609 Final Exam

Enrique Areyan
April 30, 2013

(15.1) Let $G = (V, E)$ and $S \subseteq V$. Suppose that G is an (n, d, c)-expander. By definition $|\Gamma(S)| \geq c|S|$ for all S with $|S| \leq n/2$, where $|\Gamma(S)|$ denote the set of all proper neighbors of S. In what follows, let $S \subseteq V$ be such that $|S| \leq n/2$. Consider also the following definitions:
A unique neighbor of S is a vertex in $\Gamma(S)$ connected by an edge to only one vertex in S.
Let $U \subseteq \Gamma(S)$ denote the set of unique neighbors of S and $T \subseteq \Gamma(S)$ the set of non-unique neighbors of S.
Let us count in two ways the number of edges between S and T. Denote this number by $EBST$.

(i) $EBST \leq d|S|$, since G is a d-regular graph, so in the worst case all edges in S come from to T.

(ii) $EBST \geq 2|T|$, since each member of T contributes at least 2 edges between S and T.

Therefore, $d|S| \geq EBST \geq 2|T|$. However, the neighbors of S can be partitioned as follow: $\Gamma(S) = U \cup T$. Since $U \cap T = \emptyset$, we know that $|\Gamma(S)| = |U| + |T| \iff |T| = |\Gamma(S)| - |U|$. Replacing $|T|$ in the above inequality we get:

$$d|S| \geq EBST \geq 2(|\Gamma(S)| - |U|)$$

But G is an (n, d, c)-expander, which in particular means that $|\Gamma(S)| \geq c|S|$. Thus,

$$d|S| \geq EBST \geq 2(|\Gamma(S)| - |U|) \geq 2(c|S| - |U|)$$

$$\Rightarrow d|S| \geq 2(c|S| - |U|) \Rightarrow d/2|S| \geq c|S| - |U|$$

$$\iff |U| \geq (c - d/2)|S|$$

$\square$

(15.2) Let A be a square symmetric matrix, λ one of its eigenvalues and x an eigenvector associated with λ. Consider the following statement:

$$S(n) : A^n x = \lambda^n x$$

We want to show that $S(n)$ holds for every $n \in \mathbb{N}$. The proof is by induction.

Base Case: $S(0)$ is true since: $A^0 x = Ix = x = 1 \cdot x = \lambda^0 x$.

Inductive Step: Suppose that $S(n)$ is true for $n \geq 0$. To prove $S(n+1)$ we proceed as follow:

$$\begin{array}{rcll} A^{n+1}x & = & A(A^n x) & \text{By power rule for square matrices and associativity} \\ & = & A(\lambda^n x) & \text{By inductive hypothesis} \\ & = & \lambda^n (Ax) & \text{By linearity of } A \\ & = & \lambda^n (\lambda x) & \text{Since } x \text{ is an eigenvector with eigenvalue } \lambda \\ & = & \lambda^{n+1} x & \text{Power rule} \end{array}$$

Hence, the statement $S(n+1) : A^{n+1}x = \lambda^{n+1}x$ is true, which shows the result. $\square$

(15.4) Let G be a bipartite d-regular graph on n vertices with parts of size p and q with $p + q = n$. Let A be adjacency matrix of G. Then A has the following structure:

$$A = \begin{bmatrix} \mathbf{0} & B \\ B^T & \mathbf{0} \end{bmatrix}$$

where B is a $p \times q$ matrix. Note that since G is d-regular, each row and column of B has exactly d many ones.

Claim: both d and $-d$ are eigenvalues for A with eigenvectors $(1, \cdots, 1)$ and $(1, \cdots, 1, -1, \cdots, -1)$ (p many ones and q many minus ones), respectively.

Proof: the proof follows from the definition of eigenvalues/eigenvectors, i.e. α is an eigenvalue of A if and only if $A\alpha = \alpha x$ for some vector $x \in \mathbb{F}^n$. Let $x = (1, \cdots, 1)$. Then:

$$\begin{aligned}
Ax &= \begin{bmatrix} \mathbf{0} & B \\ B^T & \mathbf{0} \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} && \text{By definition of } A \text{ and } x \\
&= \begin{bmatrix} d \\ \vdots \\ d \end{bmatrix} && \text{Since } B \text{ has exactly } d \text{ ones in each row and column} \\
&= d \begin{bmatrix} 1 \\ \vdots \\ 1 \end{bmatrix} && \text{Factoring } d \text{ out} \\
&= dx && \text{By definition of } x
\end{aligned}$$

Hence, $(1, \cdots, 1)$ is an eigenvector with eigenvalue d. Likewise, let x now be $(1, \cdots, 1, -1, \cdots, -1)$. Then:

$$\begin{aligned}
Ax &= \begin{bmatrix} \mathbf{0} & B \\ B^T & \mathbf{0} \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ 1 \\ -1 \\ \vdots \\ -1 \end{bmatrix} && \text{By definition of } A \text{ and } x \\
&= \begin{bmatrix} -d \\ \vdots \\ -d \\ d \\ \vdots \\ d \end{bmatrix} && \text{Since } B \text{ has exactly } d \text{ ones in each row and column} \\
&= -d \begin{bmatrix} 1 \\ \vdots \\ 1 \\ -1 \\ \vdots \\ -1 \end{bmatrix} && \text{Factoring } -d \text{ out} \\
&= -dx && \text{By definition of } x
\end{aligned}$$

Hence, $(1, \cdots, 1, -1, \cdots, -1)$ is an eigenvector with eigenvalue $-d$. $\square$

(13.2) Let $x \in \mathbb{F}_2^n$ be such that $x \neq \vec{0}$. Following the hint, let us fix an i with $0 \leq i \leq n$ such that $x_i = 1$. Now, partition $\mathbb{F}_2^n$ by defining the set $\mathcal{X} := \{(y, y') \in \mathbb{F}_2^n \times \mathbb{F}_2^n \mid y \text{ and } y' \text{ differ only in their } i\text{-th coordinate}\}$. First note that $\mathcal{X}$ covers $\mathbb{F}_2^n$, i.e., $\bigcup\limits_{(y,y') \in \mathcal{X}} \{y\} \cup \{y'\} = \mathbb{F}_2^n$. Since any vector belongs to only one pair it follows that $|\mathcal{X}| = |\mathbb{F}_2^n|/2$.

Finally, note that by the construction of $\mathcal{X}$, we know that for each of its pairs: $\langle x, y\rangle \neq \langle x, y'\rangle$ since y, y' differ only in the i-th coordinate. Therefore, if $\langle x, y\rangle = 0$, then $\langle x, y'\rangle = 1$. If, on the contrary $\langle x, y\rangle = 1$, then $\langle x, y'\rangle = 0$. In any case, for each pair (y, y') the vector x is orthogonal to either y or y' but not both. By the previous argument about the cardinality of $\mathcal{X}$, it follows that x is orthogonal to half of vectors in $\mathbb{F}_2^n$. $\square$

(13.9) Let $n \in \mathbb{N}$. Define the set $\mathcal{F}_n := \{f \in \mathbb{F}_2[x_1, \cdots, x_n] : d = deg(f) < n, f \not\equiv 1\}$. From this set, define the following $\mathcal{V}_d := \{v \in \mathbb{F}_2^n : v \neq 0, \text{ with at most } d+1 \text{ ones}\}$. Now, consider the following statement:

$$S(n) := \ \forall f \in \mathcal{F}_n / \exists v \in \mathcal{V}_d : f(v) = 0$$

We want to show that $S(n)$ holds for every $n \in \mathbb{N}$. The proof is by induction.

Base Case:

$S(0)$ is vacuously true since there are no polynomials of degree less than zero.

$S(1)$ is true since the only possible polynomials of degree less than 1 are: $f(x_1) = 0$ or $f(x_1) = 1$. However, we do not admit the case when $f \equiv 1$, so the only possibility is that $f(x_1) = 0$. Obviously, there exists $x_1 \in \mathcal{V}_0$ such that $f(x_1) = 0$. Take either $x_1 = 0$ or $x_1 = 1$. Both have at most $d + 1 = 0 + 1 = 1$ one.

Inductive Step: Suppose that $S(n)$ is true for $n \geq 0$. To prove $S(n+1)$ we proceed as follow:

Let $f \in \mathcal{F}_{n+1}$. We can factor f into two parts as follow:

$$f(x_1, \cdots, x_{n+1}) = f_0(x_1, \cdots, x_n)x_{n+1} + f_1(x_1, \cdots, x_n)$$

where $f_0, f_1 \in \mathcal{F}_n$. Essentially, we have factor the polynomial f in $n+1$ variables as a sum of a polynomial in the variable x_{n+1} whose coefficient is a polynomial in n variables and the rest that does not depend on x_{n+1}. (For example, the polynomial $f(x_1, x_2, x_3) = x_1x_2x_3 + x_1x_3 + x_2 = (x_1x_2 + x_1)x_3 + x_2$, in this case $f_0(x_1, x_2) = x_1x_2 + x_1$ and $f_1(x_1, x_2) = x_2$. Note that since we are working in $\mathbb{F}_2$, each monomial has at most one occurrence of each variable). Now, for f it might be that $f_1 \equiv 0$ or not, i.e., each monomial in f might have x_{n+1} or not. Let us handle these two cases separately:

If $f_1 \equiv 0$, then $f(x_1, \cdots, x_{n+1}) = f_0(x_1, \cdots, x_n)x_{n+1}$.
In this case, by inductive hypothesis, there exists $(x_1, \cdots, x_n) \in \mathcal{V}_n$ such that $f_0(x_1, \cdots, x_n) = 0$. Add a final coordinate to this vector with a zero or a one, i.e., $(x_1, \cdots, x_n, 0/1) \in \mathcal{V}_{n+1}$ and we have that $f(x_1, \cdots, x_{n+1}) = f_0(x_1, \cdots, x_n)x_{n+1} = 0 \cdot 0/1 = 0$. So, in either case we obtain the result. Note that in the case where we add a one, $(x_1, \cdots, x_n, 1)$, we have at most $d+2$ ones where $d = deg(f_0)$ so we are still in $\mathcal{V}_{n+1}$ since the degree of f is one more than the degree of f_0.

If $f_1 \not\equiv 0$ then, by inductive hypothesis, there exists $(x_1, \cdots, x_n) \in \mathcal{V}_n$ such that $f_1(x_1, \cdots, x_n) = 0$. In this case, augment this vector by adding a final zero coordinate: $(x_1, \cdots, x_n, 0) \in \mathcal{V}_{n+1}$ to obtain the desired vector: $f(x_1, \cdots, x_n, 0) = f_0(x_1, \cdots, x_n)0 + f_1(x_1, \cdots, x_n) = 0 + 0 = 0$. We do not add ones to this vector, so we can conclude that $(x_1, \cdots, x_n, 0) \in \mathcal{V}_{n+1}$ since $(x_1, \cdots, x_n) \in \mathcal{V}_n$.

In any case we have show that there exists $(x_1, \cdots, x_n, x_{n+1}) \in \mathcal{V}_d$ such that $f(x_1, \cdots, x_n, x_{n+1}) = 0$. $\square$

(13.17) Let $A_1, \cdots, A_m$ be a k-uniform, L-intersecting family of subsets of an n-element set. WLOG, suppose that $L = \{l_1, \cdots, l_s\}$.
For A_i with $i = 1, \cdots, m$ let us define the polynomial f_i in n variables by:

$$f_i(x) = \prod_{k:\ l_k < |A_i|} (< v_i, x > - l_k), \quad \text{where } x \in \mathbb{R}^n$$

and, $A_i \mapsto v_i = (v_{i1}, \cdots, v_{in})$, where $v_{ij} = 1$ if $j \in A_i$, otherwise $v_{ij} = 0$.
Observe that $f_i(v_j) = 0$ for all $1 \leq j < i \leq m$, since the dot product of v_i with x will kill all x_i such that i does not appear in A_i and leave all others such that when v_j is replaced, the sum will equal l_k and thus $l_k - l_k = 0$. Likewise, $f_i(v_i) \neq 0$ for all $1 \leq i \leq m$, since the number generated by the dot product will be greater than l_k. It follows from lemma 13.11 that the polynomials $f_1, \cdots, f_m$ are linearly independent over $\mathbb{R}$. Note that $deg(f_i) \leq s$ for all $i = 1, \cdots, m$ since the maximum intersection size between two sets is l_s.

Now, associate with each subset I of $\{1, \cdots, n\}$ of cardinallity $|I| \leq s - 1$, the following polynomial of degree at most s:

$$g_I(x) = ((\sum_{j=1}^{n} x_j) - k) \prod_{i \in I} x_i$$

Observe that for any subset $S \subseteq \{1, \cdots, n\}$:

$$g_I(S) \neq 0 \iff |S| \neq k \text{ and } I \subseteq S$$

<u>Remark:</u> We can state our goal at this point. We want to show that the set $\{f_1, \cdots, f_m\} \cup \{g_{I1}, \cdots, g_{It}\}$ is a linearly independent set and use the Linear Algebra bound in which if a set of cardinality m is linearly independent in V and $dim(V) = n$ then $m \leq n$. By theorem 13.13 we know the f_i polynomials lie in the span of $\sum_{i=0}^{s} \binom{n}{i}$ many multilinear monomials. Also, since the degree of each g_j is at most s, these polynomials also lie in the same span. But there are $\sum_{i=0}^{s-1} \binom{n}{i}$ many g_j polynomials. Therefore, if the combination of f and g form a linearly independent set we get the whole space, from which we can conclude that $m \leq \binom{n}{s}$, since a basis for this space is the combination of $\binom{n}{s}$ monomials. (end of <u>remark</u>)

Now, all that remains is filling in the details for the proof that the set $\{f_1, \cdots, f_m\} \cup \{g_{I1}, \cdots, g_{It}\}$ is a linearly independent. For this, take a linear combination and assume that is equal to zero:

$$\sum_{i=1}^{m} \lambda_i f_i + \sum_{|I| \leq s-1} \mu_I g_I = 0, \qquad \text{for some } \lambda_i, \mu_I \in \mathbb{R}$$

On the one hand, if we substitute any A_j for the variables in this equation, all the g_I's will vanish since by definition of $g_I(A_j) \neq 0 \iff |A_i| \neq k$ and $I \subseteq A_j$, but A_j belongs to a k-uniform family and hence $|A_j| = k$ for any j, which means that $g_I(A_j) = 0$. On the other, if we substitute $f_i(A_j)$ such that $i \neq j$ then $f_i(A_j) \neq 0$. Therefore $\lambda_j = 0$ for every $j = 1, \cdots, m$.
What remains is a relation among the g_I. To show that this relation must be also trivial, assume the opposite and re-write this relation as:

$$\mu_{I_1} g_{I_1} + \mu_{I_2} g_{I_2} + \cdots + \mu_{I_t} g_{I_t} = 0$$

with all $\mu_i \neq 0$ and $|I_1| \geq |I_j|$ for all $j > 1$. Substitue the first set I_1 for the variables:

$$\mu_{I_1} g_{I_1}(I_1) + \mu_{I_2} g_{I_2}(I_1) + \cdots + \mu_{I_t} g_{I_t}(I_1) = 0$$

Since $I_j \not\subseteq I_1$ it follows that $g_{I_i}(I_1) = 0$ for all but the first function. In fact, the only function that does not vanishes is g_{I_1}, so we are left with

$$\mu_{I_1} g_{I_1}(I_1) = 0 \iff g_{I_1}(I_1) = 0 \quad \text{since we assumed } \mu_i \neq 0$$

But, $I_1 \subseteq I_1$. Hence, by definition of g_{I_1} it must be that $|I_1| = k$. But I_1 is the biggest I so it follow that $|I_1| = s - 1 = k \iff s = k + 1$. But $|L| = s = k + 1$, but how can you have an intersection of two k-sets giving you a set with $k + 1$ elements? This is the contradiction we wanted so it follows that the relation among the g's is also trivial. This shows that the set $\{f_1, \cdots, f_m\} \cup \{g_{I1}, \cdots, g_{It}\}$ is a linearly independent and the result follows as explained in the above remark. $\square$