cs598maf Alg. and Geom. Complexity Theory Out: *Mon., 2023-01-23*
Revised: *2023-02-07 21:20*

Problem Set #1 (v2)

Prof. Michael A. Forbes Due: *Wed., 2023-02-08 17:00*

All problems are of equal value.

1. Let $G = (V, E)$ be an undirected bipartite graph with bipartition $V = L \sqcup R$ and $|L| = |R|$. Suppose there is a subset of preferred edges $F \subseteq E$, and a number $k \geq 0$. The *exact bipartite perfect matching problem* is to decide whether G has a perfect matching using *exactly* k edges from F. Show that the exact bipartite perfect matching problem can be efficiently solved, by using polynomial identity testing as a subroutine.

   Note: As a corollary, this problem yields an efficient randomized algorithm for exact bipartite perfect matching. In contrast, there is no efficient deterministic algorithm known.

2. An algebraic circuit over $\mathbb{R}$ is *monotone* if all field constants are non-negative. Monotone circuits can only compute polynomials over $\mathbb{R}$ with non-negative coefficients, and it is not hard to see that all such polynomials can be computed (perhaps inefficiently) by monotone circuits. It is thus natural to ask whether restricting circuits to be monotone changes the computational power. It turns out that negation can be exponentially powerful.

   However, one can show that a limited amount of non-monotonicity is without loss of generality. Show that if $f \in \mathbb{R}[\overline{x}]$ (possibly with negative coefficients) is computed by an algebraic circuit over $\mathbb{R}$ using $+$ and $\times$ gates, then f is computed by an $O(s)$ size algebraic circuit where all constants are *non-negative*, using $+$ and $\times$ gates, along with *single* subtraction gate.

3. Let p be a prime, so that $\mathbb{F}_p$ is a finite field, and $\mathbb{F}_{p^k}$ is a finite field containing $\mathbb{F}_p$. Suppose a polynomial $f \in \mathbb{F}_p[\overline{x}]$ is computable by an algebraic circuit over $\mathbb{F}_{p^k}$ of size s. Show that f is computable by an algebraic circuit over $\mathbb{F}_p$ of size $s \cdot \mathsf{poly}(k)$.

   Hint: Use that there is an element $\gamma \in \mathbb{F}_{p^k}$ that satisfies an equation $P(\gamma) = 0$ for some $P(x) = \sum_{0 \leq i \leq k} \beta_i x^i$, such that every element of $\mathbb{F}_{p^k}$ can be expressed as $\sum_{0 \leq i < k} \alpha_i \gamma^i$, where $\alpha_i \in \mathbb{F}_p$,

4. (a) Prove *Fisher's identity*

$$x_1 \cdots x_n = \frac{(-1)^n}{n!} \sum_{S \subseteq [n]} (-1)^{|S|} \left(\sum_{i \in S} x_i \right)^n ,$$

   assuming $n!$ is invertible in the field $\mathbb{F}$.

   (b) Conclude that over fields where $d!$ is invertible, that any polynomial in n variables of degree $\leq d$ can be written in the form $\sum_{i=1}^{r} \alpha_i \ell_i(\overline{x})^{d_i}$, where $\alpha_i \in \mathbb{F}$, $\deg \ell_i \leq 1$, $d_i \leq d$, and r is bounded by some exponential function of n and d.

changelog

v1 → v2 (2023-02-07 21:20)

- Deadline extended from 2023-02-06 to 2023-02-08.
- problem 4(b): Clarified that the powers of linear forms can have an additional scalar outside the powering.