0368-3168: Complexity **Fall 2023**

Assignment 2

Lecturer: Amnon Ta-Shma and Ron Zadicario *Submission Deadline: 1/12/22*

Remark. Exercises marked with (Know) are not for submission, but make sure you know how to solve them.

Problem 1 (Quantifying non-uniformity).

Definition 1 (Turing machine with advice)**.** Let $T, a : \mathbb{N} \to \mathbb{N}$ be integer functions. A language L is in the class $\mathrm{DTIME}(T(n))/a(n)$ if there exists a sequence of "advice" strings $\{\alpha_n\}_{n\in\mathbb{N}}$ such that $|\alpha_n| \leq a(n)$, and a TM M that on input x runs for at most $O(T(|x|))$ steps, such that:

$$x \in L \iff M(x, \alpha_{|x|}) = 1.$$

Note that M uses the same advice α_n on *all inputs of the same length, n.*

We further define:

Definition 2 (Polynomial time with advice)**.**

$$\mathrm{P}/a(n) := \bigcup_{k\in\mathbb{N}} \mathrm{DTIME}\Big(n^k\Big)/a(n)$$

1. Show there exists an undecidable language in $\mathrm{P}/1$.
2. Define $\mathrm{P/poly} = \bigcup_{\ell\in\mathbb{N}} \mathrm{P}/n^\ell$. Show that $\mathrm{P/poly} = \mathrm{Size(poly)}$.
3. Show that if for some constant k we have $\mathrm{SAT} \in \mathrm{P}/\lfloor k \cdot \log(n)\rfloor$, then $\mathrm{SAT} \in \mathrm{P}$.

Problem 2 (Linear Programming is P-Complete). Consider the language

$$\mathrm{LIN-PROG} = \{(A, b) \mid \exists x \in \mathbb{R}^n \quad Ax \leq b\}$$

where $A \in \mathbb{R}^{m\times n}$, $b \in \mathbb{R}^m$ and $Ax \leq b$ means point-wise inequality: $\forall i.(Ax)_i \leq b_i$.

Prove that $\mathrm{LIN-PROG}$ is P-Hard with respect to log-space reductions. Remark: It is known that $\mathrm{LIN-PROG} \in \mathrm{P}$ hence it is P-Complete.

Problem 3 (0/1 Integer Programming is NP-Complete). Consider the language

$$\mathrm{INT-PROG} = \{(A, b) \mid \exists x \in \{0, 1\}^n \quad Ax \leq b\}$$

where $A \in \mathbb{Z}^{m\times n}$, $b \in \mathbb{Z}^m$, and $Ax \leq b$ means point-wise inequality: $\forall i.(Ax)_i \leq b_i$.

Prove that $\mathrm{INT-PROG}$ is NP-Complete with respect to log-space reductions.

Problem 4 (QUAD is NP-Complete). A *quadratic equation* over n variables $x_1, \ldots, x_n$ is an equation of the form

$$\sum_{i,j \in [n]} a_{ij} x_i \cdot x_j = b$$

Where $a_{ij}, b \in \{0,1\}$, and the summation is mod 2. We say a quadratic equation is 0/1-*satisfiable* if there exists a Boolean assignment to the variables which satisfies it. We say a finite set of quadratic equations is 0/1-satisfiable if there exists a Boolean assignment which simultaneously satisfies all of the equations. Let QUAD be the language of all 0/1-satisfiable finite sets of quadratic equations. Prove that QUAD is NP-Complete.

Problem 5. (Know) We proved in class that STCON is NL-Complete with respect to Log-space reductions. We also proved that STCON $\in \mathrm{AC}^1$. Explain why this implies that $\mathrm{NL} \subseteq \mathrm{AC}^1$ (No need to write a complete proof).

Problem 6 (SUC − BoolMatPower is PSPACE-Complete). We say a circuit C represents an $n \times n$ Boolean matrix A, if $C(i,j) = A_{ij}$. Let $\langle C \rangle$ denote the encoding of a circuit C, and let $[C]$ denote the matrix C represents. Let SUC − BoolMatPower be the language of all tuples $(\langle C \rangle, n, t, i, j)$ such that C represents an $n \times n$ Boolean matrix and $([C]^t)_{ij} = 1$, where the product used is Boolean matrix product. Prove that SUC − BoolMatPower is PSPACE-Complete.

Problem 7.

Definition 3. A formula $F(x_1, \ldots, x_n)$ is a circuit such that every gate has out-degree (fan-out) 1 except the output gate with out-degree (fan-out) 0. Remark: We allow multiple variable nodes.

Prove that the language

$$\mathrm{FVAL} = \{(F, x) \mid F(x) = 1 \text{ and } F \text{ is a formula}\}$$

is in $\mathrm{L} = \mathrm{DSPACE}(O(\log n))$. For a bonus, prove that $U_L - NC^1 \subseteq \mathrm{L}$ (where U_L denotes logspace-uniform).