Computational Complexity

Lecture 14

March 20, 2020

Universiteit van Amsterdam

Plan for today

1. Recap most of the topics that we discussed in the course
2. Talk about any questions that you still have

P, NP, NP-completeness

Definition (The classes P and NP)

$$\mathsf{P} = \bigcup_{c \geq 1} \mathsf{DTIME}(n^c) \qquad \mathsf{NP} = \bigcup_{c \geq 1} \mathsf{NTIME}(n^c)$$

Definition

A *polynomial-time reduction* from $L_1 \subseteq \{0,1\}^*$ to $L_2 \subseteq \{0,1\}^*$ is a polynomial-time computable function $f : \{0,1\}^* \to \{0,1\}^*$ such that for each $x \in \{0,1\}^*$ it holds that $x \in L_1$ if and only if $f(x) \in L_2$.

Definition

A problem $L \subseteq \{0,1\}^*$ is *NP-complete* if $L \in \mathsf{NP}$ and every problem $L' \in \mathsf{NP}$ can be polynomial-time reduced to L.

Theorem (Cook-Levin)

3SAT is NP-complete.

Time Hierarchy Theorems & Relativization

Theorem (Deterministic Time Hierarchy)

If f, g are time-constructible functions such that $f(n) \log f(n)$ is $o(g(n))$, then:

$$DTIME(f(n)) \subsetneq DTIME(g(n))$$

Theorem (Nondeterministic Time Hierarchy)

If f, g are time-constructible functions such that $f(n+1)$ is $o(g(n))$, then:

$$NTIME(f(n)) \subsetneq NTIME(g(n))$$

- So P $\subsetneq$ EXP and NP $\subsetneq$ NEXP.

Theorem (Baker-Gill-Solovay)

There exist oracles $A, B \subseteq \{0,1\}^*$ such that $P^A = NP^A$ and $P^B \neq NP^B$.

Space complexity

Definition (The classes L, NL, PSPACE, NPSPACE)

$$\mathrm{L} = \mathrm{SPACE}(\log n) \qquad \mathrm{NL} = \mathrm{NSPACE}(\log n)$$
$$\mathrm{PSPACE} = \bigcup_{c\geq 1} \mathrm{SPACE}(n^c) \qquad \mathrm{NPSPACE} = \bigcup_{c\geq 1} \mathrm{NSPACE}(n^c)$$

- NL-completeness: based on *logspace reductions*.

Theorem (Space Hierarchy)

If f, g are space-constructible functions such that $f(n)$ is $o(g(n))$, then:

$$\mathit{SPACE}(f(n)) \subsetneq \mathit{SPACE}(g(n))$$

- So $\mathrm{L} \subsetneq \mathrm{PSPACE}$.

Theorem (Savitch)

$\mathit{PSPACE} = \mathit{NPSPACE}$.

Polynomial Hierarchy (PH)

Definition (The classes Σ_i^{p})

$L \subseteq \{0,1\}^*$ is in Σ_2^{p} if there exists a polynomial-time TM $\mathbb{M}$ and a polynomial q such that for all $x \in \{0,1\}^*$:

$$\begin{array}{lll} x \in L & \text{iff} & \text{there exists } u_1 \in \{0,1\}^{q(|x|)} \text{ such that} \\ & & \text{for all } u_2 \in \{0,1\}^{q(|x|)} \text{ it holds that } \mathbb{M}(x, u_1, u_2) = 1. \end{array}$$

(Similarly for all $i \geq 1$.)

Definition (The class PH)

$$\mathsf{PH} = \bigcup_{i \geq 1} \Sigma_i^{\mathsf{p}}$$

Circuits and advice

Definition (The class P/poly)

$$\mathsf{P/poly} = \bigcup_{c \geq 1} \mathsf{SIZE}(n^c)$$

P/poly consists of all $L \subseteq \{0,1\}^*$ that can be decided in polynomial time with polynomial-size advice $\{\alpha_n\}_{n \in \mathbb{N}}$.

Theorem (Karp-Lipton)

If $NP \subseteq P/poly$, then $PH = \Sigma_2^p$.

Probabilistic computation

Definition (The classes BPP, RP, ZPP)

$$\begin{aligned} \mathsf{BPP} &= \textstyle\bigcup_{c\geq 1} \mathsf{BPTIME}(n^c) \\ \mathsf{RP} &= \textstyle\bigcup_{c\geq 1} \mathsf{RTIME}(n^c) \\ \mathsf{ZPP} &= \textstyle\bigcup_{c\geq 1} \mathsf{ZPTIME}(n^c) \end{aligned}$$

- BPP: two-sided bounded error, polynomial time
- RP: one-sided bounded error, polynomial time
- ZPP: zero-sided error, expected running time polynomial

Approximation algorithms & PCP Theorem

Definition (ρ-Approximation algorithms)

Let $\rho < 1$. A ρ-approximation algorithm A for an optimization problem returns for every input $x \in \{0,1\}^*$ a solution with *quality* at least $\rho \cdot \mathrm{val}(x)$, where $\mathrm{val}(x)$ denotes the quality of an optimal solution for x.

Theorem (PCP)

There exists $\rho < 1$ such that for every $L \in NP$, there is a polynomial-time function f mapping strings to 3CNF formulas such that:

$$\begin{aligned} &\text{if } x \in L, && \text{then } val(f(x)) = 1 \\ &\text{if } x \notin L, && \text{then } val(f(x)) < \rho \end{aligned}$$

- If for every $\rho < 1$ there is a polynomial-time ρ-approximation algorithm for MAX3SAT, then $\mathrm{P} = \mathrm{NP}$.

Subexponential-time & ETH

We can solve 3SAT in time $2^{O(n)}$, where n is the number of propositional variables in the input.

Definition (δ_q)

For $q \geq 3$, let δ_q be the infimum of the set of constants c for which there exists an algorithm solving qSAT in time $O(2^{cn}) \cdot m^{O(1)}$, where n is the number of variables in the qSAT input and m the number of clauses.

Definition (ETH)

Exponential-Time Hypothesis (conjecture): $\delta_3 > 0$.

- The ETH implies that there is no $2^{o(n)}$-time algorithm algorithm that solves 3SAT, and therefore also that $\mathrm{P} \neq \mathrm{NP}$.

Average-case complexity

Definition (Distributional problems)

A *distributional problem* $\langle L, \mathcal{D} \rangle$ consists of a language $L \subseteq \{0,1\}^*$ and a sequence $\mathcal{D} = \{\mathcal{D}_n\}_{n \in \mathbb{N}}$ of probability distributions, where each $\mathcal{D}_n$ is a probability distribution over $\{0,1\}^n$.

Definition (The class distP)

$\langle L, \mathcal{D} \rangle$ is in the class distP if there exists a TM $\mathbb{M}$ that decides L and a constant $\epsilon > 0$ such that for all $n \in \mathbb{N}$:

$$\mathop{\mathbb{E}}_{x \in_{\mathsf{R}} \mathcal{D}_n} [\ \mathrm{time}_{\mathbb{M}}(x)^{\epsilon}\ ] \text{ is } O(n).$$

Definition (The classes distNP and sampNP)

distNP: all $\langle L, \mathcal{D} \rangle$ for which $L \in \mathrm{NP}$ and $\mathcal{D}$ is P-computable.
sampNP: all $\langle L, \mathcal{D} \rangle$ for which $L \in \mathrm{NP}$ and $\mathcal{D}$ is P-samplable.

Any further questions?