18.408 Topics in Theoretical Computer Science Fall 2022
Problem Set 2

1. In this problem, we will prove a variant of the Schwarz-Zippel Lemma for individual degrees, stating that for $d < q$, if $f\colon \mathbb{F}_q^m \to \mathbb{F}_q$ is a polynomial in which the individual degree of each variable is at most d, the total degree is at most D, and $f \not\equiv 0$, then $\Pr_{x \in \mathbb{F}_q^n}\left[f(x) \neq 0\right] \geqslant \left(1 - \frac{d}{q}\right)^D$.

   (a) Show that the statement holds for $n = 1$.

   (b) Prove the statement by induction on n.

Low-degree testing

2. In this question, we will consider the Plane versus Line test and analyze its soundness. Suppose that $\mathbb{F}_q$ is a field, $A_2\colon S_2(\mathbb{F}_q^m) \to \{\text{degree } d \text{ bi-variate polynomials}\}$ is an assignment to all planes, and $A_1\colon S_1(\mathbb{F}_q^m) \to \{\text{degree } d \text{ uni-variate polynomials}\}$ is an assignment to all lines such that A_2, A_1 pass the Plane versus Line test with probability at least ε, where $\varepsilon \geqslant \sqrt{\frac{dm}{q}}$.

   (a) Show that A_2 passes the Plane versus Plane test with probability at least ε^2.

   (b) Deduce the following list-decoding statement: for all $\delta > \frac{d^{10}m^{10}}{q^{1/10}}$ there is $k = k(\delta) \in \mathbb{N}$, such that for any A_1, A_2 as above, there are $f_1, \ldots, f_k\colon \mathbb{F}_q^m \to \mathbb{F}_q$ of degree at most d such that

$$\Pr_{\substack{\ell \in S_1(\mathbb{F}_q^m), P \in S_2(\mathbb{F}_q^m) \\ \ell \subseteq P}}\left[A_2[P]|_\ell \equiv A_1[\ell] \wedge \bigwedge_{i=1}^{k} A_2[P] \not\equiv f_j|_P\right] \leqslant \delta.$$

3. In this question, we will design a nearly linear size version of the Plane versus Plane test.

   Let $1 \leqslant h < q$ be powers of 2, consider the field $\mathbb{F}_q$ and take a sub-field $\mathbb{H} \subseteq \mathbb{F}_q$ of size h. We define the set of planes with directions in $\mathbb{H}^3$ as

$$S_2(\mathbb{F}_q^3, \mathbb{H}^3) = \left\{ P = a + \mathsf{Span}_{\mathbb{F}_q}(x, y) \quad a \in \mathbb{F}_q^3, x, y \in \mathbb{H}^3 \right\}.$$

   We will think of q as very large, and h as much smaller (you should think of $h = q^{0.0001}$, say).

   (a) Show that $S_2(\mathbb{F}_q^3, \mathbb{H}^3) = \frac{q^3(h^3-1)}{q^2(h-1)}$. Thus, the number of planes in $S_2(\mathbb{F}_q^3, \mathbb{H}^3)$ is nearly linear in the number of points in $\mathbb{F}_q^3$.

   (b) Show that $P_1, P_2 \in S_2(\mathbb{F}_q^3, \mathbb{H}^3)$ are parallel if and only if they can be written as $P_1 = a + L$, $P_2 = a' + L$ for a linear subspace $L = \mathsf{Span}(x, y)$ where $x, y \in \mathbb{H}^3$ and $a \neq a'$. Deduce that choosing P_1, P_2 independently, the probability they are parallel is $\frac{h-1}{h^3-1}$.

(c) Show that for every line $\ell = a + \mathsf{Span}(x)$ where $x \in \mathbb{H}^3$, the probability a random plane $P \in S_2(\mathbb{F}_q^3, \mathbb{H}^3)$ does not intersect ℓ is at most $\frac{1}{h}$.

(d) Given an assignment $B_2 \colon S_2(\mathbb{F}_q^3, \mathbb{H}^3) \to \{\text{bi-variate degree d polynomials}\}$, we define the graph $G = (V, E)$ whose vertex set is $V = S_2(\mathbb{F}_q^3, \mathbb{H}^3)$ and (P_1, P_2) is an edge if $B_2[P_1]$ and $B_2[P_2]$ agree on $P_1 \cap P_2$. Show that $\beta(G) \leqslant \frac{1}{h} + \frac{d}{q}$.

4. (Not for submission) Prove the following version of the Plane versus Plane Theorem: suppose that for $B_2 \colon S_2(\mathbb{F}_q^3, \mathbb{H}^3) \to \{\text{bi-variate degree d polynomials}\}$, sampling $P_1, P_2 \in S_2(\mathbb{F}_q^3, \mathbb{H}^3)$ that intersect in a line, we have that $B_2[P_1]|_{P_1 \cap P_2} \equiv B_2[P_2]|_{P_1 \cap P_2}$ with probability at least $\varepsilon > 100\sqrt{\frac{1}{h} + \frac{d}{q}}$. Show that there is $f \colon \mathbb{F}_q^3 \to \mathbb{F}_q$ of degree at most d such that

$$\Pr_{P \in S_2(\mathbb{F}_q^3, \mathbb{H}^3)} [f|_P \equiv B_2[P]] \geqslant \Omega(\sqrt{\varepsilon}).$$

Interactive Protocols

5. An interactive protocol consists of two entities, a verifier V which is a randomized algorithm running in polynomial time, and an all powerful prover P. When ran on an input x known both to V and P, the protocol proceeds by an exchange of messages between V and P, at the end of which V decides whether to accept or reject. We say a language L is in the class IP if there is a protocol (V, P) such that:

   (a) For every $x \in L$, Pr $[(V, P) \text{ accepts on } x] \geqslant \frac{2}{3}$.

   (b) For every $x \notin L$, and any potential prover P', Pr $[(V, P') \text{ accepts on } x] \leqslant \frac{1}{3}$.

   In words, every input in L is accepted by V with probability at least $2/3$, and for any input x outside L, no prover strategy can convince V that x is in the language.

   Show that NP $\subseteq$ IP, and that IP $\subseteq$ PSPACE.

6. (*) Consider the $\#3SAT$ problem, in which the goal the input is a 3CNF formula $\phi(x_1, \ldots, x_n) = \bigwedge_{i=1}^{m} C_i$ where each clause C_i is a conjunction of 3-literals. The goal is to output the number of satisfying assignments to ϕ. Show that $\#3SAT$ is in IP. (hint:

18.408 Topics in Theoretical Computer Science: Probabilistically Checkable Proofs
Fall 2022