cs579 Computational Complexity

Problem Set #5

Prof. Michael A. Forbes | Due: *Thu., 2023-11-16 12:00*

All problems are of equal value.

Note: there are hints on the last page, for those who want them.

1. (Sipser #10.17) Prove that, if A is a language in L, a family of branching programs $(B_1, B_2, \ldots)$ exists wherein each B_n accepts exactly the strings in A of length n and is bounded in size by a polynomial in n.

2. Suppose we modify our model of randomized computation to allow for more general models of random decisions. That is, consider a Turing Machine augmented with an additional *randomness* tape such that if the number m is written (in binary) on the tape when the TM enters the "random step" state, then the contents of the randomness tape are replaced with a uniform random element of $\{0, \ldots, m-1\}$. Show that this does not change the classes BPP and RP.

3. Let $\mathbb{F}$ be a field (such as the real or complex numbers, or a finite field), and let $\mathbb{F}[x_1, \ldots, x_n]$ be the set of n-variate polynomials with coefficients from $\mathbb{F}$. For integers $a_1, \ldots, a_n \geq 0$, a *monomial* is the product $\overline{x}^{\overline{a}} = x_1^{a_1} \cdots x_n^{a_n}$. The monomial is *multilinear* if $0 \leq a_i \leq 1$ for all i. A polynomial p is multilinear if it is a sum of multilinear monomials (with coefficients from $\mathbb{F}$), that is, $p = \sum_{\overline{0} \leq \overline{a} \leq \overline{1}} \alpha_{\overline{a}} \overline{x}^{\overline{a}}$, with $\alpha_{\overline{a}} \in \mathbb{F}$.

   (a) For $\overline{b} \in \{0,1\}^n$, show that $p_{\overline{b}} = \prod_i \frac{x_i - (1-b_i)}{b_i - (1-b_i)}$ is a multilinear polynomial, and that for $\overline{c} \in \{0,1\}^n$,
   $$p_{\overline{b}}(c) = \begin{cases} 1 & \overline{c} = \overline{b} \\ 0 & \overline{c} \neq \overline{b} \end{cases} .$$

   (b) Using (3a), show that for any boolean function $f : \{0,1\}^n \to \{0,1\}$, there *exists* a multilinear polynomial p such that $p(\overline{c}) = f(\overline{c})$ for all $\overline{c} \in \{0,1\}^n$.

   (c) Let $S \subseteq \mathbb{F}$ be a subset of the field. Show that for any *non-zero* multilinear polynomial $p \neq 0$ that choosing a uniformly random point $\overline{\alpha} \in S^n$ will yield a non-root of p with non-zero probability. Specifically, show that
   $$\Pr_{\overline{\alpha} \leftarrow S^n}[p(\overline{\alpha}) \neq 0] \geq \left(1 - \frac{1}{|S|}\right)^n .$$

   (d) Using (3c), show that for any boolean function $f : \{0,1\}^n \to \{0,1\}$, there is *at most one* multilinear polynomial p such that $p(\overline{c}) = f(\overline{c})$ for all $\overline{c} \in \{0,1\}^n$.

4. Let $\mathbb{F}_2 = \{0,1\}$ be the field of two elements. A matrix $A \in \mathbb{F}_2^{k \times n}$ is *Toeplitz* if it is constant on diagonals, that is, $A_{i+1,j+1} = A_{i,j}$ for all $0 \leq i < k$ and $0 \leq j < n$. Let $\mathrm{Toep}(\mathbb{F}_2^{k \times n})$ be the set of all such Toeplitz matrices. Define the hash function $h : \mathbb{F}_2^n \times (\mathrm{Toep}(\mathbb{F}_2^{k \times n}) \times \mathbb{F}^k) \to \mathbb{F}_2^k$ by $h(x, (A, b)) = Ax + b$. Show that h is a pairwise independent hash family. That is, when A and b are chosen uniformly at random, for any $x \neq y \in \mathbb{F}_2^n$ and $c, d \in \mathbb{F}_2^k$,
$$\Pr_{\mathsf{A} \in \mathrm{Toep}(\mathbb{F}_2^{k \times n}), \mathsf{b} \in \mathbb{F}_2^k}[h(x, (\mathsf{A}, \mathsf{b})) = c \wedge h(y, (\mathsf{A}, \mathsf{b})) = d] = \frac{1}{2^{2k}} .$$

Some hints.

2. There are two directions to this question. For the more involved direction, first consider simulating a single step of the randomness tape. What happens when the simulation fails? What happens to the simulation error when the randomness tape is called many times? How can we reduce the error of a randomized algorithm?

3c. Review Sipser's Lemma 10.15.