CS 4384  INTRODUCTION

Theory of computation comprises:

- Automata theory
- Computability theory
- Complexity theory

Q. What are capabilities/limitations of computers?

Origin of theory of computation:

- A central notion is algorithm (e.g., Euclid's algorithm for computing gcd of integers)

Theory of comp. started long time ago.
A fundamental question is: Is there an algorithm to solve a given problem? For example, consider Hilbert’s 10th problem:

**Input.** A diophantine equation system, e.g.

\[ P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n] \]

**Output.** Yes if \( \exists a_1, \ldots, a_n \in \mathbb{Z} \)

s.t. \( P_1(a_1, \ldots, a_n) = 0, \ldots, P_m(a_1, \ldots, a_n) = 0 \)

- No, otherwise

Q. Is Hilbert’s 10th problem algorithmically solvable? (Hilbert, 1900)
1930s: Turing machines, Rec. fctns → Theory of computability

1970: Matijasevic proved Hilbert's 10th problem is algorithmically unsolvable.

In 1960s:

- Linguistics: N. Chomsky intro. phrase-structured grammar
- Programming: BNF to describe syntax of ALGOL 60
- Biology: Finite automata to describe neural nets.
Automata theory:
  How to model various types of computation?

Computability theory:
  What is computability? Is a given problem computable?

Complexity theory:
  If a problem is solvable, how much resources (time/memory) does it require?
Chapter 1. Math Background

Review of graphs, relations, strings, languages, ind. def., types of proof

Functions & Relations

The Cartesian product of sets \( A, B \) is

\[ A \times B = \{ (a, b) \mid a \in A, b \in B \} \]

A function / mapping takes an input and produces an output. Same inputs produce same outputs

Set of inputs of fct. \( f \) : domain
Set of outputs contained in: range

For fct \( f \) with domain \( D \) and range \( R \) we write

\[ f : D \rightarrow R \]
For subset $A \subseteq D$ we write
\[ f(A) := \{ f(a) \mid a \in A \} \]
$f: D \to R$ is said to be
- one-one if $a \neq a' \Rightarrow f(a) \neq f(a')$
  (distinct inputs produce distinct outputs)
- onto if $f(D) = R$
  $(\forall b \in R: \exists a \in D: f(a) = b)$
- a bijection if $f$ is one-one & onto

**Notation:**

\[ \mathbb{N} = \text{set of natural numbers} \]
\[ = \{ 1, 2, 3, \ldots \} \]
\[ \mathbb{Z} = \text{set of integers} \]
\[ = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \]
\[ \mathbb{Q} = \text{set of rationals} \]
\[ \mathbb{R} = \text{set of reals} \]

For $k \geq 1$
\[ \mathbb{Z}_k = \{ 0, 1, 2, \ldots, k-1 \} \]
  = set of integers modulo $k$
If \( f: A_1 \times \cdots \times A_k \rightarrow \mathbb{R} \), then inputs of \( f \) are \( k \)-tuples \((a_1, \ldots, a_k)\). \( a_1, \ldots, a_k \) are arguments to \( f \).

\[ k = 1 : f \text{ is unary} \quad \text{fct} \]
\[ k = 2 : f \text{ is binary} \quad \text{fct} \]

Ex: \( \text{gcd} : \mathbb{Z}^2 \rightarrow \mathbb{Z} \)
Sort: \( \mathbb{Z}^k \rightarrow \mathbb{Z}^k \)

If range of \( f \) is \( \{0, 1\} \) (\( \{T, F\} \)) \( f \) is called predicate/property

Ex: \( \text{even} : \mathbb{Z} \rightarrow \{0, 1\} \)
is property of integers
\( \text{even}(0) = 1 \), \( \text{even}(-2) = 1 \), \( \text{even}(4) = 1 \)
\( \text{even}(3) = 0 \), \( \text{even}(5) = 0 \)

A property with domain \( A \times \cdots \times A = A^k \) is called a \( k \)-ary relation on \( A \).
It's a subset of \( A^k \).

\( k = 1 : \) unary rel. \( k = 2 : \) bin. rel.
Ex. (1) $\leq$ is bin. rel. on $\mathbb{N}(\mathbb{Z})$

$\leq: \mathbb{N}^2 \rightarrow \{0, 1\}$

$\leq (1, 0) = 0 \quad \leq (1, 3) = 1$

or $1 \not\leq 0 \quad 1 \leq 3$

(2) = is bin. rel. on $\mathbb{N}(\mathbb{Z})$

A k.ary rel. $R$ on a set $A$ can also be described as a subset of $A^k$.

Ex. (1) $\leq = \{ (i, j) \mid i < j \}$

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

$\subseteq \mathbb{N}^2$

(2) $= = \{ (i, i) \} \subseteq \mathbb{N}^2$
Properties of bin. rel.

Let $R$ be a bin. rel. on $A$. If $(a,b) \in R$, we write $a R b$; otherwise $a \not R b$.

$R$ is said to be

- reflexive if $a Ra \ \forall a \in A$
- irreflexive if $a \not R a \ \forall a \in A$
- symmetric if $a R b \implies b R a \ \forall a, b \in A$
- antisymmetric if $a R b \land b R a \implies a = b \ \forall a, b \in A$
- transitive if $a R b \land b R c \implies a R c \ \forall a, b, c \in A$

Ex. (1) $\leq$ on $\mathbb{N}$ is refl., antisym., trans.
(2) $<$ on $\mathbb{N}$ is irrefl., antisym., trans.

$R$ is called an equiv. rel. if $R$ is refl., sym. & trans.

Ex. For $k \geq 1$, def. $\equiv_k$ by $x \equiv_k y$ if $x - y = \lambda k$ for some $\lambda \in \mathbb{Z}$.
$\equiv_k$ is an equiv. rel.
Graphs & Digraphs

A graph is a pair \( G = (V, E) \) where
- \( V \) is set of vertices
- \( E \subseteq V \times V \) is set of edges

Ex.

![Graph diagram]

A labeled graph is a graph whose edges are assigned labels from a finite set.

Ex.

![Labeled graph diagram]

\[ \Sigma = \{a, b\} \]

Other notions concerning graphs:
- degree of a node
- path, simple path, cycle
- connected graph
A graph \( T = (V, E) \) is a tree if \( T \) is connected and cycle-free. Usually \( T \) has a distinguished node called root.

Node with degree 1 which is not a root is called a leaf; otherwise internal node.

(A single node tree has 1 leaf and 0 internal node.)

Ex.

\[ \text{root} \quad \text{leaves} \]

If edges of \( G = (V, E) \) are oriented, \( G \) is a directed graph (digraph).

Other notions concerning digraphs:
- indegree
- outdegree
- directed path, simple path, cycle
- strongly connected digraph
Strings & Languages

An alphabet $\Sigma$ (or $\Gamma$) is a finite set of symbols.

Ex: $\Sigma = \{0, 1\}$ (or $\{a, b\}$): bin. alph.
$\Sigma = \{0, 1, \ldots, 9, A, B, \ldots, Z\}$
$\Sigma = \{0\}$ (or $\{1\}$ or $\{a\}$): unary alph.

A string over $\Sigma$ is a finite sequence of symbols from $\Sigma$.

The length of a string $w$ over $\Sigma$ is the number of occurrences of symbols.

Notation: $|w|$

For $a \in \Sigma$, $|w|_a$ denotes the number of occurrences of $a$ in $w$. ($#_a(w)$)

Other notation for $|w|_a$ is $#_a(w)$.

Ex: $\Sigma = \{0, 1\}$, $w = 011001$
$|w| = 6$, $|w|_0 = 3 = #_1(w)$

The empty string is of length 0 and denoted by $\varepsilon$ or $\lambda$. 
The reverse of a string \( w = w_1 w_2 \ldots w_k \), 
\( w_1, \ldots, w_k \in \Sigma \), is \( w^R = w_k w_{k-1} \ldots w_1 \).

The concatenation of two strings 
\( x = x_1 \ldots x_m \) and \( y = y_1 \ldots y_n \) is 
\( xy = x \cdot y = x_1 \ldots x_m y_1 \ldots y_n \).

Thus: \( |xy| = |x| + |y| \)
\( \#_a(xy) = \#_a(x) + \#_a(y) \)

If \( \{ \begin{align*}
w &= xyz \\
w &= yz \\
w &= xy
\end{align*} \} \), then \( y \) is \{ \text{prefix, substring, suffix} \} of \( w \).

The lexicographic ordering of strings:
- Shorter strings precede longer ones
- Strings of same length are ordered according to dictionary ordering (assuming a total order of \( \Sigma \)).

A language over \( \Sigma \) is simply a set of strings over \( \Sigma \).

If \( w = w^R \), \( w \) is a palindrome.
Recursive Definitions

Ex: (set of well-formed parentheses strings D over $\Sigma = \{ (, ) \} )$

(1) Basis. $\varepsilon$ is in D

(2) Recursive step. If x, y are strings in D, then so are (x) and xy.

(3) Nothing else is in D unless it is obtained from (1) by finitely many applications of (2).

Ex: (set of palindromes over $\Sigma$)

(1) Basis. $\varepsilon$ and a are palindromes $\forall a \in \Sigma$

(2) Recursive step. If w is a palindrome, then so are awa, $\forall a \in \Sigma$

(3) As before ...

Remark. If $a, a \in \Sigma$, is not included in the basis, then odd length palindromes are not included in the definition.
Ex. (Ordered trees)

(1) Basis. Every single node \( n \) is an ordered tree with \( n \) being root.

(2) Recursive step. Let \( T_1, \ldots, T_k \) be ordered trees with roots \( r_1, \ldots, r_k \), and \( r \) be a new node. Then a new ordered tree \( T \) is obtained by
   - adding edges \( (r, r_i) \), \( \ldots \), \( (r, r_k) \)
   - making \( r \) root of \( T \)

(3) Nothing else is a tree unless it's obtained from (1) by finitely many applications of (2).
Inductive Proofs

Ex. Claim. \( \forall w \in D: \#_\zeta(w) = \#_\eta(w) \)

Proof. (1) Basis. \( \#_\zeta(\varepsilon) = 0 = \#_\eta(\varepsilon) \)

(2) Ind. step. Ind. Hypothesis: Assume that \( x, y \in D \) satisfy

\( \#_\zeta(x) = \#_\eta(x) \) and \( \#_\zeta(y) = \#_\eta(y) \).

Consider \( w = (x) \) or \( w = xy \).

Case 1. \( w = (x) \). Then

\[
\#_\zeta(w) = \#_\zeta((x)) \\
= \#_\zeta(x) + 1 \\
= \#_\eta(x) + 1 \text{ (ind. hyp.)} \\
= \#_\eta((x)) \\
= \#_\eta(w)
\]

Case 2. \( w = xy \)

\[
\#_\zeta(w) = \#_\zeta(xy) = \#_\zeta(x) + \#_\zeta(y) \\
= \#_\zeta(x) + \#_\eta(y) \text{ (ind. hyp.)} \\
= \#_\eta(xy) \\
= \#_\eta(w) \quad \square
\]
Ex: **Claim.** For any palindrome \( w : w = w^R \)

Proof. (1) **Basis.** \( w = \varepsilon : \varepsilon = \varepsilon^R \)
\( w = a \in \Sigma : a = a^R \)

(2) **Ind. Step**

**Ind. hyp:** Assume that a given palindrome \( x \) sat. \( x = x^R \)

Consider \( w = axa , a \in \Sigma \)

Clearly, \( w^R = (axa)^R \)
\[ = a^R x^R a = a x^R a = axa \] (ind. hyp)
\[ = w \] \( \square \)

Ex: A bin. tree is strictly binary if every internal node has exactly two children

**Claim.** For all \( n \geq 1 \), every strictly bin. tree with \( n \) leaves has \( n-1 \) internal nodes.

**Proof.**(1) **Basis.** \( n = 1 \). \( T \) is a single-node tree with 1 leaf and 0 internal node
(2) **Ind. step.**

**Ind. hyp:** Assume for some \( n \geq 1 \) that claim holds true for all strictly bin. trees with \( k \) leaves where \( 1 \leq k \leq n \).

Consider a strictly bin. tree \( T \) with \( n+1 \) leaves. Then \( T \) has the form

\[
T = T_1 \cup T_2
\]

That is, \( T \) has 2 strictly bin. sub trees \( T_1, T_2 \) with \( n_1 \) and \( n_2 \) leaves, where \( n_1 + n_2 = n+1 \).

By ind. hyp: 

\[
\begin{align*}
\text{# of intern. nodes in } T_1 &= n_1 - 1 \\
\text{# of intern. nodes in } T_2 &= n_2 - 1
\end{align*}
\]

Hence, \( \text{# of intern. nodes in } T = \text{# of intern. nodes in } T_1 + \text{# of intern. nodes in } T_2 + 1 \) = \( n_1 + n_2 - 1 \) = \( \text{root} \) = \( (n+1) - 1 = n \).
Example: (Correctness of a formula to calculate the amount of monthly payments of mortgages)

\[ P := \text{principal} = \text{loan amount} \]

\[ I := \text{yearly interest rate} \]

\[ Y := \text{monthly payment} \]

**Q.** \( Y = ? \) s.t. mortgage is paid off in 30 years given \( P \) and \( I \)?

For convenience, define monthly multiplier \( M = 1 + \frac{I}{12} \)

Let \( P_t := \text{loan amount after} \ t \text{ months} \)

Then:

\[ P_0 = P \]
\[ P_1 = P_0 \left( 1 + \frac{I}{12} \right) - Y = P_0 M - Y \]
\[ P_2 = P_1 M - Y = (P_0 M - Y) M - Y \]
\[ = P_0 M^2 - Y (1 + M) \]
\[ P_3 = P_0 M^3 - Y (1 + M + M^2) \]
\[ \vdots \]
\[ P_t = P_0 M^t - Y (1 + M + M^2 + \ldots + M^{t-1}) \]

Claim: \( P_t = PM^t - Y \frac{M^t - 1}{M - 1} \)
Claim can also be proved by ind.

\[ \text{Pf. (Claim)} \]

(1) Basis. \( t = 0 \) : \( P_0 = P \)

(2) Ind. step.

Ind. Hyp. Suppose that claim holds true for \( t = k \)

\[ k \rightarrow k+1 : \]

\[ P_{k+1} = P_k \cdot M - Y \]

\[ = \left[ P \cdot M^k - Y \cdot \frac{M^k - 1}{M-1} \right] \cdot M - Y \text{ (ind hyp)} \]

\[ = P \cdot M^{k+1} - Y \cdot \frac{M^k - 1}{M-1} \cdot M - Y \]

\[ = P \cdot M^{k+1} - Y \left( \frac{M^k - 1}{M-1} \cdot M + \frac{M-1}{M-1} \right) \]

\[ = P \cdot M^{k+1} - Y \cdot \frac{M^{k+1} - 1}{M-1} \]

\[ \therefore \]

If \( t = 360 \) \((= 30 \text{ years} \times 12)\), then

\[ P_{360} = 0 \text{ implies} \]

\[ P \cdot M^{360} - Y \left( \frac{M^{360} - 1}{M-1} \right) = 0 \]

or

\[ Y = P \cdot M^{360} \cdot \frac{M-1}{M^{360} - 1} \]

\[ = \frac{1}{12} \cdot P \cdot \frac{M^{360}}{M^{360} - 1} \]

\[ \square \]
Other types of proofs

Proof by Contradiction

Ex: Claim: \( \sqrt{2} \) is irrational

Pf. We'll make use of the following Fact: \( k \) is even \( \iff k^2 \) is even

Now suppose by way of contradiction that \( \sqrt{2} \) were rational. Then

\[
\sqrt{2} = \frac{m}{n}
\]

where \( \gcd(m, n) = 1 \), i.e., \( m, n \) are relatively prime.

Squaring both sides gives:

\[
2n^2 = m^2
\]

Clearly, \( m^2 \) is even. From above fact, it follows that \( m \) is even.

Hence, \( m = 2l \) for some \( l \).

Therefore, \( m^2 = 4l^2 = 2n^2 \)

Thus, \( n^2 = 2l^2 \).

So, \( n^2 \) is even. Again by above fact, \( n \) is even. Since \( m, n \) are both even, they cannot be rel. prime \( \implies \) Contrad. \( \square \)
Proof by construction

Most proofs in CS are constructive. We devise algorithms to construct objects we're looking for. (Mathematicians are interested in proving the existence of such objects.)

Example: A k-regular graph is a graph in which every node has degree k.

Claim. For even $n \geq 4$, there exists a 3-regular graph with $n$ nodes.

Proof. Place the $n$ nodes $0, 1, ..., n-1$ on a circle and connect opposite nodes:

\[
V = \{ 0, 1, 2, ..., n-1 \}
\]
\[
E = \{ (0,1), (1,2), ..., (n-1,0) \} \cup \{ (0, \frac{n}{2}), (1, \frac{n}{2}+1), ..., (\frac{n}{2}-1, n-1) \}
\]
Some Definitions

Let $\Sigma$ be an alphabet. Then $\Sigma^* = \text{set of all strings over } \Sigma$

e.g. $\{a, b\}^* = \{\varepsilon, a, b, aa, ab, ba, bb, \ldots\}$

For $L_i \subseteq \Sigma^*$, $i = 1, 2$, the concatenation of $L_1$ with $L_2$ is $L_1L_2 = L_1 \cdot L_2 = \{uv \mid u \in L_1, v \in L_2\}$

For $x \in \Sigma^*$ and $n \geq 0$:

$x^n = \begin{cases} \varepsilon & \text{if } n = 0 \\ x^{n-1}x & \text{otherwise} \end{cases}$

For $L \subseteq \Sigma^*$ and $n \geq 0$:

$L^n = \begin{cases} \varepsilon \quad \text{if } n = 0 \\ L^{n-1}L & \text{otherwise} \end{cases}$

Ex. $\Sigma = \{a, b\}$

(i) $L_1 = \{a, ab\} \quad L_2 = \{\varepsilon, b\}$

$L_1L_2 = \{a, ab, gb, abb\}$

So, $\text{Card} (L_1L_2) = 3 \neq \text{Card} (L_1) \times \text{Card} (L_2)$
(2) \[ L_1 = \{ a^n | n \geq 0 \} , \; L_2 = \{ b^n | n \geq 0 \} \]
\[ L_1 \cup L_2 = \{ a^m b^n | m, n \geq 0 \} \]
\[ L_1 \cup L_1 = \{ a^n | n \geq 0 \} = L \]

(3) \[ L_1 = \{ a^n | n \geq 1 \} \]
\[ L_1 \cup L_1 = \{ a^n | n \geq 2 \} \neq L \]

**Def.** For \( L \subseteq \Sigma^* \):

The Kleene closure of \( L \) is
\[ L^* = L \cup L^1 \cup L^2 \cup ... \]
\[ = \bigcup_{n=0}^{\infty} L^n \]

The positive closure of \( L \) is
\[ L^+ = L^1 \cup L^2 \cup L^3 \cup ... \]
\[ = \bigcup_{n=1}^{\infty} L^n \]

**Ex. (1)** \[ L_1 = \{ a^n | n \geq 0 \} \]
\[ L_1 \cup L_1 = L, \quad \forall n \geq 1 \]
Hence, \[ L_1^* = L_1 = L^+ \]

(2) \[ L_2 = \{ a^n | n \geq 13 \} \]
\[ L_2^* = \{ a^{12} b^{12} \cup L_2 a^{12} \cup L_2 b^{12} \cup ... = L_2 \} \]
\[ L_2^+ = L_2 \cup L_2^1 \cup L_2^2 \cup ... = L_2^+ \]