CS 373

Lecture #2

Sets, logic, induction, proofs, strings, languages, countability, undecidability.

Sets

$\mathbb{N}$ - natural numbers

$\{1, 2, 3, \ldots\}$

$\mathbb{N}_0 = \{0, 1, 2, \ldots\}$

$= \mathbb{N} \cup \{0\}$

$\mathbb{Z} = \{0, -1, 1, 2, -2, \ldots\}$

$\{0\}$

set

not a set

$X \cup 0$

printf(5);

$X \cup Y$ is defined only if
X and Y are sets.

$X \cap Y$

$\overline{X}$

$X \cup \{0\}$ - correct

$X \setminus Y = X - Y = \{x \mid x \in X, x \notin Y\}$
$= X \cap \overline{Y}$

Logic (Boolean)

set

$X \vee true$

incorrect

$\wedge$ - And

$\vee$ - Or

$\Rightarrow$ - implies

$\alpha \Rightarrow \beta$ means that "if α is true, then β is true".

$\equiv \neg\alpha \vee \beta$

"If I am a girl" $\Rightarrow$ "I will win the Nobel prize" is true.

Induction

I want to prove: $\forall n \in \mathbb{N}_0$, $P(n)$.

Establishing:

- $P(0)$
- $P(n) \Rightarrow P(n+1)$. $\forall n$.

Claim. If you establish the above, then $\forall n \in \mathbb{N}_0$, $P(n)$.

Assume: If non-empty $S \subseteq \mathbb{N}_0$, then S has a minimal number (minimum number)

Proof is by contradiction

Assume $P(0)$, $\forall n.\ P(n) \Rightarrow P(n+1)$

Assume $\forall n.\ P(n)$ is false.

Let $S = \{ n \mid P(n) \text{ does not hold} \}$

S is non-empty. So S has a minimum element – say r.

$r \neq 0$ because $P(0)$ holds. So $r > 0$.

$P(r-1)$ holds and $P(r)$ does not hold.

This contradicts $P(r-1) \Rightarrow P(r)$

Contradiction.

Proof by contradiction.

$\sqrt{p}$ for any prime p is <u>not</u> rational

By way of contradiction, assume $\sqrt{p}$ is rational, for some prime p.

$$\sqrt{p} = a/b \quad \text{where } a, b \in \mathbb{N}$$

$$p \cdot b^2 = a^2$$

$$p \cdot (q_1 q_2 q_3 \ldots)^2 = (r_1 r_2 r_3 \ldots)^2$$

Number of times p occurs on the left : odd
" " " " " " " right : even
Contradiction.

Alphabet : Σ — finite set (of "letters")

A string w over Σ is a finite sequence of letters (elements) in the alphabet

$f : [1, n] \to \Sigma$

$\Sigma = \{a, b, c\}$

a, b, b, a, c

$\equiv$ abbac

Languages

A language $L \subseteq \Sigma^*$ set of all strings/words

$L = \{a, ab, aab, aaab, \ldots\}$ is a language over Σ.

$L = \{a\}$ is a language.

Machines <u>decide</u> languages.

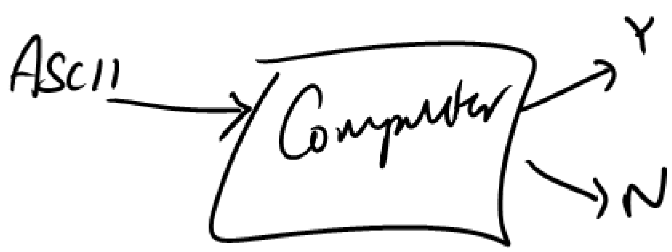
M accepts some strings and rejects/does not accept others.

M defines a language $L(M)$,
$L(M) = \{ x \mid M \text{ accepts } x \}$.

Primes $L \subseteq \{0\}^*$

$$L_{prime} = \{ 0^i \mid i \text{ is a prime} \}$$

$$\underbrace{0.0.0\ldots0}_{i}$$



Central question.

Which languages over Σ are decidable using machines?

TM
computers
automata.

Strings.

Concatenation : $x \circ y$

$abc \circ aab \equiv abcaab$

Epsilon $x \circ \epsilon = x = \epsilon \circ x$

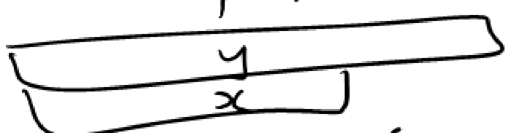
ϵ - empty string

$aab \circ \epsilon = aab$

Length : $|x|$ is the number of letters in the seq.

$|aab| = 3 \qquad |\epsilon| = 0$

Prefix. x is a prefix of y

if 

ab is a prefix of abba

$x, y \in \Sigma^*$ $\quad$ x is a prefix of y

if $\exists z \in \Sigma^* .\ xz = y$

x is a prefix of x: (since z could be ϵ).

ϵ is a prefix of x, for any x.

Suffix. x is a suffix of y
if $\exists z \in \Sigma^* : zx = y$

Substring. x is a substring of y
if $\exists z_1, z_2 \in \Sigma^*$.
$z_1 x z_2 = y$

Lex. ordering on strings. Fix ordering on Σ.
$\Sigma = \{0, 1\}$ $\quad 0 < 1$
$\Sigma^* = \{\epsilon, 0, 1, 00, 01, 10, 11, 000, 001, 010, 011, 100, 101, \ldots\}$

Countable and uncountable sets

$A = \{1, 2, 3\}$ $\quad B = \{x, y, z\}$

$f: A \to B$ $\quad$ 1-1 correspondence.

works for infinite sets

$|A| = |B|$ if there is a 1-1 correspondence $f: A \to B$

$\mathbb{N} = \{1, 2, 3 \ldots\}$

$2\mathbb{N} = \{2, 4, 6, \ldots\}$

$$f : \mathbb{N} \to 2\mathbb{N}$$
$$i \mapsto 2i$$

An infinite set A is <u>countable</u> if $|A| = |\mathbb{N}|$

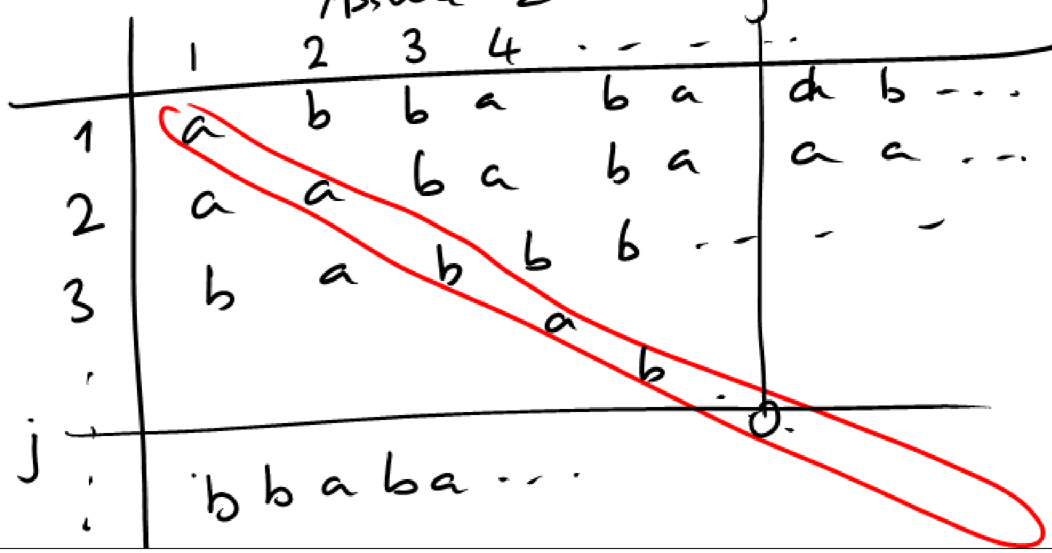
An infinite set is <u>uncountable</u> if it is not countable.

Infinite strings over Σ:

abbaababab....

Σ^∞ = set of all infinite strings.

Assume Σ^∞ was countable



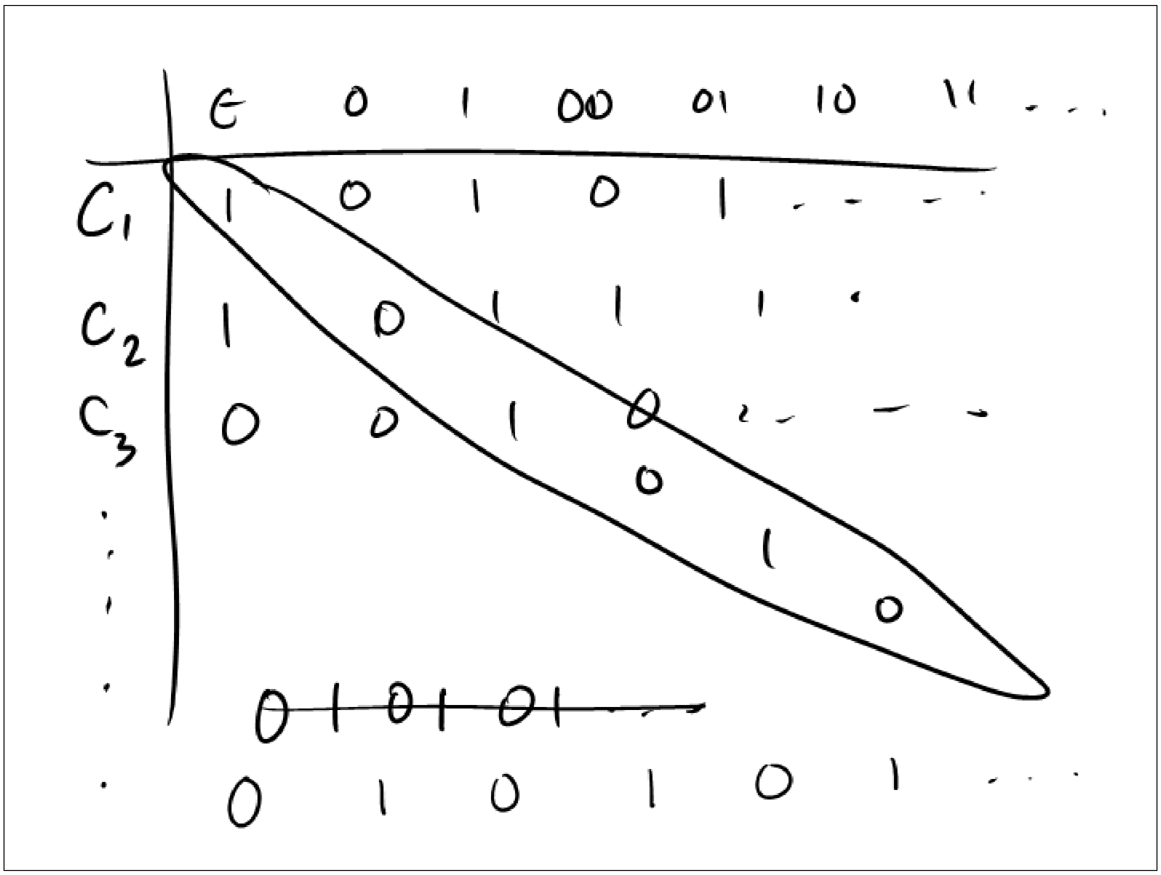
There is some language that no C-program can decide!

C-programs are strings over an alphabet.

Hence the set of all C-pgms is <u>countable</u>.

$\Sigma = \{0, 1\}$.
The set of languages over Σ is uncountable.

A language L $\Leftrightarrow$ infinite string
$\langle a\ b\ b\ a\ b\ a\ a \ldots \rangle$
$\epsilon\ 0\ 00\ 01\ 10\ 11, \ldots$


ε 0 1 00 01 10 11 ...
C1 1 0 1 0 1 ...
C2 1 0 1 1 1
C3 0 0 1 0 ...
0
1
0
0 1 0 1 0 1 ...
0 1 0 1 0 1 ...