Undergraduate Complexity Theory
Lecture 27: Hardness within P

Marcythm

July 30, 2022

1 Lecture Notes

P = efficient? $O(n^2)$ = efficient? What really awesome is like $O(n \operatorname{polylog}(n))$.

Remark 1.1. For $O(n^2)$ time vs $O(n \log n)$ the model matters. (in this lecture we use RAM model)

e.g. LCS in time $O(n^2)$ by dynamic programming. can we show it's not in time $O(n^{1.99})$? By THT we can know that $\exists L$ s.t. $L \in \mathsf{TIME}(n^2) \backslash \mathsf{TIME}(n^{1.99})$. Let base it on some assumption, dream: $\mathsf{P} \neq \mathsf{NP}$. But we don't know how to do it, so make a backup dream, then derive many consequences.

Theorem 1.2 (2010's)**.** *Assuming SETH,* $\forall \epsilon > 0 : \mathsf{LCS} \notin \mathsf{TIME}(n^{2-\epsilon})$.

there are tons of such results, $\mathsf{EDIT\text{-}DIST} \geq n^2$, $\mathsf{Graph\text{-}Diameter} \geq mn$, etc.

$\mathsf{3SUM}$: give an array a of n integers, determine if $\exists i, j, k : a_i + a_j + a_k = 0$. It's not too hard to get some algo like $O(n^2 \log n)$. With assumption $\mathsf{3SUM} \geq n^2$, we can derive: 3 points colinear $\geq n^2$, hole in bunch of triangles $\geq n^2$, etc.

APSP: all pairs shortest path, $O(n^3)$. With assumption $\mathsf{APSP} \geq n^3$, we have: Graph radius $\geq n^3$, negtive triangles $\geq n^3$, etc.

$\mathsf{k\text{-}CLIQUE}$: $\geq n^{\omega k/3}$, where ω is the best number exponent of multiplying two $n \times n$ matrices, i.e. $O(n^\omega)$ (till now $\omega = 2.3\cdots$). With assumption $\mathsf{k\text{-}CLIQUE} \geq n^{\omega k/3}$, we have: CFG parsing $\geq n^\omega$, RNA folding $\geq n^\omega$, etc.

fine-grained complexity: finer grain than just sth. is in P or not in P, figure out what is the fastest poly time algorithm. Reduction: for problem A, instance x, size n, a reduction is mapping in time $r(n)$ to problem B, instance y, size $s(n)$, s.t. $x \in A \iff y \in B$. Suppose have time $t(n)$ algo for B, can have time $t(s(n)) + r(n)$ algo for A. Conversely: no $t(s(n)) + r(n)$ time algo for A implies no $t(n)$ time algo for B.

Conjecture 1.3 (Strong ETH)**.** $\forall \epsilon > 0 : \exists k : \mathsf{k\text{-}SAT} \notin \mathsf{TIME}(2^{(1-\epsilon)n})$

Conjecture 1.4 (CNF-SETH)**.** $\forall \epsilon > 0$*, for* $\mathsf{CNF\text{-}SAT}$ *problems with* m *clauses,* n *variables,* $2^{(1-\epsilon)n} \operatorname{poly}(m)$ *time required.*

Definition 1.5. $\mathsf{DIAMETER}$: give graph G with n vertices, m edges, compute $\max_{u,v \in V} \operatorname{dist}(u, v)$.

with Dijkstra's algo, $\mathsf{DIAMETER}$ is about $O(mn)$ time. Open Question: faster than $O(mn)$ time?

Remark 1.6. Try approximation when stuck on an algorithmic problem.

ACIM'96: $\tilde{O}(m\sqrt{n})$ time for "factor 2/3 approximation", i.e. find D s.t. $2/3 \operatorname{diam}(G) \leq D \leq \operatorname{diam}(G)$.

Theorem 1.7. $\mathsf{CNF\text{-}SETH} \implies \nexists O(MN^{1-\epsilon})$ *time* $\mathsf{DIAMETER}$ *algo.*

Proof. Reduction from a $\mathsf{CNF\text{-}SAT}$ instance $\phi(x_1, x_2, \ldots, x_n)$ with m clauses to a $\mathsf{DIAMETER}$ instance G with $N = 2^{n/2} + m + 2$ vertices and $M = 2^{n/2} O(m)$ edges. This reduction runs in time $2^{n/2} \operatorname{poly}(m)$, very slow, but it's nothing comparing to the to-be-constructed $2^{(1-\epsilon)n} \operatorname{poly}(m)$ algo for $\mathsf{CNF\text{-}SAT}$. By this reduction, $\operatorname{diam}(G) = 2 + [\phi \in \mathsf{CNF\text{-}SAT}]$. If exists $O(MN^{1-\epsilon})$ time algo for exactly (cool fact: even for

2/3 approximation) DIAMETER, then exists time $2^{(1-\epsilon/2)n}$ poly(m) algo for CNF-SAT, contradicts with the CNF-SETH.

details: one vertex C_i for each clause, let C_i be a clique; two hang-out vertices s, t, connected to C_i. (main trick) Setup $2^{n/2}$ vertices X_α, one for each partial assignment α to the first $n/2$ variables. Similar $2^{n/2}$ vertices Y_β for the other half. Promise for every X_α there is at least one edge connects to it, and the same for Y_β.

Thus $\text{diam}(G) \le 3$, and $\text{diam}(G) = 2$ iff $\forall \alpha, \beta : \exists i : \{(X_\alpha, C_i), (C_i, Y_\beta)\} \subseteq E$.

Connect X_α to C_i iff C_i is <u>not</u> (already) sat'd by α. e.g. for $n = 4$, C_i for $x_1 \vee x_2 \vee x_3$ will be connected to X_{00} but not X_{10}. Consider previous promise, if some X_α is isolated, then we can know $\phi \in$ CNF-SAT, thus abandon any construction and output any graph with diameter 3. $\square$