Binary Relations

Discrete Math, Fall 2025

Konstantin Chukharev

Set Theory

- Basic operations
- Venn diagrams
- Power sets
- Cardinality
- Russell’s paradox
- ZFC axioms

Binary Relations

- Relation properties
- Equivalence classes
- Partial orders
- Functions
- Composition
- Lattices

Boolean Algebra

- Truth tables
- Logic circuits
- Normal forms
- Karnaugh maps
- Binary decision diagrams (BDDs)

Formal Logic

- Propositional logic
- Natural deduction
- Predicate logic
- Categorical logic
- Gödel’s theorems
- Automated reasoning

Relations

“In mathematics you don’t understand things. You just get used to them.”

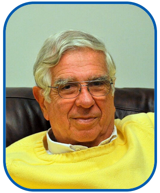
— John von Neumann

René Descartes

Évariste Galois

Ernst Schröder

Michael Rabin



Herbert Wilf

Relations as Sets

Definition 1: A *binary relation* R on sets A and B is a subset of the Cartesian product $A \times B$.

Notation: If $R \subseteq A \times B$, we write "$a\ R\ b$" to mean that element $a \in A$ is *related* to element $b \in B$.

Formally, $a\ R\ b$ iff $\langle a, b \rangle \in R$.

Note: R is used to denote both the relation itself ($a\ R\ b$) *and* the set of pairs ($R \subseteq A \times B$).

Note: the *order* of elements in the pair *matters*: $\langle a, b \rangle \in R$ denotes that a is related to b, not the other way around, unless there is *another* pair $\langle b, a \rangle$ in the relation.

Example: $R = \{\langle n, k \rangle \mid n, k \in \mathbb{N} \text{ and } n < k\}$

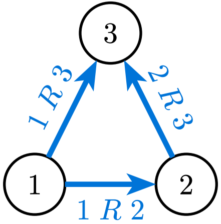
Definition 2:
- A binary relation $R \subseteq A \times B$ on two different sets A and B is called *heterogeneous*.
- A binary relation $R \subseteq M^2$ on the same set M is called *homogeneous*.

Graph Representation

Definition 3: A homogeneous relation $R \subseteq M^2$ can be represented as a *directed graph* where:

- Vertices correspond to elements of M
- There is a directed edge from x to y if $x \; R \; y$, i.e. $\langle x, y \rangle \in R$

Example: For $M = \{1, 2, 3\}$ and $R = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 1, 3 \rangle\}$, the graph has vertices $\{1, 2, 3\}$ and directed edges $1 \to 2$, $2 \to 3$, and $1 \to 3$.

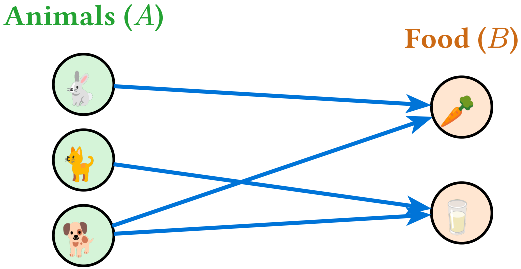


Graph Representation [2]

Definition 4: A heterogeneous relation $R \subseteq A \times B$ can be represented as a *bipartite graph* where:

- Vertices in one partition correspond to elements of A
- Vertices in the other partition correspond to elements of B
- There is a directed edge from $a \in A$ to $b \in B$ if $a\ R\ b$, i.e. $\langle a, b \rangle \in R$

Example: For animals $A = \{$🐇, 🐈, 🐕$\}$, food $B = \{$🥕, 🥛$\}$, and relation R = "likes to eat", we have the bipartite graph with animal vertices on the left side and food vertices on the right side with four edges.



Matrix Representation

Definition 5: A binary relation $R \subseteq A \times B$ can be represented as a *matrix* $M_R = [\![R]\!]$ where:

- Rows correspond to elements of A
- Columns correspond to elements of B
- $M_R[i,j] = 1$ if $a_i \; R \; b_j$, and $M_R[i,j] = 0$ otherwise

Example: Let $A = \{a, b, c\}$, $B = \{x, y\}$, and $R = \{\langle a, x\rangle, \langle b, x\rangle, \langle c, y\rangle\}$. The matrix representation is:

$$[\![R]\!] = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{where rows are } \{a, b, c\} \text{ and columns are } \{x, y\}$$

Special Relations

Definition 6: For any set M, we define these special relations:

- *Empty relation*: $\varnothing \subseteq M^2$ (no elements are related)
- *Identity relation*: $I_M = \{\langle x, x\rangle \mid x \in M\}$ (each element related only to itself)
- *Universal relation*: $U_M = M^2$ (every element related to every element)

Example: For $M = \{a, b, c\}$:

- Empty: $\varnothing$
- Identity: $\{\langle a, a\rangle, \langle b, b\rangle, (c, c)\}$
- Universal: $\{\langle a, a\rangle, \langle a, b\rangle, \langle a, c\rangle\langle b, a\rangle, \langle b, b\rangle, \langle b, c\rangle, \langle c, a\rangle, \langle c, b\rangle, \langle c, c\rangle\}$ (all 9 pairs)

Operations on Relations

Definition 7: For relations $R, S \subseteq A \times B$:

- *Union*: $R \cup S = \{\langle a, b\rangle \mid \langle a, b\rangle \in R \text{ or } \langle a, b\rangle \in S\}$
- *Intersection*: $R \cap S = \{\langle a, b\rangle \mid \langle a, b\rangle \in R \text{ and } \langle a, b\rangle \in S\}$
- *Complement*: $\overline{R} = (A \times B) \setminus R$

Definition 8: For a relation $R \subseteq A \times B$, the *converse* (or *inverse*) relation is:

$$R^{-1} = \{\langle b, a\rangle \mid \langle a, b\rangle \in R\} \subseteq B \times A$$

Example: If $R = \{\langle 1, x\rangle, \langle 2, y\rangle, \langle 2, z\rangle\}$, then $R^{-1} = \{\langle x, 1\rangle, \langle y, 2\rangle, \langle z, 2\rangle\}$.

Properties of Relations

Properties of Homogeneous Relations

Definition 9: A relation $R \subseteq M^2$ is *reflexive* if every element is related to itself:

$$\forall x \in M.\, (x \mathrel{R} x)$$

Definition 10: A relation $R \subseteq M^2$ is *symmetric* if for every pair of elements, if one is related to the other, then the reverse is also true:

$$\forall x, y \in M.\, (x \mathrel{R} y) \to (y \mathrel{R} x)$$

Definition 11: A relation $R \subseteq M^2$ is *transitive* if for every three elements, if the first is related to the second, and the second is related to the third, then the first is also related to the third:

$$\forall x, y, z \in M.\, (x \mathrel{R} y \land y \mathrel{R} z) \to (x \mathrel{R} z)$$

More Properties

Definition 12: A relation $R \subseteq M^2$ is *irreflexive* if no element is related to itself:

$$\forall x \in M.\, (x \not R\, x)$$

Definition 13: A relation $R \subseteq M^2$ is *antisymmetric* if for every pair of elements, if both are related to each other, then they must be equal:

$$\forall x, y \in M.\, (x\ R\ y \land y\ R\ x) \to (x = y)$$

Definition 14: A relation $R \subseteq M^2$ is *asymmetric* if for every pair of elements, if one is related to the other, then the reverse is not true:

$$\forall x, y \in M.\, (x\ R\ y) \to (y \not R\, x)$$

Note: *irreflexive* + *antisymmetric* = *asymmetric*.

Notes on Properties

- Reflexivity and irreflexivity are *not* mutually exclusive if $M = \varnothing$ (both are *vacuously*[1] `true`).
- Symmetry and antisymmetry are *not* mutually exclusive (e.g. identity relation).
- Asymmetry implies irreflexivity and antisymmetry.

[1] A statement “for all x in emptyset, $P(x)$” is considered `true` because there are *no counterexamples* in the empty set.

Additional Properties

Definition 15: A relation $R \subseteq M^2$ is:

- *Coreflexive* if $R \subseteq I_M$ (only related to themselves, if at all):

$$\forall x, y \in M.\, (x \mathrel{R} y) \to (x = y)$$

- *Right Euclidean* if whenever an element is related to two others, those two are related:

$$\forall x, y, z \in M.\, (x \mathrel{R} y \land x \mathrel{R} z) \to (y \mathrel{R} z)$$

- *Left Euclidean* if whenever two elements are both related to a third, they are related to each other:

$$\forall x, y, z \in M.\, (y \mathrel{R} x \land z \mathrel{R} x) \to (y \mathrel{R} z)$$

Example:

- Identity relation I_M is coreflexive. Any subset of I_M is also coreflexive.
- Equality relation "$=$" is left and right Euclidean.
- "Being in the same equivalence class" is Euclidean in both directions.

Equivalence Relations

Equivalence Relations

Definition 16: A relation $R \subseteq M^2$ is an *equivalence relation* if it is reflexive, symmetric and transitive.

Definition 17: Let $R \subseteq M^2$ be an equivalence relation on a set M. The *equivalence class* of an element $x \in M$ under R is the set of all elements related to x:

$$[x]_R = \{y \in M \mid x \mathrel{R} y\}$$

Definition 18: The *quotient set* of M by the equivalence relation R is the set of all equivalence classes:

$$M/_R = \{[x]_R \mid x \in M\}$$

Theorem 1: If $R \subseteq M^2$ is an equivalence relation, then $x \mathrel{R} y$ iff $[x]_R = [y]_R$ for all $x, y \in M$.

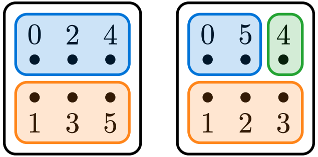
Set Partitions

Definition 19: A *partition* $\mathcal{P}$ of a set M is a family of non-empty, pairwise-disjoint subsets whose union is M:

- (Non-empty) $\forall B \in \mathcal{P}.\, (B \neq \varnothing)$
- (Disjoint) $\forall B_1, B_2 \in \mathcal{P}.\, (B_1 \neq B_2) \to (B_1 \cap B_2 = \varnothing)$
- (Cover) $\bigcup\limits_{B \in \mathcal{P}} B = M$

Elements of $\mathcal{P}$ are *blocks* (or *cells*).

Example: For $M = \{0, 1, 2, 3, 4, 5\}$: $\{\{0, 2, 4\}, \{1, 3, 5\}\}$ and $\{\{0, 5\}, \{1, 2, 3\}, \{4\}\}$ are partitions.



Partitions and Equivalence Relations

Theorem 2 (Equivalences ⇔ Partitions): Each equivalence relation R on M yields the partition $\mathcal{P}_R = \{[x]_R \mid x \in M\}$. Each partition $\mathcal{P}$ yields an equivalence $R_{\mathcal{P}}$ given by $\langle x, y \rangle \in R_{\mathcal{P}}$ iff x and y lie in the same block. These constructions invert one another.

Proof *(Sketch)*: Classes of an equivalence are non-empty, disjoint, and cover M. Conversely, "same block" relation is reflexive, symmetric, transitive. Composing the two constructions returns exactly the starting equivalence relation or partition (they are mutually inverse up to equality of sets of ordered pairs). □

Closures of Relations

Closures of Relations

Definition 20: The *closure* of a relation $R \subseteq M^2$ with respect to a property P is the smallest relation containing R that satisfies property P.

- *Reflexive closure*: $r(R) = R \cup I_M$ (smallest reflexive relation containing R)
- *Symmetric closure*: $s(R) = R \cup R^{-1}$ (smallest symmetric relation containing R)
- *Transitive closure*: $t(R)$ is the smallest transitive relation containing R

The key insight is that closure operations *add the minimum* number of pairs needed to achieve the desired property, while preserving all existing pairs in the original relation.

Reflexive Closure

Definition 21: The *reflexive closure* $r(R)$ of a relation $R \subseteq M^2$ is defined as:

$$r(R) = R \cup I_M = R \cup \{\langle x, x \rangle \mid x \in M\}$$

Example: Let $M = \{1, 2, 3\}$ and $R = \{\langle 1, 2 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle\}$.

The identity relation is $I_M = \{\langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle\}$.

The reflexive closure is:

$$r(R) = R \cup I_M = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 2, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 3 \rangle\}$$

Symmetric Closure

Definition 22: The *symmetric closure* $s(R)$ of a relation $R \subseteq M^2$ is defined as:

$$s(R) = R \cup R^{-1} = R \cup \{\langle b, a \rangle \mid \langle a, b \rangle \in R\}$$

Example: Let $M = \{1, 2, 3\}$ and $R = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 1, 3 \rangle\}$.

The converse relation is:

$$R^{-1} = \{\langle 2, 1 \rangle, \langle 3, 2 \rangle, \langle 3, 1 \rangle\}$$

The symmetric closure is:

$$s(R) = R \cup R^{-1} = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 1, 3 \rangle, \langle 2, 1 \rangle, \langle 3, 2 \rangle, \langle 3, 1 \rangle\}$$

Transitive Closure

Definition 23: The *transitive closure* $t(R)$ of a relation $R \subseteq M^2$ is the smallest transitive relation containing R.

Theorem 3: The transitive closure can be computed as:

$$t(R) = \bigcup_{n=1}^{\infty} R^n \quad \text{where } R^n = \underbrace{R \circ R \circ \ldots \circ R}_{n \text{ times}}$$

For finite sets with $|M| = k$, we have $t(R) = R^1 \cup R^2 \cup \ldots \cup R^k$.

Proof: Since M is finite, any path of length greater than $|M|$ must repeat vertices, so we only need to consider paths of length at most $|M|$. □

Transitive Closure [2]

Example (Step-by-step transitive closure computation): Let $M = \{1, 2, 3\}$ and $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$.

Step	Description	Result
Step 1:	Compute $R^1 = R$.	$R^1 = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$
Step 2:	Compute $R^2 = R \circ R$. For $\langle a, c\rangle \in R^2$, we need $\exists b : \langle a, b\rangle \in R \wedge \langle b, c\rangle \in R$. • $\langle 1, 3\rangle \in R^2$ since $\langle 1, 2\rangle \in R$ and $\langle 2, 3\rangle \in R$	$R^2 = \{\langle 1, 3\rangle\}$
Step 3:	Compute $R^3 = R^2 \circ R$. For $\langle a, c\rangle \in R^3$, we need $\exists b : \langle a, b\rangle \in R^2 \wedge \langle b, c\rangle \in R$. • No such pairs exist.	$R^3 = \varnothing$
Step 4:	Form the transitive closure: $t(R) = R^1 \cup R^2 \cup R^3$.	$t(R) = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\}$

Combined Closures

Definition 24: Closure operations can be combined to create relations with multiple properties:

- *Reflexive-symmetric closure*: $rs(R) = sr(R) = r(R) \cup s(R) \cup I_M$
- *Reflexive-transitive closure*: $rt(R) = tr(R) = t(R) \cup I_M$
- *Equivalence closure*: $rst(R) = tsr(R)$ (reflexive, symmetric, and transitive)

Theorem 4 (Commutativity of closure operations):

- Reflexive and symmetric closures commute: $rs(R) = sr(R)$
- Reflexive and transitive closures commute: $rt(R) = tr(R)$
- All three closures commute when applied together

Reflexive-Symmetric Closure

Example (Reflexive-symmetric closure): Let $M = \{1, 2, 3\}$ and $R = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$.

Method 1: Apply reflexive closure first, then symmetric

$$r(R) = R \cup I_M = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle\}$$

$$sr(R) = r(R) \cup r(R)^{-1}$$

$$= \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 3\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle\}$$

Method 2: Apply symmetric closure first, then reflexive

$$s(R) = R \cup R^{-1} = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 2, 1\rangle, \langle 3, 2\rangle\}$$

$$rs(R) = s(R) \cup I_M$$

$$= \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 2, 3\rangle, \langle 3, 2\rangle, \langle 3, 3\rangle\}$$

Both methods yield the same result, confirming commutativity.

Reflexive-Transitive Closure

Example (Reflexive-transitive closure (Kleene star)): Let $M = \{a, b, c\}$ and $R = \{\langle a, b\rangle, \langle b, c\rangle\}$.

First, compute the transitive closure:

$$t(R) = R \cup R^2 = \{\langle a, b\rangle, \langle b, c\rangle, \langle a, c\rangle\}$$

Then add reflexivity:

$$rt(R) = t(R) \cup I_M = \{\langle a, a\rangle, \langle a, b\rangle, \langle a, c\rangle, \langle b, b\rangle, \langle b, c\rangle, \langle c, c\rangle\}$$

This is equivalent to the *reflexive-transitive closure*, often denoted R^* (Kleene star).

Equivalence Closure

Example (Complete equivalence closure): Let $M = \{1, 2, 3, 4\}$ and $R = \{\langle 1, 2\rangle, \langle 3, 4\rangle\}$.

Step 1: Make it reflexive

$$r(R) = R \cup I_M = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 3, 4\rangle, \langle 4, 4\rangle\}$$

Step 2: Make it symmetric

$$sr(R) = r(R) \cup r(R)^{-1}$$

$$= \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 3, 4\rangle, \langle 4, 3\rangle, \langle 4, 4\rangle\}$$

Step 3: Make it transitive Since $\langle 1, 2\rangle, \langle 2, 1\rangle \in sr(R)$, transitivity requires $\langle 1, 1\rangle$ (already present). Since $\langle 3, 4\rangle, \langle 4, 3\rangle \in sr(R)$, transitivity requires $\langle 3, 3\rangle$ (already present).

$$tsr(R) = sr(R)$$

(no new pairs needed)

The equivalence closure partitions M into equivalence classes $\{1, 2\}$ and $\{3, 4\}$.

Equivalence Closure [2]

Example (Equivalence closure [2]): Let $M = \{a, b, c, d, e\}$ and $R = \{\langle a, b\rangle, \langle b, c\rangle, \langle d, e\rangle\}$.

Reflexive closure:

$$r(R) = R \cup \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle, \langle d, d\rangle, \langle e, e\rangle\}$$

Symmetric closure:

$$sr(R) = r(R) \cup \{\langle b, a\rangle, \langle c, b\rangle, \langle e, d\rangle\}$$

Transitive closure: We need to add pairs to ensure transitivity:

- From $\langle a, b\rangle, \langle b, c\rangle$: add $\langle a, c\rangle$
- From $\langle c, b\rangle, \langle b, a\rangle$: add $\langle c, a\rangle$

$$tsr(R) \setminus = sr(R) \cup \{\langle a, c\rangle, \langle c, a\rangle\}$$

The final equivalence relation has equivalence classes $\{a, b, c\}$ and $\{d, e\}$.

Warshall's Algorithm for Transitive Closure

Definition 25: *Warshall's algorithm* computes the transitive closure of a relation using dynamic programming with time complexity $O(n^3)$.

Given an $n \times n$ matrix M representing relation R:

```
for k = 1 to n:
    for i = 1 to n:
        for j = 1 to n:
            M[i,j] = M[i,j] OR (M[i,k] AND M[k,j])
```

Example (Warshall's algorithm step-by-step): Let $X = \{1, 2, 3, 4\}$ and relation R with matrix:

$$[\![R]\!] = M^{(0)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Warshall's Algorithm for Transitive Closure [2]

Iteration $k = 1$: Consider paths through vertex 1

$$M^{(1)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

(Added $\langle 4, 2 \rangle$: path $4 \to 1 \to 2$)

Iteration $k = 2$: Consider paths through vertex 2

$$M^{(2)} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$$

(Added $\langle 1, 3 \rangle$ and $\langle 4, 3 \rangle$)

Warshall's Algorithm for Transitive Closure [3]

Iteration $k = 3$: Consider paths through vertex 3

$$M^{(3)} = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

(Added $\langle 1, 4 \rangle$, $\langle 2, 4 \rangle$, and $\langle 4, 4 \rangle$)

Iteration $k = 4$: Consider paths through vertex 4

$$M^{(4)} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

(The relation becomes universal since there's a cycle)

Warshall's Algorithm for Transitive Closure [4]

Example (Practical application: Reachability in graphs): Consider a social network where R represents "follows" relationships:

$$R = \{\langle A, B\rangle, \langle B, C\rangle, \langle C, D\rangle, \langle A, E\rangle\}$$

Using Warshall's algorithm, we can determine *indirect influence*:

- A can influence C through B
- A can influence D through B and C
- The transitive closure shows all possible influence paths

This is crucial for analyzing *information propagation* in social networks, *dependency resolution* in software systems, and *route planning* in transportation networks.

Properties and Advanced Applications of Closures

Theorem 5 (Closure properties): For any relation $R \subseteq M^2$:

1. *Idempotency*: $r(r(R)) = r(R)$, $s(s(R)) = s(R)$, $t(t(R)) = t(R)$
2. *Monotonicity*: If $R_1 \subseteq R_2$, then $r(R_1) \subseteq r(R_2)$, etc.
3. *Extensivity*: $R \subseteq r(R)$, $R \subseteq s(R)$, $R \subseteq t(R)$
4. *Distributivity over union*: $r(R_1 \cup R_2) = r(R_1) \cup r(R_2)$, etc.

Example (Closure of the empty relation): Let $M = \{a, b, c\}$ and $R = \varnothing$.

- $r(\varnothing) = \varnothing \cup I_M = I_M = \{\langle a, a\rangle, \langle b, b\rangle, \langle c, c\rangle\}$
- $s(\varnothing) = \varnothing \cup \varnothing^{-1} = \varnothing$
- $t(\varnothing) = \varnothing$ (since $\varnothing^n = \varnothing$ for all $n \geq 1$)

The reflexive closure of the *empty* relation is the *identity* relation.

Properties and Advanced Applications of Closures [2]

Example (Closure of the universal relation): Let $M = \{1, 2\}$ and $R = M \times M = \{\langle 1, 1\rangle, \langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 2\rangle\}$.

- $r(R) = R \cup I_M = R$ (since $I_M \subseteq R$)
- $s(R) = R \cup R^{-1} = R$ (since $R = R^{-1}$ for universal relation)
- $t(R) = R$ (universal relation is already transitive)

The universal relation is its own closure under all three operations.

Properties and Advanced Applications of Closures [3]

Example (Non-commutativity with other operations): Let $M = \{1, 2, 3\}$, $R_1 = \{\langle 1, 2\rangle\}$, and $R_2 = \{\langle 2, 3\rangle\}$.

Consider $t(R_1 \cup R_2)$ vs $t(R_1) \cup t(R_2)$:

- $R_1 \cup R_2 = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$
- $t(R_1 \cup R_2) = \{\langle 1, 2\rangle, \langle 2, 3\rangle, \langle 1, 3\rangle\}$
- $t(R_1) = \{\langle 1, 2\rangle\}$
- $t(R_2) = \{\langle 2, 3\rangle\}$
- $t(R_1) \cup t(R_2) = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$

Since $\langle 1, 3\rangle \in t(R_1 \cup R_2)$ but $\langle 1, 3\rangle \notin t(R_1) \cup t(R_2)$, we have:

$$t(R_1 \cup R_2) \neq t(R_1) \cup t(R_2)$$

However: $t(R_1) \cup t(R_2) \subseteq t(R_1 \cup R_2)$ always holds.

Properties and Advanced Applications of Closures [4]

Example (Computing equivalence classes from closure): Let $M = \{1, 2, 3, 4, 5\}$ and $R = \{\langle 1, 3\rangle, \langle 2, 4\rangle, \langle 4, 5\rangle\}$.

The equivalence closure gives us:

$$\begin{aligned} \operatorname{equiv}(R) &= rst(R) \\ &= \{\langle 1, 1\rangle, \langle 1, 3\rangle, \langle 2, 2\rangle, \langle 2, 4\rangle, \langle 2, 5\rangle, \langle 3, 1\rangle, \langle 3, 3\rangle, \langle 4, 2\rangle, \langle 4, 4\rangle, \langle 4, 5\rangle, \langle 5, 2\rangle, \langle 5, 4\rangle, \langle 5, 5\rangle\} \end{aligned}$$

The equivalence classes are:

- $[1] = \{1, 3\}$
- $[2] = \{2, 4, 5\}$

This partitions M into $\{\{1, 3\}, \{2, 4, 5\}\}$.

Properties and Advanced Applications of Closures [5]

Example (Closure in directed acyclic graphs (DAGs)): Consider a dependency graph where $R = \{\langle \mathrm{A}, \mathrm{B} \rangle, \langle \mathrm{B}, \mathrm{C} \rangle, \langle \mathrm{A}, \mathrm{D} \rangle, \langle \mathrm{D}, \mathrm{C} \rangle\}$ represents “depends on” relationships.

The transitive closure reveals all indirect dependencies:

$$t(R) = R \cup \{\langle \mathrm{A}, \mathrm{C} \rangle\}$$

This shows that component A transitively depends on C through two paths:

- $A \to B \to C$
- $A \to D \to C$

In software build systems, this helps determine the complete dependency tree.

When Relation Closures Actually Matter

🎬 Netflix Knows You Too Well

Transitive closure powers recommendation systems and social networks:

- You like movie A, Alice likes A and B, so you might like B.
- Chain reactions: A → B → C → D discovers surprising connections.

That creepy moment when Netflix suggests something perfect? That's transitive closure finding paths through millions of user preferences.

💸 How Money Actually Moves

Transitive closure tracks financial flows:

- You pay bank ⇒ bank pays merchant ⇒ merchant pays supplier.
- Money laundering detection: hidden chains of transactions.

Banks use this to catch criminals who try to hide money through complex chains of fake transactions.

Key insight: If you can get from A to C by going through B, then *transitive closure* provides the *direct* $A \to C$ relation — whether it's movies, money, friends, or malware.

Order Relations

Orders

Definition 26: A relation $R \subseteq M^2$ is called a *preorder* if it is reflexive and transitive.

Definition 27: A *partial order* is a relation $R \subseteq M^2$ that is reflexive, antisymmetric, and transitive.

Definition 28: A relation $R \subseteq M^2$ is *connected* if for every pair of distinct elements, either one is related to the other or vice versa:

$$\forall x, y \in M.\, (x \neq y) \to (x \; R \; y \vee y \; R \; x)$$

Definition 29: A partial order which is also connected is called a *total order* (or *linear order*).

Chains and Antichains

Definition 30: In a partially ordered set $(M, \preceq)$:

- A *chain* is a subset $C \subseteq M$ where every two elements are comparable. Formally:

$$\forall x, y \in C.\, (x \preceq y \text{ or } y \preceq x)$$

- An *antichain* is a subset $A \subseteq M$ where no two distinct elements are comparable. Formally:

$$\forall x, y \in A.\, (x \neq y) \to (x \npreceq y \text{ and } y \npreceq x)$$

Example: Consider the divisibility relation $\mid$ on $\{1, 2, 3, 4, 6, 12\}$:

- Chain: $\{1, 2, 4, 12\}$ (since $1 \mid 2 \mid 4 \mid 12$)
- Chain: $\{1, 3, 6, 12\}$ (since $1 \mid 3 \mid 6 \mid 12$)
- Antichain: $\{2, 3\}$ (since $2 \nmid 3$ and $3 \nmid 2$)
- Antichain: $\{4, 6\}$ (since $4 \nmid 6$ and $6 \nmid 4$)

Dilworth's Theorem

Theorem 6 (Dilworth): In any finite partially ordered set, the maximum size of an antichain equals the minimum number of chains needed to cover the entire set.

Example: In the Boolean lattice $\mathcal{P}(\{a, b\})$ with inclusion:

- Maximum antichain: $\{\{a\}, \{b\}\}$ of size 2
- Minimum chain decomposition: $\{\emptyset, \{a\}\} \cup \{\{b\}, \{a, b\}\}$ with 2 chains

Examples of Orders

Example: Consider the *no longer than* relation $\preccurlyeq$ on $\mathbb{B}^*$:

$$x \preccurlyeq y \quad \text{iff} \quad \operatorname{len}(x) \leq \operatorname{len}(y)$$

This is a preorder (reflexive and transitive), and even connected, but not a partial order, since it is not antisymmetric: for example, $01 \preccurlyeq 10$ and $10 \preccurlyeq 01$, but $01 \neq 10$.

Example: The *subset* relation $\subseteq$ on $\mathcal{P}(A)$ is a partial order (reflexive, antisymmetric, transitive); typically not total, since not all subsets are comparable (e.g., $A = \{1\}$ and $B = \{2, 3\}$).

Example: *Divisibility* $|$ on $D = \{1, 2, 3, 6\}$: $1|2|6$, $1|3|6$; 2 and 3 incomparable. Partial, not total.

Example: *Lexicographic order* on A^n (induced by a total order on A) is a total order.

Composition of Relations

Composition of Relations

Definition 31: The *composition* of two relations $R \subseteq A \times B$ and $S \subseteq B \times C$ is defined as:

$$R \mathbin{;} S = S \circ R = \{\langle a, c\rangle \mid \exists b \in B.\, (a \mathrel{R} b) \land (b \mathrel{S} c)\}$$

Powers of Relations

Definition 32: For a homogeneous relation $R \subseteq M^2$, we define *powers* of R:

- $R^0 = I_M$ (identity relation)
- $R^1 = R$
- $R^{n+1} = R^n \circ R$ for $n \geq 1$

Example: Let $M = \{1, 2, 3, 4\}$ and $R = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 4 \rangle\}$ (successor relation).

- $R^1 = \{\langle 1, 2 \rangle, \langle 2, 3 \rangle, \langle 3, 4 \rangle\}$
- $R^2 = \{\langle 1, 3 \rangle, \langle 2, 4 \rangle\}$ (two steps)
- $R^3 = \{\langle 1, 4 \rangle\}$ (three steps)
- $R^4 = \varnothing$ (no four-step paths)

Theorem 7: For any relation R on a finite set with n elements:

- $R^+ = R^1 \cup R^2 \cup \ldots \cup R^n$ is a *transitive closure*.
- $R^* = R^0 \cup R^+ = I \cup R^+$ is a *reflexive-transitive closure*.

Associativity of Composition

Theorem 8: Composition of relations is associative: $(R \mathbin{;} S) \mathbin{;} T = R \mathbin{;} (S \mathbin{;} T)$.

Proof: Let $R \subseteq A \times B$, $S \subseteq B \times C$, and $T \subseteq C \times D$ be three relations.

($\subseteq$): Let $\langle a, d \rangle \in (R \mathbin{;} S) \mathbin{;} T$.

- By definition of composition: $\exists c \in C.\, (\langle a, c \rangle \in R \mathbin{;} S) \land (\langle c, d \rangle \in T)$.
- Since $\langle a, c \rangle \in R \mathbin{;} S$, we have: $\exists b \in B.\, (\langle a, b \rangle \in R) \land (\langle b, c \rangle \in S)$.
- From $\langle b, c \rangle \in S$ and $\langle c, d \rangle \in T$, we have: $\langle b, d \rangle \in S \mathbin{;} T$.
- From $\langle a, b \rangle \in R$ and $\langle b, d \rangle \in S \mathbin{;} T$, we have: $\langle a, d \rangle \in R \mathbin{;} (S \mathbin{;} T)$.

($\supseteq$): Let $\langle a, d \rangle \in R \mathbin{;} (S \mathbin{;} T)$.

- By definition of composition: $\exists b \in B.\, (\langle a, b \rangle \in R) \land (\langle b, d \rangle \in S \mathbin{;} T)$.
- Since $\langle b, d \rangle \in S \mathbin{;} T$, we have: $\exists c \in C.\, (\langle b, c \rangle \in S) \land (\langle c, d \rangle \in T)$.
- From $\langle a, b \rangle \in R$ and $\langle b, c \rangle \in S$, we have: $\langle a, c \rangle \in R \mathbin{;} S$.
- From $\langle a, c \rangle \in R \mathbin{;} S$ and $\langle c, d \rangle \in T$, we have: $\langle a, d \rangle \in (R \mathbin{;} S) \mathbin{;} T$.

Therefore, $(R \mathbin{;} S) \mathbin{;} T = R \mathbin{;} (S \mathbin{;} T)$. □

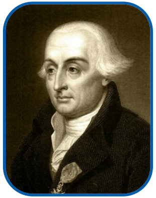
Functions

> *“A function is a machine which converts a certain class of inputs into a certain class of outputs.”*
>
> ***— Norbert Wiener***

Leonhard Euler

Augustin-Louis Cauchy

Karl Weierstrass



Joseph-Louis Lagrange

George Pólya

Norbert Wiener

Definition of a Function

Definition 33: A *function* f from a set A to a set B, denoted $f : A \to B$, is a special kind of relation $f \subseteq A \times B$ where every element of A is paired with *exactly one* element of B.

This means two conditions must hold:

1. *Functional (right-unique)*: For every $a \in A$, there is *at most one* pair $\langle a, b \rangle$ in f.

$$\forall a \in A.\, \forall b_1, b_2 \in B.\, (f(a) = b_1) \land (f(a) = b_2) \to (b_1 = b_2)$$

2. *Serial (left-total)*: For every $a \in A$, there is *at least one* pair $\langle a, b \rangle$ in f.

$$\forall a \in A.\, \exists b \in B.\, f(a) = b$$

Definition 34: A relation that satisfies the *functional* property is called a *partial function*.

A relation that satisfies *both* properties is called a *total function*, or simply a *function*.

Domain, Codomain, Range

Definition 35: For a function $f : A \to B$:

- The set A is called the *domain* of f, denoted $\operatorname{Dom}(f)$.
- The set B is called the *codomain* of f, denoted $\operatorname{Cod}(f)$.
- The *range* (or *image*) of f is the set of all values that f actually takes:

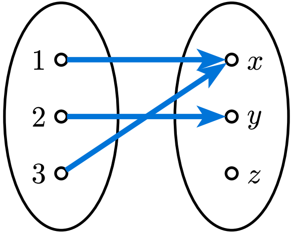
$$\operatorname{Range}(f) = \{b \in B \mid \exists a \in A.\ f(a) = b\} = \{f(a) \mid a \in A\}$$

Note: $\operatorname{Range}(f) \subseteq \operatorname{Cod}(f)$

Example: Let $A = \{1, 2, 3\}$ and $B = \{x, y, z\}$. Let $f = \{\langle 1, x \rangle, \langle 2, y \rangle, \langle 3, x \rangle\}$.

- f is a function from A to B.
- $\operatorname{Dom}(f) = A$
- $\operatorname{Cod}(f) = B$
- $\operatorname{Range}(f) = \{x, y\} \subseteq B$

We have $f(1) = x$, $f(2) = y$, $f(3) = x$.



Domain, Codomain, Range [2]

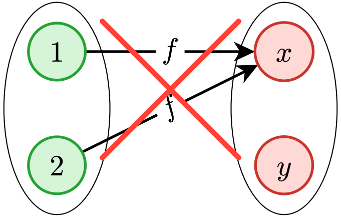
Example: Consider $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = n^2$.

- $\mathrm{Dom}(g) = \mathbb{Z}$.
- $\mathrm{Cod}(g) = \mathbb{Z}$.
- $\mathrm{Range}(g) = \{0, 1, 4, 9, ...\}$ (the set of non-negative perfect squares).

Injective Functions

Definition 36: A function $f : A \to B$ is *injective* (or *one-to-one*[2]) if distinct elements in the domain map to distinct elements in the codomain. Formally:

$$\forall a_1, a_2 \in A.\, (f(a_1) = f(a_2)) \to (a_1 = a_2)$$



Example: $f : \mathbb{N} \to \mathbb{N}$ defined by $f(n) = 2n$ is injective. If $f(n_1) = f(n_2)$, then $2n_1 = 2n_2$, so $n_1 = n_2$.

Example: $g : \mathbb{Z} \to \mathbb{Z}$ defined by $g(n) = n^2$ is *not* injective, because $g(-1) = 1$ and $g(1) = 1$, but $-1 \neq 1$.

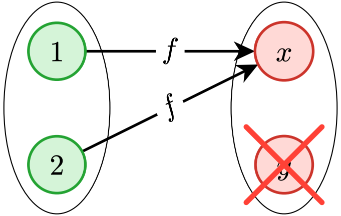
[2] Do not confuse it with *one-to-one correspondence*, which is a bijection, not just injection!

Surjective Functions

Definition 37: A function $f : A \to B$ is *surjective* (or *onto*) if every element in the codomain is the image of at least one element in the domain. Formally:

$$\forall b \in B.\, \exists a \in A.\, f(a) = b$$

For surjective functions, $\mathrm{Range}(f) = \mathrm{Cod}(f)$, i.e., there are *no "uncovered"* elements in the right side.



Example: $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^3$ is surjective. For any $y \in \mathbb{R}$, $x = \sqrt[3]{y}$ is such that $f(x) = y$.

Example: $g : \mathbb{N} \to \mathbb{N}$ defined by $g(n) = 2n$ is *not* surjective, because odd numbers in $\mathbb{N}$ (the codomain) are not in the range of g. For example, there is no $n \in \mathbb{N}$ such that $2n = 3$.

Bijective Functions

Definition 38: A function $f : A \to B$ is *bijective* if it is both injective and surjective. A bijective function establishes a *one-to-one correspondence* between the elements of A and B.

Example: $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 2x + 1$ is bijective.

- Injective: If $2x_1 + 1 = 2x_2 + 1$, then $2x_1 = 2x_2$, so $x_1 = x_2$.
- Surjective: For any $y \in \mathbb{R}$, let $x = \frac{y-1}{2}$. Then $f(x) = 2\left(\frac{y-1}{2}\right) + 1 = y - 1 + 1 = y$.

Example: The identity function $\mathrm{id}_A : A \to A$ defined by $\mathrm{id}_A(x) = x$ for all $x \in A$ is bijective.

Function Composition

Definition 39: Let $f : A \to B$ and $g : B \to C$ be two functions. The *composition* of g and f, denoted $g \circ f$ (read as "g composed with f" or "g after f"), is a function from A to C defined by:

$$(g \circ f)(a) = g(f(a))$$

Example: Let $f : \mathbb{R} \to \mathbb{R}$ be $f(x) = x^2$ and $g : \mathbb{R} \to \mathbb{R}$ be $g(x) = x + 1$.

- $(g \circ f)(x) = g(f(x)) = g(x^2) = x^2 + 1$.
- $(f \circ g)(x) = f(g(x)) = f(x + 1) = (x + 1)^2 = x^2 + 2x + 1$.

Properties of Function Composition

- *Associativity:* If $f : A \to B$, $g : B \to C$, and $h : C \to D$, then $(h \circ g) \circ f = h \circ (g \circ f)$.
- The *identity* function acts as a *neutral* element for composition:
  - $\mathrm{id}_B \circ f = f$ for any function $f : A \to B$.
  - $f \circ \mathrm{id}_A = f$ for any function $f : A \to B$.
- Composition *preserves* the properties of functions:
  - If f and g are injective, so is $g \circ f$.
  - If f and g are surjective, so is $g \circ f$.
  - If f and g are bijective, so is $g \circ f$.
- Note that in general, $g \circ f \neq f \circ g$, i.e., function composition is *not commutative*.

Inverse Functions

Definition 40: If $f : A \to B$ is a bijective function, then its *inverse function*, denoted $f^{-1} : B \to A$, is defined as:

$$f^{-1}(b) = a \quad \text{iff} \quad f(a) = b$$

Note: A function has an inverse *if and only if* it is bijective.

Example: Let $f : \mathbb{R} \to \mathbb{R}$ be $f(x) = 2x + 1$. We found it's bijective. To find $f^{-1}(y)$, let $y = 2x + 1$. Solving for x, we get $x = \frac{y-1}{2}$. So, $f^{-1}(y) = \frac{y-1}{2}$.

Theorem 9: If $f : A \to B$ is a bijective function with inverse $f^{-1} : B \to A$:

- f^{-1} is also bijective.
- $(f^{-1} \circ f)(a) = a$ for all $a \in A$ (i.e., $f^{-1} \circ f = \mathrm{id}_A$).
- $(f \circ f^{-1})(b) = b$ for all $b \in B$ (i.e., $f \circ f^{-1} = \mathrm{id}_B$).
- If $f : A \to B$ and $g : B \to C$ are both bijective, then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Image and Preimage of Sets

Definition 41: Let $f : A \to B$ be a function and let $S \subseteq A$. The *image of S under f* is the set:

$$f(S) = \{f(s) \mid s \in S\}$$

Note that $f(S) \subseteq B$. The range of f is $f(A)$.

Definition 42: Let $f : A \to B$ be a function and let $T \subseteq B$. The *preimage of T under f* (or *inverse image of T*) is the set of all elements in the domain that map into T:

$$f^{-1}(T) = \{a \in A \mid f(a) \in T\}$$

Note: The notation $f^{-1}(T)$ is used even if the inverse function f^{-1} does not exist (i.e., if f is not bijective). It always refers to the set of domain elements that map into T.

Image and Preimage of Sets [2]

Example: Let $f : \mathbb{Z} \to \mathbb{Z}$ be $f(x) = x^2$.

- Let $S = \{-2, -1, 0, 1, 2\}$. Then $f(S) = \{f(-2), f(-1), f(0), f(1), f(2)\} = \{4, 1, 0, 1, 4\} = \{0, 1, 4\}$.
- Let $T_1 = \{1, 9\}$. The preimage is $f^{-1}(T_1) = \{x \in \mathbb{Z} \mid x^2 \in \{1, 9\}\} = \{-3, -1, 1, 3\}$.
- Let $T_2 = \{2, 3\}$. The preimage is $f^{-1}(T_2) = \{x \in \mathbb{Z} \mid x^2 \in \{2, 3\}\} = \varnothing$.

Cardinality & Infinity

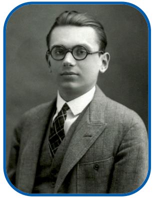
“God made the integers, all else is the work of man.”

— Leopold Kronecker

Giuseppe Peano

Leopold Kronecker

David Hilbert



Kurt Gödel

John von Neumann

Size of Sets

Definition 43: The *size* of a *finite* set X, denoted $|X|$, is the number of elements it contains.

Examples:

- Let $A = \{$🪐, 🦕, 🎻$\}$, then $|A| = 3$, since A contains *exactly 3* elements.
- Let $B = \{$🥝, 🥝, 🥝$\}$, then $|B| = 1$, since B contains *only one unique* element (the kiwi).
- $|\mathcal{P}(\{1, 2,$ 🐈 $\})| = 2^3 = 8$, since the power set consists of *all 8 possible subsets* of $\{1, 2,$ 🐈 $\}$.
- $|\varnothing| = 0$, since the *empty* set contains *no elements*.
- $|\mathbb{N}| = \infty$, since there are *infinitely many* natural numbers.
- $|\mathbb{R}| = \infty$, since there are *infinitely many* real numbers.

Cardinality of Sets

Definition 44: The *cardinality* of a set X, denoted $|X|$, is a measure of its "size".

- For *finite* sets, cardinality $|X|$ is the same as size, i.e., the number of elements in X.
- For *infinite* sets, cardinality $|X|$ describes the "type" of infinity, e.g. *countable* vs *uncountable*.

Examples:

- $|\mathbb{N}| = \aleph_0$
- $|\mathbb{Q}| = \aleph_0$
- $|\mathbb{R}| = 2^{\aleph_0} = \mathfrak{c}$

Note: $|X|$ is *not* just a number, but a *cardinal number*.

- Cardinal numbers extend natural numbers to describe sizes of infinite sets.
- The *finite* cardinal numbers are just natural numbers: $0, 1, 2, 3, \ldots$.
- The first (smallest) *infinite* cardinal is $\aleph_0$ (the cardinality of $\mathbb{N}$).
- *Arithmetic* operations on cardinal numbers *differ* from those on natural numbers.
  - For example, $\aleph_0 + 1 = \aleph_0$ and $\aleph_0 \cdot 2 = \aleph_0$.

Equinumerosity

Definition 45: Two sets A and B have the same *cardinality* and called *equinumerous*, denoted $|A| = |B|$ or $A \approx B$, iff there is a *bijection* (one-to-one correspondence) from A to B.

Theorem 10: Equinumerosity is an equivalence relation.

Proof: Let A, B, C be sets.

- *Reflexivity:* The identity map $\mathrm{id}_A : A \to A$, where $\mathrm{id}_A(x) = x$, is a bijection, so $A \approx A$.
- *Symmetry:* Suppose $A \approx B$, then there is a bijection $f : A \to B$. Since it is a bijection, its inverse f^{-1} exists and is also a bijection. Hence, $f^{-1} : B \to A$ is a bijection, so $B \approx A$.
- *Transitivity:* Suppose that $A \approx B$ and $B \approx C$, i.e., there are bijections $f : A \to B$ and $g : B \to C$. Then the composition $g \circ f : A \to C$ is also a bijection. So $A \approx C$.

□

Countable Sets

Definition 46: A set called *countable* if it is either finite or has the same cardinality as the set of natural numbers $\mathbb{N}$. Alternatively, a set is countable if there is a *bijection* from $\mathbb{N}$ to that set.

When an infinite set is *countable*, its cardinality is denoted $\aleph_0$ (*"aleph-null"*).

Example: $|\mathbb{N}_{\text{odd}} = \{1, 3, 5, ...\}| = \aleph_0$, the set of *odd* natural numbers is countable, since there is a bijection $f : \mathbb{N} \to \mathbb{N}_{\text{odd}}$ defined by $f(n) = 2n + 1$.

Example: $|\{x \in \mathbb{N} \mid x \text{ is prime}\}| = \aleph_0$, the set of *prime* numbers is countable.

Example: $|\mathbb{Z}| = \aleph_0$, the set of *integers* $(-\infty, ..., -2, -1, 0, 1, 2, ..., \infty)$ is countable, since there is a bijection $f : \mathbb{N} \to \mathbb{Z}$ defined by $f(n)$:

$$f(n) = (-1)^n \left\lceil \frac{n}{2} \right\rceil = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ -\frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases} \qquad \begin{bmatrix} f(0) & f(1) & f(2) & f(3) & f(4) & f(5) & f(6) & ... \\ \lceil \frac{0}{2} \rceil & -\lceil \frac{1}{2} \rceil & \lceil \frac{2}{2} \rceil & -\lceil \frac{3}{2} \rceil & \lceil \frac{4}{2} \rceil & -\lceil \frac{5}{2} \rceil & \lceil \frac{6}{2} \rceil & ... \\ 0 & -1 & 1 & -2 & 2 & -3 & 3 & ... \end{bmatrix}$$

Countability Constructions

Definition 47: A set X is *enumerable* if there is a surjection $e : \mathbb{N} \to X$ (equivalently a bijection with either $\mathbb{N}$ or an initial segment of $\mathbb{N}$ if X finite).

Theorem 11 (Zig-Zag Enumeration): $\mathbb{N}^2$ is countable.

Proof: List pairs by diagonals of constant sum: $\langle 0, 0\rangle$; $\langle 0, 1\rangle$, $\langle 1, 0\rangle$; $\langle 0, 2\rangle$, $\langle 1, 1\rangle$, $\langle 2, 0\rangle$; … giving a bijection with $\mathbb{N}$. □

Theorem 12: $\mathbb{Q}$ is countable.

Proof: Enumerate positive reduced fractions p/q ordered by $p + q$ and increasing p; skip non-reduced. Interleave 0 and negatives. This yields *enumeration*, hence $\mathbb{Q} \approx \mathbb{N}$. □

Pairing Functions

Definition 48: A function $f : A \times B \to \mathbb{N}$ is an arithmetical *pairing function* if it is injective.

We say that f *encodes* $A \times B$, and that $f(a, b)$ is the *code* of the pair $\langle a, b \rangle$.

Example: The *Cantor pairing function* $g : \mathbb{N}^2 \to \mathbb{N}$ is defined as:

$$g(n, k) = \frac{(n + k + 1)(n + k)}{2} + n$$

Georg Cantor

Uncountable Sets

Definition 49: A set is *uncountable* if it is not countable.

In order to prove that a set A is *uncountable*, we need to show that *no bijection* $\mathbb{N} \to A$ *can exist*.

The general strategy for showing that is to use *Cantor's diagonal argument*. Given a list of elements of A, say $x_1, x_2, \ldots$ (enumerated by natural numbers), we construct a *new* element of A that *differs* from each x_i, thus showing that the list cannot be complete, and hence no bijection can exist.

Theorem 13: B^ω is uncountable.

Proof: Recall that $\mathbb{B}^\omega$ is the set of all *infinite sequences* of elements from $\mathbb{B} = \{0, 1\}$.
For example, $\mathbb{B}^\omega$ contains sequences like 0000…, 010101…, 1110…, etc.

Suppose for contradiction that $\mathbb{B}^\omega$ is countable. Then we can *enumerate* its elements as $x_1, x_2, \ldots$, where each x_i is an infinite sequence of bits, so we can represent it as $x_i = (b_{i1}, b_{i2}, b_{i3}, \ldots)$, where $b_{ij} \in \mathbb{B}$ is the j-th bit of the i-th sequence.

Uncountable Sets [2]

Now we construct a new sequence $\Delta = \left(\overline{b}_{11}, \overline{b}_{22}, \overline{b}_{33}, \ldots\right)$, where $\overline{b}_{ii} = 1 - b_{ii}$, i.e., we flip the i-th bit of the i-th sequence. This sequence *differs* from each x_i at least in the i-th position, so it cannot be equal to any x_i, so it is *not in* the enumeration $x_1, x_2, \ldots$.

	1	2	3	$\ldots$
x_1	$\boldsymbol{b_{11}}$	b_{12}	b_{13}	$\ldots$
x_2	b_{21}	$\boldsymbol{b_{22}}$	b_{23}	$\ldots$
x_3	b_{31}	b_{32}	$\boldsymbol{b_{33}}$	$\ldots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$
Δ	$\overline{b}_{11}$	$\overline{b}_{22}$	$\overline{b}_{33}$	$\ldots$

Since Δ is constructed from the bits, it is also an *element* of $\mathbb{B}^\omega$. Thus, we have found an element of $\mathbb{B}^\omega$ that is not in the enumeration $x_1, x_2, \ldots$, contradicting the assumption that $\mathbb{B}^\omega$ is countable. □

Sets of Different Sizes

Definition 50: The cardinality of a set A is *less than or the same* as the cardinality of a set B, denoted $|A| \leq |B|$ or $A \preceq B$, if there is an *injection* (one-to-one function) from A to B.

Definition 51: Set A is *smaller* than B, denoted $|A| < |B|$ or $A \prec B$, iff there is an *injection*, but *no bijection* from A to B, i.e., $A \preceq B$ and $A \not\approx B$.

Note: Using this notation, we can say that a set X is *countable* iff $X \preceq \mathbb{N}$, and *uncountable* iff $\mathbb{N} \prec X$.

Example: $\{1, 2\} \prec \{a, b, c\}$, since there is an injection $f : \{1, 2\} \to \{a, b, c\}$ defined by $f(1) = a$ and $f(2) = b$, but no bijection exists.

Example: $\mathbb{N} \preceq \mathbb{Z}$, since there is bijection (and thus an injection) $f : \mathbb{N} \to \mathbb{Z}$.

Example: $\mathbb{Z} \preceq \mathbb{N}$, since there is bijection (and thus an injection) $f : \mathbb{Z} \to \mathbb{N}$.

Example: $\mathbb{N} \prec \mathcal{P}(\mathbb{N})$, since there is an injection $f(x) = \{x\}$, but no bijection exists.

Cantor's Theorem

Theorem 14 (Cantor): $A \prec \mathcal{P}(A)$, for any set A.

Proof: The map $f(x) = \{x\}$ is an injection $f : A \to \mathcal{P}(A)$, since if $x \neq y$, then also $\{x\} \neq \{y\}$ by extensionality, and so $f(x) \neq f(y)$. So we have that $A \preceq \mathcal{P}(A)$.

It remains to show that $A \not\approx B$. For reductio, suppose $A \approx B$, i.e., there is some bijection $g : A \to B$. Now consider $D = \{x \in A \mid x \notin g(x)\}$. Note that $D \subseteq A$, so $D \in \mathcal{P}(A)$. Since g is a bijection, there exists some $y \in A$ such that $g(y) = D$. But now we have

$$y \in g(y) \text{ iff } y \in D \text{ iff } y \notin g(y)$$

This is a contradiction, since y cannot be both *in* and *not in* $g(y)$. Thus, $A \not\approx \mathcal{P}(A)$. □

Schröder–Bernstein Theorem

Theorem 15 (Schröder–Bernstein): If $A \preceq B$ and $B \preceq A$, then $A \approx B$.

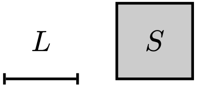
In other words, if there are injections in both directions between two sets, then there is a bijection.

Proof: Obvious, but difficult. 🤷 □

Another Cantor's Theorem

Let L be the unit line, i.e., the set of points $[0, 1]$. Let S be the unit square, i.e., the set of points $L \times L$.

Theorem 16: $L \approx S$.



Proof[3]: Consider the function $f : L \to S$ defined by $f(x) = (x, x)$. This is an injection, since if $f(a) = f(b)$, then $(a, a) = (b, b)$, so $a = b$. Thus, $L \preceq S$.

Now consider the function $g : S \to L$ that maps (x, y) to the real number obtained by *interleaving* the decimal expansions of x and y.

$$\left.\begin{aligned} x &= 0.x_1 x_2 x_3 \ldots \\ y &= 0.y_1 y_2 y_3 \ldots \end{aligned}\right\} \quad g(x, y) = 0.x_1 y_1 x_2 y_2 x_3 y_3 \ldots$$

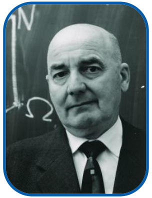
This is an injection, since if $g(a, b) = g(c, d)$, then $a_n = c_n$ and $b_n = d_n$ for all $n \in \mathbb{N}$, so $(a, b) = (c, d)$. Thus, $S \preceq L$.

By Schröder–Bernstein (Theorem 15), we have that $L \approx S$. □

[3] See https://math.stackexchange.com/a/183383 for more detailed analysis.

Order Theory

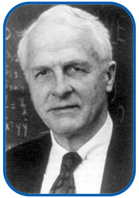
> *“Order is heaven’s first law.”*
>
> ***— Alexander Pope***



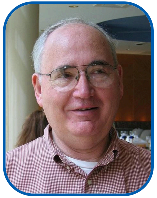
Helmut Hasse

Alfred Tarski

Emmy Noether



Garrett Birkhoff



Dana Scott

Felix Hausdorff

Partially Ordered Sets

Definition 52: A *partially ordered set* (or *poset*) $\langle S, \leq \rangle$ is a set S equipped with a partial order $\leq$.

Definition 53: A *chain* in a poset $\langle S, \leq \rangle$ is a subset $C \subseteq S$ such that any two elements $x, y \in C$ are *comparable*, i.e., either $x \leq y$ or $y \leq x$.

Definition 54: An element $x \in S$ is called a *minimal element* of a poset $\langle S, \leq \rangle$ if there is no “greater” element $y \in S$ such that $y < x$ (i.e., $y \leq x$ and $y \neq x$).

Definition 55: A *maximal element* m satisfies: there is no $y \in S$ with $m < y$.

Note: There may be multiple maximal (or minimal) elements.

Partially Ordered Sets [2]

Definition 56: The *greatest element* of a poset $\langle S, \leq \rangle$ is an element $g \in S$ that is greater than or equal to every other element in S, i.e., for all $x \in S$, $x \leq g$.

Definition 57: A *least element* (bottom) b satisfies $b \leq x$ for all $x \in S$.

Note: Greatest (top) and least (bottom) elements are *unique* when they exist.

Examples:

- $\langle \mathcal{P}(A), \subseteq \rangle$: least $\varnothing$, greatest A.
- $\langle \mathbb{N}^+, | \rangle$: least 1, no greatest element.
- $\langle \mathbb{Z}, \leq \rangle$: no least or greatest element.
- $\langle \{1, ..., 6\}, | \rangle$: least 1, no greatest element, maximal elements are 4, 5, 6.

Upper and Lower Bounds

Definition 58: In a poset $\langle S, \leq \rangle$, an element $u \in S$ is called an *upper bound* of a subset $C \subseteq S$ if it is greater than or equal to every element in C, i.e., for all $x \in C$, $x \leq u$.

Definition 59: In a poset $\langle S, \leq \rangle$, an element $l \in S$ is called a *lower bound* of a subset $C \subseteq S$ if it is less than or equal to every element in C, i.e., for all $x \in C$, $l \leq x$.

Examples:

- In $\langle \mathbb{R}, \leq \rangle$ for interval $C = (0, 1)$: every $x \leq 0$ is a lower bound; every $x \geq 1$ an upper bound.
- In $\langle \mathcal{P}(A), \subseteq \rangle$ for $C = \{\{1, 2\}, \{1, 3\}\}$: lower bounds include $\{1\}$, $\varnothing$; upper bounds include $\{1, 2, 3\}$.
- In $\langle \mathbb{Z}, | \rangle$ for $C = \{4, 6\}$: upper bounds are multiples of 12; least upper bound 12; lower bounds are divisors of 2; greatest lower bound 2.

Suprema and Infima

Definition 60: In a poset $\langle S, \leq \rangle$, the *supremum* (or *join*) of a subset $C \subseteq S$, denoted $\sup(C)$ or $\bigvee C$, is the *least upper bound* of C, i.e., an upper bound $u \in S$ s.t. for any other upper bound $v \in S$, $u \leq v$.

Note: If it exists, the least upper bound is *unique*.

Definition 61: In a poset $\langle S, \leq \rangle$, the *infimum* (or *meet*) of a subset $C \subseteq S$, denoted $\inf(C)$ or $\bigwedge C$, is the *greatest lower bound* of C, i.e., a lower bound $l \in S$ s.t. for any other lower bound $m \in S$, $m \leq l$.

Note: If it exists, the greatest lower bound is *unique*.

Examples:

- $\langle \mathbb{R}, \leq \rangle$: $\sup(\{0, 1\}) = 1$, $\inf(\{0, 1\}) = 0$, i.e., $\sup(C) = \max(C)$, $\inf(C) = \min(C)$.
- $\langle \mathcal{P}(A), \subseteq \rangle$: $\sup = \cup$, $\inf = \cap$.
- Divisibility on $\mathbb{N}_{>0}$: $\sup\{a, b\} = \operatorname{lcm}(a, b)$ (if any common multiple), $\inf\{a, b\} = \gcd(a, b)$.

Lattices

Definition 62: A poset $\langle S, \leq \rangle$ where every non-empty finite subset $C \subseteq S$ has a join (supremum) is called an *upper semilattice* (or *join-semilattice*) and denoted $\langle S, \vee \rangle$.

Definition 63: A poset $\langle S, \leq \rangle$ where every non-empty finite subset $C \subseteq S$ has a meet (infimum) is called a *lower semilattice* (or *meet-semilattice*) and denoted $\langle S, \wedge \rangle$.

Definition 64: A poset $\langle S, \leq \rangle$ that is both an upper semilattice and a lower semilattice, i.e., every non-empty finite subset has both a join and a meet, is called a *lattice*, denoted $(S, \vee, \wedge)$.

Why Lattices?

Why study lattices? Whenever you have:

- Elements that can be *compared* (ordered)
- Ways to *combine* elements (join, meet)
- Consistent behavior under combination

…you likely have a lattice! This structure appears in programming languages, databases, security systems, logic circuits, and many other areas of computer science and mathematics.

Properties of Lattices

Definition 65: A lattice is *bounded* if it has a greatest element $\top$ and a least element $\bot$.

Definition 66: A lattice is *distributive* if $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ (and dually).

Definition 67: A lattice is *modular* if $x \leq z$ implies $x \vee (y \wedge z) = (x \vee y) \wedge z$.

Note: Distributive $\Rightarrow$ modular.

Example (Powerset Lattice): $\langle \mathcal{P}(A), \subseteq \rangle$ is a bounded distributive lattice with $\vee = \cup$, $\wedge = \cap$, $\top = A$, $\bot = \emptyset$.

Why this matters: This is the foundation of set-based reasoning in:

- Database theory (relational algebra)
- Formal specification languages (Z, B-method)
- Model checking and verification

Examples of Lattices

Example (Divisibility Lattice): For positive integers, $a \leq b$ iff a divides b.

- Join: Least Common Multiple (LCM)
- Meet: Greatest Common Divisor (GCD)
- Used in: Number theory, cryptography (RSA), computer algebra systems

Example (Partition Lattice): All partitions of a set S, ordered by refinement.

- $\pi_1 \leq \pi_2$ if π_1 is a refinement of π_2 (smaller blocks)
- Join: Coarsest common refinement
- Meet: Finest common coarsening
- Applications: Clustering, database normalization

Lattices aren't just abstract algebra — they appear everywhere in computer science and mathematics.

The *join* and *meet* operations capture fundamental patterns of *combination* and *interaction*.

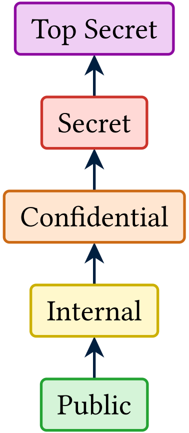
Why Lattices Matter [1]: Information Security Levels

Example: In computer security, information has *classification levels* forming a lattice:

- Elements: $\{\text{Public}, \text{Internal}, \text{Confidential}, \text{Secret}, \text{Top Secret}\}$
- Order: $\text{Public} \leq \text{Internal} \leq \text{Confidential} \leq \text{Secret} \leq \text{Top Secret}$
- Join ($\vee$): Higher classification needed to combine information
- Meet ($\wedge$): Lower classification that both pieces can be declassified to

For instance:

- $\text{Internal} \vee \text{Confidential} = \text{Confidential}$ (combination needs higher level)
- $\text{Secret} \wedge \text{Confidential} = \text{Confidential}$ (both can be declassified to this level)



Why Lattices Matter [2]: Program Analysis and Type Systems

Example: In programming language theory, *types* form lattices:

Subtype Lattice:

- Order: `int` $\sqsubseteq$ `number` $\sqsubseteq$ `any`, `string` $\sqsubseteq$ `any`
- Join: Most general common supertype (for union types)
- Meet: Most specific common subtype (for intersection types)

Control Flow Analysis:

- Elements: Sets of possible program states
- Order: Subset inclusion ($\subseteq$)
- Join: Union of possible states (at merge points)
- Meet: Intersection of guaranteed properties

Why Lattices Matter [3]: Database Query Optimization

Example: *Query execution plans* form a lattice:

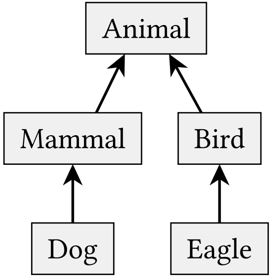
- Elements: Different ways to execute a query
- Order: "Plan A $\leq$ Plan B" if A is more efficient than B
- Join: Combine optimization strategies
- Meet: Find common optimizations

This structure helps database optimizers systematically explore the space of possible query plans.

Why Lattices Matter [4]: Concept Hierarchies and Ontologies

Example: Knowledge representation uses *concept lattices*.

For example, consider a biological taxonomy:



- Elements: Biological concepts (e.g., Animal, Mammal, Dog)
- Order: "Concept A $\leq$ Concept B" if A is a more specific type of B, e.g., "Dog $\leq$ Mammal"
- Join: Most specific common ancestor, e.g., "Mammal $\vee$ Bird $=$ Animal"
- Meet: Most general common descendant, e.g., "Bird $\wedge$ Eagle $=$ Eagle"

Why Lattices Matter [5]: Distributed Systems and Causality

Example: In distributed systems, *events* form a lattice *under causality*:

- Elements: System events with vector timestamps
- Order: “Event A $\leq$ Event B” if A causally precedes B
- Join: Latest information from both events
- Meet: Common causal history

This structure is crucial for:

- Consistent distributed databases
- Version control systems (Git DAG)
- Blockchain consensus algorithms

Why Lattices Matter [6]: Logic and Boolean Reasoning

Example: *Propositional formulas* form lattices:

- Elements: Boolean formulas over variables
- Order: $\varphi \leq \psi$ if φ implies ψ (semantic entailment)
- Join: Disjunction ($\vee$) — weaker condition
- Meet: Conjunction ($\wedge$) — stronger condition

Special case: *Boolean algebra* (`true`, `false`, $\vee$, $\wedge$, $\neg$) used in:

- Digital circuit design
- Database query languages (SQL WHERE clauses)
- Search engines (Boolean search)

TODO

- Applications of lattices in:
  - Formal concept analysis
  - Domain theory in computer science
  - Algebraic topology
  - Cryptography (lattice-based cryptography)
- Advanced topics in set theory:
  - Cardinal arithmetic
  - Ordinal numbers
  - Forcing and independence results
  - Large cardinals
- Connections to Boolean algebra (next lecture)
- Applications in formal logic and proof theory

Looking Ahead: Boolean Algebra

The next lecture will explore *Boolean algebra*, which provides the mathematical foundation for:

- Digital circuit design and computer hardware
- Propositional logic and automated reasoning
- Database query optimization
- Formal verification of software and hardware systems

Key topics will include:

- Boolean functions and their representations
- Normal forms (CNF, DNF)
- Minimization techniques (Karnaugh maps, Quine-McCluskey)
- Functional completeness and Post's theorem
- The satisfiability problem (SAT) and its computational complexity

Preview: Formal Logic

Following Boolean algebra, we will study *formal logic*, covering:

- Propositional and predicate logic
- Natural deduction and proof systems
- Completeness and soundness theorems
- Applications to program verification and AI reasoning

This progression from sets → relations → functions → Boolean algebra → logic provides a solid foundation for advanced topics in discrete mathematics and computer science.

Binary relations are the bridge between sets and functions — they model how objects *connect*, *organize*, and *interact* in mathematical structures and real-world systems.