Algebraic Methods December 7, 2016

Exercise 2

Lecturer: Amir Shpilka Hand in date: **December 28, 2016**

Instructions: Please do not copy anyone else's solution. You are allowed to consult with other classmates if you thought about the problem yourself first, but you should only ask for the idea of the solution rather than copying the entire solution. And, most importantly, you should give credit to the classmate with whom you discussed the solution.

1. An independent set in a graph is a set of vertices, no two of which are adjacent. Let G be a d-regular graph on n vertices with eigenvalues $d = \lambda_1 \geq \lambda_2 \geq \cdots$. Let $\lambda = \max(\lambda_2, |\lambda_n|)$. Give the best upper bound that you can find on the size of an independent set in G in terms of λ, d, n.

2. Let G be as in Question 1. Let $0 < \delta \leq \frac{d-\lambda_2}{8d}$ be some small constant. Show that if we remove δdn edges from the graph then there is still a connected component of size at least $(1 - \frac{2\delta d}{d-\lambda_2})n$.

3. Let G be as in Question 1. For two vertices x, y in G we denote with $\Delta(x, y)$ the distance between them, that is, the length of the shortest path between them. The diameter of G is defined as $\mathrm{diam}(G) = \max_{x,y \in V(G)} \Delta(x, y)$. Show that $\mathrm{diam}(G) \leq \frac{2\log(n)}{\log(3-\frac{\lambda_2}{d})-1} + O(1)$.

4. Let G be as in question 1. Assume that initially an adversary "infects" a subset B_0 of the vertices V. At every subsequent time step t the infected set B_t is determined to be exactly those vertices that have at least $\frac{1}{3}d$ neighbors in B_{t-1}. A graph is healthy if for every initial subset B_0 of size at most $n/4$, after a finite number T of steps we have $B_T = \emptyset$.

   Assume $\lambda < d/13$. Show that G is healthy. Moreover, the time it takes until all vertices are not infected is at most $O(\log n)$.

5. Let G be as in Question 1 and A its adjacency matrix. Let v_i be the eigenvector corresponding to the eigenvalue λ_i. Prove that for $0 \leq i \leq n-1$,

$$\lambda_{i+1} = \max_{\|v\|=1,\, v \perp \mathrm{span}\{v_1,\ldots,v_i\}} \langle Av, v \rangle.$$

6. Let G be as in Question 1. Let $h = \min_{|S| \leq n/2} \frac{e(S,S^c)}{|S|}$. Prove that $h \geq \frac{d-\lambda_2}{2}$.
   Hint: Construct an adequate $v \perp \mathbf{1}$ using an extremal set S and its complement.

7. **Cayley graphs and ϵ-biased sets.**

   Definition 1. *Let Γ be a group and $S \subset \Gamma$ be a generating set for Γ. We now define the Cayley graph of Γ with resect to S, Cay(Γ, S). The graph has $|\Gamma|$ vertices, which we identify with the elements of Γ. $\gamma_1, \gamma_2 \in \Gamma$ are connected by an edge if and only if there is an element $s \in S$ such that $\gamma_1 \cdot s = \gamma_2$ (in case of vector spaces if $\gamma_1 + s = \gamma_2$).*

In this exercise we shall only consider Cayley graphs for the group (vector space) $\Gamma = \mathbb{F}_2^n$.

Definition 2. *A multi-set $S \subset \{0,1\}^n$ is ϵ-biased if for every vector $\mathbf{0} \neq v \in \{0,1\}^n$ we have that $\left|\sum_{s \in S}(-1)^{\langle v,s\rangle}\right| \leq \epsilon \cdot |S|$. In other words,*

$$\left| \Pr_{s \in_R S}[\langle v, s\rangle = 0] - \Pr_{s \in_R S}[\langle v, s\rangle = 1] \right| \leq \epsilon.$$

(a) Prove that the second normalized eigenvalue in absolute value of the adjacency matrix of $\mathrm{Cay}(\Gamma, S)$ (i.e. $\max(\lambda_2, |\lambda_n|)/d$) is bounded by ϵ if and only if S is an ϵ-biased set.

(b) Let $S_n \subseteq \{0,1\}^n$ be a an ϵ-biased sample space of size $m = |S_n|$. Show how to construct an error correcting code from S_n. Give a lower bound on its hamming distance, in terms of ϵ and m.
Hint: Consider the elements of S_n as the rows of an $m \times n$ matrix.

(c) Let $n = \epsilon \cdot 2^m$. Let $\mathrm{bin} : \mathbb{F}_{2^m} \to \{0,1\}^m$ be an invertible linear mapping from the field with 2^m elements, viewed as a vector space over $\mathbb{F}_2$, to the m-dimensional vector space over $\mathbb{F}_2$. (i.e. we give a binary representation for every field element such that the mapping to the binary representation is a linear transformation). In particular $\mathrm{bin}(x + y) = \mathrm{bin}(x) \oplus \mathrm{bin}(y)$ (where we take a bitwise XOR). Let $E_{m,n} : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \{0,1\}^n$ be defined in the following way. The i'th output bit (for $i = 0, \ldots, n-1$) of $E_{m,n}$ is equal to $\langle \mathrm{bin}(x^i), \mathrm{bin}(y)\rangle$ modulo 2. Let $S_{m,n}$ be the image of $E_{m,n}$ (an element may appear in $S_{m,n}$ more than once). Prove that the bias of $S_{m,n}$ is at most $(n-1)/2^m$. Note that $|S_{m,n}| = O(\frac{n^2}{\epsilon^2})$.