Algebraic Methods December 24, 2016

Exercise 3

Lecturer: Amir Shpilka Hand in date: **January 11, 2017**

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. In this question we construct a new family of codes. Let $\mathcal{C}_0 \subseteq \mathbb{F}_2^d$ be a linear code. $\mathcal{C}_0$ will be the *base code* of the construction. Let $H = (L \cup R, E)$ be a d regular bipartite graph with n vertices on each side. Notice that H has nd edges and assume that they are enumerated by $\{1, \ldots, nd\}$. As usual, we shall denote the edges incident to a vertex v by $\Gamma(v)$. Define the code $C(H, \mathcal{C}_0) \subseteq \mathbb{F}_2^{nd}$ as follows:

$$C(H, \mathcal{C}_0) = \{c \in \mathbb{F}_2^{nd} \mid \forall v \in L \cup R : \ c|_{\Gamma(v)} \in \mathcal{C}_0\}.$$

In other words, $C(H, \mathcal{C}_0)$ consists of all the binary words that assign values to the edges such that, for every vertex v, the values on the edges incident to it form a codeword of $\mathcal{C}_0$, where we use the natural order on the neighbors of v induced by the enumeration of the edges.

(a) Show that $C(H, \mathcal{C}_0)$ is a linear code.

(b) Let $1 - \epsilon$ be the relative rate of $\mathcal{C}_0$ (i.e. the rate of the code divided by the length of the code). Show that the relative rate of $C(H, \mathcal{C}_0)$ is at least $1 - 2\epsilon$.

We would like to construct a code with a good distance. For this purpose we need to choose the graph H carefully.

Let $G = (V, E)$ be a graph. Define the double cover of G, denoted by H_G, as the following bipartite graph: the vertices of H_G consist of the disjoint union of two copies of V, $L \cup R$, and we put an edge between $u \in L$ to $v \in R$ if there is an edge between u and v in G. Our final code will be $C(H_G, \mathcal{C}_0)$ for some expander G and base code $\mathcal{C}_0$.

In order to bound the distance of this code we will need the bipartite version of the expander mixing lemma:

Lemma 1. *Let G be an d regular expander on n vertices with eigenvalues $\lambda_1 \geq ... \geq \lambda_n$. Let $\lambda = \max\{\lambda_2, |\lambda_n|\}$. Let $H_G = (L \cup R, E_{H_G})$ be as defined above. Then*

$$\forall S \subseteq L, T \subseteq R, \quad \left| |E_{H_G}(S,T)| - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|}.$$

(c) Prove Lemma 1.

Let λ be as defined above and denote by δ_0 the relative distance of $\mathcal{C}_0$ (i.e. the distance of the code divided by the length of the code). We wish to show that the relative distance of $C(H_G, \mathcal{C}_0)$ is at least $\delta_0(\delta_0 - \frac{\lambda}{d})$. Let $c \in C(H_G, \mathcal{C}_0)$. Denote by $F_c \subseteq E_{H_G}$ the set of all edges i such that $c_i = 1$.

(d) Show that if for every nonzero $c \in C(H_G, \mathcal{C}_0)$, $|F_c| \geq \delta_0(\delta_0 - \frac{\lambda}{d})nd$ then the relative distance of the code is at least $\delta_0(\delta_0 - \frac{\lambda}{d})$.

Fix a nonzero $c \in C(H_G, \mathcal{C}_0)$. Let $S \subseteq L$ be the set of all vertices in L that are incident to at least one edge in F_c. Similarly, Let $T \subseteq R$ be the set of all vertices in R that are incident to at least one edge in F_c.

(e) Show that $\delta_0 d\sqrt{|S||T|} \leq |F_c| \leq \frac{d|S||T|}{n} + \lambda\sqrt{|S||T|}$.

(f) Show that $|F_c| \geq \delta_0(\delta_0 - \frac{\lambda}{d})nd$ and conclude that the relative distance of the code is at least $\delta_0(\delta_0 - \frac{\lambda}{d})$.

2. Let $G = ([n], E)$ be an undirected d-regular graph with second largest eigenvalue, in absolute value, λ. Denote $\bar{\lambda} = \lambda/d$. Let $W_1, ..., W_k \subseteq [n]$ be a sequence of k subsets of vertices, each of size μn. In this question we will estimate the probability that a random walk will stay inside the set W_i for every $i \in k$ when starting from a uniformly random vertex.

We will use the following notation. Let A be the adjacency matrix of G and $\bar{A} = A/d$. Let P_i be the projection matrix on W_i. I.e. P_i is the unique matrix such that $P_i e_j = e_j$ if $j \in W_i$ and $P_i e_j = 0$ otherwise, where e_j is the vector that has 1 in the jth coordinate and zero elsewhere. Let $\mathbf{1}_n$ be the vector $\mathbf{1}_n = (\frac{1}{n}, ..., \frac{1}{n})$, and let $v_1 = P_1\mathbf{1}_n$ and $v_{i+1} = P_{i+1}\bar{A}v_i$. For a vector u we denote by $u^{\|}$ the part of u that is parallel to $\mathbf{1}_n$ and with $u^{\perp}$ its perpendicular part, such that $u = u^{\|} + u^{\perp}$. We say that a walk of length k stays inside W_i for all $1 \leq i \leq k$, if for each such i, the ith step of the walk is in W_i.

(a) Show that $\|v_k\|_1$ is the probability that a random walk on the graph G, starting from a uniformly random vertex, stays inside W_i for all $1 \leq i \leq k$. Show that it is also equal to $\sqrt{n}\left\|v_k^{\|}\right\|_2$.

(b) Let x be a vector parallel to $\mathbf{1}_n$ and y a vector perpendicular to $\mathbf{1}_n$. Show that $||(P_i x)^{\perp}||_2 \leq \sqrt{\mu(1-\mu)}||x||_2$ and $||(P_i y)^{||}||_2 \leq \sqrt{\mu(1-\mu)}||y||_2$.

(c) Define $t = 2\sqrt{(1-\mu)/\mu}$ and assume $\bar{\lambda} \leq \mu/6$. Prove that for every $i \in [k-1]$, the following statements hold.

i. $\left\|v_{i+1}^{\|}\right\|_2 \geq \left(\mu - t\bar{\lambda}\sqrt{\mu(1-\mu)}\right)\left\|v_i^{\|}\right\|_2$.

ii. $\left\|v_{i+1}^{\perp}\right\|_2 \leq \left(t\bar{\lambda} + \sqrt{\mu(1-\mu)}\right)\left\|v_i^{\|}\right\|_2$.

iii. $\left\|v_{i+1}^{\perp}\right\|_2 \leq t\left\|v_{i+1}^{\|}\right\|_2$

(d) Show that if $\bar{\lambda} \leq \mu/6$ then the probability of the above random walk to stay inside W_i for all $1 \leq i \leq k$, is at least $\mu(\mu - 2\bar{\lambda})^{k-1}$

(e) Show that this probability is at most $\mu(\mu + 2\bar{\lambda})^{k-1}$. You may want to modify section (b) for this purpose.

3. We start with some notation. A line in direction $0 \neq v \in \mathbb{R}^d$ through a point $a \in \mathbb{R}^d$, denoted $L_{a,v}$, is the set $L_{a,v} = \{a + vt \mid t \in \mathbb{R}\}$. Notice that if $b \in L_{a,v}$ then $L_{a,v} = L_{b,v}$. Consider a set $\mathcal{L} \subseteq \mathbb{R}^d$ of n lines. A pyramid in $\mathcal{L}$ is an intersection point of d lines from $\mathcal{L}$ whose directions are linearly independent. In other words, it is a point $a \in \mathbb{R}^d$ such that there are linearly independent vectors $v_1, \ldots, v_d \in \mathbb{R}^d$ with $L_{a,v_i} \in \mathcal{L}$, for all $1 \leq i \leq d$. Given $\mathcal{L}$ we denote by P the set of all pyramids in $\mathcal{L}$.[1]

(a) Consider the d dimensional grid with side $s = m^{\frac{1}{d-1}}$. Namely, consider all axis parallel lines with starting point $a \in [s]^d$. Show that this is a set of $n = md$ lines with $\Omega_d(n^{\frac{d}{d-1}})$ pyramids.[2]

We now prove that this lower bound is tight. I.e., that we cannot have an arrangement with considerably more pyramids. It is recommended to use the following guiding steps:

(b) Show that we can assume that each line in $\mathcal{L}$ passes through at least $|P|/2n$ points of P. I.e., show that if we prove the statement for this case then the general case also follows ($|P| = O_d(n^{d/(d-1)})$).

Let $e = \lfloor \frac{|P|}{2n} \rfloor$.

(c) Show that if we prove that $|P| \geq \binom{e+d}{d}$, then $|P| = O_d(n^{\frac{d}{d-1}})$.

We now show that indeed $|P| \geq \binom{e+d}{d}$. Assume for a contradiction that $|P| < \binom{e+d}{d}$. Let $g \in \mathbb{R}[x_1, ..., x_d]$ be a non zero polynomial, which has minimal degree among all polynomials that vanish on P.

(c) Show that $\deg(g) \leq e$.

Denote

$$\nabla g(y) = \left(\frac{\partial g}{\partial x_1}(y), ..., \frac{\partial g}{\partial x_d}(y) \right).$$

(d) Show that $\nabla g \equiv 0$ if and only if g is constant.

Let $a \in P$ be a pyramid and let $v_1, ..., v_d$ be d linearly independent directions of lines from $\mathcal{L}$ that pass through a. Consider $h_i(t) = g(a + tv_i)$.

(e) Show that h_i is identically zero.

(f) Show that the coefficient of the term t in h_i is $\langle \nabla g(a), v_i \rangle$.

(g) Show that one of the partial derivative of g is a non zero polynomial that vanishes on P. Conclude that $|P| \geq \binom{e+d}{d}$.

[1] In this question you should think of d as being relatively small and of m, n as going to infinity.

[2] We use the notation $\Omega_d()$ and $O_d()$ to mean that the constant may depend on the parameter d.