

ON RAPID MIXING FOR RANDOM WALKS ON NILMANIFOLDS.

DMITRY DOLGOPYAT, SPENCER DURHAM, AND MINSUNG KIM

ABSTRACT. We prove rapid mixing for almost all random walks generated by m translations on an arbitrary nilmanifold under mild assumptions on the size of m . For several classical classes of nilmanifolds, we show $m = 2$ suffices. This provides a partial answer to the question raised in [6] about the prevalence of rapid mixing for random walks on homogeneous spaces.

1. INTRODUCTION

Let G be a simply connected nilpotent Lie group and Γ be a co-compact lattice so that $M = G/\Gamma$ is a nilmanifold equipped with the Haar measure μ . A translation on M by $g \in G$ is the map $x\Gamma \mapsto gx\Gamma$. In this paper, we study random walks by a finite set of translations on M . These random walks will be defined by an $m \in \mathbb{N}$, $x \in M$, a set $F := \{g_1, \dots, g_m\} \subset G$, and an associated probability vector $\vec{p} = (p_1, p_2, \dots, p_m)$, i.e. $p_i > 0$ and $\sum p_i = 1$. The random walk is then a Markov chain where $x_n = g_k x_{n-1}$ with the probability p_k . We will let $\langle F \rangle$ denote the semigroup generated by the set F . Associated to the set F , we have an operator $\mathcal{L} : C^r(M) \rightarrow C^r(M)$ defined by

$$\mathcal{L}(A)(x) := \mathbb{E}(A(x_1)|x_0 = x) = \sum_{j=1}^m p_j A(g_j \cdot x), \quad A \in C^r(M).$$

It follows that for any $N > 1$,

$$(\mathcal{L}^N A)(x) = \mathbb{E}_x(A(x_N)) = \sum_{|W|=N} p_N(W) A(Wx),$$

where $|W|$ is the length of the word W and $p_N(W) = p_N(g_{w_N} \dots g_{w_1}) = \prod_{i=1}^N p_{w_i}$ is the probability of having walked by W at time N . Since a random walk is exactly defined by its generators, we can view the product μ^m as a measure on the space of all random walks generated by m translations. When we speak of the measure of a set of walks, we mean it with respect to this measure.

Given observables $A, B \in C^r(M)$, the correlation of A and B after time N is given by

$$\bar{\rho}_{A,B}(N) = \int (\mathcal{L}^N A)(x) B(x) d\mu(x) - \int A(x) d\mu(x) \int B(x) d\mu(x).$$

Definition 1.1. A random walk is said to be *rapid mixing* if given $q \in \mathbb{N}$, there are constants $C, r > 0$ such that for any $A, B \in C^r(M)$ and $N \in \mathbb{N}$,

$$|\bar{\rho}_{A,B}(N)| \leq C \|A\|_{C^r(M)} \|B\|_{C^r(M)} N^{-q}.$$

Below, in order to simplify the formulas, we only consider correlations of zero mean functions. This is sufficient since every function can be decomposed as a sum of a zero mean function and a constant (the mean).

Mixing plays a key role in the study of statistical properties of dynamical systems. Many classical systems are exponentially mixing (see e.g. [7, Appendix A]). The random walks we consider do not exhibit exponential mixing, so the best estimate we can hope

for is that the mixing of C^r observables occurs at a $O(N^{-q(r)})$ rate with $q(r) \rightarrow \infty$ as $r \rightarrow \infty$. This is exactly the definition of rapid mixing that we have provided. Our main result shows that most sufficiently rich walks are indeed rapid mixing. Rapid mixing is also sufficient to establish several key statistical properties, including the Central Limit Theorem, see Appendix B.

Nilmanifolds support a rich and well-studied variety of homogeneous dynamical systems. These systems, in addition to being of purely dynamical interest, are also of interest to the broader mathematical community as their dynamical properties can have important consequences in other fields, particularly number theory [10, 13] and combinatorics [14]. In part due to the complexity of their algebraic structures, dynamics on higher-dimensional nilmanifolds are not yet completely understood. In this paper, we prove the rapid mixing of almost all random walks on nilmanifolds generated by a sufficiently large (finite) number of group elements. In particular, we will define a technical algebraic condition called *m-greatness* and show that almost any random walk on an *m-great* nilmanifold supported on *m* translations is rapid mixing. We then show that every step-*s* nilmanifold is *s-great*. This leads to the following theorem which applies to all nilmanifolds.

Theorem A. For any step-*s* nilmanifold $M = G/\Gamma$, there is a constant $N_G \leq s$ such that for $m \geq N_G$, almost every random walk generated by *m* translations is rapid mixing.

The primary weakness of this theorem is that it sometimes requires more than two generators to guarantee that rapid mixing random walks are of full measure. Within certain special classes of nilmanifolds, we can overcome this deficiency. Among these are the *quasi-abelian* nilmanifolds, which have previously been studied in the context of parabolic flow dynamics [12, 19]. We also give special attention to triangular nilmanifolds and step-3 nilmanifolds, and ultimately show the following theorem.

Theorem B. If G is quasi-abelian, triangular, or step-3 or lower, then $N_G = 2$.

It is a classical theorem that for single translations on a nilmanifold, ergodicity, unique ergodicity, and minimality are equivalent and in fact only depend on the irrationality of the abelian projection of the translation. Our result is similar in that we only need an arithmetic property on the restriction of the action in the maximal torus factor. On the other hand, unlike other cases, the arithmetic property we require takes into account how higher-order commutators of the generators will act on M . In particular, the argument requires certain polynomials arising from the Lie algebra structure to be linearly independent. In fact, the relevant polynomials only depend on the coordinates of the generators in the abelianization of G , and the full measure set of rapid mixing walks we find corresponds to a full measure set of abelian parts that act Diophantinely in some sense (see Definition 3.3). It follows that Theorem A could be strengthened to say that any *m*-tuples in G that project into the aforementioned full measure set of abelian parts generate rapid mixing walks.

A rapid mixing random walk on M also satisfies the Central Limit Theorem (see Appendix B). Several results on central and local limit theorems on nilpotent Lie groups were recently obtained in [2, 3, 5, 15].

We now describe the structure of the paper. Section 2 contains preliminaries on nilpotent Lie groups, Lie algebras, and nilmanifolds. In Section 3, we define *m-greatness* as well as a relevant Diophantine property. We show that the Diophantine property implies rapid mixing (Proposition 3.7). Then, modulo a claim that connects *m-greatness*

to the Diophantine property (Proposition 3.4), we show that a full measure set of m -tuples on an m -great nilmanifold generate rapidly mixing walks. In Section 4, we show Proposition 3.4 by constructing words that act Diophantinely on appropriate tori. In Section 5, we establish that the groups listed in Theorem B are 2-great implying Theorem B. We also show Proposition 5.5 which states that any step s -nilmanifold is s -great, proving Theorem A. Finally, we provide an example of a Lie algebra that is not 2-great, showing that our technique is not sufficient to show the suspected optimal result that $N_G=2$ for all nilpotent groups.

Acknowledgement. The authors appreciate Adam Kanigowski for fruitful discussions and several suggestions for improving the quality of the initial draft. They are grateful to Bassam Fayad and Giovanni Forni for their careful readings and several comments on the draft. M.K. thanks Xuesen Na for his assistance in setting up a computer program for testing calculations.

D.D. was partially supported by the NSF grant DMS-2246983.

S.D. was partially supported by the NSF grant DMS-2101464.

M.K. was partially supported by UniCredit Bank R&D group through the ‘Dynamics and Information Theory Institute’ at the Scuola Normale Superiore, foundations for the Royal Swedish Academy of Sciences, and Carl Trygger’s Foundation for Scientific Research.

2. PRELIMINARIES ON NILMANIFOLDS

We provide a background of nilpotent Lie groups, Lie algebras and nilmanifolds. The material of this subsection is taken from [4, 18], and we also refer to [1] for additional information about general nilmanifolds.

2.1. Nilpotent Lie groups and Lie algebras. A real Lie algebra \mathfrak{g} is called *nilpotent* if the lower (descending) central series of \mathfrak{g} terminates i.e. the sequence defined by

$$(2.1) \quad \mathfrak{g} = \mathfrak{g}^{(0)} \supset \mathfrak{g}^{(1)} = [\mathfrak{g}, \mathfrak{g}] \supset \cdots \supset \mathfrak{g}^{(j)} = [\mathfrak{g}^{(j-1)}, \mathfrak{g}] \supset \cdots,$$

where $[\mathfrak{h}, \mathfrak{g}] = \{[X, Y] : X \in \mathfrak{h}, Y \in \mathfrak{g}\}$, eventually has $\mathfrak{g}^{(s)} = 0$ for some s . The *step* of \mathfrak{g} is the minimal number s that satisfies $\mathfrak{g}^{(s)} = 0$.

The lower central series of a Lie group G is defined by $G^{(0)} = G$ and $G^{(j+1)} = [G^{(j)}, G]$ where $[\cdot, \cdot]$ is the commutator bracket. A connected and simply connected Lie group G is called nilpotent if $G^{(s)}$ is equal to the trivial group for some s . A Lie group G is nilpotent if and only if its associated Lie algebra \mathfrak{g} is nilpotent. In fact, the lower central series of G and \mathfrak{g} are connected, as $G^{(j)} = \exp(\mathfrak{g}^{(j)})$.

Proposition 2.1. [4] *If G is a connected and simply connected nilpotent Lie group, then the exponential map $\exp : \mathfrak{g} \rightarrow G$ is a diffeomorphism.*

The product operation on G satisfies the Baker-Campbell-Hausdorff (BCH) formula

$$(2.2) \quad \exp(X) \exp(Y) = \exp \left(X + Y + \frac{1}{2}[X, Y] + \sum_{\alpha} c_{\alpha} X_{\alpha} \right),$$

where α is a finite (for nilpotent groups) set of labels, c_{α} are real constants, and X_{α} are iterated Lie brackets of X and Y (see [9]).

It will be convenient to denote $n_j = \dim(\mathfrak{g}^{(j)}) - \dim(\mathfrak{g}^{(j+1)})$ so that n_j is the dimension of the quotient algebra $\mathfrak{g}^{(j)}/\mathfrak{g}^{(j+1)}$ (or corresponding quotient group $G^{(j)}/G^{(j+1)}$). If $X, Y \in \mathfrak{g}$ satisfy $X - Y \in \mathfrak{g}^{(j)}$ we write that $X = Y \pmod{\mathfrak{g}^{(j)}}$.

Definition 2.2 (Malcev basis). A Malcev basis for \mathfrak{g} through the descending central series $\mathfrak{g}^{(j)}$ is a basis $X_1^{(0)}, \dots, X_{n_0}^{(0)}, \dots, X_1^{(s-1)}, \dots, X_{n_s}^{(s-1)}$ of \mathfrak{g} satisfying the following:

(1) if we set $E^j = \{X_1^{(j)}, \dots, X_{n_j}^{(j)}\}$, the elements of the set $E^j \cup E^{j+1} \cup \dots \cup E^s$ form a basis of $\mathfrak{g}^{(j)}$;

(2) if we drop the first l elements, the remaining elements span an ideal (of codimension l) of \mathfrak{g} .

If $\Gamma = \left\{ \exp \left(\sum_{j,k} m_{j,k} X_j^{(k)} \right) \right\}_{m_{j,k} \in \mathbb{Z}}$, then we say that the basis is *strongly based at*

Γ . The Lie algebra \mathfrak{g} of any nilmanifold G/Γ can be equipped with a Malcev basis strongly based at Γ . Moving forward, we will always use this basis when writing Lie algebra elements in coordinates. For convenience, we will denote by $X_i = X_i^{(0)}$. We observe that if $A \subseteq \mathbb{R}^{n_0}$, then

$$\mu(\{\alpha_{01}X_1 + \dots + \alpha_{0n_0}X_{n_0} + O(\mathfrak{g}_1) : (\alpha_{01}, \dots, \alpha_{0n_0}) \in A\}) = \mu(A),$$

i.e. for a set defined by the coefficients of the X_i , the measure of the set is exactly the Lebesgue measure of the permitted coefficients.

2.2. Nilmanifolds and Fibration. A compact *nilmanifold* is a quotient $M := G/\Gamma$ where G is a nilpotent group and Γ is a (co-compact) lattice of G . The lattice Γ exists if and only if G admits rational structural constants. We will consider the left action of G by translations on M . More precisely, for $g, h \in G$, set $g(h\Gamma) = (gh)\Gamma$. Every nilmanifold is a fiber bundle over a torus. The abelianization $G^{ab} = G/[G, G]$ is abelian, connected and simply connected, hence isomorphic to \mathbb{R}^n . Thus, there is a natural projection

$$(2.3) \quad p : G/\Gamma \rightarrow G^{ab}/\Gamma^{ab} \simeq \mathbb{T}^n.$$

For all $k \in \mathbb{N}_0$, the group $G^{(k+1)}$ is a closed normal subgroup of G , we have natural epimorphisms $\pi^{(k)} : G \rightarrow G/G^{(k+1)}$. Then, the group $G^{(k+1)} \cap \Gamma$ is a lattice of $G^{(k+1)}$. Moreover, $\Gamma_k := \pi^{(k)}(\Gamma)$ is a lattice in $N_k := G/G^{(k+1)}$ and

$$M^{(k)} := G/G^{(k+1)}\Gamma = N_k/\Gamma_k$$

is a nilmanifold. It follows that $\pi^{(k)} : M = G/\Gamma \rightarrow M^{(k)}$ is a fibration whose fibers are the orbits of $G^{(k+1)}$ on G/Γ , homeomorphic to the nilmanifolds $G^{(k+1)}/(G^{(k+1)} \cap \Gamma)$. We can also define $M_p := G^{(p)}/G^{(p+1)}\Gamma_p \simeq \mathbb{T}^{n_p}$.

2.3. Harmonic Analysis on Nilmanifolds. In this section, we wish to describe the structure of $L^2(M)$ for a nilmanifold M . To do this, we will need to describe the characters of M , denoted by \widehat{M} . For any Lie algebra \mathfrak{a} , let \mathfrak{a}^* represent its dual as a vector space. Since we have a basis for \mathfrak{g} (the Malcev basis), the coordinate functionals $X_1^{(1)*}, \dots, X_{n_{s-1}}^{(s-1)*}$ are well-defined and form a basis for \mathfrak{g}^* . Define $\pi_p : \mathfrak{g} \rightarrow \mathbb{R}^{n_p}$ by $\pi_p(V) = (X_1^{(p)*}(V), \dots, X_{n_p}^{(p)*}(V))$. Also, let $E_p^* = \{X_1^{(p)*}, \dots, X_{n_p}^{(p)*}\}$, and define Λ_p to be the set of integer linear combinations of elements of E_p^* .

Now, we will describe the structure of \widehat{M} . We say that χ is a character of level p if p is the largest integer such that χ is nontrivial on $G^{(p)}/(\Gamma \cap G^{(p)})$. Note that if χ is of level p , then χ is invariant under the action of $G^{(p+1)}$, so χ is naturally associated with a character on $M^{(p)}$. We will let $\widehat{M}^{(p)}$ denote the set of characters of level p on M . Note that $\widehat{M} - \{1_{triv}\} = \bigcup_{p=0}^{s-1} \widehat{M}^{(p)}$, where 1_{triv} here refers to the trivial character. We now wish to describe how characters of level p transform under translation by an element of

$G^{(p)}$. For any $\chi \in \widehat{M}^{(p)}$, χ has an associated nonzero functional $\lambda \in \Lambda_p$ such that for $g \in G^{(p)}$, $\chi(gx) = e^{2\pi i \lambda(\log(g))} \chi(x)$. As a slight abuse of notation, in this case, we will write $\chi = \chi_\lambda$ even though there are multiple distinct characters with this property. We define a norm on \widehat{M} by $\|\chi_\lambda\| = \|\lambda^*\|$ where λ^* is the element of \mathfrak{g} dual to λ . Finally, for any characters $\chi \in \widehat{M}$, we let

$$H_\chi = \{\varphi \in L^2(M) : \varphi(gx) = \chi(g)\varphi(x)\}.$$

We have that

$$L^2(M) = \bigoplus_{\chi \in \widehat{M}} H_\chi.$$

Moreover, when $\varphi \in C^r(G/\Gamma)$, if we write $\varphi = \sum_{\chi \in \widehat{M}} \varphi_\chi$ with $\varphi_\chi \in H_\chi$, then the weight

$$\text{functions } \varphi_\chi \text{ satisfy } \|\varphi_\chi\|_{C^0} \leq \frac{\|\varphi\|_{C^r}}{\|\chi\|^r}.$$

2.4. Main examples. In this article, we will pay special attention to two classes of Lie groups. The first class was first in [20], (see also [10] for general introduction).

Definition 2.3. A Lie algebra \mathfrak{g} is called *quasi-abelian* if it is not abelian and has an abelian subalgebra of codimension 1.

It follows from Definition 2.3 that any quasi-abelian Lie algebra \mathfrak{g} has a basis $(X, Y_{i,j})_{(i,j) \in J}$, satisfying the commutation relations

$$[X, Y_{i,j}] = Y_{i+1,j}, \quad (i, j) \in J,$$

and all other commutation relations are trivial (see [11]). We also remark that the class of quasi-abelian Lie algebra contains the class of filiform Lie algebras (see [20]), so our results also hold in the filiform case.

The next example is not quasi-abelian, but it has a tractable structure.

Definition 2.4. A Lie algebra is *triangular* if it is isomorphic to \mathfrak{t}_s —the Lie algebra of strictly upper triangular $(s+1) \times (s+1)$ matrices with the standard bracket for some s .

It follows from the definition that \mathfrak{t}_s is $\frac{1}{2}s(s+1)$ -dimensional. Letting E_{ij} represent the $(s+1) \times (s+1)$ matrix with a 1 in position (i, j) and zeroes elsewhere, we see that $\{E_{ij} : j > i\}$ forms a basis for \mathfrak{t}_s . The relationship among these basis elements are given by

$$[E_{ij}, E_{i'j'}] = \delta_{ji'} E_{ij'} - \delta_{j'i} E_{i'j}.$$

We refer to [4, 16] for additional information on triangular algebras.

2.5. Diophantine Conditions. Given a vector $v \in \mathbb{R}^d$, we say that $v \in DC(\gamma, \tau)$ if for all $n \in \mathbb{Z}^d$ and $m \in \mathbb{Z}$

$$|n \cdot v - m| \geq \frac{\gamma}{|n|^\tau}.$$

In [17], Kleinbock and Margulis show that within submanifolds of \mathbb{R}^n satisfying a linear independence condition almost every point is in $DC(\gamma, \tau)$ for some γ and τ . In particular, they show the following which is listed as Conjecture H_1 in their paper.

Theorem 2.5. [17] *Let f_1, \dots, f_n along with the constant function 1 form a linearly independent set of analytic functions from \mathbb{R}^m to \mathbb{R} . For almost every $x \in \mathbb{R}^m$, there exist $\gamma, \tau > 0$ such that $(f_1(x), \dots, f_n(x)) \in DC(\gamma, \tau)$.*

This result will provide the bridge from the Lie algebra structure to the Diophantine estimates needed to show mixing. Since the functions we will consider will always be homogeneous polynomials with positive degree, linear independence of f_1, \dots, f_n is the only condition we will need to check in order to apply this theorem in practice.

3. m -GREATNESS AND MIXING

In this section, we will first define what it means for a nilmanifold to be m -great and then show that on these manifolds, almost any m -tuple generates a rapidly mixing walk.

3.1. Linear independence of polynomials. Let $\mathcal{H}(t, \alpha) = (\mathcal{H}_1(t, \alpha), \dots, \mathcal{H}_\ell(t, \alpha))$ be a polynomial map of $\mathbb{R}^a \times \mathbb{R}^b \rightarrow \mathbb{R}^\ell$. Let

$$\mathcal{D}(\mathcal{H}) = \{\bar{t} \in \mathbb{R}^a : \mathcal{H}_1(\bar{t}, \alpha), \dots, \mathcal{H}_\ell(\bar{t}, \alpha) \text{ are linearly dependent}\}.$$

Expanding $\mathcal{H}_j(\bar{t}, \alpha) = \sum_{\mathbf{m}} c_{j,\mathbf{m}}(\bar{t})\alpha^{\mathbf{m}}$ we see that the above conditions amounts to vanishing of certain minors of the matrix $c_{j,\mathbf{m}}$ whence $\mathcal{D}(\mathcal{H})$ is an algebraic subvariety of \mathbb{R}^a . We say that \mathcal{H} is *non-degenerate* if $\mathcal{D}(\mathcal{H}) \neq \mathbb{R}^a$.

Now we describe a special polynomial mapping associated to a Lie algebra. Fix integers m and p . Consider m vectors $V_i = \sum_{j=1}^n \alpha_{ij} X_j$ with $i \in \{1, \dots, m\}$. These will correspond to the exponential coordinates of m generators of a random walk $g_1, \dots, g_m \bmod \mathfrak{g}^{(1)}$. Thus, each variable α_{ij} corresponds to the X_j coordinate of g_i . The idea is to see in coordinates what group elements will arise as we take iterated brackets. To that effect, let

$$\mathcal{H}_{m,p}(\mathbf{k}, \alpha) = [\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_p \mathbf{V}] + \mathfrak{g}^{(p+1)} \in \mathfrak{g}^{(p)} / \mathfrak{g}^{(p+1)},$$

where $\mathbf{k} = (\mathbf{k}_0, \dots, \mathbf{k}_p)$, $\mathbf{k}_q = (k_{q1}, \dots, k_{qm})$ and $\mathbf{k}_q \mathbf{V} = \sum_{i=1}^m k_{qi} V_i$.

The image of $\mathcal{H}_{m,p}$ is exactly the $\mathfrak{g}^{(p)}$ coordinates of the elements p -fold brackets of vectors in the span of the V_i . As we shall see, this will bear relation to the elements G achievable as p -fold brackets of elements of the group generated by the g_i . We use \mathbf{k} instead of t for the first parameter of this map because, while it still makes sense to evaluate this map at any real time, we will be particularly interested in $\mathcal{H}_{m,p}(\mathbf{k}, \alpha)$ that occurs as differences between two different words in the walk. These differences correspond to special values of \mathbf{k} , where \mathbf{k} counts how many times each generator was used at each step of the construction of the words used to obtain the difference $\mathcal{H}_{m,p}(\mathbf{k}, \alpha)$, and thus will always be integral. Note that we have

$$(3.1) \quad \mathcal{H}_{m,p}(\mathbf{k}, \alpha) = \sum_{i_j \in \{1, \dots, m\}} k_{0i_0} \dots k_{pi_p} M_{i_0 i_1, \dots, i_p} + \mathfrak{g}^{(p+1)}$$

where $M_{i_0 i_1, \dots, i_p} = [\dots [V_{i_0}, V_{i_1}], \dots], V_{i_p}]$. In coordinates, we see that

$$\mathcal{H}_{m,p}(\mathbf{k}, \alpha) = \sum_{\ell=1}^{n_p} P_\ell(\mathbf{k}, \alpha) X_i^{(p)} + \mathfrak{g}^{(p+1)}$$

where each $P_\ell(\mathbf{k}, \alpha)$ is a polynomial in the coordinates of \mathbf{k} and α_{ij} (in particular the α_{0j}). We will care about when the map $\mathcal{H}_{m,p}$ is degenerate, so in context we have that

$\mathcal{D}(\mathcal{H}_{m,p})$ represents the variety

$$\{\mathbf{k} \in \mathbb{R}^{m(p+1)} : P_1(\mathbf{k}, \alpha), \dots, P_{n_p}(\mathbf{k}, \alpha) \text{ are linearly dependent polynomials in } \alpha\}.$$

From now on we will suppress the $+\mathfrak{g}^{(p+1)}$ that ought to appear whenever we discuss $\mathcal{H}_{2,p}$, but we agree that $\mathcal{H}_{2,p}$ is always defined modulo $\mathfrak{g}^{(p+1)}$. We now provide a brief illustrative example.

Example 3.1. Let \mathfrak{g} be the step-3 Lie algebra of dimension 5 with the following commutation relations

$$[X_1, X_2] = Y, \quad [Y, X_1] = Z_1, \quad [Y, X_2] = Z_2.$$

with all other brackets being 0. Let $V_1 = \alpha_{11}X_1 + \alpha_{12}X_2 + \dots$, $V_2 = \alpha_{21}X_1 + \alpha_{22}X_2 + \dots$. Then $[[V_1, V_2], V_1] = (\alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21})Z_1 + (\alpha_{11}\alpha_{12}\alpha_{21} - \alpha_{12}^2\alpha_{21})Z_2 \pmod{\mathfrak{g}_3}$. Therefore

$$M_{121} = \begin{bmatrix} \alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21} \\ \alpha_{11}\alpha_{12}\alpha_{21} - \alpha_{12}^2\alpha_{21} \end{bmatrix}.$$

Suppose now we wish to compute the $\mathcal{H}_{2,2}$ for this \mathfrak{g} . To do so, we can proceed in two different ways. We could compute each $M_{i_1i_2i_3}$ and then write the sum as in (3.1). Alternatively, we can explicitly compute $[[\mathbf{k}_0\mathbf{V}, \mathbf{k}_1\mathbf{V}], \mathbf{k}_2\mathbf{V}]$ and we shall see how the $M_{i_1i_2i_3}$ appear. We will take this second approach.

$$\begin{aligned} & [[k_{01}V_1 + k_{02}V_2, k_{11}V_1 + k_{12}V_2], k_{21}V_1 + k_{22}V_2] \\ &= [(k_{01}k_{12}(\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}) - k_{02}k_{11}(\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}))Y, k_{21}V_1 + k_{22}V_2] \\ &= k_{01}k_{12}k_{21}((\alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21})Z_1 + (\alpha_{11}\alpha_{12}\alpha_{22} - \alpha_{12}^2\alpha_{21})Z_2) \\ &\quad + k_{01}k_{12}k_{22}((\alpha_{11}\alpha_{21}\alpha_{22} - \alpha_{12}\alpha_{21}^2)Z_1 + (\alpha_{11}\alpha_{22}^2 - \alpha_{12}\alpha_{21}\alpha_{22})Z_2) \\ &\quad - k_{02}k_{11}k_{21}((\alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21})Z_1 + (\alpha_{11}\alpha_{12}\alpha_{22} - \alpha_{12}^2\alpha_{21})Z_2) \\ &\quad - k_{02}k_{11}k_{22}((\alpha_{11}\alpha_{21}\alpha_{22} - \alpha_{12}\alpha_{21}^2)Z_1 + (\alpha_{11}\alpha_{22}^2 - \alpha_{12}\alpha_{21}\alpha_{22})Z_2). \end{aligned}$$

We see that $M_{i_1i_2i_3}$ is exactly the coefficient of $k_{0i_1}k_{1i_2}k_{2i_3}$, and our mapping can be written as

$$k_{01}k_{12}k_{21}M_{121} + k_{01}k_{12}k_{22}M_{122} + k_{02}k_{11}k_{21}M_{211} + k_{02}k_{11}k_{22}M_{212}.$$

In vector form, $\mathcal{H}_{2,2}$ takes form

$$\begin{aligned} & k_{01}k_{12}k_{21} \begin{bmatrix} \alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21} \\ \alpha_{11}\alpha_{12}\alpha_{21} - \alpha_{12}^2\alpha_{21} \end{bmatrix} + k_{01}k_{12}k_{22} \begin{bmatrix} \alpha_{11}\alpha_{21}\alpha_{22} - \alpha_{12}\alpha_{21}^2 \\ \alpha_{11}\alpha_{22}^2 - \alpha_{12}\alpha_{21}\alpha_{22} \end{bmatrix} \\ & - k_{02}k_{11}k_{21} \begin{bmatrix} \alpha_{11}^2\alpha_{22} - \alpha_{11}\alpha_{12}\alpha_{21} \\ \alpha_{11}\alpha_{12}\alpha_{21} - \alpha_{12}^2\alpha_{21} \end{bmatrix} - k_{02}k_{11}k_{22} \begin{bmatrix} \alpha_{11}\alpha_{21}\alpha_{22} - \alpha_{12}\alpha_{21}^2 \\ \alpha_{11}\alpha_{22}^2 - \alpha_{12}\alpha_{21}\alpha_{22} \end{bmatrix}. \end{aligned}$$

We clearly see that $\mathcal{H}_{2,2}$ is non-degenerate since even just setting $k_{01} = k_{12} = k_{21} = 1$ and $k_{02} = k_{11} = k_{22} = 0$, we get that at that value of \mathbf{k} , $\mathcal{H}_{2,2}$ evaluates to M_{121} , which has linearly independent rows. Thus, our selected value of \mathbf{k} is not in $\mathcal{D}(\mathcal{H}_{2,2})$, and thus $\mathcal{H}_{2,2}$ is non-degenerate.

3.2. m -great Lie algebras and mixing. Now, we will define the key technical property which guarantees that the set of rapid mixing m -tuples is of full measure.

Definition 3.2. A Lie algebra \mathfrak{g} is *m -great* if $\mathcal{H}_{m,i}$ is non-degenerate for every $i \in [0, s-1]$.

When a Lie algebra is not m -great, we say it is m -bad. We will call a Lie group or a nilmanifold m -great if its associated Lie algebra is m -great. We will show that m -greatness implies that the walk generated almost every m -tuple has a Diophantine property in the following sense.

Definition 3.3. Let $M = G/\Gamma$ be a step- s nilmanifold and $F = (g_1, \dots, g_m)$ be an m -tuple.

- A pair of words $W_1, W_2 \in \langle F \rangle$ is said to be *nice* on $G^{(p)}$ if they have equal length and their difference $h := W_2W_1^{-1}$ satisfies $h \in G^{(p)}$, and there exist $\gamma, \tau > 0$ such that $\pi_p(\log(h)) \in DC(\gamma, \tau)$.
- An m -tuple is said to act *Diophantinely* on M_p if there exists a pair of words that is nice on $G^{(p)}$.
- We say that an m -tuple acts *Diophantinely at all levels* if it acts Diophantinely on M_p for all $0 \leq p < s$.

Let E_m denote the set of m -tuples which act Diophantinely at all levels on a nilmanifold M , and recall that μ^m is the measure on the space of m -tuples of elements of G given by the m -fold product of the Haar measure on G with itself.

Proposition 3.4. *If $M = G/\Gamma$ is m -great, then E_m is of full measure with respect to μ^m .*

We postpone the proof to Section 4. We now show that the random walk generated by any m -tuple that act Diophantinely on all levels is rapid mixing. The key estimate to show appears in the following theorem:

Proposition 3.5. *If a random walk is generated by an m -tuple that acts Diophantinely at all levels, then there exist constants $C, a, b > 0$ such that for $A \in C^r(M)$ with zero mean,*

$$(3.2) \quad \|\mathcal{L}^N A\|_{C^0} \leq \frac{K \|A\|_{C^r}}{N^{ar-b}}.$$

Whenever (3.2) holds, it implies rapid mixing of the associated random walk since

$$(3.3) \quad |\bar{\rho}_{A,B}(N)| \leq \|\mathcal{L}^N A\|_{C^0} \|B\|_{C^0} \leq C \|A\|_{C^r} \|B\|_{C^0} N^{-(ar-b)}.$$

To prove Proposition 3.5, we will show that for any nontrivial character χ , \mathcal{L} has spectral gap on H_χ , and, moreover, that the size of the spectral gap has a polynomial lower bound in the norm of χ . We will also use the fact that the size of a C^r function's projection into H_χ is polynomially bounded in the norm of χ . Together, these estimates will allow us to prove Theorem 3.5. We now show the spectral gap.

Lemma 3.6. *Assume that F acts Diophantinely at all levels. There exist constants $C_1, C_2, \ell, \tau > 0$ such that if χ is a nontrivial character on M and $A \in H_\chi$, then*

$$\|\mathcal{L}^N A\|_{C^0} \leq C_1 (1 - C_2 \|\chi\|^{-2\tau})^{N/\ell} \|A\|_{C^0}.$$

Proof. Let $A \in H_\chi$ where $\chi \in \widehat{M}^{(i)}$. We will now fix words and constants that depend only on i and not on the particular character χ as follows. Let W_1^i and W_2^i be the nice words on $G^{(i)}$ guaranteed by the assumption that the g_i act Diophantinely at all levels. Let ℓ_i be the common length of W_1^i and W_2^i , and let γ_i, τ_i be the associated Diophantine constants.

Recall that $p_{\ell_i}(W)$ denotes the probability that the walk has moved by W at time ℓ_i . Suppressing the dependence on ℓ_i , let $\mathbf{p} = \min(p(W_1), p(W_2))$. Suppose without loss of generality that $\mathbf{p} = p(W_1)$. Then set $h = W_2W_1^{-1}$, and let $W_3, \dots, W_{m\ell_i}$ denote the remaining words with positive probability at step ℓ_i of the walk. With this notation, we have

$$\mathcal{L}^{\ell_i}(A)(x) = \mathbf{p} [A(W_1x) + A(hW_1x)] + \left[(p(W_2) - p(W_1))A(W_2x) + \sum_{j \geq 3} p(W_j)A(W_jx) \right].$$

Since $A \in H_\chi$, we have that

$$\mathbf{p}[A(W_1x) + A(hW_1x)] = \mathbf{p}[A(W_1x) + \chi(h)A(W_1x)] = (1 + \chi(h))A(W_1x).$$

Letting $\lambda \in \Lambda_p$ to be the nonzero functional such that $\chi = \chi_\lambda$, we get that

$$|1 + \chi(h)| = |1 + e^{2\pi i \lambda(\log(h))}|.$$

Since by niceness of W_1^i and W_2^i , $\log(h) \in DC(\gamma, \tau)$, we can apply Lemma A.2 from the appendix, to say that, for some constant \bar{C}_i depending only on γ_i , we have that

$$|1 + \chi(h)| \leq 2 - \bar{C}_i |\chi|^{-2\tau_i}.$$

Putting this all together, we find that

$$\mathbf{p}|A(W_1x) + A(hW_1x)| = \mathbf{p}|1 + \chi(h)||A(W_1x)| \leq 2\mathbf{p}(1 - \bar{C}_i \|\chi\|^{-2\tau_i}) \|A\|_{C^0}.$$

Turning our attention to the second term in the expression for $\mathcal{L}^{\ell_i}(A)(x)$, we see that

$$(p(W_2) - p(W_1))A(W_2x) + \sum_{j \geq 3} p(W_j)A(W_jx) \leq (1 - 2\mathbf{p}) \|A\|_{C^0}.$$

Combining these estimates, we see that on H_χ ,

$$\|\mathcal{L}^{\ell_i} A\|_{C^0} \leq 2\mathbf{p}(1 - \bar{C}_i \|\chi\|^{-2\tau_i}) \|A\|_{C^0} + (1 - 2\mathbf{p}) \|A\|_{C^0} \leq (1 - \hat{C}_i \|\chi\|^{-2\tau_i}) \|A\|_{C^0},$$

where $\hat{C}_i = 2\mathbf{p}\bar{C}_i$. We have now shown the desired result except for an unwanted dependence on the level i in the constants ℓ_i, \hat{C}_i , and τ_i . Since there are only s different levels, we only used s different word pairs with associated constants. Thus, we can simply fix $\hat{C} = \min\{\hat{C}_i\}$, $\ell = \max\{\ell_i\}$, and $\tau = \max\{\tau_i\}$. We then see that

$$\|\mathcal{L}^\ell A\|_{C^0} \leq (1 - \hat{C} \|\chi\|^{-2\tau}) \|A\|_{C^0}$$

holds independently of the value of i . Iterating this estimate $\lceil N/\ell \rceil$ times gives the result. \square

Now we put together the estimates on the behavior of \mathcal{L} on each H_χ and estimate how \mathcal{L} acts on C^r .

Proof of Proposition 3.5. First, we decompose A as $\sum_{\chi \in \widehat{M}} A_\chi$ where $A_\chi \in H_\chi$. Since A has mean 0, $A_\chi = 0$ when χ is the trivial character. Thus,

$$\|\mathcal{L}^N A\|_{C^0} \leq \sum_{\|\chi\|^{2\tau} < \sqrt{N}} \|\mathcal{L}^N A_\chi\|_{C^0} + \sum_{\|\chi\|^{2\tau} \geq \sqrt{N}} \|\mathcal{L}^N A_\chi\|_{C^0}.$$

For the first term, we will use the spectral gap of \mathcal{L} from Lemma 3.6. This gives us that when $\|\chi\|^{2\tau} < \sqrt{N}$,

$$\|\mathcal{L}^N A_\chi\|_{C^0} \leq C_1 \left(1 - \frac{C_2}{\sqrt{N}}\right)^{N/\ell} \|A\|_{C^0}.$$

Thus, since there are only $N^{\dim(M)/4\tau}$ characters satisfying $\|\chi\|^{2\tau} < \sqrt{N}$,

$$\sum_{\|\chi\|^{2\tau} < \sqrt{N}} \|\mathcal{L}^N A_\chi\|_{C^0} \leq C_1 N^{\dim(M)/4\tau} \left(1 - \frac{C_2}{\sqrt{N}}\right)^{N/\ell} \|A\|_{C^0}.$$

Setting $C_3 = C_2/\ell$ and $a = \dim(M)/4\tau$, this term is $O(N^a e^{-C_3 \sqrt{N}}) \ll N^{(r - \dim(M))/4\tau}$, so up to changing the constant K , we have dealt with the first term. Finally, we observe that since $A \in C^r$, the projection A_χ satisfies

$$\|A_\chi\|_{C^0} \leq \|A\|_{C^r} \|\chi\|^{-r}.$$

Therefore, since \widehat{M} corresponds to a lattice in $\mathbb{R}^{\dim(M)}$, we can use the classical bounds on tails of higher dimensional p -series to see that for some constant $C_4 > 0$,

$$\sum_{\|\chi\|^{2\tau} \geq \sqrt{N}} \|\mathcal{L}^N A_\chi\|_{C^0} \leq \sum_{\|\chi\| > N^{1/4\tau}} \frac{\|A\|_{C^r}}{\|\chi\|^r} \leq C_4 N^{-(r-\dim(M))/4\tau} \|A\|_{C^r}.$$

Thus, for the appropriate choice of K , a , and b , the estimate holds. \square

Theorem 3.7. *Let G/Γ be an m -great nilmanifold. The set of m -tuples in G^m which are rapid mixing has full measure with respect to μ^m .*

Proof. Whenever an m -tuple acts Diophantinely on every level, Proposition 3.5 applies. By (3.3), this is enough to conclude rapid mixing for the random walk they generate. Proposition 3.4 implies that the set of such tuples has full measure with respect to μ^m . \square

4. NICE WORDS

In this section, we prove Proposition 3.4. Our approach is to construct words in the semigroup $\langle F \rangle$ that differ by a nonzero element of $G^{(p)}$ for each p . In particular, we will find words that differ by a term that can be expressed as a p -fold bracket of elements of $\langle F \rangle$. Then, we will observe that a formula for this difference may be given as a polynomial in the exponential coordinates of the g_i . As long as the polynomials arising in this manner are linearly independent, we can apply Theorem 2.5 to conclude that, for a full measure set of walks, the words we construct act Diophantinely on the appropriate level, and thus we have nice words. This need for linear independence was the direct motivation for Definition 3.2. Once we have linear independence, Theorem 2.5 will guarantee the existence of a full measure of the set of m -tuples that act Diophantinely and thus rapidly mix.

To begin, given $p \geq 1$, let $K_p \subset (\mathbb{Z}^m)^{(p+1)}$ be the set of all indices $\mathbf{k}_0, \dots, \mathbf{k}_p$ such that $[\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_p \mathbf{V}$ can be written of the form $\log(W_1 W_2^{-1}) \bmod \mathfrak{g}^{(p+1)}$ for two words W_1 and W_2 of equal length in $\langle F \rangle$. This is the set of p -nested commutators that arise as the logarithm of the difference between two elements of our walk at some time. Thus K_p can heuristically be seen as the set of elements of \mathfrak{g}_p available to us in trying to get a self-cancellation between a character on level p pushed forward by two words in our random walk. In constructing elements of K_p , the element k_{ij} will count how many times g_j appears in the i^{th} step of the construction of the words differing by $\mathcal{H}_p(k, \alpha)$. For instance, in the setting of two generators g_1 and g_2 , since

$$\log(g_1 g_2 (g_2 g_1)^{-1}) = \log([g_1, g_2]) = [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}]$$

for $\mathbf{k}_0 = (1, 0)$ and $\mathbf{k}_1 = (0, 1)$, we have that $((1, 0), (0, 1)) \in K_2$. In terms of this set, our goal is to find an intersection between K_p and the complement of $\mathcal{D}(\mathcal{H}_{m,p})$ i.e. a difference between two words in our walk with linearly independent polynomials. The following lemmas will demonstrate a method for finding elements of K_p that will be rich enough that as long as $\mathcal{D}(\mathcal{H}_{m,p}) \neq \mathbb{R}^{n_p}$, K_p will not be contained in $\mathcal{D}(\mathcal{H}_{m,p})$ as we desire.

Lemma 4.1. *For any given $w_{-1}, \dots, w_p \in \langle F \rangle$ with $|w_{-1}| = |w_0|$, there exist words of equal length W_1 and W_2 such that*

$$W_2 W_1^{-1} \in \mathfrak{g}_p.$$

Proof. Our idea is to inductively build words a_i and b_i in $\langle F \rangle$ such that $h_i := a_i b_i^{-1} \in G^{(i)}$ and to do so with as much flexibility as possible. To begin with, we set

$$a_0 = w_{-1} \quad b_0 = w_0,$$

and

$$a_i = a_{i-1} w_i b_{i-1} \quad \text{and} \quad b_i = b_{i-1} w_i a_{i-1}.$$

Since we took $|w_{-1}| = |w_0|$, this construction will always give us words a_i and b_i satisfying $|a_i| = |b_i|$. Observe that

$$h_1 = a_0 w_1 b_0 a_0^{-1} w_1^{-1} b_0^{-1} = [a_0 b_0^{-1}, b_0 w_1],$$

and

$$h_i = a_{i-1} w_i b_{i-1} (b_{i-1} w_i a_{i-1})^{-1} = a_{i-1} (b_{i-1}^{-1} b_{i-1}) w_i b_{i-1} a_{i-1}^{-1} w_i^{-1} b_{i-1}^{-1} = [a_{i-1} b_{i-1}^{-1}, b_{i-1} w_i]$$

Since $a_{i-1} b_{i-1}^{-1} = h_{i-1}$, we can rewrite this as

$$h_i = [h_{i-1}, b_{i-1} w_i].$$

Thus, h_1 can be expressed as a single bracket, and h_i can be expressed as a bracket between h_{i-1} and another group element, so inductively h_i can always be expressed as an i -fold bracket. In particular, we get the formula

$$(4.1) \quad h_p = [\dots [[a_0 b_0^{-1}, b_0 w_1], b_1 w_2], \dots, b_{p-1} w_p],$$

so $h_p \in \mathfrak{g}^{(p)}$ as desired. \square

Lemma 4.2. *For any k satisfying $3k_{ij} < k_{i+1j}$, there exist words of equal length W_1, W_2 such that*

$$\log(W_2 W_1^{-1}) = [\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_p \mathbf{V} \quad \text{mod } \mathfrak{g}^{(p+1)}.$$

Proof. By the previous Lemma, for any w_{-1}, \dots, w_p with $|w_{-1}| = |w_0|$, we can build words that differ by $h_p \in \mathfrak{g}^{(p)}$. Moreover, h_p can be written as $a_p b_p^{-1}$ for two words of equal length in $\langle F \rangle$. If we can find $\mathbf{k}_0, \mathbf{k}_1, \dots, \mathbf{k}_p$ such that

$$\log h_p = [\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_p \mathbf{V},$$

then $(\mathbf{k}_0, \mathbf{k}_1, \dots, \mathbf{k}_p) \in K_p$. Motivated by this, we take the logarithm of both sides of (4.1) to get

$$\log(h_p) = \log([\dots [[a_0 b_0^{-1}, b_0 w_1], b_1 w_2], \dots, b_{p-1} w_p]).$$

The BCH formula allows us to move the logarithm within the brackets modulo some error that belongs to $\mathfrak{g}^{(p+1)}$, so

$$(4.2) \quad \log(h_p) = [\dots [[\log(a_0 b_0^{-1}), \log(b_0 w_1)], \log(b_1 w_2)], \dots, \log(b_{p-1} w_p)] \quad \text{mod } \mathfrak{g}^{(p+1)}.$$

Now, define a function $\mathbf{c} : \langle F, F^{-1} \rangle \rightarrow \mathbb{Z}^m$ such that $\mathbf{c}_i(W)$ is the number of times g_i appears in the word W with inverses counted as negatives. Define $\mathbf{k}_0 = \mathbf{c}(a_0 b_0^{-1})$ and $\mathbf{k}_i = \mathbf{c}(b_{i-1} w_i)$. Applying BCH again, we have that $\log(b_{i-1} w_i) = \sum_{i=1}^m \mathbf{k}_i V_i \quad \text{mod } \mathfrak{g}^{(1)}$. Applying this fact to (4.2) and using the fact that the p -fold bracket of a $\mathfrak{g}^{(1)}$ error is in \mathfrak{g}^{p+1} , we get

$$\log(h) = [\dots [\sum_{i=1}^m \mathbf{k}_{0i} V_i, \sum_{i=1}^m \mathbf{k}_{1i} V_i], \dots, \sum_{i=1}^m \mathbf{k}_{pi} V_i] = [\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_p \mathbf{V} \quad \text{mod } \mathfrak{g}^{(p+1)}.$$

Now, we have $(\mathbf{k}_0, \dots, \mathbf{k}_p) \in K_p$ which depends on our initial choice of w_{-1}, \dots, w_p . We wish to understand which sequences $\mathbf{k}_0, \dots, \mathbf{k}_p$ are possible to get as a result of that choice. Note that \mathbf{k}_0 and \mathbf{k}_1 can be taken to be any vector of nonnegative integers simply by making an appropriate choice of w_{-1}, w_0 , and w_1 . Meanwhile, for $i \geq 2$, we

have $\mathbf{k}_i = \mathbf{c}(b_{i-1}) + \mathbf{c}(w_i)$. Since by our choice of w_i we can make $\mathbf{c}(w_i)$ any nonnegative integer vector we like, this means we can choose any \mathbf{k}_i , subject to $\mathbf{k}_i \geq \mathbf{c}(b_{i-1})$. Since $\mathbf{c}(b_{i-1}) = 2\mathbf{c}(b_{i-2}) + \mathbf{c}(w_{i-1}) \leq 3\mathbf{k}_{i-1}$, if $\mathbf{k}_i \geq \mathbf{k}_{i-1}$, then $(\mathbf{k}_0, \dots, \mathbf{k}_p) \in K_p$. \square

Lemma 4.3. *K_p is Zariski dense.*

Proof. By the previous lemma, $\{k \in (\mathbb{Z}^m)^{p+1} : 3k_{ij} < k_{i+1j}\}$ is contained in K_p . It is clear that this set, when interpreted as a subset of \mathbb{R}^{mp} , is Zariski dense. It follows that K_p is a Zariski dense set. \square

Proof of Proposition 3.4. We claim that there are words W_1 and W_2 of equal length such that the coordinates of $\pi_p(\log(W_1W_2^{-1}))$ are linearly independent polynomials in α . Assume by contradiction that for all words W_1, W_2 , these polynomials are linearly dependent. That implies that any words that differ by p -nested commutators have those commutators' polynomials linearly dependent. Since K_p consists of the set of such realized commutators, this means that $K_p \subset \mathcal{D}(\mathcal{H}_{m,p})$. Since $\mathcal{D}(\mathcal{H}_{m,p})$ is an algebraic variety and by Lemma 4.3 K_p is Zariski dense, this implies that $\mathcal{D}(\mathcal{H}_{m,p}) = \mathbb{R}^{np}$. Thus, $\mathcal{H}_{m,p}$ is degenerate, contradicting the assumption that \mathfrak{g} is m -great. The claim follows.

Next, by Theorem 2.5, since the coordinate polynomials of $\pi_p(W_1W_2^{-1})$ are linearly independent, for almost every value of the α_{ij} , $\pi_p(W_1W_2^{-1}) \in DC(\gamma, \tau)$. That means that for almost every m -tuple of g_i 's $\pi_p(W_1W_2^{-1}) \in DC(\gamma, \tau)$. This implies the Proposition. \square

5. GREAT GROUPS

Now that we have established that m -greatness implies rapid mixing of almost all random walks on m elements, we wish to show that this condition is not overly restrictive. To that effect, we show that many special Lie algebras are 2-great, and that every step- s Lie algebra is s -great. This will prove Theorems A and B. Finally, we present an example of a group that is not 2-great.

We now briefly discuss how we will approach the task of proving that a Lie algebra is m -great. Given a Lie algebra \mathfrak{g} , we will pick some concrete k_p for which we will show that $\mathcal{H}_{m,p}(k_p, \alpha)$ has linearly independent polynomials i.e. $k_p \notin \mathcal{D}(\mathcal{H}_{m,p})$. To show this linear independence, we let $\{P_1, \dots, P_{n_p}\}$ be the set of n_p coordinate polynomials associated to the $X_i^{(p)}$. If there is a monomial $M_i = \alpha_{i_0j_0} \dots \alpha_{i_pj_p}$ with nonzero coefficient in P_i but zero coefficient in each P_j when $j \neq i$, we call M_i a *unique monomial* of P_i . If each P_i has a unique monomial, this is sufficient to conclude that the P_i form a linearly independent set. By finding a unique monomial of each of the P_i , we can show that the P_i form a linearly independent set. Thus, $\bar{k}_p \notin \mathcal{D}(\mathcal{H}_{2,p})$ and $\mathcal{H}_{2,p}$ is non-degenerate. From there, we will conclude 2-greatness.

5.1. 2-great algebras. Here we prove that all quasi-abelian, triangular and step-3 or lower Lie algebras are 2-great. Throughout this section, we shall denote $\bar{k}_p = ((1, 0), (0, 1)^p)$.

Proposition 5.1. *All quasi-abelian groups are 2-great*

Proof. To show this, we must show that $\mathcal{H}_{2,p}$ is nondegenerate for all $0 \leq p \leq s-1$. We recall that we defined a basis $\{X, Y_{i,j}\}_{(i,j) \in J}$ in Section 2.4. We will let

$$V_1 = \alpha_0 X + \sum_j \alpha_{0,j} Y_{0,j} \quad \text{mod } \mathfrak{g}^{(1)} \quad \text{and} \quad V_2 = \beta_0 X + \sum_j \beta_{0,j} Y_{0,j} \quad \text{mod } \mathfrak{g}^{(1)}$$

and let P_1, \dots, P_{n_p} be the coordinate polynomials in α of $\mathcal{H}_{2,p}(\bar{k}_p, \alpha)$. We will show that if P_i is the polynomial corresponding to the $Y_{i,p}$ coordinate then $\alpha_{0,i}\beta_0^p$ is a unique monomial of P_i . This is because the coefficient of $\alpha_{0,i}\beta_0^p$ in $[\dots[V_1, V_2], \dots V_2]$ is exactly $[\dots[[Y_{0,i}, X], X], \dots, X] = Y_{i,p}$. This means that each P_i has a unique monomial, so they form a linearly independent set of polynomials. Thus $\bar{k} \notin \mathcal{D}(\mathcal{H}_{2,p})$, so $\mathcal{H}_{2,p}$ is non-degenerate. Since p is arbitrary, any quasi-abelian Lie algebra is 2-great. \square

Proposition 5.2. *For any $s \in \mathbb{N}$, \mathfrak{t}_s is 2-great.*

Proof. We recall that we defined a basis $\{E_{ij}\}$ in Section 2.4. Let

$$V_1 = \sum_{i=1}^{n-1} \alpha_{0i} E_{i,i+1} \pmod{\mathfrak{g}^{(1)}} \quad \text{and} \quad V_2 = \sum_{i=1}^{n-1} \beta_{0i} E_{i,i+1} \pmod{\mathfrak{g}^{(1)}}.$$

Let P_1, \dots, P_{n_p} be the coordinate polynomials in α of $\mathcal{H}_{2,p}(\bar{k}_p, \alpha)$. We will show that if P_i is the polynomial corresponding to the $E_{i,i+p+1}$ coordinate, then $\alpha_i\beta_{i+1}, \dots, \beta_{i+p}$ is a unique monomial of P_i . This is because the coefficient of $\alpha_i\beta_{i+1}, \dots, \beta_{i+p}$ in $[\dots[V_1, V_2], \dots V_2]$ is exactly $[\dots[E_{i,i+1}, E_{i+1,i+2}], \dots, E_{i+p,i+p+1}] = E_{i,i+p+1}$. This means that each P_i has a unique monomial, so they form a linearly independent set of polynomials. Thus, $\bar{k} \notin \mathcal{D}(\mathcal{H}_{2,p})$ and so $\mathcal{H}_{2,p}$ is non-degenerate. Since p is arbitrary, any triangular Lie algebra is 2-great. \square

We now turn our attention to lower step algebras. We treat first the case of step 1 and step 2 algebras as they may be dealt with quite simply.

Lemma 5.3. *Any abelian or step 2 Lie algebra is 2-great*

Proof. We compute $\mathcal{H}_{2,0}$ and $\mathcal{H}_{2,1}$ for arbitrary groups. If $V_1 = \sum_i \alpha_i X_i$, $V_2 = \sum_i \beta_i X_i$, we have that $\mathcal{H}_{2,0}((1,0), \alpha) = V_1$ which clearly has linearly independent polynomials for coordinates. Thus $\mathcal{H}_{2,0}$ is always non-degenerate. Now, if \mathfrak{g} is non-abelian, let $X_j^{(2)} = [X_i, X_i]$. In $\mathcal{H}_{2,1}$, the monomial $\alpha_i\beta_j$ only appears as a coefficient of $X_j^{(2)}$. Thus, for any non-abelian Lie algebra $\mathcal{H}_{2,1}$ is non-degenerate. From this we conclude the Lemma. \square

Now, we show that step-3 Lie algebras are also necessarily 2-great. This is the best we can do in terms of step as there exist step-4 Lie algebras that are not 2-great as we shall see. Our proof technique will be similar to the proofs of 2-greatness that we have already presented in that we begin by fixing some choice of k which we show to be in the complement of $\mathcal{D}(\mathcal{H}_{2,2})$. It will differ in that we will show that the existence of a linear dependence between the polynomials of $\mathcal{H}_{2,2}$ contradicts the fact that \mathfrak{g} is step 3 rather than directly showing linear independence by identifying unique monomials of each polynomial.

Proposition 5.4. *Any nilpotent Lie algebra is of step 3 or less is 2-great.*

Proof. We set $V_1 = \sum_i \alpha_i X_i$, $V_2 = \sum_i \beta_i X_i$ and show that M_{121} consists of linearly independent polynomials. By way of contradiction, assume that the polynomials of M_{121} are not independent, i.e.

$$0 \equiv \lambda([V_1, V_2], V_1) \text{ for some } 0 \neq \lambda \in \mathfrak{g}^*.$$

Expanding out, we see that this would imply that

$$0 \equiv \sum_{i_1, i_2, i_3 \in I} \alpha_{i_1} \beta_{i_2} \alpha_{i_3} \lambda([X_{i_1}, X_{i_2}], X_{i_3}).$$

From this we deduce that if a given monomial $\alpha_{i_1}\beta_{i_2}\alpha_{i_3}$ has coefficient $W_{i_1i_2i_3} \in \mathfrak{g}$ in the expression $[[V_1, V_2], V_1]$, then $W_{i_1i_2i_3} \in \text{Ker}(\lambda)$. Since terms of the form $\alpha_{i_1}^2\beta_{i_2}$ occur with coefficient $[[X_{i_1}, X_{i_2}], X_{i_1}]$, we get

$$(5.1) \quad \lambda([[X_{i_1}, X_{i_2}], X_{i_1}]) = 0.$$

Next expanding the equation $\lambda([[X_{i_1} + X_{i_3}, X_{i_2}], X_{i_1} + X_{i_3}]) = 0$ as sum of monomials and using (5.1) we get

$$(5.2) \quad \lambda([[X_{i_1}, X_{i_2}], X_{i_3}] + [[X_{i_3}, X_{i_2}], X_{i_1}]) = 0.$$

Combining (5.2) with Jacobi identity

$$[[X_{i_1}, X_{i_2}], X_{i_3}] + [[X_{i_2}, X_{i_3}], X_{i_1}] + [[X_{i_3}, X_{i_1}], X_{i_2}] = 0,$$

so we get

$$(5.3) \quad \lambda(2[[X_{i_1}, X_{i_2}], X_{i_3}] + [[X_{i_3}, X_{i_1}], X_{i_2}]) = 0.$$

Swapping i_2 and i_3 we obtain

$$(5.4) \quad \lambda(2[[X_{i_1}, X_{i_3}], X_{i_2}] + [[X_{i_2}, X_{i_1}], X_{i_3}]) = 0.$$

Since the matrix defining (5.3)–(5.4) is non-degenerate, we conclude that

$$\lambda([[X_{i_1}, X_{i_2}], X_{i_3}]) = \lambda([[X_{i_3}, X_{i_1}], X_{i_2}]) = 0.$$

Since the equation above holds for arbitrary $i_1, i_2, i_3 \in I$, this implies that $\lambda=0$, a contradiction. Thus, $\mathcal{H}_{2,2}$ is non-degenerate. The fact that $\mathcal{H}_{2,0}$ and $\mathcal{H}_{2,1}$ are non-degenerate follows from Lemma 5.3, so any step-3 (or lower) Lie algebra is 2-great. \square

Combining Propositions 5.1, 5.2, and 5.5 with Theorem 3.7 gives us Theorem B.

5.2. General Lie algebras. We will now show that every nilpotent Lie algebra is m -great for sufficiently large m . Our approach will largely mirror that of the proofs of Propositions 5.1 and 5.2, but taking advantage of the larger value of m .

Proposition 5.5. *A step- s Lie algebra is s -great.*

Proof. We prove that $\mathcal{H}_{s,s-1}$ is non-degenerate. Let $V_i = \sum_{j=1}^{n_0} \alpha_{ij} X_j \bmod \mathfrak{g}^{(1)}$, and

consider $[\dots [\mathbf{k}_0 \mathbf{V}, \mathbf{k}_1 \mathbf{V}], \dots], \mathbf{k}_{s-1} \mathbf{V}]$. Let \bar{k} denote the conveniently selected parameters: $\mathbf{k}_0 = (1, 0, \dots, 0)$, $\mathbf{k}_1 = (0, 1, \dots, 0), \dots, \mathbf{k}_{s-1} = (0, 0, \dots, 1)$. We compute that the coefficient of $\alpha_{0i_0} \cdots \alpha_{s-1i_{s-1}}$ in $\mathcal{H}_{s,s-1}(\bar{k}, \alpha)$ is exactly $[\dots [[X_{i_0}, X_{i_1}], \dots, X_{i_{s-1}}]]$, so $\alpha_{0i_0} \cdots \alpha_{s-1i_{s-1}}$ will be a unique monomial for the corresponding coordinate polynomial of $\mathcal{H}_{s,s-1}$. Since each element of the basis for $\mathfrak{g}^{(s-1)}$ can be written of the form $[\dots [[X_{i_0}, X_{i_1}], \dots, X_{i_{s-1}}]]$, we get that each coordinate polynomial of $\mathcal{H}_{s,s-1}(\bar{k}, \alpha)$ has a unique monomial. Thus, the polynomials at \bar{k} are linearly independent, so $\mathcal{H}_{s,s-1}$ is non-degenerate. Since every $\mathfrak{g}/\mathfrak{g}^{(i+1)}$ is step- s or lower, the same argument will show that $\mathcal{H}_{s,i}$ is non degenerate for all $i < s$. We conclude that \mathfrak{g} is s -great. \square

Combining Proposition 5.5 with Theorem 3.7 gives us Theorem A. We also show that m -greatness is preserved by taking products and factors.

Proposition 5.6. *The property of m -greatness is closed under taking direct products or factors in the following sense:*

- If \mathfrak{g}_1 and \mathfrak{g}_2 are m -great, then $\mathfrak{g}_1 \times \mathfrak{g}_2$ is m -great.
- If \mathfrak{g} is m -great and \mathfrak{h} is a factor of \mathfrak{g} , then \mathfrak{h} is m -great.

Proof. For clarity, in this proof we will let $\mathcal{H}_{m,p}^{\mathfrak{g}}$ be the map $\mathcal{H}_{m,p}$ associated to the Lie group \mathfrak{g} . Similarly, let $\alpha_{ij}^{\mathfrak{g}}$ be the Malcev coordinates of the projection into \mathfrak{g} of the V_i . For the first part, observe that $\mathcal{H}_{m,p}^{\mathfrak{g}_1 \times \mathfrak{g}_2}(k, \alpha^{\mathfrak{g}_1 \times \mathfrak{g}_2}) = (\mathcal{H}_{m,p}^{\mathfrak{g}_1}(k, \alpha^{\mathfrak{g}_1}), \mathcal{H}_{m,p}^{\mathfrak{g}_2}(k, \alpha^{\mathfrak{g}_2}))$. Since both of the \mathfrak{g}_i 's are m -great, $\mathcal{D}(\mathcal{H}_{m,p}^{\mathfrak{g}_i})$ is a positive codimension variety. Thus, there exists a k_0 in $\mathcal{D}(\mathcal{H}_{m,p}^{\mathfrak{g}_1})^c \cap \mathcal{D}(\mathcal{H}_{m,p}^{\mathfrak{g}_2})^c$. It follows that $k \in \mathcal{D}(\mathcal{H}_{m,p})$. Thus, $\mathcal{H}_{m,p}^{\mathfrak{g}_1 \times \mathfrak{g}_2}$ is non-degenerate. Since p was arbitrary, we conclude that $\mathfrak{g}_1 \times \mathfrak{g}_2$ is m -great.

For the second part, let $\pi : \mathfrak{g} \rightarrow \mathfrak{h}$ be the factor map. It is straightforward to compute that $\mathcal{H}_{m,p}^{\mathfrak{h}} = \pi \circ \mathcal{H}_{m,p}^{\mathfrak{g}}$. Thus, the coordinates of $\mathcal{H}_{m,p}^{\mathfrak{h}}$ are the image of the coordinates of $\mathcal{H}_{m,p}^{\mathfrak{g}}$ under an epimorphism. We conclude that since $\mathcal{H}_{m,p}^{\mathfrak{g}}$ was non-degenerate, so is $\mathcal{H}_{m,p}^{\mathfrak{h}}$. Therefore, \mathfrak{h} is m -great. \square

5.3. Counter Example. Although m -greatness is a useful property, it has some weaknesses. In particular, although it is expected that on any nilmanifold almost any random walk generated by two translations will be rapid mixing, not all Lie algebras are 2-great. We provide an explicit example of such a Lie algebra.

Example 5.7. Let \mathfrak{g} be a step-4, 15-dimensional Lie algebra with a basis $\{X_1, X_2, X_3, Y_1, Y_2, Y_3, Z_1, \dots, Z_8, W\}$ and the following commutation relations:

$$\begin{aligned}
(5.5) \quad & [X_1, X_2] = Y_1, \quad [X_1, X_3] = Y_2, \quad [X_2, X_3] = Y_3, \\
& [Y_1, X_1] = Z_1, \quad [Y_1, X_2] = Z_2, \quad [Y_1, X_3] = Z_3, \\
& [Y_2, X_1] = Z_4, \quad [Y_2, X_2] = Z_5, \quad [Y_2, X_3] = Z_6, \\
& [Y_3, X_1] = Z_5 - Z_3, \quad [Y_3, X_2] = Z_7, \quad [Y_3, X_3] = Z_8, \\
& [Z_1, X_3] = 3W, \quad [Z_2, X_3] = -3W, \quad [Z_3, X_1] = -W, \\
& [Z_3, X_2] = W, \quad [Z_3, X_3] = -2W, \quad [Z_4, X_2] = -3W, \\
& [Z_5, X_1] = W, \quad [Z_5, X_2] = 2W, \quad [Z_5, X_3] = -W, \\
& [Z_6, X_2] = 3W, \quad [Z_7, X_1] = -3W, \quad [Z_8, X_1] = -3W, \\
& [Y_1, Y_2] = 4W, \quad [Y_1, Y_3] = -4W, \quad [Y_2, Y_3] = -4W,
\end{aligned}$$

while other commutation relations are zero. That these relations actually define a Lie algebra can be verified computationally, but we do not reproduce the calculations here.

Proposition 5.8. \mathfrak{g} is 2-bad.

Proof. We compute that $\mathcal{H}_{2,3} \equiv 0$ even though \mathfrak{g} is step 4. By symmetry, it suffices to check that

$$(5.6) \quad M_{1211} = [[V_1, V_2], V_1], V_1 = 0, \quad M_{1212} = [[V_1, V_2], V_1], V_2 = 0.$$

This may be verified via a computer program, and we present the detailed calculation in Appendix C. \square

This implies that for any nilmanifold which is a quotient of the Lie group associated with \mathfrak{g} , our techniques fail to show rapid mixing of any walk generated by 2 elements. The question of whether such walks are rapid mixing remains open.

APPENDIX A. LEMMA FOR APPLICATION OF DIOPHANTINE ESTIMATE

The following inequality is useful in estimating the norm of \mathcal{L} .

Lemma A.1. *There exists a $C > 0$ such that for all $\theta \in [-1/2, 1/2]$,*

$$(A.1) \quad |1 + e^{2\pi i\theta}| \leq 2 - C\theta^2.$$

Proof. Rearranging, we rewrite (A.1) as

$$C \leq \inf_{\theta \in [-1/2, 1/2]} \frac{(2 - |1 + e^{2\pi i \theta}|)}{\theta^2}.$$

Applying law of cosines and the double angle identity, the inequality becomes

$$C \leq \inf_{\theta \in [-1/2, 1/2]} \frac{2 - 2 \cos(\pi \theta)}{\theta^2}.$$

Note that the singularity of the RHS is removable since it can be rewritten as $g(\theta) := 2 \sum_{n=0}^{\infty} \frac{(\pi \theta)^{2n}}{(2n+2)!}$. Since g is positive and continuous on $[-1/2, 1/2]$ it achieves its minimum value C . \square

We comment that, in fact, the Lemma holds with $C = 8$ but we will not use this in our arguments.

Lemma A.2. *If $v \in DC(\gamma, \tau)$ and λ is a nonzero linear functional with integer coefficients, then there exists $C' > 0$ depending only on γ such that*

$$|1 + e^{2\pi i \lambda(v)}| \leq 2 - C' |\lambda|^{2\tau}.$$

Proof. Based on the Diophantine property of v , $\lambda(v)$ is congruent mod 1 to a number θ in $[-1/2, 1/2]$ satisfying $|\theta| > \gamma |\lambda|^{-\tau}$. It follows by Lemma A.1 that

$$|1 + e^{2\pi i \lambda(v)}| = |1 + e^{2\pi i \theta}| \leq 2 - C \gamma^2 |\lambda|^{-2\tau}.$$

Setting $C' = C \gamma^2$, we have completed the proof. \square

APPENDIX B. CENTRAL LIMIT THEOREM

We say that x_n satisfies CLT if there is $r > 0$ such that for any function $A \in C^r(M)$ with zero mean, $\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} A(x_n)$ converges in distribution to a Gaussian random variable with zero expectations.

Corollary B.1. *If \mathcal{L} satisfies (3.2) then x_n satisfies the CLT.*

While this result is standard we include the proof for completeness.

Proof. Let $B = (1 - \mathcal{L})^{-1} A = \sum_{n=0}^{\infty} \mathcal{L}^n A$. By (3.2) this series converges in C^0 for r large enough. Thus $B(x_n) = A(x_n) + \mathbb{E}(B(x_{n+1}) | \mathcal{F}_n)$ where \mathcal{F}_n is the σ -algebra generated by (x_0, \dots, x_n) . Summing up, we get $\sum_{n=0}^{N-1} A(x_n) = \sum_{n=1}^N \Delta_n + B(x_0) - B(x_N)$ where $\Delta_n = B(x_n) - \mathbb{E}(B(x_n) | \mathcal{F}_{n-1})$ is a martingale difference sequence. Now by the CLT for martingales (see e.g. [8, §8.2]), to prove the CLT, it is sufficient to show that the limit $\sigma^2 := \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=0}^{N-1} q_n$ exists (in probability) where $q_n = \mathbb{E}(\Delta_n^2 | \mathcal{F}_{n-1})$. Note that in our case $q_n = Q(x_{n-1})$ for a continuous function Q so the existence of the limit follows from the ergodicity of our Markov chain. \square

APPENDIX C. LIE ALGEBRA CALCULATION

Here we provide the computations relevant to Proposition 5.8. It suffices to check that $[[[V_1, V_2], V_1], V_1] = [[[V_1, V_2], V_1], V_2] = 0$ since all other triply nested brackets are either necessarily equal to one of these (up to a sign) or forced to be 0. Assume

$$V_1 = \sum_{i=1}^3 \alpha_i X_i, \quad V_2 = \sum_{i=1}^3 \beta_i X_i \text{ and we compute the following.}$$

$$\begin{aligned} [[V_1, V_2], V_1] &= (\alpha_1^2 \beta_2 - \alpha_1 \alpha_2 \beta_1) Z_1 + (\alpha_1 \alpha_2 \beta_2 - \alpha_2^2 \beta_1) Z_2 + (\alpha_1 \alpha_3 \beta_2 - \alpha_2 \alpha_3 \beta_1) Z_3 + \\ &\quad (\alpha_1^2 \beta_3 - \alpha_1 \alpha_3 \beta_1) Z_4 + (\alpha_1 \alpha_2 \beta_3 - \alpha_2 \alpha_3 \beta_1) Z_5 + (\alpha_1 \alpha_3 \beta_3 - \alpha_3^2 \beta_1) Z_6 + \\ &\quad (\alpha_1 \alpha_2 \beta_3 - \alpha_1 \alpha_3 \beta_2)(Z_5 - Z_3) + (\alpha_2^2 \beta_3 - \alpha_2 \alpha_3 \beta_2) Z_7 + (\alpha_2 \alpha_3 \beta_3 - \alpha_3^2 \beta_2) Z_8. \end{aligned}$$

$$\begin{aligned} [[[V_1, V_2], V_1], V_2] &= \left((\alpha_1^2 \beta_2 \beta_3 - \alpha_1 \alpha_2 \beta_1 \beta_3) - 3(\alpha_1 \alpha_2 \beta_2 \beta_3 - \alpha_2^2 \beta_1 \beta_3) - (\alpha_1 \alpha_3 \beta_1 \beta_2 - \alpha_2 \alpha_3 \beta_1^2) \right. \\ &\quad + (\alpha_1 \alpha_3 \beta_2^2 - \alpha_2 \alpha_3 \beta_1 \beta_2) - 3(\alpha_1 \alpha_3 \beta_2 \beta_3 - \alpha_2 \alpha_3 \beta_1 \beta_3) - 3(\alpha_1^2 \beta_2 \beta_3 - \alpha_1 \alpha_3 \beta_1 \beta_2) \\ &\quad + (\alpha_1 \alpha_2 \beta_1 \beta_3 - \alpha_2 \alpha_3 \beta_1^2) + 2(\alpha_1 \alpha_2 \beta_2 \beta_3 - \alpha_2 \alpha_3 \beta_1 \beta_2) - (\alpha_1 \alpha_2 \beta_3^2 - \alpha_2 \alpha_3 \beta_1 \beta_3) \\ &\quad + 3(\alpha_1 \alpha_3 \beta_2 \beta_3 - \alpha_3^2 \beta_1 \beta_2) - 3(\alpha_2^2 \beta_1 \beta_3 - \alpha_2 \alpha_3 \beta_1 \beta_2) - 3(\alpha_2 \alpha_3 \beta_1 \beta_3 - \alpha_3^2 \beta_1 \beta_2) \\ &\quad \left. + 2(\alpha_1 \alpha_2 \beta_1 \beta_3 - \alpha_1 \alpha_3 \beta_1 \beta_2) + (\alpha_1 \alpha_2 \beta_2 \beta_3 - \alpha_1 \alpha_3 \beta_2^2) + (\alpha_1 \alpha_2 \beta_3^2 - \alpha_1 \alpha_3 \beta_2 \beta_3) \right) W = 0. \end{aligned}$$

$$\begin{aligned} [[[V_1, V_2], V_1], V_1] &= \left(3(\alpha_1^2 \alpha_3 \beta_2 - \alpha_1 \alpha_2 \alpha_3 \beta_1) - 3(\alpha_1 \alpha_2 \alpha_3 \beta_2 - \alpha_2^2 \alpha_3 \beta_1) - (\alpha_1^2 \alpha_3 \beta_2 - \alpha_1 \alpha_2 \alpha_3 \beta_1) \right. \\ &\quad + (\alpha_1 \alpha_2 \alpha_3 \beta_2 - \alpha_2^2 \alpha_3 \beta_1) - 3(\alpha_1 \alpha_3^2 \beta_2 - \alpha_2 \alpha_3^2 \beta_1) - 3(\alpha_1^2 \alpha_2 \beta_3 - \alpha_1 \alpha_2 \alpha_3 \beta_1) \\ &\quad + (\alpha_1^2 \alpha_2 \beta_3 - \alpha_1 \alpha_2 \alpha_3 \beta_1) + 2(\alpha_1 \alpha_2^2 \beta_3 - \alpha_2^2 \alpha_3 \beta_1) - (\alpha_1 \alpha_2 \alpha_3 \beta_3 - \alpha_2 \alpha_3^2 \beta_1) \\ &\quad + 3(\alpha_1 \alpha_2 \alpha_3 \beta_3 - \alpha_2 \alpha_3^2 \beta_1) - 3(\alpha_1 \alpha_2^2 \beta_3 - \alpha_1 \alpha_2 \alpha_3 \beta_2) - 3(\alpha_1 \alpha_2 \alpha_3 \beta_3 - \alpha_1 \alpha_3^2 \beta_2) \\ &\quad \left. + 2(\alpha_1^2 \alpha_2 \beta_3 - \alpha_1^2 \alpha_3 \beta_2) + (\alpha_1 \alpha_2^2 \beta_3 - \alpha_1 \alpha_2 \alpha_3 \beta_2) + (\alpha_1 \alpha_2 \alpha_3 \beta_3 - \alpha_1 \alpha_3^2 \beta_2) \right) W = 0. \end{aligned}$$

In other words $M_{1211} = M_{1212} = 0$, so $\mathcal{H}_{2,3} \equiv 0$ even though \mathfrak{g} is step-4.

REFERENCES

- [1] Artur Avila, Giovanni Forni, Davide Ravotti, and Corinna Ulcigrai, *Mixing for smooth time-changes of general nilflows*, Advances in Mathematics **385** (2021), paper 107759.
- [2] Bénard, Timothee, Breuillard, Emmanuel *The central limit theorems on nilpotent Lie groups*, The Annals of Probability **53.2** (2025): 668-719.
- [3] Bénard, Timothee, Breuillard, Emmanuel *Local limit theorems for random walks on nilpotent Lie groups*, Probab. Theory Relat. Fields **192**, 87 5–947 (2025).
- [4] Corwin Lawrence J., Greenleaf Frederick P. *Representations of nilpotent Lie groups and their applications. Part 1: Basic theory and examples*, Cambridge studies in adv. math. **18** (1990) viii+269 pp.
- [5] Diaconis Persi, Hough Robert *Random walk on unipotent matrix groups*, Annales ENS **54** (2021) 587–625.
- [6] Dolgopyat Dmitry *On mixing properties of compact group extensions of hyperbolic systems*, Israel J. Math. **130** (2002) 157–205.
- [7] Dolgopyat Dmitry, Fayad Bassam, Liu Sixu *Multiple Borel-Cantelli lemma in dynamics and multilog law for recurrence*, J. Mod. Dyn. **18** (2022) 209–289.
- [8] Durrett Rick *Probability theory and examples*, 5th ed. Camb. Ser. Stat. Probab. Math. **49** (2019) xii+419 pp.
- [9] Dynkin Eugene *Calculation of the coefficients in the Campbell-Hausdorff formula*. Doklady Akad. Nauk SSSR **57** (1947) 323-326.

- [10] Forni Giovanni *Effective Equidistribution of nilflows and bounds on Weyl sums*, in “Dynamics and Analytic Number Theory”, Proceedings of the Durham Easter School 2014. Editors: D. Badziahin, A. Gorodnik, N. Peyerimhoff, T. Ward. London Mathematical Society, LNS 437. Cambridge University Press, 2017.
- [11] Flaminio Livio, Forni Giovanni *On effective equidistribution for higher step nilflows*. arXiv:1407.3640
- [12] Flaminio Livio, Forni Giovanni *Equidistribution of nilflows and bounds on Weyl sums*. arXiv:2302.03618.
- [13] Furstenberg Hillel, *Strict Ergodicity and Transformation of the Torus*, American J. Math. **83** (1961) 573–601.
- [14] Host Bernard, Kra Bryna *Nilpotent structures in ergodic theory*, AMS Mathematical Surveys and Monographs **236** (2018) 427pp.
- [15] Hough Robert *The local limit theorem on nilpotent lie groups*, Prob. Th. Rel. Fields **174** (2019) 761—786.
- [16] Kim Minsung *Effective equidistribution for generalized higher step nilflows*. Ergodic Theory and Dynamical Systems **42** (2022) 3656–3715.
- [17] Kleinbock, Dmitry Y., Margulis Grigorij A. *Flows on homogeneous spaces and Diophantine approximation on manifolds*. Annals of mathematics (1998): 339-360.
- [18] Raghunathan Madabusi S. *Discrete subgroups of Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete **68** (1972) ix+227 pp, Springer, New York-Heidelberg.
- [19] Ravotti Davide *Mixing for suspension flows over skew-translations and time-changes of quasi-abelian filiform nilflows*, Erg. Th. Dyn. Sys. **38** (2018) 1–30.
- [20] Vergne, Michele. *Cohomologie des algèbres de Lie nilpotentes. Application à l'étude de la variété des algèbres de Lie nilpotentes*. Bulletin de la Société mathématique de France 98 (1970): 81-116.

(DMITRY DOLGOPYAT) UNIVERSITY OF MARYLAND DEPARTMENT OF MATHEMATICS 4176 CAMPUS DRIVE COLLEGE PARK, MD 20742-4015 USA

Email address: `dmitry@umd.edu`

(SPENCER DURHAM) UNIVERSITY OF MARYLAND DEPARTMENT OF MATHEMATICS 4176 CAMPUS DRIVE COLLEGE PARK, MD 20742-4015 USA

Email address: `sdurham4@umd.edu`

(MINSUNG KIM) DEPARTMENT OF MATHEMATICS, KUNGLIGA TEKNISKA HÖGSKOLAN, LINDSTEDTSVÄGEN 25, SE-100 44 STOCKHOLM, SWEDEN

Email address: `minsung@kth.se`