HW 5 - Solutions - page 1

Thursday, May 17, 2018 2:09 PM

1) Let $L = \{x \mid b_n(f_n^{-1}(x)) = 1 \text{ where } n = |x|\}$

Note that since f_n is a permutation, f_n^{-1} is well-defined and unique.

$L \in NP \quad L = \{x \mid \exists y \; f(y) = x \text{ and } b(y) = 1\}$

poly-time computable

$co\text{-}L \in NP \quad co\text{-}L = \{x \mid \exists y \; f(y) = x \text{ and } b(y) = 0\}$

$\Rightarrow L \in co\text{-}NP.$

Suppose $L \in BPP$ Since $BPP \subseteq P/poly$, there is a polynomial-sized family of circuits $\{C_n\}$ that can compute L. Since b is a hard-bit for f, this implies that there is a poly-sized circuit family C_n' that can compute f_n^{-1} which contradicts the assertion that f is one-way.

2. $L = \{\phi(x_1, \ldots, x_n) \mid \exists y \in \{0,1\}^m \; \forall x \in \{0,1\}^n$

$m \leq n^k \cdot B$

y is an encoding of a CNF Boolean formula ϕ' with $\leq B$ clauses, and $\phi(x) = \phi'(x)$

poly-time checkable.

Thursday, May 17, 2018 2:09 PM

3. Will show that if $\Sigma_i \subseteq \bigcup_{k \geq 1} TIME(n^{\log^k n})$

and $NP \subseteq TIME(n^{\log n})$ then $\Sigma_{i+1} \subseteq \bigcup_{k \geq 1} (n^{\log^k n})$

Let $L \in \Sigma_{i+1}$, then $L \in NP^{\Sigma_i}$

L is decided by a poly-time NTM M w/ oracle A s.t. $A \in \Sigma_i$. By assumption, $A \in TIME(n^{\log^k n})$ for some k.

Define $L_{PAD} = \{ x\$^t \mid \text{where } x \in L \text{ and } t = |x|^{\log^k |x|} \}$

Consider new NTM M' that computes L_{PAD}.

On input $x\$^t$:
- Verify that the number of \$ symbols is $|x|^{\log^k |x|}$. If not, reject. Then erase \$ symbols.
- Simulate M on x. When oracle A is consulted, compute answer in time $n^{\log^k n}$.

On input $x\$^t$ where $|x| = n$
M' runs in time $poly(n) \cdot n^{\log^k n}$.
Since $|x\$^t| = n \cdot n^{\log^k n}$ M' is a poly-time NTM.

Thursday, May 17, 2018 2:09 PM

Since $NP \subseteq TIME(n^{\log n})$ $\exists$ DTM M on input $x\$^t$ runs in time $t^{\log t}$

$$= \text{time } \left(n^{\log^k n}\right)^{\log\left(n^{\log^k n}\right)}$$

$$= \text{time } \left(n^{\log^k n}\right)^{\log^{k+1} n} = n^{\log^{2k+1} n}$$

Construct a new DTM M' which also runs in time $n^{\log^{2k+1} n}$ and decides L:

On input x: add $n^{\log^k n}$ \$ symbols to x. Simulate M.

$\Rightarrow L \in TIME(n^{\log^{2k+1} n})$

4. Let $L \in NP^{QSAT}$.

There is an NTM M w/ a QSAT oracle that runs in polynomial time.

Guess: y: non-deterministic choices for M.
$z_1 \ldots z_k$: queries to QSAT oracle
$u_1 \ldots u_k$: answers to QSAT oracle

Thursday, May 17, 2018 2:44 PM

$x \in L \iff \exists y\, z_1 \cdots z_k\, u_1 \cdots u_k$

poly-time checkable by TM M'.

M w/ non-det choices y asks queries $z_1 \cdots z_k$ if it gets answers $u_1 \cdots u_k$ accepts

AND $(u_j = 1) \Rightarrow z_j \in QSAT$

AND $(u_j = 0) \Rightarrow z_j \notin QSAT$

$$z_j = \exists y_{j1} \forall y_{j2} \cdots \forall y_{jn}\, \phi_j(y_{j1}, \ldots, y_{jn})$$

$x \in L \iff \exists y_1\, z_1 \cdots z_k\, u_1 \cdots u_k$ $M'(x, y, z_1 \ldots, z_k, u_1 \ldots, u_k)$

AND $(u_j = 1) \Rightarrow \exists y_{j1} \cdots \forall y_{jn}\, \phi_j(y_{j1}, \ldots, y_{jn})$

AND $(u_j = 0) \Rightarrow \forall y_{j1} \cdots \exists y_{jn}\, \neg \phi_j(y_{j1}, \ldots, y_{jn})$.

Can convert to form:

$$\exists x_1 \forall x_2 \cdots \forall x_n \Big(M'(x_1) \text{ accepts} \wedge \phi_j(x_1 \cdots x_n) \cdots \wedge \neg \phi_k(x_1, \ldots, x_n) \cdots \Big)$$

for $u_j = 1$; $\neg$ for $u_k = 0$

poly-sized circuit. $C(x_1, \ldots, x_n)$

Convert to 3CNF using auxiliary vars $z_1 \cdots z_m$ as done in class.

$$\exists x_1 \forall x_2 \cdots \forall x_n \exists z\ \phi'(x_1, \ldots, x_n, \vec{z})$$