Can. J. Math. Vol. **44** (5), 1992 pp. 897–910

A LOWER ESTIMATE FOR CENTRAL PROBABILITIES ON POLYCYCLIC GROUPS

G. ALEXOPOULOS

ABSTRACT. We give a lower estimate for the central value $\mu^{*n}(e)$ of the nth convolution power $\mu * \cdots * \mu$ of a symmetric probability measure μ on a polycyclic group G of exponential growth whose support is finite and generates G. We also give a similar large time diagonal estimate for the fundamendal solution of the equation $(\partial/\partial t + L)u = 0$, where L is a left invariant sub-Laplacian on a unimodular amenable Lie group G of exponential growth.

0. **Introduction.**

0.1 *The discrete case.* Let G be a discrete finitely generated group, e its identity element and μ a probability measure on G.

We assume that μ is symmetric *i.e.* that $\mu(g) = \mu(g^{-1}), g \in G$ and that its support $\operatorname{supp}\mu = \{g \in G : \mu(g) \neq 0\}$ generates G.

We denote by μ^n the nth convolution power $\mu * \cdots * \mu$ of μ ($\mu * \nu(g) = \sum_{h\in G} \mu(h)\nu(h^{-1}g)$, $g \in G$).

We fix a set of generators $\{x_1, \ldots, x_p\}$ of G and we denote by $\gamma(n)$ the volume growth function of G defined by

$$\gamma(n) = \{g \in G : g = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}, \varepsilon = \pm 1, 1 \leq i_j \leq p, 1 \leq j \leq n\}, \quad n \in \mathbb{N}.$$

We say that G has *polynomial volume growth,* if there are constants $c, d > 0$ such that $\gamma(n) \leq cn^d$, $n \in \mathbb{N}$ and exponential volume growth if $\gamma(n) \geq ce^{dn}$, $n \in \mathbb{N}$.

We say that G is *polycyclic* (*cf.* [13]) if it admits a finite sequence of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_k = \{e\}$$

such that G_i is normal in G_{i-1} and G_{i-1}/G_i is cyclic.

The polycyclic groups are "essentially" those discrete groups that can be realised as lattices of connected solvable Lie groups (*cf.* [13]). They have either polynomial or exponential volume growth (*cf.* [11]), a result that it is not true for general finitely generated discrete groups (*cf.* [7]).

We say that G is *virtually polycyclic* (or *polycyclic by finite*) if it admits a normal polycyclic subgroup Γ such that G/Γ is finite.

In this article we shall prove the following:

Received by the editors August 14, 1989; revised March 7, 1991.
AMS subject classification: 31C05, 43A05, 60B15.
Key words and phrases: Polycyclic groups, volume growth, convolution power, heat kernel.

https://doi.org/10.4153/CJM-1992-055-8 Published online by Cambridge University Press

THEOREM 1. *Let G be a virtually polycyclic group of exponential volume growth and μ a symmetric probability measure on G whose support is finite and generates G. Then there are constants $A, a > 0$ such that*

$$\mu^n(e) \geq Ae^{-an^{\frac{1}{3}}}, \quad n \in 2\mathbb{N}.$$

The same ideas also give the following result, which has also been proved by V. A. Kaimanovich [10] (*cf.* also A. Raugi [12])

COROLLARY 2. *Let G and μ be as in Theorem 1. Then every bounded harmonic function u (i.e. such that $u(g) = \sum_{x \in G} u(gx)\mu(x)$, $g \in G$), is constant.*

Theorem 1 should be compared with the following:

THEOREM 3 (*cf.* N. TH. VAROPOULOS [21]). *Let G be a discrete group of exponential volume growth and μ a symmetric probability measure on G, whose support is finite and generates G. Then there are constants $B, b > 0$ such that*

$$\mu^n(e) \leq Be^{-bn^{\frac{1}{3}}}, \quad n \in \mathbb{N}$$

So Theorem 1 shows that the exponent $\frac{1}{3}$ is indeed optimal.

0.2 *The continuous case.* The above results have continuous analogues. More precisely, let G be a connected Lie group and dg a left invariant Haar measure on G. Let $\mathfrak{g}$ be the Lie algebra of G which we identify with the left invariant vector fields on G.

Having fixed a compact neighborhood V of the identity element e of G, we define the volume growth function $\gamma(n)$, $n \in \mathbb{N}$ and the distance function $\rho(x, y)$, $x, y \in G$ as follows

$$\gamma(n) = dg\text{-measure } (V^n), \quad n \in \mathbb{N}$$
$$\rho(x, y) = \rho(x^{-1}y), \ \rho(x) = \inf\{n \in \mathbb{N} : x \in V^n\}, \quad x, y \in G.$$

We say that G has polynomial volume growth if there are constants $c, d > 0$ such that

$$\gamma(n) \leq cn^d, \quad n \in \mathbb{N}$$

and exponential volume growth if

$$\gamma(n) \geq ce^{dn}, \quad n \in \mathbb{N}.$$

Connected Lie groups have either polynomial or exponential volume growth (*cf.* [8]), a property not shared by the discrete finitely generated groups (*cf.* [7]).

In this article we shall assume that G is unimodular, amenable and has exponential volume growth. In our context, amenability means that if Q is the radical of G (*i.e.* the maximal solvable subgroup of G), then G/Q is a compact semisimple Lie group (*cf.* [15]).

Let $X_1, \ldots, X_n$ be left invariant vector fields on G that satisfy Hörmander's condition, *i.e.* together with their successive Lie brackets $\left[X_{i_1}, \left[X_{i_2}, [\cdots [X_{i_{s-1}}, X_{i_s}] \cdots\right]\right]$, they generate $\mathfrak{q}$. Then according to a classical theorem of L.Hörmander [9] the operators $L = -(X_1^2 + \cdots + X_k^2)$ and $\partial/\partial t + L$ are hypoelliptic.

We denote by $p_t(x,y)$, $x, y \in G, t > 0$ the fundamental solution of the equation $(\partial/\partial t + L)u = 0$. Observe that the fact that L is a left invariant and symmetric operator implies that $p_t(x,y) = p_t(x^{-1}y)$ and $p_t(x,y) = p_t(y,x)$, $x, y \in G$, $y > 0$.

THEOREM 4. *Let G be a connected, unimodular, amenable Lie group of exponential volume growth and L, $p_t(x,y)$ as above. Then there are constants $a, A > 0$ such that*

$$p_t(x,x) \geq Ae^{-at^{\frac{1}{3}}}, \quad x \in G,\ t \geq 1. \tag{0.1}$$

A consequence of the proof of the above theorem is the following:

COROLLARY 5. *Let G and L be as in Theorem 4. Then every bounded harmonic function (i.e. every $u \in C^\infty(G)$ satisfying $\|u\|_\infty < +\infty$ and $Lu = 0$ in G) is constant.*

As in the discrete case, we also have the following:

THEOREM 6 (*cf.* N. TH. VAROPOULOS [20]). *Let G, L and $p_t(x,y)$ be as in Theorem 4. Then for all $\varepsilon > 0$ there are constants $B, b > 0$ such that*

$$p_t(x,y) \leq Be^{-bt^{\frac{1}{3}}} e^{-\frac{\rho^2(x,y)}{(4+\varepsilon)t}}, \quad x, y \in G,\ t \geq 1. \tag{0.2}$$

So, putting together (0.1) and (0.2) we have a description of the asymptotic behavior of the central value $p_t(x,x)$, $x \in G$ of the kernel $p_t(x,y)$, $x, y \in G$, as $t \longrightarrow \infty$.

Of course, one could ask the question, if a similar lower Gaussian estimate for $p_t(x,y)$, *i.e.* an estimate of the type

$$Ae^{-Bt^\alpha} e^{-\frac{\rho^2(x,y)}{Ct}} \leq p_t(x,y), \quad x, y \in G,\ t \geq 1. \tag{0.3}$$

for some $\alpha \in (0,1)$, could be true.

It is easy to see that (0.3) is not true. Indeed, if we fix a $\beta \in (\frac{\alpha+1}{2}, 1)$, then (0.3) would imply that there are constants $A', B' > 0$ such that

$$A'e^{-B't^{2\beta-1}} \leq p_t(x,y),\ x, y \in G, \quad \rho(x,y) \leq t^\beta,\ t \geq 1.$$

This estimate, together with the assumption that G has exponential volume growth, would imply that there is a constant $C' > 0$ such that

$$1 > \int_{\{y \in G: \rho(x,y) \leq t^\beta\}} p_t(x,y)\, dy \geq A'e^{-B't^{2\beta-1}} e^{C't^\beta}, \quad t \geq 1$$

which is absurd.

Finally, we point out that results similar to Theorem 1 and Corollary 2 can be stated for the heat kernel and the bounded harmonic functions on the covering $\widetilde{M}$ of a compact Riemannian manifold M when the group of the covering is polycyclic. They can be proved in a similar way.

1. **Some technical lemmas for random walks in $\mathbb{R}^p$.** This section is directly inspired from [18].

Let X_k, $k \in \mathbb{N}$ be independent, identically distributed random variables, with values in $\mathbb{R}^p$ such that

$$E[X_k] = 0, \ E[X_k^2] < +\infty, \quad k \in \mathbb{N}.$$

Also let

$$Z_k = X_1 + \cdots + X_k, \quad k \in \mathbb{N}, \ Z_0 = 0 \text{ a.s.}$$

and

$$M_n = \sup_{1 \le i \le k} |Z_i|, \quad k \in \mathbb{N}.$$

LEMMA 1.1. *There are constants $\varepsilon > 0$, $a_0 > 0$ and $k_0 \in \mathbb{N}$ such that for all $k \ge k_0$, $m \ge 1$ and $\lambda_1, \lambda_2 \in \mathbb{R}^p$ satisfying $|\lambda_1| \le \frac{\sqrt{k}}{10}$, $|\lambda_2| \le \frac{\sqrt{k}}{10}$, $a\sqrt{k} \le m$ and $a \ge a_0$ we have*

$$P\Big[\sup_{1 \le i \le k} |\lambda_1 + Z_i| \le 2m, \ |\lambda_2 + Z_k| \le \frac{\sqrt{k}}{100}\Big] > \varepsilon. \tag{1.1}$$

PROOF. It follows from Kolmogorov's inequality that there is a constant $b > 0$ such that

$$P[M_k \le m] \ge 1 - b\frac{k}{m^2}$$

and from this that

$$P\Big[\frac{M_k}{\sqrt{k}} \le a\Big] \ge 1 - \frac{bk}{a^2 k} = 1 - \frac{b}{a^2}.$$

Hence

$$P\Big[\frac{M_k}{\sqrt{k}} \le a\Big] \longrightarrow 1 \quad (a \longrightarrow +\infty). \tag{1.2}$$

On the other hand it follows from the central limit theorem that there is $\varepsilon_1 > 0$ and $k_0 \in \mathbb{N}$ such that for all $k \in \mathbb{N}$ and $\lambda \in \mathbb{R}^p$ satisfying $k \ge k_0$ and $|\lambda| \le \frac{\sqrt{k}}{2}$ we have

$$P\Big[\Big|\frac{Z_k}{\sqrt{k}} + \frac{\lambda}{\sqrt{k}}\Big| < \frac{1}{1000}\Big] > \varepsilon_1. \tag{1.3}$$

Putting (1.2) and (1.3) together we have (1.1).

LEMMA 1.2. *There are constants $c_1, c_2 > 0$, $m_0 \ge 1$ and $k_0 \in \mathbb{N}$ such that for all $k \ge n_0$, $k \in \mathbb{N}$ and $m \ge m_0$ we have*

$$P[M_k \le m] \ge c_1 e^{-c_2 \frac{k}{m^2}}. \tag{1.4}$$

PROOF. Let a_0, ε and k_0 be as in Lemma 1.1 and put $m_0 = 2[a_0\sqrt{k_0}] + 1$.
We shall consider two cases:

https://doi.org/10.4153/CJM-1992-055-8 Published online by Cambridge University Press

CASE 1. $a_0\sqrt{k} \leq m$, $k \geq k_0$, $m \geq m_0$, $k, m \in \mathbb{N}$.
In this case, it follows from (1.1) that

$$P[M_k \leq m] \geq \varepsilon \geq \varepsilon e^{-c\frac{k}{m^2}}, \quad \forall c > 0.$$

CASE 2. $a_0\sqrt{k} \geq m$, $k \geq k_0$, $m \geq m_0$, $k, m \in \mathbb{N}$.
Let $k_1 = [\frac{m^2}{2a_0^2}] - 1$. Then we have

$$k = \left[\frac{k}{k_1}\right]k_1 + k_2,\ k_2 \leq k_1,\ k_1 \geq k_0,\ \sqrt{2}a_0\sqrt{k_1} \leq m,\ a_0\sqrt{k_2 + k_1} \leq m$$

and applying (1.1) we find that

$$P[M_k \leq m] \geq \varepsilon\varepsilon^{[\frac{k}{k_1}]-1}$$

and the lemma follows.

2. **The entropy of random walks.** In this section we shall recall the definition and some properties of the entropy of random walks on groups (*cf.* [2], [4], [17], [22]), which we shall need to prove the Corollaries 2 and 5.

More precisely, let G be a locally compact, compactly generated group and dg a left invariant Haar measure on G.

Let f be a density on G, *i.e.* such that $f(g) \geq 0$, $g \in G$ and $\int f(g)\,dg = 1$, whose support $\operatorname{supp} f = \overline{\{g \in G : f(g) > 0\}}$ generates G.

Let Z_k, $k = 0, 1, 2, \ldots$ be the random walk on G defined by

$$Z_0 = 0, \text{ a.s. and } P[Z_{k+1} \in A \mid Z_k = g] = \int_A f(g^{-1}x)\,dx, \quad k = 0, 1, 2, \ldots$$

(A is a Borel subset of G).

We say that a function u is *f-harmonic* if and only if

$$u(g) = \int u(gx)f(x)\,dx, \quad g \in G.$$

We denote by f^k the kth convolution power $f * f * \cdots * f$ of f ($f * h(g) = \int f(x)h(x^{-1}g)\,dx$, $g \in G$) and we make the additional assumption that

$$\int |f^k(g)\log f^k(g)|dg < +\infty, \quad n = 1, 2, \ldots$$

(we put $t\log t = 0$ for $t = 0$).

We call the *entropy* of the random walk Z_k or of the pair $H(G,f)$ the limit

$$H(G,f) = \lim_{k \to +\infty} -\frac{1}{k}\int f^k(g)\log f^k(g)dg.$$

It can be proved that the limit exists and is finite.

THEOREM 2.1 (*cf.* [2], [4]). *Let G and f be as above. Then $H(G,f) = 0$ if and only if every bounded f-harmonic function u (i.e. such that $u(g) = \int u(gx)f(x)\,dx$, $g \in G$) is constant.*

THEOREM 2.2 (*cf.* [2], [4]). *Let G and f be as above. Then*

$$-\frac{1}{k}\log f^k(Y_k) \longrightarrow H(G,f),\ (k \longrightarrow +\infty),\ \text{in } L^1(G).$$

Furthermore, when G is discrete or f is continuous with compact support we also have convergence a.s.

3. **The proof of Theorem 1 and Corollary 2.** Since G is polycyclic by finite it has a normal subgroup $\Gamma \lhd G$, such that G/Γ is finite. Now, according to the structure theory of the polycyclic groups (*cf.* [13]), Γ admits finitely generated subgroups Γ^* and N such that

1) N is nilpotent, $N \lhd \Gamma^*$, $N \lhd G$ and Γ^*/N is abelian
2) $\Gamma^* \lhd \Gamma$, $\Gamma^* \lhd G$ and Γ/Γ^* is finite.

Let π' be the natural map $\pi': G \longrightarrow G/B$.

The group Γ^*/N being a finitely generated abelian group can be written as $\Gamma^*/N = DC$, where D is a subgroup of Γ^*/N isomorphic with $\mathbb{Z}^p$ for some $p \in \mathbb{N}$ and C a finite subgroup of Γ^*/N. So, if $B = (\pi')^{-1}(C)$, then Γ^*/B is isomorphic with $\mathbb{Z}^p$. Using this isomorphism we shall identify Γ^*/B with $\mathbb{Z}^p$. B, being a finite extension of a nilpotent group, has polynomial volume growth.

We shall first prove Theorem 1 and Corollary 2 in the case $G = \Gamma^*$, since the proof in that case is simpler and the ideas are better illustrated. The extension G/Γ^*, being finite, presents only an additional technical difficulty. In Section 3.2, we shall explain how we can deal with it.

3.1 *Case 1: $G = \Gamma^*$.* Let $\{e_1, \dots, e_p\}$ be the standard basis of $\mathbb{Z}^p$ and $x_1, \dots, x_p \in G$ such that $\pi(x_i) = e_i$, $1 \le i \le p$ where π denotes the natural map $\pi: G \longrightarrow G/B$. Then every $g \in G$ can be written in the form

$$g = y x_p^{n_p} \cdots x_1^{n_1}, \text{ with } y \in B \text{ and } n = (n_p, \dots, n_1) \in \mathbb{Z}^p.$$

Fixing $\{g_1, \dots, g_s\}$ and $\{h_1, \dots, h_r\}$ sets of generators of G and B respectively we put

$$|x|_G = \inf\{n : x = g_{i_1}^{\epsilon_1} \cdots g_{i_n}^{\epsilon_n}, 1 \le i_j \le s, \epsilon_j = \pm 1, 1 \le j \le n\}$$
$$|y|_B = \inf\{n : y = h_{i_1}^{\epsilon_1} \cdots h_{i_n}^{\epsilon_n}, 1 \le i_j \le r, \epsilon_j = \pm 1, 1 \le j \le n\}$$
$$\theta = \sup\{|x_i^{\epsilon_1} h_j^{\epsilon_2} x_i^{-\epsilon_1}|_B, \epsilon_1 = \pm 1, \epsilon_2 = \pm 1, 1 \le i \le p, 1 \le j \le r\}$$
$$\delta = \sup\{|x_i^{\epsilon_1} x_j^{\epsilon_2} x_i^{-\epsilon_1} x_j^{-\epsilon_2}|_B, \epsilon_1 = \pm 1, \epsilon_2 = \pm 1, 1 \le i, j \le p\}.$$

We also put

$$|n| = |n_p| + \cdots + |n_1| \text{ for } n = (n_p, \dots, n_1) \in \mathbb{Z}^p.$$

Observe that if $x = x_p^{n_p} \cdots x_1^{n_1}$ and $y \in B$ then

$$|xyx^{-1}|_B \le |y|_B \theta^{|n|}. \tag{3.1}$$

LEMMA 3.1. *Let $x = x_p^{n_p} \cdots x_1^{n_1}$, $n = (n_p, \dots, n_1)$, $\epsilon \in \{-1, 1\}$ and $i \in \{1, \dots, p\}$. Then there is $c > 0$ such that*

$$x x_i^{\epsilon} x^{-1} = y x_i^{\epsilon}, \text{ with } y \in B, \ |y|_B \le c e^{c|n|}. \tag{3.2}$$

PROOF. The lemma will be proved by induction on $|n|$. It is trivially true when $|n| = 0$. So, assume that it is true for $|n| \le \ell$. We shall prove that it also true for $|n| = \ell + 1$.

Let $j = \min\{i : n_i \neq 0\}$ and put $n'_j = \frac{n_j}{|n_j|}(|n_j| - 1)$, $\epsilon' = n_j - n'_j$, $x' = x_p^{n_p} \cdots x_j^{n'_j}$, $n' = (n_p, \ldots, n'_j, 0, \ldots, 0)$ and $z = x_j^{\epsilon'} x_i^{\epsilon} x_j^{-\epsilon'} x_i^{-\epsilon}$. Then

$$xx_i^{\epsilon}x^{-1} = x'x_j^{\epsilon'}x_i^{\epsilon}x_j^{-\epsilon'}(x')^{-1} = x'zx_i^{\epsilon}(x')^{-1} = x'z(x')^{-1}x'x_i^{\epsilon}(x')^{-1}.$$

Now, it follows from (3.1) that

$$|x'z(x')^{-1}|_B \leq \delta\theta^{|n'|}$$

and by the inductive hypothesis that there is $w \in B$ such that

$$x'x_i^{\epsilon}(x')^{-1} = wx_i^{\epsilon}, \quad |w|_B \leq ce^{c|n'|}.$$

So, if the constant c, chosen in the begining, is such that $c > \max(\delta, \log\theta)$, we have

$$xx_i^{\epsilon}x^{-1} = yx_i^{\epsilon},\ y = x'z(x')^{-1}w,\ |y|_B \leq \delta\theta^{|n'|} + ce^{c|n'|} \leq ce^{c(|n'|+1)} = ce^{c|n|}$$

which proves the inductive step and the lemma follows.

LEMMA 3.2. *Let $n = (n_p, \ldots, n_1)$, $\epsilon \in \{-1, 1\}$ and $i \in \{1, \ldots, p\}$. Then there is $c > 0$ such that*

$$x_p^{n_p} \cdots x_1^{n_1} x_i^{\epsilon} = yx_p^{n_p} \cdots x_i^{n_i+\epsilon} \cdots x_1^{n_1} \text{ with } y \in B,\ |y|_B \leq ce^{c|n|}. \tag{3.3}$$

PROOF. The lemma follows from (3.1), (3.2) and the observation that, if

$$z = x_i^{n_i} \cdots x_1^{n_1} x_i^{\epsilon}(x_i^{n_i} \cdots x_1^{n_1})^{-1} x_i^{-\epsilon}, \text{ and } y = x_p^{n_p} \cdots x_{i+1}^{n_{i+1}} z (x_p^{n_p} \cdots x_{i+1}^{n_{i+1}})^{-1}$$

then

$$x_p^{n_p} \cdots x_1^{n_1} x_i^{\epsilon} = x_p^{n_p} \cdots x_{i+1}^{n_{i+1}} z x_i^{n_i+\epsilon} \cdots x_1^{n_1} = yx_p^{n_p} \cdots x_i^{n_i+\epsilon} \cdots x_1^{n_1}.$$

COROLLARY 3.3. *Let $x = x_p^{n_p} \cdots x_1^{n_1}$, $w = x_p^{m_p} \cdots x_1^{m_1}$, $n = (n_p, \ldots, n_1), m = (m_p, \ldots, m_1)$ and $y, z \in B$. Then there is $c > 0$ such that*

$$yxzw = vx_p^{n_p+m_p} \cdots x_1^{n_1+m_1}, \text{ with } v \in B,\ |v|_B \leq c\big[|y|_B + |z|_B e^{c|n|} + e^{c(|m|+|n|)}\big]. \tag{3.4}$$

PROOF. The corollary follows from (3.1) and (3.3) and the observation that $yxzw = y(xzx^{-1})xw$.

COROLLARY 3.4. *There is a constant $c > 0$ such that every $g \in G$ can be written in the form*

$$g = yx_p^{n_p} \cdots x_1^{n_1}, \text{ with } y \in B,\ |y|_B \leq ce^{c|g|_G},\ |n| \leq |g|_G,\ n = (n_p, \ldots, n_1)$$

PROOF. Since all the generators g_i can be written in the form $g_i = zw$, with $z \in B$ and $w = x_p^{m_p} \cdots x_1^{m_1}$ and $g = g_{i_1} \cdots g_{i_q}$ with $q = |g|_G$, the corollary follows after applying (3.4) $|g|_G$ times.

Let X_k, $k = 1, 2, \ldots$ be independent identically distributed random variables with values in G and $P[X_k = g] = \mu(g)$, $g \in G$ and denote by Z_k, $k = 0, 1, 2, \ldots$ the right random walk in G defined by

$$Z_0 = e \text{ a.s. and } Z_k = X_1 X_2 \cdots X_k, \quad k = 1, 2, \ldots .$$

Also let $S_k = (S_{k,p}, \ldots, S_{k,1}), k = 0, 1, 2, \ldots$ be the random walk in $\mathbb{Z}^p$ defined by

$$S_0 = 0 \text{ a.s. and } S_k = \pi(X_1) + \pi(X_2) + \cdots + \pi(X_k), \quad k = 1, 2, \ldots .$$

Observe that $S_k = \pi(Z_k)$.

We put

$$X^{S_k} = x_p^{S_{k,p}} \cdots x_1^{S_{k,1}}.$$

Then it follows from (3.4) that there is $c > 0$ such that

(3.5) $$Z_k = Y_k X^{S_k}, \text{ with } Y_k \in B,\ |Y_k|_B \leq c\Big[e^{c|S_1|} + \cdots + e^{c|S_{k-1}|}\Big].$$

Let us also recall that it follows from Kolmogorov's inequality that there is $b > 0$ such that

(3.6) $$P\Big[\max_{1 \leq i \leq k} |S_i| \leq m\Big] \geq 1 - b\frac{k}{m^2}, \quad k \in \mathbb{N},\ m > 0.$$

Also let c be as in (3.5) and put

$$D_k^m = \{g \in G : g = y x_p^{n_p} \cdots x_1^{n_1},$$
$$|n_p| + \cdots + |n_1| \leq m, y \in B, |y|_B \leq cke^{cm}\}, \quad k \in \mathbb{N},\ m > 0.$$

Then, it follows from (3.5) and (3.6) that

(3.7) $$P[Y_k \in D_k^m] \geq P\Big[\sup_{1 \leq i \leq k} |S_i| \leq m\Big].$$

We have the following estimate of the number of elements $|D_k^m|$ of the set D_k^m, which follows from the fact that B has polynomial volume growth

(3.8) $$|D_n^m| \leq a_1 e^{a_2(m + \log k)}$$

(a_1, a_2 are constants, $a_1, a_2 > 0$)

PROOF OF THEOREM 1. The first thing to observe is that

(3.9) $$\mu^{2k}(e) = \sup_{g \in G} \mu^{2k}(g), \quad k \in \mathbb{N}.$$

This follows from the hypothesis that μ is symmetric using the Hölder inequality:

$$\mu^{2k}(g) = \sum_{x\in G} \mu^k(x)\mu^k(x^{-1}g) \leq \Big[\sum_{x\in G}\big(\mu^k(x)\big)^2\Big]^{\frac{1}{2}}\Big[\sum_{x\in G}\big(\mu^k(x^{-1}g)\big)^2\Big]^{\frac{1}{2}}$$
$$= \Big[\sum_{x\in G}\big(\mu^k(x)\big)^2\Big] = \mu^{2k}(e).$$

Now it follows from Lemma 1.2 that there are constants $c_1, c_2 > 0, m_0 \geq 1$ and $k_0 \in \mathbb{N}$ such that

$$P\Big[\sup_{1\leq i\leq k} |S_i| \leq m\Big] \geq c_1 e^{-c_2\frac{k}{m^2}}, \quad m \geq m_0,\ k \geq k_0,\ k \in \mathbb{N}. \tag{3.10}$$

Putting (3.6), (3.7), (3.8), (3.9) and (3.10) together we have that for all $m \geq m_0, k \geq k_0$ and $k \in 2\mathbb{N}$

$$\mu^k(e) \geq P[Y_k \in D_k^m]|D_k^m|^{-1} \geq c_1 a_1^{-1} e^{-c_2\frac{k}{m^2}-a_2 m - a_2\log k}.$$

Theorem 1 follows by optimising with respect to m.

PROOF OF COROLLARY 2. We shall prove that the entropy $H(G,\mu) = 0$. Then Corollary 2 will be a consequence of Theorem 2.1.

Let $D_k = D_k^{k^{3/4}}$. Then it follows from (3.6) and (3.7) that

$$P[Z_k \in D_k] \geq 1 - b\frac{1}{\sqrt{k}}, \quad k \in \mathbb{K}. \tag{3.11}$$

Hence

$$P[Z_k \notin D_k] \longrightarrow 0, \quad (k \longrightarrow +\infty)$$

which, in view of Theorem 2.2, implies that

$$\frac{1}{k}\sum_{g\notin D_k} \mu^k(g)\log\mu^k(g) \longrightarrow 0, \quad (k \longrightarrow +\infty). \tag{3.12}$$

On the other hand it follows from Jensen's inequality that

$$-\frac{1}{k}\sum_{g\in D_k}\mu^k(g)\log\mu^k(g) = -\frac{1}{k}|D_k|\sum_{g\in D_k}\frac{1}{|D_k|}\mu^k(g)\log\mu^k(g)$$
$$\leq -\frac{1}{k}|D_k|\Big[\sum_{g\in D_k}\frac{1}{|D_k|}\mu^k(g)\Big]\log\Big[\sum_{g\in D_k}\frac{1}{|D_k|}\mu^k(g)\Big]$$
$$= -\frac{1}{k}\mu^k(D_k)\log\frac{\mu^k(D_k)}{|D_k|}$$
$$= -\frac{1}{k}\mu^k(D_k)\log\mu^k(D_k) + \frac{1}{k}\mu^k(D_k)\log|D_k|$$

which, combined with the fact that

$$|D_K| \leq e^{k^{3/4}}, \quad k \in \mathbb{N}$$

implies that

$$\frac{1}{k}\sum_{g\in D_k}\mu^k(g)\log\mu^k(g)\longrightarrow 0,\quad (k\longrightarrow+\infty). \tag{3.13}$$

Putting (3.12) and (3.13) together we have that $H(G,\mu)=0$ and Corollary 2 follows.

3.2 *The general case.* Let π and π' be the natural maps

$$\pi\colon G\longrightarrow G/B, \text{ and } \pi'\colon G\longrightarrow G/\Gamma^*.$$

Let $X_k,\ k=0,1,2,\ldots$ and $Z_k,\ k=0,1,2,\ldots$ be as in Section 3.1 and put

$$S_k=\pi(Z_k),\qquad \xi_k=\pi'(Z_k).$$

Let us also view ξ_k as a Markov chain with state space G/Γ^* and denote by $\nu(k)$ the number of passages of ξ_k from the state $e\Gamma^*\in G/\Gamma^*$ during the first k units of time. Then it follows from the theory of Markov chains with a finite number of states (*cf.* [14]) that there is $\alpha\in(0,1)$ such that $\forall\epsilon>0$

$$P\Big[\Big|\frac{1}{k}\nu(k)-\alpha\Big|>\epsilon\Big]\longrightarrow 0,\quad (k\longrightarrow+\infty). \tag{3.14}$$

Let τ_k be the time of the kth passage of ξ_k from the state $e\Gamma^*$. Then it follows from (3.14) that $\forall\beta$ such that $0<\beta<\alpha$

$$P\big[\tau_{(\alpha-\beta)k}<k,\tau_{(\alpha+\beta)k}>k\big]\longrightarrow 1,\quad (k\longrightarrow+\infty). \tag{3.15}$$

Furthermore identifying Γ^*/B with $\mathbb{Z}^p$, we have that the random variables

$$S_{\tau_{k-1}}^{-1}S_{\tau_k},\quad k=1,2,\ldots$$

are independent identically distributed and take values in $\Gamma^*/B=\mathbb{Z}^p$.

Hence it follows from Kolmogorov's inequality that there is a constant $b>0$ such that

$$P\Big[\big|S_{\tau_{(\alpha-\beta)k}}^{-1}S_{\tau_i}\big|\le m,(\alpha-\beta)k<i<(\alpha+\beta)k\Big]\ge 1-2b\beta\frac{k}{m^2}. \tag{3.16}$$

Let $\{v_1,\ldots,v_q\}$ be a set of generators of G/B and put for $w\in G/B$

$$|v|=\inf\{n\in\mathbb{N}: v=v_{i_1}^{\epsilon_1}\cdots v_{i_n}^{\epsilon_n}, 1\le i_j\le q, \epsilon_j=\pm1, 1\le j\le n\}.$$

Choosing β very small in (3.15) and then applying (1.1) together with (3.16) we have that there are constants $c>0$, $\varepsilon>0$, $a_o>0$, $k_0\in\mathbb{N}$ such that for all $k\ge k_0$, $m\ge 1$ and $w_1,w_2\in G/B$ satisfying $|w_1|\le\frac{\sqrt{k}}{10}$, $|w_2|\le\frac{\sqrt{k}}{10}$, $a\sqrt{k}\le m$ and $a\ge a_0$ we have

$$P\Big[\sup_{1\le i\le k}|w_1S_i|\le 2m, |w_2S_k|\le\frac{\sqrt{k}}{100}\Big]>c \tag{3.17}$$

$$P\Big[\sup_{1\le i\le(\alpha-\beta)k}|w_1S_{\tau_i}|\le 2m,\ |w_2S_{\tau_{(\alpha-\beta)k}}|\le\frac{\sqrt{k}}{200},$$

$$\sup_{(\alpha-\beta)k<i<(\alpha+\beta)k}|S_{\tau_{(\alpha-\beta)k}}^{-1}S_{\tau_i}]\le\frac{\sqrt{k}}{200}\Big]>\varepsilon$$

which is an analogue of (1.1) for the random walk S_k, $k = 0, 1, 2, \ldots$. Once we have (3.17) we can prove in exactly the same way an analogue of the inequality (1.4), *i.e.* that there are constants $c_1, c_2 > 0, m_0 \geq 1$ and $k_0 \in \mathbb{N}$ such that for all $k \geq k_0, k \in \mathbb{N}$ and $m \geq m_0$ we have

$$(3.18) \qquad P\Big[\sup_{1\leq i\leq k} |S_i| \leq m\Big] \geq c_1 e^{-c_2 \frac{k}{m^2}}.$$

From now on the proof of Theorem 1 and Corollary 2 is exactly the same with their proof in the case when G/Γ^* is trivial. The only modification, of course, is that now we shall have to fix elements $z_1, \ldots, z_\ell \in G$ such that $G/\Gamma^* = \{z_1\Gamma^*, \ldots, z_\ell\Gamma^*\}$ and $x_1, \ldots, x_p \in \Gamma^*$ as in Section 3.1 and we write every $g \in G$ in the form

$$g = yxz_i, \text{ with } y \in B,\ x = x_1^{n_1} \cdots x_1^{n_1}, \quad 1 \leq i \leq \ell.$$

4. **The proof of Theorem 4 and Corollary 5.** The proof of Theorem 4 and Corollary 5 is similar to the proof of Theorem 1 and Corollary 2. So we shall try to use similar notations.

Let Q, N and M be the radical the nil-radical and a Levi subgroup of G, respectively (*cf.* [15]). Q and N are, respectively, closed solvable and nilpotent subgroups of G. M is a semisimple subgroup of G. The assumption that G is amenable implies that M is compact. Furthermore

$$(4.1) \qquad G = QM \text{ and } [G, G] \subseteq NM$$

($[G, G]$ is the closed analytic subgroup of G generated by the elements $[g, h] = ghg^{-1}h^{-1}, g, h \in G$ of G).

It follows from (4.1) that G/NM is a connected abelian Lie group. Hence it can be written as

$$G/NM = DC$$

where D and C are closed subgroups of G/NM, C is compact and D is isomorphic with $\mathbb{R}^p$ for some $p \in \mathbb{N}$. Let π' be the natural map $\pi' \colon G \longrightarrow G/NM$ and put

$$B = \pi'^{-1}(C).$$

Then B, being a compact extension of a nilpotent group, has polynomial volume growth.

Let π denote the natural map $\pi \colon G \longrightarrow G/B$. Since G/B is isomorphic with $\mathbb{R}^p$ there are left invariant vector fields $X_1, \ldots, X_p$ on G such that the map

$$\phi \colon \mathbb{R}^p \longrightarrow G/B,\ \phi \colon t = (t_p, \ldots, t_1) \longrightarrow \pi(\exp t_pX_p \cdots \exp t_1X_1)$$

is a Lie group isomorphism. Using ϕ we shall identify G/B with $\mathbb{R}^p$.

Observe that every $g \in G$ can be written in the form

$$g = yx \text{ with } x = \exp t_pX_p \cdots \exp t_1X_1 \text{ and } y \in B.$$

We put

$$|t| = |t_p| + \cdots + |t_1| \text{ for } t = (t_p, \ldots, t_1) \in \mathbb{R}^p.$$

We fix a symmetric compact neighborhood $V \subseteq G$ of the identity element e of G and $U \subseteq B$ a symmetric compact neighborhood of e in B and we put

$$|x|_G = \inf\{n \in \mathbb{N} : x \in V^n\}$$
$$|y|_B = \inf\{n \in \mathbb{N} : y \in U^n\}$$
$$\theta = \sup\{|\exp sX_i y \exp -sX_i|_B, y \in U, |s| \leq 1, 1 \leq i \leq p\}$$
$$\delta = \sup\{|\exp sX_i \exp rX_j \exp -sX_i \exp -rX_j|_B, |s| \leq 1, |r| \leq 1, 1 \leq i, j \leq p\}.$$

Observe that, if $\rho(.,.)$ is as in Section 0.1, then $\rho(e, g) = |g|_G$, $g \in G$.

Arguing in the same way as in Section 4, we can prove successively that there is a constant $c > 0$ such that for all $y, z \in B$, $x = \exp t_p X_p \cdots \exp t_1 X_1$, $w = \exp s_p X_p \cdots \exp s_1 X_1$, $t = (t_p, \ldots, t_1)$, $s = (s_p, \ldots, s_1) \in \mathbb{R}^n$, $r \in \mathbb{R}$, $|r| \leq 1$, $1 \leq i \leq p$ we have

$$|xyx^{-1}|_B \leq |y|_B \theta^{|t|} \tag{4.1}$$

$$x \exp rX_i x^{-1} = h \exp rX_i, \text{ with } h \in B, |h|_B \leq ce^{c|t|} \tag{4.2}$$

$$\exp t_p X_p \cdots \exp t_1 X_1 \exp rX_i = v \exp t_p X_p \cdots \exp(t_i + r)X_i \cdots \exp t_1 X_1, \quad \text{with } v \in B,\ |v|_B \leq ce^{c|t|} \tag{4.3}$$

$$yxzw = v \exp(t_p + s_p)X_p \cdots \exp(t_1 + s_1)X_1, \quad \text{with } v \in B,\ |v|_B \leq c[|y|_B + |z|_B e^{c|t|} + e^{c(|t|+|s|)}] \tag{4.4}$$

and that all $g \in G$ can be written as

$$g = y \exp t_p X_p \cdots \exp t_1 X_1, \text{ with } |y|_B \leq ce^{c|g|_G},\ |t| \leq |g|_G,\ t = (t_p, \ldots, t_1). \tag{4.5}$$

Let $f(g) = p_1(e, g)$, $g \in G$. Then it follows from (0.2) that there are constants $c, d > 0$ such that

$$|f(g)| \leq ce^{-d|g|_G^2}, \quad g \in G \tag{4.6}$$

and from this that there are constants $c, d > 0$ such that

$$\int_{\{g \in G : |g|_G \geq m\}} f(g)\, dg \leq ce^{-dm^2}, \quad m > 0. \tag{4.7}$$

Also, if f^n denotes the nth convolution power $f * \cdots * f$ of f ($f * h(g) = \int f(x)h(x^{-1}g)\, dx$, $g \in G$), then $f^n(g) = p_n(e, g)$, $g \in G$.

Proceeding as in Section 3, we consider independent identically distributed random variables X_k, $k = 1, 2, \ldots$, with values in G and $P[X_k \in A] = \int_A f(g) dg$ (A a Borel subset of G). Then it follows from (4.7) that there are constants $c, d > 0$ such that

$$P\Big[\sup_{1 \leq i \leq k} |X_i|_G \geq m\Big] \leq cke^{-dm^2}, \quad m > 0. \tag{4.8}$$

Let Z_k, $k = 0, 1, 2, \ldots$ be the right random walk in G defined by

$$Z_0 = e \text{ a.s. and } Z_k = X_1 X_2 \cdots X_k, \quad k = 1, 2, \ldots .$$

Also let $S_k = (S_{k,p}, \ldots, S_{k,1}), k = 0, 1, 2, \ldots$ be the random walk in $\mathbb{R}^p$ defined by (recall that G/B has been identified with $\mathbb{R}^p$)

$$S_0 = 0 \text{ a.s. and } S_k = \pi(X_1) + \pi(X_2) + \cdots + \pi(X_k), \quad k = 1, 2, \ldots$$

Observe that $S_k = \pi(Z_k)$.

We put

$$X^{S_k} = \exp S_{k,p} X_p \cdots \exp S_{k,1} X_1.$$

Then it follows from (4.4) that there is $c > 0$ such that

$$\text{(4.9)} \qquad \begin{gathered} Z_k = Y_k X^{S_k}, \text{ with } Y_k \in B, \\ |Y_k|_B \leq c\Big[e^{c|X_1|_G} + e^{c(|S_1| + |X_2|_G)} + \cdots + e^{c(|S_{k-1}| + |X_k|_G)}\Big]. \end{gathered}$$

It follows from Kolmogorov's inequality that there is $b > 0$ such that

$$\text{(4.10)} \qquad P\Big[\max_{1 \leq i \leq k} |S_i| \leq m\Big] \geq 1 - b\frac{k}{m^2}, \quad k \in \mathbb{N},\ m > 0.$$

Let c be as in (4.9) and put

$$\begin{aligned} D_k^m = \{g \in G : g = y \exp t_p X_p \cdots \exp t_1 X_1, |t_p| + \cdots + |t_1| \\ \leq m, y \in B, |y|_B \leq cke^{2cm}\}, \quad k \in \mathbb{N},\ m > 0. \end{aligned}$$

Then, it follows from (4.8), (4.9), (4.10) and Lemma 1.2 that there are constants $a, b, c, d > 0$ such that that

$$\text{(4.11)} \qquad \begin{aligned} P[Y_k \in D_k^m] &\geq P\Big[\sup_{1 \leq i \leq k} |S_i| \leq m, \sup_{1 \leq i \leq k} |X_i|_G \leq m\Big] \\ &\geq ae^{-b\frac{m}{k^2}} - cke^{-dm^2}, \quad m > 0,\ k \in \mathbb{N}. \end{aligned}$$

We also have the following estimate of the volume $|D_k^m|$ of the set D_k^m, which follows from the fact that B has polynomial volume growth

$$\text{(4.12)} \qquad |D_n^m| \leq a_1 e^{a_2(m + \log k)}$$

(a_1, a_2 are constants, $a_1, a_2 > 0$).

PROOF OF THEOREM 4. Arguing in the same way as in the proof of Theorem 1, we can see that

$$f^k(e) = p_k(e, e) = p_k(x, x) = \sup_{y \in G} p_k(x, y), \quad x \in G$$

and that

$$p_t(x, x) \geq p_{[t]+1}(x, x) = f^{[t]+1}(e)$$

($[t]$ is the integral part of $t \in \mathbb{R}$).

This observation, together with (4.11) and (4.12) implies that there are constants a, b, c, d, a_1, $a_2 > 0$ such that

$$p_t(x,x) \geq \left[ae^{-b\frac{t}{m^2}} - cke^{-dm^2}\right]a_1 e^{-a_2(m+\log t)}, \quad m > 0,\ t \geq 1$$

and Theorem 4 follows by optimising with respect to m.

PROOF OF COROLLARY 5. We observe that if u is a bounded harmonic function then $u(x) = \int p_t(x,y)u(y)\,dy$, $x \in G$, hence $u(x) = \int u(xy)f(y)\,dy$, $x \in G$ and therefore u is a bounded f-harmonic function. Arguing in the same way as in the proof of Corollary 2, we can prove that every bounded f-harmonic function is constant and the corollary follows.

REFERENCES

1. A. Avez, *Harmonic functions on groups*, Diff. Geom. and Relativity, (1976), 27–32.

2. G. Alexopoulos, *On the mean distance of random walks on groups*, Bull. Sci. Math. (2) **III**(1987), 189–199.

3. Y. Derrienic, *Quelques applications du théorème ergodique sous-additif*, Astérisque **74**, 183–201.

4. ———, *Entropie, théorèmes limites et marches aléatoires*, Lecture Notes in Math. **1210**.

5. R. I. Grigorchuk, *Degrees of growth of finitely generated groups and the theory of invariant means*, Math. USSR, Izvestiya **25**(1985).

6. M. Gromov, *Groups of polynomial growth and expanding maps*, Publications mathématiques de l' I.H.E.S. **53**(1981).

7. Y. Guivarc'h, *Lois de grands nombres et rayon spectrale d' une march aléatoire sur un group de Lie*, Astérisque **74**(1980), 47–99.

8. ———, *Croissance polynômiale et périodes des fonction harmoniques*, Bull. Soc. Math. France, **101** (1973), 333–379.

9. L. Hörmander, *Hypoelliptic second order differential operators*, Acta Math. **119**(1967), 147–171.

10. V. A. Kaimanovich, *Brownian motion and harmonic functions on coverings of manifolds. An entropy approach*, Soviet Math. Doklady (3) **33**(1986), 812–816.

11. J. Milnor, *Growth of finitely generated solvable groups*, J. Diff. Geom. **72**(1968), 447–449.

12. A. Raugi, *Fonctions harmoniques sur les groupes localement compacts à base dénombrable*, Bull. Soc. Math. France, Mémoire **54**(1977), 5–118.

13. M. S. Ragunathan, *Discrete subgroups of Lie groups*, Springer-Verlag.

14. A. N. Shiryayev, *Probability*, Springer-Verlag, 1984.

15. V. S. Varadarajan, *Lie groups, Lie algebras and their Representations*, Springer-Verlag, 1984.

16. N. Th. Varopoulos, *Analysis on Lie groups*, J. Funct. Analysis (2) **76**(1988), 346–410.

17. ———, *Information theory and harmonic functions*, Bull. Sci. Math. (2^e) **110**(1986), 347–389.

18. ———, *A potential theoritic property of solvable groups*, Bull. Sci. Math. (2^e) **108**(1983), 263–273.

19. ———, *Théorie du potentiel sur les groupes et les variétés*, C.R. Acad. Sci. Paris (6) **302** I (1986), 203–205.

20. ———, *Analysis and geometry on groups*, Proceeding of the I.C.M., Kyoto, (1990), to appear.

21. ———, *Groups of superpolynomial growth*, preprint, 1990.

22. A. M. Vershik and V. A. Kaimanovich, *Random walks on discrete groups: Boundary and entropy*, The Annals of Probability (3) **11**(1983), 457–490.

23. J. A. Wolf, *Growth of finitely generated solvable groups and curvature of Riemannian manifolds*, J. Diff. Geom. **2**(1968), 421–446.

Université de Paris-Sud
Mathématiques, Bât. 425
91405 Orsay Cedex
France