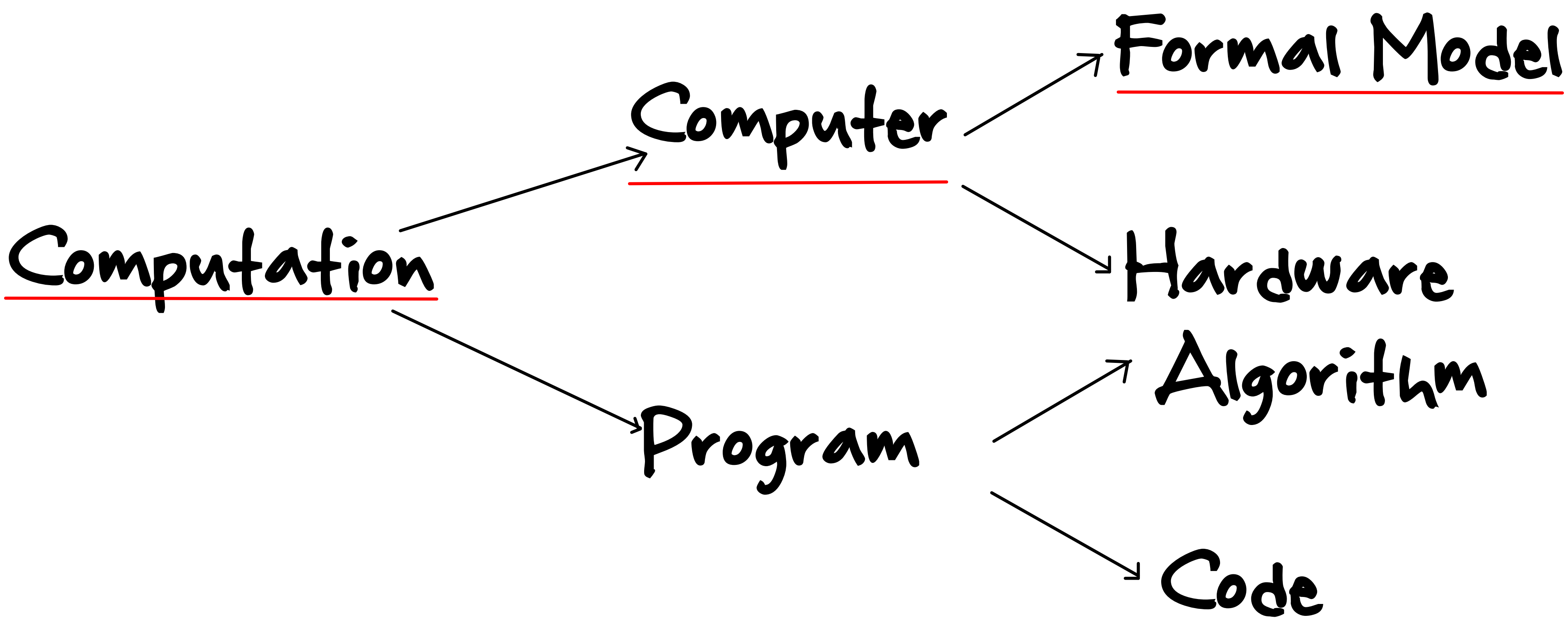
CSE322 Theory of Computing

Do not sign-up if you are against
the idea of proving anything to anyone

Formal Models of Computation



What is computation and computer?

What can be computed?

What "cannot" be computed?

CSE621

✗ What can & cannot be "efficiently" computed?

Outline : 3 models of computer

Wk 1-4: Finite Automaton

(Pattern matching/Regular expressions)

Wk 5-7: Pushdown Automaton

(Syntax checking of C, Python, etc.)

Wk 8-13: Turing Machine

(~~Interpret, understand~~ C Python programs)

as capable as C or Python

$|h_2 - h_1| + |h_3 - h_2| + \cdots + |h_k - h_{k-1}|$ divisible by 10?

$(h_2 - h_1), (h_3 - h_2) \cdots,$

Lec 1

* Formal characterization

* Logically correct proofs

Level 1: Technique → Proof by induction on ...
Proof by pigeonhole principle on ...
Proof by counterexample to ...
Proof by showing example of ...

+ Main idea (for partial marks) 20%

Level 2: Proper complete proof (for full marks)

(learn through homeworks & tutorials)

You must be really good at writing proofs !!!

Sample Proof

sqrt(2) is irrational

Level-1: Proof by assuming that $\sqrt{2} = \frac{a}{b}$ for integers a & b without any common factor (i.e. gcd(a,b) = 1) and reaching a contradiction.

Level-2: a*a = 2b*b. Therefore, a*a is even. If a was odd, then a*a would be odd. Therefore, a must be even. Therefore, a=2d and a*a=4d*d. So, 2d*d=b*b, i.e., 2 | b*b which means that b*b must be even. If b was odd, then b*b would be odd. So b must be even. Then a and b would be both divisible by 2 contradicting gcd(a,b)=1. #

$\overline{A \cup B} = \bar{A} \cap \bar{B}$

L1: Proof by showing that (i) $x \in \overline{A \cup B} \Rightarrow x \in \bar{A} \cap \bar{B}$ [i.e. $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$]

(ii) $x \in \bar{A} \cap \bar{B} \Rightarrow x \in \overline{A \cup B}$ [i.e. $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$]

L2: Explain

Planar graphs are not 3-colorable

L1: Proof by showing example of a planar graph which can only be coloured using 4-colours.

Key Terms

Don't say "... can be done ..."
"... can be shown ..."
"... can be constructed ..."

Alphabet

finite set of symbols

$\Sigma_1 = \{a, b, c, d, \dots\}$

$\Sigma_2 = \{1, 2, 3, (, \}, +, *\}$

Strings/Words

$\Sigma = \{1, \varepsilon\}$ not empty string

sequence of symbols from alphabet

aabb over Σ_1

1++*(over Σ_2

shorthand $aabb \equiv a^2 b^2$

How to denote empty string?

Length of string: $|x|$

Collections of strings: sets, sequences, tuples

can be represented using sets

$(a, b) \neq (b, a)$

$(a, b, c) = ((a, b), c)$

can be represented using sets

$(a, b) = \{\{a\}, \{a, b\}\}$

A : any set of symbols

$A^2 = \{ a_1 . a_2 : a_1 \in A, a_2 \in A \}$

B = set of strings

$B^2 = \{ b_1 b_2 : b_1 \in B, b_2 \in B \}$

Cartesian Product of Sets, Kleene-star and plus

$\Sigma^i = \{ s_1 s_2 \dots s_i \mid s_i \in \Sigma \}$ = all sequences of length i over Σ (alphabet)

($s_1 s_2 \dots s_i$: i-length strings)

$\Sigma^0 = \{ \epsilon \}$

$\Sigma^* = \Sigma^0 \cup \Sigma^1 \cup \Sigma^2 \dots$

Kleene star : all finite length strings

$\Sigma^+ = \Sigma^1 \cup \Sigma^2 \cup \dots$

no Σ^0
all non-empty finite strings

Language

set of finite strings (infinite or finite)

$\{aabb, ab, \epsilon\}$ (ϵ: empty string)

$\{ \}$ (empty language)

$\{ \epsilon \}$

(Discrete) Computational Problems

Function problems: output is many-valued

Decision problems: output is Boolean

Language L = set of strings, from a universe, which
satisfy some property

Language and Decision problems are EQUIVALENT!

Decision problem = question of deciding membership of input in some particular language.

(Discrete) Computational Problems

Decision problems: output is Boolean, decide if input has a specified property.

- Does input x represent adj.mat. of a conn. graph?
- Does input x represent two coprime integers?

Language and Decision problems are EQUIVALENT!

Input: list LI of integers

Q: Does LI have any duplicate?

Represent the above problem as membership of L:

$L = \{ \langle x1 \ldots xk \rangle$: k is integer, x_i are integers &

there exists distinct i and j s.t. $x_i = x_j \}$

String

$A = \{1,2,3\}$ ε, $(1,\varepsilon)$, $(2,\varepsilon)$, $(3,\varepsilon)$, $(1,(1,\varepsilon))$, $(2,(3,\varepsilon))$

11 23

Is $(1,2)$ a string?

2 is not a string

12321

$(1,(2,(3,(2,(1,\varepsilon)))))$

A string w over an alphabet A is

* nothing (called as "empty string", denoted ε) e
* or (a,x) where a is a symbol from A and x is a string
* nothing else

2 $(2,\varepsilon)$

symbol tuple

Length of a string x is denoted $|x|$ and is defined as

$|x| = 0$ if x is the empty string,

$= 1 + |y|$ if $x = (a,y)$

$|(1,(2,(3,(2,(1,\varepsilon)))))| = 5$

String

also xy

concatenation of two strings is denoted $x.y$ and is defined as

$x.y = y$ if $x = e$,

$= (a, z.y)$ if $x = (a, z)$ — $a \in A$, z is a string over A

$(1,(2,\varepsilon)) \cdot (2,(1,\varepsilon))$

12 · 21 · 1221

① $(1, (2,\varepsilon) \cdot (2,(1,\varepsilon)))$

② $= (1,(2, (\varepsilon \cdot (2,(1,\varepsilon)))))$

③ $= (1,(2,(2,(1,\varepsilon))))$

Can you prove that $e.e = e$? ✓

Can you prove that $x.e = e.x = x$?

$x \cdot \varepsilon = x$

Suppose x has length 1. So, $x = (a, e)$.

$$\text{LHS} = (a,e).e = (a, e.e) = (a,e) = x = \text{RHS}$$

Suppose x has length 2. So, $x = (a, y)$ with $|y| = 1$.

$$\text{LHS} = (a,y).e = (a,(y.e)) = (a,y) = x = \text{RHS}$$

(case above)

Suppose x has length 3 ...

Prove that x.e=x

Exercise: $\varepsilon \cdot x = x$

Level-1: Prove by induction on the length of x.

Exercise: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

$\Rightarrow \quad = x \cdot y \cdot z = xyz$

Level-2:

Base case: |x|=0, i.e., x=e.

LHS=e.e=e

RHS=e which equals LHS. Hence the base case is true. ✓

Induction hypothesis: Assume that ~~y~~ z.e=y whenever |~~y~~ z| <= k. (general z)

Induction step: Consider any arbitrary x of length k+1.

Now, x=(a,y) where a is some symbol and y is some string of length k.

LHS=(a,y).e=(a,y.e)= (using IH) (a,y)=x=RHS.

(a,y) = x; .e: by defn.