COLLOQUIUM MATHEMATICUM

VOL. 74 1997 NO. 2

SOME REMARKS ON THE RANDOM WALK ON FINITE GROUPS

BY

ROMAN URBAN (WROCŁAW)

1. Introduction. Let G be a finite group and let S be a set of generators of G. Suppose that S is not contained in a coset of a subgroup of G. Then for every probability measure μ such that $\operatorname{supp}\mu = S$ we have

$$\lim_{n\to\infty} \|\mu^{*n} - \lambda\|_X = 0, \tag{1.1}$$

where λ is the equidistributed probability measure on G: $\lambda(g) = 1/|G|$, and $\|\cdot\|_X$ denotes a suitable norm on the space of functions on G. The speed of convergence in (1.1) depends on the group and the particular set of generators as well as the norm $\|\cdot\|_X$ chosen. The problem of estimating this speed has been thoroughly studied by many authors, in particular by Diaconis; see e.g. [1] and the literature quoted there.

In this note we are interested in questions concerning comparison of speeds of convergence to λ. On the one hand, we take convolution powers of a single probability measure supported on a fixed symmetric set S of generators, and on the other hand, convolution products of sequences of probability measures each supported on S.

It has been noticed [2] that in the important case of the symmetric group $\mathcal{S}_n$ and the set of generators consisting of the transpositions there exist n probability measures $\mu_1, \ldots, \mu_n$ supported on S such that

$$\lambda = \mu_1 * \ldots * \mu_n. \tag{1.2}$$

There are, however, groups and symmetric sets S of generators for which (1.2) does not hold for any finite set of probability measures supported on S. We exhibit some examples in Section 5. So there are groups and their generating sets for which to achieve equilibrium by sampling elements from a given set of generators, infinitely many steps are necessary, regardless of whether we use the same sampling method or we change it at every step. It is reasonable to conjecture that in general the latter method should be faster. In other words, for a given probability measure μ supported on S the convolution product of a well chosen sequence of probability measures

1991 *Mathematics Subject Classification*: 60J15, 43A05.

supported on S should converge faster to the equilibrium measure λ than the convolution powers of μ.

In this note our first aim is to prove this conjecture in a number of cases. A simple compactness argument shows that given a symmetric set S of generators there is a symmetric probability measure μ_S such that

$$\|\mu - \lambda\|_{l^2 \to l^2} \geq \|\mu_S - \lambda\|_{l^2 \to l^2}$$

for every symmetric probability measure μ with support in S. Hence, since for symmetric measures ν,

$$\|\nu^{*n}\|_{l^2 \to l^2} = \|\nu\|^n_{l^2 \to l^2} \tag{1.3}$$

we have

$$\|\mu^{*n} - \lambda\|_{l^2 \to l^2} \geq \|\mu_S^{*n} - \lambda\|_{l^2 \to l^2}$$

for every symmetric probability measure μ with support in S.

In several cases we identify the measure μ_S explicitly.

As the first step in showing that the convolution products of a suitable sequence of probability measures converge faster than the convolution powers of single measure we study the following question. Given a probability measure μ supported in S, do there exists two probability measures μ_1, μ_2 both supported in S such that

$$\|\mu^{*2n} - \lambda\|_X \geq q^n \|(\mu_1 * \mu_2)^{*n} - \lambda\|_X, \tag{1.4}$$

for all n, where $q > 1$?

Of course for applications the most interesting case is when the distance between measures is measured by the l^1-norm. In Section 6 we make a few remarks about (1.4) for the case $X = l^1(G)$.

2. Preliminaries. A *representation* π of G is a homomorphism of G into the group of invertible linear maps of a finite-dimensional complex vector space V. We write d_π for the dimension of V and think of $\pi(x)$ as a $d_\pi \times d_\pi$ matrix. Without loss of generality we may assume that all representations π considered are *unitary*, i.e. $\pi(x)$ is a unitary matrix for all $x \in G$. A representation π is *irreducible* if V admits no $\pi(G)$ invariant subspaces other than $\{0\}$ or V. Two representations $\pi_1 : G \to \mathrm{GL}(V_1)$ and $\pi_2 : G \to \mathrm{GL}(V_2)$ are *equivalent* if there is a linear isomorphism $\varrho : V_1 \to V_2$ such that $\varrho\pi_1(x) = \pi_2(x)\varrho$ for all $x \in G$.

Let G be the product $G_1 \times G_2$ of two groups with multiplication defined coordinatewise. Let $\pi_1 : G_1 \to \mathrm{GL}(V_1)$ and $\pi_2 : G_2 \to \mathrm{GL}(V_2)$ be representations. Define a representation $\pi_1 \otimes \pi_2 : G_1 \times G_2 \to \mathrm{GL}(V_1 \otimes V_2)$ by $\pi_1 \otimes \pi_2(x, y)v_1 \otimes v_2 = \pi_1(x)v_1 \otimes \pi_2(y)v_2$. Then if π_1 and π_2 are irreducible, then $\pi_1 \otimes \pi_2$ is irreducible. Moreover, each irreducible representation of $G_1 \times G_2$ is equivalent to a representation $\pi_1 \otimes \pi_2$, where π_i is an irreducible

representation of G_i. If f is a function on G and π is a representation, define

$$\widehat{f}(\pi) = \sum_{x \in G} f(x)\pi(x).$$

The transform $\widehat{f}$ is the analog of the Fourier transform. It converts convolution into multiplication: $\widehat{f * g}(\pi) = \widehat{f}(\pi)\widehat{g}(\pi)$.

If f is a function on G we denote by T_f the operator from $l^2(G)$ into $l^2(G)$ defined by $T_f g = g * f$. If μ is a symmetric probability measure (i.e. $\sum \mu(x) = 1$, $\mu \geq 0$, $\mu(x) = \mu(x^{-1})$), then the operator T_μ has real eigenvalues $1 = \beta_0 \geq \ldots \geq \beta_{|G|-1} \geq -1$. Moreover, if the support of μ is not contained in a coset of a subgroup, then $1 = \beta_0 > \beta_1 \geq \ldots \geq \beta_{|G|-1} > -1$. The operator norm $\|f\|_{l^2 \to l^2}$ of a function f is, by definition, the $l^2 \to l^2$ norm of the convolution operator T_f, i.e. $\|f\|_{l^2 \to l^2} = \|T_f\|_{l^2 \to l^2}$. Let λ denote the probability measure which is uniformly distributed on a finite group G, i.e. $\lambda(x) = |G|^{-1}$ for all $x \in G$. Of course,

$$\widehat{\lambda}(\pi) = \begin{cases} \mathrm{Id} & \text{for the trivial representation,} \\ 0 & \text{for every nontrivial irreducible representation.} \end{cases}$$

It is well known that for every probability measure μ (not necessarily symmetric), $\|\mu - \lambda\|_{l^2 \to l^2} = \max \|\widehat{\mu}(\pi)\|_{l^2 \to l^2}$, where the maximum is taken over all irreducible and nontrivial unitary representations of a group G.

3. Main results. Let $S = S^{-1}$ be a symmetric set of generators of a group G. Define a function

$$\nu_\varepsilon(x) = \begin{cases} \varepsilon, & x = e, \\ -\varepsilon/(|S| - 1), & x \in S \backslash \{e\}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.1}$$

THEOREM 3.1. *Let G be a finite group, and $S = S^{-1} \neq G$ be a set of generators of G such that*:

(i) *the neutral element $e \in S$,*
(ii) $|S| \geq 3$.

Let μ be a symmetric probability measure with support S such that

$$\mu * \nu_\varepsilon = \nu_\varepsilon * \mu,$$

where ν_ε is defined in (3.1). *Then there exist symmetric probability measures μ_1 and μ_2 with support S such that, for all n,*

$$\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^2 \to l^2} < \|\mu^{*2n} - \lambda\|_{l^2 \to l^2}. \tag{3.2}$$

P r o o f. We define $\mu_1 = \mu + \nu_\varepsilon$ and $\mu_2 = \mu - \nu_\varepsilon$.

It is enough to prove inequality (3.2) in the case when $n = 1$. Indeed, (3.2) for $n = 1$ implies

$$\begin{aligned}\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^2\to l^2} &= \|(\mu_1 * \mu_2 - \lambda)^{*n}\|_{l^2\to l^2} \le \|\mu_1 * \mu_2 - \lambda\|^{*n}_{l^2\to l^2}\\ &< \|\mu^{*2} - \lambda\|^n_{l^2\to l^2} = \|\mu^{*2n} - \lambda\|_{l^2\to l^2}.\end{aligned}$$

Now we notice that $\widehat{\nu}_\varepsilon(\pi)$ is invertible when π is an irreducible, nontrivial unitary representation. In fact,

$$\begin{aligned}\|\mathbf{I} - \widehat{\nu}_\varepsilon(\pi)\|_{l^2\to l^2} &= \left\|(1-\varepsilon)\mathbf{I} + \frac{\varepsilon}{|S|-1}\sum_{x\in S\setminus\{e\}}\pi(x)\right\|_{l^2\to l^2}\\ &\le 1 - \varepsilon + \varepsilon\left\|\frac{1}{|S|-1}\sum_{x\in S\setminus\{e\}}\pi(x)\right\|_{l^2\to l^2} < 1,\end{aligned}$$

because

$$\left\|\frac{1}{|S|-1}\sum_{x\in S\setminus\{e\}}\pi(x)\right\|_{l^2\to l^2} < 1.$$

Since μ and ν_ε commute and are symmetric, $\widehat{\mu}$ and $\widehat{\nu}_\varepsilon$ are diagonal (in a suitable basis) and all eigenvalues of $\widehat{\nu}_\varepsilon$ are nonzero, since $\widehat{\nu}_\varepsilon$ is invertible. We have

$$\begin{aligned}\max\|\widehat{\mu_1 * \mu_2}(\pi)\|_{l^2\to l^2} &= \max\|(\widehat{\mu}(\pi) + \widehat{\nu}_\varepsilon(\pi))(\widehat{\mu}(\pi) - \widehat{\nu}_\varepsilon(\pi))\|_{l^2\to l^2}\\ &= \max\|\widehat{\mu}(\pi)^2 - \widehat{\nu}_\varepsilon(\pi)^2\|_{l^2\to l^2},\end{aligned}$$

where the maximum is taken over all irreducible, nontrivial representations of G. Thus for sufficiently small ε the right side of the above equality is less than $\max\|(\widehat{\mu}(\pi))^2\|_{l^2\to l^2}$. ∎

Recall that if a function f on G has the property

$$\forall t, x \in G, \qquad f(t^{-1}xt) = f(x), \tag{3.3}$$

then f is *central*, i.e. $f * g = g * f$ for every function g on G.

Theorem 3.1 implies the following

Corollary 3.4. *Let G be a finite group, and $S = S^{-1} \neq G$ be a set of generators of G such that*:

(i) $e \in S_0$,
(ii) $|S| \ge 3$,
(iii) $\forall t \in G$, $t^{-1}St = S$.

Let μ be a symmetric probability measure with support S. Then there exist symmetric probability measures μ_1 and μ_2 with support S such that (3.2) *holds.*

Proof. Indeed, (iii) implies that ν_ε as defined in (3.1) is central. ∎

4. Examples. A direct application of Corollary 3.2 gives the following result about the symmetric group $\mathcal{S}_n$.

PROPOSITION 4.1. *Let S = the set of all transpositions in $\mathcal{S}_n$. Let μ be a probability measure such that* $\operatorname{supp}\mu = S$. *Then the measures μ_1, μ_2 defined in the proof of Theorem* 3.1 *have the property that*

$$\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^2\to l^2} < \|\mu^{*2n} - \lambda\|_{l^2\to l^2}.$$

Given a group G and a symmetric set S of generators with $e \in S$ and $|S| \geq 3$, if the measure μ_S is *central* and symmetric, then (1.3) implies that the modification of μ_S as in Theorem 3.1 yields two probability measures μ_1, μ_2 and a $q < 1$ such that

$$\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^2\to l^2} < q^n \|\mu^{*2n} - \lambda\|_{l^2\to l^2}$$

for any probability measure μ supported in S.

In the examples which follow we identify the measure μ_S for some finite groups G and some particular sets S of generators.

EXAMPLE 1. Let $G = \mathbb{Z}_2^m$, $S = S^{-1} = \{e_1, \ldots, e_m, \mathbf{0}\}$, where $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 on the ith place and $\mathbf{0} = (0, \ldots, 0)$. Then μ_S is uniformly distributed on S.

Indeed,

$$\|\mu_S - \lambda\|_{l^2\to l^2} = \max_{\chi\neq 0} \left| \frac{1}{m+1} + \frac{1}{m+1} \sum_{j=1}^{m} \cos \pi\chi_j \right|,$$

where $\chi = (\chi_1, \ldots, \chi_m)$ and $\chi_j \in \{0, 1\}$. It is easy to see that the maximum is attained for $\chi = (1, 0, \ldots, 0)$ and is equal to $(m-1)/(m+1)$. Let μ be a probability measure with support in S. Let

$$\gamma_0 = \mu(\mathbf{0}) \quad \text{and} \quad \gamma_j = \mu(e_j) \quad \text{for } j = 1, \ldots, m.$$

Then

$$\|\mu - \lambda\|_{l^2\to l^2} = \max_{\chi\neq 0} \left| \gamma_0 + \sum_{j=1}^{m} \gamma_j \cos \pi\chi_j \right|.$$

We consider three cases:

(i) $\gamma_0 \geq 1/2$,
(ii) $\gamma_0 \leq 1/(m+1)$,
(iii) $1/(m+1) < \gamma_0 < 1/2$.

In case (i), $\gamma_i \leq 1/2$ for some i. Then

$$\|\mu - \lambda\|_{l^2\to l^2} \geq |\gamma_0 + \ldots + \gamma_{i-1} - \gamma_i + \gamma_{i+1} + \ldots + \gamma_m| = 1 - 2\gamma_i.$$

Here the character χ has 1 on the ith place and zero elsewhere. Also $1-2\gamma_i \geq (m-1)/(m+1)$, because $\gamma_i \leq 1/(2m)$.

In case (ii),

$$\|\mu-\lambda\|_{l^2\to l^2} \geq \Big|\gamma_0 - \sum_{j=1}^{m}\gamma_j\Big| = |\gamma_0-(1-\gamma_0)| = 1-2\gamma_0.$$

Here $\chi=(1,\dots,1)$. Also $1-2\gamma_0 \geq (m-1)/(m+1)$ since $\gamma_0 \leq 1/(m+1)$.

In case (iii), $\gamma_i \leq 1/(m+1)$ for some i. Thus if χ has 1 on the ith place and zero elsewhere we obtain $\|\mu-\lambda\|_{l^2\to l^2} \geq 1-2\gamma_i \geq (m-1)/(m+1)$.

EXAMPLE 2. Let $G=\mathbb{Z}_{k_1}\oplus\ldots\oplus\mathbb{Z}_{k_m}$, where k_j are odd integers >3. Let $S=S^{-1}=\{\pm e_1,\dots,\pm e_m\}$, where $e_i=(0,\dots,0,1,0,\dots,0)$. Define

$$x_i=\cos\frac{2\pi}{k_i}, \qquad \gamma_i^0=((1-x_i)((1-x_1)^{-1}+\ldots+(1-x_m)^{-1}))^{-1},$$

for $i=1,\dots,m$. Then for m large,

$$\mu_S(\pm e_i)=\gamma_i^0/2, \qquad i=1,\dots,m.$$

In particular, for $k_1=\ldots=k_m$ the measure μ_S is uniformly distributed on the set S of generators.

Let μ be a symmetric probability measure with support in S and let

$$\mu(\pm e_i)=\gamma_i/2, \qquad i=1,\dots,m.$$

The characters of G are of the form $\chi=(\chi_1,\dots,\chi_m)$, where each $\chi_j \in \{0,1,\dots,k_j-1\}$. Let $A=\{\chi:\chi_j=1$ for one fixed j and zero elsewhere$\}$. Then

$$\begin{aligned}\|\mu-\lambda\|_{l^2\to l^2} &= \max_{\chi\neq 0}\Big|\sum_{j=1}^{m}\gamma_j\cos\frac{2\pi\chi_j}{k_j}\Big| \geq \max_{\chi\in A}\Big|\sum_{j=1}^{m}\gamma_j\cos\frac{2\pi\chi_j}{k_j}\Big| \\ &= \max\{1-\gamma_1(1-x_1),\dots,1-\gamma_m(1-x_m)\}.\end{aligned}$$

We have

$$\max\{1-\gamma_1(1-x_1),\dots,1-\gamma_m(1-x_m)\} \geq 1-((1-x_1)^{-1}+\ldots+(1-x_m)^{-1})^{-1}.$$

Indeed, if $\gamma_i=\gamma_i^0$ for all i, then

$$\begin{aligned}1-\gamma_1(1-x_1) &= \ldots = 1-\gamma_m(1-x_m) \\ &= 1-((1-x_1)^{-1}+\ldots+(1-x_m)^{-1})^{-1}.\end{aligned}$$

If $\gamma\neq\gamma^0$ then $\gamma_i<\gamma_i^0$ for some i. Then

$$1-\gamma_i(1-x_i) \geq 1-((1-x_1)^{-1}+\ldots+(1-x_m)^{-1})^{-1}.$$

Now it suffices to show that

$$\|\mu_S-\lambda\|_{l^2\to l^2}=1-((1-x_1)^{-1}+\ldots+(1-x_m)^{-1})^{-1},$$

i.e. that

$$\|\mu_S - \lambda\|_{l^2 \to l^2} = \max_{\chi \in A} \left| \sum_{j=1}^{m} \gamma_j^0 \cos \frac{2\pi \chi_j}{k_j} \right|.$$

But this follows from the fact that the only character $\widetilde{\chi} \notin A$ for which

$$|\widehat{\mu}_S(\widetilde{\chi})| > \max_{\chi \in A} |\widehat{\mu}_S(\chi)|$$

is $\widetilde{\chi} = ((k_1 - 1)/2, \ldots, (k_m - 1)/2)$. However, for m large the opposite inequality holds:

$$\frac{1}{a} \sum_{j=1}^{m} \frac{\cos \frac{\pi}{k_j}}{1 - \cos \frac{2\pi}{k_j}} \leq \frac{1}{a} + \frac{1}{a} \sum_{j=2}^{m} \frac{1}{1 - \cos \frac{2\pi i}{k_j}}, \qquad m \gg 1,$$

where $a = ((1 - x_1)^{-1} + \ldots + (1 - x_m)^{-1})^{-1}$.

EXAMPLE 3. Let $G = Q_2 = \{\pm 1, \pm i, \pm j, \pm k\}$ be the quaternion group (see [4], p. 52). Let $S = S^{-1} = \{1, \pm i, \pm j\}$. Then $\mu_S(\pm i) = \mu_S(\pm j) = 1/6$, $\mu_S(1) = 1/3$.

Q_2 has four one-dimensional representations (characters):

$$\chi_0 \equiv 1,$$
$$\chi_1(\pm 1) = +1, \quad \chi_1(\pm i) = +1, \quad \chi_1(\pm j) = -1, \quad \chi_1(\pm k) = -1,$$
$$\chi_2(\pm 1) = +1, \quad \chi_2(\pm i) = -1, \quad \chi_2(\pm j) = +1, \quad \chi_2(\pm k) = -1,$$
$$\chi_3(\pm 1) = +1, \quad \chi_3(\pm i) = -1, \quad \chi_3(\pm j) = -1, \quad \chi_3(\pm k) = +1,$$

and one (faithful) two-dimensional representation π:

$$\pm 1 \mapsto \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \pm i \mapsto \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$
$$\pm j \mapsto \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \pm k \mapsto \pm \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}.$$

Let μ be a symmetric probability measure supported in S. Let

$$\mu(\pm i) = \alpha/2, \quad \mu(\pm j) = \beta/2, \quad \mu(1) = \gamma.$$

Then

$$\widehat{\mu}(\chi_0) = 1, \quad \widehat{\mu}(\chi_1) = 1 - 2\beta, \quad \widehat{\mu}(\chi_2) = 1 - 2\alpha, \quad \widehat{\mu}(\chi_3) = -1 + 2\gamma,$$
$$\widehat{\mu}(\pi) = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma \end{pmatrix}.$$

Hence

$$\|\mu - \lambda\|_{l^2 \to l^2} = \max\{|1 - 2\alpha|, |1 - 2\beta|, |-1 + 2\gamma|, \gamma\} \geq 1/3.$$

Indeed, we see that either $\gamma \geq 1/3$ or $|-1 + 2\gamma| \geq 1/3$. We also calculate that $\|\mu_S - \lambda\|_{l^2 \to l^2} = 1/3$.

EXAMPLE 4. Let $G = D_4$ be the dihedral group (see [4], p. 51). It has two generators a and b such that $a^4 = e,\ b^2 = e,\ bab = a^3$.

Let $S = S^{-1} = \{e, a, a^3, b\}$. Then $\mu_S(a) = \mu_S(a^3) = \mu_S(b) = \mu_S(e) = 1/4$. Let μ be a symmetric probability measure supported in S. As before we calculate the Fourier transform of μ. We write $\mu(e) = \gamma$, $\mu(a) = \mu(a^3) = \alpha/2$, $\mu(b) = \beta$. Then

$$\widehat{\mu}(\chi_0) = 1, \quad \widehat{\mu}(\chi_1) = 1 - 2\beta, \quad \widehat{\mu}(\chi_2) = -1 + 2\gamma, \quad \widehat{\mu}(\chi_3) = 1 - 2\alpha,$$
$$\widehat{\mu}(\pi) = \begin{pmatrix} \gamma - \beta & 0 \\ 0 & \gamma + \beta \end{pmatrix}.$$

Thus

$$\|\mu - \lambda\|_{l^2 \to l^2} = \max\{|1 - 2\alpha|, |1 - 2\beta|, |-1 + 2\gamma|, \gamma + \beta\} \geq 1/2.$$

Hence

$$\begin{aligned} \|\mu - \lambda\|_{l^2 \to l^2} &\geq \max\{|1 - 2\beta|, |-1 + 2\gamma|\} \geq (|1 - 2\beta| + |-1 + 2\gamma|)/2 \\ &\geq |2 - 2\beta - 2\gamma|/2 = \alpha. \end{aligned}$$

But $\|\mu_S - \lambda\|_{l^2 \to l^2} = 1/2$.

5. Factorization. Now we present a few examples of groups G and their generating symmetric sets S for which the equidistributed probability measure λ on G does not admit a factorization (1.2) with the measures $\mu_1, \ldots, \mu_n$ being supported on S. We also exhibit some cases when such a factorization exists.

PROPOSITION 5.1. *Let $G = \mathbb{Z}_p$, $S = S^{-1} = \{-a, \ldots, -1, 1, \ldots, a\}$, where $a < p/4$. Then λ has no factorization.*

P r o o f. For every probability measure μ supported by S we have

$$\widehat{\mu}(k) = \sum_{j=1}^{a} \gamma_j \cos \frac{2\pi kj}{p}$$

where $0 \leq k \leq p - 1$, $\gamma_j = 2\mu(j) = 2\mu(-j)$. Thus $\widehat{\mu}(1) > 0$, because $\cos \frac{2\pi j}{p} > 0$ for $1 \leq j \leq a$. Consequently, for every sequence $\mu_1, \mu_2, \ldots$ of such measures, $\prod_{j=1}^{n} \widehat{\mu}_j(1) > 0$. ∎

PROPOSITION 5.2. *Let $G = \mathbb{Z}_k^m$, where k is odd and $k > 3$, $S = S^{-1} = \{\pm e_1, \ldots, \pm e_m\}$, where $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$. Then λ has no factorization.*

P r o o f. We have

$$\widehat{\mu}(\chi) = \sum_{j=1}^{m} \gamma_j \cos \frac{2\pi \chi_j}{k},$$

where

$$\chi = (\chi_1, \dots, \chi_m), \qquad \chi_j \in \{0, \dots, k-1\},$$
$$\gamma_j = 2\mu((0, \dots, 0, 1, 0, \dots, 0)) = 2\mu(-(0, \dots, 0, 1, 0, \dots, 0)).$$

Notice that $\widehat{\mu}((1,1,\dots,1)) = \cos\frac{2\pi}{k}\sum_{j=1}^{m}\gamma_j = \cos\frac{2\pi}{k} > 0$, because k is odd and greater than 3. Thus $\prod_{j=1}^{n}\widehat{\mu}_j((1,1,\dots,1)) > 0$ for any sequence $\mu_1, \mu_2, \dots$ ∎

PROPOSITION 5.3. *Let $G = \mathbb{Z}_2^m$ and $S = \{\pm e_1, \dots, \pm e_m, \mathbf{0}\}$, where $\mathbf{0} = (0, \dots, 0)$ and $e_j = (0, \dots, 0, 1, 0, \dots, 0)$. Then λ has a factorization.*

Proof. Let μ be a probability measure with support in S. The Fourier transform of μ is

$$\widehat{\mu}(\chi) = \mu(\mathbf{0}) + \sum_{j=1}^{m}\mu(e_j)\cos\pi\chi_j,$$

where $\chi = (\chi_1, \dots, \chi_m)$, $\chi_j \in \{0, 1\}$.

Let χ be a nontrivial character. It is sufficient to construct a probability measure μ_χ supported in S such that $\widehat{\mu}_\chi(\chi) = 0$. Assume that $\chi_{j_1} = \dots = \chi_{j_k} = 1$ and $\chi_l = 0$ for $l \neq j_1, \dots, j_k$. Then $\widehat{\mu} = \mu(\mathbf{0}) - \mu(e_{j_1}) - \dots - \mu(e_{j_k})$. For μ_χ we take a measure such that $\mu_\chi(\mathbf{0}) = \mu_\chi(e_{j_1}) + \dots + \mu_\chi(e_{j_k})$ and $\mu_\chi(\mathbf{0}) > 0$; then indeed $\widehat{\mu}_\chi(\chi) = 0$. ∎

PROPOSITION 5.4. *Let G be the generalized quaternion group Q_m, where $m \geq 5$ (see [4], p. 52). G is a group of order $4m$ with two generators a and b such that a has order $2m$, $b^4 = 1$, $b^2 = a^m$, $bab^{-1} = a^{2m-1} = a^{-1}$. Let*

$$S = S^{-1} = \{a^0, a, a^{2m-1}, b, a^m b\}.$$

Then λ has no factorization.

Proof. For every probability measure μ supported on S we have (using notation from [4]), for $\varrho = \exp(\pi i/m)$,

$$\widehat{\mu}(\pi_{\varrho^2}) = \begin{pmatrix} \gamma - \beta + \alpha\cos\frac{2\pi}{m} & 0 \\ 0 & \gamma + \beta + \alpha\cos\frac{2\pi}{m} \end{pmatrix},$$

where $\gamma = \mu(e)$, $\alpha/2 = \mu(a) = \mu(a^{2m-1})$ and $\beta/2 = \mu(b) = \mu(a^m b)$. We see that

$$\gamma + \beta + \alpha\cos\frac{2\pi}{m} > 0. \ ∎$$

PROPOSITION 5.5. *Let G be the generalized quaternion group Q_m, where $2 \leq m \leq 4$. Let $S = S^{-1} = \{a^0, a, a^{2m-1}, b, a^m b\}$. Then λ has a factorization.*

Proof. It is easy to check that for every representation π of G there is a measure μ_π such that $\widehat{\mu}_\pi(\pi) = 0$. ∎

PROPOSITION 5.6 [2]. *Let $G = \mathcal{S}_n$ be the symmetric group and $S = \{(i,j) : i,j \in \{1,\dots,n\}\}$. Then λ has a factorization.*

P r o o f. We define $n-1$ measures as follows. Let μ_1 be the probability measure which is uniformly distributed on $\{(1,1),(1,2),\dots,(1,n)\}$, μ_2 uniformly distributed on $\{(2,2),(2,3),\dots,(2,n)\}$ and so on. It is clear $\mu_1 * \dots * \mu_{n-1} = \lambda$. ∎

6. The l^1-norm. We begin by showing

PROPOSITION 6.1. *Let G be a finite group and S an arbitrary subset of G. Then for every n such that $|G| \geq |S|^n \geq |S^n|$ we have*

$$\|\mu_1 * \dots * \mu_n - \lambda\|_{l^1} \geq \|\mu_S^{*n} - \lambda\|_{l^1} \tag{6.1}$$

for μ_S being the probability measure uniformly distributed on S and $\{\mu_n\}$ an arbitrary sequence of probability measures with supports in S.

P r o o f. We have

$$\begin{aligned}\|\mu_1 * \dots * \mu_n - \lambda\|_{l^1} &= \sum_{x\in S^n} \left|\mu_1 * \dots * \mu_n(x) - \frac{1}{|G|}\right| + \sum_{x\in G\setminus S^n} \frac{1}{|G|} \\ &\geq 1 - \frac{|S^n|}{|G|} + \frac{|G| - |S^n|}{|G|} = 2 - \frac{2|S^n|}{|G|}.\end{aligned} \tag{6.2}$$

We rewrite (6.2) for $\mu_1 = \dots = \mu_n = \mu_S$:

$$\|\mu_S^{*n} - \lambda\|_{l^1} = \sum_{x\in S^n} \left|\mu_S^{*n}(x) - \frac{1}{|G|}\right| + \sum_{x\in G\setminus S^n} \frac{1}{|G|}.$$

Since $\mu_S^{*n}(x) \geq |S|^{-n}$ for all $x \in S^n$ and $|G| \geq |S|^n$, we have $\mu_S^{*n}(x) - |G|^{-1} \geq 0$, whence

$$\|\mu_S^{*n} - \lambda\|_{l^1} = 2 - \frac{2|S^n|}{|G|}$$

and so (6.1) is proved. ∎

Proposition 6.1 shows that for the l^1-norm for small n no sequence can be better than a convolution power of the measure uniformly distributed on S. For large n, however, the situation may be different.

We need some notions and facts from [3].

Let G be (as before) a finite group. For a symmetric set S of generators we define the *volume growth* function $V(n)$ by

$$V(n) = |S^n|.$$

The *diameter* γ of G with respect to S is defined by

$$\gamma = \min\{n : V(n) = |G|\}.$$

We say that the group G has (A,d)-*moderate growth* with respect to S if there are positive constants A and d such that

$$\frac{V(n)}{V(\gamma)} \geq \frac{1}{A}\left(\frac{n}{\gamma}\right)^d, \qquad 1 \leq n \leq \gamma.$$

THEOREM 6.2 ([3], Theorem 3.2). *Let G be a finite group with generating set S. Suppose G has (A,d)-moderate growth with respect to S. Let μ be a symmetric probability measure on G with $\eta = \inf\{\mu(x) : x \in S\backslash\{e\}\} > 0$. Then*

$$\|\mu - \lambda\|^n_{l^2\to l^2} \leq \|\mu^{*n} - \lambda\|_{l^1} \leq 2B\|\mu - \lambda\|^{n-\gamma^2}_{l^2\to l^2},$$

where $B = 2^{d(d+3)/4}A^{1/2}\eta^{-d/4}$. ∎

Now we are able to formulate

THEOREM 6.3. *Let G be a finite group with symmetric set S of generators which contains e and is invariant under inner automorphisms of G. Suppose G has (A,d)-moderate growth with respect to S. Let μ_S be uniformly distributed on S. Clearly, μ_S is central. Then there exists $n_0 \in \mathbb{N}$ such that*

$$\forall n \geq n_0, \qquad \|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^1} < \|\mu_S^{*2n} - \lambda\|_{l^1} \tag{6.3}$$

and

$$\forall n \in \mathbb{N}, \qquad \frac{\|\mu_S^{*2n} - \lambda\|_{l^1}}{\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^1}} \geq Ka^n, \qquad K > 0, a > 1, \tag{6.4}$$

where

$$\mu_1 = \mu + \nu_\varepsilon, \qquad \mu_2 = \mu - \nu_\varepsilon$$

and ν is defined by (3.1).

Proof. Because

$$\|\mu_S^{*2n} - \lambda\|_{l^1} \geq \|\mu_S^{*2n} - \lambda\|_{l^2\to l^2} = \|\mu_S - \lambda\|^{2n}_{l^2\to l^2},$$

it is sufficient to show (using Theorem 6.2) that for large n,

$$\|\mu_S - \lambda\|^{2n}_{l^2\to l^2} > C\|\mu_1 * \mu_2 - \lambda\|^n_{l^2\to l^2},$$

where $C = 2^{d(d+3)/4}2A^{1/2}(1/|S|)^{-d/4}\|\mu_1 * \mu_2 - \lambda\|^{-\gamma^2}_{l^2\to l^2}$. But from the proof of Theorem 3.1 we know that

$$\|\mu_S^{*2} - \lambda\|_{l^2\to l^2} > \|\mu_1 * \mu_2 - \lambda\|_{l^2\to l^2}.$$

Thus (6.4) follows from Theorem 6.2, since

$$\frac{\|\mu_S^{*2n} - \lambda\|_{l^1}}{\|(\mu_1 * \mu_2)^{*n} - \lambda\|_{l^1}} \geq \frac{\|\mu_S^{*2} - \lambda\|^n_{l^2\to l^2}}{C}\|\mu_1 * \mu_2 - \lambda\|^n_{l^2\to l^2}.$$ ∎

Remark 6.4. Theorem 6.3 remains true without the assumption of (A,d)-moderate growth, but then one might need more iterations of the measure $\mu_1 * \mu_2$.

P r o o f. Instead of Theorem 6.2 we use the inequality

$$\|\mu-\lambda\|_{l^2\to l^2} \le \|\mu-\lambda\|_{l^1} \le \sqrt{|G|}\,\|\mu-\lambda\|_{l^2\to l^2},$$

which is true for every probability measure μ on G. Then we obtain

$$\begin{aligned}
\|\mu_S^{*2n}-\lambda\|_{l^1} &\ge \|\mu_S^{*2n}-\lambda\|_{l^2\to l^2}\\
&> |G|^{1/2}\|\mu_1*\mu_2-\lambda\|^n_{l^2\to l^2} && \text{(for large } n)\\
&= |G|^{1/2}\|(\mu_1*\mu_2)^n-\lambda\|_{l^2\to l^2} && (\mu_1*\mu_2 \text{ is hermitian})\\
&\ge \|(\mu_1*\mu_2)^n-\lambda\|_{l^1}. \ \blacksquare
\end{aligned}$$

Acknowledgements. The author is grateful to Andrzej Hulanicki for his ideas, help and encouragement.

REFERENCES

[1] P. Diaconis, *Group Representations in Probability and Statistics*, IMS, Hayward, 1986.

[2] —, *Application of non-commutative Fourier analysis to probability problems*, in: Lecture Notes in Math. 1362, Springer, 1982, 51–100.

[3] P. Diaconis and L. Saloff-Coste, *Moderate growth and random walk on finite groups*, Geom. Funct. Anal. 4, (1994), 1–36.

[4] E. Hewitt and K. A. Ross, *Abstract Harmonic Analysis II*, Springer, Berlin, 1970.

Institute of Mathematics
Wrocław University
Pl. Grunwaldzki 2/4
50-384 Wrocław, Poland
E-mail: urban@math.uni.wroc.pl

Received 12 November 1996;
revised 26 February 1997