

Motivation

Bernhard Nebel und Christian Becker-Asano

Course Content

- *Introduction to logic*
 - ★ *Propositional*
 - ★ *First order logic*

- *Theoretical foundations of computer science*
 - ★ *Automata Theory*
 - ★ *Formal languages, grammars*
 - ★ *Decidability*
 - ★ *Computational Complexity*

Theoretical Computer Science motivation

- *Overall question :*
 - ★ *What are the fundamental capabilities and limitations of computers ?*
- *Subquestions :*
 - ★ *What is the meaning of computation ?*
 - ★ *Automata theory*
 - ★ *What can be computed ?*
 - ★ *Computability/Decidability theory*
 - ★ *What can be computed efficiently ?*
 - ★ *Computational complexity*

What is the meaning of computation ?

➤ 1930-50s : Automata theory ?

★ Various mathematical models of computers

- ★ Automata theory

- ★ Turing Machines

- ★ Grammars (Noam Chomsky)

- ★ Practical :

 - ★ Many devices (dishwashers, telephones, ...)

 - ★ Compilers and languages

 - ★ Protocols

What can be computed ?

- *What can be computed using Turing Machines?*
 - ★ *Some problems can be solved algorithmically*
 - ★ *E.g. sorting*
 - ★ *Others cannot :*
 - ★ *E.g. the halting problem determine whether Turing machine M accepts w or not*
 - ★ *May not terminate (if M loops)*
 - ★ *E.g. Goedel : no algorithm can decide in general whether statements in number theory are true or false*
 - ★ *Practical :*
 - ★ *It is important to know what can be computed and what not*

What can be computed efficiently ?

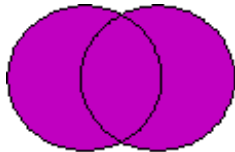
➤ *Examples*

- ★ *Sorting can be done efficiently*
- ★ *Scheduling cannot be done efficiently*
 - ★ *University lectures*
- ★ *Complexity theory gives an explanation*
 - ★ *NP-hard problems*
- ★ *Practical :*
 - ★ *Important to know how hard your problem is*
 - ★ *Cryptography*

Some mathematical concepts: Sets

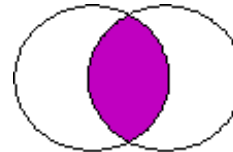
- A set is a group of objects
 - ★ $\{4,7,12\}$, the empty set is denoted \emptyset or $\{\}$
- Membership is denoted with \in and \notin :
 - ★ $4 \in \{4,7,12\}$ and $5 \notin \{4,7,12\}$
- Subset \subseteq and proper subset \subset :
 - ★ $\{12,4,7\} \subseteq \{4,7,12\}$ and $\{4,7\} \subset \{4,7,12\}$
- Union (\cup) and intersection (\cap):

★ $A \cup B$



and

$A \cap B$



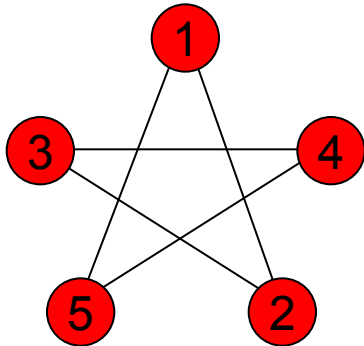
Mathematical concepts: Sequences and Sets

- Sequence is a list of object in some order:
 - ★ $(4,7,12)$ is not the same as $(12,7,4)$
- Finite or infinite sequences:
 - ★ finite are often called *tuples*, or *k-tuples* (a tuple with k elements).
A 2-tuple is called a *pair*.
- Power set
 - ★ $A = \{0,1\}$ the power set $A^P = \{\{\}, \{0\}, \{1\}, \{0,1\}\}$
- Cartesian product or cross product
 - ★ $A = \{a, b\}$ and $B = \{1,2,3\}$
 $A \times B = \{\{a, 1\}, \{a, 2\}, \{a, 3\}, \{b, 1\}, \{b, 2\}, \{b, 3\}\}$

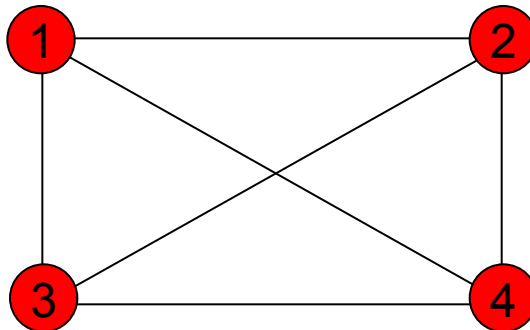
Some mathematical concepts: Graphs

► Graphs $G = (V, E)$

$$G_1 = (\{1,2,3,4,5\}, \{\{1,2\}, \{2,3\}, \{3,4\}, \{4,5\}, \{5,1\}\})$$

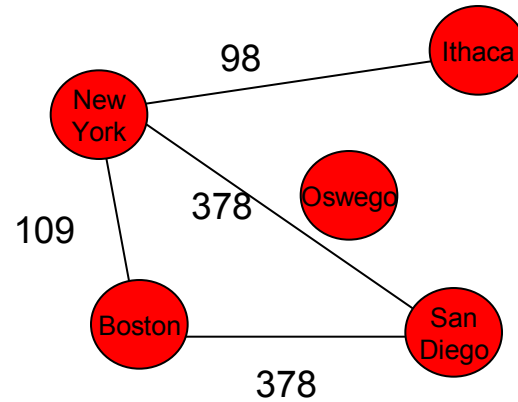


$$G_2 = (\{1,2,3,4\}, \{\{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}\})$$

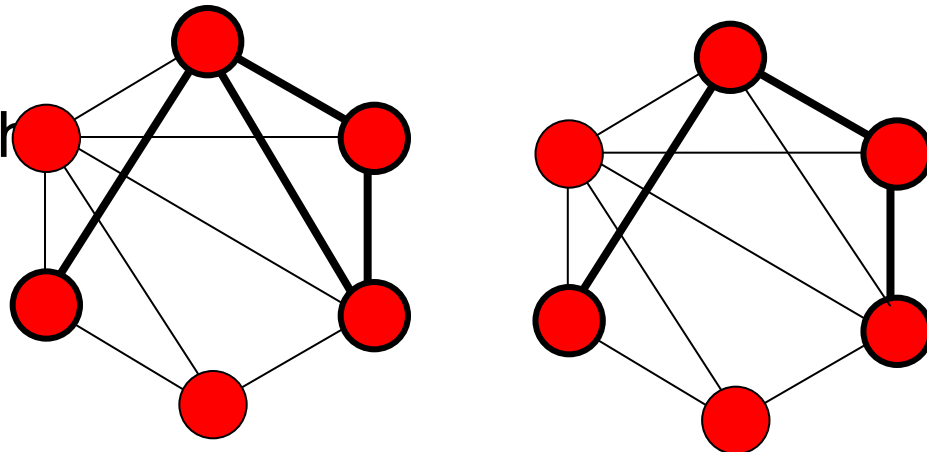


Some mathematical concepts: Graphs II

➤ Labelled

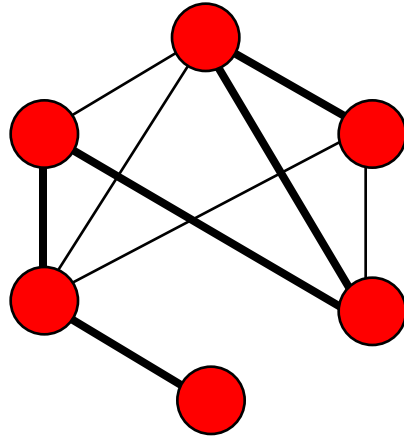


➤ Subgraph
induced subgraph

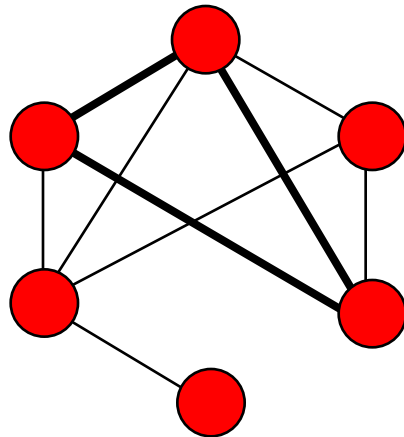


Some mathematical concepts: Graphs III

➤ Path

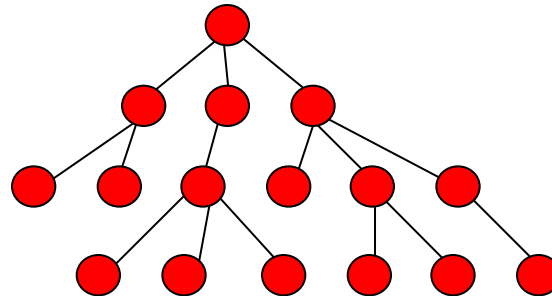


➤ Cycle

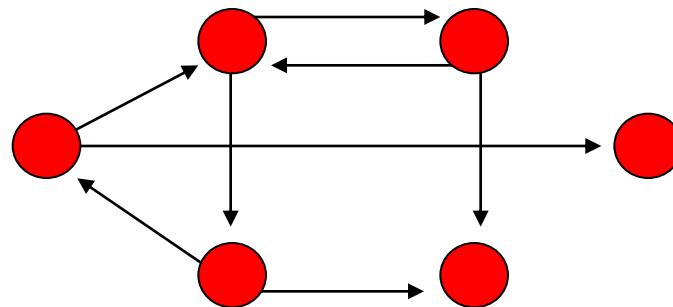


Some mathematical concepts: Graphs IV

➤ Trees



➤ Directed Graph



Strings and Languages

- Alphabet = set of symbols
 - ★ e.g.: $\Sigma = \{a, b, c\}$
- String = sequence of symbols over alphabet
 - ★ e.g. aabbabcca
- Length $|w|$ = number of symbols in w
- Empty string = ε
- $aabb$ is substring of $aaabbbbccc$
- xy concatenation of two strings x and y
- $x^k = x \dots x$ (z.B. $x^3 = xxx$)
- Language is a set of strings (over an alphabet Σ)

Mathematical proofs

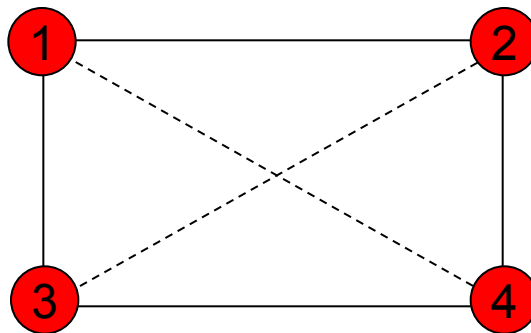
- *Various types of proofs*
 - ★ *Direct proof*
 - ★ *Proof by construction/counterexample*
 - ★ *Proof by contradiction (indirect proof, reductio ad absurdum)*
 - ★ *Proof by induction*
- *How formal?*
 - ★ *Formal enough to be convincing to your audience*

Direct proof

- Strategy: Logically derive conclusions from your premises until you arrive at the desired conclusion.
- Example:
Let a, b, c be integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.
- Proof:
 - ★ From $a \mid b$, we get: (1) ex. integer k_1 s.t. $b = k_1 \cdot a$
 - ★ From $b \mid c$, we get: (2) ex. integer k_2 s.t. $c = k_2 \cdot b$
 - ★ From (1) and (2) we get: (3) ex. integers k_1, k_2 s.t. $c = k_2 \cdot k_1 \cdot a$
 - ★ From (3) we get: (4) ex. integer k s.t. $c = k \cdot a$ (namely, $k = k_2 \cdot k_1$)
 - ★ From (4) we get that $a \mid c$.

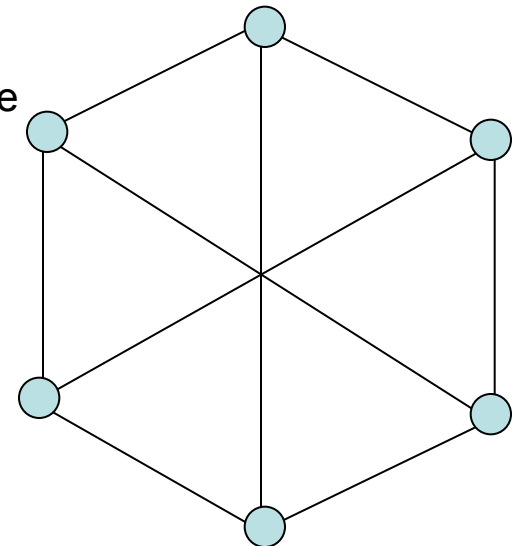
Proof by construction

- *Objective: prove that a particular type of object exists*
 - ★ *Proof strategy: Demonstrate how to construct the object.*
- **Example:**
 - ★ **Definition:** A graph is k -regular if all vertices have degree k
 - ★ **Theorem:** For all even numbers $n > 2$, there exists a 3-regular graph with n nodes



Proof by Construction II

- Proof: (Let $n > 2$ be an even number.)
 - $G = (V, E)$ with
 - ★ $V = \{0, 1, \dots, n - 1\}$ and
 - ★ $E = \{\{i, i + 1\} \mid \text{for } 0 \leq i \leq n - 2\} \cup \{\{n - 1, 0\}\} \cup \{\{i, i + n/2\} \mid \text{for } 0 \leq i \leq n/2 - 1\}$
 - ★ \rightarrow every vertex has exactly three neighbours:
 - ★ its predecessor in the cycle $0, 1, 2, \dots, n - 1, 0$
 - ★ its successor in the cycle
 - ★ its „mirror image“ $n/2$ positions before/ahead in the cycle
- Why do we need $n > 2$ as a requirement?



Proof by contradiction

- **Theorem:** $\sqrt{2}$ is irrational
- **Proof strategy:**
 - ★ Assume that the theorem is not true.
 - ★ Show that this leads to a contradiction, and hence the theorem must be true.

Proof by Contradiction

- **Theorem:** $\sqrt{2}$ is irrational
- **Proof:** Assume the theorem is not true, then:

□

$$\sqrt{2} = \frac{b}{a} \quad \text{where } a \text{ and } b \text{ are integers and } \frac{b}{a} \text{ is reduced.}$$

$$2 = \frac{b^2}{a^2}$$

$$2a^2 = b^2 \quad \text{hence, } b^2 \text{ is even, hence } b \text{ is even}$$

now, we can write $b = 2c$, which gives:

$$2a^2 = 4c^2 \quad \text{divide by 2, gives:}$$

$$a^2 = 2c^2 \quad \text{hence, } a^2 \text{ is even, hence } a \text{ must be even}$$

CONTRADICTION

Proof by induction

- *Prove a statement $S(X)$ about a family of objects (e.g. integers, trees) in two parts :*
 - ★ *Basis: prove for one or several small values of X directly*
 - ★ *Inductive step: Assume $S(Y)$ for Y smaller than X ; prove $S(X)$ using that assumption*
- *Applies to*
 - ★ *Natural numbers*
 - ★ *Inductively defined objects (structured induction)*

Inductively defined: example

Rooted binary trees are inductively defined

- **Basis:** a single node is a tree and that node is the root of the tree

- **Induction:** if T_1 and T_2 are rooted binary trees, then the tree constructed as follows is a rooted binary tree:
 - ★ Begin with a new node N
 - ★ Add copies of T_1 and T_2
 - ★ Add edges from N to T_1 and T_2

Proof by induction: example

Theorem: A binary tree with n leaves has $2n - 1$ nodes

➤ Basis:

★ if a tree has one leaf, then it is a one node tree $2 * 1 - 1 = 1$

➤ Induction:

★ assume $S(T)$ for trees with fewer nodes than T , in particular for subtrees of T (*i.e. use the theorem as an assumption, and use the smaller trees of T , namely U and V to prove it*)

★ T must be a root plus two subtrees U and V

★ If U and V have x and y leaves respectively and T has z leaves, then
 $z = x + y$

★ By the induction assumption, U and V have $2x - 1$ and $2y - 1$ nodes, resp.

★ Then T has

$$\begin{aligned} & 1 + (2x - 1) + (2y - 1) \text{ nodes:} \\ & 1 + (2x - 1) + (2y - 1) \\ & = 2(x + y) - 1 \\ & = 2z - 1 \end{aligned}$$

(*q. e. d.*)