Eigenvalues, random walks and Ramanujan graphs

David Ellis

1 The Expander Mixing lemma

We have seen that a bounded-degree graph is a good edge-expander if and only if if has large spectral gap. If $G = (V, E)$ is a d-regular graph, then its Laplacian matrix satisfies

$$L = dI - A,$$

where A is the adjacency matrix of G. Hence, if A has eigenvalues $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$, where $\lambda_1 = d$, then the second smallest eigenvalue of L is given by

$$\mu_2 = d - \lambda_2.$$

As we proved earlier, $\mu_2/2 \leq h(G) \leq \sqrt{2d\mu_2}$ for any graph G with maximum degree at most d, so if G is d-regular, we have

$$\frac{d - \lambda_2}{2} \leq h(G) \leq \sqrt{2d(d - \lambda_2)}.$$

Hence, if λ_2 is small compared to d, then G has high edge-expansion ratio. It turns out that if both λ_2 and $|\lambda_n|$ are small, then G has a stronger property: for any two disjoint subsets $S, T \subset V(G)$, the number of edges of G between S and T is close to the expected number in a random d-regular graph.

Definition. *If $G = (V, E)$ is a d-regular, n-vertex graph, we write*

$$\nu(G) = \max\{\lambda_2, |\lambda_n|\},$$

where $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ are the eigenvalues of the adjacency matrix of G. We call $\nu(G)$ the 'second spectral modulus' of G. (Warning: this is non-standard terminology.)

Observe that $\lambda_2 < d$ if and only if G is connected, and $\lambda_n > -d$ if and only if G is non-bipartite, so $\nu < d$ if and only if G is both connected and non-bipartite. The following result is easy to prove, but is of great importance:

Lemma 1 (Alon's Expander Mixing lemma). *Let $G = (V, E)$ be a d-regular, n-vertex graph, let A be the adjacency matrix of G, and let $d = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ be the eigenvalues of A, repeated with their multiplicities. Let $\nu = \max\{\lambda_2, |\lambda_n|\}$. Then for any two subsets $S, T \subset V(G)$, we have*

$$\left| e(S,T) + e(S \cap T) - \frac{d}{n}|S||T| \right| \leq \nu\sqrt{(|S| - |S|^2/n)(|T| - |T|^2/n)} \leq \nu\sqrt{|S||T|}.$$

If S and T are disjoint, we have

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \leq \nu\sqrt{(|S| - |S|^2/n)(|T| - |T|^2/n)} \leq \nu\sqrt{|S||T|}.$$

Remark. *Note that in a uniform random (labelled) d-regular graph on V, if $S, T \subset V$ are disjoint, then the expected number of edges between S and T is*

$$\frac{d}{n-1}|S||T|.$$

Proof. This is very similar to the proof of Hoffman's theorem, which in fact follows from the $S = T$ case of the first statement above. Let $\mathbf{1} = v_1, v_2, \ldots, v_n$ be an orthonormal basis of eigenvectors corresponding to $d = \lambda_1, \lambda_2, \ldots, \lambda_n$. Express the indicator functions 1_S, 1_T as linear combinations of the v_i's:

$$1_S = \sum_{i=1}^{n} a_i v_i, \quad 1_T = \sum_{i=1}^{n} b_i v_i.$$

Let $\alpha = |S|/n$, and let $\beta = |T|/n$. Note that $a_1 = \langle 1_S, \mathbf{1} \rangle = \alpha$, $b_1 = \langle 1_T, \mathbf{1} \rangle = \beta$, and

$$\sum_{i=1}^{n} a_i^2 = \langle 1_S, 1_S \rangle = \alpha, \quad \sum_{i=1}^{n} b_i^2 = \langle 1_T, 1_T \rangle = \beta.$$

Observe that

$$e(S,T) + e(S \cap T) = \sum_{s \in S,\ t \in T} A_{s,t} = n\langle 1_S, A1_T \rangle = n\sum_{i=1}^{n} \lambda_i a_i b_i$$

and therefore, using the Cauchy-Schwarz inequality,

$$\begin{aligned} |e(S,T) + e(S \cap T) - nd\alpha\beta| &\leq n\sum_{i=2}^{n} \lambda_i a_i b_i \\ &\leq n\nu\sqrt{\sum_{i=2}^{n} a_i^2 \sum_{i=1}^{n} b_i^2} \\ &= n\nu\sqrt{(\alpha - \alpha^2)(\beta - \beta^2)}. \end{aligned}$$

Hence,

$$\left| e(S,T) + e(S \cap T) - \frac{d}{n}|S||T| \right| \leq \nu\sqrt{(|S| - |S|^2/n)(|T| - |T|^2/n)}$$

as required. □

Bilu and Linial [1] proved a partial converse to the Expander Mixing lemma: namely, if $G = (V, E)$ is a d-regular graph such that the number of edges between any two disjoint sets of vertices is 'close' to the expected number in a random d-regular graph on V, then the second spectral modulus of G is small:

Theorem 2 (Bilu, Linial)**.** *Let $G = (V, E)$ be a d-regular, n-vertex graph, and suppose that for any two disjoint sets $S, T \subset V(G)$, we have*

$$\left| e(S,T) - \frac{d}{n}|S||T| \right| \leq \rho\sqrt{|S||T|}. \tag{1}$$

Then

$$\nu(G) \leq C\rho(1 + \log_2(d/\rho)),$$

where C is an absolute constant.

The minimum ρ such that (1) holds is called the *discrepancy* of G. So we see that if d is fixed and relatively large, then for d-regular graphs, small discrepancy is roughly equivalent to small second spectral modulus.

2 Random walks on graphs

It turns out that for d-regular graphs G, $\nu(G)$ determines how fast the simple symmetric random walk on G coverges to the uniform distribution on $V(G)$! Recall the following

Definition. *Let $G = (V, E)$ be a finite graph. Let x_0 be any vertex of G. The* simple symmetric random walk on G starting from x_0 *is the random walk $(X_0, X_1, X_2, \ldots)$ on $V(G)$ defined as follows. At time* 0*, we start at x_0 (i.e., we set $X_0 = x_0$). If at time t, we are at a vertex x_t (i.e., $X_t = x_t$), then at time $t+1$, we jump to a random neighbour y of x, chosen uniformly at random from the set of all neighbours of x in G (i.e., we set $X_{t+1} = y$).*

So for each $x \in V(G)$,

$$\mathbb{P}\{X_{t+1} = y | X_t = x\} = A_{x,y}/d(x) = \begin{cases} 1/d(x) & \text{if } y \in \Gamma(x); \\ 0 & \text{otherwise.} \end{cases}$$

Hence, the random walk $(X_0, X_1, X_2, \ldots)$ is a discrete-time Markov chain with transition matrix P given by

$$P_{x,y} = A_{x,y}/d(x).$$

Of course, we may also choose the starting-vertex from some probability distribution $\mathbf{p}^{(0)}$ on $V(G)$ (meaning that X_0 has distribution $\mathbf{p}^{(0)}$, rather than δ_{x_0}, as above). We let $\mathbf{p}^{(t)}$ denote the probability distribution of X_t. It turns out that if $G = (V, E)$ is a finite, connected, non-bipartite graph with m edges, then starting from *any* initial distribution $\mathbf{p}^{(0)}$, the simple symmetric random walk on G converges to

$$\mu := \left(\frac{d(x)}{2m} \right)_{x \in V}.$$

Formally, $\mathbf{p}^{(t)} \Rightarrow \mu$ as $t \to \infty$, i.e. $p_x^{(t)} \to d(x)/2m$ as $t \to \infty$ for each $x \in V$. For a proof of this fact, see for example [2].

Of course, if G is bipartite, the simple symmetric random walk on G need not converge: if we start at an appropriate vertex, it will be in one part at all even times and in the other at all odd times.

If G is a regular graph, then the distribution μ above is the uniform distribution on $V(G)$. Hence, if G is a regular, connected, non-bipartite graph, then the simple symmetric random walk on G converges to the uniform distribution on $V(G)$. The following theorem shows that $\nu(G)$ controls the rate of this convergence.

Theorem 3. *Let G be a d-regular, n-vertex graph which is connected and non-bipartite, and let $\gamma = \nu(G)/d$. Then for any initial distribution $\mathbf{p}^{(0)}$, the simple symmetric random walk on G satisfies*

$$\sqrt{\sum_{x \in V(G)} (p_x^{(t)} - 1/n)^2} < \gamma^t,$$

so

$$|p_x^{(t)} - 1/n| < \gamma^t \quad \forall x \in V(G).$$

Proof. Note that the transition matrix of the simple symmetric random walk on G is simply

$$P = A/d,$$

where A is the adjacency matrix of G. Moreover, the distribution $\mathbf{p}^{(t)}$ of X_t is given by

$$\mathbf{p}^{(t)} = P^t(\mathbf{p}^{(0)}).$$

Equip $\mathbb{R}^V$ with the inner product

$$\langle f, g \rangle = \frac{1}{n} \sum_{x \in V} f(x)g(x).$$

Let $v_1, v_2, \ldots, v_n$ be an orthonormal basis of eigenvectors of A, with corresponding eigenvalues $d = \lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$; choose v_1 to be the all-1's vector $\mathbf{1}$. The v_i's are also eigenvectors of P^t, with corresponding eigenvalues $\tilde{\lambda}_i := (\lambda_i/d)^t$. Write $\mathbf{p}^{(0)}$ as a linear combination of these eigenvectors:

$$\mathbf{p}_0 = \sum_{i=1}^n a_i v_i.$$

Then

$$a_1 = \langle \mathbf{p}^{(0)}, v_1 \rangle = 1/n,$$

and

$$\sum_{i=1}^n a_i^2 = \langle \mathbf{p}^{(0)}, \mathbf{p}^{(0)} \rangle = \sum_{x \in V} (p_x^{(0)})^2/n \leq 1/n.$$

We have

$$\mathbf{p}_t = P^t(\mathbf{p}^{(0)}) = \sum_{i=1}^n \tilde{\lambda}_i^t a_i v_i = \tfrac{1}{n}\mathbf{1} + \sum_{i=2}^n (\tilde{\lambda}_i)^t a_i v_i.$$

We now estimate the Eucildean norm of the difference between $\mathbf{p}^{(t)}$ and the uniform distribution $\mathbf{u} := \frac{1}{n}\mathbf{1}$. We have

$$||\mathbf{p}^{(t)} - \mathbf{u}||_2 = ||\sum_{i=2}^n \tilde{\lambda}_i^t a_i v_i||_2 \leq \nu^t \sqrt{\sum_{i=2}^n a_i^2} \leq \nu^t \sqrt{1/n - 1/n^2} < \nu^t/\sqrt{n}.$$

In other words,

$$\sqrt{\frac{1}{n}\sum_{x\in V}(p_x^{(t)}-1/n)^2} < \nu^t/\sqrt{n},$$

so

$$\sqrt{\sum_{x\in V}(p_x^{(t)}-1/n)^2} < \nu^t.$$

Therefore,

$$|\mathbf{p}_x^{(t)}-1/n| < \gamma^t$$

for each $x \in V(G)$, as required. $\square$

For two probability distributions $\mathbf{p}$ and $\mathbf{q}$ on V, we write

$$||\mathbf{p}-\mathbf{q}||_{l^2} = \sqrt{\sum_{x\in V}(p_x-q_x)^2}.$$

The previous theorem says that the simple symmetric random walk on a connected, non-bipartite, d-regular graph satisfies

$$||\mathbf{p}^{(t)}-\mathbf{u}||_{l^2} < \gamma^t.$$

We define the *mixing rate* of the simple symmetric random walk on G to be

$$\max\left\{\lim_{t\to\infty}||\mathbf{p}^{(t)}-\mathbf{u}||_{l^2}^{1/t} : \ \mathbf{p}_0=\delta_{x_0} \text{ for some } x_0\in V\right\}.$$

It is easy to see that the mixing rate is equal to γ.

3 Ramanujan graphs

The importance of $\nu(G)$ for d-regular graphs G raises the following question: if $G=(V,E)$ is a d-regular, n-vertex graph, how small can $\nu(G)$ be? We have the following easy result:

Lemma 4. *If G is an n-vertex, d-regular graph, then*

$$\nu(G) \geq \sqrt{d(1-\tfrac{d-1}{n-1})}.$$

Proof. Let A be the adjacency matrix of G. We consider A^2. Note that the eigenvalues of A^2 are $d^2=\lambda_1^2,\lambda_2^2,\ldots,\lambda_n^2$. We have

$$\sum_{i=1}^n \lambda_i^2 = \text{Trace}(A^2) = nd,$$

since the trace of A^2 is simply the number of closed walks of length 2 in G, which is the sum of the degrees of the vertices of G. Hence,

$$d^2+\nu^2(n-1) \geq nd.$$

Rearranging gives the desired bound. $\square$

A more complicated argument proves a sharper bound (which turns out to be asymptotically sharp):

Theorem 5. *Let $G = (V, E)$ be a d-regular graph. Let D be the diameter of G. Then*

$$\nu(G) \geq 2\sqrt{d-1}\left(1 - c\frac{\log D}{D}\right).$$

where c is an absolute constant.

Remark. *In fact, Alon and Boppana proved a stronger statement, namely,*

$$\lambda_2(G) \geq 2\sqrt{d-1}(1 - c'/D^2),$$

where c' is an absolute constant. This was also proved by Friedman slightly later, using a different method.

As we saw earlier, if G is an n-vertex, d-regular graph, then the diameter D of G satisfies

$$D \geq \log_{d-1}(n-1) + \log_{d-1}(1 - 2/d) \geq \Omega_d(\log n).$$

Hence, Theorem 5 implies the following

Corollary 6. *If G is an n-vertex, d-regular graph, then*

$$\nu(G) \geq 2\sqrt{d-1}\left(1 - O_d\left(\frac{\log\log n}{\log n}\right)\right).$$

This is asymptotically sharp: as we will see later, if $d \geq 3$, then almost all d-regular graphs on $[n]$ have

$$\nu(G) \leq 2\sqrt{d-1} + o_d(1).$$

(Here, $o_d(1)$ denotes a function of n and d that tends to zero as $n \to \infty$, for any fixed d.)

Proof of Theorem 5: Let $G = (V, E)$ be as in the statement of the theorem; let A be the adjacency matrix of G. We will bound $\nu = \nu(G)$ from below by considering a high even power of the adjacency matrix, A^{2k}. The eigenvalues of A^{2k} are

$$d^{2k} = \lambda_1^{2k}, \lambda_2^{2k}, \ldots, \lambda_n^{2k}.$$

Observe that

$$\nu^{2k} = \max_{\substack{f \in \mathbb{R}^V:\\ f \perp \mathbf{1}}} \frac{f^\top A^{2k} f}{f^\top f}.$$

We will find a function $f \in \mathbb{R}^V$ whose values sum to zero, such that the 'Rayleigh quotient',

$$\frac{f^\top A^{2k} f}{f^\top f},$$

is large. Choose any two vertices $x, y \in V(G)$ such that $d_G(x, y) = D$; define

$$f(v) = \begin{cases} 1 & \text{if } v = x; \\ -1 & \text{if } v = y; \\ 0 & \text{otherwise.} \end{cases}$$

We then have

$$\frac{f^\top A^{2k} f}{f^\top f} = \frac{(A^{2k})_{x,x} + (A^{2k})_{y,y} - 2(A^{2k})_{x,y}}{2}.$$

Note that for any $v, w \in V(G)$, $(A^{2k})_{v,w}$ is precisely the number of walks in G of length $2k$ from v to w. If we choose k such that $2k < D$, then there are no walks in G of length $2k$ from x to y, so $(A^{2k})_{x,y} = 0$, and we have

$$\frac{f^\top A^{2k} f}{f^\top f} = \frac{(A^{2k})_{x,x} + (A^{2k})_{y,y}}{2}.$$

Note that $(A^{2k})_{v,v}$ is the number of walks in G of length $2k$, starting and ending at v. We claim that for *any* vertex $v \in V(G)$, we have

$$(A^{2k})_{v,v} \geq t_{d,2k},$$

where $t_{d,2k}$ denotes the number of walks of length $2k$ in the *infinite, rooted d-regular tree T_d*, starting and ending at the root vertex v_0. To see this, we first define a graph homomorphism ϕ from T_d to G. Define $\phi(v_0) = v$. Then choose any bijection from the d 'children' of v_0 in T_d to the d neighbours of v in G, and use it to define ϕ on the d children of v_0. Continue iteratively; suppose we have defined $\phi(v_i)$. Choose any bijection from the d 'children' of v_i in T_d to the d neighbours of $\phi(v_i)$ in G, and use it to define ϕ on the d children of v_i in T_d.

Clearly, each closed walk of length $2k$ in T_d, starting and ending at the root vertex v_0, maps under ϕ to a different closed walk in G, starting and ending at v. The claim follows immediately.

It remains to obtain a lower bound for the so-called 'tree numbers' $t_{d,2k}$. In fact, good estimates, a recursion formula, and their generating function are known, but a crude lower bound will suffice for our purposes.

To each closed walk of length $2k$ in T_d, starting and ending at v_0, we may associate a *sign sequence* $\epsilon_1, \epsilon_2, \ldots, \epsilon_{2k}$ of length $2k$, where $\epsilon_i = 1$ if the ith step of the walk is down, and $\epsilon_i = -1$ if it is up. Each sign sequence has the following two properties:

1. $\sum_{i=1}^{2k} \epsilon_i = 0$;
2. $\sum_{i=1}^{j} \epsilon_i \geq 0$ for all j.

Conversely, any sign sequence with these two properties is the sign sequence of at least $(d-1)^k$ of our closed walks, since at each of the k downward steps, we may choose any of the $d-1$ children of the current vertex. (Of course, we could improve our estimate by taking into account the fact that whenever we are at the root vertex, we have d choices, but this is unnecessary for our purposes.)

Exercise. *The number of sign sequences satisfying the two properties above is precisely the kth Catalan number $C_k = \frac{1}{k+1}\binom{2k}{k}$.*

It follows that

$$t_{d,2k} \geq (d-1)^k C_k = (d-1)^k \frac{1}{k+1}\binom{2k}{k}.$$

Hence,

$$t_{d,2k} \geq (d-1)^k \frac{1}{k+1} \frac{a2^{2k}}{\sqrt{k}} \geq \frac{a'}{k^{3/2}} (2\sqrt{d-1})^{2k},$$

where $a, a' > 0$ are absolute constants. Since $(A^{2k})_{x,x}, (A^{2k})_{y,y} \geq t_{d,2k}$, we have

$$\nu^{2k} \geq t_{d,2k} \geq \frac{a'}{k^{3/2}} (2\sqrt{d-1})^{2k}.$$

Taking the $(2k)$th root of the inequality above gives:

$$\nu \geq 2\sqrt{d-1} \left(1 - C\frac{\log_2 k}{k}\right),$$

where C is an absolute constant. Choosing $k = \lfloor (D-1)/2 \rfloor$ gives

$$\nu \geq 2\sqrt{d-1} \left(1 - c\frac{\log_2 D}{D}\right),$$

where c is an absolute constant, proving the theorem. □

We now come to a crucial definition:

Definition. *A d-regular graph G is said to be a* Ramanujan graph *if* $\nu(G) \leq 2\sqrt{d-1}$.

By Corollary 6, for any $\epsilon > 0$, if n is sufficiently large depending on ϵ, then any d-regular n-vertex graph G has $\nu(G) \geq 2\sqrt{d-1} - \epsilon$, so Ramanujan graphs have 'asymptotically' the minimum possible second spectral modulus. One of the most important problems in theoretical computer science was to construct arbitrarily large d-regular Ramanujan graphs, for some fixed d. This was achieved in 1988 by Lubotzsky, Phillips and Sarnak [4], and independently by Margulis [5]:

Theorem 7 (Lubotzsky-Phillips-Sarnak / Margulis, 1988)**.** *Let let p be a prime such that $p \equiv 1$ (mod. 4). For any prime q such that $q \equiv 1$ (mod. 4) and such that p is a quadratic residue (mod. q), there exists a $(p+1)$-regular Ramanujan graph with $\frac{1}{2}q(q^2-1)$ vertices. Hence, there exist arbirarily large $(p+1)$-regular Ramanujan graphs. Moreover, these can be explicitly constructed; they are Cayley graphs on* $\mathrm{PSL}(2, q)$*, with explicit generating sets.*

Remark. *In 1994, Morgenstern [6] extended this to all $d = p^k + 1$, where $k \in \mathbb{N}$ and p is a prime such that $p \equiv 1$ (mod. 4).*

We now describe the construction of Lubotzsky-Phillips-Sarnak / Margulis. Recall that if q is a prime,

- $\mathrm{GL}(2, q)$, the *general linear group over* $\mathbb{Z}_q$, is the group of all invertible 2×2 matrices with entries in $\mathbb{Z}_q$;
- $\mathrm{SL}(2, q)$, the *special linear group over* $\mathbb{Z}_q$, is the subgroup of $\mathrm{GL}(2, q)$ consisting of all matrices with determinant 1, and
- $\mathrm{PSL}(2, q)$, the *projective special linear group over* $\mathbb{Z}_q$, is the quotient of $\mathrm{SL}(2, q)$ by the normal subgroup consisting of the scalar matrices, $\pm I$:

$$\mathrm{PSL}(2, q) = \mathrm{SL}(2, q)/\{\pm I\}.$$

We have

$$|\mathrm{GL}(2,q)| = (q^2-1)(q^2-q), \quad |\mathrm{SL}(2,q)| = q(q^2-1), \quad |\mathrm{PSL}(2,q)| = \tfrac{1}{2}q(q^2-1).$$

It follows from a theorem of Jacobi that for any $n \in \mathbb{N}$, the number of integer solutions $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ to

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$$

is

$$8 \sum_{\substack{r|n:\\ 4\nmid r}} (r+1).$$

If n is a prime $\equiv 1 \pmod{4}$, then for any $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ with $a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$, one of the a_i's must be odd, and the rest must be even. It follows that for any prime p such that $p \equiv 1 \pmod{4}$, the set

$$T = \{(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 : \ a_0^2 + a_1^2 + a_2^2 + a_3^2 = p, \ a_0 \in \mathbb{N}, \ a_0 \text{ is odd}\}$$

has size $p+1$. We now use T to define the generating set of a Cayley graph on $\mathrm{PSL}(2,q)$, where q is a prime such that $q \equiv 1 \pmod{4}$, and p is a quadratic residue (mod. q). Since $q \equiv 1 \pmod{4}$, -1 is a quadratic residue (mod. q), so may choose $i \in \mathbb{Z}$ such that $i^2 \equiv -1 \pmod{q}$. Since p is a quadratic residue (mod. q), we may choose $b \in \mathbb{Z}$ such that $b^2 \equiv p \pmod{q}$.

Now consider the set

$$S'' = \left\{ \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix} : \ (a_0, a_1, a_2, a_3) \in T \right\}.$$

Each matrix in S'' has determinant $p \equiv b^2 \pmod{q}$, so multiplying each matrix by b^{-1} produces a set S' of matrices in $\mathrm{SL}(2,q)$:

$$S' = \{b^{-1}M'' : \ M'' \in S''\} \subset \mathrm{SL}(2,q).$$

Finally, we let $\pi : \mathrm{SL}(2,q) \to \mathrm{PSL}(2,q)$ denote the quotient homomorphism, and we take $S = \pi(S') = \{\pi(M') : \ M' \in S'\}$, the projection of S. It is easy to check that S is symmetric ($M \in S \Rightarrow M^{-1} \in S$). We let

$$G_{p,q} = \mathrm{Cay}(\mathrm{PSL}(2,q), S).$$

Using some results of Eichler and Igusa concerning the Ramanujan conjecture (a deep conjecture in number theory, which remains unknown), Lubotzsky et al and Margulis were able to prove that

$$\nu(G_{p,q}) = 2\sqrt{p} = 2\sqrt{d-1}$$

—so the graphs $G_{p,q}$ are Ramanujan graphs. The proof employs techniques from representation theory and number theory, and is too long and complex to be given here. An excellent and highly accessible discussion can be found in [3], in which a weaker result is proved: namely, that the graphs $G_{p,q}$ have spectral gap at least c, for some absolute constant $c > 0$. Representation theory comes in because for *any* group Γ, the eigenspaces of *any* Cayley graph on Γ are representations of Γ.

A useful feature of the above construction is that it is fully explicit. The neighbourhood of a prescribed vertex $v \in \mathrm{PSL}(2, q)$ can be computed in only $(p+1)$ steps: one simply computes vs for each $s \in S$.

The following is widely believed, but is known only for integers d of the form $p^k + 1$, where $k \in \mathbb{N}$ and p is a prime $\equiv 1$ (mod. 4):

Conjecture 1. *For* any $d \geq 3$*, there exist arbirarily large d-regular Ramanujan graphs.*

Similarly, if these do exist, it would be of great interest to give explicit constructions.

It turns out that for any $d \geq 3$, almost all d-regular graphs on $[n]$ (for nd even) are 'almost' Ramanujan:

Theorem 8. *For any $d \geq 3$, almost surely,*

$$\nu(G(n,d)) \leq 2\sqrt{d-1} + o_d(1).$$

Here, $o_d(1)$ denotes a function of d and n that tends to zero as $n \to \infty$, for any fixed d.

Hence, as one might expect, the simple symmetric random walk on a uniform random d-regular graph G has (almost) the fastest possible mixing rate. It is surprising (and somewhat miraculous) that the intrinsically algebraic construction of Lubotzsky-Phillips-Sarnak / Margulis shows the 'best possible' mixing behaviour that 'random' d-regular graphs (almost) show.

Theorem 8 follows from the corresponding result for $R(n,d)$, proved by Friedman, and the fact that the models $G(n,d)$ and $R(n,d)$ are contiguous (see the notes from Lecture 13).

Theorem 9 (Friedman)**.** *For any $d \geq 3$, almost surely,*

$$\nu(R(n,d)) \leq 2\sqrt{d-1} + o_d(1).$$

One of the main ideas behind Friedman's proof is the 'trace method': bounding the eigenvalues of A by looking at the trace of high powers of A (or of related matrices), as in the proof of Theorem 5. (Recall that $\mathrm{Trace}(A^{2k})$ is simply the number of closed walks in G of length $2k$; it is also the sum of the $(2k)$th powers of the eigenvalues of A.) Unfortunately, the proof is extremely long, involving many technical estimates.

Hoory and Novikov have independently made the following

Conjecture 2 (Hoory / Novikov)**.** *For any $d \geq 3$, there exists $c_d \in (0,1)$ such that*

$$\mathbb{P}\{G(n,d) \text{ is Ramanujan}\} \to c_d \qquad \text{as } n \to \infty.$$

This would give a positive answer to Conjecture 1 above, although it would not help with the problem of explicit construction.

References

[1] Bilu, Y., Linial, N., Lifts, Discrepancy and Nearly Optimal Spectral Gap, *Combinatorica* Volume 6, Issue 5 (2006) pp. 495-591.

[2] Bollobás, B., *Modern Graph Theory*, Graduate Texts in Mathematics, Springer, 1998.

[3] Davidoff, G., Sarnak, P., Valette, A., *Elementary Number Theory, Group Theory, and Ramanujan Graphs*, London Mathematical Society Student Texts **55**, *Cambridge University Press*, 2003.

[4] Lubotzsky, A., Phillips, R., Sarnak, P., Ramanujan graphs, *Combinatorica* Volume 8, Issue 3 (1988), pp. 261-277.

[5] Margulis, G. A., Explicit group-theoretic constructions of combinatorial schemes and their applications in the construction of expanders and concentrators, *Problems of Information Transmission* Volume 24, Issue 1 (1988), pp. 39-46.

[6] Morgenstern, M., Existence and explicit constructions of $(q+1)$-regular Ramanujan graphs for every prime power q, *Journal of Combinatorial Theory, Series B*, Volume 62, Issue 1 (1994), pp. 44-62.