Expansion properties of random Cayley graphs and vertex transitive graphs

Demetres Christofides Klas Markström

October 23, 2005

Abstract

The Alon-Roichman theorem states that for every $\varepsilon > 0$ there is a constant $c(\varepsilon)$, such that the Cayley graph of a finite group G with respect to $c(\varepsilon)\log|G|$ elements of G, chosen independently and uniformly at random, has expected second largest eigenvalue less than ε. In particular, such a graph is an expander with high probability.

Landau and Russell, and independently Loh and Schulman, improved the bounds of the theorem. Following Landau and Russell we give a simpler proof of the result, improving the bounds even further. When considered for a general group G, our bounds are in a sense best possible.

We also give a generalisation of the Alon-Roichman theorem to random coset graphs.

1 Introduction

We say that a graph $X = (V, E)$ is an (n, d, ε)-***expander*** if it is a graph on n vertices, with maximum degree at least d, such that for every subset W of its vertices of size at most $n/2$, we have $|N(W) \setminus W| \geqslant \varepsilon W$, where $N(W)$ denotes the neighbourhood of W. The ***(vertex) expansion constant*** of X is the largest ε such that X is an (n, d, ε)-expander.

Expanders have many applications in theoretical computer science. The most useful ones, are ***linear expanders***: Families of graphs $\{X_i\}_{i\geqslant 1}$ such that each X_i is an (n_i, d, ε)-expander, with d and ε fixed, and n_i tending to infinity. Although it is not difficult to show via probabilistic methods that such families do exist, it has been quite hard to find explicit examples. Expanders whose degree is polylogarithmic in the number of vertices have also proved useful.

Alon and Roichman [5] proved that 'random Cayley graphs are expanders'. Recall that the ***Cayley diagram*** of a group G with respect to a multiset S of elements of G is the directed multigraph whose vertices are the elements of G and whose set of (directed) edges is the multiset of all ordered pairs (x, y) such that $y = sx$ for some $s \in S$. (I.e. if s appears k times in the multiset S, then there are k directed edges from x to sx.) Ignoring orientation but retaining multiple edges we get the ***Cayley graph*** $X(G,S)$ of G with respect to S. Note that this graph is $2|S|$-regular and it is connected if and only if S generates G.

One way to show that a graph has a given expansion property is via linear algebra. Recall that the ***adjacency matrix*** $A = A(X)$ of a graph X of order n is the $n \times n$ matrix (with rows and columns indexed by the vertices of X) defined by

$$A_{xy} = \begin{cases} 1 & \text{if } xy \text{ is an edge;} \\ 0 & \text{otherwise.} \end{cases}$$

More generally, if X is a multigraph, then A_{xy} is defined to be the number of edges joining x and y, where we use the convention that A_{xx} is twice the number of loops at x. If the graph is d-regular we can also define the ***normalised adjacency matrix*** $T = T(X)$ of X, by $T = \frac{1}{d}A$. Note that T is a real symmetric matrix, so it has an orthonormal basis of (real) eigenvectors. We'll write

$$\lambda_0 \geqslant \lambda_1 = \lambda_1(G) \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{n-1}$$

for its eigenvalues. (Warning: Some authors use the same notation for the eigenvalues of the adjacency matrix.) It can be easily checked that $\lambda_0 = 1$ and $|\lambda_i| \leqslant 1$ for every i. We will also denote by $\mu = \mu(G)$ the second largest element of the multiset of the absolute values of the eigenvalues of T. (I.e. $\mu = \max\{|\lambda_1|, |\lambda_{n-1}|\}$.) The relation between linear algebra and expansion properties of a graph comes from the following result of Alon and Milman (see [2, 3, 4]) which essentially says that if μ is bounded away from 1, then G is a good expander.

Lemma 1 (Alon-Milman [4]). *Let X be a d-regular graph on n vertices. Then X is an $(n, d, \frac{2-2\lambda_1}{3-2\lambda_1})$-expander. In particular it is an $(n, d, \frac{2-2\mu}{3-2\mu})$-expander.* □

Alon and Roichman used random walks on random Cayley graphs to prove the following:

Theorem 2 (Alon-Roichman [5]). *For every $\varepsilon > 0$ there is a $c(\varepsilon) > 0$, depending only on ε such that for every finite group G,*

$$\mathbb{E}(\mu(X(G,S))) \leqslant \varepsilon,$$

where S is a multiset of $c(\varepsilon)\log|G|$ elements of G chosen independently and uniformly at random.[1]

It can be easily shown using martingales (see [5]) that μ is concentrated around its mean. Hence, by Theorem 2 we have:

Theorem 3. *For every $\delta > 0$, there is a $c'(\delta) > 0$ depending only on δ, such that for every finite group G, the Cayley graph $X(G,S)$ is an $(n, 2|S|, \delta)$-expander with high probability*[2] *as $|G| \to \infty$, where S is a multiset of $c'(\delta)\log|G|$ elements of G chosen independently and uniformly at random.*

[1] All logarithms in this paper will be natural, unless otherwise stated.

[2] Meaning that the probability tends to 1.

Landau and Russell [9] and independently Loh and Schulman [10] gave new proofs of Theorem 2, replacing $\log |G|$ by $\log D(G)$, where $D(G)$ is the sum of the dimensions of the irreducible representations of the group G. This satisfies $\sqrt{|G|} < D(G) \leqslant |G|$. (See the next section for more details.) We will usually write D instead of $D(G)$ when the choice of G is clear. Landau and Russell also improved the constant $c(\varepsilon)$. Although their proof is correct, they used some tail bounds on operator valued random variables from a recent paper of Ahlswede and Winter [1] which are unfortunately flawed. The $\ln(2)$ in Lemma 6 and Theorem 19 in [1] should be dropped. These arose from an unfortunate misuse of the natural logarithm as a base 2 logarithm. As a consequence, the Landau-Russell method does not prove their claimed bound. However, using a corrected version of the Ahlswede and Winter result, the new bound on $c(\varepsilon)$ is still better than what was previously known.

We will follow an approach similar to that of Landau and Russell to give a simpler proof of the following version of Theorem 2.

Theorem 4. *For every $0 < \varepsilon < 1$, there is a function*

$$k = k(D) \leqslant \left(\frac{2}{\varepsilon^2} + o(1)\right) \log D$$

such that for every finite group G,

$$\mathbb{E}(\mu(X(G,S))) \leqslant \varepsilon,$$

where S is a multiset of k elements of G chosen independently and uniformly at random. The $o(1)$ term is with respect to increasing D.

The expression we get for k is

$$k = \left(\frac{1}{H_{1/2}\left(\frac{1+\varepsilon}{2}\right)} + o(1)\right) \log D,$$

where H_p is the ***weighted entropy function***

$$H_p(x) = x \log\left(\frac{x}{p}\right) + (1-x)\log\left(\frac{1-x}{1-p}\right).$$

Theorem 4 is an easy corollary of the following theorem.

Theorem 5. *Let S be a multiset of k elements of a finite group G chosen independently and uniformly at random. Then, for every $0 < \varepsilon < 1$,*

$$\Pr(\mu(X(G,S)) \geqslant \varepsilon) \leqslant 2D \exp\left\{-kH_{1/2}\left(\frac{1+\varepsilon}{2}\right)\right\}.$$

Taking $k = \frac{1}{H_{1/2}((1+\varepsilon)/2)}[\log D + b + \log 2]$ we get $\Pr(\mu \geqslant \varepsilon) \leqslant e^{-b}$. Since μ takes values in $[0, 1]$ we have $\mathbb{E}\mu \leqslant (1 - e^{-b})\varepsilon + e^{-b} \leqslant \varepsilon + e^{-b}$. To deduce Theorem 4, replace ε by $\varepsilon' = \varepsilon(1 - \delta)$ and b by $-\log(\varepsilon\delta)$ where $\delta = \delta(D)$ tends to 0 as D tends to infinity and $\log 1/\delta = o(\log D)$.

As we will see later, Theorem 5 is essentially the best possible theorem one could have for a general group G. To improve on the theorem, one possibly needs to know more about the structure of the specific group under consideration.

Recall that a graph X is called ***vertex transitive*** if for every two vertices x, y of X, there is an automorphism ϕ of X such that $\phi(x) = y$. Cayley graphs are vertex transitive graphs. However, there are vertex transitive graphs which are not Cayley graphs, the smallest such graph being the Petersen graph. As Sabidussi [12] observed, every vertex transitive graph can be obtained using the following construction based on cosets of a group:

Given a group G and a subgroup H of G, the ***coset diagram*** of G modulo H with respect to a multiset S of elements of G is defined as follows: Its vertices are the right cosets of H in G, and there is a directed edge from Hx to Hy if and only if $yx^{-1} \in HSH$. The multiplicity of each directed edge from Hx to Hy is defined to be the number of elements s of the multiset S such that $yx^{-1} \in HsH$. Note that the definition of the coset diagram is indeed well-defined, i.e. it does not depend on the choice of representatives for the cosets of H. We can now define the ***coset graph*** $X(G, H, S)$ of G modulo H with respect to the multiset S by retaining multiple edges and ignoring orientation. It is not difficult to check that $X(G, H, S)$ is a regular graph of degree $2\sum_{s \in S} \frac{|HsH|}{|H|}$. Note that if H is a normal subgroup of G, then the Cayley graph $X(G/H, S)$ is isomorphic to the coset graph $X(G, H, S)$.

As we will see in section 5, using similar ideas as in the proof of Theorem 5 we can extend Theorem 5 to show that random coset graphs have good expansion properties.

For the reader's convenience, we recall in Section 2 all the results from representation theory that we will need. Proofs of the results can be found in many books, for example in Serre [13]. In Section 3 we give the proof of Theorem 5. In Section 4 we extend Theorem 5 to coset graphs. Finally in Section 5, we discuss some related results.

2 Some Representation Theory

A ***representation*** ρ of a finite group G is a homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a vector space over $\mathbb{C}$. The ***dimension*** d_ρ of ρ is simply the dimension of V. Equip V with an inner product $\langle , \rangle$. One can now replace $\langle , \rangle$ with a new inner product

$\langle , \rangle'$ which is preserved under the action of ρ. Indeed define

$$\langle v, w \rangle' = \frac{1}{|G|} \sum_{g \in G} \langle \rho(g)v, \rho(g)w \rangle.$$

In this way, we may (and we will) consider ρ as a homomorphism into the unitary group of V.

We say that a subspace W of V is ***invariant*** if it is fixed by ρ. (I.e. $\rho(g)W \subseteq W$ for every $g \in G$.) It is then easily checked that the restriction $\rho_W : G \to \mathrm{GL}(W)$ is a representation. We say that ρ is ***irreducible*** if there is no non-trivial invariant subspace.

Theorem (Complete Reducibility). *Any representation ρ can be decomposed into irreducible representations $\rho = \rho_1 \oplus \ldots \oplus \rho_k$. (Meaning $V = W_1 \oplus \ldots W_k$ where each W_i is invariant and $\rho_i = \rho_{W_i}$ is irreducible.)*

We say that two representations $\rho : G \to \mathrm{GL}(V)$ and $\rho' : G \to GL(V')$ are ***equivalent*** if there exists an isomorphism $\phi : V \to V'$ such that the following diagram commutes for every $g \in G$.

$$\begin{tikzcd}
V \arrow[r, "\phi"] \arrow[d, "\rho(g)"'] & V' \arrow[d, "\rho'(g)"] \\
V \arrow[r, "\phi"'] & V'
\end{tikzcd}$$

Theorem. *A finite group G has only a finite number of irreducible representations up to equivalence.*

Two important representations are the ***trivial representation*** $1 : G \to \mathrm{GL}(\mathbb{C})$; $g \mapsto id$ and the ***regular representation*** $R : G \to \mathrm{GL}(\mathbb{C}[G])$, where $\mathbb{C}[G]$ is the vector space over $\mathbb{C}$ generated by the elements of G, defined by $(Rg)(\sum \alpha_h h) = \sum \alpha_h gh = \sum \alpha_{g^{-1}h} h$. It is an important fact that R decomposes as

$$R = \bigoplus \underbrace{\rho \oplus \cdots \oplus \rho}_{\dim \rho}$$

where the sum is over a complete set of inequivalent irreducible representations of G. In particular, since $\mathbb{C}[G]$ has dimension $|G|$, we deduce that $|G| = \sum (d_\rho)^2$. We define $D = D(G)$ by $D = \sum d_\rho$ and observe that $\sqrt{|G|} < D(G) \leqslant |G|$.

Given a subgroup H of a group G, by restricting to H, we can consider any representation ρ of G as a representation of H. It could be the case that ρ is an irreducible representation of G, but when restricted to H is not any more irreducible. We define $D(G, H)$ to be the sum of the dimensions of the irreducible representations of G which, when decomposed into irreducible representations of H, do not contain the trivial representation of H. For example, it is not hard to show that if H is normal in G, then $D(G/H) = D(G, H)$.

3 Proof of Theorem 5

Let $s_1, \ldots, s_k$ be elements of G chosen independently and uniformly at random. Let

$$s = \frac{1}{2k} \sum_{i=1}^{k} (s_i + s_i^{-1})$$

and observe that the matrix of the linear operator

$$R(s) = \frac{1}{2k} \sum_{i=1}^{k} (R(s_i) + R(s_i^{-1}))$$

with respect to the standard basis of $\mathbb{C}[G]$ (i.e. $\{g : g \in G\}$) is just the normalised adjacency matrix T of $X(G,S)$. But the eigenvalue 1 corresponds to the trivial representation, so (by the decomposition of R) we deduce that $\mu = \max_\rho \|\rho(s)\|$ where ρ runs over all irreducible non-trivial representations of G. Here, $\|.\|$ denotes the ***operator norm***, defined by $\|A\| = \sup_{\|x\|=1} \|Ax\|$.

So we are left with estimating $\|\rho(s)\|$ for every non-trivial irreducible representation ρ. Loh and Schulman proceeded via random walks as in the original Alon-Roichman proof. Landau and Russell used the aforementioned result of Ahlswede and Winter. Our approach is to use the following version of the Hoeffding-Azuma inequality:

Theorem 6 (Hoeffding [7]). *Let $X_0, X_1, \ldots, X_n$ be a martingale such that $-r_i \leqslant X_i - X_{i-1} \leqslant 1 - r_i$ for some constants $r_1, \ldots, r_n$. Let $r = \frac{1}{n}\sum_{i=1}^{n} r_i$. Then for every $\varepsilon > 0$,*

$$\Pr(|X - \mathbb{E}X| \geqslant \varepsilon n) \leqslant 2\exp\{-nH_r(r+\varepsilon)\}.$$

Now fix a non-trivial irreducible representation ρ of G and let A_i be the operator $\frac{1}{2}[\rho(s_i) + \rho(s_i^{-1})]$. Let $\mu_1, \ldots, \mu_{d_\rho}$ be the eigenvalues of $\frac{1}{2}\sum_{i=1}^{k} A_i$, arranged in decreasing order of magnitude of their absolute values. Let X be an eigenvalue of $\frac{1}{2}\sum_{i=1}^{k} A_i$ chosen uniformly at random. We have

$$\mathbb{E}X = \frac{1}{2d_\rho} \sum_{i=1}^{k} \mathbb{E}(\mathrm{Tr}\,(A_i)) = \frac{k}{2d_\rho |G|} \mathrm{Tr}\left(\sum_{g \in G} \rho(g)\right) = 0.$$

Indeed, the matrix of the operator $\sum_{g\in G} R(g)$ with respect to the standard basis of $\mathbb{C}[G]$ is the 'all 1 matrix'. In particular it has rank 1. But so does the matrix of the trivial representation. Hence, by the decomposition of R, $\sum_{g \in G} \rho(g)$ is the zero operator. (If the reader prefers he can just use the orthogonality relations.)

We now let $X_i = \mathbb{E}(X|A_1, \dots, A_i)$ and note that $X_0, \dots, X_k$ is a martingale with $|X_i - X_{i-1}| \leqslant \frac{1}{2}$ for every i. Indeed, arguing as above one shows that $X_i - X_{i-1} = \frac{\mathrm{Tr}(A_i)}{2\dim\rho}$. But $\rho(s_i)$ and $\rho(s_i^{-1})$ are unitary operators, hence $|\mathrm{Tr}(A_i)| \leqslant \dim\rho$. Applying the Hoeffding-Azuma inequality, we deduce that

$$\Pr(|X| \geqslant \varepsilon k) \leqslant 2\exp\{-kH_{1/2}(1/2+\varepsilon)\}.$$

In particular, we deduce that

$$\begin{aligned}\Pr(\|\rho(s)\| \geqslant \varepsilon) &= \Pr\left(\left\|\frac{1}{k}\sum_{i=1}^{k} A_i\right\| \geqslant \varepsilon\right) \\ &= \Pr\left(|\mu_1| \geqslant \frac{\varepsilon k}{2}\right) \leqslant \sum_{i=1}^{d_\rho} \Pr\left(|\mu_i| \geqslant \frac{\varepsilon k}{2}\right) \\ &= d_\rho \Pr\left(|X| \geqslant \frac{\varepsilon k}{2}\right) \leqslant 2d_\rho \exp\left\{-kH_{1/2}\left(\frac{1+\varepsilon}{2}\right)\right\}.\end{aligned}$$

Summing over all irreducible non-trivial representations of G completes the proof of Theorem 5. □

In the proof, it was important that we could use the Hoeffding-Azuma inequality to show that X was concentrated around its expectation. However, what was crucial in the proof was that we could calculate the expectation of X. If instead we had taken X to be the second largest eigenvalue of $\frac{1}{2}\sum_{i=1}^{k} A_i$, then we would still be able to obtain the same concentration result, however we would have no clue about the expectation of X.

4 Coset Graphs

Let G be a finite group, H a subgroup of G and S is a multiset of elements of G, chosen independently and uniformly at random. We want to show that if S is large enough, then $X = X(G, H, S)$ is a good expander. As before, the aim would be to deduce this from the spectral properties of X. However, it seems that it is not easy to show that $\mu(X)$ is as small as one would hope for. The following simple lemma will enable us to deduce that X is a good expander by looking at a related graph Y for which $\mu(Y)$ can be computed more easily. Recall that a ***stochastic matrix*** is a matrix P with entries in $[0, 1]$ such that the elements in each row of P sum to 1.

Lemma 7. *Let X be a d-regular graph on n vertices. Let $\mu^* = \mu^*(X)$ be the infimum of the second largest eigenvalue in absolute value of P, where P runs over all $n \times n$ symmetric stochastic matrices satisfying $P_{ij} = 0$ whenever $T(X)_{ij} = 0$. Then X is an $(n, d, \frac{2-2\mu^*}{3-2\mu^*})$-expander.*

Proof. Immediate if we note that two graphs which have the same underlying simple graph, have the same expansion constant. Indeed, this observation says that the lemma is true if the entries of the matrix are rational. We can easily pass to matrices which also have irrational entries by taking limits. □

For further discussion of this lemma, see section 5.3.

So, instead of looking at the spectrum of X, we can look at the spectrum of any graph Y which has the same underlying simple graph as X. We define Y as follows: Its vertex set is the set of right cosets of H in G, and the multiplicity of the edge (Hx, Hy) is the number of possible ways to express y as $h_1 s h_2 x$ where $h_1, h_2 \in H$ and $s \in S$ or $s^{-1} \in S$. Note that Y is $2|H||S|$-regular and it has indeed the same underlying simple graph as H.

We claim that every eigenvalue of Y, is also an eigenvalue of the Cayley graph Y' of G with respect to the multiset HSH. This follows from the fact that Y' a the 'blow-up' of Y. I.e. Y' is obtained from Y by replacing each vertex by $|H|$ new vertices corresponding to the elements of the coset, and replacing each edge by a $K_{|H|,|H|}$ on the corresponding vertices. Thus, the normalised adjacency matrix of Y' can be written up as a $\frac{|G|}{|H|} \times \frac{|G|}{|H|}$ matrix of $|H| \times |H|$ blocks, with ...... It then easily follows that if $v = (v_1, \ldots, v_{|G|/|H|})$ is an eigenvector of Y with eigenvalue λ, then $v' = (v_1, \ldots, v_1, \ldots, v_{|G|/|H|}, \ldots, v_{|G|/|H|})$ is an eigenvector of Y' with eigenvalue λ.

Thus, in order to show that X is a good expander, it is enough to show that $\mu(Y')$ is bounded away from 1.

Theorem 8. *With the above notation, we have*

$$\Pr(\mu(Y') \geqslant \varepsilon) \leqslant 2D(G,H) \exp\left\{-|S| H_{1/2}\left(\frac{1+\varepsilon}{2}\right)\right\}.$$

Proof. As in the proof of Theorem 5 we get

$$\begin{aligned}\Pr(\mu(Y') \geqslant \varepsilon) &\leqslant \sum_{\rho} \Pr\left(\left\|\rho\left(\frac{1}{2|S||H|^2} \sum_{\substack{h_1,h_2 \in H\\ s\in S}} (h_1 s h_2 + h_1 s^{-1} h_2)\right)\right\| \geqslant \varepsilon\right)\\ &\leqslant \sum_{\|\sum_{h\in H}\rho(h)\| \neq 0} \Pr\left(\left\|\rho\left(\frac{1}{2|S|}\sum_{s\in S}(s+s^{-1})\right)\right\| \geqslant \frac{\varepsilon |H|^2}{\|\sum_{h\in H}\rho(h)\|^2}\right)\end{aligned}$$

The result will follow by showing that $\|\sum \rho(h)\|$ is equal to $|H|$ or 0, depending on whether ρ, as a representation of H, contains the trivial representation of H or not. But if ρ contains the trivial representation of H, then clearly $\|\sum \rho(h)\| = |H|$, while if it does not, then it decomposes into a sum of irreducible representations ρ_i of H such that each $\sum \rho_i(h)$ is the zero operator. This completes the proof. □

5 Further Comments and Results

5.1 Comparison with some lower bounds

Alon and Roichman also showed that if $G = \mathbb{Z}_2^m$, S is any subset of elements of G, and $\mu(X(G,S)) \leqslant 1-\delta$, then the following must hold:

$$\sum_{i<\frac{\delta|S|}{4}} \binom{|S|}{i} 2^m < 2^l.$$

In particular this implies that $|S| \geqslant \left(1 + \Omega_m\left(\delta \log\left(\frac{1}{\delta}\right)\right)\right) m.$

The following result, proven by Alon and Roichman for abelian groups, shows that this lower bound is essentially sharp as an upper bound for every group.

Theorem 9. *For every sufficiently small $\delta > 0$, there is an $\varepsilon = O\left(\delta \log\left(\frac{1}{\delta}\right)\right)$ such that for every finite group G, $\mu(X(G,S)) \leqslant 1-\delta$ with high probability as $D \to \infty$, where S is a multiset of $(1+\varepsilon)\log_2 D$, chosen independently and uniformly at random.*

Proof. Taking

$$k = \frac{\log D + b + \log 2}{H_{1/2}(1-\delta/2)} = \frac{2(\log D + b + \log 2)}{(2-\delta)\log(2-\delta) + \delta \log \delta}$$

we deduce that $\Pr(\mu \geqslant 1-\delta) \leqslant e^{-b}$ and we can then proceed as before. The result follows by noting that as $\delta \to 0$ then

$$\frac{2}{(2-\delta)\log(2-\delta) + \delta\log\delta} \sim \frac{1}{\log 2} + \frac{\delta \log\left(\frac{1}{\delta}\right)}{2(\log 2)^2}. \qquad \square$$

Since Theorem 9 is a direct consequence of Theorem 5 and since it is essentially sharp for $G = \mathbb{Z}_2^m$, then in order to improve on Theorem 5 it seems we would have to take into consideration more of the structure of the group that we are concerned with.

5.2 Ramanujan-like Cayley graphs

It is known (see e.g. [8]) that the second largest eigenvalue of any d-regular graph on n vertices is at least

$$\frac{2\sqrt{d-1}}{d}\left(1 + O\left(\left(\frac{\log d}{\log n}\right)^2\right)\right).$$

This is essentially best possible; there are explicit constructions of ***Ramanujan graphs*** (see e.g. [11]), d-regular graphs with second largest eigenvalue at most $\frac{2\sqrt{d-1}}{d}$. We can show that random Cayley graphs are quite close to being Ramanujan.

Theorem 10. *For every $\delta > 0$ and every group G, if S is a set of k elements of G, chosen independently and uniformly at random, then $\mu(X(G,S)) \leqslant (\sqrt{2}+\delta)\sqrt{\frac{\log D}{k}}$ with high probability as $D \to \infty$.*

Proof. Immediate by Theorem 5 since

$$\Pr\left(\mu(X(G,S)) \geqslant (\sqrt{2}+\delta)\sqrt{\frac{\log D}{k}}\right) \leqslant 2D^{1-(1+\delta/\sqrt{2})^2}. \qquad \square$$

Taking $k = (\log D)^r$, for some fixed r, we deduce that with high probability, such a Cayley graph has second eigenvalue at most $\frac{\sqrt{2}+\delta}{\sqrt{k}} k^{1/2r}$.

5.3 Discussion of Lemma 7

In section 4, we used Lemma 7 to pass to a matrix which had easily computable second largest eigenvalue. We now give two examples where Lemma 7 is used to improve the bound for the expansion constant.

Example 1. We begin with a connected 3-regular non-bipartite graph X. This guarantees that $\mu(X) < 1$. It is well known that each 3-regular graph has a perfect matching. We actually pick X such that it has a perfect matching M whose removal does not leave a Hamiltonian cycle. We now replace each edge of X not in M by n new edges to get new graph X_n. Clearly, $\mu^*(X_n) \leqslant \mu(X) < 1$. On the other hand, the normalised adjacency matrices of X_n tend to the normalised adjacency matrix of $X \setminus M$ in the operator norm, say. Since the eigenvalues vary continuously, we deduce that $\mu(X_n) \to \mu(X \setminus M) = 1$ as $n \to \infty$.

In the above example, we used Lemma 7 to get a better expansion constant for the multigraphs X_n than the one given by Lemma 1. However this was in a sense not a genuine example. All we did was to take a simple graph and produce some multigraphs with the same adjacencies, which had very bad spectral properties. So now we present an example of a simple graph X such that we can show that $\mu^*(X) < \mu(X)$.

Example 2. We take $X = K_4 \times C_{10}$. This can be viewed as a Cayley graph of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{10}$. Using the representation theoretic approach of section 3, one can show that $\mu(X) = \frac{7+\sqrt{5}}{10} = 0.9236\ldots$. Consider the subgraph $Y = C_4 \times C_{10}$ of X. We give each edge of Y a weight of $\frac{6}{5}$ and each other edge a weight of $\frac{1}{5}$ to get a new (weighted) graph Z. Note that Z is a regular graph. It can be checked that $\mu^*(X) \leqslant \mu(Z) = \frac{23}{25} = 0.92 < \mu(X)$.

When can one use this method to improve the bound for the expansion constant? In the above example, we had a regular graph X which had some local dense parts together with some global other structure, and the global structure was responsible for the expansion of X. Picking a matching Y in each of these local parts and putting higher weights on the edges of $X \setminus Y$ we obtained a regular weighted graph Z. Why should we have $\mu(Z) < \mu(X)$? There is a relationship between $\mu(X)$ and random walks on the vertices of X. The smaller $\mu(X)$ is, the faster the random walk on the vertices of X will converge to the normal distribution and vice versa (see e.g. [6, Chapter IX]). Intuitively, by having less weight in most edges of these dense local parts (but large weight in some of their edges) we would expect a random walk to spend less time in each local part, and hence to converge faster to the uniform distribution. We believe that in situations like this, where we have better local expansion properties than globally, one has a fairly good chance to be able to use Lemma 7 to deduce a better bound for the expansion properties for the graph X.

Acknowledgements

The first author is supported by grants from the Engineering and Physical Sciences Research Council and from the Cambridge Commonwealth Trust. The work was done while the second author was visiting the Department of Pure Mathematics and Mathematical Statistics of the University of Cambridge, and he would like to thank the department for its hospitality and also the Royal Physiographic Society in Lund for the grant, making this visit possible.

References

[1] R. Ahlswede and A. Winter, Strong converse for identification via quantum channels, IEEE Trans. Inform. Theory **48** (2002), 569–579.

[2] N. Alon, Eigenvalues and expanders, Combinatorica **6** (1986), 83–96.

[3] N. Alon and V. D. Milman, λ_1, isoperimetric inequalities for graphs, and superconcentrators, J. Combin. Theory Ser. B **38** (1985), 73–88.

[4] N. Alon and V. D. Milman, Eigenvalues, expanders and superconcentrators, in *Twenty-fifth annual symposium on foundations of computer science*, Academic Press, Orlando, FL, 1986, 320–322.

[5] N. Alon and Y. Roichman, Random Cayley graphs and expanders, Random Structures Algorithms **5** (1994), 271–284.

[6] B. Bollobás, *Modern graph theory*, Springer, New York, 1998.

[7] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Amer. Statist. Assoc. **58** (1963), 13–30.

[8] N. Kahale, On the second eigenvalue and linear expansion of regular graphs, in *Expanding graphs*, Amer. Math. Soc., Providence, RI, 1993, 49–62.

[9] Z. Landau and A. Russell, Random Cayley graphs are expanders: a simple proof of the Alon-Roichman theorem, Electron. J. Combin. **11** (2004), Research Paper 62.

[10] P.-S. Loh and L. J. Schulman, Impoved expansion of Random Cayley Graphs, Discrete Math. Theor. Comput. Sci. **6** (2004), 523–528.

[11] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, Combinatorica **8** (1988), 261–277.

[12] G. Sabidussi, Vertex-transitive graphs, Monatsh. Math. **68** (1964), 426–438.

[13] J.-P. Serre, *Linear representations of finite groups*, Springer, New York, 1977.

Demetres Christofides: Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, CB3 0WB, United Kingdom; dc282@cam.ac.uk

Klas Markström: Department of Mathematics and Mathematical Statistics, Umeåuniversitet, SE-901 87, Umeå, Sweden; Klas.Markstrom@math.umu.se