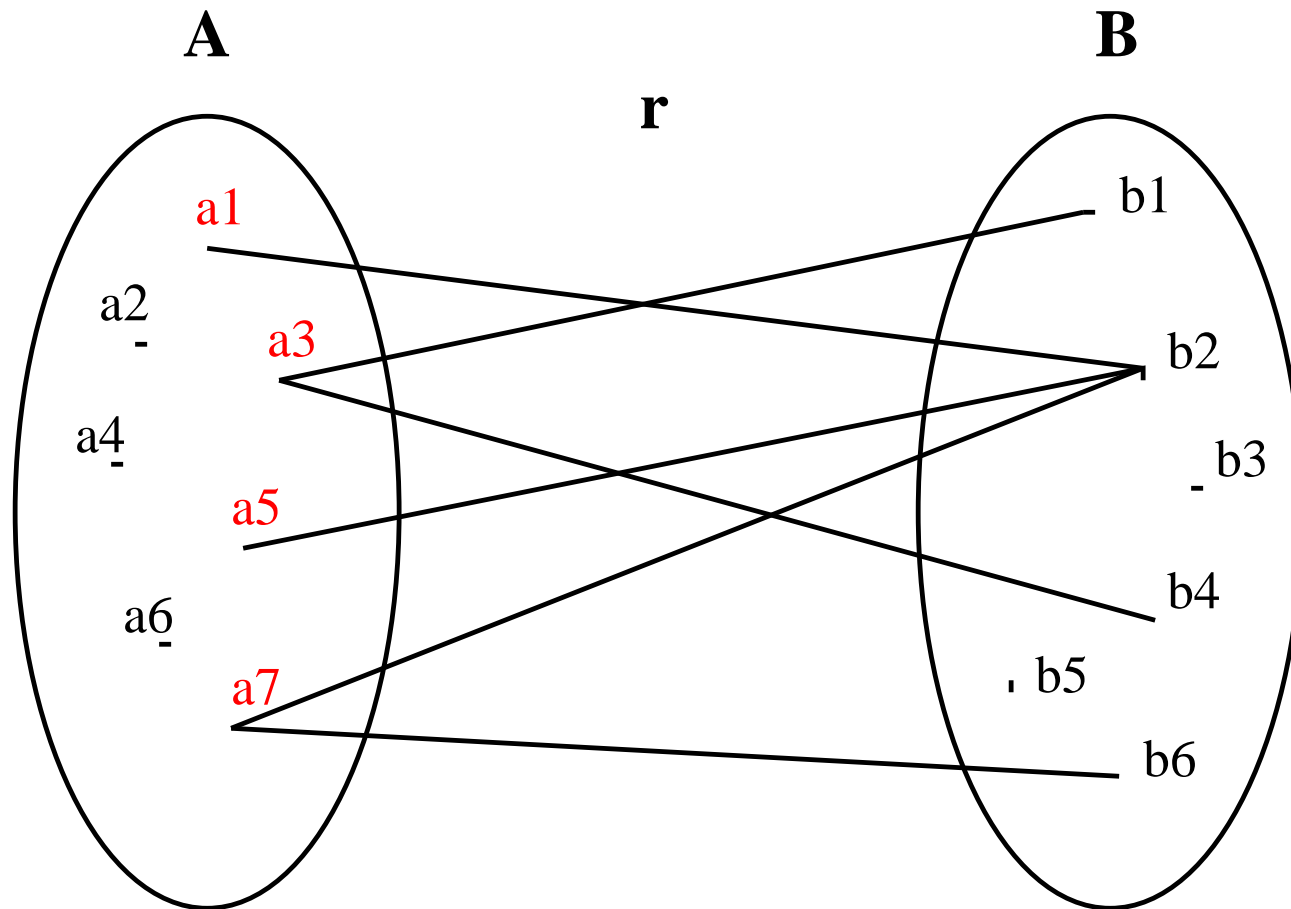
inter ( $S$ )

$\cap x \cdot (x \in S \wedge P \mid T)$

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

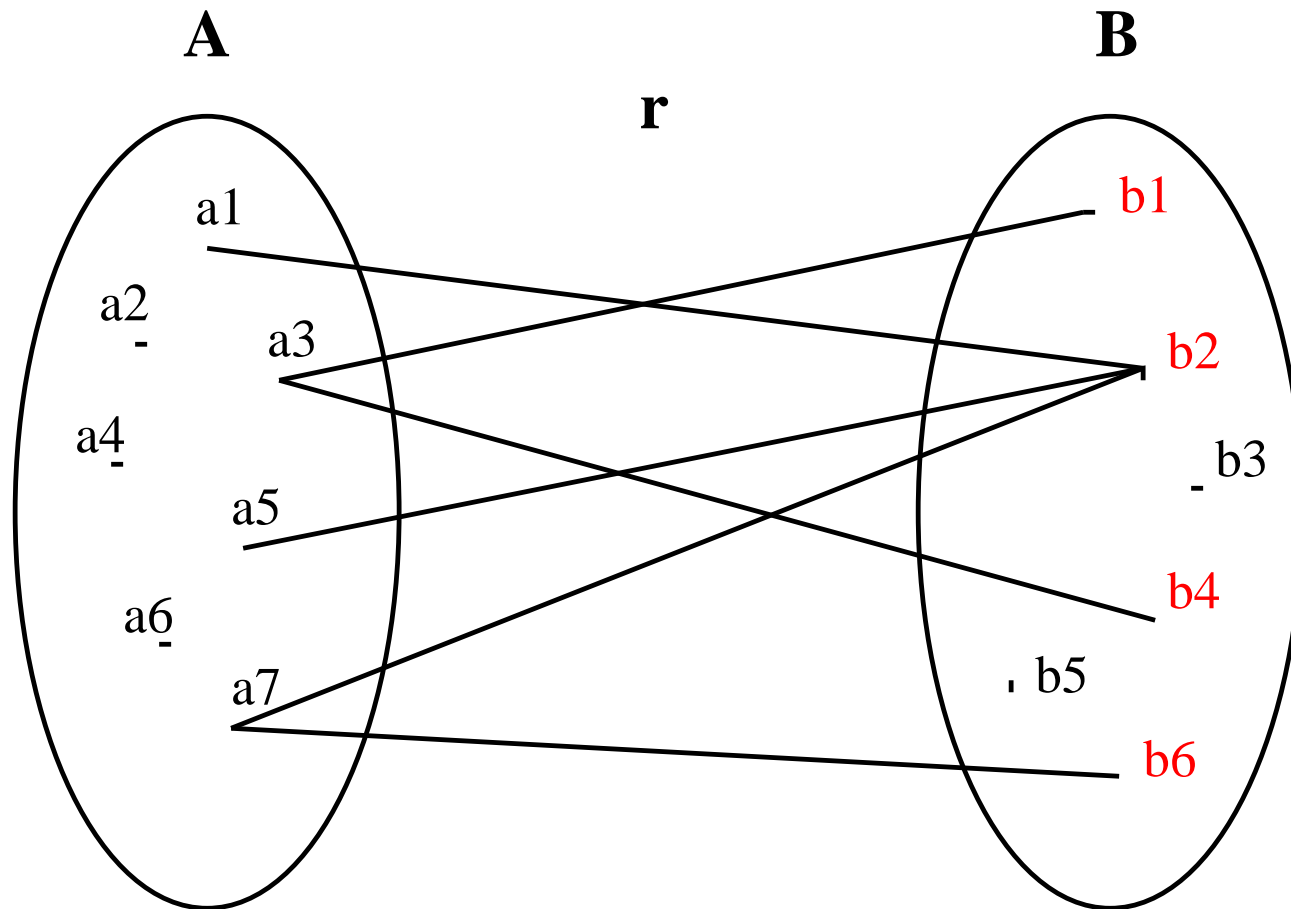


$$r \in A \leftrightarrow B$$

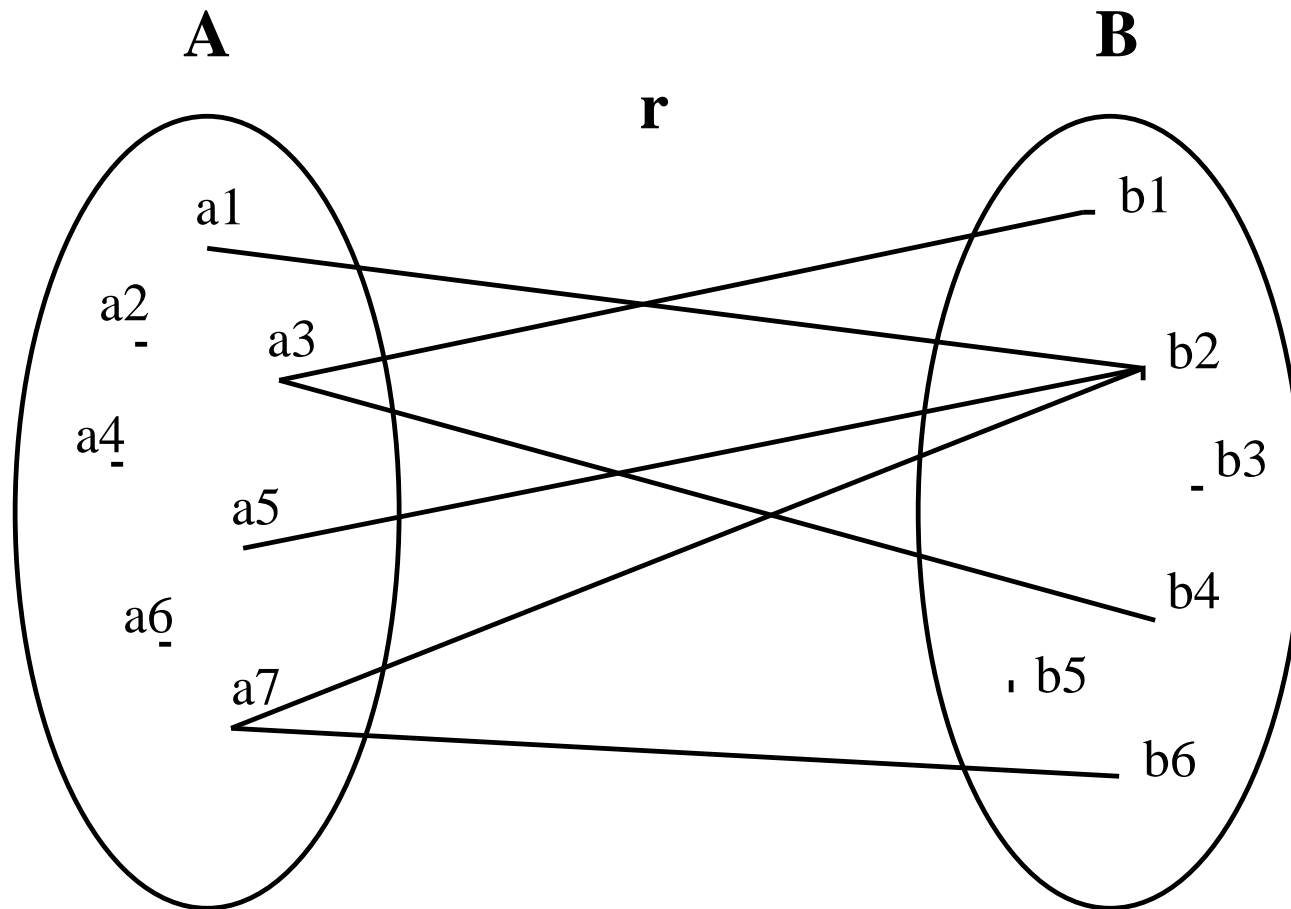


$$\text{dom}(r) = \{a1, a3, a5, a7\}$$





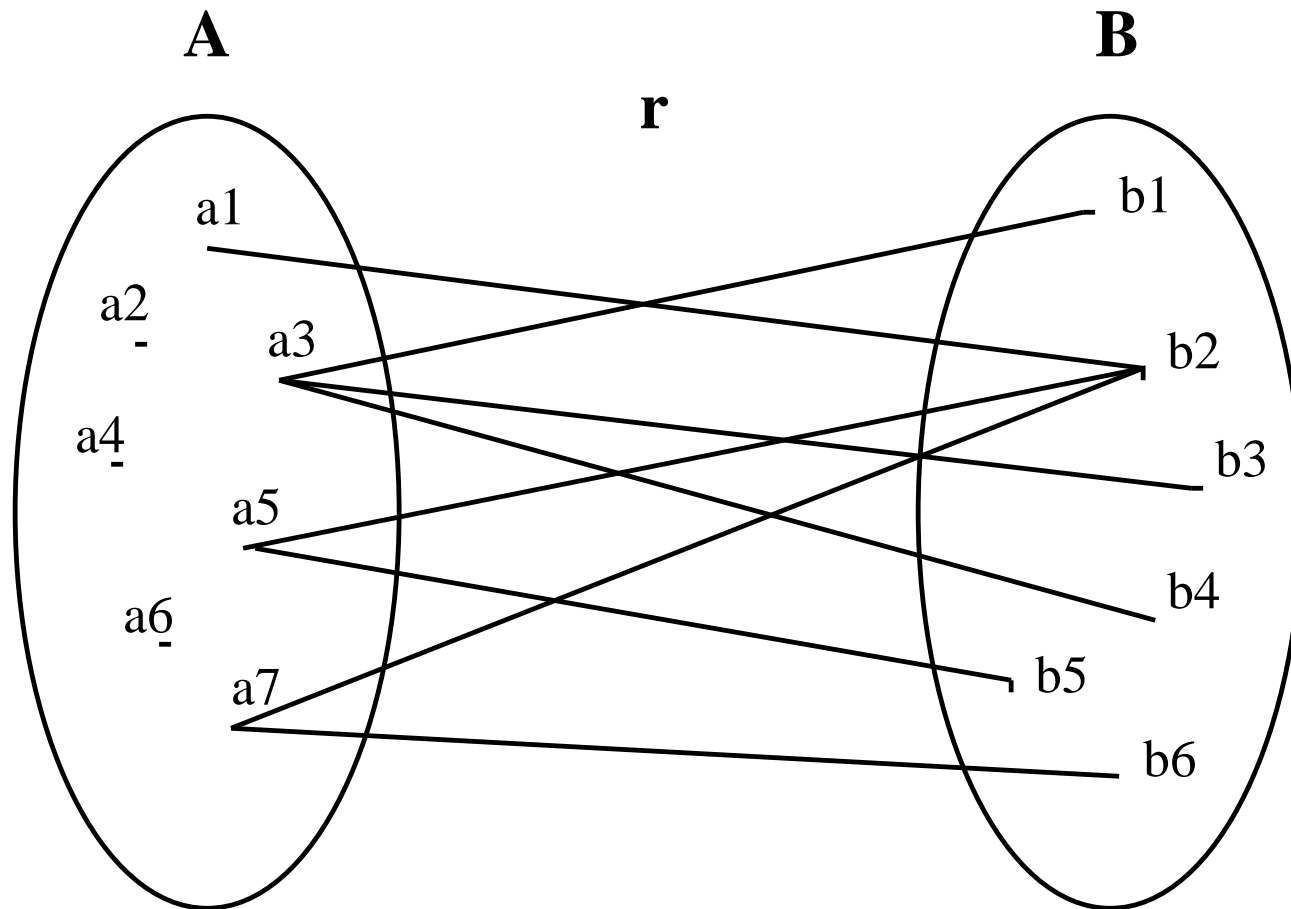
$$\text{ran}(r) = \{b_1, b_2, b_4, b_6\}$$



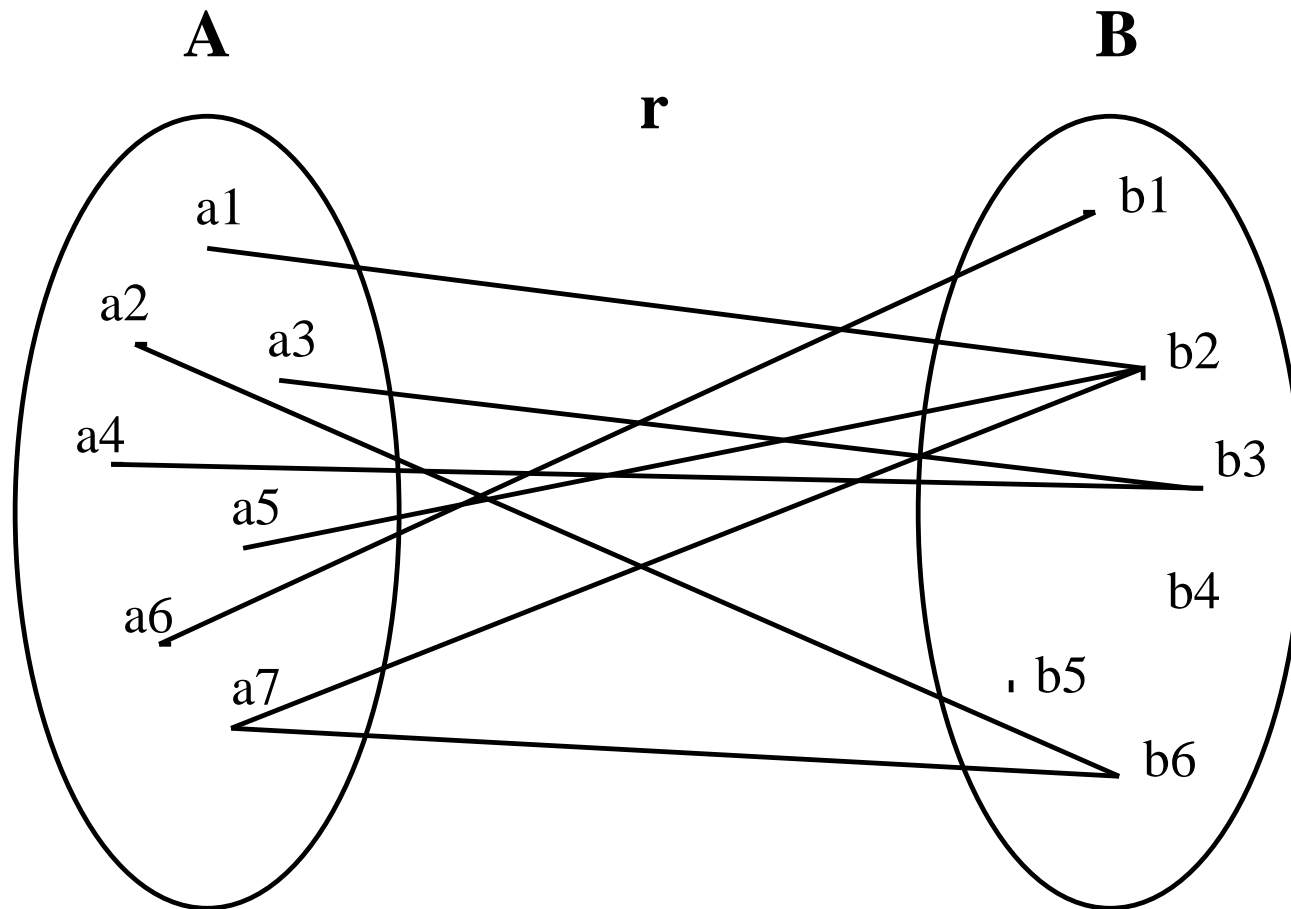
$$r^{-1} = \{b1 \mapsto a3, b2 \mapsto a1, b2 \mapsto a5, b2 \mapsto a7, b4 \mapsto a3, b6 \mapsto a7\}$$

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

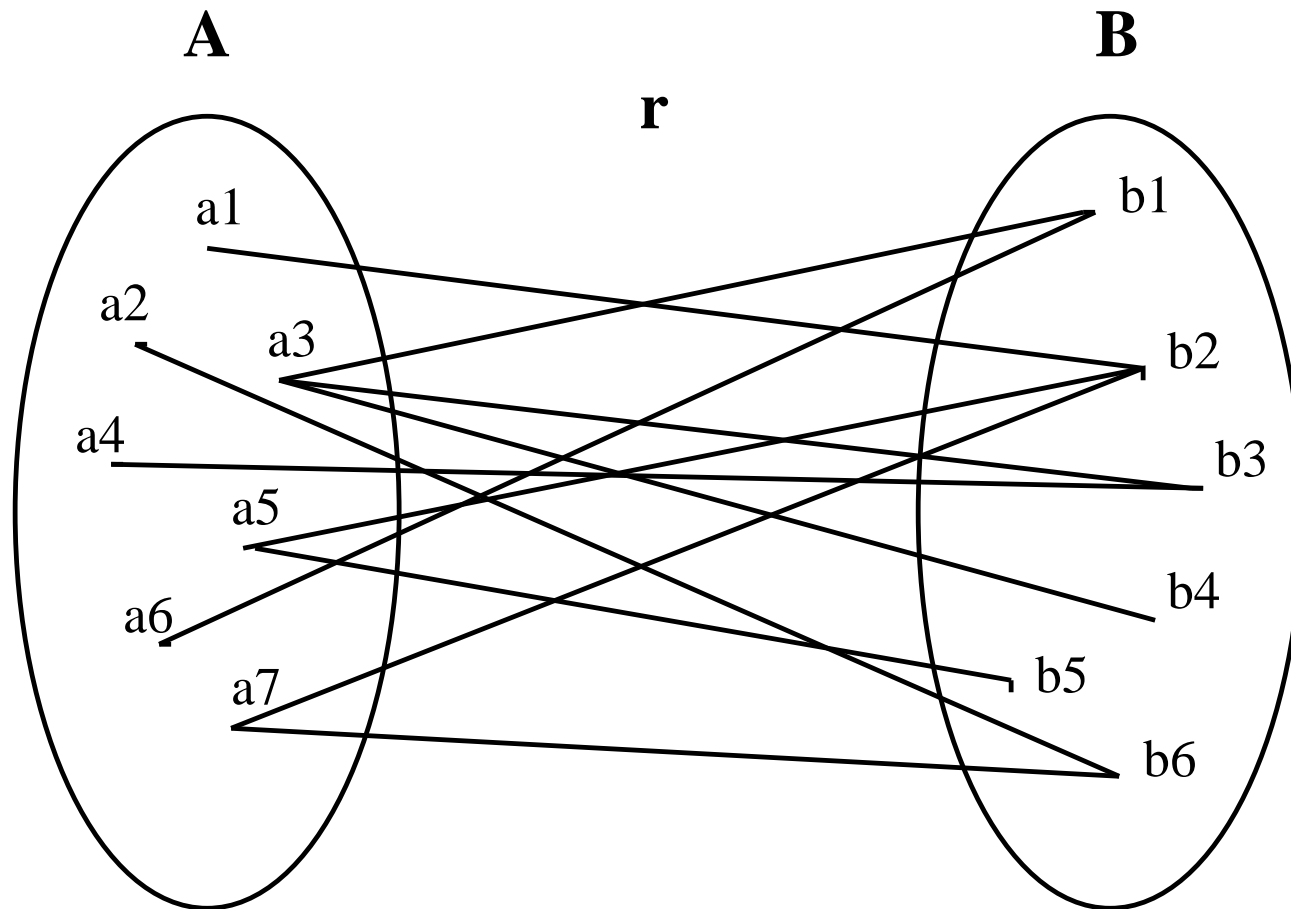
Partial surjective binary relations	$S \leftrightarrow\!\!\!\rhd T$
Total binary relations	$S \Leftrightarrow\!\!\!\rhd T$
Total surjective binary relations	$S \Leftrightarrow\!\!\!\rhd\!\!\!\rhd T$



$$r \in A \leftrightarrow B$$



$$r \in A \leftrightarrow B$$

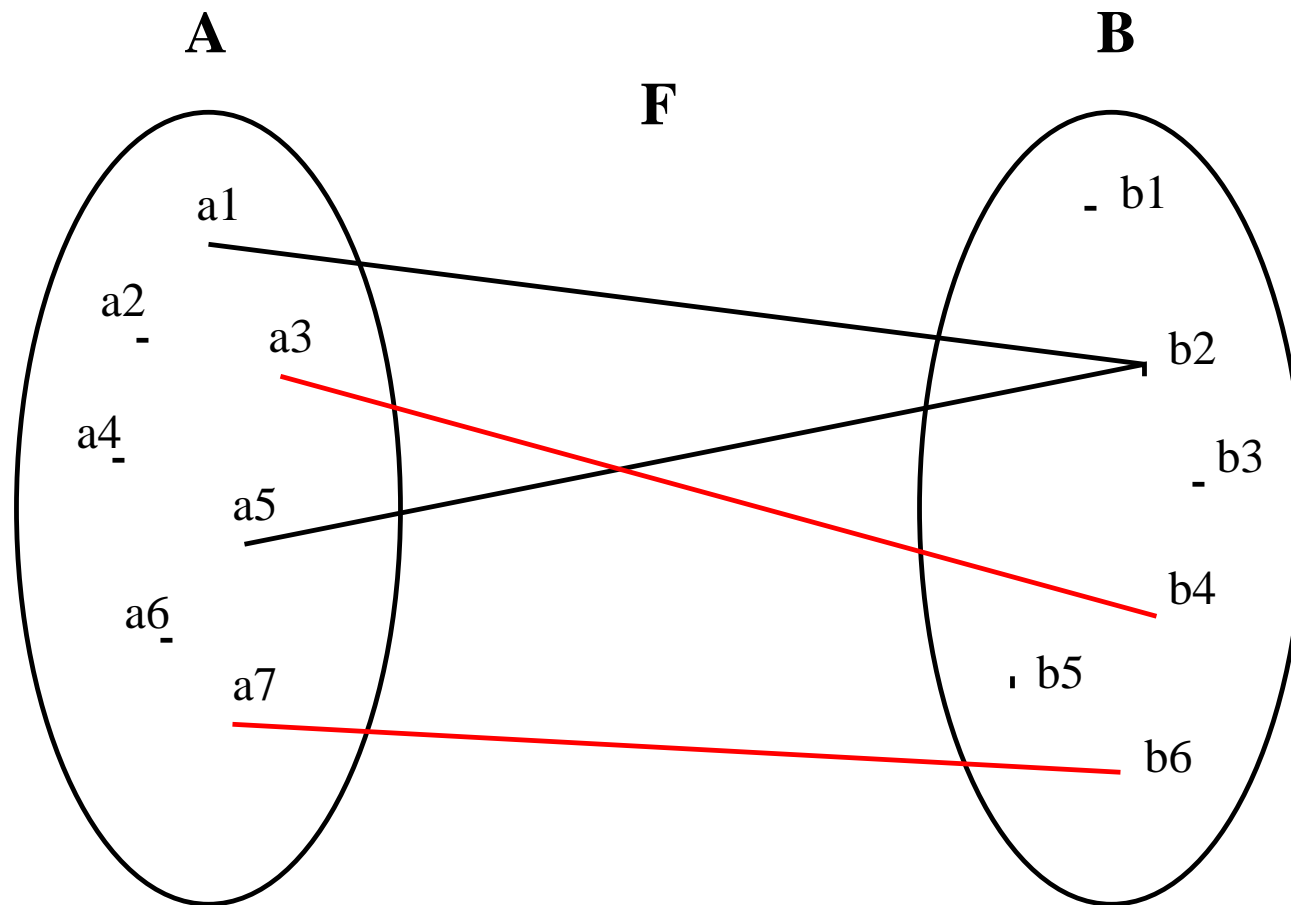


$$r \in A \leftrightarrow B$$

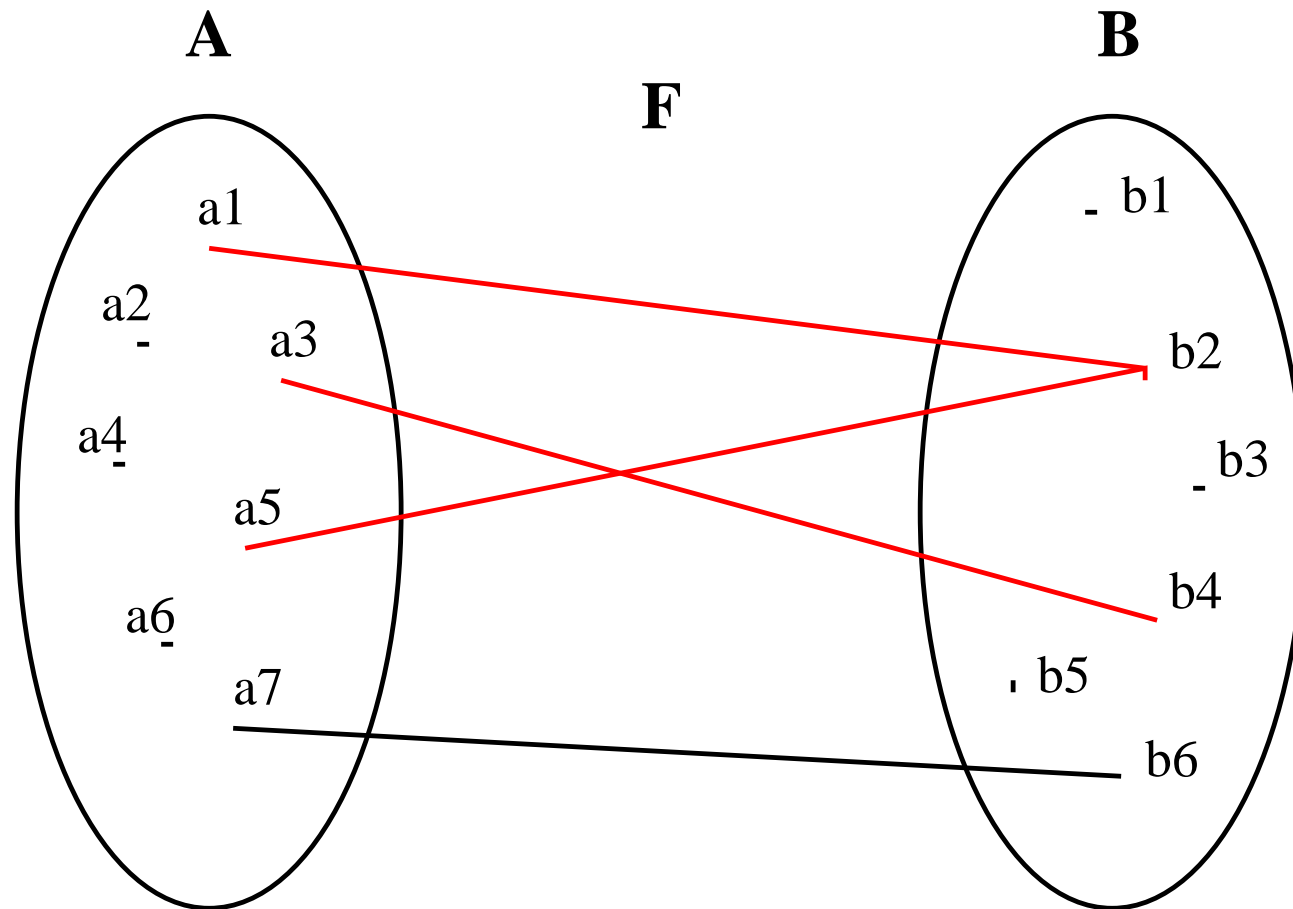
Left Part	Right Part
$r \in S \leftrightarrow\!\!\!\rightarrow T$	$r \in S \leftrightarrow T \wedge \text{ran}(r) = T$
$r \in S \leftarrow\!\!\!\rightarrow T$	$r \in S \leftrightarrow T \wedge \text{dom}(r) = T$
$r \in S \leftrightarrow\!\!\!\rightarrow T$	$r \in S \leftrightarrow\!\!\!\rightarrow T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



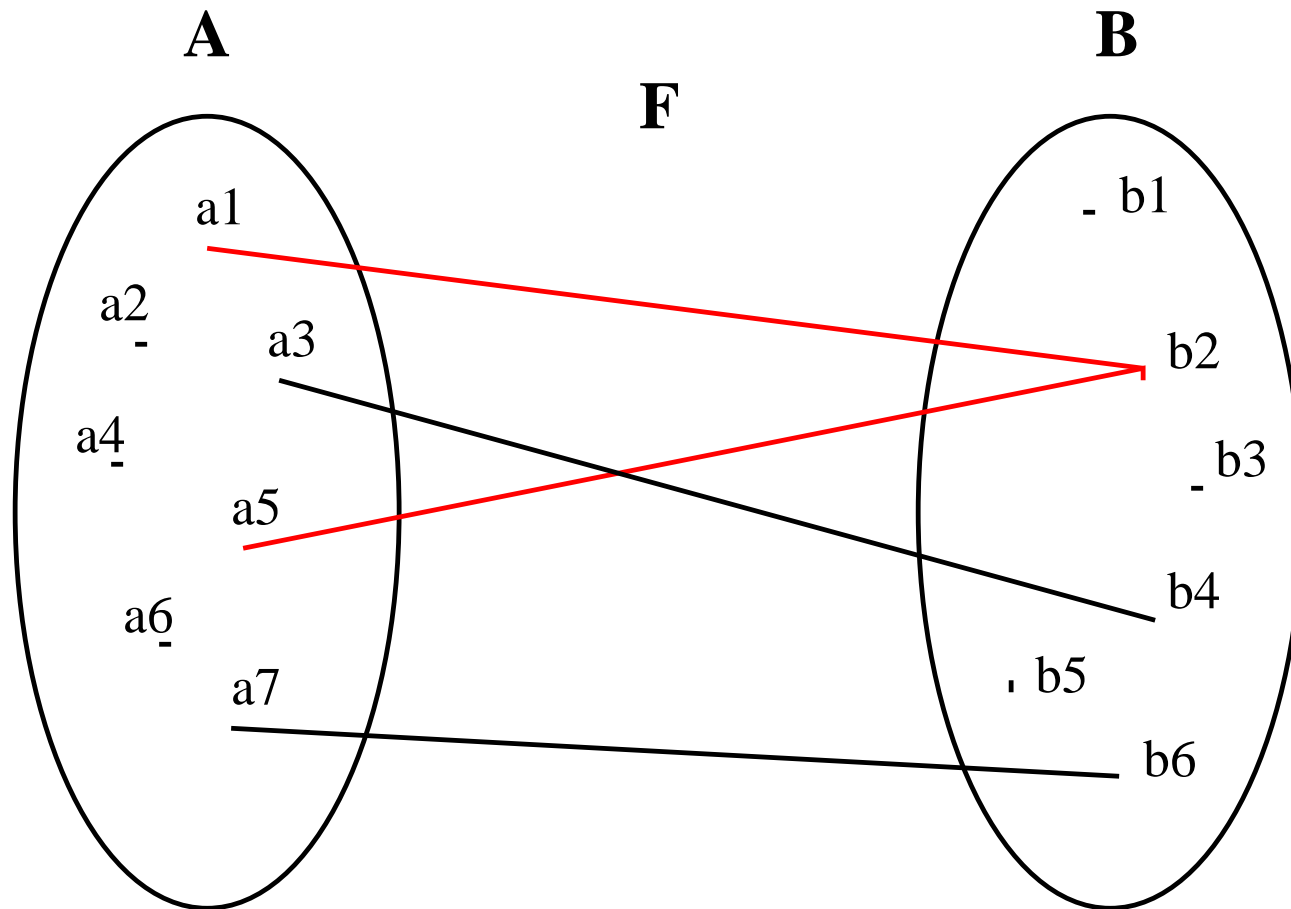
Domain restriction	$S \triangleleft r$
Range restriction	$r \triangleright T$
Domain subtraction	$S \triangleleft r$
Range subtraction	$r \triangleright T$



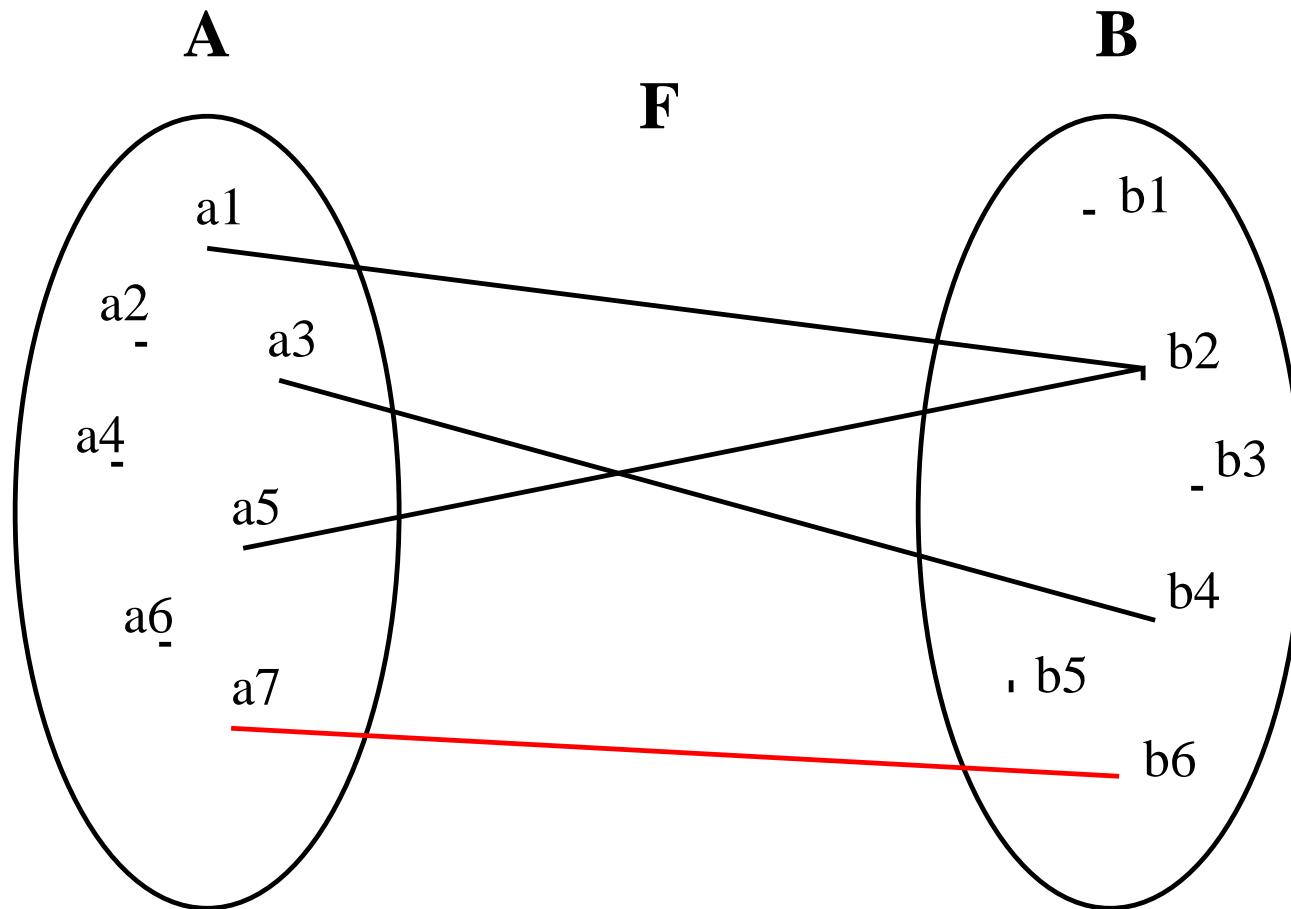
$$\{a3, a7\} \triangleleft F$$



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



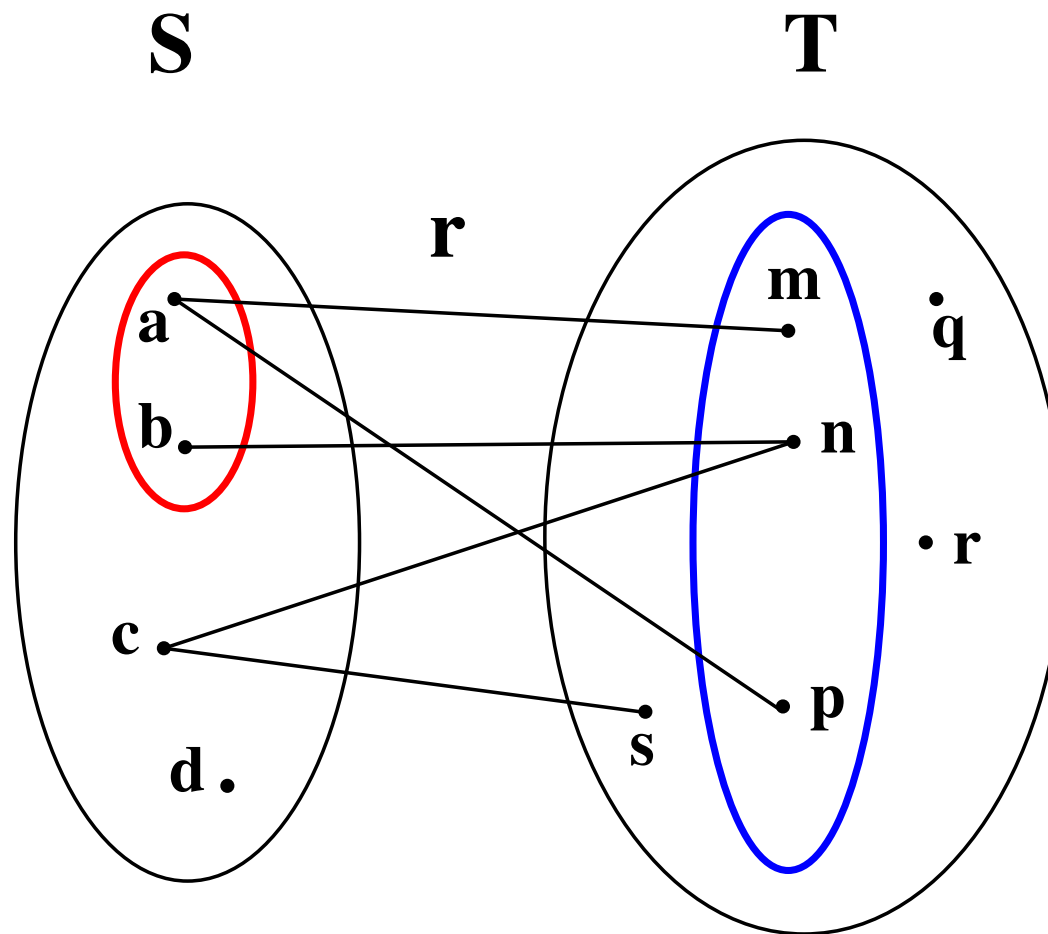
$$\{a3, a7\} \triangleleft F$$



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

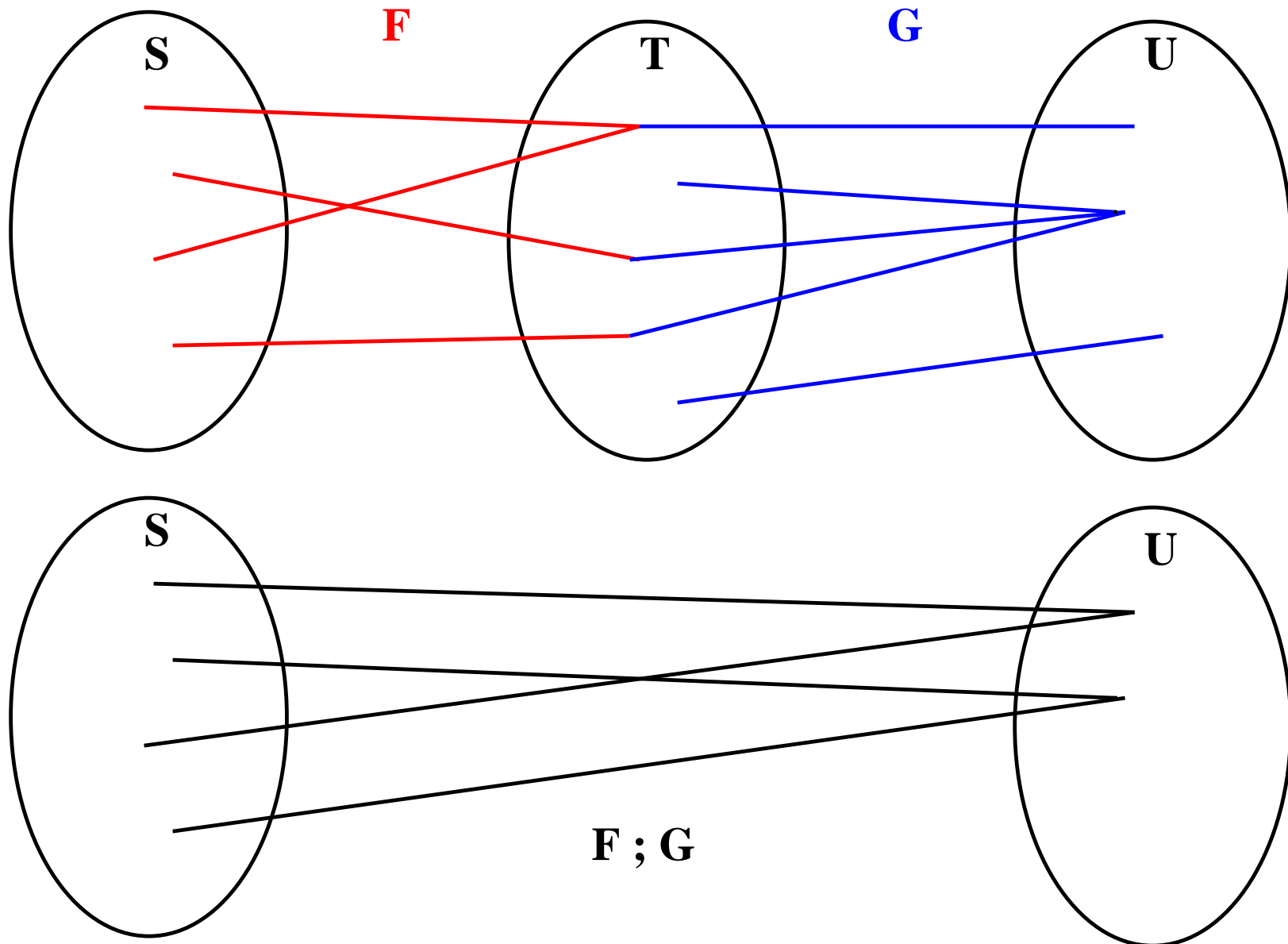
Left Part	Right Part
$E \mapsto F \in S \triangleleft r$	$E \in S \wedge E \mapsto F \in r$
$E \mapsto F \in r \triangleright T$	$E \mapsto F \in r \wedge F \in T$
$E \mapsto F \in S \triangleleft r$	$E \notin S \wedge E \mapsto F \in r$
$E \mapsto F \in r \triangleright T$	$E \mapsto F \in r \wedge F \notin T$

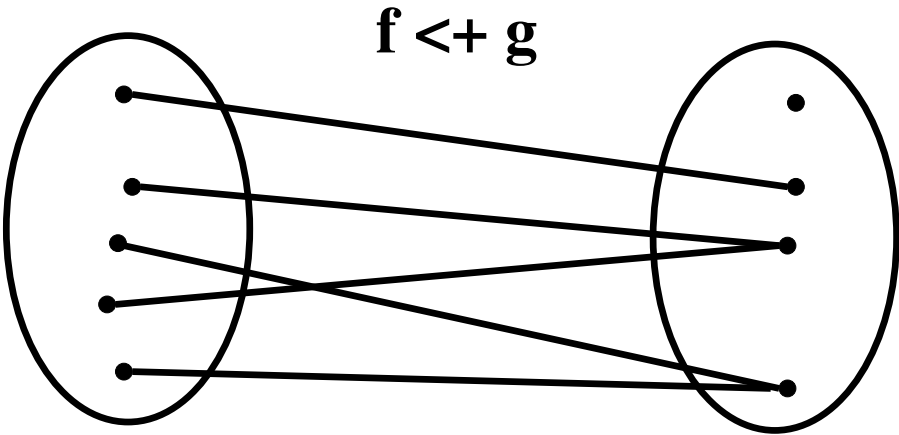
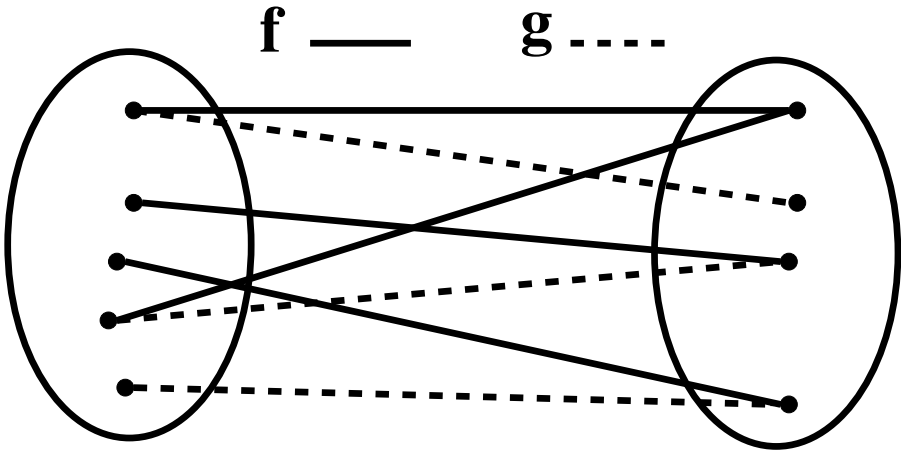
Image	$r[w]$
Composition	$p ; q$
Overriding	$p \triangleleft q$
Identity	$\text{id}(S)$

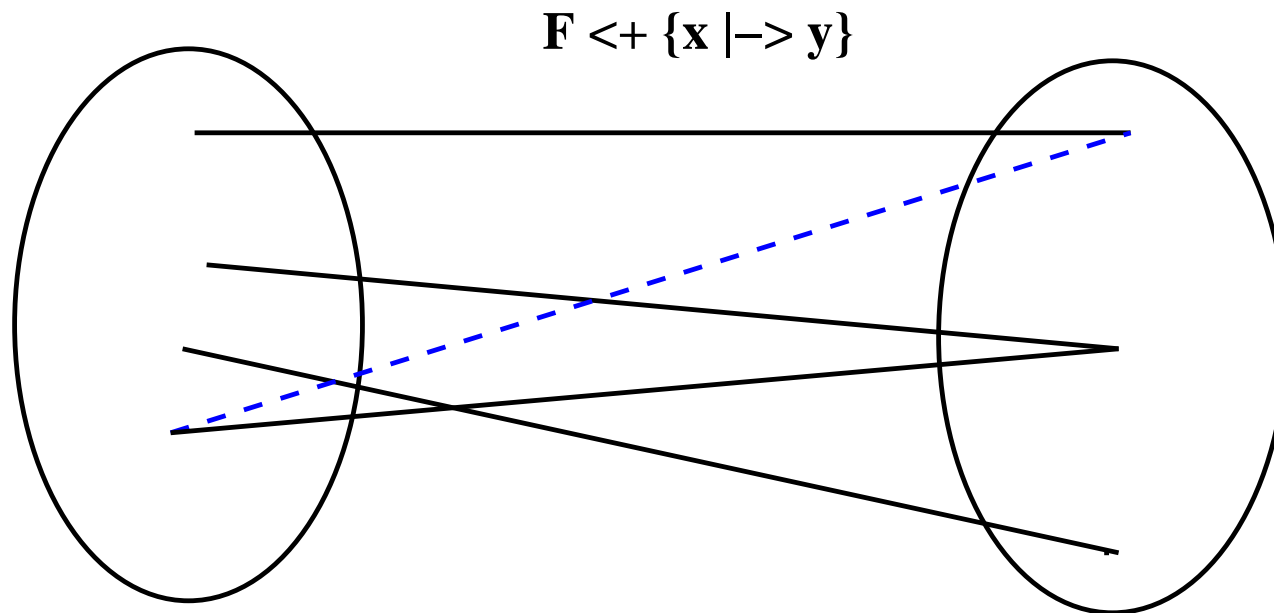
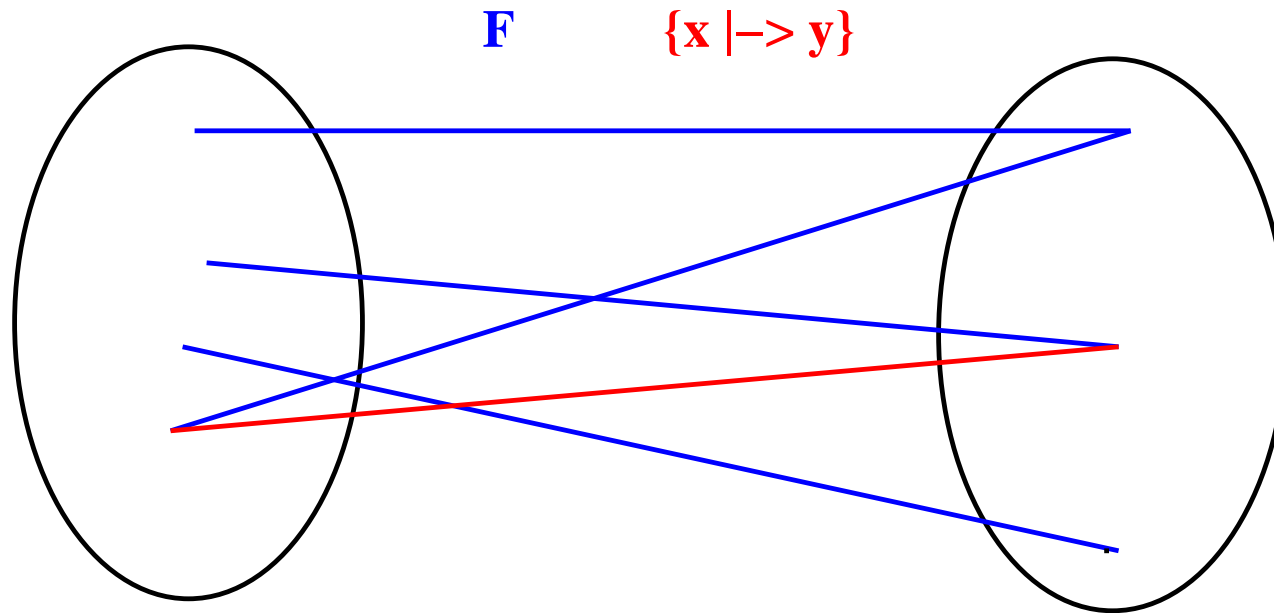


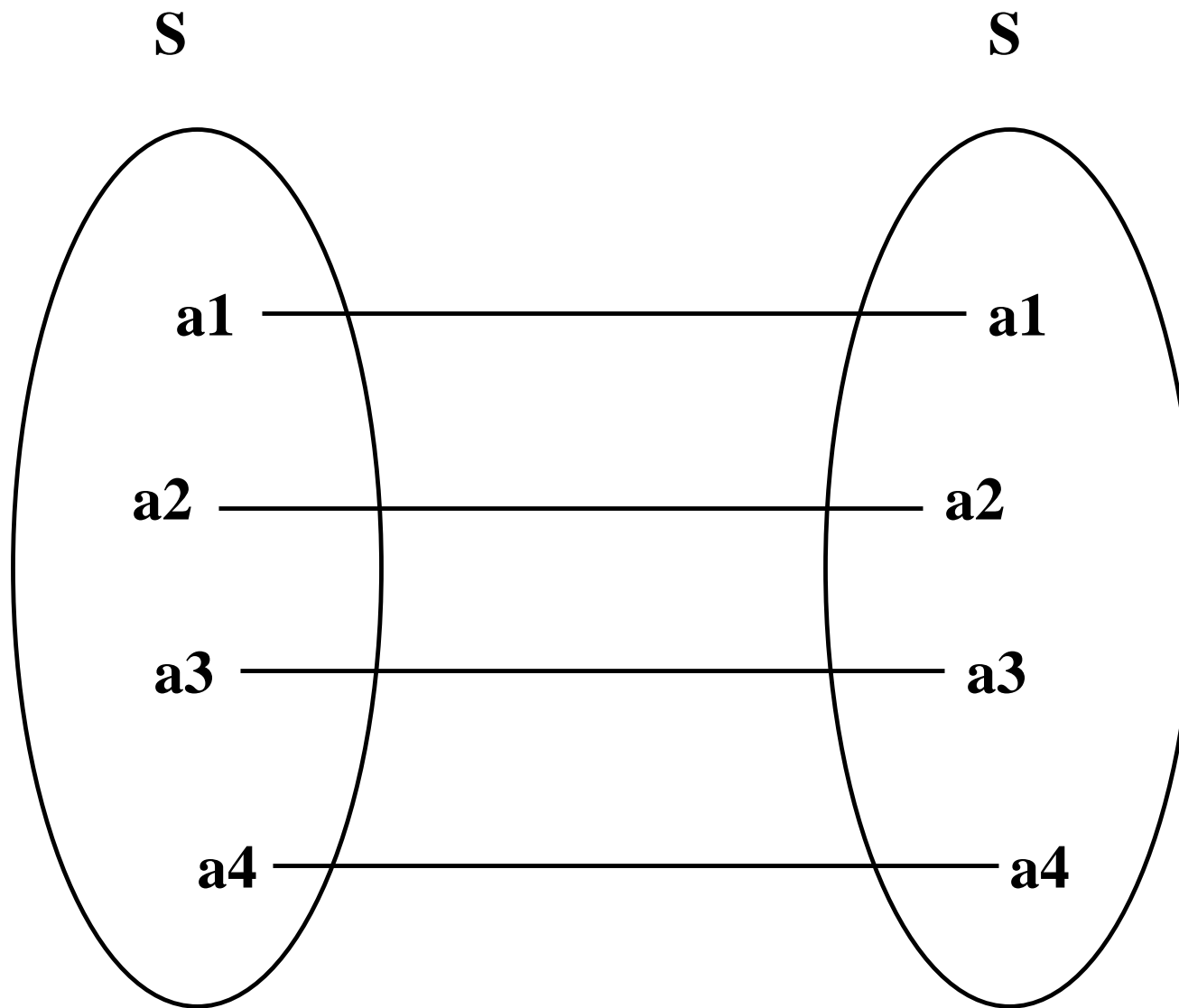
$$r[\{a, b\}] = \{m, n, p\}$$











$F \in r[w]$	$\exists x \cdot (x \in w \wedge x \mapsto F \in r)$
$E \mapsto F \in (p ; q)$	$\exists x \cdot (E \mapsto x \in p \wedge x \mapsto F \in q)$
$E \mapsto F \in p \triangleleft q$	$(\text{dom}(q) \triangleleft p) \cup q$
$E \mapsto F \in \text{id}$	$F = E$

Direct Product	$p \otimes q$
First Projection	$\text{prj}_1$
Second Projection	$\text{prj}_2$
Parallel Product	$p \parallel q$

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

$S \leftrightarrow T$	$S \triangleleft r$	$r[w]$	$\text{prj}_1$
$\text{dom}(r)$	$r \triangleright T$	$p ; q$	$\text{prj}_2$
$\text{ran}(r)$	$S \triangleleft r$	$p \triangleleft q$	$\text{id}(S)$
$r^{-1}$	$r \triangleright T$	$p \otimes q$	$p \parallel q$



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

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

$$(S \triangleleft r)^{-1} = r^{-1} \triangleright S$$

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

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

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

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

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

...

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

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

$r$  is symmetric

$$r \cap r^{-1} = \emptyset$$

$r$  is asymmetric

$$r \cap r^{-1} \subseteq \text{id}$$

$r$  is antisymmetric

$$\text{id} \subseteq r$$

$r$  is reflexive

$$r \cap \text{id} = \emptyset$$

$r$  is irreflexive

$$r; r \subseteq r$$

$r$  is transitive

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

$$r = r^{-1} \quad \forall x, y \cdot x \in S \wedge y \in S \Rightarrow (x \mapsto y \in r \Leftrightarrow y \mapsto x \in r)$$

$$r \cap r^{-1} = \emptyset \quad \forall x, y \cdot x \mapsto y \in r \Rightarrow y \mapsto x \notin r$$

$$r \cap r^{-1} \subseteq \text{id} \quad \forall x, y \cdot x \mapsto y \in r \wedge y \mapsto x \in r \Rightarrow x = y$$

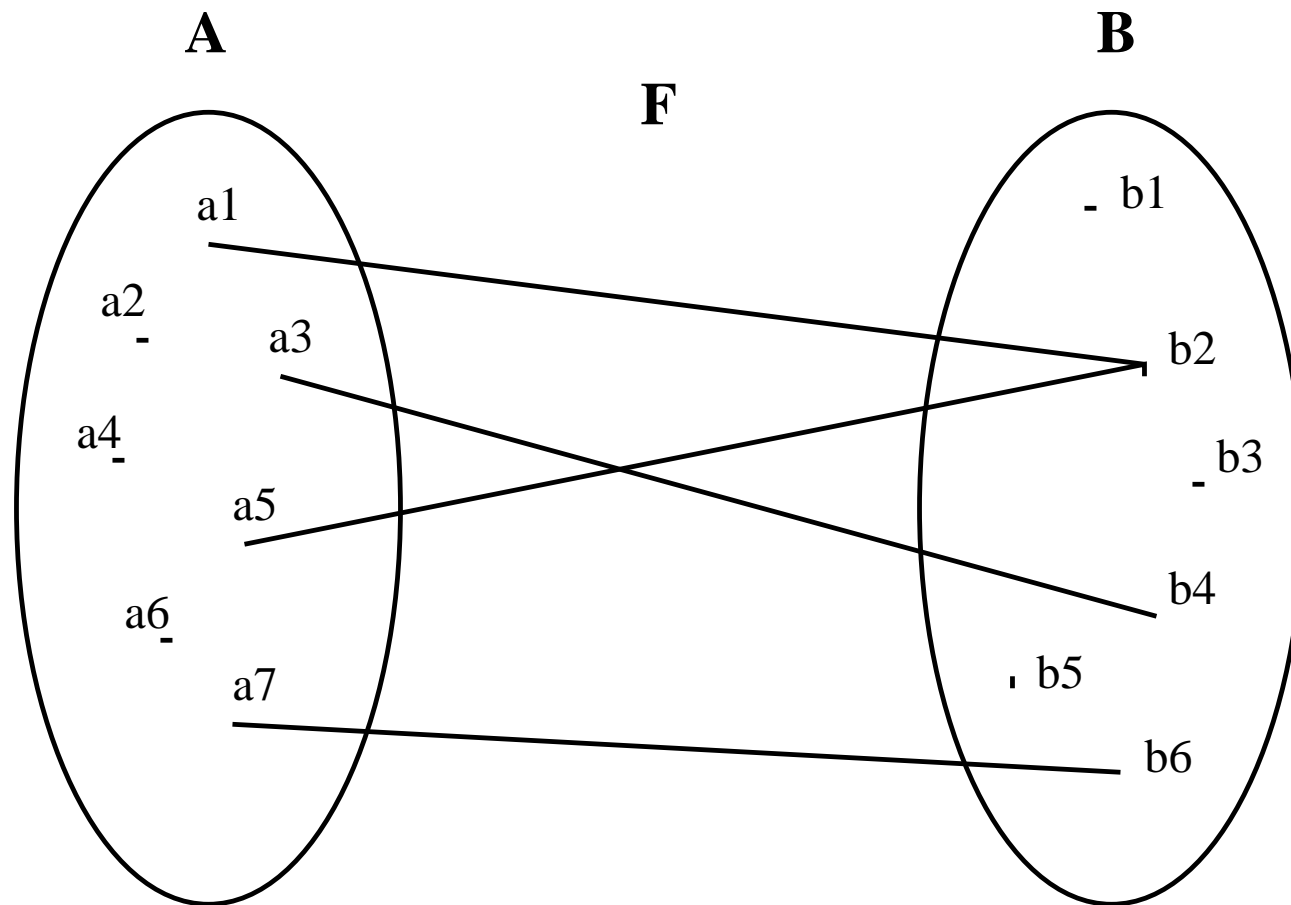
$$\text{id} \subseteq r \quad \forall x \cdot x \in S \Rightarrow x \mapsto x \in r$$

$$r \cap \text{id} = \emptyset \quad \forall x, y \cdot x \mapsto y \in r \Rightarrow x \neq y$$

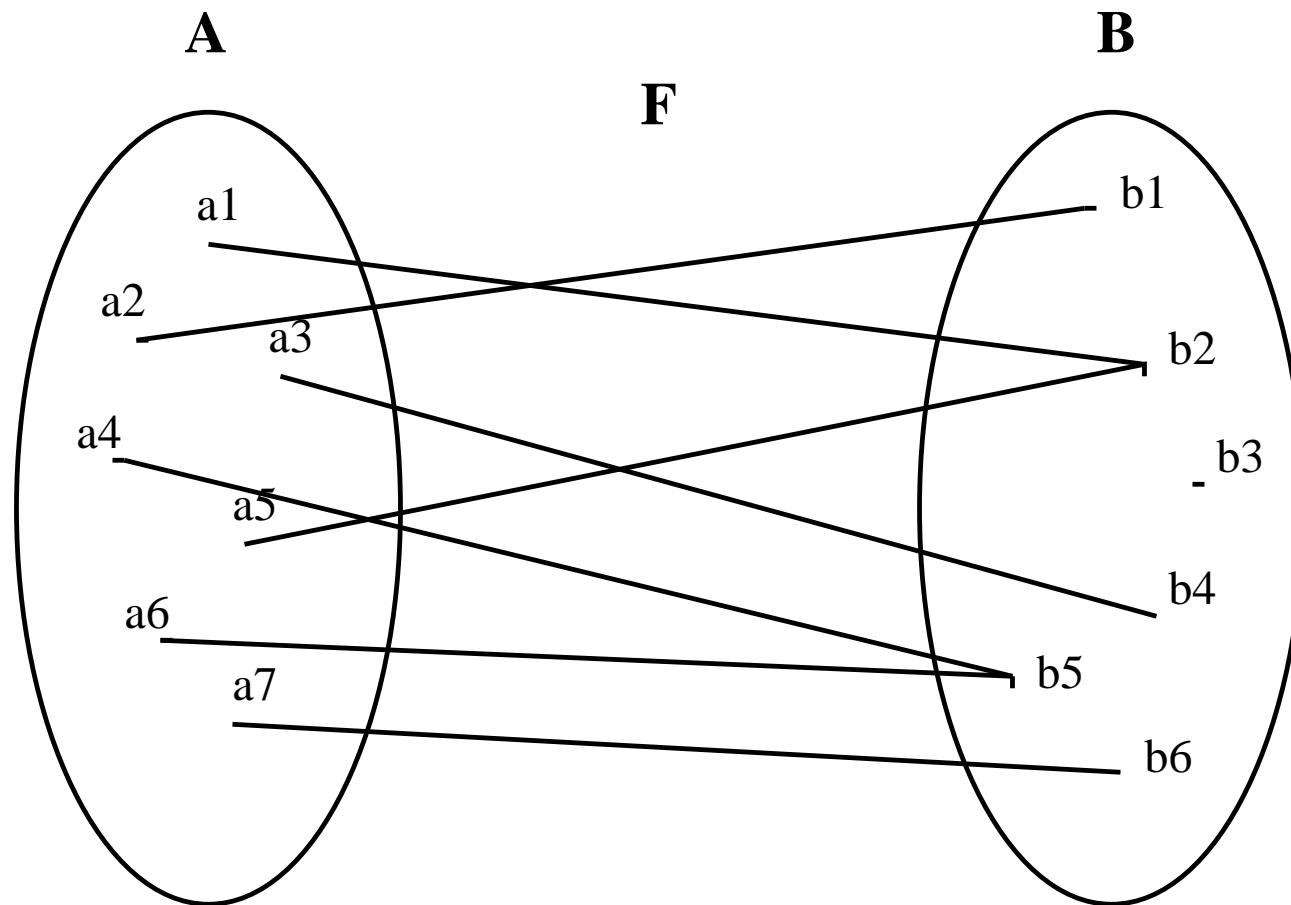
$$r; r \subseteq r \quad \forall x, y, z \cdot x \mapsto y \in r \wedge y \mapsto z \in r \Rightarrow x \mapsto z \in r$$

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

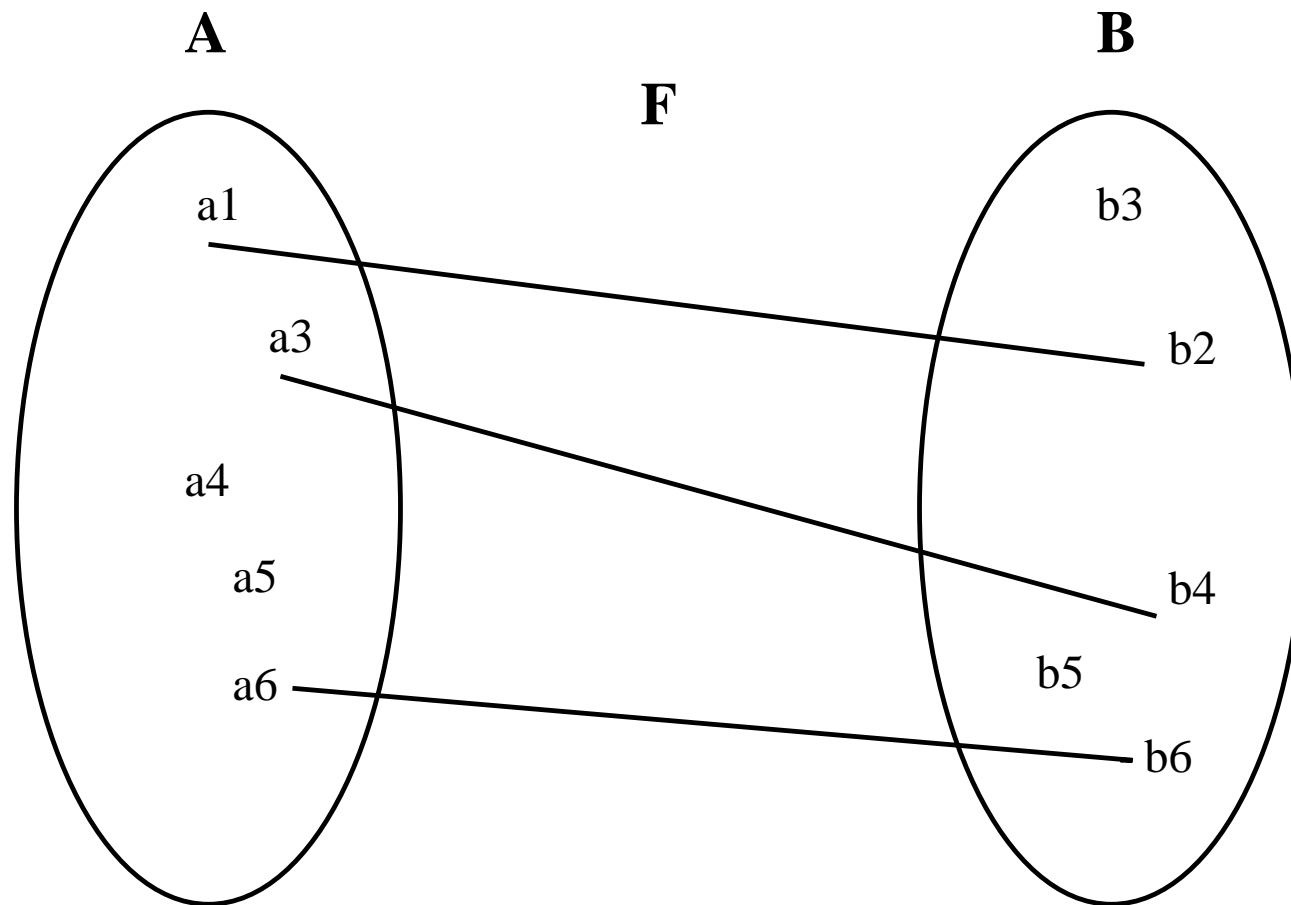
Partial functions	$S \rightarrowtail T$
Total functions	$S \rightarrow T$
Partial injections	$S \rightarrowtail\!\!\rightarrow T$
Total injections	$S \rightarrow\!\!\rightarrow T$



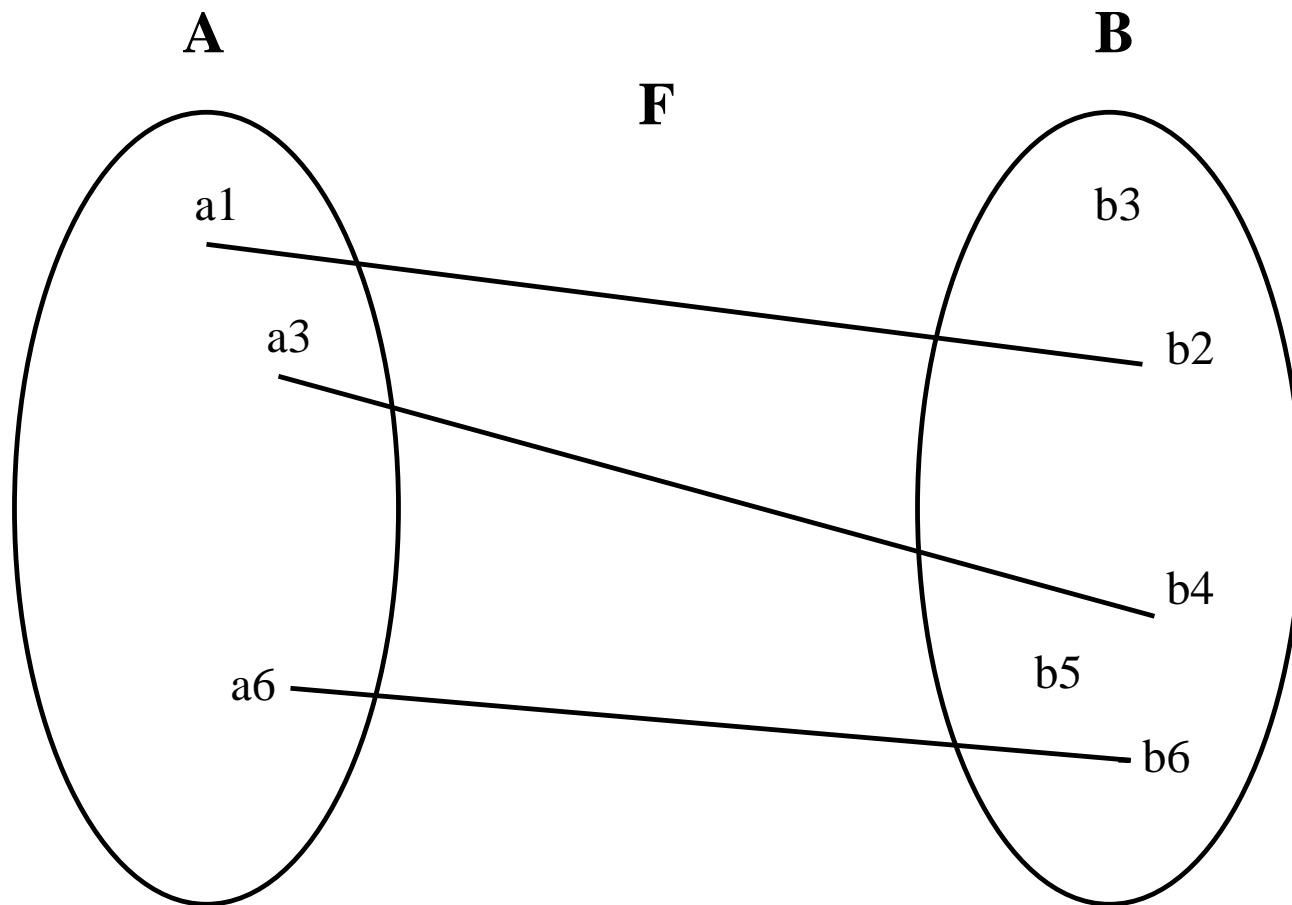
$$F \in A \rightarrowtail B$$



$$F \in A \rightarrow B$$



$$F \in A \rightarrowtail B$$



$$F \in A \rightarrow B$$



Left Part	Right Part
$f \in S \twoheadrightarrow T$	$f \in S \leftrightarrow T \quad \wedge \quad (f^{-1} ; f) = \text{id}(\text{ran}(f))$
$f \in S \rightarrow T$	$f \in S \twoheadrightarrow T \quad \wedge \quad s = \text{dom}(f)$
$f \in S \rightharpoonup T$	$f \in S \twoheadrightarrow T \quad \wedge \quad f^{-1} \in T \twoheadrightarrow S$
$f \in S \rightharpoonrightarrow T$	$f \in S \rightarrow T \quad \wedge \quad f^{-1} \in T \twoheadrightarrow S$

- The predicate:

$$f^{-1} ; f \subseteq \text{id}$$

- 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:

$$f^{-1} ; f \subseteq \text{id}$$

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

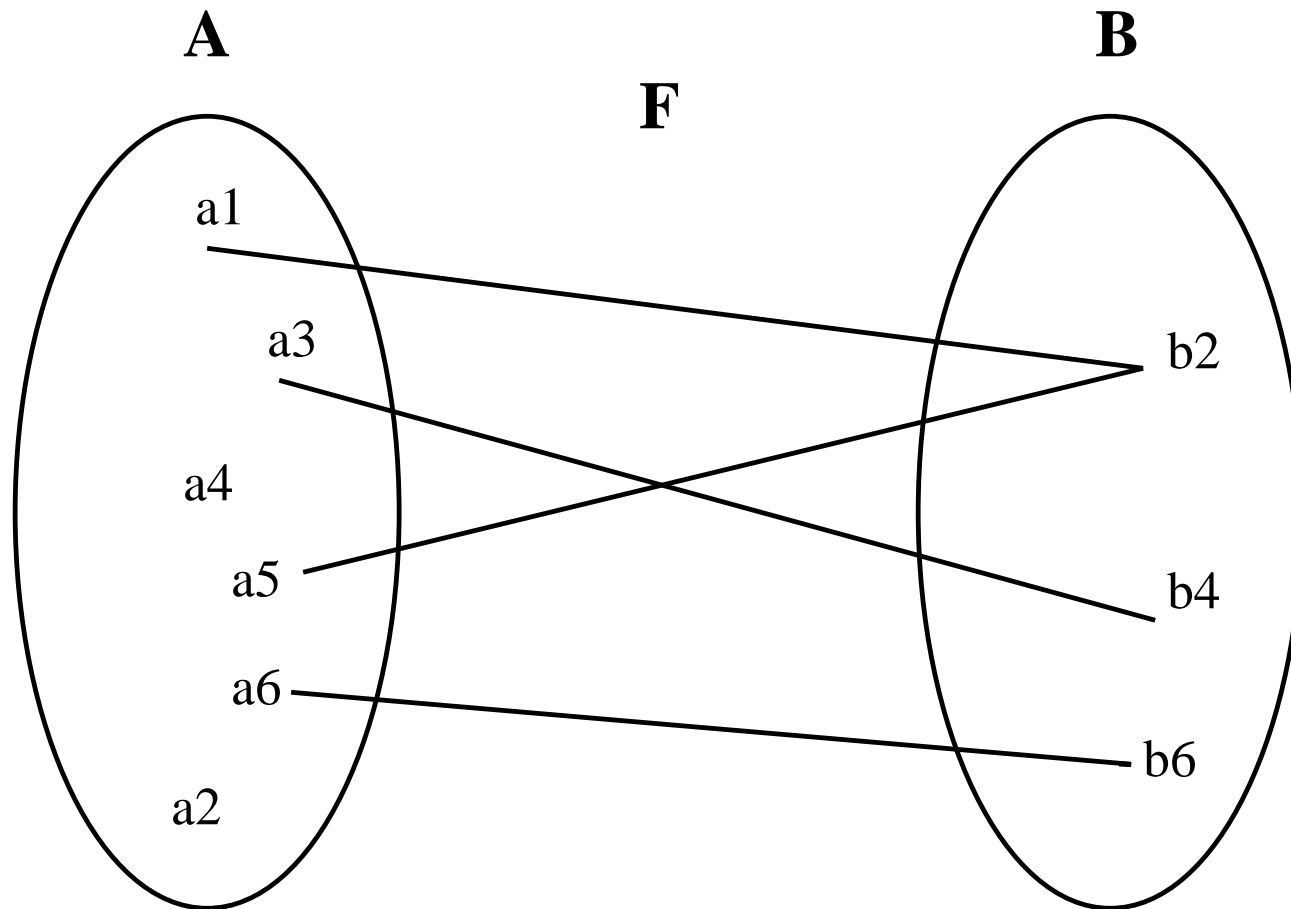
$$\forall y, z \cdot y \mapsto z \in (f^{-1} ; f) \Rightarrow y = z$$

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

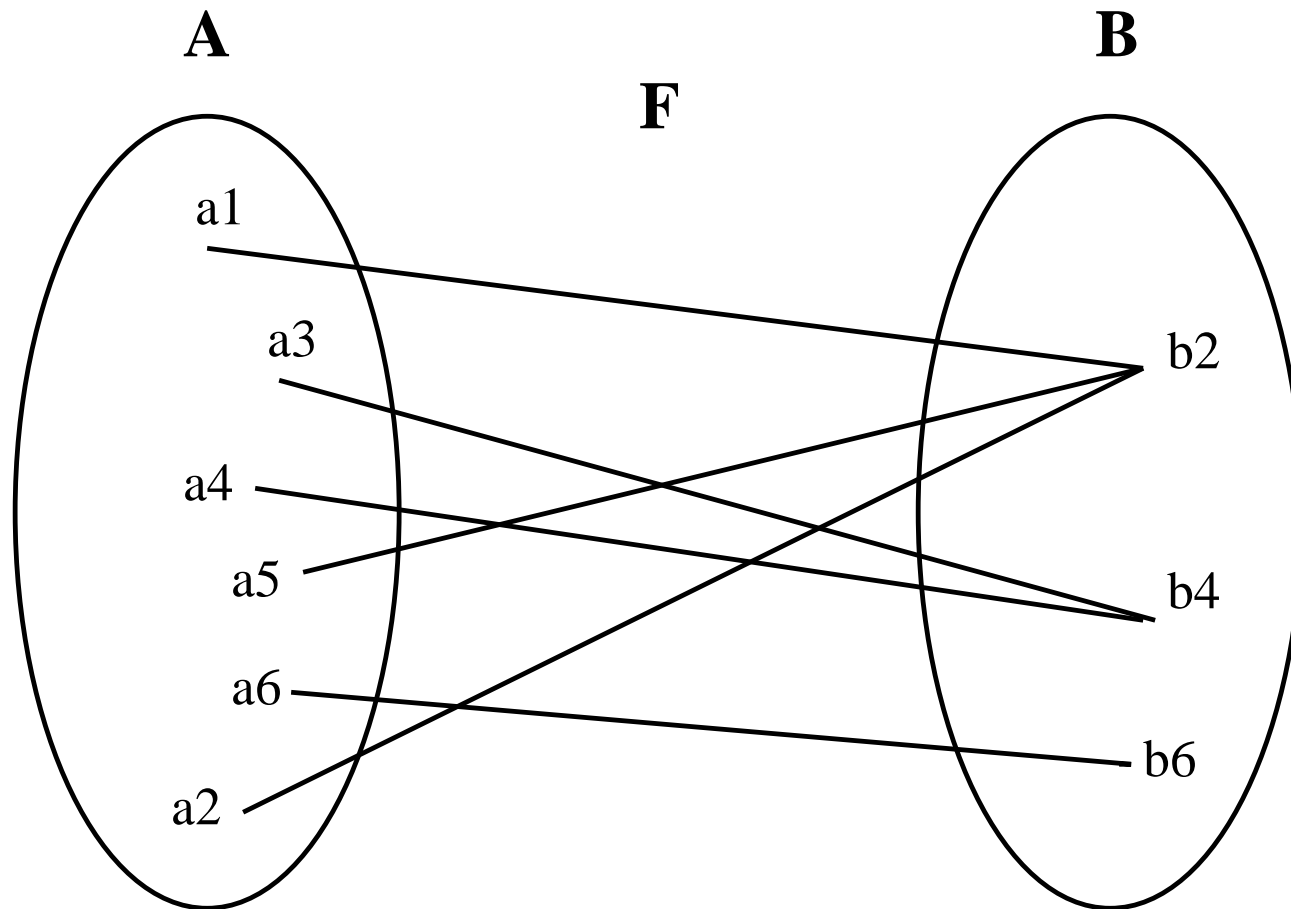
$$\forall y, z \cdot (\exists x \cdot x \mapsto y \in f \wedge x \mapsto z \in f) \Rightarrow y = z$$

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

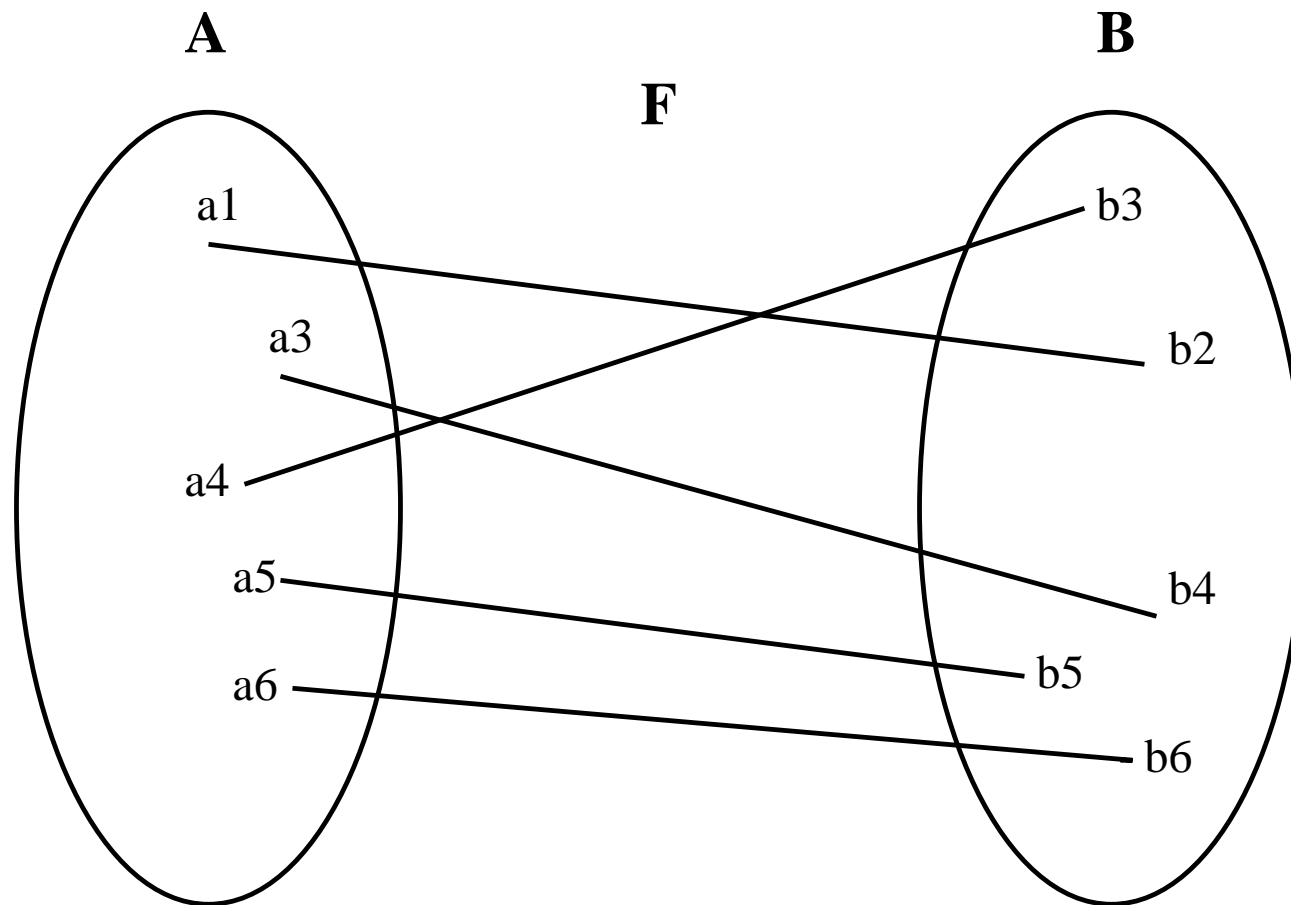
Partial surjections	$S \twoheadrightarrow T$
Total surjections	$S \rightarrow T$
Bijections	$S \xrightarrow{\sim} T$



$$F \in A \rightarrow B$$



$$F \in A \twoheadrightarrow B$$



$$F \in A \rightarrow B$$

Left Part	Right Part
$f \in S \dashv\!\!\rightarrow T$	$f \in S \rightarrow T \quad \wedge \quad T = \text{ran}(f)$
$f \in S \twoheadrightarrow T$	$f \in S \rightarrow T \quad \wedge \quad T = \text{ran}(f)$
$f \in S \rightrightarrows T$	$f \in S \rightarrow T \quad \wedge \quad f \in S \twoheadrightarrow T$

$S \rightarrowtail T$	$S \dashrightarrowtail T$
$S \rightarrow T$	$S \dashrightarrow T$
$S \rightharpoonuptail T$	$S \dashrightarrowtail T$
$S \rightharpoonup T$	



$S \times T$	$S \setminus T$	$r^{-1}$	$r[w]$	id	$\{x \mid x \in S \wedge P\}$
$\mathbb{P}(S)$	$S \leftrightarrow T$ $S \leftrightarrow\!\!\!\rightarrow T$	$S \triangleleft r$ $S \triangleleft\!\!\! r$	$p ; q$	$S \twoheadrightarrow T$ $S \rightarrow T$	$\{x \cdot x \in S \wedge P \mid E\}$
$S \subseteq T$	$S \leftrightarrow\!\!\!\rightarrow T$ $S \leftrightarrow T$	$r \triangleright T$ $r \triangleright\!\!\! T$	$p \triangleleft q$	$S \twoheadleftarrow T$ $S \rightarrow\!\!\! T$	$\{a, b, \dots, n\}$
$S \cup T$	dom $(r)$ ran $(r)$	prj <sub>1</sub>	$p \otimes q$	$S \twoheadrightarrow\!\!\! T$ $S \rightarrow\!\!\! T$	union $\cup$
$S \cap T$	$\emptyset$	prj <sub>2</sub>	$p \parallel q$	$S \twoheadrightarrow\!\!\! T$	inter $\cap$

Given a **partial function**  $f$ , we have

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

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

- 
- 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)

- 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  $V \setminus \{f\}$ .

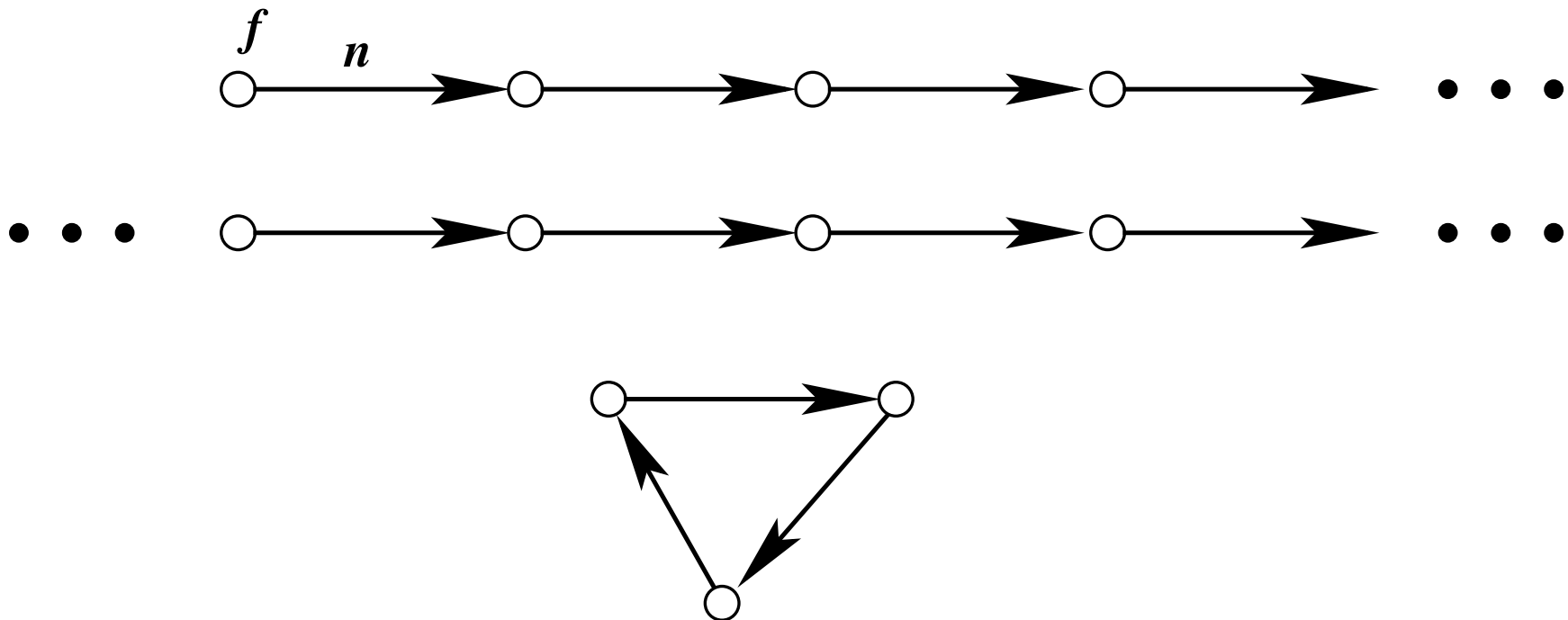


This can be formalized as follows:

$$\text{axm\_1 : } f \in V$$

$$\text{axm\_2 : } n \in V \mapsto V \setminus \{f\}$$

- However, **axm\_1** and **axm\_2** are not sufficient
- We must say that there are:
  - no cycles
  - no 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  $n^{-1}$ .

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

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

$$S \subseteq n[S]$$

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

$$\text{axm\_3 : } \forall S \cdot S \subseteq n[S] \Rightarrow S = \emptyset$$



axm\_1 :  $f \in V$

axm\_2 :  $n \in V \rightsquigarrow V \setminus \{f\}$

axm\_3 :  $\forall S \cdot S \subseteq n[S] \Rightarrow S = \emptyset$

- From axm\_3

$$\text{axm\_3} : \quad \forall S \cdot S \subseteq n[S] \Rightarrow S = \emptyset$$

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

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

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

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



- 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:  $V = \{x \mid x \in V \wedge P(x)\}$
- For this, we instantiate  $T$  with  $\{x \mid x \in V \wedge P(x)\}$  in **thm\_2**:

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

- This requires proving successively:

$$P(f)$$

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



$$\text{axm\_1 : } f \in V$$

$$\text{axm\_2 : } n \in V \mapsto V \setminus \{f\}$$

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

$$\text{axm\_1 : } 0 \in \mathbb{N}$$

$$\text{axm\_2 : } succ \in \mathbb{N} \mapsto \mathbb{N} \setminus \{0\}$$

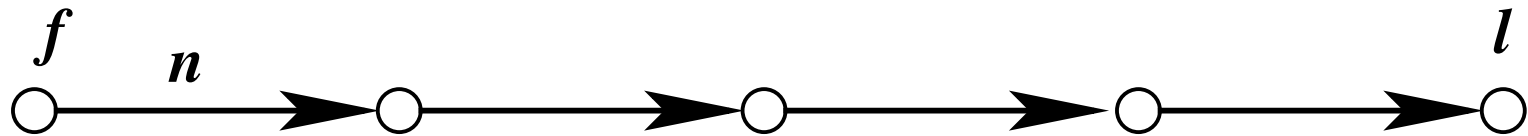
This corresponds to the **four first Peano Axioms**



$$\text{thm\_2 : } \forall T . f \in T \wedge (\forall x . x \in T \Rightarrow n(x) \in T) \Rightarrow V = T$$

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

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



- Here are the axioms of finite lists

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

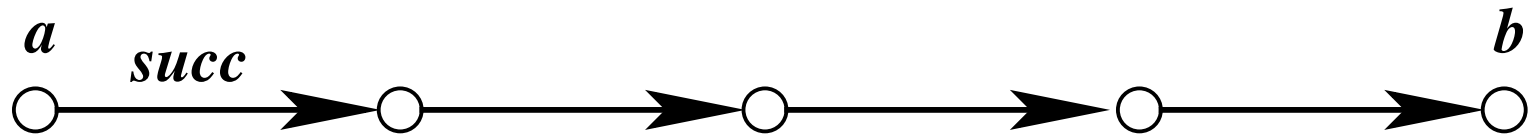
$$\mathbf{axm\_2} : l \in V$$

$$\mathbf{axm\_3} : n \in V \setminus \{l\} \rightsquigarrow V \setminus \{f\}$$

$$\mathbf{axm\_4} : \forall S \cdot S \subseteq n[S] \Rightarrow S = \emptyset$$

- 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.

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



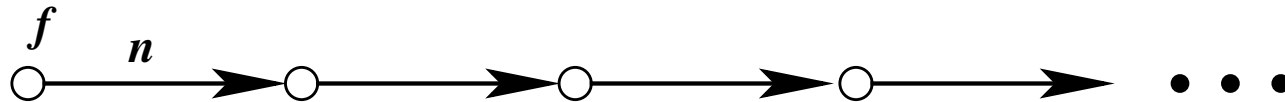
It is easy to prove the following:

$$a \in a .. b$$

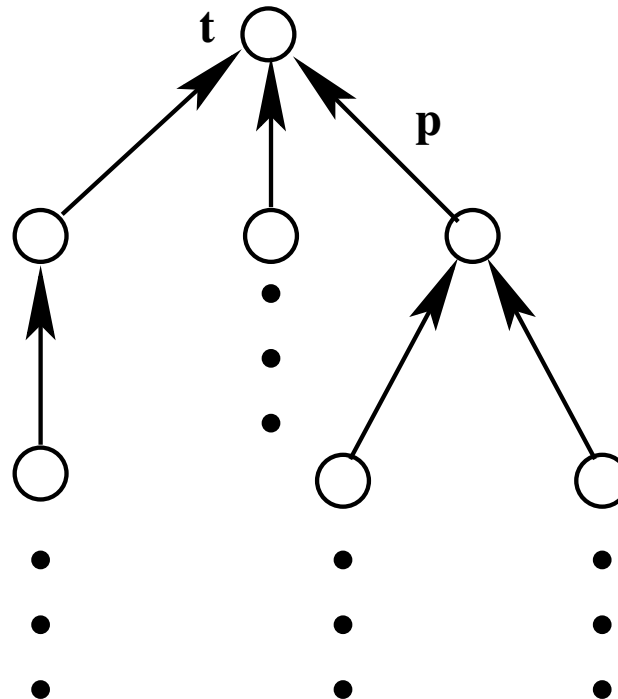
$$b \in a .. b$$

$$(a .. b - 1) \triangleleft succ \in (a .. b) \setminus \{b\} \rightsquigarrow (a .. b) \setminus \{a\}$$

- 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



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

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

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

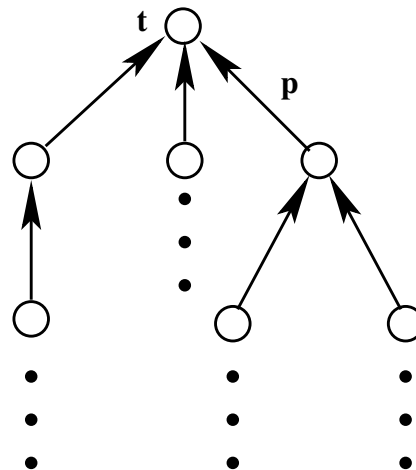
We define an **induction rule** which generalise that of infinite lists.

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

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

**thm\_1** can be further unfolded to the following equivalent one:

$$\begin{aligned} \text{thm\_2: } \quad & \forall T \cdot t \in T \\ & \forall x \cdot x \in V \setminus \{t\} \wedge p(x) \in T \Rightarrow x \in T \\ & \Rightarrow \\ & V = T \end{aligned}$$

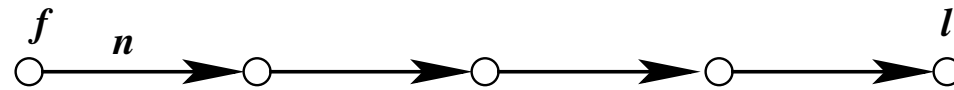




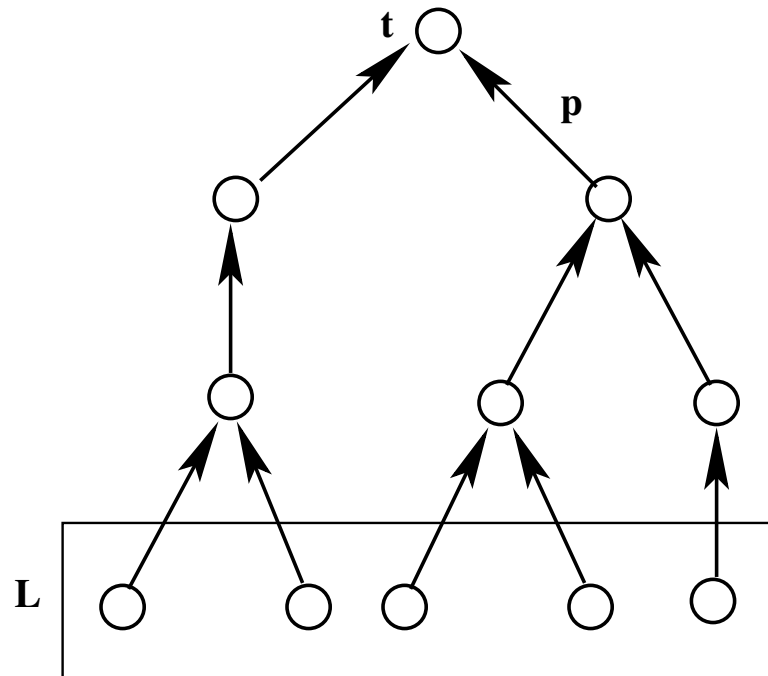
$$\begin{aligned} & p^{-1}[T] \subseteq T \\ \Leftrightarrow & \\ & \forall x \cdot x \in p^{-1}[T] \Rightarrow x \in T \\ \Leftrightarrow & \\ & \forall x \cdot (\exists y \cdot y \in T \wedge x \mapsto y \in p) \Rightarrow x \in T \\ \Leftrightarrow & \\ & \forall x \cdot (\exists y \cdot y \in T \wedge x \in \text{dom}(p) \wedge y = p(x)) \Rightarrow x \in T \\ \Leftrightarrow & \\ & \forall x \cdot x \in V \setminus \{t\} \wedge p(x) \in T \Rightarrow x \in T \end{aligned}$$

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

- 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**.

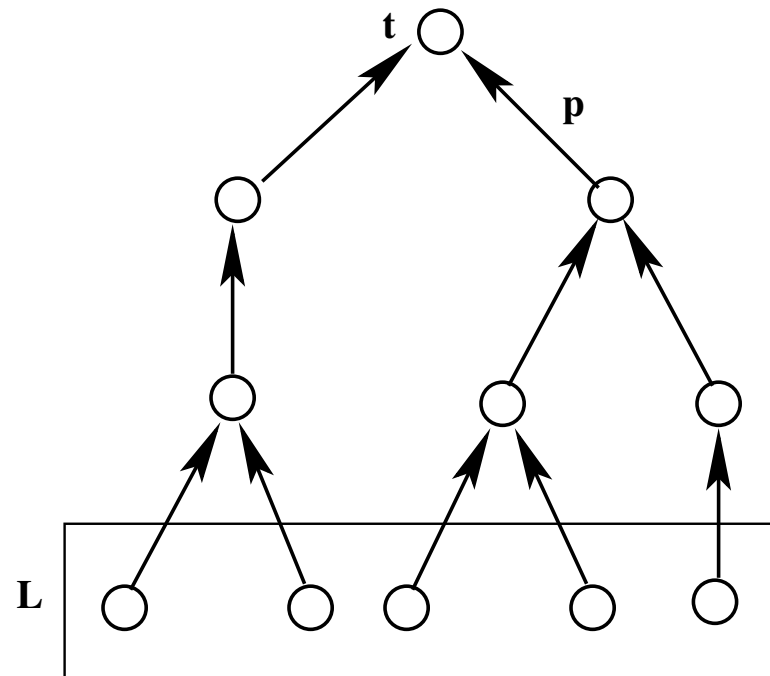


$$\text{axm\_1 : } t \in V$$

$$\text{axm\_2 : } L \subseteq V$$

$$\text{axm\_3 : } p \in V \setminus \{t\} \rightarrow V \setminus L$$

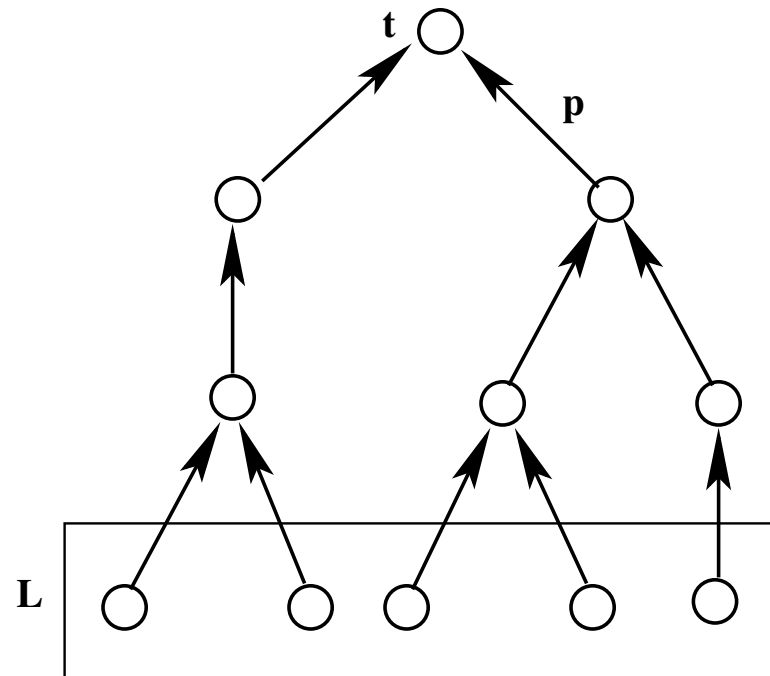
$$\text{axm\_4 : } \forall S \cdot S \subseteq p^{-1}[S] \Rightarrow S = \emptyset$$



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

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

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



Let  $a$ ,  $b$  and  $c$  be three binary relations:

$$a \in S \leftrightarrow T$$

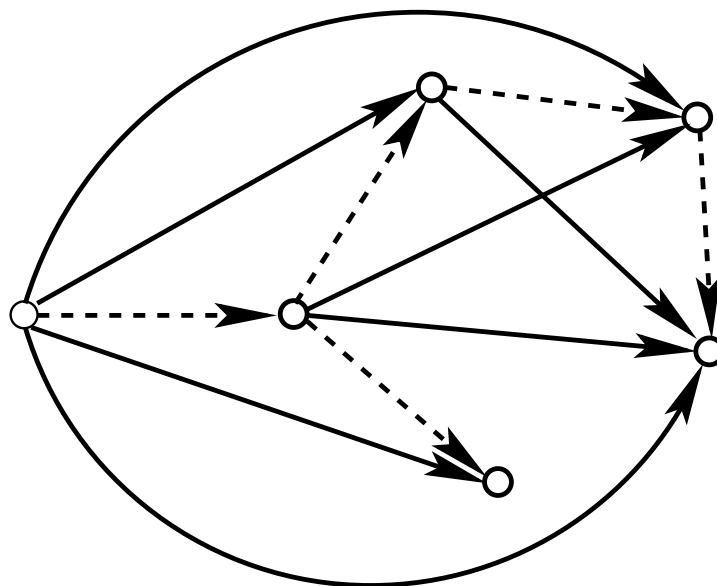
$$b \in T \leftrightarrow U$$

$$c \in S \leftrightarrow U$$

We have then the following theorem:

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

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



$$\text{axm\_1 : } r \in S \leftrightarrow S$$

$$\text{axm\_2 : } \text{cl}(r) \in S \leftrightarrow S$$

$$\text{axm\_3 : } r \subseteq \text{cl}(r)$$

$$\text{axm\_4 : } \text{cl}(r) ; r \subseteq \text{cl}(r)$$

$$\text{axm\_5 : } \forall p \cdot r \subseteq p \wedge p ; r \subseteq p \Rightarrow \text{cl}(r) \subseteq p$$

$$\text{thm\_1 : } \text{cl}(r) ; \text{cl}(r) \subseteq \text{cl}(r)$$

$$\text{thm\_2 : } \text{cl}(r) = r \cup r ; \text{cl}(r)$$

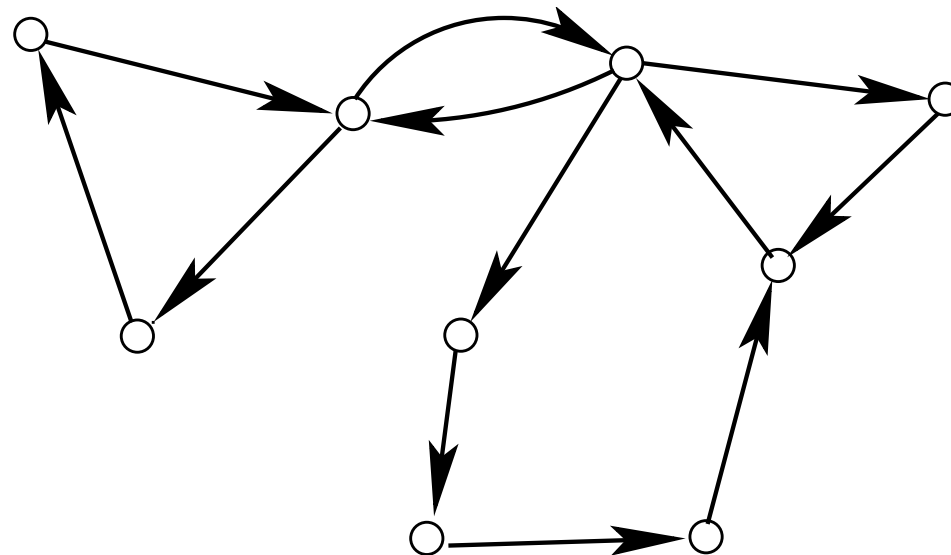
$$\text{thm\_3 : } \text{cl}(r) = r \cup \text{cl}(r) ; r$$

$$\text{thm\_4 : } \forall s \cdot r[s] \subseteq s \Rightarrow \text{cl}(r)[s] \subseteq s$$

$$\text{thm\_5 : } \text{cl}(r^{-1}) = \text{cl}(r)^{-1}$$



- 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  $r$



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

$$\text{axm\_2} : \quad V \times V \subseteq \text{cl}(r)$$

- Basic property

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

- This is an induction rule