Complexity Theory

Final Exam

(3h duration)

December 18, 2012

Each exercise is worth 2 points, except for (3b) which is worth 1 point[1]. Required definitions and hints for the exercises follow below. Feel free to use the book, or your own notes.

Exercise 1. Prove that the "exact one-two" function $E_{12}^{(n)}$ has degree exactly 2^n over the field $\mathbb{R}$, i.e., that $\deg_{\mathbb{R}}(E_{12}^{(n)}) = 2^n$.

Exercise 2. Prove that $A \in \mathrm{P}/poly$ if and only if $A \in \mathrm{P}^{\mathrm{SPARSE}}$.

Exercise 3. (a) Prove that $\mathrm{BPP}^{\mathrm{BPP}} = \mathrm{BPP}$.
(b) (bonus) Prove that $\mathrm{NP}^{\mathrm{BPP}} \subseteq \mathrm{BPP}^{\mathrm{NP}}$.

Exercise 4. Prove that $\mathrm{P}/n^2 \subseteq \mathrm{P}/n^3$; then prove that this inclusion is strict.

Exercise 5. Show that if $\mathrm{EXP} \subseteq \mathrm{PSPACE}/poly$, then $\mathrm{EXP} = \mathrm{PSPACE}$

[1] Exercise (3b) is worth *1 bonus point*, meaning that the exam is being graded to $5 \times 2 + 1 = 11$ points. We recommend you do not worry about exercice 3b, and leave it for doing at the end of the exam if you can spare the time.

Definitions

Definition 1 (Exact one-two function)**.** The "exact one-two" function $E_{12}^{(n)}$ is the boolean function defined inductively by:

(i) $E_{12}^{(1)}(x_1, x_2, x_3) = 1$ if exactly 1 or exactly 2 of the inputs x_1, x_2, x_3 are equal to 1, and $E_{12}^{(1)}(x_1, x_2, x_3) = 0$ otherwise, i.e.,

$$E_{12}^{(1)}(x_1, x_2, x_3) = 1 \iff |\{x_i | x_i = 1, i = 1, 2, 3\}| \in \{1, 2\}.$$

(ii) $E_{12}^{(n+1)} = E_{12}^{(1)}(E_{12}^{(n)}, E_{12}^{(n)}, E_{12}^{(n)})$, i.e.

$$E_{12}^{(n+1)}(x_1, \ldots, x_{3^{n+1}}) =$$
$$E_{12}^{(1)}(E_{12}^{(n)}(x_1, \ldots, x_{3^n}), E_{12}^{(n)}(x_{3^n+1}, \ldots, x_{2\times 3^n}), E_{12}^{(n)}(x_{2\times 3^n+1}, \ldots, x_{3^{n+1}}))$$

Definition 2 ($\deg_{\mathbb{F}}(f)$)**.** Let $\mathbb{F}$ be some field. A function $f : \{0,1\}^n \to \{0,1\}$, is *represented* by a multivariate polynomial $p \in \mathbb{F}[x_1, \ldots, x_n]$ if

$$p(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$$

for every $x_1 \ldots x_n \in \{0,1\}^n$ (in the left $0, 1$ are the additive and multiplicative identities of the field $\mathbb{F}$).

The *degree* of f over $\mathbb{F}$, $\deg_{\mathbb{F}}(f)$, is the smallest degree of any polynomial representing f.

Definition 3 (Sparse set)**.** A set $S \subseteq \{0,1\}^*$ is called *sparse* if it has polynomial density, i.e., if there exists a constant c such that

$$|S \cap \{0,1\}^n| \leq n^c + c.$$

We use SPARSE to denote the class of all sparse sets.

Hints for the various exercises

Exercise 1. Begin by proving that $\deg_{\mathbb{R}}(E_{12}^{(n)}) \leq 2^n$, and then argue that equality holds based on what you learned of multivariate polynomials.

Exercise 2. Use a sparse set S to encode the advice, and vice versa. Remember to prove the implication clearly in both directions.

Exercise 3. Use a union bound to control the error. For (3b), the union bound must go over all certificates.

Exercise 4. The proof (that we thought of) is through a mix of counting and diagonalization. Note that given an advice string $\alpha_1 \ldots \alpha_{n^c}$, it naturally induces a set A of strings of length n, such that the i-th string of length n (in the lexicographical order) is in A iff $\alpha_i = 1$.

Exercise 5. Note that to any given oblivious exponential-time machine M deciding a set $A \in$ EXP there corresponds a set $B \in$ EXP which encodes the *tableau* of the computation of M; for instance, we may define B by having $\langle x, t, q, \sigma \rangle \in B$ if and only if the symbol under the tape head is σ, and M is in state q, at the t-th step of the computation of M on input x.