Undergraduate Complexity Theory Lecture 8: NP

Marcythm

July 12, 2022

1 Lecture Notes

Conjecture 1.1. $P \neq NP(\iff 3-SAT \notin P)$

Conjecture 1.2 (Exponential Time Hypothesis). $\exists \delta > 0 : 3\text{-SAT} \notin \mathsf{TIME}((1+\delta)^n)$

Conjecture 1.3 (Strong ETH). $\forall \delta > 0 : \exists k : \mathsf{k-SAT} \notin \mathsf{TIME}((2-\delta)^n)$

SETH \Longrightarrow ETH \Longrightarrow P \neq NP.

Theorem 1.4 (ABV '15). SETH implies $\forall \epsilon > 0$, cannot solve LCS in time $O(n^{2-\epsilon})$.

idea of NP: for many problems ∃ brute force algo, enumerate (exp many) "candidate sol"s and check in poly-time if each is a genuine sol. e.g. ST-PATH, HAMILTONIAN-PATH, 3-COL, CIRCUIT-SAT, COMPOSITE.

two features:

- 0. "candidate sol"s are encodable by strings with polynomial length.
- 1. \exists poly-time algo to <u>check</u> if a candidate sol is a genuine sol.

Informally, a problem is in NP if a checking algo exists. "candidate sol" are also called "potential sol", "witness", "certificate", etc. A problem highly believed not in NP: UN-3COL.

Definition 1.5. An algorithm(TM) V is a verifier for language L if

- 1. V takes as input a pair $\langle x, y \rangle$
- 2. $\forall x : x \in L \iff \exists y : V(\langle x, y \rangle)$ accepts.

Definition 1.6. Verifier V is said to be "polynomial time" if $V(\langle x,y\rangle)$ runs in time $O(|x|^k)$ for some $k\in\mathbb{N}$.

Remark 1.7. Subtlety: V's runtime is measured in terms of |x|.

Definition 1.8. $NP = \{L : L \text{ has a poly-time verifier}\}$

e.g. $\mathsf{SQUARES} = \{ \langle B \rangle : B \in \mathbb{N}, \exists x \in \mathbb{N} : x^2 = B \} \in \mathsf{NP}. \ \mathsf{3COL} \in \mathsf{NP}.$

Subtlety in verifier of SQUARE: mark the input as $\langle x, y \rangle$, after interpreting $x = \langle B \rangle$, only read first |x| symbols of y. If |y| > |x|, then reject.

Theorem 1.9. $P \in NP$.

Proof. Let $L \in P$, thus \exists a poly-time TM M s.t. $x \in L \iff M(x)$ accepts. Consider the TM V that runs on input $\langle x, y \rangle$: Do M(x), then ...

- 1. Claim V is poly-time verifier. ...
- 2. Claim V verifies L. ...

About P = NP, upcoming: Cook-Levin Theorem: $P = NP \iff 3SAT \in P$.

2 Reading

$2.1 \quad \text{Sipser 7.3 (The Class NP)}$

definition of verifier, NP (by verifiers), and $\mathsf{NTIME}.$