Expander Course - Homework set 2

Due: April 8 (first class after Pesach)
(Same due date as for exercise 1).

All graphs in this problem set are undirected, connected and have no self loops (but may have parallel edges). n will always denote the size (number of vertices) of the graph. A d-regular graph on n vertices is denoted (n, d)-graph. We let $\mu_0(G) \geq \cdots \geq \mu_{n-1}(G)$ be the eigenvalues of the adjacency matrix of G, and $\lambda(G) = max_{i \geq 1}|\mu_i(G)|$. An (n, d)-graph G is a (n, d, λ)-graph if $\lambda(G) \leq \lambda d$.

All assymptotic O and Ω notation means a fixed multiplicative constant (upper and lower) bound respectively, independent of all other parameters.

Problem 1.

1. Prove that an (n, d)-graph G is connected iff $\mu_1(G) < \mu_0(G)$
2. Prove that an (n, d)-graph G is bipartite (=2-colorable) iff $\lambda_{n-1} = -d$.

Problem 2. Prove that for every n, d and every (n, d, λ)-graph

1. $\Omega(Diam(G)) \leq Mix(G) \leq O(\log n / \log(1/\lambda))$
2. $\chi(G) \geq 1/\lambda$

Conclude the bounds for Ramanujan graphs, and compare to random graphs from the last exercise.

While the bounds above show that Ramanujan graphs can be as good as random for some parameters, the two problems below demonstrate that in other parameters the consequence of the eigenvalue bound is weaker than what random graphs give.

Definition 1. A graph G is an a-expander if for every two vertex subsets S, T of size at least n/a there is an edge (s, t) of G with $s \in S$ and $t \in T$.

Problem 3.

1. Prove that for every n, a there exist (n, d)-graphs which are a-expanders with $d = O(a \log a)$.
2. Prove that every (n, d, λ)-graph is $1/\lambda$-expander. Conclude that a Ramanujan (n, d)-graph is and a-expander with $d = O(a^2)$.

Definition 2. 1. A (k, c)-expander is a graph in which every set S of size at most k has $|\Gamma(S)| \geq c|S|$.

2. A unique neighbour of S is a vertex in $\Gamma(S)$ connected by an edge to only one vertex in S.

Problem 4. 1. Prove that every subset S in a (k, c)-expander has at least $\Omega(|S|(c - \frac{d}{2})$ unique neighbours.

2. Prove that for any $d \geq 30$ there exists (n, d)-graphs which are $(n/50d, 3/4d)$-expanders.

3. Prove that an (n, d, λ)-graph is a $(\rho n, 1/(\rho + \lambda^2))$-expander for any $0 < \rho < 1$. Conclude that Ramanujan graphs are $(4/d^2, d/4)$-expanders. **Comment:** This result can be improved to give expansion of $d/2 - \epsilon$ in Ramanujan graphs, and there are Ramanujan graphs whose expansion is $d/2$.

Definition 3. Let F be a collection of real functions on some finite domain X. Let U be the uniform distribution on X. A distribution D on X is called an ϵ *discrepancy set* (or *ϵ-pseudorandom*) for F if for every function $f \in F$, the average value of f under U and under D differ by at most ϵ (i.e., $|E[f(U)] - E[f(D)]| \leq \epsilon$).

Interesting pseudorandom distributions are usually those with small support (or low entropy). Typically the functions studied are Boolean, namely characteristic functions of sets. The collections typically correspond to functions computed by efficient algorithms in some computational model. The following exercise shows that expanders yield pseudorandom distributions for low communication protocols, defined next.

Definition 4. Alice and Bob have each an m bit input, resp. x and y. They wish to compute some fixed Boolean function $f(x, y)$. A protocol P for f is a specification for each player of which bits to send at every round, given its input and the bits sent so far. $c(P)$ is the communication complexity of the protocol P, defined as the maximum number of bits sent on the worst case choice of inputs. $c(f)$, the communication complexity of f is the minimum $c(P)$ over all protocols for f.

Problem 5. Let G be an $(2^m, d, 2^{-6c})$-graph. We define a distribution D on strings of length $2m$ by choosing a random edge of the graph G.[1] Prove that the distribution D is 2^{-c}-pseudorandom for the class of all functions $f : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}$ of communication complexity c.

Note that d can be taken to be $2^{O(c)}$, so the entropy of D is only $m + O(c)$ while the entropy of a completely random input is $2m$. We'll see later in the course how to build on top of this idea for much greater savings in pseudorandomness for small space computations.

Hint: Observe that a protocol for computing f with c bits of communication partitions the matrix describing the function to at most 2^c generalized rectangles (i.e., cartesian products of a subset of the rows with a subset of the columns) which are constant on f. Use the expander mixing lemma on each one.

[1] Note that since G is undirected, if there is an edge between x and y then the pairs (x, y) and (y, x) will have equal probability in the distribution D.