1. Motivation

Malte Helmert and Andreas Karwath

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?

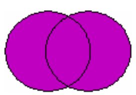
- *What can be computed using Turing Machines?*
  - *Some problems can be solved algorithmically*
    - *E.g. sorting a list of numbers*
  - *Others cannot:*
    - *E.g. the halting problem: determine whether a given program will ever terminate*
    - *E.g. Gödel: no algorithm can decide in general whether statements in number theory are true or false*
  - *Practical:*
    - *It is important to know what can be computed and what not*

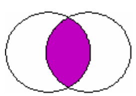
What can be computed efficiently?

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

Some mathematical concepts: sets

- A set is a group of objects (unordered, no duplicates)
  - {4,7,12}
  - { x | x is a natural number, x is even }
  - empty set: $\emptyset$ 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 $A \cap B$





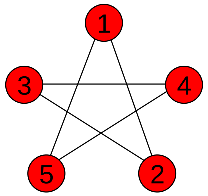
Mathematical concepts: sequences and sets

- Sequence is a list of objects in some order:
  - $\langle 4,7,12 \rangle$ is not the same as $\langle 12,7,4 \rangle$
  - $\langle 4,4 \rangle$ is not the same as $\langle 4 \rangle$
  - Convention: often use (…) instead of $\langle … \rangle$
- Finite or infinite sequences:
  - finite sequences often called *tuples*, or *k-tuples* (a tuple with *k* elements). A 2-tuple is called a *pair.*
- Power set
  - power set $\mathcal{P}(A)$: set of all subsets of A
  - $A = \{0,1\} \Rightarrow$ power set $\mathcal{P}(A) = \{\{\},\{0\},\{1\},\{0,1\}\}$
- Cartesian product or cross product
  - $A = \{a,b\}$ and $B = \{1,2,3\}$
    $\Rightarrow A \times B = \{\langle a, 1\rangle, \langle a, 2\rangle, \langle a, 3\rangle, \langle b,1\rangle, \langle b, 2\rangle, \langle b, 3\rangle\}$

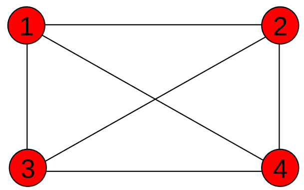
Some mathematical concepts: graphs

- Graph $G=(V,E)$ (vertices and edges)

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

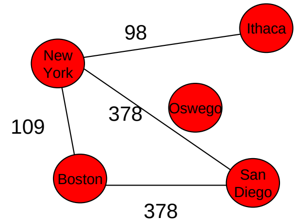


G_2= ({1,2,3,4}, {{1,2}, {1,3}, {1,4}, {2,3}, {2,4}, {3,4}})

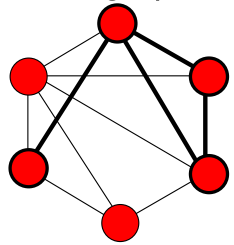


Some mathematical concepts: Graphs II

- Labelled, weighted

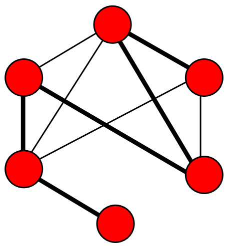


- Subgraph, induced subgraph

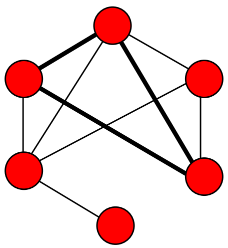


Some mathematical concepts: Graphs III

- (Simple) path

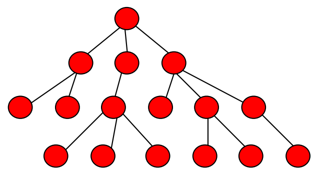


- (Simple) cycle

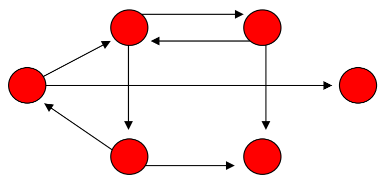


Some mathematical concepts: Graphs IV

- Tree



- Directed graph



Strings and languages

- Alphabet = set of symbols
  - e.g.: $\Sigma = \{a,b,c\}$
- Word/string = finite sequence of symbols over alphabet
  - e.g. aabbabcca
- Length |w| = number of symbols in w
- Empty word = ε
- *aabb* is subword of *aaabbbbccc*
- *xy* concatenation of two words *x* and *y*
- $x^k = x...x$ (e.g. $x^3 = xxx$)
- Language is a set of words (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

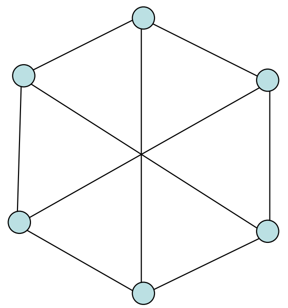
- Strategy: Logically derive conclusions from your premises until you arrive at the desired conclusion.
- Example:
  Let a, b, c be integers. If a | b and b | c, then a | c.
- Proof:
  - From $a \mid b$, we get: (1) ex. integer k_1 s.t. $b = k_1 \cdot a$
  - From $b \mid c$, we get: (2) ex. integer k_2 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, $k = k_2 k_1$)
  - 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:
  - G=(V,E) with
    - V = {0,1,...,n-1} and
    - E = {{i,i+1} | for 0 ≤ i ≤ n-2 } ∪ {{n-1,0}} ∪ {{i, i+n/2} | 0 ≤ i ≤ n/2-1 }}
    - → every vertex has exactly three neighbours:
      - its predecessor in the cycle 0, 1, 2, …, n-1, 0
      - its successor in the cycle
      - its "mirror image" n/2 positions before/ahead in the cycle



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 that the theorem is not true. Then:

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

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

$2a^2 = b^2$ hence, b^2 is even, hence b is even

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

$2a^2 = 4c^2$ divide by 2, gives:

$a^2 = 2c^2$ hence, a^2 is even, hence a 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 object constructed as follows is a rooted binary tree:
  - Begin with a new node *N as the root*
  - 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, and 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 *u* and *v* leaves respectively and *T* has *t* leaves, then $t = u + v$
  - By the induction assumption, *U* and *V* have *2u-1* and *2v-1* nodes, respectively
  - Then *T* has 1+*(2u-1)*+*(2v-1)* nodes

$$
\begin{aligned}
&1+(2u-1)+(2v-1)\\
&= 2(u+v)-1\\
&= 2t-1
\end{aligned}
$$