CONVOLUTION OF DISCRETE MEASURES ON LINEAR GROUPS

[1]Mei-Chu Chang

Abstract Let $p, q \in \mathbb{R}$ such that $1 < p < 2$ and $\frac{2}{p} = 1 + \frac{1}{q}$. Define

$$\|f\|_p' = \max_{x, G_1} \Big(\sum_{y \in G_1} |f(xy)|^p \Big)^{1/p} \tag{*}$$

where G_1 is taken in some class of subgroups specified later. We prove the following two theorems about convolutions.

Theorem 2. *Let $G = SL_2(\mathbb{C})$ equipped with the discrete topology. Then there is a constant $\tau = \tau_p > 0$ such that for $f \in \ell^p(G)$*

$$\|f * f\|_q^{1/2} \leq C \|f\|_p^{1-\tau} (\|f\|_p')^\tau,$$

where the maximum in $(*)$ is taken over all abelian subgroups $G_1 < G$ and $x \in G$.

Theorem 3. *There is a constant $C = C_p > 0$ and $1 > \tau = \tau_p > 0$ such that if $f \in \ell^p\big(SL_3(\mathbb{Z})\big)$, then*

$$\|f * f\|_q^{1/2} \leq C \|f\|_p^{1-\tau} (\|f\|_p')^\tau$$

where the maximum in $(*)$ is taken over all nilpotent subgroups G_1 of $SL_3(\mathbb{Z})$ and $x \in SL_3(\mathbb{Z})$.

This paper is a continuation of our earlier work [C] on product theorems in the groups SL_2 and SL_3.We show here how they may be applied to obtain nontrivial convolution estimates of discrete measures on $SL_2(\mathbb{C})$ and $SL_3(\mathbb{Z})$ (see Theorem 2 in

[1]partially supported by NSF.

2000 Mathematics Subject Classification. 05A99, 15A99, 05C25; 20G40, 20D60, 11B75 .

Keywords: unimodular group, measure convolution

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

§1 and Theorem 3 in §2). Random walks and decay estimates for iterated convolutions of a fixed symmetric measure ν on a group G is a well studied topic on which there is an extensive literature(some further considerations on the relation to our results appear in §3 of the paper). We are not aware however of prior work that has to do with single convolutions of arbitrary measures (keeping in mind of course the 'Kunze-Stein' type phenomena but those have to do with convolution in Lebesgue spaces $L(G)$), except for very recent developments such as [BG1] and [BG2] (that are part of the motivation for this work). Roughly speaking, the general sense of our results on convolution, as expressed in Theorem 2 and Theorem 3,is that a gain on the usual inequality appears as soon as the measure does not put much weight on a coset of a nilpotent subgroup. This principle, that likely has extensions beyond the particular cases studied here, is formulated in a qualitative form, without specifying the exponents. (See §3 Remark 2.) That could be done however as all our arguments are effective, but the result would not be very pleasing. The reason is that the nature of our present technique does not allow to be very efficient in this respect. The simplest case to study further from the point of view of obtaining precise inequalities (recall Kesten's theorem [K] for the random walk), would be convolution on the free group. The very recent work of A.Razborov [R] provides indeed the optimal product theorem for general subsets of the free group.

For a set A, denote $A^n = A \cdots A = \{a_1 \cdots a_n : a_i \in A\}$, the *n-fold product set* of A.

The precise statements from [C] are the following.

Theorem A. *Let A be a finite subset of $SL_2(\mathbb{C})$. Then one of the following alternatives holds.*

(i) *A is contained in a virtually abelian subgroup*

(ii) $|A^3| > c|A|^{1+\delta}$ *for some absolute constant $\delta > 0$.*

Theorem B. *For all $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset SL_3(\mathbb{Z})$ is a finite set, then one of the following alternatives holds.*

(i) *A intersects a coset of a nilpotent subgroup in a set of size at least $|A|^{1-\varepsilon}$.*

(ii) $|A^3| > |A|^{1+\delta}$.

From the product theorems for sets obtained above, one may derive convolution inequalities. The passage from the "set-theoretical" to the "statistical" result is achieved using the "Balog-Szemeredi-Gowers Theorem". The version we need in our context is that of discrete sets in non-abelian groups (see [T] for the precise statements).

Notations and Conventions.

1. Let G be a discrete group. For any $f \in \ell^p(G)$ the ℓ^p norm is$\|f\|_p = \left(\sum_{x\in G} |f(x)|^p\right)^{1/p}$.

2. $f * g(x) = \sum_{y\in G} f(y)g(xy^{-1})$.

3. For $p \in \mathbb{R}$, p' is defined as $\frac{1}{p} + \frac{1}{p'} = 1$.

4. For a set A, $\mathcal{X}_A$ is the indicator function of A.

5. We use A^n for both the n-fold product set and n-fold Cartesian product when there is no ambiguity.

6. $A^{[n]} = (\{1\} \cup A \cup A^{-1})^n$, the set of $\leq n$-fold products of elements in $A \cup A^{-1}$.

7. $\mathrm{Tr}(g)$ is the trace of g.

8. Note that the properties under consideration (e.g. the size of a set of matrices or the trace of a matrix) are invariant under base change (i.e. conjugation by an invertible matrix).

9. We follow the trend that ε, (respectively, δ, or C) may represent various constants, even in the same setting. Also, $f(x) \sim g(x)$ means $f(x) = cg(x)$ for some constant c which may depend on some other parameters.

Facts.

(1) $\sum_{x\in G} f(x)^\theta g(x)^{1-\theta} \leq (\sum f(x))^\theta (\sum g(x))^{1-\theta}$.

(2) $\|f * g\|_p \leq \|f\|_1 \; \|g\|_p$.

(3) $\|f * g\|_\infty \leq \|f\|_{p'} \; \|g\|_p$.

(4) $\|f * g\|_q \leq \|f\|_{p_1} \; \|g\|_{p_2}$, where $\frac{1}{p_1} + \frac{1}{p_2} = 1 + \frac{1}{q}$.

§1 The $SL_2(\mathbb{C})$ case.

Proposition 1.

(i) *Let $G = SL_2(\mathbb{C})$ and let $A \subset G$ be a finite set such that*

$$\|\mathcal{X}_A * \mathcal{X}_A\|_2 > \frac{1}{K}|A|^{3/2}, \text{ with } K > 1. \tag{1.1}$$

Then there is a coset S of an abelian subgroup of G such that

$$|A \cap S| > K^{-C}|A|, \tag{1.2}$$

where C is an absolute constant.

(ii) *Let $G = SL_3(\mathbb{Z})$ and let $A \subset G$ be a finite set such that*

$$\|\mathcal{X}_A * \mathcal{X}_A\|_2 > |A|^{\frac{3}{2}-\varepsilon}, \text{ for some } \varepsilon > 0. \tag{1.3}$$

Then there is a coset S of a nilpotent subgroup of G such that

$$|A \cap S| > |A|^{1-\delta}, \tag{1.4}$$

where $\delta = \delta(\varepsilon) \to 0$ as $\varepsilon \to 0$.

Proof. Statement (i) is obtained combining the Balog-Szemeredi-Gowers Theorem with Theorem A and statement (ii) similarly using Theorem B instead. We will only prove statement (i).

The assumption (1.1) is equivalent to the following statement on $E(A, A)$, the "multiplicative energy" in the sense of [TV]

$$E(A, A) = |\{(x_1, x_2, x_3, x_4) \in A \times \cdots \times A : \ x_1x_2 = x_3x_4\}| > \frac{1}{K^2}\, |A|^3.$$

According to the Balog-Szemeredi-Gowers theorem in the version from [T], there exist an absolute constant C_1 and a "K^{C_1}-approximative group" (characterized by properties (a) and (b) below) H of G with the following properties (See Theorem 2.48 in [TV].)

(a) $H = H^{-1}$, and $1 \in H$.

(b) There is a subset $X \subset G$, with $|X| < K^{C_1}$ such that

$$H^2 \subset HX \cap XH.$$

(c) $|A| \le |H| < K^{C_1}|A|$.

(d) There is an element $x \in G$ such that

$$|A \cap xH| > \frac{1}{K^{C_1}}\, |A|.$$

Iterating (b) gives

$$|H^3| < |H^2X| \le |HX^2| < K^{2C_1}|H|. \tag{1.8}$$

The inequality (1.2) in the proposition only requires justification if $K \le |A|^{1/C}$. We choose C large enough such that $2C_1/C < \delta$. Property (c), inequality (1.8), and Theorem A imply that

$$|H^3| < |H|^{1+\delta}$$

and H is contained in a virtually abelian subgroup G' of G. In fact G' has an abelian subgroup G_1 of index ≤ 2. Hence for some $\xi \in G$, we have $|H \cap \xi G_1| \geq \frac{1}{2}|H|$. In particular,

$$|H \cap \xi G_1| \geq \frac{1}{K^C}\,|H|. \tag{1.6}$$

In (d), let $A_1 = A \cap xH$. We have

$$|A_1| > K^{-C}|A|, \tag{1.7}$$

and

$$|HA_1^{-1}| < |H^2| < |X|\,|H| < K^C|H|. \tag{1.8}$$

Clearly, for any sets H and A_1, we have

$$\mathcal{X}_H \leq \frac{1}{|A_1|} \sum_{x_1 \in HA_1^{-1}} \mathcal{X}_{x_1 A_1}. \tag{1.9}$$

Applying (1.9) on the set $H \cap \xi G_1$, together with (1.6), we obtain

$$\begin{aligned} K^{-C}|H| \leq & \frac{1}{|A_1|} \sum_{x_1 \in HA_1^{-1}} |x_1 A_1 \cap \xi G_1| \\ \leq & \frac{1}{|A_1|}\,|HA_1^{-1}| \max_{x_1 \in HA_1^{-1}} |x_1 A_1 \cap \xi G_1|. \end{aligned}$$

Therefore, there exists $x_1 \in HA_1^{-1}$ such that

$$|A_1 \cap x_1^{-1}\xi G_1| \geq K^{-C}\,|H|\,\frac{|A_1|}{|HA_1^{-1}|} > K^{-3C}|A|$$

by (1.7) and (1.8). Hence (1.2) follows. □

We may also establish a more functional analytic statement that is reminiscent of the Kuntz-Stein theorem on convolution of $L^2\big(SL_2(\mathbb{R})\big)$-functions.

Theorem 2. *Let $G = SL_2(\mathbb{C})$ equipped with the discrete topology, and let $p, q \in \mathbb{R}$ such that $1 < p < 2$ and*

$$\frac{2}{p} = 1 + \frac{1}{q}. \tag{1.10}$$

Then there is a constant $\tau = \tau_p > 0$ such that for $f \in \ell^p(G)$

$$\|f * f\|_q^{1/2} \leq C\|f\|_p^{1-\tau}(\|f\|_p')^{\tau}, \tag{1.11}$$

where we define

$$\|f\|'_p = \max_{x,G_1} \Big(\sum_{y\in G_1} |f(xy)|^p \Big)^{1/p}$$

and the maximum is taken over all abelian subgroups $G_1 < G$ and $x \in G$.

Remark. Inequality (1.11) holds in particular for ℓ^p-functions on a free group. Certainly in this case, it would be interesting to find out what is the precise constant τ.

Proof of Theorem 2.

We may assume $f \geq 0$ and $\|f\|_p = 1$.

Breaking up G into level sets of f, we let

$$A_j = \{x \in G : 2^{-j-1} < f(x) \leq 2^{-j}\}.$$

It is easy to see that

$$f \leq \sum_{j\in\mathbb{Z}_+} 2^{-j} \mathcal{X}_{A_j} < 2f, \tag{1.12}$$

where the A_j are disjoint and

$$\sum 2^{-pj}\, |A_j| \sim 1. \tag{1.13}$$

In particular,

$$|A_j| \lesssim 2^{pj}. \tag{1.14}$$

Denote

$$\mathcal{X}_j = \mathcal{X}_{A_j}.$$

Let

$$\|f * f\|_q = \alpha, \text{ for some } 0 < \alpha \leq 1. \quad \text{(See Fact 4.)}$$

We will show that

$$\|f\|'_p > \alpha^C \tag{1.15}$$

for some constant $C = C_p$.

The claim (1.11) then immediately follows.

By (1.12), it is sufficient that we work on the function $f = \sum_{j\in\mathbb{Z}_+} 2^{-j}\mathcal{X}_j$.

Let

$$\beta = \min(\alpha^q, \alpha^{\frac{1}{p-1}}).$$

$$
\begin{aligned}
&I = \big\{ j \in \mathbb{Z}_+ : |A_j| > \beta\, 2^{pj} \big\} \\
&I' = \bigcup_{j\in I} \big\{ k \in \mathbb{Z}_+ : 2^{-|k-j|} > \beta \big\} = \bigcup_{j\in I} \big\{ k \in \mathbb{Z}_+ : |k-j| < \log_2 \frac{1}{\beta} \big\}.
\end{aligned}
$$

Hence

$$|I| < \frac{1}{\beta}, \quad \text{ and } \quad |I'| \lesssim \frac{1}{\beta} \log \frac{1}{\beta}. \tag{1.16}$$

Write

$$f = f_1 + f_2 + f_3,$$

where

$$
\begin{aligned}
f_1 &= \sum_{j\in I} 2^{-j} \mathcal{X}_j, \\
f_2 &= \sum_{j\in I'\setminus I} 2^{-j} \mathcal{X}_j, \\
f_3 &= \sum_{j\notin I'} 2^{-j} \mathcal{X}_j.
\end{aligned}
$$

Hence

$$
\begin{aligned}
\alpha = \|f*f\|_q &\le \|(f-f_3)*(f-f_3)\|_q + 2\|f_1 * f_3\|_q + 2\|f_2*f_3\|_q + \|f_3*f_3\|_q \\
&\le \|(f-f_3)*(f-f_3)\|_q + 2\|f_1*f_3\|_q + \|(f-f_1)*(f-f_1)\|_q.
\end{aligned} \tag{1.17}
$$

(Here we use the shorthand that $2\,\|f*g\|_q = \|f*g\|_q + \|g*f\|_q$.)

Claim. $\alpha \lesssim \ \|(f-f_3)*(f-f_3)\|_q$.

Proof of Claim.

First, by Fact 2, we have

$$
\begin{aligned}
\|f_1 * f_3\|_q \le & \sum_{\substack{j\in I \\ 2^{-|k-j|}\le\beta}} 2^{-j-k} \|\mathcal{X}_j * \mathcal{X}_k\|_q \\
& < \sum_{\substack{k>j \\ 2^{j-k}\le\beta}} 2^{-j-k} \|\mathcal{X}_j\|_1 \ \|\mathcal{X}_k\|_q + \sum_{\substack{k<j \\ 2^{k-j}\le\beta}} 2^{-j-k} \|\mathcal{X}_j\|_q \ \|\mathcal{X}_k\|_1,
\end{aligned}
$$

where the first term is bounded by

$$\begin{aligned}\sum_j \sum_{\substack{k>j\\ 2^{j-k}\le\beta}} 2^{-j-k}|A_j|\,2^{k\frac{p}{q}} &\lesssim \sum_j 2^{-j}\,|A_j|\,(\beta 2^{-j})^{1-\frac{p}{g}}\\ &< \beta^{1-\frac{p}{q}}\sum_j 2^{-j(2-\frac{p}{q})}|A_j|\\ &\sim \beta^{1-\frac{p}{q}} = \beta^{p-1} \le \alpha,\end{aligned}$$

estimating the geometry series $\sum_{k>j,2^k\ge\frac{2j}{\beta}} 2^{-k(1-\frac{p}{q})}$, and using (1.10) and (1.13). Similarly, we bound the second term by α. Thus

$$\|f_1 * f_3\|_q \lesssim \alpha. \tag{1.18}$$

Next,

$$\|(f-f_1)*(f-f_1)\|_q \le \sum_{j,k\notin I} 2^{-j-k}\|\mathcal{X}_j * \mathcal{X}_k\|_q,$$

and from definition of I

$$\begin{aligned}\sum_{j\le k;j,k\notin I} 2^{-j-k}\|\mathcal{X}_j * \mathcal{X}_k\|_q &\le \sum_{j\le k,k\notin I} 2^{-j-k}\,|A_j|(\beta\,2^{pk})^{1/q}\\ &\le\ \beta^{1/q}\sum_j 2^{-j}2^{-j(1-p/q)})\,|A_j|\\ &\lesssim\ \beta^{1/q}\le\alpha.\end{aligned}$$

Hence

$$\|(f-f_1)*(f-f_1)\|_q \lesssim \alpha. \tag{1.19}$$

The claim follows from (1.18) and (1.19). □

The claim implies that for some $j\le k\in I'$

$$2^{-j-k}\|\mathcal{X}_j * \mathcal{X}_k\|_q \gtrsim \alpha\beta^2\Big(\log\frac{1}{\beta}\Big)^{-2}.$$

Let

$$\gamma = \alpha\beta^2\Big(\log\frac{1}{\beta}\Big)^{-2}.$$

Then $\gamma > \alpha^{c(p)}$ for some constant $c(p)$, and

$$\|\mathcal{X}_j * \mathcal{X}_k\|_q \gtrsim \gamma\, 2^{j+k}. \tag{1.20}$$

Also, Fact 2 and (1.10) imply that

$$\gamma \lesssim 2^{-j-k}\|\mathcal{X}_j\|_1\, \|\mathcal{X}_k\|_q \leq 2^{-j-k}2^{pj}2^{\frac{p}{q}k} = 2^{(p-1)(j-k)}. \tag{1.21}$$

Assume $2 \leq q < \infty$ (for $1 < q < 2$ the argument is similar). We have

$$\begin{aligned}\|\mathcal{X}_j * \mathcal{X}_k\|_q &\leq \|\mathcal{X}_j * \mathcal{X}_k\|_\infty^{1-\frac{2}{q}}\, \|\mathcal{X}_j * \mathcal{X}_k\|_2^{\frac{2}{q}}\\ &\leq 2^{pk(1-\frac{2}{q})}\, \|\mathcal{X}_j * \mathcal{X}_k\|_2^{\frac{2}{q}}\end{aligned}$$

and by (1.20) and (1.21)

$$\begin{aligned}\|\mathcal{X}_j * \mathcal{X}_k\|_2 &\gtrsim \left(\gamma 2^{j+k-pk(1-\frac{2}{q})}\right)^{\frac{q}{2}}\\ &\gtrsim \gamma^q 2^{\frac{p}{2}(j+2k)}\\ &\gtrsim \gamma^{q+\frac{1}{2}\frac{p}{p-1}}\, 2^{\frac{3}{2}pk} = \alpha^{c'(p)}2^{\frac{3}{2}pk}.\end{aligned} \tag{1.22}$$

Denote

$$A = A_j \cup A_k.$$

Since $j \leq k$,

$$|A| \lesssim 2^{pk}.$$

Also, by Fact 2 and (1.22)

$$|A|^{3/2} = \|\mathcal{X}_A\|_1\, \|\mathcal{X}_A\|_2 \geq \|\mathcal{X}_A * \mathcal{X}_A\|_2 > \alpha^{c'(p)}2^{\frac{3}{2}pk} \gtrsim \alpha^{c'(p)}\, |A|^{\frac{3}{2}}.$$

Hence

$$2^{-kp}\, |A| \geq \alpha^{c(p)}, \tag{1.23}$$

and

$$\|\mathcal{X}_A * \mathcal{X}_A\|_2 > \alpha^{c'(p)}\, |A|^{\frac{3}{2}}. \tag{1.24}$$

Invoking Proposition 1 (i), we obtain therefore that

$$|A \cap S| > \alpha^{C(p)}|A|, \tag{1.25}$$

where S is a coset of an abelian subgroup.

Hence, by (1.23)

$$\begin{aligned}\|f\|'_p &\geq \Big(\sum_{x\in S}|f(x)|^p\Big)^{1/p}\\ &\gtrsim 2^{-j}|S\cap A_j|^{1/p}+2^{-k}|S\cap A_k|^{1/p}\\ &> 2^{-k}|S\cap A|^{1/p}\\ &> \alpha^{C(p)}2^{-k}|A|^{1/p}\\ &> \alpha^{C'(p)}\end{aligned}$$

which is (1.15).

This proves Theorem 2.

§2 The $SL_3(\mathbb{Z})$ case.

Our goal in this section is to establish the analogue of Theorem 2 for $G = SL_3(\mathbb{Z})$, defining now

$$\|f\|'_p = \max_{x, G_1}\Big(\sum_{y\in G_1}|f(xy)|^p\Big)^{1/p}$$

and the maximum being taken over all nilpotent subgroups G_1 of G and $x\in G$.

This requires however to prove the analogue of Proposition 1 (i) in $SL_3(\mathbb{Z})$ (with "abelian" replaced by "nilpotent"), which is a stronger statement then Proposition 1 (ii) (which covers only the case when $\log M \sim \log|A|$). 'This will require to revisit the arguments in [C] and refine some of those steps.Thus at this point, a certain familiarity with the method explained in [C] is desirable.

Once the counterpart of Proposition 1 (i) for $SL_3(\mathbb{Z})$ is obtained, the proof of Theorem 2 for $SL_3(\mathbb{Z})$ (Theorem 3 below) proceeds exactly the same way.

We will use the following proposition proved in [C]

Proposition C. *If $A\subset GL_3(\mathbb{C})$ is a finite set and M large, then one of the following holds.*

(1) There is $\tilde{g}\in A^{[3]}$ such that $|Tr\,(\tilde{g}A)| > M$,

(2) There is a subset A' of $A, |A'| > M^{-C}|A|$ (C an absolute constant) such that A' is contained in a coset of a nilpotent subgroup.

Let $A\subset SL_3(\mathbb{Z})$ be a finite set and M be a large number, such that

$$|A^3| < M|A| \tag{2.1}$$

and

$$|A \cap S| < M^{-C}|A| \tag{2.2}$$

whenever S is a coset of a nilpotent subgroup of $G = SL_3(\mathbb{Z})$.

In (2.2), C is an absolute constant and our aim in what follows is to show that if we take C large enough, a contradiction follows.

Applying Proposition C, we obtain $\tilde{g} \in A^{[3]}$ such that

$$|Tr\, \tilde{g}A| > M^{C_1} \tag{2.3}$$

$\big($as a consequence of assumption (2.2)$\big)$, where $C_1(C) \to \infty$ as $C \to \infty$.

For any $x \in G$, let C_x be the conjugacy class containing x,

$$C_x = \{g^{-1}xg : g \in G\}. \tag{2.4}$$

Let Q be the number of non-congugate elements in $A^{[4]}$, i.e.

$$Q = |\{C_x : x \in A^{[4]}\}|.$$

By (2.3)

$$Q \geq M^{C_1}.$$

From Helfgott's argument (see also [C] §4 Claim 1), we obtain a subset $D \subset A^{-1}A$ of simultaneously diagonalizable matrices with

$$|D| = Q \geq M^{C_1}. \tag{2.5}$$

Next, we aim to amplify the number of conjugacy classes.

We fix a basis in which the elements of D are diagonal. Therefore, each $g \in D$ is diagonal with diagonal entries $\Lambda(g) = \{\lambda_1(g), \lambda_2(g), \lambda_3(g)\}$ forming a system of conjugate units in O_K. Here O_K denotes the unit group of a certain extension field K of Q with $[K : \mathbb{Q}] \leq 6$.

Case 1. There exists an element $h = (h_{ij}) \in A$ such that every column of h has at least two nonzero entries.

Note that our assumption implies that every row of h has at least two nonzero entries. Hence

(*) *For i fixed, there exist $k \neq k'$ and j, with $h_{ik} \neq 0, h_{ik'} \neq 0, h_{kj} \neq 0, h_{k'j} \neq 0$.*

($\diamond$) *Given i and j, there exists k with $h_{ik} \neq 0, h_{kj} \neq 0$.*

Let us fix such $h \in A$.

Also let $z \in SL_3(\mathbb{Z})$ be any (fixed) element, which we will specify later.

We consider the set

$$\Big\{g^{(1)}hg^{(2)}h\cdots hg^{(\ell)}z:\ g^{(1)},\cdots,g^{(\ell)}\in D\Big\} \tag{2.6}$$

For $\bar{g} = \big(g^{(1)}\cdots g^{(\ell)}\big) \in D^\ell = D \times \cdots \times D$, we let

$$\bar{g}_z = g^{(1)}h\,g^{(2)}h\cdots g^{(\ell)}z \tag{2.7}$$

be in the set (2.6). Then

$$\operatorname{Tr}\bar{g}_z = \sum_{i,\dots,i_\ell} h_{i_1i_2}\cdots h_{i_{\ell-1}i_\ell}\ z_{i_\ell i_1}\ \lambda_{i_1}\big(g^{(1)}\big)\cdots\lambda_{i_\ell}\big(g^{(\ell)}\big),$$

which we consider as a polynomial in $\lambda_i\big(g^{(j)}\big) \in O_K$ with $1 \le i \le 3$, and $1 \le j \le \ell$.

Thus

$$\operatorname{Tr}\bar{g}_z = \sum_{1\le s\le t} a_s x_s, \tag{2.8}$$

where

$$x_s = \lambda_{i_1}\big(g^{(1)}\big)\cdots\lambda_{i_\ell}\big(g^{(\ell)}\big) \in O_K, \tag{2.9}$$

$a_1,\dots,a_t$ are the non-vanishing coefficients

$$a_s = h_{i_1i_2}h_{i_2i_3}\dots h_{i_{\ell-1}i_\ell}z_{i_\ell i_1} \neq 0, \tag{2.10}$$

and s corresponds to the multi-index $(i_1,\dots,i_\ell)$ such that (2.10) holds.

We will use the following some result derived from the Subspace theorem by Evertse, Schlickewei, and Schmidt [ESS].

Proposition D. *Let $G < \langle\mathbb{C}^*,\cdot\rangle$ be a multiplicative group of rank r and fix an integer $t \ge 2$. Let $a_1,\dots,a_{2t} \in \mathbb{C}\backslash\{0\}$. There is a set $E \subset \mathbb{C}$ depending on $a_1,\dots,a_{2t}$,*

$$|E| < C(r,t)$$

such that the following holds.

Let $\mathcal{A}$ be a finite subset of $G^t = G \times \cdots \times G$ and such that

$$\frac{x_i}{x_j} \notin E \text{ for all } x = (x_s)_s \in \mathcal{A} \text{ and } 1 \le i \neq j \le t. \tag{2.11}$$

Then

$$\big|\{(x,x')\in\mathcal{A}\times\mathcal{A}:\ a_1x_1+\cdots+a_tx_t = a_{t+1}x'_1+\cdots+a_{2t}x'_t\}\big| < C(r,t)|\mathcal{A}|. \tag{2.12}$$

Proposition D'. *Let G be as in Proposition D. Given $a_1, \dots, a_t \in \mathbb{C}\backslash\{0\}$, there is a subset $E \subset \mathbb{C}$ with $|E| < C(r,t)$, such that if $\mathcal{A}$ is a finite subset of $G^t = G \times \cdots \times G$ satisfying (2.11), then*

$$\Big|\Big\{\sum_{s=1}^{t} a_s x_s : \ x \in \mathcal{A}\Big\}\Big| > \frac{1}{C(r,t)}|\mathcal{A}|.$$

Let $\mathcal{D} \subset D^\ell = D \times \cdots \times D$ consisting of all $\bar{g} = \big(g^{(1)}, \cdots, g^{(\ell)}\big)$ such that $(x_1, \cdots, x_t)$ arisen from $\bar{g}$ via (2.8)-(2.10) satisfies

$$\frac{x_i}{x_j} \in E \text{ for } 1 \leq i \neq j \leq t.$$

Let $\mathcal{A}$ be the image of $D^\ell \backslash \mathcal{D}$ under the map

$$\psi : D^\ell \backslash \mathcal{D} \to \mathcal{A} \to 0$$

given by

$$\bar{g} = \big(g^{(1)}, \dots, g^{(\ell)}\big) \mapsto x = (x_s)_{1 \leq s \leq t}$$

(notice that $\mathcal{D}$ and $\mathcal{A}$ may obviously be taken independently of z).

From Proposition D', it follows then that

$$\Big|\big\{\text{Tr } \bar{g}_z : \ \bar{g} \in D^\ell \backslash \mathcal{D}\big\}\Big| > \frac{|\mathcal{A}|}{C(\ell)}.$$

But for our purpose, we need the stronger statement provided by Proposition D. Thus by (2.12)

$$\Big|\Big\{(x, x') \in \mathcal{A} \times \mathcal{A} : \sum a_s x_s = \sum a_s x'_s\Big\}\Big| < C(\ell)|\mathcal{A}|.$$

Next we examine the map ψ in (2.11) for its bijective properties. We will show that

$$|\psi^{-1}(x)| < 4^{\ell-4} \ |D|^4$$

.

Take $i_1, \dots, i_{\ell-4}$ such that $h_{i_1 i_2} \neq 0, \dots, h_{i_{\ell-5} i_{\ell-4}} \neq 0$.

Take $i_{\ell-3} \neq i'_{\ell-3}$ and $i_{\ell-2}$ such that $h_{i_{\ell-4}\, i_{\ell-3}} \neq 0$, $h_{i_{\ell-4}\, i'_{\ell-3}} \neq 0$, $h_{i_{\ell-3}\, i_{\ell-2}} \neq 0$ and $h_{i'_{\ell-3}\, i_{\ell-2}} \neq 0$. (This is possible by (*).) Finally, take i_ℓ such that $z_{i_\ell\, i_1} \neq 0$ and $i_{\ell-1}$ satisfying $h_{i_{\ell-2}\, i_{\ell-1}} \neq 0$ and $h_{i_{\ell-1}\, i_\ell} \neq 0$. (This is possible by ($\diamond$).)

Hence

$$s \leftrightarrow (i_1, \dots , i_{\ell-4}, i_{\ell-3}, i_{\ell-2}, i_{\ell-1}, i_\ell)$$

and

$$s' \leftrightarrow (i_1, \dots , i_{\ell-4}, i'_{\ell-3}, i_{\ell-2}, i_{\ell-1}, i_\ell)$$

are admissible (meaning that (2.10) holds) and

$$\frac{x_s}{x_{s'}} = \frac{\lambda_{i_{\ell-3}}(g^{(\ell-3)})}{\lambda_{i'_{\ell-3}(g^{(\ell-3)})}}.$$

Hence by the following fact, (x_s) determines $g^{(\ell-3)} \in D$, up to four choices.

Fact 5. Let $D \subset GL_3(\mathbb{C})$ be a set of diagonal matrices obtained from a subset of $SL_3(\mathbb{Z})$ after base change. Then given any $z \in \mathbb{C}$, for $i \neq j$, there are at most four elements $g \in D$ for which

$$\frac{\lambda_i(g)}{\lambda_j(g)} = z,$$

where $\lambda_i(g)$ and $\lambda_j(g)$ are the eigenvalues of g.

Similarly we recover $g^{(\ell-4)}, \dots , g^{(2)}$. Consequently the map ψ has multiplicity at most $4^{\ell-4}|D|^4$ and (2.11)-(2.13) imply that

$$\begin{aligned} &\left|\left\{(\bar{g}, \bar{g}') \in (D^\ell \backslash \mathcal{D}) \times (D^\ell \backslash \mathcal{D}) : \text{ Tr } \bar{g}_z = \text{Tr } \bar{g}'_z\right\}\right| \\ <&C(\ell)\ |D|^8 |\mathcal{A}| \\ <&C(\ell)\ |D|^{\ell+8}. \end{aligned} \tag{2.13}$$

This statement is valid for all $z \in SL_3(\mathbb{Z})$.

Next, we prove

Claim 1.

$$\sum_{\bar{g} \in D^\ell \backslash \mathcal{D}} |C_{\bar{g}_z} \cap A| < C(\ell)\ |D|^{\frac{\ell+8}{2}}\ |A|, \qquad \text{for any } z \in SL_3(\mathbb{Z}).$$

Proof of Claim 1.

Denote

$$n(\tau) = \left|\left\{\bar{g} \in D^\ell \backslash \mathcal{D} : \ C_{\bar{g}_z} = C_\tau\right\}\right|.$$

Hence

$$\sum_\tau n(\tau) = |D^\ell \backslash \mathcal{D}| \sim |D|^\ell,$$

and by (2.13), we clearly also have that

$$\sum n(\tau)^2 < C(\ell)|D|^{\ell+8}. \tag{2.14}$$

Estimate using Cauchy-Schwartz and (2.14)

$$\begin{aligned}\sum_{\bar{g}\in D^\ell\backslash\mathcal{D}} |C_{\bar{g}_z} \cap A| &= \sum_\tau n(\tau)|C_\tau \cap A| \\ &\leq \Big[\sum_\tau n(\tau)^2\Big]^{1/2} \Big[\sum_\tau |C_\tau \cap A|^2\Big]^{1/2} \\ &< C(\ell)|D|^{\frac{\ell+8}{2}}\ |A|. \end{aligned} \tag{2.15}$$

Here $z \in SL_3(\mathbb{Z})$ is still arbitrary. □

Let

$$A_1 = A^{[3\ell]}.$$

Next, we prove

Claim 2.

$$\sum_{\bar{g}\in D^\ell\backslash\mathcal{D}} |C_{\bar{g}_z} \cap A| \gtrsim Q^{\ell-1}\frac{|A|^2}{|A_1|}, \quad \text{for some } z \in A_1.$$

Proof. Averaging $\sum_{\bar{g}\in D^\ell\backslash\mathcal{D}} |C_{\bar{g}_z} \cap A|$ over all $z \in A_1$, we have

$$\frac{1}{|A_1|}\sum_{z\in A_1}\sum_{\bar{g}\in D^\ell\backslash\mathcal{D}} |C_{\bar{g}_z} \cap A| = \frac{1}{|A_1|}\sum_{\bar{g}\in D^\ell\backslash\mathcal{D}}\sum_{z\in A_1} |C_{\bar{g}_z} \cap A|. \tag{2.16}$$

Fix $\bar{g} \in D^\ell\backslash\mathcal{D}$. We want to show

$$\sum_{z\in A_1} |C_{\bar{g}_z} \cap A| \geq \frac{|A|^2}{Q}. \tag{2.17}$$

Denote

$$n_0(\tau) = \big|\{z' \in A : C_{z'} = C_\tau\}\big| = |C_\tau \cap A|.$$

Since $|\{\tau : n_0(\tau) \neq 0\}|$ is the number of non-conjugate elements of A, it is $\leq Q$. $\big($ cf (2.4)$\big)$ We obtain

$$|A| = \sum_\tau n_0(\tau) \leq \big|\{\tau : n_0(\tau) \neq 0\}\big|^{1/2} \Big[\sum n_0(\tau)^2\Big]^{1/2}$$
$$\leq Q^{1/2}\Big[\sum n_0(\tau)\ |C_\tau \cap A|\Big]^{1/2}$$

Hence

$$\sum n_0(\tau)\ |C_\tau \cap A| \geq \frac{|A|^2}{Q}. \tag{2.18}$$

Taking z of the particular form

$$z = \big(g^{(1)} h \cdots g^{(\ell)}\big)^{-1} z', \text{ with } z' \in A,$$

by (2.18), we certainly have

$$\sum_{z \in A_1} |C_{\bar{g}_z} \cap A| \geq \sum_{z' \in A} |C_{z'} \cap A| = \sum_\tau n_0(\tau)\ |C_\tau \cap A| \geq \frac{|A|^2}{Q}.$$

Therefore, by (2.5) and (2.17), (2.16) is bounded below by

$$\frac{1}{|A_1|}\ |D^\ell \backslash \mathcal{D}|\ \frac{|A|^2}{Q} \sim |D|^\ell\ \frac{|A|^2}{|A_1|\ Q} = Q^{\ell-1} \frac{|A|^2}{|A_1|}.$$

This concludes the proof of Claim 2. □

Putting together Claim 1 and Claim 2, we conclude that

$$C(\ell)\ |D|^{\frac{\ell+8}{2}}\ |A| \gtrsim Q^{\ell-1} \frac{|A|^2}{|A_1|}.$$

Hence we proved that

$$|A_1| > \frac{1}{C(\ell)}\ Q^{\frac{\ell}{2}-5}\ |A| > \frac{1}{C(\ell)}\ M^{C_1(\frac{\ell}{2}-5)}\ |A|, \tag{2.19}$$

by (2.5).

Recalling assumption (2.1), we also have $\big($see [TV], or Proposition 1.6 in [C]$\big)$ that

$$|A_1| < M^{3(3\ell-2)}\ |A|.$$

Taking $\ell = 12$ in (2.19), and taking C_1 $\big($hence C in (2.2)$\big)$ large enough, a contradiction follows. Hence we completed the argument for Case 1.

Case 2. Every element in A has a column with exactly one nonzero entry.

Thus we can assume that there is a subset $A_1 \subset A$ with $|A_1| \geq \frac{|A|}{9}$ and elements $g \in A_1$ have the form

$$g = \begin{pmatrix} \lambda & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix}.$$

Let

$$B = \left\{ \bar{g} \in SL_2(\mathbb{C}) :\ \exists\, g \in A_1,\ g = \left(\begin{array}{c|cc} \lambda & * & * \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{$\lambda'\bar{g}$}} \\ 0 & & \end{array} \right),\ \text{where } \lambda' = \frac{\det g}{\lambda} \right\},$$

and we have a map $A_1 \to B$ by sending $g \to \bar{g}$ in the above sense.

Pigeonholing guaranteers an element $\bar{g}_1 \in B$ and a subset $A_2 \subset A_1$ with

$$|A_2| > \frac{|A_1|}{|B|} \gtrsim \frac{|A|}{|B|} \tag{2.20}$$

such that

$$\forall g \in A_2,\ \bar{g} = \bar{g}_1.$$

Therefore, for all $g \in g_1^{-1} A_2$,

$$g = \begin{pmatrix} \lambda & * & * \\ 0 & \lambda' & 0 \\ 0 & 0 & \lambda' \end{pmatrix}.$$

The following fact implies that $\lambda = 1$ and $\lambda' = \pm 1$.

Fact 6. Let $f(x) \in \mathbb{Z}[x]$ be a monic cubic polynomial over $\mathbb{Z}$. Then either $f(x)$ is irreducible over $\mathbb{Q}$ and has three distinct roots, or one of the roots is in $\mathbb{Q}$ and the other two roots are quadratic conjugates, or $f(x)$ has three roots in $\mathbb{Q}$. Hence if the constant term of $f(x)$ is -1, the only possible multiple roots are $1, 1, 1$ or $1, -1, -1$.

Case 2.(i). $|B| < M^{C_2/\delta}$ (where δ refers to Theorem B).

Let

$$S = g_0 \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\},$$

some coset of a nilpotent group. Here $g_0 = g_1$, if more than half of $g_1^{-1} A_2$ have $\lambda' = 1$. Otherwise $g_0 = g_1 \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$.

By (2.20), we have

$$|A \cap S| \gtrsim |A_2| \gtrsim M^{-C_2/\delta} |A|$$

contradicting assumption (2.2).

Case 2.(ii). $|B| \geq M^{C_1/\delta}$

Claim. $|B^3| < |B|^{1+\delta}$

Proof. Otherwise, assume $|B^3| > |B|^{1+\delta} > M^{C_1} |B|$.

For each $b \in B^3$, denote

$$g_b^{(1)}, g_b^{(2)}, g_b^{(3)} \in A_1$$

elements such that

$$\overline{g_b^{(1)}}\ \overline{g_b^{(2)}}\ \overline{g_b^{(3)}} = b.$$

We note that

$$g_{b_1}^{(1)}\ g_{b_1}^{(2)}\ g_{b_1}^{(3)}\ A_2 \bigcap g_{b_2}^{(1)}\ g_{b_2}^{(2)}\ g_{b_2}^{(3)}\ A_2 \ = \ \emptyset, \text{ for } b_1 \neq b_2.$$

Clearly

$$|A^{[4]}| \geq |A_1^4| \geq \Big| \bigcup_{b \in B^3} g_b^{(1)} g_b^{(2)} g_b^{(3)} A_2 \Big| = \sum_{b \in B^3} |A_2| > M^{C_1} |B| \frac{|A_1|}{|B|} \gtrsim M^{C_2} |A|.$$

This contradicts (2.1) for C_1 large enough. □

Therefore, Theorem B permits us to assume B contained in some coset of an abelian subgroup G_1 of $SL_2(\mathbb{C})$.

After change basis, elements in G_1 can be triangularized simultaneously. Either half of $B \subset xG_1$ are of the form $x \begin{pmatrix} \lambda' & * \\ 0 & \lambda' \end{pmatrix}$ for some $\lambda' \in \mathbb{C}$, or half are of the form

$x\begin{pmatrix}\lambda_1 & * \\ 0 & \lambda_2\end{pmatrix}$ with $\lambda_1, \lambda_2 \in \mathbb{C}$. The remark below implies that we may assume the factorization is over $\mathbb{Z}$.

Remark. If $B = \xi T \subset SL_n(\mathbb{Z})$ with $\xi \in SL_n(\mathbb{C})$, and $T \subset SL_n(\mathbb{C})$ all upper triangular or all diagonal, then there exists $\xi' \in SL_n(\mathbb{Z})$ and $T' \subset SL_n(\mathbb{Z})$ all upper triangular or all diagonal and $B = \xi' T'$.

Proof. We pick any $t \in T$, and let $\xi' = \xi t \in B \in SL_n(\mathbb{Z})$. Then $T' := (\xi t)^{-1}B = t^{-1}T \subset SL_n(\mathbb{Z})$, all upper triangular or all diagonal, and $B = (\xi t)T'$.

There are 2 possibilities.

Case 2.(ii).(a).

$$A_1 \subset \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{λx}} \\ 0 & & \end{array}\right)\left\{\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}, \text{ where } \lambda = 1 \text{ or } -1\right\}.$$

Therefore, half of elements in A_1 are in some coset of a nilpotent subgroup of G.

Case 2.(ii).(b).

$$A_1 \subset \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{x}} \\ 0 & & \end{array}\right)\left\{\begin{pmatrix} \lambda_1 & * & * \\ 0 & \lambda_2 & * \\ 0 & 0 & \lambda_3 \end{pmatrix}\right\}$$

Let

$$A_1' = \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{x}} \\ 0 & & \end{array}\right)^{-1} A_1,$$

and let

$$B' = \left\{\bar{g} \in SL_2(\mathbb{Z}) : \exists\, g \in A_1',\ \ g = \left(\begin{array}{c|c} \multirow{2}{*}{$\lambda\bar{g}$} & * \\ & 0 \\ \hline 0\ 0 & \lambda' \end{array}\right)\right\},$$

all upper triangular.

Repeating previous reasoning distinguishing Cases (i) and (ii), we have

$$A_1' \subset \left(\begin{array}{c|c} \multirow{2}{*}{x'} & 0 \\ & 0 \\ \hline 0\ 0 & 1 \end{array}\right)\left\{\begin{pmatrix} \lambda_4 & 0 & * \\ 0 & \lambda_5 & 0 \\ 0 & 0 & \lambda_6 \end{pmatrix}\right\}.$$

Let

$$A_1'' = \left(\begin{array}{c|c} x' & \begin{matrix} 0 \\ 0 \end{matrix} \\ \hline 0\;0 & 1 \end{array}\right)^{-1} A_1',$$

and let

$$B'' = \left\{ \bar{g} = \begin{pmatrix} \bar{g}_{11} & \bar{g}_{12} \\ 0 & \bar{g}_{22} \end{pmatrix} \in SL_2(\mathbb{Z}) : \; \exists\, g \in A_1'', \; g = \begin{pmatrix} \bar{g}_{11} & 0 & \bar{g}_{12} \\ 0 & \lambda & 0 \\ 0 & 0 & \bar{g}_{22} \end{pmatrix} \right\},$$

all upper triangular.

Repeating again, we obtain

$$B'' \subset \begin{pmatrix} x_{11}'' & x_{12}'' \\ 0 & x_{22}'' \end{pmatrix} \left\{ \begin{pmatrix} \bar{\lambda}_6 & \bar{0} \\ 0 & \lambda_7 \end{pmatrix} \right\}.$$

Hence

$$A_1'' \subset \begin{pmatrix} x_{11}'' & 0 & x_{12}'' \\ 0 & 1 & 0 \\ 0 & 0 & x_{22}'' \end{pmatrix} \left\{ \begin{pmatrix} \lambda_6 & 0 & * \\ 0 & \lambda_5 & 0 \\ 0 & 0 & \lambda_7 \end{pmatrix} \right\}.$$

Obviously this contradicts (2.2).

This concludes the proof that if $A \subset SL_3(\mathbb{Z})$ is a finite set and M a large constant, then either

$$|A^3| > M|A|$$

or

$$|A \cap S| > M^{-C}|A|$$

for some coset S of some nilpotent subgroup of $SL_3(\mathbb{Z})$.

From the discussion in the beginning of §1, we therefore obtain the following analogue of Theorem 2 for $SL_3(\mathbb{Z})$.

Theorem 3. *Let $p, q \in \mathbb{R}$ such that $1 < p < 2$ and*

$$\frac{2}{p} = 1 + \frac{1}{q}.$$

Then there is a constant $C = C_p > 0$ and $1 > \tau = \tau_p > 0$ such that if $f \in \ell^p\big(SL_3(\mathbb{Z})\big)$, then

$$\|f * f\|_q^{1/2} \leq C\|f\|_p^{1-\tau}(\|f\|_p')^{\tau}$$

defining

$$\|f\|'_p = \max_{x,G_1} \Big(\sum_{y\in G_1} |f(xy)|^p\Big)^{1/p}$$

and the max taken over all nilpotent subgroups G_1 of $SL_3(\mathbb{Z})$ and $x \in SL_3(\mathbb{Z})$.

§3. Further comments

1. Let $G = SL_2(\mathbb{Z})$ or $G = SL_3(\mathbb{Z})$ (we may also replace $\mathbb{Z}$ by the integers O_K in a finite extension K of $\mathbb{Q}$).

Let $\mu \in \ell^1_+(G), \|u\|_1 = 1$. Hence by Theorem 3 applied with $q = 2$, $p = \frac{4}{3}$,

$$\|\mu * \mu\|_2^{1/2} \leq C\|\mu\|_{4/3}^{1-\tau}(\|\mu\|'_{4/3})^\tau$$

and we estimate

$$\begin{aligned}\|\mu_{4/3}\| &\leq \|\mu\|_2^{1/2}\\ \|\mu\|'_{4/3} &\leq (\|\mu\|'_1)^{1/2}(\|\mu\|'_2)^{1/2}\\ &\leq (\|\mu\|'_1)^{1/2}\|\mu\|_2^{1/2}.\end{aligned}$$

Therefore

$$\|\mu * \mu\|_2 \leq C(\|\mu\|'_1)^\tau \|\mu\|_2. \tag{3.1}$$

Recall that

$$\|\mu\|'_1 = \max_{x,G_1} \Big[\sum_{y\in G_1} \mu(xy)\Big]$$

with $x \in G$ and G_1 a nilpotent subgroup of G. Taking μ symmetric $\big($i.e. $\mu(x) = \mu(x^{-1})\big)$, (3.1) is equivalent to

$$(\mu * \mu * \mu * \mu)(e) \leq C(\|\mu\|'_1)^{2\tau}\ (\mu * \mu)(e).$$

Decay estimates for iterated convolution of a given measure ν on G have been extensively studied in the literature, but to our knowledge, no prior results provide a nontrivial bound for a single convolution.

We recall some well known facts.

Let Γ be a symmetric finite generating set for a linear group G in characteristic zero.

Denote d_Γ the word metric with respect to Γ and by

$$B_\Gamma(n) = \{x \in G : d_\Gamma(x,e) \leq n\}$$

the corresponding balls. Then either $|B_\Gamma(n)|$ grows exponentially in n or G is virtually nilpotent. The first alternative occurs if G is not virtually solvable (hence by Tits' alternative [Ti] contains a free group on 2 generators) or if G is solvable but not virtually nilpotent. A uniform statement on the exponential growth for non virtually nilpotent G may be found in [EMO], where it is proven that

$$\inf_\Gamma \lim_{n\to\infty} |B_\Gamma(n)|^{1/n} > 1$$

where the infinum is taken over all finite generating sets Γ of G.

Let us next consider the corresponding random walk and denote

$$\nu = \nu_\Gamma = \frac{1}{|\Gamma|}\sum_{g\in\Gamma}\delta_g$$

the symmetric probability measure on G.

We are interested in the decay of $\nu^{(\ell)}(e)$ of the ℓ-fold convolution power of ν. There are three cases. If G is not virtually solvable, then there is exponential decay for $\ell \to \infty$

$$\nu^{(\ell)}(e) < e^{-c\ell}. \tag{3.2}$$

If G is solvable but not virtually nilpotent then

$$\nu^{(\ell)}(e) < e^{-c\ell^{1/3}} \tag{3.3}$$

(and this estimate is best possible, cf [Var]). If G is nilpotent, then there is power-like decay and more precisely for $\ell \to \infty$

$$\nu^{(\ell)}(e) = o(\ell^{-d/2}) \tag{3.4}$$

where $d = d(G) = \sum_{k\geq 1} k$ rank (G_k/G_{k+1}) and $G_{k+1} = [G_k, G]$ (see [CSV]).

Assume G not virtually solvable. Returning to (3.1), (3.3), we may easily estimate $\|\nu^{(\ell)}\|_1'$. Indeed, let H be a nilpotent subgroup and denote

$$\delta = \sum_{x\in H}\nu^{(\ell)}(x)$$

$$\nu_\ell = \frac{1}{\delta}\nu^{(\ell)}|_H.$$

From (3.2), (3.4) one gets

$$\begin{aligned} e^{-c\ell m} &\geq \nu^{(\ell m)}(e) \\ &\geq \delta^m \nu_\ell^{(m)}(e) \\ &> \frac{1}{C(\ell)} m^{-d/2} \delta^m. \end{aligned}$$

Hence letting $m \to \infty$, it follows

$$\begin{aligned} &\nu^{(\ell)}(H) = \delta \leq e^{-c\ell} \\ &\|\nu^{(\ell)}\|_1' \leq e^{-c\ell}. \end{aligned}$$

On the other hand, for solvable groups, the estimate on $\|\nu^{(\ell)}\|_1'$ may be much worse. Consider the quotient map $\pi : G \to G/[G,G]$ and let $\pi[\nu]$ be the image measure on the abelian group $G/[G,G]$.

Since $\pi[\nu]^{(\ell)}(e) > \ell^{-C}$ for $\ell \to \infty$, it follows that

$$\nu^{(\ell)}([G,G]) > \ell^{-C}$$

and $[G,G]$ may be nilpotent for G solvable.

2. Returning to the Remark after Theorem 2 concerning the free group F_2 on 2 generators, it may indeed be of interest to find a direct proof of the inequality

$$\|f * f\|_q^{1/2} \leq C\|f\|_p^{1-\tau}(\|f\|_p')^\tau \tag{3.5}$$

where $1 < p < q < \infty, \frac{2}{p} = 1 + \frac{1}{q}, f \in \ell^p(F_2)$ and

$$\|f\|_p' = \max_{x_1 y \in F_2} \Big(\sum_{n\in\mathbb{Z}} |f(xy^n)|^p\Big)^{1/p}.$$

Notice that obvious necessary conditions for (3.5) to hold is that

$$\tau \leq \min\Big(p-1, 1-\frac{p}{2}\Big).$$

References

[BG1]. Bourgain,A.Gamburd, *Uniform expansion bounds for Caley graphs of $SL^2(p)$*, Annals Math (to appear).

[BG2]. ——, *On the spectral gap for finitely generated subgroups of $SU(2)$*, Inventiones (to appear).

[B]. E. Breuillard, *On Uniform exponential growth for solvable groups*, (preprint).

[BT]. E.Breuillard,T.Gelander, *Cheeger constant and algebraic entropy of linear groups*, IMRN, 2005, n56, 3511-3523.

[CSV]. T. Coulhon, L. Saloff-Coste,, N. Varopoulos, *Analysis and geometry on groups*, Cambridge Tracts in Math 1000, Cambridge UP, 1992.

[C]. M.-C. Chang, *Product theorems in SL_2 and SL_3*, J. Math. Jussieu (to appear).

[EMO]. A. Eskin, S. Mozes, H. Oh, *On Uniform exponential growth for linear groups*, Invent. 160, (2005), 1-30.

[ESS]. J.-H. Evertse, H. Schlickewei, W. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math 155, (2002), 807-836.

[H]. H. Helfgott, *Growth and generation in $SL_2(\mathbb{Z}/\mathbb{Z}_p)$*, Annals (to appear).

[K]. K H.Kesten, *Symmetric random walks on groups*, TAMS 92 (1959), 336-354.

[R]. A.Razborov, *A product theorem in Free groups*, preprint.

[T]. T. Tao, *Product set estimates in non-commutative groups*, math. CO/0601431.

[TV]. T. Tao, V. Vu, *Additive Combinatorics*, Cambridge University Press (2006).

[Ti]. J. Tits, *Free subgroups in linear groups*, J. Algebra 20, (1972), 250-270.

Mathematics Department, University of California, Riverside CA 92521

E-mail address: mcc@math.ucr.edu