Theory of Formal Languages and Automata

Lecture 1

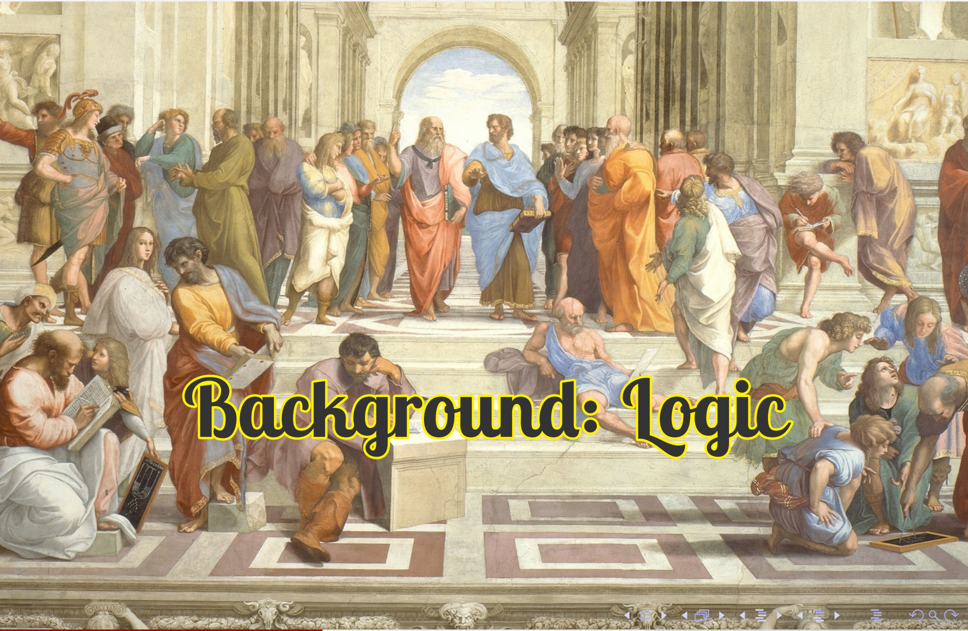
Mahdi Dolati

Sharif University of Technology

Fall 2025

February 8, 2025

- Background:
  - Boolean Logic
  - Sets
  - Functions and Relations
  - Graphs



Background: Logic

Background: Boolean Logic

- Mathematical system built around the two values True and False
- A foundation of digital electronics and computer design
- Boolean values: True and False
  - Representation: True by 1 and False by 0
  - Model two possibilities: High/low voltage, true/false statement, yes/no answer
- Boolean operations: Used for combining simple statements into more complex Boolean expressions
  - Negation: NOT, designated with the symbol $\neg$
  - Conjunction: AND, designated with the symbol $\wedge$
  - Disjunction: OR, designated with the symbol $\vee$

Summary of Boolean operations:

$$
\begin{array}{lll}
0 \wedge 0 = 0 & 0 \vee 0 = 0 & \neg 0 = 1 \\
0 \wedge 1 = 0 & 0 \vee 1 = 1 & \neg 1 = 0 \\
1 \wedge 0 = 0 & 1 \vee 0 = 1 & \\
1 \wedge 1 = 1 & 1 \vee 1 = 1 &
\end{array}
$$

Combining statements (P and Q are called the operands of the operation):

- $P \wedge Q$
- $P \vee Q$

Background: Boolean Logic

More Boolean operations:

- Exclusive or: XOR, designated with the symbol $\oplus$
- Equality: designated with the symbol $\leftrightarrow$
- Implication: designated with the symbol $\rightarrow$

$$
\begin{array}{lll}
0 \oplus 0 = 0 & 0 \leftrightarrow 0 = 1 & 0 \rightarrow 0 = 1 \\
0 \oplus 1 = 1 & 0 \leftrightarrow 1 = 0 & 0 \rightarrow 1 = 1 \\
1 \oplus 0 = 1 & 1 \leftrightarrow 0 = 0 & 1 \rightarrow 0 = 0 \\
1 \oplus 1 = 0 & 1 \leftrightarrow 1 = 1 & 1 \rightarrow 1 = 1
\end{array}
$$

Background: Boolean Logic

Can express all Boolean operations in torem of the AND and NOT operations

$$
\begin{aligned}
P \vee Q &\equiv \neg(\neg P \wedge \neg Q) \\
P \rightarrow Q &\equiv \neg P \vee Q \\
P \leftrightarrow Q &\equiv (P \rightarrow Q) \wedge (Q \rightarrow P) \\
P \oplus Q &\equiv \neg(P \leftrightarrow Q)
\end{aligned}
$$

Distribution law:

$$
\begin{aligned}
P \wedge (Q \vee R) &\equiv (P \wedge Q) \vee (P \wedge R) \\
P \vee (Q \wedge R) &\equiv (P \vee Q) \wedge (P \vee R)
\end{aligned}
$$

Background: Boolean Logic

- Quantifier:
  - Universal (for all):
    - Symbol: $\forall$
    - Example:

$$\forall x \ P(x) \rightarrow Q(x). \tag{1}$$

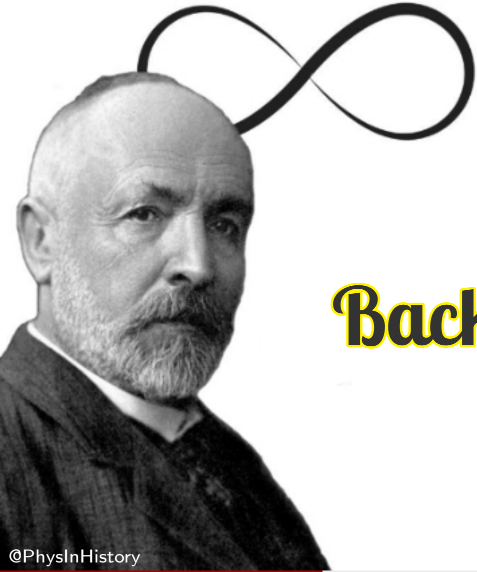
  - Existential (there exists)
    - Symbol: $\exists$
    - Example:

$$\exists x \ P(x) \rightarrow Q(x). \tag{2}$$

  - Combinations:

$$\forall x \exists y \ P(y) > Q(x). \tag{3}$$

- Quantifier: Negation
  - $$\neg(\forall x\ P(x) \rightarrow Q(x)) = \exists x\ \neg(P(x) \rightarrow Q(x)) \quad (4)$$
    $$= \exists x\ \neg(\neg P(x) \vee Q(x)) \quad (5)$$
    $$= \exists x\ (P(x) \wedge \neg Q(x)) \quad (6)$$
  - $$\neg(\exists x\ P(x) \rightarrow Q(x)) = \forall x\ \neg(P(x) \rightarrow Q(x)) \quad (7)$$
    $$= \forall x\ (P(x) \wedge \neg Q(x)) \quad (8)$$
  - $$\neg(\forall x \exists y\ P(y) > Q(x)) = \exists x \forall y\ \neg(P(y) > Q(x)) \quad (9)$$
    $$= \exists x \forall y\ P(y) \leq Q(x) \quad (10)$$



Background: Sets

Background: Sets

- A group of objects.
  - Objects in a set are called its elements or members.
- Definition:
  - List

$$A = \{1, 2, 3\}. \tag{11}$$

  - Dots (infinite set)

$$\mathcal{N} = \{1, 2, 3, \dots\}, \tag{12}$$

$$\mathcal{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}, \tag{13}$$

  - Rule (using set-builder notation):
    - Defining sets by properties is also known as set comprehension and set abstraction.

$$B = \{n | n = m^2 \textbf{ and } m \text{ is an integer}\}. \tag{14}$$

Background: Sets

- Set membership and nonmembership:

$$1 \in \{1, 2, 3\}, \tag{15}$$
$$4 \notin \{1, 2, 3\}, \tag{16}$$

- Cardinality: the number of elements of the set. $|A| = 3$
- Subset:

$$A \subseteq \mathcal{N} \equiv a \in A \to a \in \mathcal{N}, \tag{17}$$

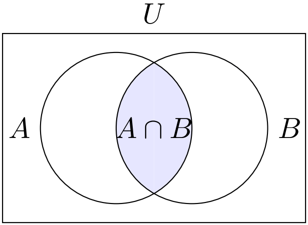
- Proper subset:

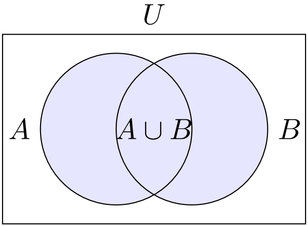
$$A \subsetneq \mathcal{N} \equiv A \subseteq \mathcal{N} \textbf{ and } A \text{ is not equal to } \mathcal{N}, \tag{18}$$

- Multiset: Number of occurrences is important.

$$\{5\} \textbf{ vs. } \{5, 5\}, \tag{19}$$

- Empty set: $\{\}$, $\emptyset$
- Singleton set: $\{10\}$
- Unordered pair: $\{10, 30\}$
- Union: $C = A \cup B$
- Intersection: $C = A \cap C$
- Difference: $C = B - A$
- Complement: $C = \overline{B}$
- Venn diagram





- Empty set:

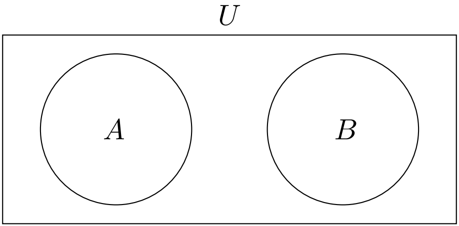
$$A \cup \emptyset = A \tag{20}$$
$$A \cap \emptyset = \emptyset \tag{21}$$
$$A - \emptyset = A \tag{22}$$
$$\emptyset - A = \emptyset \tag{23}$$
$$\overline{\emptyset} = U \tag{24}$$

- DeMorgan's Laws:

$$\overline{A \cup B} = \overline{A} \cap \overline{B} \tag{25}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B} \tag{26}$$
$$\tag{27}$$

Background: Sets

- Disjoint sets: $\emptyset = A \cap B$



Background: Sets

- Powerset: Is is set of sets
- Powerset of A is the set of all the subsets of A: 2^A

Example

$A = \{a, b, c\}$
$2^A = \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

- $|2^A| = 2^{|A|}$
- $\emptyset \in 2^A$

Theorem (Cantor Theorem)

For any set A,

$$|A| < |\mathcal{P}(A)|. \tag{28}$$

Background: Sequences and Tuples

- Sequence: A list of objects in some order

$$D = (5, 3, 13), \tag{29}$$

- Order and repetition does matter in a sequence
- Tuple: A finite sequence
- k-tuple: A sequence with k elements
- 2-tuple: Ordered pair

Background: Cartesian Product

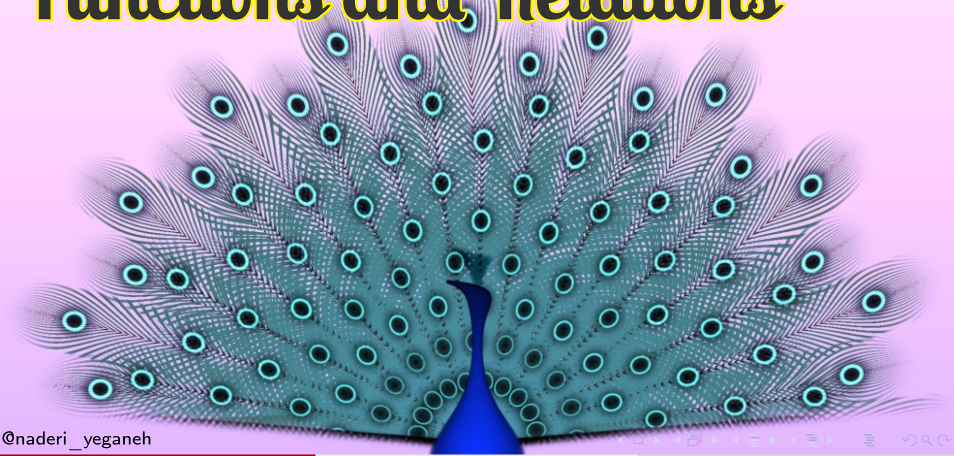
- Cartesian product or Cross product: $A \times B$
- $A \times B$: Set of all ordered pairs (a, b) such that $a \in A$ and $b \in B$
- Cartesian product of k sets: $A_1 \times \cdots \times A_k = \{(a_1, \ldots, a_k) | a_i \in A_i\}$

Example

$A = \{1, 2\}$
$B = \{x, y, x\}$
$A \times B = \{(1, x), (1, y), (1, z), (2, x), (2, y), (2, z)\}$
$A \times B \times A = \{(1, x, 1), (1, x, 2), (1, y, 1), (1, y, 2), (1, z, 1), (1, z, 2),$
$(2, x, 1), (2, x, 2), (2, y, 1), (2, y, 2), (2, z, 1), (2, z, 2)\}$

- $A^k = \underbrace{A \times \cdots \times A}_{\text{k}}$

Background: Functions and Relations



@naderi_yeganeh

Background: Functions and Relations

- A function (mapping) is an object that sets up an input-output relationship

$$f(a) = b. \tag{30}$$

- f maps a to b
- Domain: Set of possible inputs
- Range: Set of possible outputs

$$f : D \to R. \tag{31}$$

- A function is onto the range if it uses all the elements of the range

Example

Addition function: add: $\mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}$
Absolute function: abs: $\mathcal{Z} \times \mathcal{Z} \to \mathcal{Z}$

Background: Functions and Relations

Example

$f : \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, 3, 4\}$

n	$f(n)$
0	1
1	2
2	3
3	4
4	0

$\mathcal{Z}_m = \{0, 1, \ldots, (m-1)\}$
$f : \mathcal{Z}_5 \rightarrow \mathcal{Z}_5$
$f(n) \equiv (n+1) \mod 5$

- Injective, one-to-one function:
  - $a_1 \neq a_2 \rightarrow f(a_1) \neq f(a_2)$.

Example

$f : \{0, 1, 2, 3, 4\} \rightarrow \{0, 1, 2, 3, 4\}$

n	$f(n)$
0	1
1	2
2	3
3	4
4	0

n	$f(n)$
0	1
1	2
2	1
3	2
4	1

- Bijection, one-to-one correspondence, or invertible function:
  - Injective and onto

Example

- $f : \{0,1,2,3,4\} \to \{0,1,2,3,4\}$

n	$f(n)$
0	1
1	2
2	3
3	4
4	0

n	$f(n)$
0	1
1	2
2	1
3	2
4	1

n	$f(n)$
0	1
1	2
2	3
3	4

- When cardinality of the domain and range is not equal:
  - $f : \{0,1,2,3\} \to \{0,1,2,3,4\}$
  - $f : \{0,1,2,3,4\} \to \{0,1,2,3\}$

- Two sets A and B are of equal **cardinality**, written as

$$|A| = |B|, \tag{32}$$

if and only if there exists a bijective function $f: A \to B$.

- We write

$$|A| \leq |B|, \tag{33}$$

if there exists $C \subseteq B$ such that $|C| = |A|$.

- We write

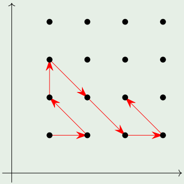
$$|A| < |B|, \tag{34}$$

if $|A| \leq |B|$ and $|A| \neq |B|$.

- Set A is finite if there is some integer $n \geq 0$ such that $|A| = |\{1, 2, \ldots, n\}|$.
- Set A is infinite if it is not finite.
- Set A is denumerable if it can be put in a one-to-one correspondence with $\mathcal{N}$.
- Set A is countable if it is finite or denumeratble.
- Set A is uncountable if it is not countable.

Example

- Countable:
  - Positive integers: $1, 2, 3, \ldots$
  - Integers: $0, 1, -1, 2, -2, 3, -3, \ldots$
  - Pairs of positive integers:
  - Rational numbers between zero and one:
    - $\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, \ldots$
    - $\frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{4}, \quad , \frac{3}{4}, \ldots$



- Uncountable:
  - The interval $[0, 1]$.
  - $\mathcal{P}(\mathcal{N})$.
  - Set of all functions $f : \mathcal{N} \to \{0, 1\}$.

- Cardinality of sets:
  - Finite: Number elements in the set,
  - Infinite: A special object called transfinite cardinal number.
- First transfinite cardinal number $\aleph_0 := |\mathcal{N}|$.
- Second transfinite cardinal number is $\aleph_1 := |\mathcal{R}|$ according to continuum hypothesis (CH):
  - First of Hilbert's 23 problems (presented in 1900),
  - Cantor, in 1874, proved that $\mathfrak{c} = |\mathbb{R}| = 2^{\aleph_0} > \aleph_0$,
  - Hypothesis: $\nexists S \; \aleph_0 < |S| < \mathfrak{c}$.
  - Cohen and Gödel proved that the answer to CH is independent of ZFC.

Background: Functions and Relations

- k-ary function
  - k: arity of the function
  - Domain of f is $A_1 \times \dots A_k$
  - Input of f is a k-tuple $(a_1, \dots a_k)$
  - a_i is an argument to f
- unary function: $k = 1$
- binary function: $k = 2$
- Prefix notation: $add(a, b)$
- Infix notation: $a + b$

Background: Functions and Relations

- Predicate or property
  - A function
  - Its range is $\{True, False\}$
  - Example: even(n). even(3)=False, even(6)=True.
- Relation, or k-ary relation or k-ary relation on A
  - A property
  - Its domain is a set of k-tuples $A \times \cdots \times A$
  - 2-ary relation: Binary relation
  - Use infix for binary relation: $a < b$, $x = y$
- The statement alone implies the True case:

$$aRb \equiv aRb = True \tag{35}$$

$$R(a_1, \ldots, a_k) \equiv R(a_1, \ldots, a_k) = True \tag{36}$$

Background: Functions and Relations

- Describe predicates with sets
- $P : D \rightarrow \{True, False\}$
- (D, S), where $S = \{a \in D | P(a) = True\}$
- S is sufficient if D is obvious from the context

Example

beats	Scissors	Paper	Store
Scissors	False	True	False
Paper	False	False	True
Stone	True	False	False

{ (Scissors, Paper), (Paper, Store), (Stone, Scissors) }

Background: Functions and Relations

- Types of relations R on set A:
  1. R is reflexive:
  $$\forall x \in A \quad xRx. \tag{37}$$
  2. R is symmetric:
  $$\forall x, y \in A \quad xRy \to yRx. \tag{38}$$
  3. R is anti-symmetric:
  $$\forall x, y \in A \quad xRy \text{ and } yRx \to x = y. \tag{39}$$
  4. R is transitive:
  $$\forall x, y, z \in A \quad xRy \text{ and } yRz \to xRz. \tag{40}$$

Background: Functions and Relations

- Equivalence relation: Special type of binary relation
- Binary relation R is an equivalence relation if:
  1. R is reflexive.
  2. R is symmetric.
  3. R is transitive.

Example

Relation $\equiv_7$: $\mathcal{N}^2 \to \{True, False\}$
$i \equiv_7 j$, if $(i - j)$ is a multiple of 7

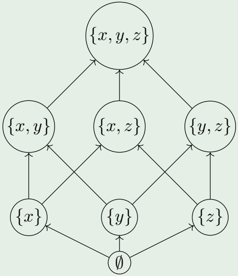
1. Reflexive: $i \equiv_7 i$, as $(i - i) = 0$ is a multiple of 7
2. Symmetric: $i \equiv_7 j$ implies $j \equiv_7 i$, as $(j - i)$ is a multiple of 7 if $(i - j)$ is a multiple of 7
3. Transitive: $i \equiv_7 j$ and $j \equiv_7 k$ implies $i \equiv_7 k$, as $i - k = (i - j) + (j - k)$ is the sum of two multiples of 7

Background: Functions and Relations

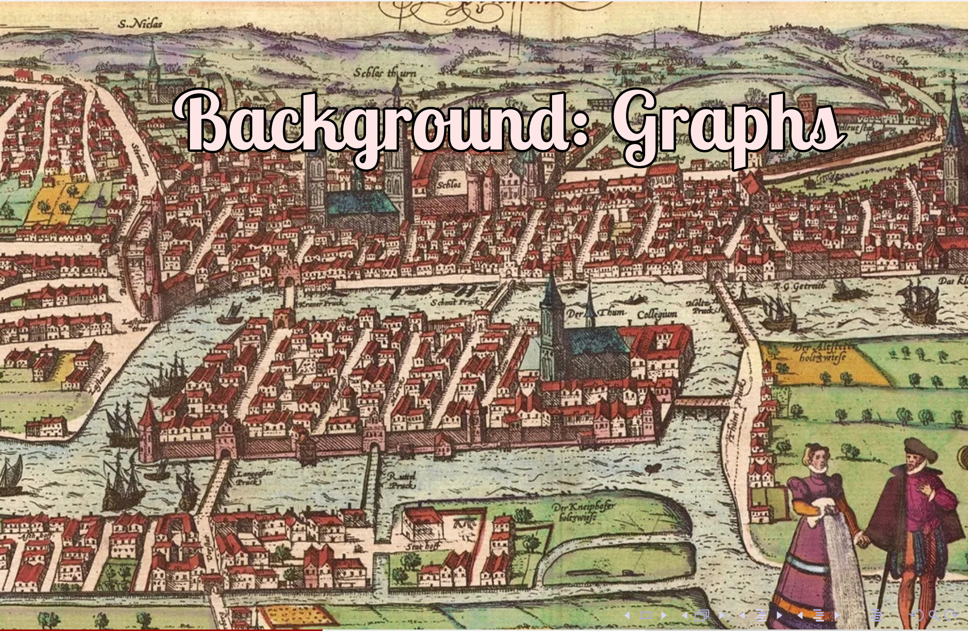
- Partial ordering relation: Special type of binary relation
- Binary relation R is a partial ordering relation if:
  1. R is reflexive.
  2. R is anti-symmetric.
  3. R is transitive.

Example

- Each set is a subset of itself.
- If $A \subseteq B$ and $B \subseteq A$, then A is equal to B.
- If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

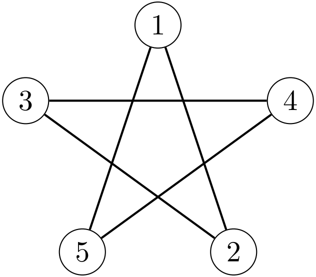


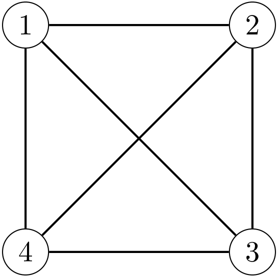
Background: Graphs



Background: Graphs

Graph: A set of points with lines connecting some of the points
Points: Nodes or vertices
Lines: Edges



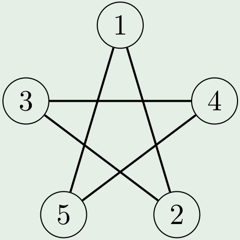


Degree: Number of edges at a node
Only one edge between each pair of nodes
Self-loop

Background: Graphs

- $G = (V, E)$
- $(i, j) \in E$, where $i, j \in V$
- Undirected graph: (i, j) and (j, i) represent the same edge
  - Describe with unordered pairs $\{i, j\}$

Example



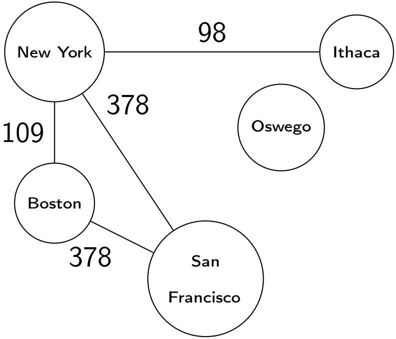
$(\{1,2,3,4,5\}, \{(1,2),(2,3),(3,4),(4,5),(5,1)\})$

Background: Graphs

Examples:

- V=cities, E=connecting highways
- V=people, E=friendships between people

Labeled graph: label nodes and/or edges

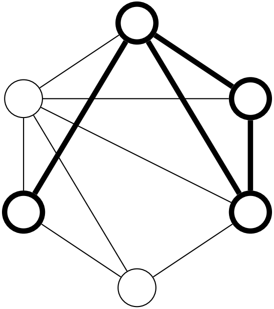


Background: Graphs

Subgraph: G is a subgraph of H

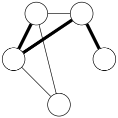
- Nodes of G are a subset of the nodes of H
- Edges of G are the edges of H on the corresponding nodes

Example: G (shown darker) is a subgraph of H

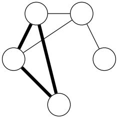


Background: Graphs

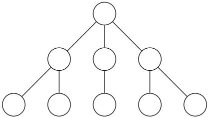
- Path: A sequence of nodes connected by edges
- Simple path: A path that does not repeat any nodes
- Connected graph: There is a path between every pair of nodes
- Cycle: A path that starts and ends in the same node
- Simple Cycle: Has at least three nodes and only repeats the first and last nodes
- Tree: A connected graph that has no simple cycles
- Leave: Node of degree one
- Root: A designated node



(a) A path



(b) A cycle

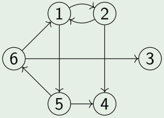


(c) A tree

Background: Graphs

- Directed graph: Has arrows instead of lines
- Outdegree: Arrows pointing from the node
- Indegree: Arrows pointing to the node
- Ordered pair (i, j): Edge from i to j

Example



$$(\{1,2,3,4,5,6\}, \{(1,2),(1,5),(2,1),(2,4),(5,4),(5,6),(6,1),(6,3)\}) \tag{42}$$

Background: Graphs

- Directed path: A path in which all the arrows pint in the same direction as its steps
- Strongly connected: A directed path connects every two nodes

Can depict binary relations with directed graphs:

- Binary relation: R
- Domain: $D \times D$
- Directed graph: $G = (D, E)$, $E = \{(x, y) | xRy\}$

Example

Relation *beats*