JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
S 0894-0347(00)00356-8
Article electronically published on October 18, 2000

THE PRODUCT REPLACEMENT ALGORITHM AND KAZHDAN'S PROPERTY (T)

ALEXANDER LUBOTZKY AND IGOR PAK

Introduction

A problem of great importance in computational group theory is to generate (nearly) uniformly distributed random elements in a finite group G. A good example of such an algorithm should start at any given set of generators, use no prior knowledge of the structure of G, and in a polynomial number of group operations return the desired random group elements (see [Bb2]). Then these random elements can be used further to determine the structure of G.

In a pioneer paper [Bb1] Babai found such an algorithm which provably generates (nearly) uniformly distributed random elements in $O(\log^5 |G|)$ group multiplications, too many for practical applications. A different heuristic, the *"product replacement algorithm"*, was designed by Leedham-Green and Soicher [LG], and studied by Celler et al. in [CLMNO]. In spite of the fact that very little theoretical justification was known, practical experiments showed excellent performance. So, it quickly became the most popular "practical" algorithm to generate random group elements, and was included in the two most frequently used group algebra packages GAP ([Sc]) and MAGMA ([BCP]).

A systematic and quantitative approach was carried out by Diaconis and Saloff-Coste [DS1], [DS2] (see also [Bb2], [CG]), but their results did not reveal the mystery of the truly outstanding performance of the algorithm. The aim of this paper is to propose a conceptual explanation based on Kazhdan's property (T) from representation theory of Lie groups and to improve some of the previous estimates on the running time.

The product replacement algorithm works as follows ([CLMNO]): Given a finite group G, let $\Gamma_k(G)$ 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 $\Gamma_k(G)$ 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 $1 \le i \ne j \le k$, then apply one of the following four operations with equal probability:

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

Received by the editors January 5, 2000 and, in revised form, August 23, 2000.
2000 *Mathematics Subject Classification.* Primary 60B15; Secondary 05C25, 22D10, 60J10.
Key words and phrases. Random walks on groups, Kazhdan's property (T), nilpotent groups.

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.

Another way to describe the algorithm is to define on $\Gamma_k(G)$ a structure of a graph induced by maps $R_{i,j}^{\pm}$ and $L_{i,j}^{\pm}$. This turns $\Gamma_k(G)$ into a $4k(k-1)$-regular graph with no orientation on edges, but with loops when $k > d(G)$, where $d(G)$ is the minimal number of generators of G. Now the algorithm consists of running a nearest neighbor random walk on this graph (for t steps) and returning a random component. We refer to this random walk as the *product replacement random walk*. By abuse of notation, we denote this graph $\Gamma_k(G)$ as well.

Our work grew from the following observation: Let F_k be the free group on k generators $x_1, \ldots, x_k$. For every group G, the set $\Gamma_k(G)$ can be identified with $\mathrm{Epi}(F_k, G)$ — the set of epimorphisms from F_k onto G. Now, the group $A = \mathrm{Aut}(F_k)$ acts on $E = \mathrm{Epi}(F_k, G)$ in the following way: If $\alpha \in A$ and $\varphi \in E$, $\alpha(\varphi) = \varphi \cdot \alpha^{-1}$. Moreover the moves $R_{i,j}^{\pm}$ and $L_{i,j}^{\pm}$ defined above correspond to Nielsen moves[1] on $\Gamma_k(F_k)$. Each such move on $\Gamma_k(F_k)$ defines an automorphism of F_k. Let $A^+ \leq A$ be a subgroup generated by these automorphisms. Following [Ge], we call A^+ the *special automorphism group* of F_k. It is of index two in A (see Proposition 1.2 below), and the projection of A^+ to $GL_k(\mathbb{Z}) = \mathrm{Aut}(F_k/[F_k, F_k])$ is exactly $SL_k(\mathbb{Z})$.

Now one can deduce from here that $\Gamma_k(G)$ are quotient graphs of the Cayley graph of A^+ with respect to the generators $R_{i,j}^{\pm}$ and $L_{i,j}^{\pm}$.

A longstanding conjecture asserts that $A = \mathrm{Aut}(F_k)$ (at least for k large enough, say $k \geq 4$) has Kazhdan's property (T) (see §2 for a definition). The same therefore applies to A^+. Now, if this is the case, then by a fundamental result of Margulis, the finite quotient graphs of the Cayley graph of A^+ are expanders (see §2 for a definition). This would imply that $\Gamma_k(G)$ are expanders. Random walks on expanding graphs mix very rapidly. This would explain the outstanding performance of the product replacement algorithm.

Formulating the above in precise terms we get:

Theorem 1. $\mathrm{Aut}(F_k)$ *(or equivalently* $A^+(F_k)$*) has Kazhdan's property (T). Then for every finite group* G *generated by* k *elements, the mixing time* $\mathrm{mix}_{(g)}$ *of the lazy random walk starting at* (g) *on a connected component* $\Gamma' \subset \Gamma_k(G)$*,* $(g) \in \Gamma'$*, is bounded as*

$$\mathrm{mix}_{(g)} = C(k) \log |G|,$$

where $C(k)$ *depends only on* k*.*

By a *"lazy"* product replacement random walk we mean a random walk on a graph $\Gamma_k(G)$ in which with probability $1/2$ we stay put and with probability $1/2$ we move to a neighbor. This is a technical condition which enables us to avoid the periodicity problem (see §2 below).

It is not clear how well founded the conjecture is that $\mathrm{Aut}(F_k)$ has (T) (see the discussion in §5). We prove some partial results in this direction.

Let W be a characteristic subgroup of F_k. There is a natural homomorphism $\pi : \mathrm{Aut}(F_k) \to \mathrm{Aut}(F_k/W)$. Denote $\pi(A^+)$ by $A^+(F_k/W)$, and call it the special automorphism group of F_k/W. For general W the group $A^+(F_k/W)$ can have an infinite index in $\mathrm{Aut}(F_k/W)$.

[1] To be precise, they correspond to a subset of Nielsen moves.

Theorem 1′. *If the special automorphism group $A^+(F_k/W)$ has (T), then the conclusion of Theorem 1 is satisfied for every finite quotient G of F_k/W.*

We indeed prove that in a number of interesting cases the special automorphism group has (T). For example, if W is the commutator subgroup of F_k, then $A^+(F_k/W)$ is $SL_k(\mathbb{Z})$ which indeed has (T) if $k \geq 3$. Moreover, the Nielsen moves are projected to the elementary matrices for which Shalom [Sh2] estimated the Kazhdan constant. We can deduce:

Theorem 2. *Let G be an abelian group, let $(g) = (g_1, \ldots, g_k)$ be the initial generating k-tuple, and let $\Gamma' \subset \Gamma_k(G)$ be a connected component containing (g). Then for the mixing time of the lazy product replacement random walk starting at (g), we have*

$$\operatorname{mix}_{(g)} \leq C \cdot k^5 \cdot \log |G|,$$

where C is a universal constant.

A similar result was proved in [DS1] for groups of the form $(\mathbb{Z}_p)^m$, where p is a prime. A somewhat more general but weaker version was announced by the second named author in [P1], [PB].

The following result is a generalization of Theorem 2 to nilpotent groups of fixed class:

Theorem 3. *Let $W = \gamma_{i+1}(F_k)$, where $\gamma_{i+1}(F_k)$ is the $(i+1)$-th term of the lower central series of F_k. Then $A^+(F_k/W)$ has (T) for every $k \geq 3$. Hence for a fixed k and i and any nilpotent group G of class at most i we have*

$$\operatorname{mix}_{(g)} \leq C(k,i) \cdot \log |G|,$$

where $\operatorname{mix}_{(g)}$ is the mixing time of the lazy product replacement random walk starting at $(g) \in \Gamma_k(G)$ on a connected component $\Gamma' \subset \Gamma_k(G)$, $\Gamma' \ni (g)$.

In other words, the mixing time is linear in $\log |G|$. This should be compared with [DS2], where only a subexponential bound (in $\log |G|$) is given under the same assumptions. The behavior of the constants $C(k,i)$ in Theorem 3 and $C(k)$ in Theorem 1 are intimately connected with computing Kazhdan constants. Estimating Kazhdan constants is usually a very difficult problem, but a breakthrough was made recently by Shalom [Sh1], [Sh2]. See §5 for a discussion.

The paper is organized as follows. In §1 we define the graph Γ_k and look at some of its functorial properties. In §2 we define the mixing time and relate it to the Kazhdan constant and the eigenvalue gap. In §3 we prove Theorem 2 by showing that graphs $\Gamma_k(G)$ are expanders when G is abelian. In §4 we prove Theorem 3 by showing that $A^+\big(F_k/\gamma_{i+1}(F_k)\big)$ has property (T). We finish with concluding remarks in §5.

1. The graph $\Gamma_k(G)$

Let G be a group and $k \geq d(G)$. Consider $\Gamma_k(G)$ to be the set of all k-tuples of generators $(g_1, \ldots, g_k)$ of G. We define a structure of graphs on $\Gamma_k(G)$ by connecting $(g_1, \ldots, g_k)$ to $(g_1, \ldots, g_i g_j^{\pm 1}, \ldots, g_k)$ and to $(g_1, \ldots, g_j^{\pm 1} g_i, \ldots, g_k)$ for every (i,j), $1 \leq i, j \leq k$, $i \neq j$. This turns $\Gamma_k(G)$ into a $4k(k-1)$-regular oriented graph (with possibly loops and multiple edges).

Let us note that the graphs $\Gamma_k(G)$ are not necessarily connected. In fact, the graphs $\Gamma_k(G)$ for $k = d(G)$ can have an arbitrarily large number of connected

components (see [DG], [P3]). It is not hard to see that $\Gamma_k(G)$ is connected when G is abelian and $k \geq d(G) + 1$ (see [DG], [P3]). Further, Dunwoody [Du2] showed that if G is a finite solvable group and $k \geq d(G) + 1$, then $\Gamma_k(G)$ is connected. A longstanding conjecture of Wiegold[2] asserts that $\Gamma_k(G)$ is connected for every simple group if $k \geq 3$. In a pioneering paper [Gi] Gilman proves the Wiegold conjecture for $G = PSL_2(p)$. Also, M. Evans confirms the conjecture for $G = PSL(2, 2^m)$ and Suzuki groups $Sz(2^{2m-1})$, where $m \geq 2$ (see [P3] and references therein).

One way to get around the connectivity problem was found by the second named author in [P2], where it was shown that for large simple groups G the graphs $\Gamma_k(G)$, $k \geq 3$, have "large" connected components (see [P2], [P3] for details). Then the random walk on the "large" connected component suffices for the purposes of the algorithm.

While our main interest is in $\Gamma_k(G)$ for finite groups G, it is of interest to look at the following example:

Example 1.1. Let $F = F_k$ be the free group on k generators $x_1, \ldots, x_k$, and let $R^{\pm}_{i,j}$, $L^{\pm}_{i,j}$ be the following automorphisms of F_k:

$$R^{\pm}_{i,j}(x_i) = x_i x_j^{\pm 1} \quad \text{and} \quad R^{\pm}_{i,j}(x_l) = x_l \quad \text{if } l \neq i,$$
$$L^{\pm}_{i,j}(x_i) = x_j^{\pm 1} x_i \quad \text{and} \quad R^{\pm}_{i,j}(x_l) = x_l \quad \text{if} \quad l \neq i.$$

We will call these automorphisms the *Nielsen moves* (see [MKS]). A classical result of Nielsen (see [MKS]) shows that $\mathrm{Aut}(F_k)$ is generated by the Nielsen moves and elementary automorphisms of permutation and inversion of generators.

Proposition 1.2. *Let $A^+(F_k)$ be the subgroup of $\mathrm{Aut}(F_k)$ generated by Nielsen moves. Then $A^+(F_k)$ is a normal subgroup of index two in $\mathrm{Aut}(F_k)$.*

This proposition seems to be well known (cf. [Ge]). Here is an easy proof.

Proof. Let $A^+(F_k)$ be the subgroup of $\mathrm{Aut}(F_k)$ generated by Nielsen moves. Let us show that $A^+(F_k)$ is a normal subgroup of index two in $\mathrm{Aut}(F_k)$.

Indeed, consider the automorphisms $T_{i,j} = L^-_{i,j} \cdot L^+_{i,j} \cdot R^-_{i,j}$, which act on F_k as follows:

$$T_{i,j} \,:\, x_i \to x_j^{-1},\ x_j \to x_i,\ x_l \to x_l, l \neq i, j\,.$$

Note also that

$$T^2_{i,j} \,:\, x_i \to x_i^{-1},\ x_j \to x_j^{-1},\ x_l \to x_l,\ l \neq i, j\,.$$

Thus the automorphisms $T_{i,j}$ generate a subgroup of index two in a hyperoctahedral group $H_k \simeq S_k \ltimes \mathbb{Z}_2^k$ of all permutations and inversion of variables.

By Nielsen's theorem, one can obtain any generating k-tuple $(y) = (y_1, \ldots, y_k) \in \Gamma_k(F_k)$ from $(x_1, \ldots, x_k)$ by Nielsen moves, transpositions $x_i \leftrightarrow x_j$ and inversions $x_i \to x_i^{-1}$. Now apply the same Nielsen moves, and use $T_{i,j}$ instead of transpositions, and $T^2_{i,j}$ instead of inversions. It is easy to see that one can obtain an element $(y_1, \ldots, y_{k-1}, y_k)$ or $(y_1, \ldots, y_{k-1}, y_k^{-1})$ by such moves. This immediately implies that $A^+(F_k)$ is of index at most two in $\mathrm{Aut}(F_k)$.

[2]The Wiegold conjecture is formulated in terms of the so-called T-systems. We present here a modified version of the conjecture. We refer to [P3] for a connection and references.

Now consider a natural projection $\pi : \mathrm{Aut}(F_k) \to \mathrm{Aut}(F_k/[F_k, F_k]) \simeq GL_k(\mathbb{Z})$. Observe that $\pi(R^{\pm}_{i,j}) = \pi(L^{\pm}_{i,j}) \in SL_k(\mathbb{Z})$ and corresponds to elementary transvections, for all $i \neq j$. Therefore $\pi(A^+) = SL_k(\mathbb{Z})$ and A^+ has index exactly two in $\mathrm{Aut}(F_k)$. □

Proposition 1.3. *The graph $\Gamma_k(F_k)$ has two connected components. Each of them is isomorphic to the right Cayley graph of the special automorphism group $A^+(F_k)$ with respect to the Nielsen moves.*

Indeed, $\mathrm{Aut}(F_k)$ acts simply transitively on the vertices of $\Gamma_k(F_k)$. This gives a one to one correspondence ι between $\mathrm{Aut}(F_k)$ and $\Gamma_k(F_k)$ defined as

$$\iota : \alpha \in \mathrm{Aut}(F_k) \to (\alpha(x_1), \ldots, \alpha(x_k)).$$

It is easy to see that $\alpha R^{\pm}_{i,j}$ and $\alpha L^{\pm}_{i,j}$ correspond to the neighbors of $\iota(\alpha) \in \Gamma_k(G)$. This shows that $\Gamma_k(F_k)$ is the Cayley graph of $\mathrm{Aut}(F_k)$ with respect to the Nielsen moves. As they do not generate the group but rather a subgroup of index two, the graph $\Gamma_k(F_k)$ has two connected components, each one isomorphic to $\mathrm{Cayley}\big(A^+(F_k); \{R^{\pm}_{i,j}, L^{\pm}_{i,j}\}\big)$.

Let H and G be two groups and φ an epimorphism from H onto G. Then φ induces a map $\Gamma_k(\varphi) : \Gamma_k(H) \to \Gamma_k(G)$, where

$$\Gamma_k(\varphi) \,:\, (h_1, \ldots, h_k) \,\to\, (\varphi(h_1), \ldots, \varphi(h_k))\,,$$

provided that $\Gamma_k(H)$ is not empty, i.e. when $k \geq d(H)$. It is easy to see that $\Gamma_k(\varphi)$ is a *morphism* (projection) of graphs which preserve adjacency relations.

Proposition 1.4. *If $\varphi : H \to G$ is an epimorphism between* finite *groups, then $\Gamma_k(\varphi)$ is a surjective morphism provided $k \geq d(H)$.*

The assertion of surjectivity of $\Gamma_k(\varphi)$ is equivalent to the following proposition known as the Gaschütz Lemma:

Proposition 1.5 (Gaschütz)**.** *Let $\varphi : H \to G$ be an epimorphism between finite groups, let $k \geq d(H)$, and let $(g_1, \ldots, g_k)$ be a generating k-tuple of G. Then there exists a generating k-tuple $(h_1, \ldots, h_k)$ of H with $\varphi(h_i) = g_i$ for $i = 1, \ldots, k$.*

The proof of the Gaschütz Lemma can be found in [Gr] (Proposition 6.14, p.39). Note that it immediately implies the following:

Corollary 1.6. *If $\varphi : H \to G$ is an epimorphism between two finite groups and $k \geq d(H)$, then the number of connected components of $\Gamma_k(G)$ is bounded by that of $\Gamma_k(H)$.*

It should be noted however that Propositions 1.4 and 1.5 and Corollary 1.6 do not hold when $H = F_k$. In fact, $\Gamma_k(F_k)$ has two connected components while it is known that there are finite groups with an arbitrary number of components in $\Gamma_k(G)$ (see [Du1], [DG]). Let us remark that the connected components measure to what extend the Gaschütz Lemma holds for $\varphi : F_k \to G$. We have:

Proposition 1.7. *Let $\varphi : F_k \to G$ be an epimorphism. Let $(g) \in \Gamma_k(G)$ and $(g) = (\varphi(x_1), \ldots, \varphi(x_k))$, and suppose (g) and $(g') \in \Gamma_k(G)$, $(g') = (g'_1, \ldots, g'_k)$, lie in the same connected component of $\Gamma_k(G)$. Then there exist $(y_1, \ldots, y_k) \in \Gamma_k(F_k)$ which lie in the same connected component of $\Gamma_k(F_k)$ as $(x_1, \ldots, x_k) \in \Gamma_k(F_k)$, and such that $\varphi(y_i) = g'_i$ for every $i = 1, \ldots, k$.*

Proof. By connectivity, (g') is obtained from (g) by an application of a series of Nielsen moves $R_{i,j}^{\pm}$ and $L_{i,j}^{\pm}$ on $\Gamma_k(G)$. Apply the same sequence to $(x_1, \ldots, x_k)$ to get the desired $(y_1, \ldots, y_k)$. □

We call a projection of graph X *onto* Y which preserves a graph structure a *morphism* $\psi : X \to Y$ of graphs X, Y, i.e. maps adjacent vertices into adjacent vertices.

Corollary 1.8. *Let $X = \mathrm{Cayley}(A^+(F_k); \{R_{i,j}^{\pm}, L_{i,j}^{\pm}\})$ be the Cayley graph of $A^+(F_k)$ with respect to the Nielsen generators. Then for every G and every connected component Y of $\Gamma_k(G)$, there exists a graph morphism $\psi : X \to Y$.*

The above morphism can also be defined as follows. Identify $\Gamma_k(G)$ with the set $\mathrm{Epi}(F_k, G)$ of all epimorphisms $\varphi : F_k \twoheadrightarrow G$, where an epimorphism φ is identified with $(\varphi(x_1), \ldots, \varphi(x_k))$. Then $A = \mathrm{Aut}(F_k)$ acts on $E = \mathrm{Epi}(F_k, G)$ by: $\alpha(\varphi) = \varphi \circ \alpha^{-1}$ for $\alpha \in \mathrm{Aut}(F_k)$ and $\varphi \in E$. Fix $\varphi : F_k \to G$ and let B be the subgroup of $A^+ = A^+(F_k)$ defined as $B = \{\alpha \in A^+ \,|\, \alpha(\varphi) = \varphi\}$. Then A^+/B is naturally identified with the connected component of $(g) = (\varphi(x_1), \ldots, \varphi(x_k))$ in $\Gamma_k(G)$. Indeed, if $\alpha_1, \alpha_2 \in A^+$, then $\alpha_1 B = \alpha_2 B$ if and only if $\alpha_1(\varphi) = \alpha_2(\varphi)$. Moreover, $\big[R_{i,j}^{\pm} \circ \alpha\big](\varphi)$ and $\big[L_{i,j}^{\pm} \circ \alpha\big](\varphi)$ are exactly the neighbors of $\alpha(\varphi)$. We conclude:

Corollary 1.9. *For every G and every $(g) \in \Gamma_k(G)$, the connected component of (g) in $\Gamma_k(G)$ is isomorphic to the Schreier graph of the special automorphism group $A^+(F_k)$ with respect to the Nielsen moves and modulo some finite index subgroup of $A^+(F_k)$.*

Here the *Schreier graph* is the quotient of the left Cayley graph of $A^+(F_k)$ by the subgroup B defined above.

For later purposes, we need to generalize our results from free groups to "relatively free groups".

Let W be a characteristic subgroup of F_k, i.e. $\alpha(W) = W$ for every $\alpha \in \mathrm{Aut}(F_k)$. There is a natural homomorphism $\pi : \mathrm{Aut}(F_k) \to \mathrm{Aut}(F_k/W)$. Denote $\pi(A^+(F_k))$ by $A^+(F_k/W)$, and call it the special automorphism group of F_k/W. Note that in general π is not necessarily an epimorphism, so $A^+(F_k/W)$ can be of large (even infinite) index in $\mathrm{Aut}(F_k/W)$. Still, the Nielsen moves generate $A^+(F_k/W)$ and we have a slight generalization of Corollary 1.9.

Proposition 1.10. *Let W be a characteristic subgroup of F_k and let G be a finite quotient of F_k/W. Then every component of $\Gamma_k(G)$ is a Schreier graph of $A^+(F_k/W)$ with respect to the Nielsen moves and modulo some finite index subgroup of $A^+(F_k/W)$.*

Example 1.11. Let $W = [F_k, F_k]$ be the commutator subgroup of F_k. Then $\mathrm{Aut}(F_k/W) = GL_k(\mathbb{Z})$ and $A^+(F_k/W) = SL_k(\mathbb{Z})$. The Nielsen moves $R_{i,j}^{\pm}$ and $L_{i,j}^{\pm}$ give the elementary matrices $E_{i,j}^{\pm}$ with 1's along the diagonal, ± 1 at the (i, j) entry, and 0 elsewhere. We therefore conclude:

Proposition 1.12. *Let G be a finite abelian graph. Then any connected component of $\Gamma_k(G)$ is a Schreier graph of $SL_k(\mathbb{Z})$ with respect to the elementary matrices $E_{i,j}^{\pm}$ (each appears twice) modulo a finite index subgroup of $SL_k(\mathbb{Z})$.*

Remark 1.13. It is not difficult to see that a finite index subgroup of $SL_k(\mathbb{Z})$ in Proposition 1.12 is a congruence subgroup containing $\mathrm{Ker}\big(SL_k(\mathbb{Z}) \to SL_k(\mathbb{Z}/m\mathbb{Z})\big)$,

where $m = \exp(G)$ is the smallest number l s.t. $l \cdot a = 0$ for every $a \in G$. Clearly, m divides $|G|$. Recall also that $\Gamma_k(G)$ is connected when $k \geq d(G) + 1$.

Example 1.14. Define the lower central series of F_k by $\gamma_1(F_k) = F_k$ and $\gamma_{i+1}(F_k) = [F_k, \gamma_i(F_k)]$. Let $W = \gamma_{i+1}(F_k)$, so F_k/W is the "free nilpotent group of class i". Let $A^+(F_k/W)$ and $\mathrm{Aut}(F_k/W)$ be as above. It is known that when $k \geq 2$ and $i \geq 4$, $A^+(F_k/W)$ is of infinite index in $\mathrm{Aut}(F_k/W)$ (see [An], [Bh]). Nevertheless, we still have that for every nilpotent group G of class i, every connected component of $\Gamma_k(G)$ is a quotient of the Cayley graph of $A^+(F_k/W)$ with respect to the Nielsen moves.

2. Mixing time, expanders and Kazhdan's property (T)

Recall the definition of the product replacement random walk from the introduction: We start at some given generating k-tuple $(g) = (g_1, \ldots, g_k)$ and at each step apply a random move $R_{i,j}^{\pm}$ or $L_{i,j}^{\pm}$. Recall also that this walk can be defined as a random walk on the graph $\Gamma_k(G)$ (see §1). In this section we do not consider the question of whether $\Gamma_k(G)$ is connected, but rather concentrate on the mixing time of the walk on a connected component Γ' which contains (g). Note that by definition $\Gamma' \subset \Gamma_k(G)$ must also be a $4k(k-1)$-regular graph.

Let Γ be a connected d-regular simple graph (edges are unoriented, but loops and multiple edges are allowed). Assume also that Γ is not bipartite, for example it has at least one loop. Fix a vertex $v \in \Gamma$ and denote by Q_v^t the probability distribution of the nearest neighbor random walk $\mathcal{W} = \mathcal{W}(\Gamma, v)$ on Γ starting at v after t steps. Since Γ is connected and non-bipartite, the random walk has a stationary distribution, which is uniform since Γ is regular:

$$Q_v^t(w) \to \frac{1}{|\Gamma|}, \quad \text{as} \quad t \to \infty, \quad \text{for all} \ w \in \Gamma.$$

Recall the definition of the *total variation distance*:

$$\|P - Q\|_{\mathrm{tv}} = \max_{B \subset \Gamma} |P(B) - Q(B)| \ = \ \frac{1}{2} \sum_{w \in \Gamma} \big|P(w) - Q(w)\big|,$$

where P, Q are two probability distributions on Γ. By U we denote a uniform distribution. Now define a *mixing time* mix_v of the random walk $\mathcal{W}$ as follows:

$$\mathrm{mix}_v \ = \ \min \left\{ t \,|\, \|Q_v^t(w) - U\|_{\mathrm{tv}} < \frac{1}{e} \right\}.$$

In this section we present (mostly classical) bounds on the mixing times via spectral and isoperimetric properties of Γ.

Denote by A the adjacency matrix of the graph Γ and let $\mathcal{P} = \frac{1}{d}A$ be the transition matrix of the random walk $\mathcal{W}$. Let $n = |\Gamma|$ and let

$$1 = \beta_0(\mathcal{P}) > \beta_1(\mathcal{P}) \geq \cdots \geq \beta_{n-1}(\mathcal{P}) > -1$$

be the eigenvalues of $\mathcal{P}$. Denote $\beta(P) = \max\{|\beta_1(\mathcal{P})|, |\beta_{n-1}(\mathcal{P})|\}$. A classical and easy bound on the variation distance gives:

$$\|Q_v^t - U\|_{\mathrm{tv}} \ \leq \ \frac{\sqrt{|X|}}{2} \beta(\mathcal{P})^t.$$

From here we immediately have $\mathrm{mix}_v < C(\beta) \log |\Gamma|$. More precisely:

Proposition 2.1. *Let $\alpha(\Gamma) = 1-\beta_1(\Gamma)$ be the spectral gap of Γ. Then for the total variation distance $\|Q_v^t - U\|_{\text{tv}}$, $v \in \Gamma$, of the random walk $\mathcal{W}$ on Γ we have:*

$$\|Q_v^t - U\|_{\text{tv}} \le e^{-c}, \quad \textit{for} \quad t \ge \frac{\log|\Gamma| + c}{\min\{\alpha, \beta_{n-1}+1\}}.$$

In particular, for the mixing time mix_v *we have:*

$$\text{mix}_v \ \le \ \frac{1}{\min\{\alpha, \beta_{n-1}+1\}} \ (\log|\Gamma| + 1).$$

Now recall the definition of the *lazy* random walk $\mathcal{W}'$ (see e.g. [Ch]) which is a random walk on Γ which with probability $1/2$ stays and with probability $1/2$ moves to a uniform neighbor. An easy argument shows that

$$\text{mix}'_v \le 2\,\text{mix}_v,$$

where mix' is the mixing time of $\mathcal{W}'$ (see e.g. [Bb1], [Ch]). This implies that by making the walk lazy we can slow the walk by the factor at most 2, but sometimes, of course, can speed it up if the gap $|\beta_{n-1} - (-1)|$ is small.

Now observe that the transition matrix becomes $P' = \frac{1}{2}(P + Id)$, and for the eigenvalues we have $\beta_1(P') = (\beta_1(P)+1)/2$, $\beta_{n-1}(P') \ge 0$. Thus we have $\beta(P') = \beta_1(P')$ and $\alpha(P') = \alpha(P)/2$. We conclude:

Proposition 2.1′. *Let $\alpha(\Gamma) = 1-\beta_1(\Gamma)$ be the spectral gap of Γ. Then for all $c > 0$ the total variation distance $\|Q_v^t - U\|_{\text{tv}}$, $v \in \Gamma$, of the lazy random walk $\mathcal{W}$ on Γ satisfies:*

$$\|Q_v^t - U\|_{\text{tv}} \le e^{-c}, \quad \textit{for} \quad t \ge \frac{2\log|\Gamma|}{\alpha} + \frac{2c}{\alpha}.$$

In particular, for the mixing time mix_v *we have:*

$$\text{mix}'_v \ \le \ \frac{2}{\alpha} \ (\log|\Gamma| + 1). \qquad \square$$

From now on we will restrict our attention to estimates on β_1 which suffice to analyze mixing of lazy random walks. We start with the following definition:

Definition 2.2. A finite d-regular graph Γ is called an *ε-expander* if for every subset of vertices $B \subset \Gamma$, $|B| \le |\Gamma|/2$, we have $|\partial B| \ge \varepsilon|B|$, where

$$\partial B = \{v \in \Gamma \,|\, v \notin B, \text{ but } v \text{ is adjacent to a vertex in } B\}.$$

It is well known that expanders can be very large (with the same d) and have spectral gap bounded away from zero. The inverse is also true (see [Ch], [Lu1] for references and details).

There are various methods in the literature to construct expanders, but usually it is not easy to prove that some given families of graphs are ε-expanders with the same ε. Margulis was the first one to give explicit examples which he constructed using property (T).

Definition 2.3. A topological group G is said to have (Kazhdan) *property (T)* if there exists a compact subset Q of G such that $\mathcal{K} = \mathcal{K}(G,Q) > 0$, where

$$(*) \qquad \mathcal{K}(G,Q) = \inf_{\rho} \inf_{v} \max_{q \in Q} \ \frac{\|\rho(q)\,v - v\|}{\|v\|}\,,$$

where ρ runs over all unitary representations $(\mathcal{H}, \rho)$ of G which do not contain the trivial representation (i.e., no non-zero G-fixed vector), and v runs over all vectors $v \ne 0$ in $\mathcal{H}$.

We say that (Q, ε) is a *Kazhdan constant* for G if $\varepsilon \leq \mathcal{K}(G, Q)$.

Now let Γ be a discrete group. It is well known and not difficult to prove that if Γ has (T), then Γ is finitely generated, and if (Q, ε) is a Kazhdan constant for Γ, then Q generates Γ.

Proposition 2.4. *Let Γ be a discrete group generated by a finite set S. Assume Γ has property (T) with Kazhdan constant $(S, \mathcal{K})$. Then for every finite index subgroup N of Γ, the Schreier graph X on Γ/N with respect to S is an ε-expander with $\varepsilon \geq \alpha \geq \mathcal{K}^2/2|S|$, where $\alpha(X) = 1 - \beta_1(X)$ is a spectral gap of X.*

The proof can be found in [HRV], Corollary to Proposition III, p. 89.

Proposition 2.5. *Using the conditions of Proposition 2.4, assume that there is a finite group $H < \mathrm{Aut}(\Gamma)$ such that $H(S) = S$ and the action of H on S has m equal size orbits. Then one can improve the eigenvalue gap bound as follows:*

$$\alpha \geq \frac{\mathcal{K}^2}{2\,m}.$$

The proof will appear in a forthcoming paper [PZ]. Let us note that one can always take $H = \{1\}$. Then $m = |S|$ and the bound in Proposition 2.5 coincides with a bound in Proposition 2.4.

3. $\Gamma_k(G)$ as expanders

We can now combine the preliminary results we presented in §1 and §2 to deduce:

Theorem 3.1. *Let W be a characteristic subgroup of F_k, let $\pi : \mathrm{Aut}(F_k) \to \mathrm{Aut}(F_k/W)$ and let $A^+(F_k/W) = \pi(A^+(F_k))$ be the special automorphism group of F_k/W generated by the set Υ of Nielsen moves. If $A^+(F_k/W)$ has Kazhdan's property (T), then there exists an $\varepsilon > 0$ such that for every finite quotient G of F_k/W, every connected component Γ' of $\Gamma_k(G)$ is an ε-expander, for some $\varepsilon > 0$.*

Moreover, for all $c > 0$ the total variation distance $\|Q^t_{(g)} - U\|_{\mathrm{tv}}$ and the mixing time $\mathrm{mix}'_{(g)}$ of the lazy random walk $\mathcal{W}'$ on Γ' starting at $(g) \in \Gamma'$ satisfy:

$$\|Q^t_{(g)} - U\|_{\mathrm{tv}} \leq e^{-c} \quad \textit{for} \quad t \geq \frac{16 \log|\Gamma|}{\mathcal{K}^2} + \frac{16 \cdot c}{\mathcal{K}^2}\,,$$

$$\textit{and} \quad \mathrm{mix}'_{(g)} \leq \frac{16}{\mathcal{K}^2}\,(\log|\Gamma'| + 1)\,,$$

where $(\Upsilon, \mathcal{K})$ is a Kazhdan constant for $A^+(F_k/W)$.

Proof. Let Υ be the set of Nielsen moves. By Proposition 1.10, Γ' is a Schreier graph of $A^+(F_k/W)$ with respect to Nielsen moves, and by Proposition 2.4 every such Schreier graph is an ε-expander for an $\varepsilon > 0$ which depends only on $\mathcal{K}(A^+(F_k/W), \Upsilon)$. Notice that a symmetric group $S_k \subset A^+(F_k)$ preserves Υ ($S_k(\Upsilon) = \Upsilon$), and has exactly 4 orbits. Now Proposition 2.5 gives a bound on the eigenvalue gap and, finally, Proposition 2.1′ gives a desired bound on the mixing time. □

Ideally, we would like to apply Theorem 3.1 to the characteristic subgroup $W = \{1\}$, the trivial group. But this is a well-known open problem:

Open Problem 3.2. *Does $\mathrm{Aut}(F_k)$ (or equivalently $A^+(F_k)$) have Kazhdan's property (T)?*

Clearly the answer for $k = 2$ is negative since $GL_2(\mathbb{Z})$ is a quotient of $\mathrm{Aut}(F_2)$ and the latter does not have (T). It follows from [Mc] that the answer for $k = 3$ is also negative. On the other hand, for some non-trivial W, $A^+(F_k/W)$ does have (T).

Theorem 3.3. *a) For $k \geq 3$, the group $SL_k(\mathbb{Z})$ has Kazhdan's property (T).*

b) $\mathcal{K}\big(SL_k(\mathbb{Z}), \{E^{\pm}_{i,j}\}\big) = \Omega\big(\frac{1}{k^2}\big)$, where $E^{\pm}_{i,j}$, $i \neq j$, is an elementary matrix with ones on the diagonal, ± 1 at (i,j), and zeroes elsewhere.

Proof. Part *a*) is a classical result of Kazhdan (see [Lu1]). Part *b*) is a recent result of Shalom [Sh2]. □

Now, if W is the commutator subgroup of F_k, then $A^+(F_k/W) \simeq SL_k(\mathbb{Z})$ and the Nielsen moves give the elementary matrices (see Example 1.11). Recall also that $\Gamma_k(G)$ is connected for G abelian and $k \geq d(G) + 1$. We obtain:

Theorem 3.4. *Let G be a finite abelian group and $k \geq \max\{3, d(G)+1\}$. Fix any generating k-tuple $(g) \in \Gamma_k(G)$. Then for all $c > 0$ the total variation distance $\|Q^t_{(g)} - U\|_{\mathrm{tv}}$ and the mixing time $\mathrm{mix}'_{(g)}$ of the lazy random walk $\mathcal{W}'$ on Γ' starting at $(g) \in \Gamma'$ satisfy:*

$$\|Q^t_{(g)} - U\|_{\mathrm{tv}} \leq e^{-c} \quad \textit{for} \quad t \geq C\, k^5 \log|G| + c \cdot C'\, k^4,$$

$$\mathrm{mix}'_{(g)} \leq C''\, k^5 \log|G|\,,$$

where C, C', C'' are universal constants.

Proof. By Theorem 3.3 part *b*) we have $\mathcal{K} = \Omega(1/k^2)$. Further,

$$\log|\,\Gamma_k(G)| \leq \log\big(|G|^k\big) = k \log|G|.$$

Therefore by Theorem 3.1 we immediately have:

$$\mathrm{mix}'_{(g)} \leq \frac{16}{\mathcal{K}^2} \log|\Gamma_k(G)| \leq C\, k^5 \log|G|.$$

The total variation distance is bounded analogously. This completes the proof. □

Remark 3.5. (*i*) In [Sh1] Shalom showed that

$$\mathcal{K}\big(SL_k(\mathbb{Z}), \{E^{\pm}_{i,j}\}\big) \geq \frac{1}{33\,k^2 - 11\,k + 1122}.$$

Combined with the estimates in Theorem 3.1, the constants C, C', C'' can be explicitly computed.

(*ii*) When G is abelian and $k = d(G)$ the graph $\Gamma_k(G)$ can have many connected components, each of equal size (see [DG]). In this case one can generalize the result of the theorem to the same bound for mixing on the connected component containing the starting point (g) of the random walk.

(*iii*) Theorem 3.4 remains true also for $k = 2$. By Remark 1.13, it suffices that the congruence quotients of $SL_2(\mathbb{Z})$ are expanders. This is indeed the case: In spite of the fact that $G = SL_2(\mathbb{Z})$ does not have property (T), it has property (τ) with respect to the congruence subgroups $\Gamma(m) = (\mathrm{Ker}(SL_2(\mathbb{Z})) \to SL_2(\mathbb{Z}/m\mathbb{Z}))$, $m \geq 1$. Hence there exists a common $\epsilon > 0$ such that for every Schreier graph X of $SL_2(\mathbb{Z})$ modulo $\Gamma(m)$ we have $\alpha(X) > \epsilon$. This follows from the celebrated result of Selberg asserting that $\lambda_1\big(\Gamma(m) \setminus \mathbb{H}\big) \geq 3/16$, where $\mathbb{H}$ is the upper half plane with its hyperbolic metric and $\lambda_1(M)$ means the bottom of the positive spectrum of the Laplacian on the manifold M (see [Lu1], [Lu2] for details).

Let us mention here that the notion of congruence subgroups can be extended to the non-commutative setting:

Definition 3.6. Let B be any group and $\Gamma \leq \mathrm{Aut}(B)$. For a characteristic subgroup N of a finite index in B define $\Gamma(N) = \mathrm{Ker}\big(\Gamma \to \mathrm{Aut}(B/N)\big)$. A subgroup of Γ containing $\Gamma(N)$ for some such N will be called a *congruence subgroup* of Γ.

It is not difficult to see that if B is a finitely generated residually finite group, then the congruence subgroups define a Hausdorff topology on Γ. If $B = \mathbb{Z}^k$ and $\Gamma = SL_k(\mathbb{Z}) \leq \mathrm{Aut}(\mathbb{Z}^k)$, the congruence topology is just the usual one.

Now one can formulate a "congruence subgroup problem" in this setting. In particular, for $B = F_k$:

Open Problem 3.7. *Is every finite index subgroup of* $\mathrm{Aut}(F_k)$ *a congruence subgroup?*

Recall that for $SL_k(\mathbb{Z})$, $k \geq 3$, every finite index subgroup is a congruence, while for $k = 2$ this is not the case [BMS] (compare [Mo] for a related question).

Let us return to our main interest, finding bounds on the mixing time of the product replacement random walk. Observe that it is actually not necessary that $A^+(F_k/W)$ have property (T). One can check along the proof that it suffices to have "property (τ) with respect to congruence subgroups" (compare with Remark 1.13). Note that the latter is called the "Selberg property" in [Lu2].

So far, we have presented a completely satisfactory result for abelian groups, which explains the outstanding performance of the product replacement algorithm for these groups. Let us consider now the case of nilpotent groups.

As in §2, define the lower central series of a group G by $\gamma_1(G) = G$ and $\gamma_{i+1}(G) = [G, \gamma_i(G)]$. A group G is called nilpotent of class i if $\gamma_{i+1}(G) = 1$. For any group G the group $\gamma_{i+1}(G)$ is a characteristic subgroup of G and $F_k/\gamma_{i+1}(F_k)$ is called the *free nilpotent group of class i on k generators*. Let Υ be the set of Nielsen moves in $\mathrm{Aut}(F_k)$. We shall denote by Υ_i the image $\pi_i(\Upsilon)$ of the Nielsen moves under the natural map $\pi_i : \mathrm{Aut}(F_k) \to \mathrm{Aut}(F_k/\gamma_{i+1}(F_k))$.

Theorem 3.8. *For every $k \geq 3$ and $i \geq 1$ the special automorphism group of the free nilpotent group of class i on k generators $A_k(i) = A^+(F_k/\gamma_{i+1}(F_k))$ has Kazhdan's property (T).*

Theorem 3.8 will be proved in §4. It is a direct generalization of part a) of Theorem 3.3. From Theorem 3.8 we can now deduce:

Theorem 3.9. *For fixed $i \geq 1$ and $k \geq 3$ and for every nilpotent group of class at most i the mixing time of the lazy random walk on any connected component X of $\Gamma_k(G)$ is bounded by $C(k,i) \cdot \log|G|$, where $C = C(k,i)$ is a constant depending only on k and i.*

Proof. This is a corollary of Theorem 3.8 and Theorem 3.1. □

Remark 3.10. Recall that $\Gamma_k(G)$ is connected for $k \geq d(G) + 1$ ([Du2]). Therefore in this case one obtains a complete answer for the performance of the algorithm (cf. [P3]).

One can extend Selberg's theorem to show that Theorem 3.9 is valid for $k = 2$. We will not present the details as the case $k = 2$ is of interest only for cyclic groups and thus covered by Theorem 3.4 and Remark 3.5.

Finally, in §5 we discuss the estimates on the constant C that one can obtain by various methods.

4. Automorphism groups of free nilpotent groups

In this section we prove that $A_k(i)$ has property (T), completing the proof of Theorem 3.8.

Let $F_k(i)$ be the free nilpotent group on k generators and class i. For every finitely generated torsion free nilpotent group G one has a central series

$$G = G_1 > G_2 > \cdots > G_r > G_{r+1} = \{e\}\,,$$

where $G_i/G_{i+1} \simeq \mathbb{Z}$. By choosing $x_i \in G_i \setminus G_{i+1}$ such that $x_i G_{i+1}$ generates G_i/G_{i+1} one gets a "Malcev basis" for G: every $g \in G$ can be written as

$$g = x_1^{a_1} \cdot x_2^{a_2} \cdot \ldots \cdot x_r^{a_r},$$

with $a_i \in \mathbb{Z}$ for $1 \le i \le r$. Identifying G with $\mathbb{Z}^r$ via $g \to (a_1, \ldots, a_r)$, P. Hall ([H]) showed that the group operations are given by polynomials with rational coefficients. One can use these polynomials to extend the group operations from $\mathbb{Z}^r$ to $\mathbb{R}^r$, thus embedding G in a simply connected unipotent group U (the "Malcev embedding" of Γ). Moreover, every automorphism of G can be extended to an automorphism of U.

Applying all this to $G = F_k(i)$ we get a free nilpotent group $U = U_k(i)$ over $\mathbb{R}$, and an embedding of $\mathrm{Aut}(F_k(i))$ in $\mathrm{Aut}(U_k(i))$. The latter is a Lie group ([Ho], Corollary 15.9).

The group theoretic structure of $\mathrm{Aut}(F_k(i))$ was described by Andreadakis [An]: First, denote $J = \mathrm{Ker}\big(\mathrm{Aut}(F_k(i)) \to \mathrm{Aut}(F_k(i-1))\big)$. Every $\alpha \in J$ is an automorphism which takes each of the free generators $x_1, \ldots, x_k$ of $F_k(i)$ to $x_1\zeta_1, \ldots, x_k\zeta_k$, where $\zeta_1, \ldots, \zeta_k \in \gamma_i(F_k)/\gamma_{i+1}(F_k)$. It is not difficult to check that $\alpha \to (\zeta_1, \ldots, \zeta_k)$ defines an isomorphism from J onto $\big(\gamma_i(F_k)/\gamma_{i+1}(F_k)\big)^k$. From the Witt formula ([MKS], Theorem 5.11) and by induction we can now deduce that $\mathrm{Aut}(F_k(i))$ is an extension:

$$(*) \quad 1 \to \widetilde{M}_k(i) \to \mathrm{Aut}(F_k(i)) \to GL_k(\mathbb{Z}) \to 1\,,$$

where $\widetilde{M}_i$ is the group of IA-automorphisms of $F_k(i)$, i.e. the group of automorphisms which act trivially on the commutator quotient. The group $\widetilde{M}_i$ is a nilpotent group of class $(i-1)$ and of Hirsh rank m_i:

$$m_k(i) = k \left(\sum_{j=1}^{i-1} \frac{1}{j} \sum_{d \,|\, j} \mu(d)\, k^{j/d} \right),$$

where μ is a classical Möbius function. See [An] for details.

The group $\mathrm{Aut}(U_k(i))$ has a similar structure:

$$(**) \quad 1 \to \widetilde{N}_k(i) \to \mathrm{Aut}(F_k(i)) \xrightarrow{\pi} GL_k(\mathbb{R}) \to 1\,,$$

where $\widetilde{N}_k(i)$ is a simply connected nilpotent group of dimension $m_k(i)$.

Now, from the description it is clear that $\mathrm{Aut}(F_k(i))$ is a discrete subgroup of $\mathrm{Aut}(U_k(i))$. It is not a lattice there, but it is a lattice in the preimage of $SL_k^{\pm}(\mathbb{R})$ under π, where $SL_k^{\pm}(\mathbb{R})$ denotes the group of matrices of determinant ± 1.

Unlike $(*)$, the sequence $(**)$ splits, and so

$$\mathrm{Aut}(U_k(i)) = \widetilde{N}_k(i) \rtimes SL_k^{\pm}(\mathbb{R}).$$

Let us look now at $A_k(i)$, which is the image of $A^+(F_k)$ in $\mathrm{Aut}(F_k(i))$, as a subgroup of $\mathrm{Aut}(U_k(i))$. Let $M_k(i)$ be the intersection of $A_k(i)$ with $\widetilde{M}_k(i)$.

We have that $M_k(i)$ is a discrete subgroup of $\widetilde{N}_k(i)$; it is a subgroup of

$$\widetilde{M}_k(i) = \mathrm{Ker}\big(\mathrm{Aut}(F_k(i)) \to GL_k(\mathbb{Z})\big),$$

which is a lattice in $\widetilde{N}_k(i)$. Let $N_k(i)$ be the Zariski closure of $M_k(i)$ in $\widetilde{N}_k(i)$. One can prove by induction on the dimension of a nilpotent unipotent group that every subgroup of a lattice is a lattice in its Zariski closure. Hence $M_k(i)$ is a lattice in $N_k(i)$.

The image of $A_k(i)$ in $SL_k^{\pm}(\mathbb{R})$ is $SL_k(\mathbb{Z})$ which is Zariski dense in $SL_k(\mathbb{R})$, and since $A_k(i)$ normalizes $M_k(i)$, $SL_k(\mathbb{R})$ normalizes $N_k(i)$. We can summarize:

Proposition 4.1. *The group $A_k(i)$ is a lattice in the Lie group $G_k(i) = N_k(i) \rtimes SL_k(\mathbb{R})$.*

Proposition 4.2. *For $k \geq 3$ and $i \geq 1$, the Lie group $G_k(i) = N_k(i) \rtimes SL_k(\mathbb{R})$ has property (T). Moreover, if (Q, ε) is a Kazhdan constant for $SL_k(\mathbb{R})$, then (Q, ε) is a Kazhdan constant for $G_k(i)$ (and thus independent of i).*

Proof. It follows from [W] (see also [Sh3]) that a group like $G_k(i)$, i.e. a semidirect product of a nilpotent unipotent group and a connected non-compact semisimple Lie group with property (T), has Kazhdan's property (T) if and only if $G_k(i) = [G_k(i), G_k(i)]$. Now, since $A_k(i)$ is Zariski dense in $G_k(i)$ it therefore suffices to show that $[A_k(i), A_k(i)]$ is of finite index in $A_k(i)$. To see this it is enough to show that $[A, A]$ is of finite index in A, where $A = A^+(F_k)$. In fact $[A, A]$ is equal to A as can be seen from the explicit presentation for A given by Gersten [Ge]. The second statement of the Proposition, follows from a more general result:

Proposition 4.3. *Let $G = N \rtimes H$ be a semidirect product of a connected non-compact semisimple Lie group H without compact factors and a unipotent Lie group N. Assume G has property (T) (this happens if and only if H has (T) and $[N, H] = N$). Let (Q, ε) be a Kazhdan constant for H. Then (Q, ε) is a Kazhdan constant also for G.*

Proof. Let us first observe that for every representation σ of G without a G-invariant vector, all matrix coefficients $g \to \langle \sigma(g)\, v, u\rangle$ go to zero as g goes to infinity along H. Indeed, let us first prove this when σ is irreducible. Then $K = \mathrm{Ker}(\sigma)$ is a normal subgroup of G. If K contains H, then by condition of the theorem we have:

$$K \geqslant [K, N] \geqslant [H, N] = N$$

and so K also contains N. This implies that $K = G$ and σ is the trivial representation, which is a contradiction. Now, if K does not contain H, then $K \cap H$ is a proper subgroup of H, and hence the image of H in G/K is non-compact. Moreover, it is also non-compact in $(G/K)/Z(G/K)$ since H has no infinite abelian normal subgroups. Our claim (for irreducible representations) now follows from the Howe-Moore Theorem for groups with radical ([HM], Theorem 6.1, p. 86.) The general case follows from a standard direct integral argument (cf. [Z], Proposition 2.3.2), after observing that by the assumption on σ almost every irreducible representation which appears in a decomposition of σ into irreducibles is non-trivial.

Now let (V, ρ) be a unitary representation of G on a Hilbert space V, and assume that V has a (Q, ε)-invariant vector, i.e. a unit vector v with $\|\rho(q)v - v\| \leq \varepsilon$ for

every $q \in Q$. We need to prove that V has a G-invariant vector. By the assumption, V has an H-invariant unit vector w. If V does not contain a G-invariant vector, then by the previous observation, the matrix coefficient $\langle \rho(g)\, w, w\rangle$ must go to 0 as g goes to ∞ along H. But this is a contradiction since $\langle \rho(g)\, w, w\rangle = \|w\|^2$ for $g \in H$. This finishes the proof. □

Proof of Theorem 3.8. By Proposition 4.1, $A_k(i)$ is a lattice in $G_k(i)$, and by Proposition 4.2, $G_k(i)$ has property (T). It is well known (see [K]) that a lattice in a locally compact group with (T) has (T) as well. This completes the proof. □

5. Concluding remarks

While our results show the relevance of Kazhdan's property (T) to the analysis of the product replacement algorithm, it is not easy to apply property (T) to get quantitative estimates on the mixing time. The reason is the difficulty in estimating Kazhdan constants (cf. [Bu]). Even when one can get estimates on Kazhdan constants, they are not necessarily for the desired finite (or compact) set.

Recently Shalom made a breakthrough in the study of explicit Kazhdan constants. In [Sh1] he showed that for $G = SL_k(\mathbb{R})$ the set Q of the two matrices $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ embedded in the upper 2×2 left corner of $SL_k(\mathbb{R})$ form a Kazhdan constant with $\varepsilon = \sqrt{2-\sqrt{3}}$ ($\approx .51$). So, by Proposition 4.2 the same holds for the groups $G_k(i)$ there, independent of k and i.

Unfortunately, knowing Kazhdan constants for a Lie group is only part of the work (in fact, a small part) of computing Kazhdan constants for a lattice.

Let us remark first that having Kazhdan constants for the $G_k(i)$'s independent of i does not give any indication that the same holds for $A_k(i)$. For example, look at the groups $H_m = (\mathbb{R}^3)^m \rtimes SL_3(\mathbb{R})$, where $SL_3(\mathbb{R})$ acts as a standard module on each copy of $\mathbb{R}^3$. By Proposition 4.3 the groups H_m have Kazhdan constants independent of m, but it is not difficult to see that this is not the case for $(\mathbb{Z}^3)^m \rtimes SL_3(\mathbb{Z})$, which is a lattice in H_m.

In [Sh1] Shalom showed a general method of how to pass from a Kazhdan constant (a compact set Q and a number ε) of a Lie group G to a Kazhdan constant (a finite set and a number) for a lattice Γ in it. In principle, one might be able to apply it to our case to get explicit Kazhdan constants for $A_k(i)$, but the best bound one could possibly obtain by this approach will decrease exponentially in i.

Note also that Shalom's method in [Sh1] gives an explicit number, but with respect to a subset of Γ on which there is only a partial knowledge. In our case we will also have to replace the set of generators obtained by Shalom's method with the set of Nielsen's generators, paying an additional price on the estimate.

In [Sh2], Shalom presented a completely different method to compute directly the Kazhdan constant of $SL_k(\mathbb{Z})$ with respect to the elementary matrices $E^{\pm}_{i,j}$. These are exactly the Nielsen generators for the group $A_k(1)$! He showed that the Kazhdan constant is at least $\Omega(1/k^2)$ (and at most $O(1/\sqrt{k})$). We have already used this remarkable result in Theorem 3.4. Again, it seems his method can work also for $A_k(i)$, but will give Kazhdan constants which will decrease exponentially (as a function of the class i and k). Definitely, these results are far from satisfactory. We hope that our work will provide an additional motivation for the ongoing efforts to improve estimates of Kazhdan constants.

Let us make a remark about Open Problem 3.2. It follows from [Gi] that the infinitely many alternating groups are quotients of $A^+(F_k)$. Therefore if $\mathrm{Aut}(F_k)$ (or equivalently $A^+(F_k)$) has Kazhdan's property (T), then one can make Cayley graphs on the symmetric (alternating) groups into a sequence of expanders. This would solve positively Open Problem 10.3.4 and negatively Open Problem 10.3.2 in [Lu1].

Finally, we present a few remarks regarding the product replacement algorithm. Let us first note that the actual implementation uses only moves $L_{i,j}^+$ and $R_{i,j}^+$ (see [CLMNO]). In this paper we add the moves $L_{i,j}^-$ and $R_{i,j}^-$ to simplify the analysis. Observe that the resulting Markov chain is then reversible. It is worth mentioning that, as shown in [DS2], the original version can be analyzed as well by reducing to a reversible version. We leave it to the reader whether a similar reduction can be done in this case.

Another variant of the product replacement random walk, using only $L_{i,j}^{\pm}$, was studied in [DS2]. It might be helpful to note that in the case of nilpotent groups this is the same walk, so our analysis holds. We do not know whether there is a difference in the general case (cf. [P1]).

Let us note that the connectivity problem was successfully removed by the second author [P2] who showed that in a few interesting cases the graphs $\Gamma_k(G)$ have a large connected component and thus the random walk on such a component outputs a (nearly) uniform generating k-tuple.

In a different direction, we should warn the reader that the ability to sample a uniform generating k-tuple does not necessarily give a way to generate random elements in the group. In particular, the distribution of components of random elements $(g) \in \Gamma_k(G)$ can have a strong bias, sometimes even detectable by a short line program. We refer to a recent result [BP] of Babai and the second named author for details.

Acknowledgements

We are indebted to Yehuda Shalom for many useful discussions about his works [Sh1], [Sh2] and the current paper. In particular, Theorem 4.3 was proved with his collaboration. We also thank Persi Diaconis, Gregory Margulis, Andrzej Żuk, and an anonymous referee for helpful remarks.

This work was carried out while the first named author was visiting the Department of Mathematics at Yale University, whose warm hospitality and support are gratefully acknowledged.

The second named author was supported by an NSF Postdoctoral Research Fellowship in Mathematical Sciences.

References

[An] S. Andreadakis, *On the automorphisms of free groups and free nilpotent groups*, Proc. London Math. Soc. (3) **15** (1965), 239–268. MR **32:**5746

[Bb1] L. Babai, *Local expansion of vertex-transitive graphs and random generation in finite groups*, in Proc 23^{rd} ACM STOC (1991), 164–174.

[Bb2] L. Babai, *Randomization in group algorithms: Conceptual questions*, in Groups and Computation II (L. Finkelstein, W.M. Kantor, eds.) DIMACS Workshops on Groups and Computation (1997). MR **98k:**68092

[BP] L. Babai, I. Pak, *Strong bias of group generators: an obstacle to the "product replacement algorithm"*, in Proc. 11^{th} SODA (2000), 627–635. CMP 2000:12

[Bh] S. Bachmuth, *Automorphisms of free metabelian groups*, Trans. Amer. Math. Soc. **118** (1965), 93–104. MR **31:**4831

[BMS] H. Bass, J. Milnor, J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Publ. Math. IHES **33** (1967), 59–137. MR **39:**5574

[BCP] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system,* in "Computational algebra and number theory (London, 1993)", J. Symbolic Comput. **24** (1997), 235–265. MR **98f:**68006

[Bu] M. Burger, *Kazhdan constants for* $SL(3, \mathbb{Z})$, J. Reine Angew. Math. **413** (1991), 36–67. MR **92c:**22013

[CLMNO] 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. MR **96h:**20115

[Ch] F.R.K. Chung, *Spectral Graph Theory* (CBMS Regional Conference Series in Mathematics, No. 92), American Mathematical Society, Providence, RI, 1994. MR **97k:**58183

[CG] F.R.K. Chung, R.L. Graham, *Random walks on generating sets for finite groups*, The Electronic J. of Comb. **4 No 2.** (1997), #R7. MR **98c:**60087

[DG] P. Diaconis, R. Graham, *The graph of generating sets of an abelian group*, Colloq. Math. **80** (1999), 31–38. MR **2000f:**20124

[DS1] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of abelian groups*, Prob. Th. Rel. Fields **105** (1996), 393–421. MR **98a:**60093

[DS2] P. Diaconis, L. Saloff-Coste, *Walks on generating sets of groups*, Invent. Math. **134** (1998), 251–199. MR **2000e:**60013

[Du1] M.J. Dunwoody, *On T-systems of groups*, J. Austral. Math. Soc. **3** (1963), 172–179. MR **27:**3706

[Du2] M.J. Dunwoody, *Nielsen Transformations*, in Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967) (1970), 45–46. MR **41:**5472

[Ge] S. M. Gersten, *A presentation for the special automorphism group of a free group*, J. Pure Appl. Algebra **33** (1984), 269–279. MR **86f:**20041

[Gi] R. Gilman, *Finite quotients of the automorphism group of a free group*, Canad. J. Math. **29** (1977), 541–551. MR **55:**8186

[Gr] K. W. Gruenberg, *Relation modules of finite groups,* CBMS Regional Conference Series in Mathematics, No. 25, American Mathematical Society, Providence, R.I., 1976. MR **56:**15743

[H] P. Hall, *The Edmonton notes on nilpotent groups,* in *The collected works of Philip Hall*, Clarendon Press, Oxford, 1988. MR **90b:**01108

[HRV] 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. MR **94j:**22007

[Ho] G. Hochschild, *Introduction to affine algebraic groups*, Holden-Day, San Francisco, 1971. MR **43:**3268

[HM] R. Howe, C. Moore, *Asymptotic properties of unitary representations*, J. Funct. Anal. **32** (1979), 72–96. MR **80g:**22017

[K] D. A. Kazhdan, *On the connection of the dual space of a group with the structure of its closed subgroups* (Russian), Funkcional. Anal. i Prilozhen. **1** (1967), 71–74.

[LG] C. Leedham–Green, personal communication.

[Lu1] A. Lubotzky, *Discrete Groups, Expanding Graphs and Invariant Measures*, Birkhauser, Boston, 1994. MR **96g:**22018

[Lu2] A. Lubotzky, *Eigenvalues of the Laplacian, the first Betti number and the congruence subgroup problem*, Ann. of Math. (2) **144** (1996), 441–452. MR **98h:**22013

[MKS] W. Magnus, A. Karrass, D. Solitar, *Combinatorial group theory. Presentations of groups in terms of generators and relations* (Second edition), Dover, New York, 1976. MR **34:**7617 (review of first edition)

[Mc] J. McCool, *A faithful polynomial representation of* $Out F_3$, Math. Proc. Cambridge Philos. Soc. **106** (1989), 207–213. MR **90j:**20079

[Mo] S. Moses, *On the congruence subgroup problem for tree lattices,* in "Lie groups and ergodic theory (Mumbai, 1996)", Tata Inst. Fund. Res., Bombay, 1998, pp. 143–149.

[P1] I. Pak, *Generating random elements in solvable groups*, preprint (1999).

[P2] I. Pak, *On the graph of generating sets of a simple group*, preprint (1999).

[P3] I. Pak, *What do we know about the product replacement random walk?*, to appear in *Groups and Computations III*.

[PB] I. Pak, S. Bratus, *On sampling generating sets of finite groups and the product replacement algorithm*, Proc. ISSAC'99, 1999, pp. 91–96.

[PZ] I. Pak, A. Żuk, in preparation, 2000.

[Sc] M. Schönert et al., *GAP – Groups, Algorithms, and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany, 1995.

[Sh1] Y. Shalom, *Explicit Kazhdan constants for representations of semisimple and arithmetic groups*, Annales de L'Institut Fourier, to appear.

[Sh2] Y. Shalom, *Bounded generation and Kazhdan's property (T)*, Publ. Math. IHES, to appear.

[Sh3] Y. Shalom, *Invariant measures for algebraic actions, Zariski dense subgroups and Kazhdan's property (T)*, Trans. Amer. Math. Soc. **351** (1999), 3387–3412. MR **99m:**22008

[W] S. P. Wang, *On the Mautner phenomenon and groups with property (T)*, Amer. J. Math. **104** (1982), 1191–1210. MR **84g:**22033

[Z] R. J. Zimmer, *Ergodic theory and semisimple groups,* in: Monographs in Mathematics, **81**, Birkhauser, Boston, MA, 1984. MR **86j:**22014

Department of Mathematics, Hebrew University, Givat Ram, Jerusalem 91904, Israel
E-mail address: alexlub@math.huji.ac.il

Department of Mathematics, Yale University, New Haven, Connecticut 06520
E-mail address: paki@math.yale.edu
Current address: Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139
E-mail address: pak@math.mit.edu