Probabilistically Checkable Proofs	Spring 2008

Exercise no. 2

Due: March 26th, 2008

For a finite field $\mathbb{F}$ and a natural number d, we denote by $\mathbb{F}_{\leq d}[x_1, \ldots, x_n]$ the set of polynomials of degree at most d over variables $x_1, \ldots, x_n$. For $\vec{a}_0, \ldots, \vec{a}_k \in \mathbb{F}^n$ the degree-k *curve* defined by $\vec{a}_0, \ldots, \vec{a}_k$ is $c[\vec{a}_0, \ldots, \vec{a}_k] \doteq \{\vec{a}_0 + \vec{a}_1 \cdot t + \ldots + \vec{a}_k \cdot t^k \mid t \in \mathbb{F}\}$. For $\vec{a}, \vec{b} \in \mathbb{F}^n$, we denote the *line* defined by $\vec{a}, \vec{b}$ by $\ell[\vec{a}, \vec{b}] \doteq c[\vec{b}, \vec{a}]$. The *restriction* of a function $f : \mathbb{F}^n \to \mathbb{F}$ to the curve $c = c[\vec{a}_0, \ldots, \vec{a}_k]$ is the function $f_{|c} \in \mathbb{F}[t]$ defined by $f_{|c} \doteq f(\vec{a}_0 + \vec{a}_1 \cdot t + \ldots + \vec{a}_k \cdot t^k)$.

1. **Low degree curves.** Prove the following:
   (a) *Restriction to a low degree curve:* The restriction of a polynomial $f \in \mathbb{F}_{\leq d}[x_1, \ldots, x_n]$ to a degree-k curve is of degree at most dk.
   (b) *Interpolation:* Let $t_0, \ldots, t_k \in \mathbb{F}$ be $k+1$ different scalars. Given points $\vec{x}_0, \ldots, \vec{x}_k \in \mathbb{F}^n$, there is a unique degree-k curve $\gamma : \mathbb{F} \to \mathbb{F}^n$ such that $\gamma(t_i) = \vec{x}_i$ for every $i \in \{0, \ldots, k\}$.

2. **Hitting a set.** Fix a set $A \subseteq \mathbb{F}^n$. Pick $\vec{a}, \vec{b} \in \mathbb{F}^n$ uniformly at random and let $X = X(\vec{a}, \vec{b})$ be the random variable counting the fraction of points on the line $\ell = \ell[\vec{a}, \vec{b}]$ that fall into A, i.e., $\frac{|\ell \cap A|}{|\ell|}$. Prove:
   (a) *Expectation:* $\mathbf{E}_{\vec{a},\vec{b}}[X] = \frac{|A|}{|\mathbb{F}^n|}$.
   (b) *Concentration:* For $\varepsilon, \delta \in (0,1)$ such that $\varepsilon \geq \sqrt{\frac{1}{\delta|\mathbb{F}|}}$, we have
   $$\Pr_{\vec{a},\vec{b}}\left[\left|X - \frac{|A|}{|\mathbb{F}^n|}\right| \geq \varepsilon\right] \leq \delta$$
   Hint: Use Chebyshev's inequality stating that for any random variable X with finite variance and every $\varepsilon > 0$, $\Pr[|X - \mathbf{E}[X]| \geq \varepsilon] \leq \frac{\mathrm{Var}[X]}{\varepsilon^2}$.

3. **The Schwartz-Zippel lemma:** Prove that for two *different* polynomials $p, q \in \mathbb{F}_{\leq d}[x_1, \ldots, x_n]$,
   $$\Pr_{\vec{x} \in \mathbb{F}^n}[p(\vec{x}) = q(\vec{x})] \leq \frac{d}{|\mathbb{F}|}$$

4. **All-zero test.** Let $\mathbb{F}$ be a finite field. Let $H \subseteq \mathbb{F}$. Let m and d be natural numbers. Assume that d and m are sufficiently smaller than $|\mathbb{F}|$. Denote $n = |\mathbb{F}^m|$ where $|\mathbb{F}| = \mathrm{poly}\log n$. Given a polynomial $p \in \mathbb{F}_{\leq d}[x_1, \ldots, x_m]$, we would like to check whether p is zero on *all* the points in H^m.
   (a) *Polynomial identity testing algorithm.* Assume $H = \mathbb{F}$. Design an efficient algorithm that uses $O(\log n)$ random bits and makes one query to p:
      - If $p \equiv 0$, the algorithm should always output YES.
      - If $p \not\equiv 0$, the algorithm should output YES with probability at most $\frac{1}{2}$.
   (b) *All-zero tester.* Assume $|H| \ll |\mathbb{F}|$. Design an efficient verifier that uses $O(\log n)$ random bits and makes $\mathrm{poly}\log n$ queries to p and to a proof π:
      - If for every $\vec{x} \in H^m$, $p(\vec{x}) = 0$, there should exist a proof π, on which the verifier always accepts.
      - If there is $\vec{x} \in H^m$ such that $p(\vec{x}) \neq 0$, then for *any** purported proof π, the verifier accepts with probability at most $\frac{1}{2}$.

   (*) Do not address "low degree testing". Instead of handling *any* purported proof, you may assume that the proof contains truth-tables of low degree polynomials.

5. **Approximation by polynomials.** Consider a function $f : \mathbb{F}^n \to \mathbb{F}$. Let d be a natural number. Let $\delta \in [0, 1]$.

   - We say that a polynomial $p \in \mathbb{F}_{\leq d}[x_1, \ldots, x_n]$ δ-*approximates* f, if they agree on at least δ fraction of the points, i.e., $\Pr_{\vec{x} \in \mathbb{F}^n}[f(\vec{x}) = p(\vec{x})] \geq \delta$.
   - Let $L^{\delta}_{\leq d}[f]$ be the set of all polynomials $p \in \mathbb{F}_{\leq d}[x_1, \ldots, x_n]$ that δ-approximate f.
   - Let $agr_{\leq d}(f)$ be the largest fraction of points δ on which some polynomial of degree at most d δ-approximates f, i.e., $L^{\delta}_{\leq d}[f] \neq \emptyset$.

   Show:

   (a) *List is short:* For a large enough agreement $\delta \geq 2\sqrt{\frac{d}{|\mathbb{F}|}}$, the list is short $\left|L^{\delta}_{\leq d}[f]\right| \leq \frac{2}{\delta}$.

   (b) *Some functions cannot be approximated:* There exists a function $f^* : \mathbb{F}^n \to \mathbb{F}$ such that $agr_{\leq d}(f^*) \leq \frac{d+1}{|\mathbb{F}|}$.

   (c) *Approximations of restrictions:* $\mathbf{E}_{\vec{a}, \vec{b} \in \mathbb{F}^n}\left[agr_{\leq d}(f_{|\ell[\vec{a}, \vec{b}]})\right] \geq agr_{\leq d}(f)$.