Chapter 30

Expanders II

By Sariel Har-Peled, December 30, 2015[①]

> Be that as it may, it is to night school that I owe what education I possess; I am the first to own that it doesn't amount to much, though there is something rather grandiose about the gaps in it.
>
> – Gunter Grass, The tin drum.

30.1. Bi-tension

Our construction of good expanders, would use the idea of composing graphs together. To this end, in our analysis, we will need the notion of bi-tension. Let $\widetilde{\mathsf{E}}(\mathsf{G})$ be the set of *directed* edges of G; that is, every edge $xy \in E(\mathsf{G})$ appears twice as $(x \to y)$ and $(y \to x)$ in $\widetilde{\mathsf{E}}$.

Definition 30.1.1. For a graph G, let $\gamma_2(\mathsf{G})$ denote the *bi-tension* of G; that is, the smallest constant, such that for any two function $f, g : V(\mathsf{G}) \to \mathbb{R}$, we have that

$$\mathop{\mathbf{E}}_{x,y\in V}\left[|f(x)-g(y)|^2\right] \le \gamma_2(\mathsf{G}) \mathop{\mathbf{E}}_{(x\to y)\in\widetilde{\mathsf{E}}}\left[|f(x)-g(y)|^2\right]. \tag{30.1}$$

The proof of the following lemma is similar to the proof of Lemma 30.3.1. The proof is provided for the sake of completeness, but there is little new in it.

Lemma 30.1.2. *Let $\mathsf{G} = (V, E)$ be a connected d-regular graph with n vertices. Then $\gamma_2(\mathsf{G}) = \dfrac{1}{1-\widehat{\lambda}}$, where $\widehat{\lambda} = \widehat{\lambda}(\mathsf{G})$, where $\widehat{\lambda}(\mathsf{G}) = \max\left(\widehat{\lambda}_2, -\widehat{\lambda}_n\right)$, where $\widehat{\lambda}_i$ is the ith largest eigenvalue of the random walk matrix associated with G.*

Proof: We can assume that $\mathbf{E}[f(x)] = 0$. As such, we have that

$$\mathop{\mathbf{E}}_{x,y\in V}\left[|f(x)-g(y)|^2\right] = \mathop{\mathbf{E}}_{x,y\in V}\left[(f(x))^2\right] - 2\mathop{\mathbf{E}}_{x,y\in V}[f(x)g(y)] + \mathop{\mathbf{E}}_{y\in V}\left[(g(y))^2\right] = \mathop{\mathbf{E}}_{x,y\in V}\left[(f(x))^2\right] + \mathop{\mathbf{E}}_{y\in V}\left[(g(y))^2\right]. \tag{30.2}$$

Let Q be the matrix associated with the random walk on G (each entry is either zero or $1/d$), we have

$$\begin{aligned}\rho = \mathop{\mathbf{E}}_{(x\to y)\in\widetilde{\mathsf{E}}}\left[|f(x)-g(y)|^2\right] &= \frac{1}{nd}\sum_{(x\to y)\in\widetilde{\mathsf{E}}}(f(x)-g(y))^2 = \frac{1}{n}\sum_{x,y\in V}\mathsf{Q}_{xy}(f(x)-g(y))^2 \\ &= \frac{1}{n}\sum_{x\in V}\Big((f(x))^2+(g(x))^2\Big) - \frac{2}{n}\sum_{x,y\in V}\mathsf{Q}_{xy}f(x)g(y).\end{aligned}$$

Let $\mathcal{B}(\mathsf{Q}) = \langle v_1,\ldots,v_n\rangle$ be the orthonormal eigenvector basis defined by Q (see Definition 30.3.3), with eigenvalues $\widehat{\lambda_1}\geq\widehat{\lambda_2}\geq\cdots\geq\widehat{\lambda_n}$, respectively. Write $f=\sum_{i=1}^n\alpha_i v_i$ and $g=\sum_{i=1}^n\beta_i v_i$. Since $\mathbf{E}[f(x)]=0$, we have that $\alpha_1=0$. Now, $\mathsf{Q}_{xy}=\mathsf{Q}_{yx}$, and we have

$$\begin{aligned}\sum_{x,y\in V}\mathsf{Q}_{xy}f(x)g(y) &= \sum_{x,y\in V}\mathsf{Q}_{yx}\left(\sum_i\alpha_i v_i(x)\right)\left(\sum_j\beta_j v_j(y)\right) = \sum_{i,j}\alpha_i\beta_j\sum_{y\in V}v_j(y)\sum_{x\in V}\mathsf{Q}_{yx}v_i(x) \\ &= \sum_{i,j}\alpha_i\beta_j\sum_{y\in V}v_j(y)\Big(\widehat{\lambda_i}v_i(y)\Big) = \sum_{i,j}\alpha_i\beta_j\widehat{\lambda_i}\left\langle v_j,v_i\right\rangle = \sum_{i=2}^n\alpha_i\beta_i\widehat{\lambda_i}\sum_{y\in V}(v_i(y))^2 \\ &\leq \widehat{\lambda}\sum_{i=2}^n\frac{\alpha_i^2+\beta_i^2}{2}\sum_{y\in V}(v_i(y))^2 \leq \frac{\widehat{\lambda}}{2}\sum_{i=1}^n\sum_{y\in V}\Big((\alpha_i v_i(y))^2+(\beta_i v_i(y))^2\Big) \\ &= \frac{\widehat{\lambda}}{2}\sum_{y\in V}\Big((f(y))^2+(g(y))^2\Big)\end{aligned}$$

As such,

$$\begin{aligned}\mathop{\mathbf{E}}_{(x\to y)\in\widetilde{\mathsf{E}}}\left[|f(x)-g(y)|^2\right] &= \frac{1}{nd}\sum_{(x\to y)\in\widetilde{\mathsf{E}}}|f(x)-g(y)|^2 = \frac{1}{n}\sum_{y\in V}\Big((f(y))^2+(g(y))^2\Big) - \frac{1}{n}\sum_{x,y\in V}\frac{2f(x)g(y)}{d} \\ &= \frac{1}{n}\sum_{y\in V}\Big((f(y))^2+(g(y))^2\Big) - \frac{2}{n}\sum_{x,y\in V}\mathsf{Q}_{xy}f(x)g(y) \\ &\geq \left(\frac{1}{n}-\frac{2}{n}\cdot\frac{\widehat{\lambda}}{2}\right)\sum_{y\in V}\Big((f(y))^2+(g(y))^2\Big) = \Big(1-\widehat{\lambda}\Big)\left(\mathop{\mathbf{E}}_{y\in V}\Big[(f(y))^2\Big]+\mathop{\mathbf{E}}_{y\in V}\Big[(g(y))^2\Big]\right) \\ &= \Big(1-\widehat{\lambda}\Big)\mathop{\mathbf{E}}_{x,y\in V}\Big[|f(x)-g(y)|^2\Big],\end{aligned}$$

by Eq. (30.2). This implies that $\gamma_2(\mathsf{G})\leq 1/\Big(1-\widehat{\lambda}\Big)$. Again, by trying either $f=g=v_2$ or $f=v_n$ and $g=-v_n$, we get that the inequality above holds with equality, which implies $\gamma_2(\mathsf{G})\geq 1/\Big(1-\widehat{\lambda}\Big)$. Together, the claim now follows. ■

30.2. Explicit construction

For a set $U\subseteq V$ of vertices, its *characteristic vector*, denoted by $x=\chi_U$, is the n dimensional vector, where $x_i=1$ if and only if $i\in U$.

The following is an easy consequence of Lemma 30.3.2.

Lemma 30.2.1. *For a d-regular graph G the vector $\mathbf{1}^n=(1,1,\ldots,1)$ is the only eigenvector with eigenvalue d (of the adjacency matrix $\mathsf{M}(\mathsf{G})$), if and only if G is connected. Furthermore, we have $|\lambda_i|\leq d$, for all i.*

Our main interest would be in the second largest eigenvalue of M. Formally, let

$$\lambda_2(\mathsf{G}) = \max_{x \perp \mathbf{1}^n, x \neq 0} \left| \frac{\langle x\mathsf{M}, x \rangle}{\langle x, x \rangle} \right|.$$

We state the following result but do not prove it since we do not need it for our nafarious purposes (however, we did prove the left side of the inequality).

Theorem 30.2.2. *Let G be a δ-expander with adjacency matrix M and let $\lambda_2 = \lambda_2(\mathsf{G})$ be the second-largest eigenvalue of M. Then*

$$\frac{1}{2}\left(1 - \frac{\lambda_2}{d}\right) \leq \delta \leq \sqrt{2\left(1 - \frac{\lambda_2}{d}\right)}.$$

What the above theorem says, is that the expansion of a $[n, d, \delta]$-expander is a function of how far is its second eigenvalue (i.e., λ_2) from its first eigenvalue (i.e., d). This is usually referred to as the *spectral gap*.

We will start by explicitly constructing an expander that has "many" edges, and then we will show to reduce its degree till it become a constant degree expander.

30.2.1. Explicit construction of a small expander

30.2.1.1. A quicky reminder of fields

A *field* is a set $\mathbb{F}$ together with two operations, called addition and multiplication, and denoted by $+$ and $\cdot$, respectively, such that the following axioms hold:

(i) Closure: $\forall x, y \in \mathbb{F}$, we have $x + y \in \mathbb{F}$ and $x \cdot y \in \mathbb{F}$.

(ii) Associativity: $\forall x, y, z \in \mathbb{F}$, we have $x + (y + z) = (x + y) + z$ and $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(iii) Commutativity: $\forall x, y \in \mathbb{F}$, we have $x + y = y + x$ and $x \cdot y = y \cdot x$.

(iv) Identity: There exists two distinct special elements $0, 1 \in \mathbb{F}$. We have that $\forall x \in \mathbb{F}$ it holds $x + 0 = a$ and $x \cdot 1 = x$.

(v) Inverse: There exists two distinct special elements $0, 1 \in \mathbb{F}$, and we have that $\forall x \in \mathbb{F}$ there exists an element $-x \in \mathbb{F}$, such that $x + (-x) = 0$.

Similarly, $\forall x \in \mathbb{F}$, $x \neq 0$, there exists an element $y = x^{-1} = 1/x \in \mathbb{F}$ such that $x \cdot y = 1$.

(vi) Distributivity: $\forall x, y, z \in \mathbb{F}$ we have $x \cdot (y + z) = x \cdot y + x \cdot z$.

Let $q = 2^t$, and $r > 0$ be an integer. Consider the finite field $\mathbb{F}_q$. It is the field of polynomials of degree at most $t - 1$, where the coefficients are over $\mathbb{Z}_2$ (i.e., all calculations are done modulus 2). Formally, consider the polynomial

$$p(x) = x^t + x + 1.$$

It it irreducible over $\mathbb{F}_2 = \{0, 1\}$ (i.e., $p(0) = p(1) \neq 0$). We can now do polynomial arithmetic over polynomials (with coefficients from $\mathbb{F}_2$), where we do the calculations modulus $p(x)$. Note, that any irreducible polynomial of degree n yields the same field up to isomorphism. Intuitively, we are introducing the n distinct roots of $p(x)$ into $\mathbb{F}$ by creating an extension field of $\mathbb{F}$ with those roots.

An element of $\mathbb{F}_q = \mathbb{F}_{2^t}$ can be interpreted as a binary string $b = b_0 b_1 \ldots, b_{t-1}$ of length t, where the corresponding polynomial is

$$\mathrm{poly}(b) = \sum_{i=0}^{t-1} b_i x^i.$$

The nice property of $\mathbb{F}_q$ is that addition can be interpreted as a `xor` operation. That is, for any $x, y \in \mathbb{F}_q$, we have that $x + y + y = x$ and $x - y - y = x$. The key properties of $\mathbb{F}_q$ we need is that multiplications and addition can be computed in it in polynomial time in t, and it is a field (i.e., each non-zero element has a unique inverse).

30.2.1.1.1. Computing multiplication in $\mathbb{F}_q$. Consider two elements $\alpha, \beta \in \mathbb{F}_q$. Multiply the two polynomials $\mathrm{poly}(\alpha)$ by $\mathrm{poly}(\beta)$, let $\mathrm{poly}(\gamma)$ be the resulting polynomial (of degree at most $2t-2$), and compute the remainder $\mathrm{poly}(\beta)$ when dividing it by the irreducible polynomial $p(x)$. For this remainder polynomial, normalize the coefficients by computing their modules base 2. The resulting polynomial is the product of α and β.

For more details on this field, see any standard text on abstract algebra.

30.2.1.2. The construction

Let $q = 2^t$, and $r > 0$ be an integer. Consider the linear space $\mathbb{G} = \mathbb{F}_q^r$. Here, a member $\alpha = (\alpha_0, \ldots, \alpha_r) \in \mathbb{G}$ can be thought of as being a string (of length $r+1$) over $\mathbb{F}_q$, or alternatively, as a binary string of length $n = t(r+1)$.

For $\alpha = (\alpha_0, \ldots, \alpha_r) \in \mathbb{G}$, and $x, y \in \mathbb{F}_q$, define the operator

$$\rho(\alpha, x, y) = \alpha + y \cdot \left(1, x, x^2, \ldots, x^r\right) = \left(\alpha_0 + y, \alpha_1 + yx, \alpha_2 + yx^2, \ldots, \alpha_r + yx^r\right) \in \mathbb{G}.$$

Since addition over $\mathbb{F}_q$ is equivalent to a xor operation we have that

$$\begin{aligned}\rho(\rho(\alpha, x, y), x, y) &= \left(\alpha_0 + y + y, \alpha_1 + yx + yx, \alpha_2 + yx^2 + yx^2, \ldots, \alpha_r + yx^r + yx^r\right) \\ &= (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_r) = \alpha.\end{aligned}$$

Furthermore, if $(x, y) \neq (x', y')$ then $\rho(\alpha, x, y) \neq \rho(\alpha, x', y')$.

We now define a graph $\mathsf{LD}(q, r) = (\mathbb{G}, E)$, where

$$E = \left\{ \alpha\beta \;\middle|\; \begin{array}{l} \alpha \in \mathbb{G}, x, y \in \mathbb{F}_q \\ \beta = \rho(\alpha, x, y) \end{array} \right\}$$

Note, that this graph is well defined, as $\rho(\beta, x, y) = \alpha$. The degree of a vertex of $\mathsf{LD}(q, r)$ is $\left|\mathbb{F}_q\right|^2 = q^2$, and $\mathsf{LD}(q, r)$ has $N = |\mathbb{G}| = q^{r+1} = 2^{t(r+1)} = 2^n$ vertices.

Theorem 30.2.3. *For any $t > 0, r > 0$ and $q = 2^t$, where $r < q$, we have that $\mathsf{LD}(q, r)$ is a graph with q^{r+1} vertices. Furthermore, $\lambda_1(\mathsf{LD}(q, r)) = q^2$, and $\lambda_i(\mathsf{LD}(q, r)) \leq rq$, for $i = 2, \ldots, n$.*

In particular, if $r \leq q/2$, then $\mathsf{LD}(q, r)$ is a $\left[q^{r+1}, q^2, \frac{1}{4}\right]$-expander.

Proof: Let M be the $N \times N$ adjacency matrix of $\mathsf{LD}(q, r)$. Let $L : \mathbb{F}_q \to \{0, 1\}$ be a linear map which is onto. It is easy to verify that $\left|L^{-1}(0)\right| = \left|L^{-1}(1)\right|$[2]

We are interested in the eigenvalues of the matrix M. To this end, we consider vectors in $\mathbb{R}^N$. The ith row an ith column of M is associated with a unique element $b_i \in \mathbb{G}$. As such, for a vector $v \in \mathbb{R}^N$, we denote by

[2] Indeed, if $Z = L^{-1}(0)$, and $L(x) = 1$, then $L(y) = 1$, for all $y \in U = \left\{x + z \;\middle|\; z \in Z\right\}$. Now, its clear that $|Z| = |U|$.

$v[b_i]$ the ith coordinate of v. In particular, for $\alpha = (\alpha_0, \ldots, \alpha_r) \in \mathbb{G}$, let $v_\alpha \in \mathbb{R}^N$ denote the vector, where its $\beta = (\beta_0, \ldots, \beta_r) \in \mathbb{G}$ coordinate is

$$v_\alpha[\beta] = (-1)^{L\left(\sum_{i=0}^{r} \alpha_i \beta_i\right)}.$$

Let $V = \left\{ v_\alpha \;\middle|\; \alpha \in \mathbb{G} \right\}$. For $\alpha \neq \alpha' \in V$, observe that

$$\langle v_\alpha, v_{\alpha'} \rangle = \sum_{\beta \in \mathbb{G}} (-1)^{L\left(\sum_{i=0}^{r} \alpha_i \beta_i\right)} \cdot (-1)^{L\left(\sum_{i=0}^{r} \alpha'_i \beta_i\right)} = \sum_{\beta \in \mathbb{G}} (-1)^{L\left(\sum_{i=0}^{r} \left(\alpha_i + \alpha'_i\right) \beta_i\right)} = \sum_{\beta \in \mathbb{G}} v_{\alpha+\alpha'}[\beta] \,.$$

So, consider $\psi = \alpha + \alpha' \neq 0$. Assume, for the simplicity of exposition that all the coordinates of ψ are non-zero. We have, by the linearity of L that

$$\langle v_\alpha, v_{\alpha'} \rangle = \sum_{\beta \in \mathbb{G}} (-1)^{L\left(\sum_{i=0}^{r} \alpha_i \beta_i\right)} = \sum_{\beta_0 \in \mathbb{F}_q, \ldots, \beta_{r-1} \in \mathbb{F}_q} (-1)^{L(\psi_0 \beta_0 + \cdots + \psi_{r-1} \beta_{r-1})} \sum_{\beta_r \in \mathbb{F}_q} (-1)^{L(\psi_r \beta_r)}.$$

However, since $\psi_r \neq 0$, the quantity $\left\{ \psi_r \beta_r \;\middle|\; \beta_r \in \mathbb{F}_q \right\} = \mathbb{F}_q$. Thus, the summation $\sum_{\beta_r \in \mathbb{F}_q} (-1)^{L(\psi_r \beta_r)}$ gets $\left| L^{-1}(0) \right|$ terms that are 1, and $\left| L^{-1}(0) \right|$ terms that are -1. As such, this summation is zero, implying that $\langle v_\alpha, v_{\alpha'} \rangle = 0$. Namely, the vectors of V are orthogonal.

Observe, that for $\alpha, \beta, \psi \in \mathbb{G}$, we have $v_\alpha[\beta + \psi] = v_\alpha[\beta]\, v_\alpha[\psi]$. For $\alpha \in \mathbb{G}$, consider the vector $\mathsf{M} v_\alpha$. We have, for $\beta \in \mathbb{G}$, that

$$\begin{aligned}
(\mathsf{M} v_\alpha)[\beta] = \sum_{\psi \in \mathbb{G}} \mathsf{M}_{\beta\psi} \cdot v_\alpha[\psi] = \sum_{\substack{x,y \,\in\, \mathbb{F}_q \\ \psi = \rho(\beta, x, y)}} v_\alpha[\psi] = \sum_{x,y \,\in\, \mathbb{F}_q} v_\alpha[\beta + y(1, x, \ldots, x^r)] \\
= \left(\sum_{x,y \,\in\, \mathbb{F}_q} v_\alpha[y(1, x, \ldots, x^r)] \right) \cdot v_\alpha[\beta] \,.
\end{aligned}$$

Thus, setting $\lambda(\alpha) = \sum_{x,y \,\in\, \mathbb{F}_q} v_\alpha[y(1, x, \ldots, x^r)] \in \mathbb{R}$, we have that $\mathsf{M} v_\alpha = \lambda(\alpha) \cdot v_\alpha$. Namely, v_α is an eigenvector, with eigenvalue $\lambda(\alpha)$.

Let $p_\alpha(x) = \sum_{i=0}^{r} \alpha_i x^i$, and let

$$\begin{aligned}
\lambda(\alpha) = \sum_{x,y \,\in\, \mathbb{F}_q} v_\alpha[y(1, x, \ldots, x^r)] \in \mathbb{R} = \sum_{x,y \in \mathbb{F}_q} (-1)^{L(y p_\alpha(x))} \\
= \sum_{\substack{x,y \in \mathbb{F}_q \\ p_\alpha(x) = 0}} (-1)^{L(y\ p_\alpha(x))} + \sum_{\substack{x,y \in \mathbb{F}_q \\ p_\alpha(x) \neq 0}} (-1)^{L(y\ p_\alpha(x))}.
\end{aligned}$$

If $p_\alpha(x) = 0$ then $(-1)^{L(y\ p_\alpha(x))} = 1$, for all y. As such, each such x contributes q to $\lambda(\alpha)$.

If $p_\alpha(x) \neq 0$ then $y\ p_\alpha(x)$ takes all the values of $\mathbb{F}_q$, and as such, $L(y\ p_\alpha(x))$ is 0 for half of these values, and 1 for the other half. Implying that these kind terms contribute 0 to $\lambda(\alpha)$. But $p_\alpha(x)$ is a polynomial of degree r, and as such there could be at most r values of x for which the first term is taken. As such, if $\alpha \neq 0$ then $\lambda(\alpha) \leq rq$. If $\alpha = 0$ then $\lambda(\alpha) = q^2$, which implies the theorem. ■

This construction provides an expander with constant degree only if the number of vertices is a constant. Indeed, if we want an expander with constant degree, we have to take q to be as small as possible. We get the relation $n = q^{r+1} \leq q^q$, since $r \leq r$, which implies that $q = \Omega(\log n / \log\log n)$. Now, the expander of Theorem 30.2.3 is q^2-regular, which means that it is not going to provide us with a constant degree expander.

However, we are going to use it as our building block in a construction that would start with this expander and would inflate it up to the desired size.

30.3. From previous lectures

Lemma 30.3.1. *Let* $\mathsf{G} = (V, E)$ *be a given connected* d*-regular graph with* n *vertices. Then* $\gamma(\mathsf{G}) = \frac{1}{1-\widehat{\lambda}_2}$*, where* $\widehat{\lambda}_2 = \lambda_2/d$ *is the second largest eigenvalue of* Q*.*

Lemma 30.3.2. *Let* G *be an undirected graph, and let* Δ *denote the maximum degree in* G*. Then,* $\left|\widehat{\lambda}_1(\mathsf{G})\right| = \left|\widehat{\lambda}_1(\mathsf{M})\right| = \Delta$ *if and only one connected component of* G *is* Δ*-regular. The multiplicity of* Δ *as an eigenvector is the number of* Δ*-regular connected components. Furthermore, we have* $\left|\widehat{\lambda}_i(\mathsf{G})\right| \leq \Delta$*, for all* i*.*

Definition 30.3.3. Given a random walk matrix Q associated with a d-regular graph, let $\mathcal{B}(\mathsf{Q}) = \langle v_1, \ldots, v_n \rangle$ denote the *orthonormal eigenvector basis* defined by Q. That is, $v_1, \ldots, v_n$ is an orthonormal basis for $\mathbb{R}^n$, where all these vectors are eigenvectors of Q and $v_1 = 1^n/\sqrt{n}$. Furthermore, let $\widehat{\lambda}_i$ denote the ith eigenvalue of Q, associated with the eigenvector v_i, such that $\widehat{\lambda}_1 \geq \widehat{\lambda}_2 \geq \cdots \geq \widehat{\lambda}_n$.