0368-4159: A first course in derandomization 13/1/19

Take-Home Exam

Amnon Ta-Shma and Noam Parzanchevski

General instructions:

1. The deadline for the exam is 17/02/19.
2. Submit your (typed) solution by mail to amnon@tau.ac.il.
3. Work must be done alone.
4. If you had to use an electronic source, state it explicitly within the relevant question.

1 k-wise independence (15 points)

Our goal in this question is to prove:

Claim 1. *Let $X \subseteq \{0,1\}^n$ be a k-wise independent distribution over $\{0,1\}^n$, then $|X| \geqslant \Omega\left(n^{k/2}\right)$*

1. Give an explicit construction that given a prime power n and $k \leq n$ outputs an $n \times k$ matrix over $\mathbb{F}_n$ such that any $k \times k$ minor is invertible over $\mathbb{F}_n$.

2. For an infinite sequence of input lengths n, give an explicit construction of a pairwise independent distribution D over $\mathbb{F}_2^{n-1}$ with $|D| = n$.

3. Prove that $D \subseteq \{0,1\}^n$ is a k-wise independent distribution if and only if $\hat{D}(S) = 0$ for every S with $0 < |S| \leq k$.

4. Let $d = \frac{k}{2}$ and denote $t = \sum_{i=0}^{d} \binom{n}{i}$. Let $X \subseteq \{0,1\}^n$ with $|X| < t$. Show that there is a function $f : \{0,1\}^n \to \mathbb{R}$ which satisfies:

   - $f(x) = 0$ for every $x \in X$.
   - f is not identically zero.
   - $\hat{f}(S) = 0$ for every S with $|S| > d$.

5. Conclude that for any constant k, any k-wise independent distribution over $\{0,1\}^n$ has support size at least $\Omega(n^{k/2})$.

2 (k, ε)-bias (15 points)

In class we talked about k-wise independence and ε-bias. It is known that:

- For $n = 2^t$ and $k \leq n$ there exists an $n \times \frac{\log n}{2} k$ matrix over $\mathbb{F}_2$ such that any k rows are independent over $\mathbb{F}_2$.
- There exist an ε-biased distributions $D \subseteq \{0,1\}^m$ with support size $O(\frac{m}{\varepsilon^2})$.

Definition 2. *A distribution $X \subseteq \{0,1\}^n$ is k-wise ε-biased, if for every $t \leqslant k$ and $I = \{i_1, \ldots, i_t\} \subseteq [n]$ the random variable $X_{i_1} \circ \cdots \circ X_{i_t}$ is ε-biased.*

Construct a k-wise ε-biased distribution $X \subseteq \{0,1\}^n$ using $\log \log n + \log k + 2 \log \frac{1}{\varepsilon} + O(1)$ bits of randomness.

3 Expansion and Codes (25 points)

For a D-regular undirected graph $G = (V, E)$ over N vertices:

- $\lambda(G)$ is its second largest eigenvalue in absolute value.
- The vertex expansion of a set $A \subseteq V$ is $e(A) \stackrel{\text{def}}{=} \frac{|\Gamma(A)|}{|A|}$ where $\Gamma(A) = \{w \in V \mid \exists v \in A : (v, w) \in E\}$.

For a subset $A \subseteq V$ the *density* of A is $\rho(A) \stackrel{\text{def}}{=} \frac{|A|}{|V|}$. For a family $G = \{G_n\}_{n \in \mathrm{N}}$ where G_n is a D-regular graph over n vertices, we say G is (α, c)–expanding if for for all n large enough, and all sets A of density at most α, $e(A) \geq c$.

1. Prove that for every $G = (V, E)$ and $A \subseteq V$,
$$e(A) \geqslant \frac{1}{\rho(A) + (1 - \rho(A))\lambda(G)^2}.$$
2. Let $G = \{G_n\}_{n \in \mathrm{N}}$ be a family of D-regular Ramanujan graphs. Show that there exists some constant $\alpha > 0$ such that G is $(\alpha, D/4)$ expanding.
3. Prove that you can never guarantee more than $D - 1$ expansion.

We remark that, in fact, in Ramanujan graphs the true expansion approaches (with n) at least $D/2$, and this is tight in the sense that there are Ramanujan graphs with expansion at most $D/2$.

4. Prove that for a fixed D, a random $G = \{G_n\}$ of a family of D-regular *directed* graphs, w.h.p., there exists some constant $\alpha > 0$ such that G is $(\alpha, D - 10)$ expanding. (A similar phenomenon is true for undirected graphs, but we need first to define the model of a random D-regular undirected graph).

Next, we consider expansion in unbalanced bi-partite graphs with n vertices on the left and βn on the right for $0 < \beta < 1$ (thus, in a sense, the graph is condensing). We look at a family $G = \{G_n\}_{n \in \mathrm{N}}$, where $G_n = (V_n, W_n, E_n)$ with left degree D, $|V_n| = n$ and $|W_n| = \beta n$. We say G is (α, c)–expanding if for all n large enough, and all sets $A \subseteq V$ of density at most α, $e(A) \geq c$.

5. Prove that for a fixed β and D a random $G = \{G_n\}_{n \in \mathrm{N}}$ with regular left-degree D is $(\alpha, D-10)$ expanding, for some constant $0 < \alpha < 1$.

We remark that there are explicit constructions of such graphs with $(\alpha, \frac{2D}{3})$ expansion.

Definition 3. *Let $G = (V, W, E)$ be a left D-regular undirected graph. The code $C(G) \subseteq \{0, 1\}^{|V|}$ is defined as follows:*

$$C(G) = \left\{ x \in \{0,1\}^{|V|} \;\middle|\; \forall w \in W : \sum_{v : v \in \Gamma(w)} x_v = 0 \right\}$$

Where addition is done in $\mathbb{F}_2$.

6. Show that $C(G)$ is a linear code with rate at least $(1 - \beta)n$.
7. Prove that if G is (α, c)-expanding for $c > D/2$ then $C(G)$ is asymptotically good. Specifically, prove that the distance of $C(G)$ is at least αn.

4 Universal traversal sequences (20 points)

Definition 4. *Let F be a family of D-regular labelled graphs. We say the string $\sigma = (\sigma_1, \dots, \sigma_T) \in [D]^T$ is a* universal traversal sequence *(UTS) for F if for every graph G in F and every vertex v of G, the walk σ starting at v will visit all the vertices of the graph.*

As usual, let $G = (V, E)$ a D-regular, connected, undirected, non-bipartite graph over n vertices, A_G the normalized adjacency matrix of G, $\lambda_1 > \lambda_2 > \cdots > \lambda_n$ the spectrum of A_G, and $\bar{\lambda} = \max\{-\lambda_n, \lambda_2\}$.

Fact 5. $\bar{\lambda} \leqslant 1 - \frac{1}{2dn^3}$.

1. Let $\mathcal{G}$ be the family of all D-regular, connected, undirected, non-bipartite graphs over n where D is some constant. Show that there is a polynomial $p(n)$ such that for any $G = (V, E) \in \mathcal{G}$ and pair of vertices $s, t \in V$, the probability that a random walk of length $p(n)$ from s *does not* reach t is at most $2^{-n^{10}}$.

2. Prove that there exists a UTS for $\mathcal{G}$ of length $poly(n)$

5 Eps-bias amplification (25 points)

In this question we construct an ε-biased distribution using some base ε_0-biased distribution and a family of expander graphs.

1. Let $D \subseteq \{0,1\}^n$ be an ε-biased distribution (i.e. - D is flat over its support and has ε-bias) and let $G = (V, E)$ be a d-regular λ-expander where $|V| = |D|$ and we identify the vertices of G with the elements in D.

   We now define a new distribution D' by sampling an *ordered* edge in G and outputting the sum of its vertices: $D' = \{x_i + x_j \mid (x_i, x_j) \in E\}$.

   Prove that D' is at most $(\lambda + \varepsilon^2)$-biased. What is the support size of D'?

2. Suppose X_0 is ε_0-biased over $\{0,1\}^k$ with support size D_0 for $\varepsilon_0 < 1/2$, and you have $[N, D, \lambda]$ expanders with $\lambda = \frac{2}{\sqrt{D}}$ for any N, D you wish.

   Prove that by repeating this process i times, you get an $\varepsilon_i = \frac{1}{2}(2\varepsilon_0)^{2^i}$-biased distribution over $\{0,1\}^k$ with support size $\prod_{j=0}^{i} D_j$ where for any $1 \leqslant j \leqslant i$: $D_j = \frac{64}{(2\varepsilon_0)^{2^{j+2}}}$.

   Remark: The parameters here are meant to help you with analysis. Anything that is correct and is enough (or better) to solve the next item is good.

3. Use Justesen code and the above recursion to given an ε-biased distribution over $\{0,1\}^k$ with support size $\tilde{O}(\frac{k}{\varepsilon^8})$, where the $\tilde{0}$ suppresses multiplicative logarithmic terms.

Good luck!!!