Improved Expansion of Random Cayley Graphs
Po-Shen Loh, Leonard J. Schulman

To cite this version:

HAL Id: hal-00959024
https://hal.inria.fr/hal-00959024
Submitted on 13 Mar 2014
Improved Expansion of Random Cayley Graphs

Po-Shen Loh† and Leonard J. Schulman‡

1Churchill College, University of Cambridge, Cambridge, CB3 0DS, UK
email: lpo@alumni.caltech.edu
2Department of Computer Science, California Institute of Technology, Pasadena, CA 91125, USA
email: schulman@caltech.edu


Alon and Roichman (1994) proved that for every $\varepsilon > 0$ there is a finite $c(\varepsilon)$ such that for any sufficiently large group $G$, the expected value of the second largest (in absolute value) eigenvalue of the normalized adjacency matrix of the Cayley graph with respect to $c(\varepsilon)\log |G|$ random elements is less than $\varepsilon$. We reduce the number of elements to $c(\varepsilon)\log D(G)$ (for the same $c$), where $D(G)$ is the sum of the dimensions of the irreducible representations of $G$. In sufficiently non-abelian families of groups (as measured by these dimensions), $\log D(G)$ is asymptotically $(1/2)\log |G|$. As is well known, a small eigenvalue implies large graph expansion (and conversely); see Tanner (1984) and Alon and Milman (1984, 1985). For any specified eigenvalue or expansion, therefore, random Cayley graphs (of sufficiently non-abelian groups) require only half as many edges as was previously known.

Keywords: expander graphs, Cayley graphs, second eigenvalue, logarithmic generators

1 Introduction

All groups considered in this paper are finite.

Definition 1 Let $G$ be a group, and $S \subset G$ be a multiset. The Cayley graph $X(G,S)$ is the multigraph on vertex set $G$, with $n$ undirected edges connecting $g$ and $tg$ if $t$ appears $n$ times in the multiset union $S \sqcup S^{-1}$, where $S^{-1}$ is the multiset $\{s^{-1} : s \in S\}$. The normalized adjacency matrix $A^*_X(G,S)$ is $1/(2|S|)$ times the adjacency matrix of $X(G,S)$.

Definition 2 Let $M$ be an $n \times n$ matrix with real eigenvalues $x_1, \ldots, x_n$, where $|x_1| \geq \cdots \geq |x_n|$. Define $\lambda(M) = |x_1|$ and $\mu(M) = |x_2|$. Write $\mu(X(G,S))$ for $\mu(A^*_X(G,S))$.

Definition 3 Let $D(G)$ be the sum of the dimensions of the irreducible representations of $G$. 

---

†Supported in part by the Marshall family, a Caltech Summer Undergraduate Research Fellowship, and an NSF REU supplement.
‡Supported in part by NSF CAREER grant 0049092 and by a grant from the Okawa Foundation.
Observe that $|G|^{1/2} < D(G) \leq |G|$. The upper bound is met only by abelian groups but is approached also by other groups whose irreducible representations are mostly low-dimensional, such as dihedral groups. The lower bound is approached, in the sense that $\log D(G) \sim (1/2) \log |G|$, by a variety of families of groups possessing mostly high-dimensional irreducible representations.

Examples:

(a) The affine group $A_p$ over the prime field $GF(p)$. $|A_p| = p(p - 1)$, while $D(A_p) = 2p - 2$.

(b) The symmetric group $S_n$. $|S_n| = n!$, hence $\log |S_n| = n \log n - O(n)$, while $D(S_n) \in e^{O(\sqrt{n})}\sqrt{n}$, hence $\log D(S_n) \in (1/2)n \log n + O(\sqrt{n})$.

(For the upper bound on $D(S_n)$, take the number of irreducible representations of $S_n$ times the maximum of their dimensions. The first of these is $p(n)$, the number of partitions of $n$, which has the asymptotic behavior $p(n) \sim \frac{1}{4n\sqrt{3}}e^{\pi\sqrt{2n/3}}$. The second was shown by Vershik and Kerov (1985) to be bounded above by $e^{-k\sqrt{n}\sqrt{n}}$ for a positive constant $k$.)

**Theorem 1** For any $\varepsilon > 0$ the following holds for every sufficiently large group $G$. Let $S$ be a multiset of $c(\varepsilon) \log D(G)$ uniformly and independently sampled elements of $G$, for $c(\varepsilon) = 4e/\varepsilon^2$. Then we have $E[\mu(X(G,S))] < (1 + o(1))\varepsilon$.

(Here and throughout $o(1)$ allows for a quantity tending to 0 for large $|G|$.) Russell and Landau (2004) have independently obtained a similar result.

As a detail note that in Alon and Roichman (1994), $S$ is generated by sampling without repetition (i.e., $S$ is a set), while we employ sampling with repetition. The principal benefit of this is to simplify the argument, but it also leads to some sharpening: the value of $c(\varepsilon)$ obtained in Alon and Roichman (1994) is slightly larger than given here, while substituting sampling with repetition into their argument leads to the same $c(\varepsilon)$.

2 Proof

The combinatorial outline of the proof follows that of Alon and Roichman; the heart of the improvement lies in taking a certain union bound over the irreducible representations, rather than over the entire regular representation, of the group.

2.1 *Decomposition into irreducible representations*

Fix a group $G$, and let $S$ be a multiset of $N$ elements of $G$. Let $T = S \cup S^{-1}$; let $\alpha$ be the element in the group algebra $\mathbb{C}[G]$ defined by:

$$\alpha = \sum_{t \in T} \frac{1}{|T|} t.$$

Let the operator $L$ be the left-action of $\alpha$ on $\mathbb{C}[G]$. Its matrix representation with respect to the standard basis is the normalized adjacency matrix of $X(G,S)$. The Fourier Transform $\mathcal{F}$ is an algebra isomorphism from $\mathbb{C}[G]$ to $\bigoplus_{1 \leq \ell \leq \mathcal{M}_d} \mathcal{M}_d$, where $\mathcal{K}$ is the number of irreducible representations of $G$, and $\mathcal{M}_d = \text{Mat}_{d \times d}(\mathbb{C})$. Hence the eigenvalues of $L$ are the same as the eigenvalues of the left-action of $\mathcal{F}(\alpha)$ on $\bigoplus \mathcal{M}_d$. Explicitly,
Improved Expansion of Random Cayley Graphs

\[ \mathcal{F}(\alpha) = \bigoplus_{r=1}^{R} \left( \sum_{t \in T} \frac{1}{|T|} \rho_r(t) \right), \]

where \( \rho_r : G \rightarrow M_r \) are the (unitary) irreducible representations, expressed with respect to fixed bases. Focus on an arbitrary component \( r \) of \( \mathcal{F}(\alpha) \): let \( \Psi_r = (1/|T|) \sum_{t \in T} \rho_r(t) \).

Since \( \Psi_r \) is an average of unitary matrices, its eigenvalues are bounded in absolute value by 1. Let \( \rho_1 \) be the one-dimensional trivial representation \( \rho_1 : G \mapsto \mathbb{C} \). Then for any \( S \), \( \Psi_1 = 1 \). Therefore, \( \mu(X(G,S)) = \lambda(A) \), where \( A \) is the following block-diagonal matrix:

\[
A = \begin{pmatrix}
Psi_2 & 0 & \ldots & 0 \\
0 & Psi_3 & \ldots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & Psi_R
\end{pmatrix}.
\]

2.2 From eigenvalues to random walks

Fact 1 Let \( M \) be a square matrix with real eigenvalues. Then for every positive integer \( m \),

\[ \lambda(M) \leq (\text{Tr}(M^{2m}))^{1/2m}. \]

Because of the symmetric construction of \( T \), \( A \) is Hermitian. By convexity,

\[ E[\mu(X(G,S))] \leq (E[\text{Tr}(A^{2m})])^{1/2m}. \]

Since \( A \) is block-diagonal, \( A^{2m} \) shares the same block structure, with blocks \( \Psi_i^{2m} \) (\( 2 \leq i \leq R \)).

\[
\text{Tr}(A^{2m}) = \sum_{r=2}^{R} \text{Tr}(\Psi_r^{2m})
= \sum_{r=2}^{R} \left( \sum_{t_1, \ldots, t_{2m} \in T} \frac{\chi_r(t_1 \cdots t_{2m})}{|T|^{2m}} \right)
= \sum_{r=2}^{R} \sum_{g \in G} \chi_r(g) \frac{N_g}{|T|^{2m}},
\]

where \( \chi_r \) is the character of \( \rho_r \) and \( N_g \) is the number of ways to produce \( g \) as a product of \( 2m \) (not necessarily distinct) elements of \( T \).

Definition 4 Let RW denote the following random walk process.

1. Choose a uniform random word of length \( 2m \) from the free monoid on the \( N \) letters \( \{a_1, a_2, \ldots, a_N\} \) (e.g., \( a_2a_5a_2^{-1}a_1^{-1}a_2a_3 \)).

2. Reduce the word in the free group (e.g., \( a_2a_5a_2^{-1}a_1^{-1}a_2a_3 \rightarrow a_2a_1^{-1}a_1^{-1}a_2a_3 \)).
Uniformly and independently assign (not necessarily distinct) group elements to the letters that appear in the remaining word, and evaluate the product in $G$.

Let $\text{RW}_g$ be the event that the result is $g$. Therefore, $\Pr(\text{RW}_g) = \frac{N_g}{|T|^{2m}}$, so

$$E[\text{Tr}(A^{2m})] = \sum_{g \in G} \Pr(\text{RW}_g) \sum_{r=2}^R \Re \chi_r(g).$$

### 2.3 Mixing in the random walk

**Definition 5** Let $\omega$ be a reduced word as obtained via step (2) of process $\text{RW}$ (definition 4). Say that $\omega$ has a **singleton** if there is an $i$ such that the number of occurrences of $a_i$ in $\omega$ plus the number of occurrences of $a_i^{-1}$ in $\omega$ is exactly one.

Let $\Omega$ be the event that the reduced word has a singleton. Now:

$$\sum_{g \in G} \Pr(\text{RW}_g) \sum_{r=2}^R \Re \chi_r(g)$$

$$= \sum_{g \in G} \Pr(\Omega \land \text{RW}_g) \sum_{r=2}^R \Re \chi_r(g) + \sum_{g \in G} \Pr(\overline{\Omega} \land \text{RW}_g) \sum_{r=2}^R \Re \chi_r(g)$$

$$\leq \sum_{g \in G} \Pr(\Omega \land \text{RW}_g) \sum_{r=2}^R \Re \chi_r(g) + \Pr(\overline{\Omega}) D(G). \hspace{1cm} (1)$$

**Lemma 1** $\Pr(\text{RW}_g | \Omega) = 1/|G|$.

**Proof:** In step (3) of $\text{RW}$ (definition 4), assign the singleton element last; then, there will exist a unique group element that makes $\omega$ evaluate to $g$. □

**Comment:** This lemma replaces an upper bound of $1/|G| + O(m/G^2)$ in Alon and Roichman (1994), the additional term being the result of their requiring distinct assignments in step (3). This additional term leads in turn to an extra summand of $e^{-b}$ in the analogue, in their work, of the center expression in Inequality (2).

By Lemma 1 and the orthogonality of characters, the first term of Bound (1) vanishes. Combining our inequalities:

$$E[\mu(X(G,S))] \leq (E[\text{Tr}(A^{2m})])^{1/2m} \leq \Pr(\overline{\Omega})^{1/2m} D(G)^{1/2m}.$$

To bound $\Pr(\overline{\Omega})$, we follow the spirit of Alon and Roichman (1994) and define the following two events in terms of the quantity $M = 2m(1 - \log \log 2m / \log 2m)$:

(A) After step (2) of $\text{RW}$ (definition 4), the length of the reduced word is less than $M$.

(B) After step (2) of $\text{RW}$ (definition 4), the length of the reduced word is at least $M$, but there are no singletons.
Clearly, $\Pr(\Omega) \leq \Pr(A) + \Pr(B)$. Alon and Roichman (1994) produced these bounds:

$$\Pr(A) \leq 2^{2m (2/N)^m \log \log 2m / \log 2m}$$
$$\Pr(B) \leq 2^{M (m/N)^M / 2}.$$  

Substituting $N = c(\varepsilon) \log D(G)$ and $2m = (1/b) \log D(G)$, for any constant $b$, we obtain an expression almost identical to one of Alon and Roichman (1994), except that $|G|$'s are replaced by $D(G)$'s:

$$\Pr(\Omega)^{1/2m} D(G)^{1/2m} \leq (1 + o(1)) e^{b \sqrt{\frac{2}{bc(\varepsilon)}}} \leq (1 + o(1)) \varepsilon$$  \hspace{1cm} (2)

where we use the choices $c(\varepsilon) = 4e/e^2$ and $b = 1/2$. \hfill \Box
References


