# On Kazhdan Constants and Mixing of Random Walks

IGOR PAK
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139 USA
E-mail: pak@math.mit.edu

ANDRZEJ ŻUK
CNRS, Ecole Normale Supérieure de Lyon
Unité de Mathématiques Pures et Appliquées
46, Allée d'Italie, F-69364 Lyon cedex 07 France
E-mail: azuk@umpa.ens-lyon.fr
&
Department of Mathematics, University of Chicago
5734 S. University Avenue, Chicago, Illinois 60637, USA
E-mail: zuk@math.uchicago.edu

**Abstract**

Let $G$ be a group with Kazhdan's property (T), and let $S$ be a *transitive* generating set (there exists a group $H \subset \mathrm{Aut}(G)$ which acts transitively on $S$.) In this paper we relate two definitions of the Kazhdan constant and the eigenvalue gap in this case. Applications to various random walks on groups, and the product replacement random algorithm, are also presented.

## 1 Introduction

Let $G$ be a group generated by a finite set $S$. We say that a unitary representation $\pi : G \to \mathcal{U}(\mathcal{H}_\pi)$ *almost has invariant vectors* if for every $\varepsilon > 0$ there exists a vector $u_\varepsilon \in \mathcal{H}_\pi$ such that $\|\pi(s)u_\varepsilon - u_\varepsilon\| < \varepsilon \|u_\varepsilon\|$ for every $s \in S$. The group $G$ is said to have *Kazhdan's property* (T) (see [16]), if every unitary representation $\pi$ of $G$ which almost has invariant vectors has a non-zero invariant vector.

It is known (see [14]) that if the group $G$ has property (T) then there exists a positive constant $\varepsilon(S) > 0$, which might depend on the set $S$ (see [12]), such that for every unitary representation $\pi : G \to \mathcal{U}(\mathcal{H}_\pi)$ with no invariant vectors and for every $u \in \mathcal{H}_\pi$ one has:

$$\max_{s \in S} \|\pi(s)u - u\| \, \geq \, \varepsilon(S) \, \|u\|. \tag{1}$$

The largest such a constant $K = \bigl(\varepsilon(S)\bigr)^2$ is called the *Kazhdan constant* with respect to the set $S$. The main result of this paper is a new inequality between $\varepsilon$ and the eigenvalue gap of Schreier graphs of $G$.

Let $H \subset G$ be a subgroup of finite index. A Schreier graph $\Gamma = \Gamma(G/H, S)$ is defined to have cosets $G/H$ as vertices, and unoriented edges corresponding to multiplication by $S$ on the left. Denote by $A$ the adjacency matrix of $\Gamma$, and let $1 = \lambda_0 > \lambda_1 \geq \ldots \geq \lambda_{|\Gamma|} \geq -1$ be the eigenvalues of $A/|S|$. Denote by $\beta = 1 - \lambda_1$ the eigenvalue gap of $\Gamma$.

We say that $\Phi \subset \mathrm{Aut}(G)$ is *$S$-preserving* (write $H(S) = S$), if $\phi(s) \in S$ for all $\phi \in \Phi$ and $s \in S$. We say that $S$ is *transitive*, if there exists $\Phi \subset \mathrm{Aut}(G)$ such that $\Phi$ is $S$-preserving and acts transitively on $S$.

**Theorem 1** *Let $G$ be a group with a finite generating set $S$, and suppose there exists a finite $S$-preserving subgroup $\Phi \subset \mathrm{Aut}(G)$. Let us denote by $S_1, \ldots, S_n$ the partition of $S$ into orbits under $\Phi$. Let*

$$\alpha = \min_{i=1,\ldots,n} \left\{ \frac{|S_i|}{|S|} \right\}.$$

*Finally, let $\Gamma = \Gamma(G/H, S)$ be a finite Schreier graph with an eigenvalue gap $\beta$. Then*

$$\beta \geq \frac{\alpha K}{2}.$$

The result of Theorem 1 improves and generalizes the lower bound for the eigenvalue gap

$$\beta \, \geq \, \frac{K}{2\,|S|}$$

obtained in [15]. When $|S|$ is bounded, these lower bounds are essentially the same, but when (as often the case) the size of $S$ grows, while $S$ remains transitive, Theorem 1 gives a much sharper bound on the eigenvalue gap. We illustrate this in several cases of Cayley graphs of $S_n$ and $\mathrm{SL}(n, \mathbb{F}_q)$, where Theorem 1 is used to obtain sharp bounds on the eigenvalue gap and the mixing time of random walks on certain Cayley graphs. We also obtain a $\rho < 1 - \frac{c}{n^4}$ bound on the spectral radius $\rho$ of $\mathrm{SL}(n, \mathbb{Z})$, generated by elementary transvections (see section 6.)

The rest of the paper is constructed as follows. In the next section we present a new inequality for two variants of the Kazhdan constants. Then we elaborate on connection with the eigenvalue gap and prove Theorem 1. In section 4 we consider random walks on groups and mixing time. Section 5 is dedicated to examples. It is split into two subsections, dealing with Cayley graphs of $S_n$ and $\mathrm{SL}(n, \mathbb{F}_q)$, respectively. In the last section 6, we apply Theorem 1 to the analysis of product replacement algorithm. We conclude with final remarks.

# 2 Two Kazhdan constants

Let $G_0^*$ denote the space of unitary representations of $G$ with no invariant non-zero vectors. One can ask for the best constant in the inequality (1). For many applications it is also natural to consider the mean instead of the maximum over the generators $s \in S$ in the inequality (1). Thus we have two possible natural definitions of Kazhdan constants $K(G,S)$ and $\overline{K}(G,S)$:

$$\begin{aligned} K &= K(G,S) = \inf_{\pi \in G_0^*} \inf_{u \in \mathcal{H}_\pi} \max_{s \in S} \frac{\|\pi(s)u - u\|^2}{\|u\|^2} && (2) \\ \overline{K} &= \overline{K}(G,S) = \inf_{\pi \in G_0^*} \inf_{u \in \mathcal{H}_\pi} \frac{1}{|S|} \sum_{s \in S} \frac{\|\pi(s)u - u\|^2}{\|u\|^2}. && (3) \end{aligned}$$

In a general case one has the following estimate

$$K \geq \overline{K} \geq \frac{K}{|S|}. \tag{4}$$

But in some cases one can improve these inequalities. Namely:

**Proposition 1** *Let $G$ be a group generated by a finite set $S$ for which there exists a finite $S$-preserving subgroup $\Phi \subset \mathrm{Aut}(G)$ such that $\Phi$ acts transitively on $S$. Then*

$$K = \overline{K}.$$

**Proof** By (4), we have $\overline{K} \leq K$. Let us prove that $\overline{K} \geq K$. For $\varepsilon > 0$ let $\pi \in G_0^*$ and let $u \in \mathcal{H}_\pi$ be such that

$$\frac{\sum_{s \in S} \|u - \pi(s)u\|^2}{|S| \cdot \|u\|^2} \leq \overline{K} + \varepsilon.$$

Denote $N = |\Phi|$, and suppose $\Phi = \{\phi_1, \ldots, \phi_N\}$. Consider $\overline{\mathcal{H}} = \oplus_{i=1}^N \mathcal{H}_\pi$, a direct sum of $N$ copies of $\mathcal{H}$. Let $\overline{\pi} : G \to \mathcal{U}(\overline{\mathcal{H}})$ be a unitary representation defined as follows. For $\gamma \in G$ and $v = (v_1, \ldots, v_N) \in \oplus_{i=1}^N \mathcal{H}_\pi$, let

$$\overline{\pi}(\gamma)(v) = (\pi \circ \phi_1(\gamma) v_1, \ldots, \pi \circ \phi_N(\gamma) v_N).$$

It is clear that $\overline{\pi}$ has no invariant non-zero vectors. Let $\overline{u} = (u, \ldots, u) \in \overline{\mathcal{H}}$. We have:

$$\max_{s \in S} \frac{\|\overline{\pi}(s)\overline{u} - \overline{u}\|^2_{\overline{\mathcal{H}}}}{\|\overline{u}\|^2_{\overline{\mathcal{H}}}} = \max_{s \in S} \frac{\sum_{i=1}^N \|\pi \circ \phi_i(s)u - u\|^2_{\mathcal{H}}}{\sum_{i=1}^N \|u\|^2_{\mathcal{H}}}.$$

As the last expression does not depend on $s \in S$, we have

$$\max_{s\in S} \frac{\|\overline{\pi}(s)\overline{u} - \overline{u}\|^2_{\overline{\mathcal{H}}}}{\|\overline{u}\|^2_{\overline{\mathcal{H}}}} = \frac{\sum_{i=1}^N \|\pi \circ \phi_i(s)u - u\|^2_{\mathcal{H}}}{\sum_{i=1}^N \|u\|^2_{\mathcal{H}}} = \sum_{s\in S} \frac{\|\pi(s)u - u\|^2_{\mathcal{H}}}{|S| \cdot \|u\|^2_{\mathcal{H}}} \leq \overline{K} + \varepsilon,$$

which implies

$$K \leq \overline{K} + \varepsilon$$

and finishes the proof as $\varepsilon > 0$ can be arbitrarily small. □

Even if the subgroup $\phi \subset \mathrm{Aut}(G)$ does not act transitively on the generating subset $S$, in some cases one can still obtain nontrivial estimates. Namely:

**Proposition 2** *Let $G$ be a group generated by a finite set $S$ for which there exists a finite $S$-preserving subgroup $\Phi \subset \mathrm{Aut}(G)$. Let us denote by $S_1, \ldots, S_n$ the partition of $S$ into orbits under $\Phi$. Then*

$$\overline{K} \geq K \min_{i=1,\ldots,n} \left\{ \frac{|S_i|}{|S|} \right\}.$$

**Proof** For $\varepsilon > 0$ let $\pi \in G_0^*$ and let $u \in \mathcal{H}_\pi$ be such that

$$\frac{\sum_{s\in S} \|u - \pi(s)u\|^2}{|S| \cdot \|u\|^2} \leq \overline{K} + \varepsilon.$$

Let $\overline{\mathcal{H}} = \oplus_{i=1}^N \mathcal{H}_\pi$, $\overline{\pi} : G \to \mathcal{U}(\overline{\mathcal{H}})$ be as in the proof of Proposition 1. Again, it is clear that $\overline{\pi}$ has no invariant non-zero vectors. Let $\overline{u} = (u, \ldots, u) \in \overline{\mathcal{H}}$. Recall that

$$\max_{s\in S} \frac{\|\overline{\pi}(s)\overline{u} - \overline{u}\|^2_{\overline{\mathcal{H}}}}{\|\overline{u}\|^2_{\overline{\mathcal{H}}}} = \max_{s\in S} \frac{\sum_{i=1}^N \|\pi \circ \phi_i(s)u - u\|^2_{\mathcal{H}}}{\sum_{i=1}^N \|u\|^2_{\mathcal{H}}}.$$

The last expression does not depend on the generator $s \in S$ but only on the orbit $S_i$ that contains $s$. Let $s_1, \ldots, s_n$ be any representatives for the orbits $S_1, \ldots, S_n$. Then we have:

$$\begin{aligned}
\max_{s\in S} \frac{\|\overline{\pi}(s)\overline{u} - \overline{u}\|^2_{\overline{\mathcal{H}}}}{\|\overline{u}\|^2_{\overline{\mathcal{H}}}} &= \max_{i=1,\ldots,n} \sum_{s\in S_i} \frac{\|\pi(s)u - u\|^2_{\mathcal{H}}}{|S_i| \cdot \|u\|^2_{\mathcal{H}}} \\
&\leq \max_{i=1,\ldots,n} \sum_{s\in S} \frac{\|\pi(s)u - u\|^2_{\mathcal{H}}}{|S_i| \cdot \|u\|^2_{\mathcal{H}}} \\
&\leq \max_{i=1,\ldots,n} \left\{ \frac{|S|}{|S_i|} \right\} \sum_{s\in S} \frac{\|\pi(s)u - u\|^2_{\mathcal{H}}}{|S| \cdot \|u\|^2_{\mathcal{H}}} \\
&\leq \max_{i=1,\ldots,n} \left\{ \frac{|S|}{|S_i|} \right\} \left(\overline{K} + \varepsilon\right),
\end{aligned}$$

which implies

$$K \leq \max_{i=1,\ldots,n} \left\{ \frac{|S|}{|S_i|} \right\} \left(\overline{K} + \varepsilon\right).$$

Since as $\varepsilon > 0$ can be arbitrarily small, this completes the proof. □

## 3 The eigenvalue gap

As in the introduction, let $H \subset G$ be a subgroup of finite index. Consider a Schreier graph $\Gamma = \Gamma(G/H, S)$, and let $\beta = 1 - \lambda_1$ be the eigenvalue gap of $\Gamma$.

**Proposition 3** *Let $\Gamma = \Gamma(G/H, S)$ be a finite Schreier graph. Then $\beta \geq \overline{K}/2$.*

Different versions of the proposition can be found in [14, 15, 17, 19]. We present here a short proof for completeness.

**Proof** Let $\langle \cdot, \cdot \rangle$ denote the scalar product on the space of real functions on the Schreier graph $\Gamma$ with the weight $|S|$. Then the space $l^2_0(\Gamma)$ of functions orthogonal to constant functions, with the action of $\Gamma$ by the multiplication on the left, gives a unitary representation with no invariant vectors. Consider the (normalized) Laplace operator $\Delta$ on $l^2_0(\Gamma)$, i.e.

$$\Delta f(x) = f(x) - \frac{1}{|S|} \sum_{y \sim x} f(y),$$

where $f \in l^2_0(\Gamma)$, $x, y$ are vertices of $\Gamma$ and $x \sim y$ means that $x$ and $y$ are connected by an edge. Then

$$\begin{aligned}
2\beta &= \inf_{f \in l^2_0(\Gamma)} \frac{2\langle \Delta f, f \rangle}{\langle f, f \rangle} \\
&= \inf_{f \in l^2_0(\Gamma)} \frac{\sum_{s \in S} \sum_{\gamma \in \Gamma} |f(s\gamma) - f(\gamma)|^2}{\sum_{\gamma \in \Gamma} f^2(\gamma) |S|} \\
&= \inf_{f \in l^2_0(\Gamma)} \frac{1}{|S|} \sum_{s \in S} \frac{\sum_{\gamma \in \Gamma} |f(s\gamma) - f(\gamma)|^2}{\sum_{\gamma \in \Gamma} f^2(\gamma)} \\
&\geq \inf_{\pi \in G^*_0} \inf_{u \in \mathcal{H}_\pi} \frac{1}{|S|} \sum_{s \in S} \frac{\|\pi(s)u - u\|^2}{\|u\|^2} = \overline{K}.
\end{aligned}$$

□

From Proposition 3, one can immediately deduce Theorem 1, the main result of this paper:

**Proof of Theorem 1.** By Propositions 2, 3, we have:

$$\beta \geq \frac{\overline{K}}{2} \geq \left( \min_i \frac{|S_i|}{|S|} \right) \frac{K}{2} = \frac{\alpha K}{2}. \qquad \square$$

Now let us extend Proposition 3 to infinite Schreier graphs. Let $\Gamma = \Gamma(G/H, S)$ be an infinite Schreier graph of the group $G$ generated by a finite set $S$, $|S| = k$, and the subgroup $H$. Define a *spectral radius* $\rho = \rho(G/H, S)$ :

$$\rho = \lim_{n \to \infty} \left( \frac{a_n}{|S|} \right)^{1/n},$$

where $a_n$ is the number of loops of length $\leq n$ in $\Gamma$ starting and ending at id. Existence of the limit follows from submultiplicativity $a_{m+n} \leq a_m a_n$ (see e.g. [13]).

**Proposition 4** *Let* $\Gamma = \Gamma(G/H, S)$ *be an infinite Schreier graph. Then* $\rho \leq 1 - \overline{K}/2$.

**Proof** Denote by $\lambda_0$ the bottom of the spectrum of the Laplace operator $\Delta$ on $l^2(\Gamma)$. Then

$$\rho = 1 - \lambda_0.$$

The same argument as in the proof of Proposition 3 gives

$$\rho \leq 1 - \overline{K}/2.$$

□

Before we finish this section, let us note a relationship between the eigenvalue gap for Cayley graphs and Schreier graphs.

**Proposition 5** *Let $G$ be a finite group, and let $S$ be a generating set. Consider a Cayley graph* $\Gamma = \Gamma(G, S)$ *and a Schreier graph* $\Gamma_1 = \Gamma_1(G/H, S)$. *Then* $\beta(\Gamma) \leq \beta(\Gamma_1)$.

This proposition is well known in a much greater generality (see e.g. [2]).

# 4 Random walks on groups

Consider a finite group $G$ and a symmetric set of generators $S = S^{-1}$. Define a *random walk* $\mathcal{W} = \{X_t\}$ on $G$ as follows:

$$X_0 = \mathrm{id}, \quad X_{t+1} = X_t \cdot s,$$

where $s \in S$ is chosen uniformly and independently at each $t \geq 0$. One can think of $\mathcal{W}$ as of nearest neighbor random walk on the Cayley graph $\Gamma = \Gamma(G, S)$.

Denote by $\mathrm{Q}^t(g) = \mathbf{P}(X_t = g)$ the probability that the walk $\mathcal{W}$ is at $g$ at time $t$. Unless $\Gamma$ is bipartite, the walk $\mathcal{W}$ converges to a uniform distribution:

$$\mathrm{Q}^t(g) \to \frac{1}{|G|}, \quad \text{as} \ \ t \to \infty.$$

We define a *mixing time* $\mathbf{mix} = \mathbf{mix}(G, S)$ as follows:

$$\mathbf{mix} \ = \ \min \left\{ t : \mathrm{Q}^t(g) \geq \frac{1}{2\,|G|}, \ \ \forall g \in G \right\}.$$

We refer to [2] for this and other definitions of the mixing time.

From now on, to avoid periodicity problem, we consider only *lazy* random walks $\mathcal{W}_\circ = \widetilde{\mathcal{W}}(G, S)$ on $G$, defined as follows:

$$Y_0 = \mathrm{id}, \quad Y_{t+1} = Y_t \cdot s^\epsilon,$$

where $s \in S$ and $\epsilon \in \{0, 1\}$ are chosen uniformly and independently at each $t \geq 0$. One can define walk $\mathcal{W}_\circ = \{Y_t\}$ as a nearest neighbor random walk on $\Gamma = \Gamma(G, S)$, where before each step the walker flips a fair coin to decide whether to make this step or stay put.

By analogy with the classical case, we define the probability distribution $\mathrm{Q}^t_\circ$ and the mixing time $\mathbf{mix}_\circ$. It is well known and easy to see (see [2, 7, 21]) that

$$\frac{1}{2\beta(G,S)} < \mathbf{mix}_\circ(G, S) < \frac{16 \log |G|}{\beta(G,S)},$$

where $\beta = \beta(G, S)$ is the eigenvalue gap defined as above.

Finally, one can define a random walk $\mathcal{W} = \mathcal{W}(G/H, S)$ as a nearest neighbor random walk on the Schreier graph $\Gamma = \Gamma(G/H, S)$. The above definitions have a straightforward extension to this case.

**Corollary 1** *In condition of Theorem 1, for the mixing time* $\mathbf{mix}_\circ$ *of the lazy random walk* $\mathcal{W}_\circ = \mathcal{W}_\circ(G/H, S)$*, we have:*

$$\mathbf{mix}_\circ < \frac{32 \log |\Gamma|}{\alpha\, K}.$$

# 5 Examples

Computing or even estimating Kazhdan constants is a delicate matter, and has been done only in few special cases. Here we consider two special cases which seem of particular interest for applications.

## 5.1 Symmetric group and adjacent transpositions

Let $G = S_n$ be a symmetric group with a generating set

$$R_n = \{(1, 2), (2, 3), \ldots, (n-1, n)\}.$$

Very recently, in two subsequent papers [3, 4], Bacher and de la Harpe computed *exactly* the eigenvalue gap $\beta$ of the Cayley graph $\Gamma = \Gamma(S_n, R_n)$, and a Kazhdan constant $K = K(S_n, R_n)$:

$$\beta = \frac{2\left(1 - \cos\frac{\pi}{n}\right)}{(n-1)} = \frac{\pi^2}{n^3} + O\left(\frac{1}{n^4}\right), \quad \text{and} \quad K = \frac{24}{n^3 - n} = \frac{24}{n^3} + O\left(\frac{1}{n^4}\right).$$

Consider the biggest subgroup $\Phi \subset \mathrm{Aut}(S_n) = S_n$, such that $\Phi(R_n) = R_n$. Clearly, there exists only one nontrivial symmetry given by an involution $\omega = (n, n-1, \dots, 1) \in S_n$. Thus $|\Phi| = 2$ in this case. Now Theorem 1 gives us a poor estimate:

$$\beta \,\geq\, \frac{|\Phi|\, K}{2\,|R_n|} \,=\, \frac{24}{n^4} + O\left(\frac{1}{n^5}\right),$$

where $n$ is assumed to be odd so that each orbit has size $|\Phi| = 2$. On the other hand, we will show that Propositions 3 and 2 are virtually tight in a related case.

Consider a bigger generating set $R'_n = R_n \cup \{(1, n)\}$. By definition, the Kazhdan constant $K' = K(S_n, R'_n)$ satisfies $K' \geq K$. Since a group of cyclic transformations $\Phi \simeq \mathbb{Z}_n$ acts transitively on $R'_n$, we have:

$$\beta' \,\geq\, \frac{K'}{2} \,\geq\, \frac{K}{2} \,=\, \frac{12}{n^3} + O\left(\frac{1}{n^4}\right),$$

where $\beta'$ is the eigenvalue gap for the Cayley graph $\Gamma' = \Gamma(S_n, R'_n)$. This is even sharper than the estimate given by the comparison technique [8] in this case:

$$\beta' \,\geq\, \beta\, \frac{|R_n|}{|R'_n|} \,=\, \frac{\pi^2}{n^3} + O\left(\frac{1}{n^5}\right)$$

(note that $\pi^2 \approx 9.87 < 12$.) At the same time this is easily of the right order of magnitude as can be seen from the following argument.

Consider a Schreier graph $\Gamma_1 = \Gamma(S_n/S_{n-1}, R'_n)$, where $S_{n-1} = \mathrm{Stab}(1)$ acts by permuting elements $\{2, \dots, n\}$. Observe that $\Gamma_1 \simeq \Gamma(\mathbb{Z}_n, \{\pm 1, 0^{n-2}\}) = \Gamma_2$, i.e. a circle with $n-2$ loops at each vertex. By Proposition 5, we have $\beta' \leq \beta(\Gamma_1)$. Since

$$\beta(\mathbb{Z}_n, \{\pm 1\}) \,=\, 1 - \cos\frac{2\pi}{n} \,=\, \frac{2\pi^2}{n^2} + O\left(\frac{1}{n^4}\right),$$

we immediately have

$$\beta' \,\leq\, \beta(\Gamma_1) \,=\, \frac{2}{n}\,\beta(\mathbb{Z}_n, \{\pm 1\}) \,=\, \frac{4\pi^2}{n^3} + O\left(\frac{1}{n^5}\right).$$

Note here that $4\,\pi^2 \approx 39.48 > 12$.

Few words about random walks $\mathcal{W}_\circ = \mathcal{W}_\circ(S_n, R_n)$, $\mathcal{W}'_\circ = \mathcal{W}_\circ(S_n, R'_n)$, and the mixing times $\mathbf{mix}_\circ$ and $\mathbf{mix}'_\circ$, respectively. In this case, Corollary 1 gives only a bound $O(n^4 \log n)$ for both mixing times. On the other hand, a tight upper bound $O(n^3 \log n)$ can be proved in both cases by means of comparison technique [8] or a coupling argument [1]. A matching lower bound $\Omega(n^3 \log n)$ was recently obtained in [27].

### 5.2 Special linear group and transvections

Let $G = \mathrm{SL}(n, \mathbb{Z})$, and let $S = \{E_{i,j}^{\pm 1}, 1 \le i \ne j \le n\}$, where $E_{i,j}$ is a matrix with 1 on diagonal and at $(i,j)$, and 0 elsewhere. These matrices are called *elementary transvections*. It is known that $\langle S \rangle = G$ for $n > 2$ (see e.g. [20]).

In this special case Y. Shalom [26] recently obtained bounds on the Kazhdan constants $K = K\bigl(\mathrm{SL}(n, \mathbb{Z}), \{E_{i,j}^{\pm 1}\}\bigr)$, when $n \ge 3$ :

$$\frac{c_1}{n} > K > \frac{c_2}{n^4},$$

where $c_1, c_2 > 0$ are universal constants.

Now observe that a group of permutations $\Phi \simeq S_n$ acts on $\mathrm{SL}(n, \mathbb{Z})$ by permuting coordinates and has two orbits $O_1 = \{E_{i,j}\}$ and $O_1 = \{E_{i,j}^{-1}\}$ of the same size $n(n-1)$. Therefore, by Propositions 2 and 4, the spectral radius $\rho = \rho(\mathrm{SL}(n, \mathbb{Z}), S)$ satisfies

$$\rho \le 1 - \frac{\overline{K}}{2} \le 1 - \frac{K}{2 \cdot 2} < 1 - \frac{c_3}{n^4},$$

where $c_3 = c_2/4$ is also a universal constant. Although computation and estimates on the spectral radius has played a crucial role in the study of probability on (infinite) groups [13, 28], until now such an estimate was not possible to obtain.

Consider now a related case $G' = \mathrm{SL}(n, \mathbb{F}_q)$, with a generating set $S$ as above. The above estimates on Kazhdan constants for $SL(n, \mathbb{Z})$ hold also for $SL(n, \mathbb{F}_q)$ (see [26]). Therefore from Proposition 3 and above estimates, we immediately have:

$$\beta' = \beta\bigl(\mathrm{SL}(n, \mathbb{F}_q), S\bigr) > \frac{c_3}{n^4}.$$

It is interesting to compare this bound with a weaker bound obtained in [9] by different means:

$$\beta > \frac{1}{8\Delta^2} > \frac{c_4}{n^4 (\log q)^2},$$

where $\Delta = \Delta\bigl(\mathrm{SL}(n, \mathbb{F}_q), S\bigr)$, is the diameter of the Cayley graph $\Gamma'$. Here the first inequality follows from the conductance bound in this case (also called *isoperimetric* or *Cheeger inequality*), while the second follows from elementary arguments and expansion property of $\Gamma\bigl(\mathrm{SL}(2, \mathbb{F}_q), S\bigr)$ (see [9, 17] for details).

As for mixing time of the lazy random walk $\mathcal{W}_\circ = \mathcal{W}_\circ\bigl(\mathrm{SL}(n, \mathbb{F}_q), S\bigr)$, Corollary 1 and $\log |G| = n^2 \log q$ gives us

$$\mathbf{mix}_o \le c_5 n^6 \log q.$$

Again, it is interesting to compare this bound with that obtained in [9] by use of the comparison technique:

$$\mathbf{mix}_o \le c_6 n^4 (\log q)^3.$$

Since the two bounds are incomparable, and there seem to be no good lower bound, it is conceivable that one can combine the techniques to improve these bounds.

# 6 The product replacement algorithm

The product replacement algorithm (PRA) is a recent heuristic designed to generate random elements in finite groups [6, 22]. In its heart, the PRA consists of a simple random walk, called the product replacement random walk, on generating $k$-tuples of a finite group. In the recent years, there has been much effort to study this random walk and prove rigorous results about its mixing time (see e.g. [9, 10, 11, 18, 23]). Despite recent progress, the rapid mixing of this random walk remains a mystery.

In this section, we follow [18] to reformulate the problem in terms of the Schreier graphs. Then we show how Theorem 1 can be applied to obtain sharper bounds on the mixing time of the product replacement random walk.

The product replacement algorithm works as follows [6]: Given a finite group $G$, let $\daleth_k(G)$ be the set of $k$-tuples $(g) = (g_1, \dots, g_k)$ of elements of $G$ such that $\langle g_1, \dots, g_k \rangle = G$. We call elements of $\daleth_k(G)$ the *generating k-tuples.* Given a generating $k$-tuple $(g_1, \dots, g_k)$, define a *move* on it in the following way: choose uniformly a pair $(i, j)$, such that $1 \leq i \neq j \leq k$, then apply one of the following four operations with equal probability :

$$R^{\pm}_{i,j} \ : \ (g_1, \dots, g_i, \dots, g_k) \to (g_1, \dots, g_i \cdot g_j^{\pm 1}, \dots, g_k),$$

$$L^{\pm}_{i,j} \ : \ (g_1, \dots, g_i, \dots, g_k) \to (g_1, \dots, g_j^{\pm 1} \cdot g_i, \dots, g_k).$$

Note that these moves map a generating $k$-tuple into a generating $k$-tuple. Now apply these moves $t$ times and return a random component of the resulting generating $k$-tuple. This is the desired "random" element of the group $G$. Of course, here and below we assume that $k \geq d(G)$, where $d(G)$ is the minimum number of generators of $G$.

We shall think of $\daleth_k(G)$ as of a $4k(k-1)$-regular graph with vertices as above and edges corresponding to moves $R^{\pm}_{i,j}$ and $L^{\pm}_{i,j}$. Now the product replacement random walk can be defined as a nearest neighbor random walk on $\Gamma_k(G)$. The main problem in the subject is to determine the mixing time $\mathbf{mix}_\circ = \mathbf{mix}_\circ\big(\Gamma_k(G)\big)$. We refer to an extensive survey article [22] for a review on the mixing time, connectivity of $\Gamma_k(G)$, and other problems which arise in the analysis of PRA.

Following [18], consider the case when $G = F_k$. Then the moves $R^{\pm}_{i,j}, L^{\pm}_{i,j}$ are (a subset of) the Nielsen generators, and generate a subgroup $\mathrm{Aut}^+(F_k) \subset \mathrm{Aut}(F_k)$ of index two. Denote by $\Upsilon$ the set automorphisms of $F_k$ corresponding to $R^{\pm}_{i,j}, L^{\pm}_{i,j}$. Since $d(G) \leq k$, we have $\mathrm{Aut}^+(F_k)$ acts on $\daleth_k(G)$ with $\Upsilon$. Therefore, the graph $\daleth_k(G)$ is isomorphic to a Schreier graph of $\mathrm{Aut}^+(F_k)$:

$$\daleth_k(G) \simeq \Gamma(\mathrm{Aut}^+(F_k)/H, \Upsilon),$$

for some $H \subset \mathrm{Aut}^+(F_k)$.

The question whether $\mathrm{Aut}^+(F_k)$ (or, equivalently, $\mathrm{Aut}(F_k)$) has Kazhdan's property (T) is an open problem (see [17]). Assume this is true, i.e. suppose $K = K(\mathrm{Aut}^+(F_k), \Upsilon) > 0$. Observe that a permutation group $\Phi = S_k$ acts on $\mathrm{Aut}^+(F_k)$, and $\Upsilon$ has four orbits of the same size ($\alpha = 1/4$). Then by Theorem 1 we obtain:

$$\beta\bigl(\daleth_k(G)\bigr) \,\geq\, \frac{\alpha K}{2} \,\geq\, \frac{K}{8}.$$

While our assumption is by no means justified, in some special cases much progress been made. In [18] it was proved that a special group of automorphisms of a free nilpotent group of class $\ell - 1$ with at most $k$ generators $A(k,\ell) = \mathrm{Aut}^+(F_k/\gamma_\ell(F_k))$ has Kazhdan's property (T). Following [18], we observe that $\daleth_k(G) \simeq \Gamma\bigl(A(k,\ell)/H', \Upsilon'\bigr)$, where $\Upsilon'$ are the natural generators of $A(k,\ell)$, obtained by projection of $\Upsilon$. In a similar manner, we conclude that if $G$ is nilpotent, $d(G) < k$ and the nilpotency class $\ell(G) < \ell$, then

$$\beta\bigl(\daleth_k(G)\bigr) \,\geq\, \frac{K'}{8},$$

where $K' = K(A(k,\ell), \Upsilon') > 0$.

We should note that we need connectivity of $\daleth_k(G)$ for general groups. When $G$ is nilpotent and $k > d(G)$, this is known indeed (see [22] for proofs and references). Now, using the mixing time bound and $\log|\daleth_k(G)| < k \log|G|$, we get:

**Corollary 2** *Let $G$ be a nilpotent group of class $\ell(G) < \ell$, such that $d(G) < k$. Let $K = K\bigl(\mathrm{Aut}^+(F_k/\gamma_\ell(F_k)), \Upsilon'\bigr) > 0$ be the Kazhdan constant. Then the the mixing time $\mathbf{mix}_\circ$ of the lazy product replacement random walk on $\daleth_k(G)$ satisfies*

$$\mathbf{mix}_\circ < \, 256\, k\, \log|G|\, \frac{1}{K}. \quad \square$$

# 7 Final Remarks

The question of estimating Kazhdan constants goes back to J.-P. Serre, and to de la Harpe and Valette [14]. The difficulty of this task can be seen from the first breakthrough [5], where the Kazhdan constant for $\mathrm{SL}(3,\mathbb{Z})$ was estimated. Most recently, new advanced techniques were introduced [25, 26, 29]. Still, as of now, there are very few cases when the Kazhdan constant is estimated, and perhaps only two or three examples when it is computed exactly.

In the literature, many versions of the Kazhdan constants have been studied, with differences mostly due to various restrictions on representations considered in the definition. The notion of $\overline{K}$ seems to be new. It arose from an attempt to improve the inequality $\beta \geq \frac{K}{2\,|S|}$, obtained in [15]. Basically, Proposition 1 implies that $|S|$ is irrelevant when $S$ is a transitive set of generators. Roughly similar improvements are well known for the Cheeger (or isoperimetric) inequality [2]. Unfortunately, the straightforward 'averaging' idea used there can not be applied to Kazhdan constants.

The random walks on finite group are special cases of finite Markov chains, which are of intense interest in probability, computer science, statistical physics, etc. There are several different techniques and a large number of results regarding eigenvalue gap and mixing time, in this special case, as well as for general Markov chains [2, 7]. We hope that an approach based on Kazhdan's property (T) will grow to become an established technique for random walks on finite groups, very much as it became standard for creating expanders [17].

The product replacement algorithm is a practical heuristic which showed a remarkable performance in experiments [6]. Even sharp results, such as a recent polynomial bound on the mixing time (for $k = \Omega^*(\log |G|)$), seem to pale in comparison with the 'reality'. It was not until [18], that the mysterious rapid mixing received an explanation. Although the assumption that $\mathrm{Aut}(F_k)$ has Kazhdan't property (T) may be false, we remain optimistic that $\mathrm{Aut}(F_k)$ has property ($\tau$) for a certain family of normal subgroups [17], and thus the graphs $\beth_k(G)$ are expanders, when $k$ is fixed and $|G| \to \infty$.

**Acknowledgements**

We are grateful to Persi Diaconis, Alex Lubotzky, Gregory Margulis, Laurent Saloff-Coste and Yehuda Shalom for the interesting and helpful discussions on the subject. We thank an anonymous referee for pointing typos and historical comments.

The second author wishes to thank Cornell University for the hospitality in the Fall of 1999, when the results were discovered. The first author was partially supported by NSF Postdoctoral Research Fellowship.

# References

[1] D. Aldous, *Random walks on finite groups and rapidly mixing Markov chains*, Lecture Notes in Mathematics **986** (1983), 243–297.

[2] D. Aldous, J. Fill, *Reversible Markov Chains and Random Walks on Graphs*, monograph in preparation, 1996.

[3] R. Bacher, *Valeur propre minimale du laplacien de Coxeter pour le groupe symtrique*, J. Algebra **167** (1994), 460–472.

[4] R. Bacher, P. de la Harpe, *Exact values of Kazhdan constants for some finite groups*, J. Algebra **163** (1994), 495–515.

[5] M. Burger, *Kazhdan constants for $SL(3, \mathbb{Z})$*, J. Reine Angew. Math. **413** (1991), 36–67.

[6] F. Celler, C.R. Leedham-Green, S. Murray, A. Niemeyer, and E.A. O'Brien *Generating random elements of a finite group*, Comm. Alg. **23** (1995), 4931–4948.

[7] P. Diaconis, *Group Representations in Probability and Statistics*, IMS, Hayward, California, 1988.

[8] P. Diaconis, L. Saloff-Coste, *Comparison techniques for random walk on finite groups*, Ann. Probab. **21** (1993), 2131–2156.

[9] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of abelian groups*, Probability Theory Related Fields **105** (1996), 393–421.

[10] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. **134** (1998), 199–251.

[11] A. Gamburd, I. Pak, *Expansion of product replacement graphs*, preprint, 2001

[12] T. Gelander, A. Żuk, *Dependance of Kazhdan constants on generating subsets*, Israel J. Math. (to appear).

[13] R. Grigorchuk, P. de la Harpe, *On problems related to growth, entropy, and spectrum in group theory*, J. Dynam. Control Systems **3** (1997), 51–89.

[14] P. de la Harpe, A. Valette, *La propriété (T) de Kazhdan pour les groupes localement compacts*, Astérisque, **175**, 1989.

[15] P. de la Harpe, A.G. Robertson, A. Valette, *On the spectrum of the sum of generators for a finitely generated group*, Israel J. Math., **81** (1993), 65–96.

[16] D. Kazhdan, *Connection of the dual space of a group with the structure of its closed subgroups*, Funct. Anal. and its Appl. **1** (1967), 71–74.

[17] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhäuser, 1994.

[18] A. Lubotzky, I. Pak, *The product replacement algorithm and Kazhdan's property (T)*, Journal of AMS **52** (2000), 5525–5561.

[19] G. A. Margulis, *Explicit constructions of expanders*, Problems of Information Transmission, **9** (1973), 325–332.

[20] J. Milnor, *Introduction to algebraic $K$-theory*, Annals of Mathematics Studies, No. 72, Princeton University Press, 1971.

[21] I. Pak, *Random walks on groups: Strong uniform time approach*, Ph.D. Thesis, Harvard University, 1997.

[22] I. Pak, *What do we know about the product replacement algorithm?*, in "Groups and Computation III" (W. Kantor, A. Seress, eds.), de Gruyter, Berlin, 2001, 301–347.

[23] I. Pak, *The product replacement algorithm is polynomial*, in Proc. FOCS'2000, IEEE, 476–485.

[24] L. Saloff-Coste, *Lectures on finite Markov chains*, in *Lectures on probability theory and statistics* (Saint-Flour, 1996), 301–413, Lecture Notes in Math. **1665**, Springer, Berlin, 1997.

[25] Y. Shalom, *Explicit Kazhdan constants for representations of semisimple and arithmetic groups*, Annales de L'Institut Fourier **50** (2000), 833–863.

[26] Y. Shalom, *Bounded generation and Kazhdan's property (T)*, Publ. Math. IHES **90** (1999), 145–168.

[27] D. Wilson, *Mixing times of lozenge tiling and card shuffling Markov chains*, manuscript.

[28] W. Woess, *Random walks on infinite graphs and groups*, Cambridge University Press, Cambridge, 2000.

[29] A. Żuk, *Property (T) and Kazhdan constants for discrete groups*, preprint.