CSCI-661: FOUNDATIONS OF COMPUTER SCIENCE THEORY

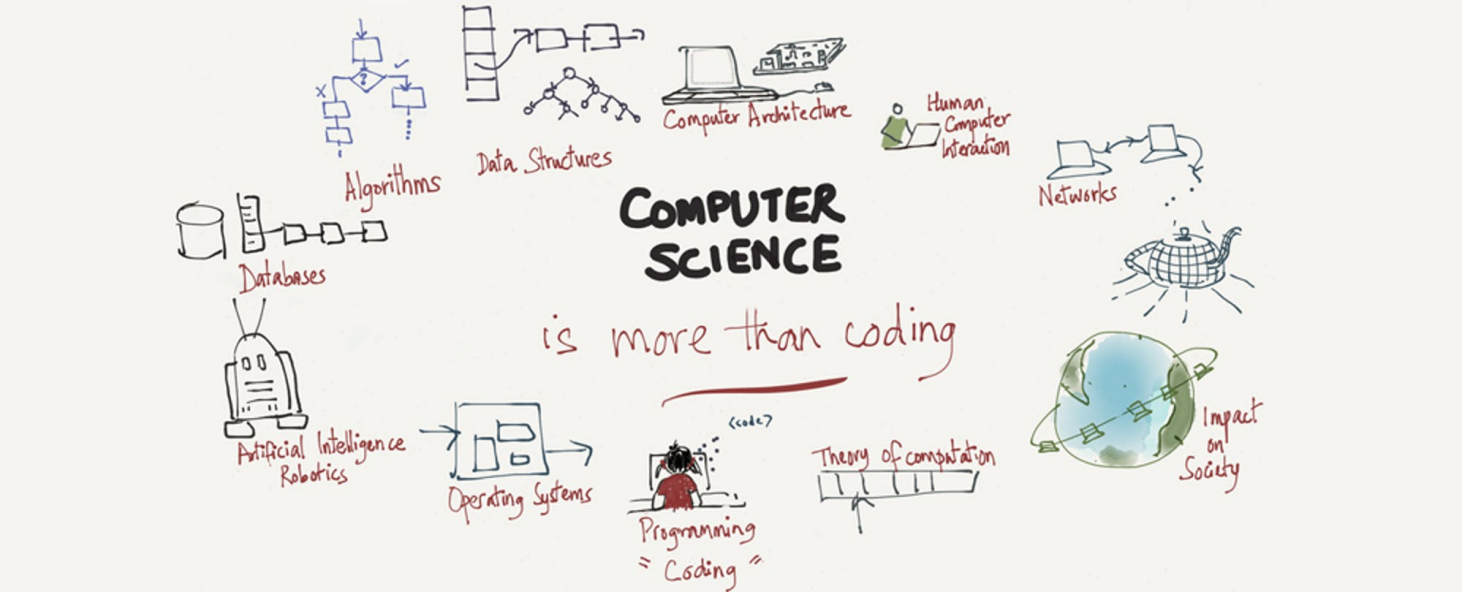
Instructor: Stanisław Radziszowski

Based on slides from Aaron Deever and Monika Polak

Overview of the Course

Foundations of CS Theory

- formalization of computation
- various models of computation (increasing difficulty/power)
- what can / cannot be done ?



Why a Theory Course?

– relevant to practice

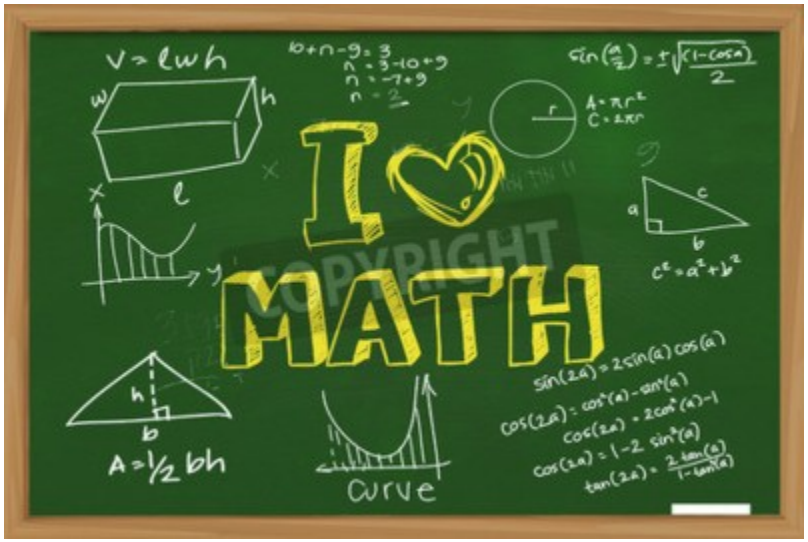
- grammars for programming languages
- finite automata & regular expressions for pattern matching of strings
- NP-completeness to determine required time complexity (e.g. for cryptography)

– problem solving skills independent of current technology (specific programming languages, etc.), ability to express ideas clearly, succinctly, and correctly

Introduction

- **Automata Theory**
  - mathematical models of computation
- **Computability Theory**
  - what can be computed ?
- **Complexity Theory**
  - which problems are computationally hard / easy ?

Discrete Math Review



Outline

- Sets
- Relations
- Proofs

Sets

- A set is a collection of elements.
  - Finite set – has finite number of elements
    - $A = \{ 1, 3, 5, 6, 9 \}$
  - Infinite Set – has infinite number of elements
    - $B = \{ x \mid x \text{ is an odd integer} \}$
  - Null (Empty) set – has no elements.
    - $\varnothing$

Sets

- Describing a set
  - Enumeration – list all elements
    - $A = \{ 1, 3, 5, 6, 9 \}$
  - Describe set based on one or more properties of the members
    - $B = \{ x \mid x \text{ is an odd integer and } x > 10 \}$
      - The notation $B = \{ x \mid P(x) \}$ is interpreted as “B is the set of all x such that P(x) is true”

- Membership
  - If an element x is a member of a set A, we write:
    - $x \in A$.
  - If an element x is not a member of a set A, we write:
    - $x \notin A$
- Subsets
  - A is a subset of B if all elements of A are also in B.
  - $A \subseteq B$ if $x \in A$ implies $x \in B$
  - $A = B$ is the same as saying $A \subseteq B$ and $B \subseteq A$.
- Power Set
  - Set of all subsets of A
  - Sometimes written as P(A)

Sets – Cardinality

- Cardinality
  - For set A, |A| represents the cardinality of the set
    - |A| = the number of elements in the set
  - A = { 1, 3, 5, 6, 9 }
    - |A| = 5
  - If |B| = 0, then B = ∅
  - If |A| = N
    - How many elements in P(A)?
    - 2^N

Set Operations

- Union
  - $A \cup B$ = set consisting of all elements in either A or B or both.
- Intersection
  - $A \cap B$ = set of elements that are in both A and B
  - If $A \cap B = \varnothing$, A and B are disjoint.
- Difference
  - $A - B$ = set of all elements of A that are not elements of B
- Complement (with respect to a universal set U)
  - A' = All elements in U that are not in A
  - $U - A$

Set Operations

- $A = \{ 1, 3, 5, 6, 9 \}$
- $B = \{ x \mid x \text{ is an odd integer} \}$

- $A \cup B = \{ x \mid x = 6 \text{ or } x \text{ is an odd integer} \}$
- $A \cap B = \{ 1, 3, 5, 9 \}$
- $A - B = \{ 6 \}$
- $B' = \{ x \mid x \text{ is an even integer} \}$
  - With respect to the universal set of integers.

Set Operations

- What's another way to write A – B ?
  - $A \cap B'$
- Suppose A, B are finite sets.
  - How can $|A \cup B|$ be written in terms of
    - $|A|$, $|B|$, and $|A \cap B|$?
    - $|A \cup B| = |A| + |B| - |A \cap B|$
  - What must be true if $|A \cup B| = |A| + |B|$?
    - A and B are disjoint
    - $A \cap B = \varnothing$

(Some) Laws Involving Sets

- Commutative
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Associative
  - $A \cup (B \cup C) = (A \cup B) \cup C$
  - $A \cap (B \cap C) = (A \cap B) \cap C$
- Distributive
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(Some) Laws Involving Sets

- DeMorgan
  - $(A \cup B)' = A' \cap B'$
  - $(A \cap B)' = A' \cup B'$
- Other
  - $(A')' = A$
  - $A \cap A' = \varnothing$
  - $A \cup A' = U$ (universal set)
  - $A \cup \varnothing = A$
  - $A \cap \varnothing = \varnothing$

Cartesian Product of Sets

- A x B = set of ordered pairs (a,b) such that
  - $a \in A$ and $b \in B$.
- A x B x C = set of ordered triplets (a, b, c) such that
  - $a \in A$ and $b \in B$ and $c \in C$
- In general: $A_1 \times A_2 \times \ldots \times A_n$ = the set of all n-tuples $(a_1, a_2, \ldots, a_n)$ such that
  - $a_i \in A_i$ for all i.

Relations

- Means to relate or associate a member of one set with a member of another
  - Relation from A to B is simply a subset of A x B
    - If $a \in A$ is related to $b \in B$ then $(a, b) \in R$
    - Can also be written aRb
    - Or R(a) contains b
  - Could involve more than 2 sets; we'll stick with two
    - Binary relation from A to B

Binary Relation Expressed as a Function

- Binary relation from A to B is simply a subset of A x B
  - If $a \in A$ is related to $b \in B$ then $(a, b) \in R$
- Convert to a function:
  - A x B as input (domain)
  - {TRUE, FALSE} as output (range)
  - $f : A \times B \rightarrow \{TRUE, FALSE\}$
  - $f(a,b) = TRUE$ is equivalent to saying aRb

Binary Relation on A

- Sometimes we are interested in how members of a set are related to other members of the same set
  - Instead of referring to a binary relation from A to A
  - We'll refer to a binary relation *on* A

Equivalence Relations

- If R is a binary relation on A (i.e. R is a subset of A x A), R is an equivalence relation if:
  - R is reflexive
    - for all a in A, $(a,a) \in R$
  - R is symmetric
    - for all a, b in A, if $(a,b) \in R$ then $(b,a) \in R$
  - R is transitive
    - for all a, b, c in A, if $(a,b) \in R$ and $(b,c) \in R$ then $(a,c) \in R$

Example Binary Relations on A

- Are any of these equivalence relations on the set A of integers?
- Which properties **hold** / **break**?
  - aRb if $a < b$ — **Re** / **Sy** / **Tr**
  - aRb if $a \leq b$ — **Re** / **Sy** / **Tr**
  - aRb if $a=b$ — **Re** / **Sy** / **Tr**
  - aRb if $|a - b| < 5$ — **Re** / **Sy** / **Tr**
  - aRb if $|a| = |b|$ — **Re** / **Sy** / **Tr**
  - aRb if $a = |b|$ — **Re** / **Sy** / **Tr**
  - aRb if a and b are relatively prime — **Re** / **Sy** / **Tr**

THANKS FOR YOUR ATTENTION!