HONORS ALGORITHMS

2025-03-03

HOMEWORK PAGE: REFRESH

Σ finite alphabet

Complexity classes:

classes languages $L \subseteq \Sigma^*$

$\mathcal{R}$ = { computable languages }

membership problem decidable by an algorithm

RE = { computably enumerable lang. }

P = { poly.time computable languages }

$NP = \{$"poly. time verifiable languages"$\}$

"solvability of a puzzle"

witness (of YES answer)

$3COL = \{$ 3-colorable graphs $\}$ — 3-coloring

$HAM = \{$ Hamiltonian graphs $\}$ — Ham cycle

$FACT = \{(x,y) \mid x,y \in \mathbb{N}, (\exists d \in \mathbb{N})(2 \le d \le y \wedge d \mid x)\}$ — d

$COMPOSITES = \{$ composites $\}$ — nontriv divisor

x is composite if $x \in \mathbb{N}$, $x \ge 2$, not a prime

Diophantine equation ← looking for integer sol's

polynomial equ w integer coeff's

$$x^3 + y^3 = z^4 + 7$$

Thm $\boxed{\text{not in NP}}$: "a solution" is not necessarily an acceptable witness

x^N $\quad N$ n-digits

2^N has 2^n digits

Suppose all degrees bounded

not an issue: verifying non-existence X

↳ coNP question

not an issue: ∃ multiple solutions

witness must be verifiable
in time poly(n)
n: length of input

∴ witness must be a short string
poly(n) length

Solvability of dioph equ's
of bded degree: undecidable

→ No computable bd on length
of sol's if they exist

Def of "$L \in NP$"

$L \subseteq \Sigma^*$

$L \in NP \iff \exists L_1 \subseteq \Sigma_1^*$

and $C \in \mathbb{N}$ s.t. ← bounding size of witness

$L_1 \in P$ ← the judge

s.t.

$\underbrace{(\forall x \in \Sigma^*)}_{\text{input for membership query in } L}(x \in L \leftrightarrow (\exists w \in \Sigma_1^*) \cdot$

↑ witness

$\cdot (|w| \leq |x|^C \wedge (x, w) \in L_1))$

length of string

an NP-def. of L is L_1

~~$w \in L_1$~~

Karp·reduction $L_1 \propto_{Karp} L_2$

$$f : \Sigma_1^* \longrightarrow \Sigma_2^*$$

s.t.

① f is poly.time computable

WARNING: $f \notin P$
b/c not a decision problem

② $(\forall x \in \Sigma_1^*)(x \in L_1 \Longleftrightarrow f(x) \in L_2)$

L_1 is Karp·reducible to L_2 $\quad L_1 \propto_{Karp} L_2$
if $\exists\ L_1 \to L_2$ Karp reduction

DO If $L_1 \propto_K L_2$ and $L_2 \in P$
then $L_1 \in P$

DO Karp·reducibility is transitive

EX If $L_1 \propto_K L_2$ and $L_2 \in NP$ then $L_1 \in NP$

$$\mathrm{coNP} = \{ \Sigma_L^* \setminus L \mid L \in \mathrm{NP} \}$$

DO $\quad P \subseteq NP$

$\therefore \quad P = coP \subseteq coNP$

$\therefore \quad P \subseteq NP \cap coNP$

<u>Conj</u> $\quad \neq$

candidate: $\quad FACT \in NP \cap \underbrace{coNP}_{\text{nontriv}}$

<u>Conj</u> $\quad FACT \notin P$