Randomized Algorithms 2013A – Problem Set 2

Robert Krauthgamer

November 20, 2012

1. Let B be a randomized algorithm that approximates some function $f(x)$ as follows:

$$\forall x, \quad \Pr\left[B(x) \in (1 \pm \varepsilon) f(x)\right] \geq 2/3.$$

Let algorithm C output the median of $O(\log \frac{1}{\delta})$ independent executions of algorithm B on the same input. Prove that

$$\forall x, \quad \Pr\left[C(x) \in (1 \pm \varepsilon) f(x)\right] \geq 1 - \delta.$$

2. Let A, B, C be three $n \times n$ matrices over a field F such that $AB \neq C$. Show that if $r \in \{0,1\}^n$ is chosen uniformly at random, then $\Pr[ABr \neq Cr] \geq 1/2$.

Use the above to design a randomized algorithm that checks, given three such matrices as input, whether $AB = C$. The algorithm should run in time $O(n^2)$, without any matrix multiplication.

If necessary, assume the field F is just $GF[2]$ or $\mathbb{Q}$.

Extra credit:

3. Let $X_1, \ldots, X_n \in \{-1, +1\}$ be chosen independently uniformly at random, and fix m distinct non-empty subsets $S_1, \ldots, S_m \subseteq [n]$.

   (a) Define the polynomial $p(x_1, \ldots, x_n) := \sum_{i=1}^m (\prod_{k \in S_i} x_k)$, and show that with high (constant) probability (over the choice of the X_i's), $|p(X_1, \ldots, X_n)| \leq O(\sqrt{m})$.

   Example: $p(X_1, X_2, X_3) = X_1 + X_2 + X_3 + X_1 X_2$ can be viewed as four steps of a random walk on $\mathbb{Z}$, where the first two steps completely determine the fourth one.

   Hint: Use the second moment method.

   (b) Show that the assertion in part (a) holds also when the X_i's are independent standard gaussians $N(0,1)$.

   (c) Generalize part (a) to a polynomial $p'(x_1, \ldots, x_n) = \sum_{i=1}^m (a_i \prod_{k \in S_i} x_k)$, where $a_1, \ldots, a_m \in \mathbb{R}$ are fixed coefficients.

   Hint: The bound should depend on the norm of the vector $\vec{a} = (a_1, \ldots, a_m)$.