6.842 Randomness and Computation May 7, 2014

Homework 11

Lecturer: Ronitt Rubinfeld *Due Date: May 15, 2014 (Optional)*

Homework guidelines: You may work with other students, as long as (1) they have not yet solved the problem, (2) you write down the names of all other students with which you discussed the problem, and (3) you write up the solution on your own. No points will be deducted, no matter how many people you talk to, as long as you are honest. If you already knew the answer to one of the problems (call these "famous" problems), then let me know that in your solution writeup – it will not affect your score, but will help me in the future. It's ok to look up famous sums and inequalities that help you to solve the problem, but don't look up an entire solution.

The following problems are to be turned in. You should upload your solution to Stellar as a pdf file.

1. **(Worst-case to average-case reductions for the permanent)** Let $n \in \mathbb{N}$ and assume that $q > n$. For any matrix $M \in \mathbb{F}_q^{n\times n}$, the *permanent* of M is defined by:

$$Perm(M) = \sum_{\sigma \in S_n} \prod_{i \in [n]} M_{i,\sigma(i)}$$

where S_n denotes the set of all permutations of $[n]$.

Show that if there exists a deterministic polynomial time algorithm computing $Perm(M)$ with probability at least $1 - \frac{1}{10(n+1)}$ on a random matrix $M \in_R \mathbb{F}_q^{n\times n}$, then there exists a randomized polynomial-time algorithm computing *any* given matrix $M \in \mathbb{F}_q^{n\times n}$ with probability at least 0.9 (over the internal randomness of the algorithm).

Hint:

- Note that for any two fixed matrices $M, X \in \mathbb{F}_q^{n\times n}$, $Perm(M + tX)$ is a univariate polynomial in $t \in \mathbb{F}_q$ of degree at most n.
- You can use the standard fact from linear algebra that the determinant of the Vandermonde matrix
$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^d \\ 1 & x_2 & x_2^2 & \dots & x_2^d \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_{d+1} & x_{d+1}^2 & \dots & x_{d+1}^d \end{pmatrix}$$
is non-zero if and only if $x_i \neq x_j$ for every $i \neq j \in [d+1]$.

2. We say that a distribution H over $\{0,1\}^n$ has density δ if for every $x \in \{0,1\}^n$,

$$\Pr[H = x] \leq 1/(\delta 2^n)$$

We say that a distribution D over $\{0,1\}^n$ is K-flat if D is the uniform distribution over a subset of $\{0,1\}^n$ with size at least K. Prove that for every k, every 2^{-k}-density distribution H is a convex combination of 2^{n-k}-flat distributions. That is, there are N 2^{n-k}-flat distributions $D_1, \ldots, D_N$ and nonnegative numbers $\alpha_1, \ldots, \alpha_N$ such that $\sum_{i=1}^{N} \alpha_i = 1$ and H is equivalent to the distribution obtained by picking i with probability α_i and then picking a random element from D_i.

3. Recall that a distribution X over $\{0,1\}^n$ with min-entropy at least k is called an (n,k)-source. Prove that for every function $Ext : \{0,1\}^n \to \{0,1\}^m$, there exists an $(n, n-1)$-source X and a bit $b \in \{0,1\}$ such that $\Pr[Ext(X)_1 = b] = 1$ (where $Ext(X)_1$ denotes the first bit of $Ext(X)$). Prove that this implies that $\Delta(Ext(X), U_m) \geq 1/2$ where Δ is the statistical distance.