Can. J. Math. Vol. **46** (5), 1994 pp. 1073–1092

DIFFUSION ON LIE GROUPS II

N. TH. VAROPOULOS

ABSTRACT. The heat kernel of an amenable Lie group satisfies either $p_t \sim \exp(-ct^{1/3})$ or $p_t \sim t^{-a}$ as $t \longrightarrow \infty$. We give a condition on the Lie algebra which characterizes the two cases.

RÉSUMÉ. Pour le noyau de la chaleur sur un groupe de Lie moyennable on a soit $p_t \sim \exp(-ct^{1/3})$, soit $p_t \sim t^{-a}$ (lorsque $t \longrightarrow \infty$). On donne une condition sur l'algèbre de Lie qui caracterise les deux cas.

0. **Introduction.** Let G be a connected real Lie group which is not assumed to be unimodular. Let $X_1, \ldots, X_k$ be left invariant fields on G (*i.e.*, $Xf_g = (Xf)_g, f_g(x) = f(gx)$) and let $\Delta = -\sum X_j^2$ and $T_t = e^{-t\Delta}$ be the left laplacian and the left diffusion semigroup which they generate. I shall assume throughout that Δ is subelliptic (*i.e.* the X_i's are generators of the Lie algebra, *cf.* [1], [2], [3]). I shall denote by $dg = d^\ell g$ (resp. $d^r g$) the left (resp. right) Haar measure on G and by $p_t(x,y) = \phi_t(y^{-1}x)$ $(x, y \in G)$ the corresponding "left" diffusion kernel:

$$T_t f(x) = \int_G p_t(x,y) f(y)\, dy, \quad f \in C_0^\infty(G),\ t > 0.$$

Let $\mathfrak{g}$ be the Lie algebra of G and let $\mathfrak{n} \subset \mathfrak{q} \subset \mathfrak{g}$ denote the radical and the nilradical of $\mathfrak{g}$ (*cf.* [4], [5]). $\mathfrak{q}/\mathfrak{n} = V$ and $\mathfrak{n}/[\mathfrak{n}, \mathfrak{n}] = W$ are then abelian Lie algebras that can be identified with real vector spaces; furthermore, the derivation ad on $\mathfrak{g}$ induces ad: $V \longrightarrow \mathfrak{gl}(W)$ $(= \mathrm{End}_{\mathbf{R}}(W))$. An $\mathbf{R}$-linear complex valued mapping $\lambda: V \longrightarrow \mathbf{C}$ is called a *root* if there exists $0 \neq w \in W \otimes \mathbf{C}$ such that $\big(\mathrm{ad}\, v - \lambda(v)\big)w = 0$ $(\forall v \in V)$ (*cf.* [4]). We shall then consider $L_1, \ldots, L_n \in V^*$ $(n \geq 0)$ the finitely many non zero real parts of these roots and we shall say that G satisfies condition (NC) if the convex hull:

$$\mathcal{L} = \left\{ \sum_{j=1}^{n} \alpha_j L_j \,;\, \alpha_j \geq 0 \ \sum \alpha_j = 1 \right\} \subset V^*$$

is such that $0 \notin \mathcal{L}$. The condition (NC) is in particular verified if

$$\{L_1, \ldots, L_n\} = \emptyset \subset V^*.$$

In this paper I shall prove the following:

Received by the editors December 22, 1992.
AMS subject classification: Primary: 22E30, 43A80; secondary: 60J60, 60J65.

THEOREM 1. *Let G be as above and let us assume that G is amenable and satisfies the condition* (NC). *There exists then $\nu > 0$ such that:*

$$\phi_t(g) \geq t^{-\nu} \tag{0.1}$$

for every t large enough (depending on g).

The following remarks will help to clarify this theorem.

(i) If G is non-amenable the above estimate cannot possibly hold. Indeed, the fact that $\phi_t(g) = 0(e^{-\lambda t})$ $(t \longrightarrow \infty)$ for some positive $\lambda > 0$ and some (or equivalently all) $g \in G$ can be taken as a definition of *non*-amenability (*cf.* [7]).

(ii) If the condition (NC) does not hold then the condition (C) of [8] holds and then we have proved in [8] that there exists $c > 0$ s.t.

$$\phi_t(g) = 0(e^{-ct^{1/3}}) \quad (\forall g \in G). \tag{0.2}$$

(iii) One should also observe that for any amenable G we have:

$$\phi_t(e) \geq c^{-1}e^{-ct^{1/3}}, \quad t \geq 1 \tag{0.3}$$

for some $c > 0$. This has been proved in [9], [10]. In the course of the proof of Theorem 1, an independent proof of the above lower estimate (0.3) will also emerge.

(iv) The above theorem is in some ways a very unsatisfactory "qualitative" result. The main "raison d'être" of this theorem is that in conjunction with the estimate (E) of [8], it gives a geometric "dichotomy" between the groups that satisfy condition (NC) and those which do not, in terms of the polynomial behaviour of the heat kernel. The "ultimate" result to aim for, is to obtain, under the (NC) condition, the correct asymptotics:

$$\phi_t(g) \sim C(g)t^{-\nu} \quad (t \longrightarrow \infty)$$

where $\nu = \nu(G, \Delta)$ is computable in terms of the geometry of the roots and Δ. I shall address myself to this problem in a future paper *cf.* [20]. Observe however that in general, the above ν *does* depend on Δ and is *not* a group invariant. For some groups, in fact, by changing Δ, one can make ν take *any* value $\geq \nu_0(G)$. None of these facts will be proved in this paper.

(v) It is enough to prove the estimate (0.1) for $g = e$ or even prove the integrated result:

$$\int_\Omega \phi_t(g)\, dg \geq ct^{-\nu}; \quad t \geq 1$$

for some fixed Ω neighbourhood of the neutral element. The general result follows then by the local Harnack estimate (*cf.* [1], [2]).

(vi) This remark is purely algebraic and will not be used in the rest of this paper. Let $\mathfrak{h} \subset \mathfrak{q}$ be a Cartan subalgebra of the real soluble algebra $\mathfrak{q}$, and let $\alpha_1, \ldots, \alpha_k \in (\mathfrak{h}_{\mathbb{C}})^*$ be the weights of the Zassenhaus decomposition (*cf.* [5], Chapter II, §4) of the action of $\mathrm{ad}(\mathfrak{h} \otimes \mathbb{C})$ on $\mathfrak{q} \otimes \mathbb{C}$. Then instead of defining the condition (NC) as above with the L_j' s we can define the condition (NC) analogously but where we replace the L_j's by the

$\tilde{L}_j$'s that are the *nonzero* $\mathrm{Re}(\alpha_j|_{\mathfrak{h}}) \in \mathfrak{h}^*$. We obtain thus an equivalent definition. Indeed it is clear that the α_j's can be identified to elements of $\mathfrak{h} \otimes \mathbb{C}/\mathfrak{n} \otimes \mathbb{C} \cong V \otimes \mathbb{C}$ (*cf.* [6], Proposition 17, §4.5, Chapter VI). It is then easy to see (this is essentially outlined in the course of the proof of Lemma 1.2, §1) that the real convex cone generated by the α_j's and the real convex cone generated by the roots λ are identical. This proves the assertion. Using our original definition of the (NC) condition we can readily see that if $\mathfrak{g}$ is an (NC) algebra then $\mathfrak{g}/\mathfrak{s}$, any quotient of $\mathfrak{g}$, is also an (NC) algebra. (This fact follows also very easily from our main analytic characterisation of the (NC) condition (*cf.* Remark (iv)). Observe on the other hand that a subalgebra of an (NC) algebra is not in general (NC). To construct an example let V be an arbitrary real vector space V and let $\{L_1, \ldots, L_k\} \subset V^*$ be an arbitrary subset. Let also $Q = \mathbb{R}^k \lambda V$ where the action is defined by $v(x_j)_{j=1}^k = \Big(\big(\exp L_j(v)\big)x_j\Big)_{j=1}^k$. Q is then a soluble group whose roots are exactly $L_1, \ldots, L_k$.

We can also see very easily that the "Iwasawa groups" (*i.e.* the soluble groups of the form AN that appear in the Iwasawa decomposition of a semisimple group $G = \mathrm{KAN}$) are all (NC) groups. One can also verify very easily that a unimodular group is (NC) if and only if it is an R-group (*cf.* [12] for the definition) *i.e.* if and only if it has polynomial volume growth (*cf.* [12]).

Let us finally consider G a general connected real Lie group which does not necessarily satisfy the condition (NC), and let Δ and ϕ_t have the same meaning as before. Let further $m(g) = d^r g/dg$ (normalised by $m(e) = 1$) be the modular function on G and $\tilde{\Delta} = m^{1/2}\Delta m^{-1/2}$. The operator $\tilde{\Delta}$ has a closure on $L^2(G\,; dg)$ which is a positive self adjoint operator on $L^2(G\,; dg)$. The complex powers $\tilde{\Delta}^\alpha = m^{1/2}\Delta^\alpha m^{-1/2}$ ($\alpha \in \mathbb{C}$) can thus be defined by spectral theory. We have then

THEOREM. *Let G, $\tilde{\Delta}$, ϕ_t be as above and let us assume that $\alpha \in \mathbb{C}$, $n > 0$, $1 < p \leq 2 \leq q < +\infty$ are such that $\mathrm{Re}\,\alpha > 0$, $1/q = 1/p - \frac{\mathrm{Re}\,\alpha}{n}$, $\phi_t(e) = 0(t^{-n/2})$ $(t > 0)$. Then $\tilde{\Delta}^{-\alpha/2}\colon L^p(G;dg) \longrightarrow L^q(G;dg)$ is a bounded operator.*

The proof of this theorem will appear elsewhere *cf.* [20] and will not be given in this paper. This theorem should be compared with the corresponding results for unimodular groups (*cf.* [1], [2]) and with the fact (*cf.* [19]) that when $m \not\equiv 1$, then $\tilde{\Delta}^{-1/2+is}\colon L^2(G\,; dg) \longrightarrow L^p(G;dg)$ is bounded for $s \in \mathbb{R}$, $2 < p < +\infty$, $1/2 - 1/p \leq 1/\delta$ where $\delta > 0$ is the "local dimension" (*i.e.* $\phi_t(e) = 0(t^{-\delta/2})$ $t \longrightarrow 0$).

Let us further denote by

$$\tilde{\Delta} = \int_0^\infty \lambda \, dE_\lambda$$

the spectral decomposition of $\tilde{\Delta}$ on $L^2(G\,; dg)$. Then the above theorem implies immediately (by factorising: $L^p \longrightarrow L^2 \longrightarrow L^2 \longrightarrow L^q$) that $m(\tilde{\Delta}) = \int_0^\infty m(\lambda)\, dE_\lambda$ is $L^p \longrightarrow L^q$ bounded provided that $m(\lambda) = 0(\lambda^{-a/2})$ ($\forall \lambda > 0$ and $a > 0$ fixed) and $1/q = 1/p - a/n$ (where $n > 0$ is as in the theorem and $1 < p \leq 2 \leq q < +\infty$). This last formulation of our result is of course the natural generalisation of a classical theorem of Hardy and Littlewood (*cf.* [18]).

The second theorem that we shall prove in this paper shows that the above polynomial lower bound of $\phi_t(e)$ has nothing to do with differential operators but is a result on convolution powers of measures. Let $d\mu(g) = \varphi(g)\,dg$ be a compactly supported symmetric probability measure on G (*i.e.* the mapping $x \mapsto x^{-1}$ takes μ onto itself: $\check{\mu} = \mu$) where $\varphi(g) \in C_0(G)$, and let us consider $d\mu_n(g) = \varphi_n(g)\,dg$ where $\mu_n = \mu^{*n}$ is the convolution power of μ. We have then:

THEOREM 2. *Let G be as in Theorem 1 and let μ and $\varphi_n(g)$ be as above; there exists then $\nu > 0$ such that*

$$\varphi_n(g) \geq n^{-\nu} \tag{0.4}$$

for every n large enough (depending on g).

The following remarks (i)–(iii) are easy to verify. The verification will be left to the reader because none of these remarks is really essential in what follows.

REMARK. (i) For any $d\mu = \psi(g)\,dg$ with $\psi \in L^2$ and compactly supported we have $d\mu^{*2} = \varphi\,dg$ with $\varphi \in C_0(G)$. From this we see that the continuity of the density is not really essential in the above theorem.

(ii) The conclusion of Theorem 2 can equivalently be stated as follows:

For every neighbourhood Ω of the neutral element of G we have:

$$\mu_n(\Omega) \geq n^{-\nu}\,; \quad n > c$$

for some $\nu, c > 0$ large enough (*cf.* end of §3).

(iii) This remark applies both to Theorem 1 and Theorem 2: For the proof of these theorems we may as well assume that G is *simply connected*. This will be *assumed throughout* this paper. Indeed for a general group G we can "lift" the generator Δ or μ appropriately to $\tilde{G} \longrightarrow G$, the simply connected cover of G. Once the theorem has been proved on $\tilde{G}$ it follows automatically for G. To see this, one uses the local Harnack estimates, in the case of Theorem 1, or the obvious discrete analogue of this Harnack estimates in the case of Theorem 2 (*cf.* end of §3).

What is less trivial, and in fact anything but easy to verify, is the following remark.

REMARK. The compactness of the support of μ is *not* essential for the conclusion of Theorem 2 to hold. Some very fast, say superpolynomial, decay of the mass distribution of μ at infinity is good enough. Nor is it necessary to consider convolution powers of the same measure. We could consider instead $\mu_n = \mu^{(1)} * \mu^{(2)} * \cdots * \mu^{(n)}$ provided that the $\mu^{(j)}$'s satisfy the required conditions uniformly in $j = 1, 2, \ldots$.

The modifications that have to be made in the proofs to give the above generalisation lie entirely at a probabilistic level in the setting of §4. I decided not to give this most general theorem because it would have multiplied at least by five the size of §4—an effort that seemed disproportionate compared with the improvement that it would give.

GUIDE TO THE READER. The actual proof of the two theorems is given in §2 and §3. Section 1 and §4 are essentially mutually independent and independent of §2 and

§3. Section 1 contains the "Geometry background" needed and uses the theory of Lie algebras. Section 4 contains the "Probabilistic background" and requires some familiarity with probabilistic potential theory. In a first reading, the reader could skim through §1 and §4 and go straight to the heart of the matter *i.e.* §2 and §3.

In a final paragraph §5 I indicate the changes that one can make in §2 and §3 to give a "new" proof the lower exponential estimate (0.3). This new proof may not be very interesting, especially since it has a number of features in common with the original proof and with another more recent proof given in [11]. The only reason for including it is that I feel it rounds out nicely the present circle of ideas.

1. **The construction of a special section of the nilradical.** Let G be a simply connected Lie group, and $\mathfrak{g}$ its Lie algebra. As in §0, denote the radical and nilradical of $\mathfrak{g}$ by $\mathfrak{r}$ and $\mathfrak{q}$ respectively. I shall denote by $N \subset Q \subset G$ the corresponding analytic subgroups. These are simply connected, closed subgroups, and Q is soluble. The notation $\mathfrak{q}/\mathfrak{n} = V$ and the notation $\lambda: V \longrightarrow \mathbb{C}$ for the roots introduced in §0 will also be preserved.

It is clear that $Q/N = V \cong \mathbb{R}^m$. Note that I shall use the same letter V for the vector group Q/N and the Lie algebra $\mathfrak{q}/\mathfrak{n}$. This should cause no confusion. Since G is simply connected, there are canonical projections π and p_M such that

$$\pi: G \longrightarrow G/N \cong V \times M \xrightarrow[p_M]{} M$$

where M is a semisimple group (*cf.* [4] Corollary 3.16.4 and Theorem 3.18.13). We can also embed $\theta: M \longrightarrow G$ isomorphically so that $p_M \circ \pi \circ \theta =$ identity and $\theta(M)$ is a closed group known as a Levi subgroup. I shall drop the letter θ from here on, and simply set $M \subset G$. This embedding gives us a very satisfactory section of $G \longrightarrow G/Q$. Most of the remainder of this paragraph will be devoted to the construction and analysis of an appropriate section of π itself.

Such a section will be constructed by first constructing $\sigma: V \longrightarrow Q$, $\sigma(V) = \Sigma \subseteq Q$ a section of $Q \longrightarrow Q/N$. We shall identify V with $\mathbb{R}^m$ and define:

$$(1.1) \qquad \sigma(t_1, \ldots, t_m) = x_1(t_1) \cdots x_m(t_m) \in Q\,; \quad (t_1, \ldots, t_m) \in \mathbb{R}^m = V$$

where $x_i(t) = \exp(te_i)$ $(1 \leq i \leq m)$ and where we choose the $e_i \in \mathfrak{q}$ so that $\{d\pi(e_i)\,;\ 1 \leq i \leq m\}$ is a basis of V. It is clear that the mapping σ constructed in this way is a section. It will be important in what follows to choose the $e_i \in \mathfrak{q}$, $1 \leq i \leq m$, not in an arbitrary fashion but in such a way that the Lie algebra they generate $\mathfrak{a} = \mathrm{Alg}(e_1, \ldots, e_m) \subseteq \mathfrak{q}$ is nilpotent. That this is possible was shown in [13]. By using the general theory of Lie algebras we can give an alternative direct proof of this fact: let $\mathfrak{n}_0 \subset \mathfrak{q}$ be a Cartan subalgebra of $\mathfrak{q}$. Such an algebra is nilpotent and $d\pi(\mathfrak{n}_0) \subset V$ is a Cartan subalgebra of V (*cf.* [6], VI, §4.5, Proposition 17). Therefore $d\pi(\mathfrak{n}_0) = V$ and the above choice of the e_i's is clearly possible. In [13] a more precise result was proved:

LEMMA (G. ALEXOPOULOS). *Let $\mathfrak{m} \subset \mathfrak{g}$ be the Lie algebra of $M \subset G$. It is then possible to choose the above $e_1, \ldots, e_m \in \mathfrak{q}$ so that the Lie algebra $\mathfrak{a}$ which they generate is nilpotent* and $[\mathfrak{a}, \mathfrak{m}] = 0$.

Indeed $\mathfrak{m}$, is semisimple, it acts by ad on $\mathfrak{q}$, and stabilises $\mathfrak{n}$. There exists then (*cf.* [4], p. 222) $W \subset \mathfrak{q}$ some direct complement of $\mathfrak{n}$ in $\mathfrak{q}$ for that action. But since $[\mathfrak{m}, \mathfrak{q}] \subset \mathfrak{n}$ it follows that $[\mathfrak{m}, W] = 0$. Let us denote $\{x \in \mathfrak{q},\ [\mathfrak{m}, x] = 0\}$, which is a subalgebra, by $\mathfrak{q}_0$. Then $W \subset \mathfrak{q}_0$ and therefore $\mathfrak{q}_0/\mathfrak{q}_0 \cap \mathfrak{n} = V$. (The use of the subalgebra $\mathfrak{q}_0$ was suggested to me by G. Alexopoulos: oral communication). If we apply our previous argument to the soluble algebra $\mathfrak{q}_0$ we have a proof of the lemma.

I shall now establish, once and for all, a number of important notations that will be used in the remainder of the paper. Let G be as above. Denote by $d_G(x, y)$, $(x, y \in G)$ the left-invariant Riemannian distance induced on G by some fixed (but, *a priori*, arbitrary) scalar product $\langle .\ , . \rangle$ on $\mathfrak{g}$. I shall also write $|x|_G = d_G(e, x)$ $(x \in G)$ where $e \in G$ is the neutral element. It is clear enough that if $H \subset G$ is a closed connected Lie subgroup then there exists $C > 0$ such that

$$d_G(x, y) \leq C d_H(x, y)\ ; \quad x, y \in H. \tag{1.2}$$

The reverse inequality is in general false of course. Much of the remainder of this section will be related to the estimate:

$$d_H(x, y) \leq C \exp\Big(C d_G(x, y)\Big)\ ; \quad x, y \in H \tag{1.3}$$

which, as we shall see, holds if $H = N$ is the nilradical of G.

REMARK. Observe that in the definition of $d_G(.\ , .)$ and for (1.2) to hold we do not need the assumption that G is simply connected.

Concerning the Section Σ (1.1) let us observe that:

$$C^{-1}|t| \leq |\sigma(t)|_G,\ |\sigma(t)|_Q \leq C|t|\ ; \quad t \in V$$

for some $C > 0$ independent of t. The easiest way to verify this is to use the general fact that, if H is a normal subgroup of G, and π is the canonical projection onto G/H, then

$$d_{G/H}\Big(\pi(x), \pi(y)\Big) \leq C d_G(x, y)\ ; \quad x, y \in G$$

for some $C > 0$ independent of x, y. The estimate $|\sigma(t)|_G \geq C^{-1}|t|$ then follows from the fact that $G/N \cong V \times M$.

We shall first recall some easy facts from group theory. Let G be a discrete group and let $g_1, \ldots, g_s \in G$. We shall say that $x \in G$ is a *commutator of length* p $(p \geq 2)$ on the elements $g_1, \ldots, g_s$ if $x = [y, g_k]$ or $x = [g_k, y]$ with $1 \leq k \leq s$ and where y is a commutator on the elements $g_1, \ldots, g_s$ of length $p - 1$. The commutators of length 1 will be by definition the elements $g_1, \ldots, g_s$. Two such commutators will be called *formally distinct* if they can be written in two distinct ways as a succession of the symbols "[,],

g_k, comma". Two formally distinct commutators may, of course, very well give rise to the same group element.

Let now F be a free group freely generated by the elements $x_1, \dots, x_s \in F$. Let also $\sigma \in \mathfrak{S}_s$ a permutation on s letters. We have then

$$x_{\sigma(1)} \cdots x_{\sigma(s)} = x_1 x_2 \cdots x_s \omega$$

where $\omega \in F$ is a finite product of formally distinct commutators on $x_1, \dots, x_s$. The proof is an easy induction on s where the inductive step relies on the observation that for any $2 \leq j \leq s$.

$$x_1 x_2 \cdots x_s = x_2 x_3 \cdots x_j x_1 x_{j+1} \cdots x_s \tilde{\omega}$$

where again $\tilde{\omega}$ is a product of formally distinct commutators that *involve* x_1. The details will be left to the reader.

Observe now that the total numbers of formally distinct commutators on $g_1, \dots, g_s \in G$ of length at most k is bounded above by $(s+3)^{10k}$. From the above two facts we immediately deduce the following:

LEMMA (NIL-GP). *Let G be a nilpotent (discrete group). Then there exists $C > 0$ s.t. for any $s \geq 1$ any $g_1, \dots, g_s \in G$ and any $\sigma \in \mathfrak{S}_s$ we have*

$$g_{\sigma(1)} \cdots g_{\sigma(s)} = g_1 \cdots g_s \omega$$

where $\omega \in G$ is a product of at most $(s+C)^C$ commutators on $g_1, \dots, g_s$ of length at most C.

We shall also need some elementary facts from linear algebra. Let $s \geq 1$ and let

$$T_j = (t^{(j)}_{\alpha,\beta}) \in M_{p\times p}(\mathbb{C}), \quad 1 \leq j \leq s$$

be (strictly) upper triangular matrices (*i.e.* $t^{(j)}_{\alpha,\beta} = 0$ if $\alpha \leq \beta$). Let also $M_j = \lambda_j I + T_j$ where $\lambda_j \in \mathbb{C} \setminus \{0\}$ $(1 \leq j \leq s)$. We have then:

$$M_1 \cdots M_s = \lambda_1 \cdots \lambda_s \sum_{\alpha, i_j} (\lambda_{i_1} \cdots \lambda_{i_\alpha})^{-1} T_{i_1} \cdots T_{i_\alpha}.$$

In the above summation all the terms for which $\alpha > p$ are 0. The following lemma is therefore an immediate consequence of this fact.

LEMMA 1.1. *Let M_j, $1 \leq j \leq s$ be as above, let $u, \rho \in \mathbb{R}$, and let us assume that:*

$$|T_j| \leq e^u, \ |\lambda_j^{-1}| \leq e^u \quad (1 \leq j \leq s) \ ; \ |\lambda_1 \cdots \lambda_s| \leq e^\rho. \tag{1.4}$$

There exists then $C = C(p)$, depending only on the dimension such that

$$|M_1 \cdots M_s| \leq C s^C e^{\rho + Cu} \leq C s^C (e^{C\rho} + e^{Cu})$$

where the $|\cdot|$ denotes the operator norm of the matrix for the standard scalar product space $\mathbb{C}^p$.

Let us now recall the standard notation for $\mathrm{Ad}(g)$ $(g \in G)$ which can be identified to a linear automorphism of $\mathfrak{n}$ and also of $\mathfrak{n}_C = \mathfrak{n} \otimes \mathbb{C}$, the complexified space, so that $\mathrm{Ad}(G) \subset \mathrm{GL}_{\mathbb{C}}(\mathfrak{n}_C) \subset \mathcal{L}_{\mathbb{C}}(\mathfrak{n}_C)$. I shall denote by $|\cdot|_{\mathfrak{n}}$ the standard operator norm on $\mathcal{L}_{\mathbb{C}}(\mathfrak{n}_C)$ (induced by some fixed scalar product on $\mathfrak{n}$). We have then

LEMMA 1.2. *Let $g_j = \sigma(t_j) \in \Sigma \subset Q$, $t_j \in V = \mathbb{R}^m$ $(1 \leq j \leq s)$, let $\tau, \rho > 0$, and let us assume that:*

$$|g_j|_G \leq \tau \quad 1 \leq j \leq s\ ;\ L_k(t_1 + \cdots + t_s) \leq \rho, \quad 1 \leq k \leq n$$

where $L_1, \ldots, L_n$ are as in §0. Then there exists C (depending only on $\mathfrak{g}$) such that:

$$|\operatorname{Ad}(g_1)\operatorname{Ad}(g_2)\cdots\operatorname{Ad}(g_s)|_{\mathfrak{n}} \leq Cs^C e^{C\rho + C\tau}. \tag{1.5}$$

PROOF. The algebra $\mathfrak{a} = \operatorname{Alg}(e_1, \ldots, e_m)$, by the action of ad, induces a nilpotent Lie algebra of (complex) linear transformations on $\mathfrak{n}_C$. The classical Zassenhaus decomposition applies (*cf.* [5], II, 4) and the following facts hold: We can decompose $\mathfrak{n}_C = \mathfrak{n}_1 \oplus \cdots \oplus \mathfrak{n}_t$ as a direct sum of subspaces each of which is invariant by the action of ad $\mathfrak{a}$. Furthermore on each such subspace $\mathfrak{n}_r$ a basis can be chosen so that

$$\operatorname{ad} x|_{\mathfrak{n}_r} = \alpha(x)I + T(x)\ ; \quad x \in \mathfrak{a} \tag{1.6}$$

where $\alpha: \mathfrak{a} \longrightarrow \mathbb{C}$ is the "weight" that corresponds to $\mathfrak{n}_r$ and $T(x)$ is a (strictly) upper triangular matrix. It is clear also that $\alpha(x) = 0$ if $x \in \mathfrak{a} \cap \mathfrak{n}$, so that α can be identified with $\alpha: V \longrightarrow \mathbb{C}$ a complex valued $\mathbb{R}$-linear functional on $V = \mathfrak{q}/\mathfrak{n} = \mathfrak{a}/\mathfrak{n} \cap \mathfrak{a}$. We also recall the standard fact that for each weight α as above there exist finitely many (not necessarily distinct) roots $\lambda_1, \ldots, \lambda_\nu: V \longrightarrow \mathbb{C}$ such that $\alpha = \lambda_1 + \cdots + \lambda_\nu$. [Indeed: V acts by ad on each $\mathfrak{p}^\ell = \mathfrak{n}^\ell/\mathfrak{n}^{\ell+1}$ with $\mathfrak{n}^\ell = [\mathfrak{n}_C[\mathfrak{n}_C[\cdots \mathfrak{n}_C]\cdots]$. The root space decomposition of $\mathfrak{p} = \mathfrak{n}_C/[\mathfrak{n}_C, \mathfrak{n}_C]$ induces thus, by the Jacobi identity, a root space decomposition of each $\mathfrak{p}^\ell$ and the corresponding roots are sums of the form $\lambda_1 + \cdots + \lambda_\nu$. Let then α be a weight as above and let $0 \neq \omega \in \mathfrak{n}_r$ be such that $(\operatorname{ad} x)\omega = \alpha(x)\omega$ $(x \in V)$. Also let ℓ be the largest integer for which $\omega \in \mathfrak{n}^\ell$. Then $\omega \pmod{\mathfrak{n}^{\ell+1}}$ is a common eigenvector and $\alpha(x)$ can be identified with a common eigenvalue of the action of V on $\mathfrak{p}^\ell$. It follows therefore that for each $x \in V$ $\alpha(x) = \lambda_1(x) + \cdots + \lambda_\nu(x)$ (where the λ's that we have to take, *a priori*, depend on x). But since there are at most countably many (in fact only finitely many) sums of roots $\lambda_{i_1} + \cdots + \lambda_{i_p}$, we conclude that α has the required form $\lambda_1 + \cdots + \lambda_\nu$].

For every $g = \sigma(t) = x_1(t_1)\cdots x_m(t_m) \in \Sigma$, $t = (t_1, \ldots, t_m) \in \mathbb{R}^m \cong V$ we have, with our previous notation,

$$\operatorname{Ad}(g) = \prod_{i=1}^{m} \operatorname{Ad}[x_i(t_i)] = \prod_{i=1}^{m} \operatorname{Ad}[\exp(t_i e_i)].$$

$\operatorname{Ad} g$, stabilises the subspaces $\mathfrak{n}_1, \ldots, \mathfrak{n}_t$, and its restriction on each of these spaces is a linear transformation, which for the same basis as in (1.6), has the form

$$\operatorname{Ad} g|_{\mathfrak{n}_r} = (e^{\alpha(t)}I) + \tilde{T}, \quad t = (t_1, \ldots, t_m)$$

where t is identified with $\Sigma t_j e_j \in \mathfrak{a}$. Here $\tilde{T}$ is again a (strictly) upper triangular matrix and a moment's reflection shows that there exists a constant $C > 0$ such that

$$|\tilde{T}| \leq C\exp(C|t|)\ ; \quad t \in \mathbb{R}^m.$$

This shows that the estimate (1.5) is an automatic consequence of Lemma 1.1 provided that we take $u \sim \tau$ in (1.4).

Let us now denote quite generally by

$$\tau_g(x) = g^{-1}xg\ ; \quad g, x \in G\ ;$$

it is then immediate from the fact $d\tau_g = \mathrm{Ad}(g)$ $(g \in G)$ that:

$$d_N\big(\tau_g(x), \tau_g(y)\big) \leq |\mathrm{Ad}(g)|_{\mathfrak{n}} d_N(x, y)\ ; \quad x, y \in N,\ g \in G. \tag{1.7}$$

Let us also denote $B(r) = \{x \in N\ ;\ |x|_N \leq r\}$ the ball of radius r in N and let us assume that $g_1, \ldots, g_s \in \Sigma$ satisfy the conditions of Lemma 1.2. It follows then from (1.5) and (1.7) that for all $r > 0$ we have

$$B(r)g_1g_2\cdots g_s \subset g_1g_2\cdots g_sB\Big(Cs^Cr(e^{C\rho} + e^{C\tau})\Big). \tag{1.8}$$

We shall now push this circle of ideas one step further. We shall consider, as in Lemma 1.2, a sequence $g_i = \sigma(t_i) \in \Sigma$, $i = 1, \ldots, s$ and assume that $|g_i|_G \leq \tau$, $1 \leq i \leq s$. But we shall also make the following additional assumption:

$$L_k(t_p + t_{p+1} + \cdots + t_s) \leq \rho \quad 1 \leq p \leq s\ ;\ 1 \leq k \leq n. \tag{1.9}$$

The conclusion will then be that for all $r > 0$ we have:

$$\begin{aligned} g_1B(r)g_2B(r)\cdots g_sB(r) &\subset g_1\cdots g_sB\Big(Crs^C(e^{C\rho} + e^{C\tau})\Big) \\ &\subset \sigma(t_1 + \cdots + t_s)B\Big(C(r+1)s^C(e^{C\rho} + e^{C\tau})\Big) \end{aligned} \tag{1.10}$$

where $C > 0$ as before only depends on the Lie algebra. The proof of the first inclusion is an easy induction on s where we use (1.9) and our previous inclusion (1.8). The second inclusion follows from the Nil-Gp Lemma and the fact that all the $x_i(t_j)$ lie in a nilpotent group. Observe also that all the commutations of elements of Q lie in N and that we can obtain a polynomial bound of say:

$$|[x_1(n), x_2(m)]| = |[x_1(1)\cdots x_1(1), x_2(1)\cdots x_2(1)]|_N\ ; \quad n, m = 1, 2, \ldots$$

by the Nil-Gp Lemma. The inclusions (1.10) will be basic in §3. We shall draw here a first consequence. Let $x_1, \ldots, x_s \in N$ be such that $|x_j|_N \leq 1$ $(1 \leq j \leq s)$, and let us assume that $g_1, \ldots, g_s \in \Sigma$ are such that $|g_j| \leq 1$ and $g_1g_2\cdots g_s \in N$. It then follows from (1.10) with $r = \tau = 1$, $\rho \sim Cs$ that:

$$g_1x_1g_2x_2\cdots g_sx_s \in B(Ce^{Cs}) \subset N.$$

This is but a reformulation of (1.3) where $H = N$ and $G = Q$.

Using the above lemma of G. Alexopoulos we shall now extend the above results to the section $\Sigma \cdot M \subset G$ of $\pi: G \longrightarrow G/N \cong V \times M$. Indeed this lemma allows us to choose Σ such that $[\Sigma, M] = e$ in G. If $g_1, \ldots, g_s$ are as in (1.10) and if $m_1, \ldots, m_s \in M$ are such that $|m_jm_{j+1}\cdots m_s| \leq c$ $(1 \leq j \leq s)$ (observe that $|m|_G \approx |m|_M$ $m \in M$), then

$$g_1m_1B(r)g_2m_2B(r)\cdots g_sm_sB(r) \subseteq \sigma(t_1+\cdots+t_s)m_1\cdots m_sB\Big(C(r+1)s^C(e^{C\rho}+e^{C\tau})\Big) \tag{1.11}$$

https://doi.org/10.4153/CJM-1994-061-6 Published online by Cambridge University Press

where here C depends on c. The proof is once more done by induction on s, and the use of the Nil-Gp Lemma.

Observe that in this paper we shall apply (1.11) only in the case where M is compact, and then the condition $|m_j \cdots m_s| \leq c$ is automatic. The reason is that for an amenable Lie group G the Levi subgroup M is always compact. If we assume that M is compact and apply (1.11) with $\tau = 1$ we see that (1.3) holds when H is the nilradical of G.

Before ending this section we shall make a final geometric observation that will be needed later on. Let us adopt throughout the notation $\pi(g) = \dot{g} \in G/N = V \times M$ $(g \in G)$ and let $g = \sigma(t).m.n$, $m \in M$, $n \in N$ be the corresponding "coordinate decomposition" of g with respect to these sections. It is then clear that for all $c > 0$ there exists $C > 0$ s.t. $C^{-1}(|t| + |m|_M) \leq |\dot{g}|_{G/H} \leq C(|t| + |m|_M)$ $(|t| + |m|_M \geq c)$ and also $C^{-1}(|t| + |m|_M) \leq |\sigma(t)m|_G \leq C(|t| + |m|_M)$. For compact M, on the section $\Sigma.M$, the large distances from e are thus measured on the t coordinate. From the above it follows also that $|n|_G \leq C|g|_G$ and therefore, when M is compact that:

$$|n|_N \leq C\exp(C|g|_G). \tag{1.12}$$

2. **The disintegration of the convolution kernel.** The set up in this section is the following: G is a locally compact group and $N \subset G$ is a normal closed subgroup and both G/N and N are unimodular. We shall consider $\mu \in \mathbb{P}(G)$ a symmetric probability measure (*i.e.* the involution $\alpha: x \longrightarrow x^{-1}$ stabilises that measure $\check{\alpha}(\mu) = \mu$).

We shall consider also $\mu_n = \mu^{*n}$ the convolution powers of μ and, to simplify notation, we shall assume that each μ_n $(n \geq 1)$ has a continuous density $\mu_n = \phi_n(g)d^r g = \phi_n(g)m(g)\,dg$ where dg (resp. $d^r g$) is the left (resp. right) invariant measure on G and $d^r g = m(g)\,dg$.

A good example of the above setup is a Lie group as considered in the introduction where N is its nilradical. Let us denote then by $d\mu_t(g) = \phi_t(g)\,d^r g = \phi_t(g)m(g)\,dg$ where $\phi_t(g)$ is the left diffusion kernel (*cf.* [8]). Since $T_t f = f * \mu_t$ $(t > 0)$ and since T_t is a self adjoint operator on $L^2(G\,; d^r g)$ it follows that $\check{\alpha}(\mu_t) = \mu_t$ $(t > 0)$. In this example we even have a continuous time semigroup of measures and not just the discrete sequence μ_n. I shall preserve the continuous time notation μ_t for the rest of this section (with the understanding that in the general case t only takes the discrete values $t = 1, 2, \ldots$).

For the rest of this section we shall have to fix also, once and for all, $S \subset G$ a Borel section of $\pi: G \longrightarrow G/N$ (*i.e.* π is (1-1) and "onto" on S) such that $e \in S$. In this paragraph the section S will be arbitrary, but for our applications S will be the section $\Sigma \cdot M$ that we constructed in the previous paragraph. In this paragraph we shall use (and abuse!) the following notation: $\dot{g} = \pi(g) \in G/N$ $(g \in G)$ and more often than not we shall drop the "dot" and denote by $g \in G/N$ and then proceed to identify $g \in G/N$ with an element $g \in S$. The reader will have keep track at every step whether the point g lies in G/N or S.

The next step is to disintegrate μ_t on the fibers of $\pi: G \longrightarrow G/N$ (*i.e.* the cosets of N) so that:

$$\mu_t = \int_{G/N} \lambda_{t,g}\,dg\,; \quad t > 0$$

where $dg = d_{G/N}g$ denotes here the Haar measure on G/N (which is a unimodular group) and $\lambda_{t,g} \in M(gN)$ $(g \in S;\ t > 0)$. We shall consider the identification of gN with N.

$$I(g): x \leftrightarrow gx\ ; \quad x \in N,\ g \in S.$$

Under $I(g)$, the measure $\lambda_{t,g}$ is identified to:

$$d\lambda_{t,g}(x) = \theta_{t,g}(x)\, d_N x\ ; \quad g \in G/N$$

where $\theta_{t,g} \in L^1(N)$ and $d_N x$ is the Haar measure of N.

The standard disintegration of the Haar measure on G:

$$\int_G f(g)\, dg = \int_{G/N} \left(\int_N f(gh)\, dh \right) d\dot{g}\ ; \quad f \in C_0(G) \tag{2.1}$$

implies that:

$$\theta_{t,g}(x) = \phi_t(gx)m(g)\ ; \quad t > 0,\ x \in N,\ g \in S. \tag{2.2}$$

The fact that $\check{\alpha}(\mu_t) = \mu_t$ implies that $\phi_t(g^{-1}) = \phi_t(g)m(g)$ and the semigroup property $\mu_t * \mu_s = \mu_{t+s}$ and (2.1) implies that

$$\begin{aligned} \phi_{2t}(e) &= \int_G \phi_t(g)\phi_t(g^{-1})\, d^r g = \int_G \phi_t(g)\phi_t(g^{-1})m(g)\, dg = \int_G \phi_t^2(g)m(g)^2\, dg \\ &= \int_{G/N} \int_N \phi_t^2(gn)m^2(gn)\, dn\, d\dot{g}. \end{aligned}$$

We thus finally conclude from (2.2) that:

$$\phi_{2t}(e) = \int_{G/N} \|\theta_{t,g}\|^2_{L^2(N)}\, dg. \tag{2.3}$$

I shall now explain the mechanism of the proof of the lower estimate (0.1) in Theorems 1 and 2 of §0. What I will prove in the next section is that there exists a large $c > 0$ s.t.

$$\int_{g \in G/N, |g| \le cn^c} \left(\int_{|x| \le cn^c} \theta_{n,g}(x)\, dx \right) dg \ge c^{-1} n^{-c}. \tag{2.4}$$

This is some kind of control of the rapidity with which the "total mass of the diffusion escapes at infinity". This estimate says, under the condition (NC) on G, that escape rate is polynomial.

Once the estimate (2.4) has been established, our lower estimates and Theorems 1 and 2 follow easily. Indeed using Hölders inequality on the "inside" integral of (2.4) we obtain

$$C^{-1} n^{-C} \le \int_{g \in G/N, |g| \le cn^c} \|\theta_{n,g}\|_{L^2(N)}\, dg\ ; \quad n \ge 1 \tag{2.5}$$

where $C > 0$ is some new constant. This is because, under the assumptions of Theorems 1 and 2, N is taken to be the nilradical, and is therefore of polynomial volume growth. Under the same assumption, G/N is also of polynomial volume growth, so one more use of Hölder's inequality shows that

$$\int_{g \in G/N, |g| \le cn^c} \|\theta_{n,g}\|_{L^2(N)}\, dg \le Cn^c \left(\int_{G/N} \|\theta_{n,g}\|^2_{L^2(N)}\, dg \right)^{1/2}. \tag{2.6}$$

Combining (2.5) (2.6) and (2.3) Theorems 1 and 2 follow.

3. **The proof of the theorems.** In this section G, N, M, V, Σ will be as in §1 and M will be assumed compact. It will be convenient to reformulate the estimate (2.4) in probabilistic terms and make systematic use of probabilistic language.

Let $\mu \in \mathbb{P}(G)$ be some probability measure on G; we shall then consider the left-invariant random walk on G controlled by μ. More precisely we shall consider $\{Z_n \in G\ ;\ n \geq 0\}$ the G-valued Markov chain that is determined by $\mathbb{P}[Z_j \in A / Z_{j-1} = x] = \mu(x^{-1}A)$ for any $A \subset G$ and $j = 1, 2, \ldots$. We shall denote then by $\mathbb{P}(\cdot) = \mathbb{P}_e(\cdot) = \mathbb{P}(\cdot / Z_0 = e)$; clearly then $\mathbb{P}[Z_n \in A] = \mu^{*n}(A) = \mu_n(A)$ where we use the notation of the previous paragraph. It will also be convenient to write $Z_n = \gamma_1\gamma_2\cdots\gamma_n$ ($\gamma_j \in G$) so that under the probability $\mathbb{P}$ $\{\gamma_j \in G\ ;\ j = 1, \ldots\}$ is a sequence of G-valued independent variables each with common distribution μ on G. We can also write $Z_n = \dot{Z}_n\Lambda_n$ ($n \geq 1$) with $\dot{Z}_n \in \Sigma \cdot M$, $\Lambda_n \in N$ where we use the section Σ, the Levi subgroup, and the notations of §1. The estimate (2.4) where we take for $S = \Sigma \cdot M$ in §2 is then clearly equivalent with the assertion that there exists $c > 0$ large enough such that:

$$\mathbb{P}[|\dot{Z}_s|_{G/N} \leq cs^c\ ;\ |\Lambda_s|_N \leq cs^c] \geq c^{-1}s^{-c}\ ; \quad s \geq 1. \tag{3.1}$$

To prove this estimate we shall define three sequences of events (for $s = 1, 2, \ldots$):

$$A_s = \{|\gamma_j|_G \leq C \log s\ ;\ 1 \leq j \leq s\} \tag{3.2}$$

$$B_s = \{|\dot{Z}_s|_{G/N} \leq Cs^c\}. \tag{3.3}$$

To define the third sequence of events we write: $\dot{\gamma}_j = (X_j, m_j) \in V \times M = G/N$ so that in terms of our section $\Sigma \cdot M$ we have $\dot{\gamma}_j = \sigma(X_j)m_j \in \Sigma \cdot M \subset G$. We shall then use the $L_1, \ldots, L_n \in V^*$ (*cf.* §0) to define (for $s \geq 1$):

$$C_s = \{L_k(X_p + X_{p+1} + \cdots + X_s) \leq C\ ;\ 1 \leq p \leq s, 1 \leq k \leq n\}. \tag{3.4}$$

The constants $C, c > 0$ that appear in the definition of the above events are appropriately large and will be chosen later.

On the event A_s we have (*cf.* (1.12))

$$\gamma_j = \dot{\gamma}_j n_j\ ; \quad n_j \in N,\ |n_j|_N \leq C\exp(c \log s) \leq Cs^C\ ; \quad 1 \leq j \leq s. \tag{3.5}$$

With our previous notation on the other hand we have:

$$\dot{\gamma}_1 n_1 \dot{\gamma}_2 n_2 \cdots \dot{\gamma}_s n_s = \dot{Z}_s\Lambda_s.$$

By (1.11) therefore we see that on the event $A_s \cap C_s$ we have $|\Lambda_s|_N \leq Cs^C$. Our estimate (3.1) and therefore equivalently (2.4) is thus a consequence of the following estimate:

$$\mathbb{P}[A_s \cap B_s \cap C_s] \geq Cs^{-C}\ ; \quad s \geq 1. \tag{3.6}$$

Observe that up to now the only property of the measure $\mu \in \mathbb{P}(G)$ that we have used (in §2) is the symmetry of that measure (*i.e.* $d\mu(x) = d\mu(x^{-1})$). It is for the proof of the estimate (3.6) that we shall need to impose additional conditions on μ. We shall first

prove Theorem 1; for this we need to prove estimate (3.6) when $d\mu(g) = \phi_1(g)\, d^r g$ where $\phi_1(g)$ is the left diffusion kernel of $e^{-\Delta}$. In this case the variables X_j $(j \geq 1)$ above are equidistributed, centered, independent, *non degenerate* normal variables. Indeed, to obtain the density of X_j one can project the diffusion generated by Δ on G by the mappings $G \longrightarrow G/N \cong M \times V \longrightarrow V$. It follows that the density of X_j is the density of the diffusion kernel of $e^{-\Delta_V}$ on V where Δ_V is a second order constant coefficient self adjoint subelliptic operator. Δ_V is therefore elliptic and by coordinate change becomes the standard Laplacian.

The proof of the estimate (3.6) in that case relies on the following:

LEMMA 3.1. *Let $X_1, X_2, \ldots, \in V$ be independent, centered, identically distributed, nondegenerate normal variables and let C_s $(s \geq 1)$ be defined as in (3.4) where the $L_1, \ldots, L_k$ satisfy the condition (NC) of §0. Then there exists $C > 0$, independent of $s \geq 1$ such that $\mathbb{P}(C_s) \geq s^{-C}$ $(s \geq 2)$.*

The proof of this lemma is not trivial and will be given in the next paragraph. Given this lemma the estimate (3.6) is a consequence of the following two estimates that are valid for $s \geq 1$ ($\sim$ stands for "complement"):

$$\mathbb{P}(\sim A_s) \leq s\mathbb{P}[|\gamma_1| \geq C_1 \log s] \leq C \exp\left(-c(\log s)^2\right); \tag{3.7}$$

$$\mathbb{P}(\sim B_s) \leq C\mathbb{P}[|X_1 + \cdots + X_s| \geq Cs^c] \leq C \exp(-Cs^{2c-1}) \tag{3.8}$$

where the $c > 0$ in (3.8) is the same c as in the definition of B_s, *cf.* (3.3), and for the estimate (3.8) to hold we must set $c > 1/2$. The left hand inequality of (3.8) holds because of what was said at the end of §1. The first inequality of (3.7) comes from independence and the second from the standard (but nontrivial) Gaussian estimate of $\phi_1(g)$ (*cf.* [1], [2], [8]).

The proof of Theorem 1 is now complete. Indeed, what has just been shown and (2.3) proves (0.1) for $t = 2n$, $n = 1, 2, \ldots$. The standard parabolic local Harnack estimate that the function $u(t, g) = \phi_t(g)$ satisfies for g in some neighbourhood of e (*cf.* [1], [2]) completes the proof for the other values of t.

Our next task is to prove Theorem 2. For this we need the estimate (3.6) in the case when $d\mu(g) = \varphi(g)\, dg$ where $\varphi(g) \in C_0^\infty(G)$ is a compactly supported continuous function. In this case the variables X_j involved in (3.6) have distribution $\mathbb{P}[X_j \in dx] = d\nu(x)$ where as before $\nu \in \mathbb{P}(V)$ is obtained from μ by projecting through the two mappings $G \longrightarrow G/N = M \times V \longrightarrow V$. Clearly ν is symmetric and has a continuous compactly supported density. We also have:

LEMMA 3.2. *Let $X_1, \ldots, X_n \cdots \in V$ be independent identically distributed variables with a common distribution $\nu \in \mathbb{P}(V)$ that satisfies the above conditions. Let further C_s $(s \geq 1)$ be defined as in (3.4) where the $L_1, \ldots, L_k$ satisfy the condition (NC) of §0. Then there exists $C > 0$ independent of $s \geq 1$ such that $\mathbb{P}(C_s) \geq s^{-C}$ $(s \geq 2)$.*

The proof of this lemma will, once more, be given in the next section. The proof of (3.6) is now easy. Indeed it suffices to prove the analogue of (3.7) and (3.8). The analogue

of (3.7) is now trivial because of the compactness of the support of μ. The analogue of (3.8) is less trivial but is an immediate consequence of the classical Bernstein inequality (*cf.* [14]) provided that $1/2 < c < 1$.

We obtain therefore, as before, that

$$\varphi_{2n}(e) \geq cn^{-C}\ ; \quad n = 1, 2, \ldots. \tag{3.9}$$

To deduce the same result for odd values of the parameter, the following "discrete Harnack" estimate could be used. Let $\sigma = \mu^{*2} = \psi(g)\,dg$. Then there exists a neighbourhood Ω of e and ε_0 such that $\psi(g) > \varepsilon_0$ $(g \in \Omega)$. Therefore it follows that if we use the notation $\sigma^{*n} = \psi_n(g)\,dg$ then $\psi_2(g) \geq \varepsilon_0 > 0$ for $g \in \operatorname{supp}\sigma$, and therefore $\psi_1(g) \leq C\psi_2(h)$, $g \in G$, $h \in \Omega.\operatorname{supp}\sigma$, a neighbourhood of $\operatorname{supp}\sigma$. From this it follows that there is a neighbourhood Ω of e such that

$$\psi_1(g) \leq C\psi_2(h)\ ; \quad g, h \in G,\ g^{-1}h \in \Omega.$$

But then with the same C we have:

$$\psi_n(g) \leq C\psi_{n+1}(h)\ ; \quad g, h \in G,\ g^{-1}h \in \Omega,\ n \geq 1.$$

If we iterate this result a number of times and use (3.9), we conclude that for any compact set $K \subset G$, and $n \geq 1$ large enough, we have $\varphi_{2n}(x) \geq cn^{-C}$ $(x \in K)$. The estimate (0.4) for *every* value of n (odd or even) follows immediately from this.

4. **The condition (NC) and potential theory.** This section is independent from the rest of the paper and has nothing to do with Lie groups. Let $V \cong \mathbb{R}^{d+1}$ be a real vector space and let $\mathcal{L} = (L_1, \ldots, L_k) \subset V^*$ be a finite set of (real) linear functionals. We shall say that the above set of linear functionals satisfies the condition (NC) if none of them is 0 and if $0_{V^*} \notin$ convex hull of $\mathcal{L}$ (the condition (NC) holds in particular if $\mathcal{L} = \emptyset$). We shall now associate to any set $\mathcal{L} \subset V^* \setminus \{0\}$ as above, whether it verifies (NC) or not, and to any $\alpha \geq 0$ a set:

$$W = W(\mathcal{L}; \alpha) = \{x \in V\ ;\ \mathcal{L}_j(x) < \alpha\ ;\ 1 \leq j \leq k\} \subset V.$$

For any $0 \neq x_0 \in V$ and $0 < \varphi_0 \leq \pi/2$, $a \geq 0$, I shall also denote by

$$C(x_0\ ;\ \varphi_0, a) = \{x \in V / x + ax_0 \neq 0\ ;\ \operatorname{Angle}(x_0, x + ax_0) < \varphi_0\}.$$

This is of course an open conical region with vertex at $-ax_0$, whose axis lies along x_0. We have, clearly, that $0 \in C(x_0, \varphi_0, a)$ if $a > 0$ and we also have:

LEMMA 4.1. *The $\mathcal{L} \subset V^* \setminus \{0\}$ satisfies the condition (NC) if and only if there exists $0 \neq x_0 \in V$ and $0 < \varphi_0 \leq \pi/2$ such that for all $\alpha > 0$ there exists $a > 0$ $W(\mathcal{L}\ ;\ \alpha) \supset C(x_0\ ;\ \varphi_0, a)$.*

Indeed (NC) is verified if and only if:

$$(\Sigma \alpha_j L_j = 0\ ;\ \alpha_j \geq 0,\ 1 \leq j \leq k) \Rightarrow (\alpha_j = 0,\ 1 \leq j \leq k).$$

Let $C(\mathcal{L})$ denote the convex cone generated by $\mathcal{L}$. The implication above holds if and only if the conditions $x, y \in C(\mathcal{L})$, $x + y = 0$ together imply that $x = y = 0$. A moments reflexion shows that this last statement is equivalent to the fact that convex cone$(\mathcal{L}) \subset C(x_0^* ; \varphi_1, 0) \subset V^*$ for some $0 \neq x_0^* \in V^*$, $0 \leq \varphi_1 < \pi/2$ and is therefore also equivalent to the fact that $W(\mathcal{L}, 0)$ (which is just the dual cone of $C(\mathcal{L})$) satisfies $W(\mathcal{L}, 0) \supset C(x_0, \pi/2 - \varphi_1, 0)$ for some $0 \neq x_0 \in V$. Our lemma is now evident.

I shall now denote by $b(t) = \big(b_1(t), \ldots, b_n(t)\big) \in V = \mathbb{R}^m$ $(t > 0 \ ; \ b(0) = 0)$ the standard Brownian motion. We shall need the following:

LEMMA 4.2. *(i) Let $\mathcal{L} \subset V^* \setminus \{0\}$ and let us assume that it satisfies the condition (NC) then for every $\alpha > 0$ there exists $C > 0$ s.t.*

$$\mathbb{P}[b(t) \in W(\mathcal{L} ; \alpha) \ ; \ 0 < t < T] \geq C^{-1} T^{-C} \ ; \quad T \geq 1. \tag{4.1}$$

(ii) Let $\mathcal{L} \subset V^* \setminus \{0\}$ satisfy the condition (C) (i.e. it fails to satisfy the condition (NC)). Then for every $a > 0$ there exists a $C > 0$ s.t.

$$\begin{aligned} C \exp(-C^{-1} T^{1/3}) &\geq \mathbb{P}[b(t) \in W(\mathcal{L} ; aT^{1/3}) \ ; \ 0 < t < T] \\ &\geq C^{-1} \exp(-CT^{1/3}) \ ; \quad T \geq 1. \end{aligned} \tag{4.2}$$

Only part (i) will be essential in this paper and I shall presently give the proof. The left hand side (upper) estimate of (4.2) of part (ii) is what was used in [8]. The proof of the right hand side of (4.2) is contained in the well-known estimate:

$$\mathbb{P}[|b_1(t)| \leq \alpha \ ; \ 0 < t < T] \geq C \exp\left(-C \frac{T}{\alpha^2}\right)$$

(*cf.* [15] for an elementary proof). The proof of part (i) of this lemma is a very easy consequence of the following:

LEMMA 4.3. *For every $0 < \varphi_0 < \pi/2$ and every $0 \neq x_0 \in V$ there exists $u \geq 0$ continuous and non negative on the closure $C(x_0 \ ; \ \varphi_0, 0)$ that is subharmonic and not identically zero on $C(x_0 \ ; \ \varphi_0, 0)$. Furthermore u vanishes on the boundary of $C(x_0, \varphi_0, 0)$ and satisfies the estimate*

$$|u(x)| = 0(|x|^A) \quad (x \longrightarrow \infty). \tag{4.3}$$

for some $A > 0$.

If we are prepared to use the general theory, we can even guarantee that u is harmonic in $C(x_0, \varphi_0, 0)$ and to prove that such a u is essentially unique. I shall presently give, however, an elementary direct proof of the above lemma which is closer to the ideas that are needed to deal with the non-Gaussian case and with Lemma 3.2.

The way to deduce Lemma 4.2(i) from Lemma 4.3 is straightforward. Indeed let τ be the exit time of $b(t)$ from $C(x_0, \varphi_0, a)$ for some positive $a > 0$ and $0 < \varphi_0 < \pi/2$, and

let u be as in Lemma 4.3 in $C(x_0, \varphi_0, a)$ (*i.e.* we translate to bring 0 to a). It follows that $u\big(b(t \wedge \tau)\big)$ is a (Brownian) submartingale and therefore:

$$u(x) \leq \mathbf{E}_x u\big(b(t \wedge \tau)\big) \; ; \quad t > 0 \;\; x \in C(x_0, \varphi_0, a).$$

If we choose x such that $u(x) \neq 0$, we obtain by Hölder's inequality:

$$0 < u(x) \leq \mathbf{E}_x\big[I(\tau > t) u\big(b(t)\big)\big] \leq (\mathbb{P}[\tau > t])^{1/2} \Big\{\mathbf{E}\Big(u\big(b(t)\big)\Big)^2\Big\}^{1/2} \leq C t^A (\mathbb{P}[\tau > t])^{1/2}$$

because of (4.3). Lemma 4.2 follows from that estimate. Indeed if we use the Markov property we can pass from starting probability at zero $\mathbb{P}_0$ to any other starting probability $\mathbb{P}_x$. Lemma 3.1 follows by giving the time parameter $t = 1, 2, \ldots$ integer values.

To give the proof of Lemma 4.3 we introduce polar coordinates on $\mathbb{R}^{d+1}$ with $r = |x|$, $x \in \mathbb{R}^{d+1}$ and assume that x_0 is pointing towards the north pole of the unit sphere S^d. The coordinates on S^d are $(\varphi, \theta_1, \ldots, \theta_{d-1})$ where φ is the colatitude (*i.e.* angle with the north pole) and $0 \leq \theta_i \leq 2\pi$ $(1 \leq i \leq d-1)$. With these coordinates our region can be expressed as

$$C(x_0, \varphi_0, 0) = [-\varphi_0 < \varphi < \varphi_0].$$

Using the well known properties of zonal harmonics that can be expressed in terms of ultraspherical (or Gegenbauer) polynomials (*cf.* [16]), and then the standard results on the zeros of these polynomials (*cf.* [17]), we see that for every $k \geq 1$ sufficiently large we can find $U(x)$ a homogeneous harmonic polynomial on $\mathbb{R}^{d+1}$ of degree k that is independent of θ_i $(1 \leq i \leq d-1)$ and has the form:

$$U(x) = r^k U_k(\varphi) \; ; \quad 0 \leq \varphi \leq \pi \; ; \tag{4.4}$$

we can further demand that the function $U_k(\varphi)$ is negative for $\varphi \in]\varphi_1, \varphi_2[$, is positive for $\varphi \in]\varphi_2, \varphi_3[$, and is negative again for $\varphi \in]\varphi_3, \varphi_4[$. Here we assume that $0 < \varphi_1 < \varphi_2 < \varphi_3 < \varphi_4 \leq \varphi_0$. It is clear then that the function

$$u(x) = U(x) \quad \varphi \in [\varphi_2, \varphi_3] \; ; \quad u(x) = 0 \quad \varphi \notin [\varphi_2, \varphi_3]$$

satisfies all the conditions of Lemma 4.3.

I shall now generalise the above considerations in the setting of discrete potential theory. Let $\mu \in \mathbb{P}(\mathbb{R}^{d+1})$ be a symmetric probability measure on $\mathbb{R}^{d+1}$ let us denote by

$$\tilde{\Delta} = \delta - \mu \; ;$$

and let us assume that

$$\alpha = \sup\{|x| \; ; x \in \operatorname{supp} \mu\} < +\infty.$$

For any open set $\Omega \subset \mathbb{R}^{d+1}$ we shall say that u is μ-subharmonic on Ω if u is upper semicontinuous on Ω and if

$$\tilde{\Delta} u f(x) \leq 0 \; ; \quad \forall x \in \Omega^\alpha = \{x \in \Omega \quad d(x, \sim \Omega) > \alpha\}.$$

https://doi.org/10.4153/CJM-1994-061-6 Published online by Cambridge University Press

The interest of the above definition lies in the following probabilistic interpretation:

Let $(Z_n \in V)$ be the Markov chain induced by the random walk $X_1 + X_2 + \cdots$ where the X_i's are equidistributed independent variables with probability distribution $\mathbb{P}[X_i \in dx] = d\mu(x)$, and let $\tau = \inf\{n/Z_n \notin \tilde{\Omega}\}$ where $\tilde{\Omega} \subset \Omega^\alpha$ is arbitrary. Then the process $u_n = u(Z_{\tau\wedge n})$ is a submartingale for any starting probability $\mathbb{P}[Z_0 = x] = 1$ $(x \in \tilde{\Omega})$.

The proof is easy: We denote by $\mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots \subset \mathcal{F}_n \subset \cdots$ the fields induced by the Markov chain ($\mathcal{F}_n = \mathcal{F}(Z_1, \ldots, Z_n)$) and we clearly have:

$$\mathbf{E}[u_n / \mathcal{F}_{n-1}] = \sum_{m=1}^{n-1} u(Z_m) I(\tau = m) + \mathbf{E}\big(u(Z_n) I(\tau \geq n) / \mathcal{F}_{n-1}\big).$$

The conditional expectation on the right can be rewritten:

$$\mathbf{E}[u(Z_{n-1} + X_n) I(Z_{n-1} \in \tilde{\Omega}) I(\tau \geq n) / \mathcal{F}_{n-1}] = E_n$$

and the μ-subharmonicity of u implies that:

$$E_n \geq u(Z_{n-1}) I(\tau \geq n) = u(Z_{\tau\wedge n-1}) I(\tau \geq n)$$

because $[\tau \geq n] \in \mathcal{F}_{n-1}$.

We shall now explain the strategy of the proof of Lemma 3.2.:

With fixed $0 < \varphi_0 < \pi/2$ and x_0 pointing towards the north pole of S^d (as in the proof of Lemma 4.3) we shall find $\tilde{u}$ a function on $C(x_0, \varphi_0, 0)$ that is continuous up to the boundary of $C(x_0, \varphi_0, 0)$ and satisfies $u(x) = 0(|x|^C)$ at infinity for some $C > 0$ and which also satisfies the following conditions: first of all $\tilde{u}$ is μ-subharmonic in

$$\Omega_0 = C(x_0, \varphi_0, 0) \cap [|x| > C_0]$$

for some $C_0 > 0$. Denote $\{x \in C(x_0, \varphi_0, 0)\ ;\ \tilde{u}(x) > 0\}$ by Ω. Then there exist $C_1 \geq C_0$ and $\tilde{\Omega}$ some connected component of $\Omega_1 = \Omega \cap [|x| > C_1]$ such that $\sup_{\omega\in\tilde{\Omega}} \tilde{u}(\omega) = +\infty$ and such that:

$$d(\tilde{\Omega}\ ;\ \sim \Omega_0) > \alpha\ ; \quad d(\tilde{\Omega}\ ;\ \Omega_1 \setminus \tilde{\Omega}) > \alpha. \tag{4.5}$$

Let then $\tau = \inf\{n/Z_n \notin \tilde{\Omega}\}$. The conditions (4.5) imply then that there exists $C_2 > 0$ s.t. $\tilde{u}(Z_\tau) \leq C_2$. In fact the only reason whey we cannot take $C_2 = 0$ is that the first jump out of $\tilde{\Omega}$ may take place at $|Z_\tau| \leq C_1$. For any $x \in \tilde{\Omega}$ for which $\tilde{u}(x) > C_2$ the above submartingale property implies that

$$0 < \tilde{u}(x) \leq \mathbf{E}_x[\tilde{u}(Z_{t\wedge n})] = \mathbf{E}[\tilde{u}(Z_n) I(\tau > n)] + \mathbf{E}[\tilde{u}(Z_\tau) I(\tau \leq n)] \leq \mathbf{E}[\tilde{u}(Z_n) I(\tau \geq n)] + C_2.$$

The same argument as in the proof of Lemma 4.2(i) finishes then the proof of Lemma 3.2.

What remains to be done is to construct the above function $\tilde{u}$ that has the required properties. To be able to make that construction we shall have to assume that the quadratic form

$$\Sigma q_{ij}\lambda_i\lambda_j = \int_{\mathbb{R}^{d+1}} \Big(\sum_{i=1}^{d+1} \lambda_i x_i\Big)^2 d\mu(x)\ ; \quad \lambda \in \mathbb{R}^{d+1}$$

https://doi.org/10.4153/CJM-1994-061-6 Published online by Cambridge University Press

is nonsingular. This condition is of course satisfied in our case because the density of the variables X_i is continuous. By a linear change of variables we see that we may then assume that $(q_{ij}) = I = (\delta_{ij})$ is the identity matrix. Using a Taylor development, we then see that the corresponding Laplacian $\delta - \mu = \tilde{\Delta}$ satisfies:

$$|(\Delta - \tilde{\Delta})f(x)| \leq C \sup_{|x-y|\leq\alpha} |f'''(y)| \; ; \quad f \in C^\infty \tag{4.6}$$

where $\Delta = -\Sigma \frac{\partial^2}{\partial x_i^2}$ is the euclidean Laplacian.

Let now $U(x)$ and $U_k(\varphi)$ be as in (4.4) with k large enough and satisfying the same sign changes that where imposed there; φ_i $(i = 1, 2, 3, 4)$ have here the same meaning as in the few lines that follows (4.4). It is then clear from (4.6) that $\tilde{\Delta}U(x) \leq C|x|^{k-3}$. Direct computation and (4.6) on the other hand show that, for $k \geq 1$ large enough, there exists $C, c > 0$ such that $\tilde{\Delta}r^k \leq -cr^{k-2}$ for $|x| = r > C$. It follows that for k and $C_0 > 0$ large enough the function:

$$\tilde{u}(x) = U(x) + C_0 r^{k-1}$$

is μ-subharmonic in the region

$$\Omega_0 = C(x_0, \varphi_0, 0) \cap [|x| > C_0].$$

The above function has all the other required properties. First of all, its polynomial growth at infinity is evident. Let next $\varphi_2 < \varphi' < \varphi_3$ and let $x' \in \mathbb{R}^{d+1}$ lie on a ray from the origin that has colatitude φ'. Then $\tilde{u}(x') = |x'|^k u(\varphi') + C_0|x'|^{k-1}$ which tends to ∞ as $|x'| \longrightarrow \infty$. Fix such an x' for which $\tilde{u}(\lambda x') > 0$ $(\forall \lambda \geq 1)$ and let Ω' be the connected component of x' in Ω. The set $\tilde{\Omega} = \Omega' \cap [|x| > C_1]$ for C_1 large enough satisfies the required conditions (4.6). The last verification, if a trifle tedious to write down, is entirely elementary and can best be done by drawing a picture. What is essential in the above verification is that if $|\bar{x}| \longrightarrow \infty$ with fixed colatitude $\bar{\varphi}$ such that $u(\bar{\varphi}) \neq 0$, then the correcting term $C_0|\bar{x}|^{k-1}$ is negligible compared with the principal term $|\bar{x}|^k u(\bar{\varphi})$. The details will be left to the reader.

5. **The exponential lower bound.** In this section I shall explain the modifications that one can make to the proofs §2 and §3 to obtain a proof of the lower exponential estimate (0.3). This estimate is due to G. Alexopoulos (*cf.* [9], [10]). I shall explain these modifications in the context of continuous time diffusion in the spirit of Theorem 1. A similar proof in the spirit of Theorem 2, can also be given for the convolution powers μ^{*n} of an appropriate measure.

We are now working on a general simply connected Lie group G, as we did throughout in this paper, but we impose now *no* conditions on the real parts of the roots $L_1, \ldots, L_n \in V^*$ (in other words the condition (NC) is not assumed to hold). Everything in §2 is as before except that now instead of the estimate (2.4) the estimate that we shall have to prove is:

$$\int_{g\in G/N, |g|\leq cn^c} \left(\int_{|x|\leq c\exp(cn^{1/3})} \theta_{n,g}(x)\, dx \right) \geq c^{-1} \exp(-cn^{1/3}). \tag{5.1}$$

The modifications in (2.5) and (2.6) are then obvious and (0.3) follows. The modifications needed in §3 to give the proof of (5.1) are rather obvious. Indeed (3.1) becomes

$$\mathbb{P}[|\dot{Z}_s|_{G/N} \leq cs^c \; ; \; |\Lambda_s| \leq c\exp(cs^{1/3})] \geq c^{-1}\exp(-cs^{1/3}) \; ; \quad s \geq 1. \tag{5.2}$$

The definition of A_s in (3.2) has to be modified to:

$$A'_s = \{|\gamma_j|_G \leq C_1 s^{1/3} \; ; \; 1 \leq j \leq s\}.$$

The definition of B_s is as in (3.3), but it is important now that the c in (3.3) is $c > 2/3$. The definition of C_s in (3.4) has to be modified

$$C'_s = \{|L_k(X_p + X_{p+1} + \cdots + X_s)| \leq C_2 s^{1/3} \; ; \; 1 \leq p \leq s, 1 \leq k \leq n\}.$$

The $C_1, C_2 > 0$ and $c > 0$ have to be chosen again at the end.

By §3 it is then clear that on the event $A'_s \cap C'_s$ we have $|n_j|_N \leq C\exp(Cs^{1/3})$ $(1 \leq j \leq s)$ and therefore also $|\Lambda_s|_N \leq C\exp(Cs^{1/3})$. Therefore instead of (3.6) what we now have to prove is:

$$\mathbb{P}[A'_s \cap B_s \cap C'_s] \geq c\exp(-cs^{1/3}) \; ; \quad s \geq 1. \tag{5.3}$$

Instead of Lemma 3.1, which is a consequence of Lemma 4.2(i), what we now have to use for the proof of (5.3) is the lower estimate of Lemma 4.2(ii), which, incidentally, is much easier to prove.

With the above indications the reader can fill in the details, I am sure.

References

1. N. Th. Varopoulos, *Analysis on Lie groups*, J. Funct. Anal. (2) **76**(1988), 346–410.
2. N. Th. Varopoulos, L. Saloff-Coste and T. Coulhon, *Analysis and geometry on groups*, Cambridge Univ. Press, 1992.
3. L. Hörmander, *Hypoelliptic second order operators*, Acta Math. **119**(1967), 147–171.
4. V. S. Varadarajan, *Lie groups, Lie algebras and their representations*, Prentice-Hall, 1984.
5. N. Jacobson, *Lie algebras*, Interscience, 1962.
6. C. Chevalley, *Théorie de groupes de Lie, tome III*, Hermann, 1955.
7. H. Reiter, *Classical harmonic analysis and locally compact groups*, Oxford, Math. Monograph, 1968.
8. N. Th. Varopoulos, *Diffusion on Lie groups*, Canad. J. Math. (2) **46**(1994), 438–448.
9. G. Alexopoulos, *Fonctions harmoniques bornées sur les groupes résolubles*, C. R. Acad. Sci. Paris **305** (1987), 777–779.
10. ———, *A lower estimate for central probability on polycyclic group*, Canad. J. Math. (5) **44**(1992), 897–910.
11. W. Hebisch, *On heat kernels on Lie groups*, preprint.
12. Y. Guivarc'h, *Croissance polynômiale et périodes des fonctions harmoniques*, Bull. Soc. Math. France **101**(1973), 333–379.
13. G. Alexopoulos, *An application of homogenization theory to harmonic analysis: Harnack inequalities and Riesz transforms on Lie groups of polynomial growth*, Canad. J. Math. (4) **44**(1992), 691–727.
14. I. A. Ibragimov and Yu. V. Linnik, *Independent and stationary sequences of random variables*, Wolters-Noordhoff, 1971.
15. N. Th. Varopoulos, *A potential theoretic property of soluble groups*, Bull. Sci. Math. (2) **108**(1983), 263–273.

16. E. M. Stein and G. Weiss, *Introduction to Fourier analysis on Euclidean spaces*, Princeton Univ. Press, 1971.
17. G. Szegö, *Orthogonal polynomials*, Amer. Math. Soc. Colloq. Publ. **XXIII**, 1939.
18. L. Hörmander, *Estimates for translation invariant operators in L^p spaces*, Acta Math. **104**(1960), 93–139.
19. N. Th. Varopoulos, *Sobolev inequalities on Lie groups and symmetric spaces*, J. Funct. Anal. **86**(1989), 19–40.
20. ———, *Théorie de Hardy-Littlewood sur les groupes de Lie*, C. R. Acad. Sci. Paris Ser. I **316**(1993), 999–1003.

Université de Paris VI
4 Place Jussieu
75005 Paris
France