Journal of the Inst. of Math. Jussieu (2011) **10**(1), 37–57
doi:10.1017/S1474748010000150

APPROXIMATE GROUPS. I
THE TORSION-FREE NILPOTENT CASE

EMMANUEL BREUILLARD[1] AND BEN GREEN[2]

[1] *Laboratoire de Mathématiques Université Paris-Sud 11, 91405 Orsay cedex, France* (emmanuel.breuillard@math.u-psud.fr)
[2] *Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WA, UK* (b.j.green@dpmms.cam.ac.uk)

(Received 23 June 2009; accepted 25 January 2010)

Abstract We describe the structure of 'K-approximate subgroups' of torsion-free nilpotent groups, paying particular attention to Lie groups.

Three other works, by Fisher *et al.*, by Sanders and by Tao, have appeared that independently address related issues. We comment briefly on some of the connections between these papers.

Keywords: approximate group; nilpotent progression; additive combinatorics; Freiman's theorem

AMS 2010 *Mathematics subject classification:* Primary 11B30

Contents

1. Introduction

Approximate groups

A fair proportion of the subject of additive combinatorics is concerned with approximate analogues of exact algebraic properties, and the extent to which they resemble those algebraic properties. In this paper we are concerned with approximate groups.

By an *ambient group* we simply mean some group in which all the objects being discussed are contained, so that it makes sense to talk about multiplication of elements, inverses and the identity element. Suppose that A is a finite set in some ambient group. What does it mean to say that A is an approximate subgroup?

It is well known to all students of group theory that A is a genuine subgroup if, and only if, we have $xy^{-1} \in A$ whenever $x, y \in A$. Perhaps the most natural way in which a set A may be *approximately* a subgroup, then, is if the set $AA^{-1} = \{xy^{-1} : x, y \in A\}$ has cardinality not much bigger than $|A|$, perhaps $|AA^{-1}| \leqslant K|A|$ for some constant K.

Sets with this property are said to have *small doubling* and this is indeed a commonly encountered condition in additive combinatorics. It is a perfectly workable notion of approximate group in the abelian setting and the celebrated Freĭman–Ruzsa theorem describes subsets of $\mathbb{Z}$ with this property (we will state it below). However, in the foundational work of Tao [**18**] it was noted that in noncommutative settings a somewhat different, though closely related, notion of approximate group is more natural. We now give Tao's definition.

Definition 1.1 (approximate groups). Let $K \geqslant 1$. A set A in some ambient group is called a K-approximate group if

(i) it is symmetric, i.e. if $a \in A$ then $a^{-1} \in A$, and the identity lies in A;

(ii) there is a symmetric subset X lying in $A \cdot A$ with $|X| \leqslant K$ such that $A \cdot A \subseteq X \cdot A$.

This definition gives rise to some very pleasant properties, and we shall list them in § 3. In that section we also briefly recall the relation between approximate groups in this sense and sets with small doubling.

Our aim in this paper is to 'describe' the structure of approximate subgroups of torsion-free nilpotent groups in terms of more explicit algebraic objects. A companion paper [**2**] tackles the same question for solvable subgroups of $\mathrm{GL}_d(\mathbb{C})$. Tao [**19**] has addressed questions of this type, working in fact with solvable groups in general. In his paper he introduces the following rather nice paradigm for 'describing' sets by others.

Definition 1.2 (control). Suppose that A and B are two sets in some ambient group, and that $K \geqslant 1$ is a parameter. We say that A is K-controlled by B, or that B K-controls A, if $|B| \leqslant K|A|$ and there is some set X in the ambient group with $|X| \leqslant K$ and such that $A \subseteq (X \cdot B) \cap (B \cdot X)$.

This is essentially equivalent to saying that A and B have roughly the same size and that A is covered by a few left-translates of B and also by a few right-translates of B. Indeed if $A \subseteq \bigcup_{i=1}^{k} x_i B$ and also $A \subseteq \bigcup_{j=1}^{l} B y_j$, then we may take $X = \{x_1, \dots, x_k, y_1, \dots, y_l\}$ in the definition above; the other direction of the equivalence is even more obvious.

In § 3 we will discuss (following Tao's paper extremely closely) how this notion of control interacts with the aforementioned notions of approximate group and small doubling.

The structure of approximate subgroups of torsion-free *abelian* groups is described by the Freĭman–Ruzsa theorem [**7**, **15**]. The bounds in the following version of it, which is

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

stated in the language introduced above, are due to Chang [**3**]. Here and for the remainder of the paper the letter C represents an absolute constant which could be computed explicitly if desired: different instances of the letter may denote different constants. We will often use subscripts to indicate dependence on other parameters: for example, C_s is an absolute constant depending on s.

Theorem 1.3 (Freĭman–Ruzsa; Chang). *Let G be a torsion-free abelian group and let $K \geqslant 1$ be a parameter. Suppose that $A \subseteq \mathbb{Z}$ is a K-approximate group. Then A is e^{CK^C}-controlled by a set P of the form*

$$P = \{l_1x_1 + \cdots + l_kx_k : |l_1| \leqslant L_1, \ldots, |l_k| \leqslant L_k\},$$

for some $x_1, \ldots, x_k \in \mathbb{Z}$, where $k \leqslant CK^C$.

A set P of this form is called a *generalized arithmetic progression*, or progression for short.* The number k is referred to as the *dimension* of k.

The Freĭman–Ruzsa theorem is usually stated and proved only for subsets of $\mathbb{Z}$ and not for torsion-free abelian groups in general. Simple modifications allow one to obtain the more general statement, and we will remark further on this later on.

Let us turn now to nilpotent groups, pausing to recall the definition. Let G be a group and suppose that $s \geqslant 1$ is an integer. If the lower central series defined by

$$G_0 = G_1 = G, \quad G_2 = [G, G_1], \quad G_3 = [G, G_2], \quad \ldots$$

terminates with $G_{s+1} = \{\mathrm{id}_G\}$, then we say that G is s-step nilpotent. A prototypical example of a torsion-free nilpotent group G is a group of upper triangular matrices with ones on the diagonal, such as the Heisenberg group

$$G = \begin{pmatrix} 1 & \mathbb{R} & \mathbb{R} \\ 0 & 1 & \mathbb{R} \\ 0 & 0 & 1 \end{pmatrix},$$

which is an example of a 2-step nilpotent (Lie) group.

Here is an example of an approximate subgroup of the Heisenberg group. It is also discussed quite explicitly in Tao's paper [**19**].

Take

$$u_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad u_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

and consider also the commutator

$$[u_1, u_2] := u_1^{-1}u_2^{-1}u_1u_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

* There is a very slight difference between the terminology used in this paper and that which is standard: typically, a progression is a set of the form $\{x_0 + l_1x_1 + \cdots + l_kx_k : 0 \leqslant l_i < L_i\}$. We have found it convenient to disallow the presence of x_0 in this paper and to use the more symmetric condition $|l_i| \leqslant L_i$. Note, however, that every progression in our sense is economically contained in one according to the more standard definition, and vice versa (though one might need to increase the dimension by 1).

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Let $L_1, L_2 \geqslant 1$ be integers. Then the set $A := \{u_1^{l_1} u_2^{l_2} [u_1, u_2]^{l_{12}} : |l_1| \leqslant L_1,\ |l_2| \leqslant L_2,\ |l_{12}| \leqslant L_1 L_2\}$ consists of the matrices

$$\left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : |x| \leqslant L_1,\ |y| \leqslant L_2,\ |z| \leqslant L_1 L_2 \right\}$$

and it is not hard to check that $A \cup A^{-1}$ is a K-approximate group for some absolute constant K.

The set A is obviously a close analogue of the generalized progressions considered in the abelian setting. The construction may be generalized, but to do this we must first discuss commutators in more detail. Suppose that G is an s-step nilpotent group and that $u_1, \dots, u_k \in G$. We may inductively assign a *weight vector* $\chi \in \mathbb{N}_0^k$ to every (formal) commutator involving the u_is by setting $\chi(u_i) = e_i$ and defining χ inductively on higher commutators via $\chi([c, c']) = \chi(c) + \chi(c')$. Thus if $k = 4$ then $\chi([u_1, u_2]) = (1, 1, 0, 0)$ and $\chi([u_1, [u_2, u_4]]) = (1, 1, 0, 1)$. We follow Hall [**10**, Chapter 11] in defining *basic commutators*. This is a (non-unique) extension of $u_1, \dots, u_k$ to an ordered list $u_1 \prec \cdots \prec u_t$ in which $u_{k+1}, \dots$ are certain commutators involving $u_1, \dots, u_k$. We suppose that they are ordered so that commutators with the same weight vector are consecutive, and so that higher-order commutators come before lower order ones. If c_i, c_j have already been admitted as basic commutators then $c_k = [c_i, c_j]$ qualifies as basic if $c_i \succ c_j$ and if, writing $c_i = [c_s, c_t]$, $c_j \succeq c_t$.

For example when $k = s = 3$ we have $t = 14$, a possible listing of the basic commutators being u_1, u_2, u_3, $[u_2, u_1]$, $[u_3, u_2]$, $[u_3, u_1]$, $[[u_2, u_1], u_1]$, $[[u_2, u_1], u_2]$, $[[u_2, u_1], u_3]$, $[[u_3, u_1], u_1]$, $[[u_3, u_1], u_2]$, $[[u_3, u_1], u_3]$, $[[u_3, u_2], u_2]$, $[[u_3, u_2], u_3]$. Note incidentally the formula of Witt, which states that the number of basic commutators of order r on k generators is

$$\frac{1}{r} \sum_{d|r} \mu(d) k^{r/d}.$$

Write $\chi(j)$ for the weight vector of the commutator u_j. If $L = (L_1, \dots, L_k)$ is a vector of positive integers and $\chi \in \mathbb{N}_0^k$, we define $L^\chi := L_1^{\chi_1} \cdots L_k^{\chi_k}$.

Definition 1.4 (nilpotent progressions). Suppose that G is an s-step nilpotent group and that $u_1, \dots, u_k \in G$. Let $L = (L_1, \dots, L_k)$ be a vector of positive integers. Then the nilpotent progression $P(u_1, \dots, u_k; L)$ on generators $u_1, \dots, u_k$ with lengths L is the set $\{u_1^{l_1} \cdots u_t^{l_t} : |l_j| \leqslant L^{\chi(j)}\}$, where $u_1, u_2, \dots, u_t$ is the ordered list of basic commutators involving the u_i.

Any s-step nilpotent progression is the homomorphic image of a nilpotent progression in $\Gamma_{k,s}$, the *free* s-step nilpotent group on k generators. We have found this to be the right way to think about nilpotent progressions: to study them, one should establish homomorphism-invariant properties of nilpotent progressions in the free nilpotent group.

Consideration of the free case reveals our reason for involving only *basic* commutators, since by restricting to these the elements $u_1^{l_1} \cdots u_t^{l_t}$ of a nilpotent progression in the free nilpotent group are all distinct. This follows from the results of [**10**, Chapter 11].

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

We are now in a position to state our main theorem, which is the analogue of the Freĭman–Ruzsa theorem in the nilpotent setting.

Theorem 1.5. *Let Γ be a torsion-free s-step nilpotent group, and suppose that $A \subseteq \Gamma$ is a K-approximate subgroup. Then there are elements $u_1, \dots, u_k \in \Gamma$, $k \leqslant K^{C_s}$, and lengths $L = (L_1, \dots, L_k)$ such that A is $\mathrm{e}^{K^{C_s}}$-controlled by the nilpotent progression $P(u_1, \dots, u_k; L)$.*

The proof of this theorem occupies the majority of the paper. However, in the later sections we gather some properties of nilpotent progressions which may be of interest in their own right. We also comment on the connection between our results and those of Sanders [**16**].

2. Strategy of the proof

The key idea for establishing Theorem 1.5, already implicit in [**18**] and described explicitly in [**6**], is to use a little Lie theory. We may clearly suppose, in proving Theorem 1.5, that Γ is finitely generated. An embedding theorem of Mal'cev [**14**] states that every finitely generated torsion-free nilpotent group embeds as a co-compact discrete subgroup of a simply connected nilpotent Lie group of the same step. It therefore suffices to establish Theorem 1.5 when Γ is a subgroup of a simply connected s-step nilpotent Lie group, say G (the Heisenberg group is an example of such a group).

Working in this setting enables us to exploit the Lie algebra $\mathfrak{g} = \log G$. It is well known in the theory of simply connected nilpotent Lie groups (see, for example, [**1**]) that there are mutually inverse diffeomorphisms $\exp : \mathfrak{g} \to G$ and $\log : G \to \mathfrak{g}$ between the group G and its Lie algebra $\mathfrak{g}$, which is a vector space $\mathbb{R}^{\dim(G)}$ together with an additional bracket operation $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ which is antisymmetric, bilinear and satisfies the Jacobi identity.

In the case of the Heisenberg group we may identify $\mathfrak{g}$ with the vector space

$$\begin{pmatrix} 0 & x & z \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix}.$$

The exponential map $\exp : \mathfrak{g} \to G$ is then simply the usual exponentiation of matrices.

In the Lie algebra setting it is quite natural to consider a different type of nilpotent progression which, to distinguish it from the nilpotent progressions already described, we call a *nilbox*. To define nilboxes we must first describe commutators in $\mathfrak{g}$.

We consider first the free nilpotent Lie algebra $\mathfrak{n}_{k,s}$ with generators $X_1, \dots, X_k$. We will be looking at higher-order commutators such as $[X_1, [X_2, X_5]]$, and once again we will associate a weight vector $\chi \in \mathbb{N}_0^k$ to each of these. The definition is the same as before (in the example just given, $\chi = (1, 1, 0, 0, 1, \dots)$). We have a decomposition $\mathfrak{n}_{k,s} = \bigoplus_\chi V_\chi$ into *weight spaces* V_χ, where V_χ consists of commutators with a fixed weight χ. Just as for group commutators, we may extend $X_1, \dots, X_k$ to an ordered list $X_1, \dots, X_t$ of *basic commutators*. The definition of these is precisely the same as for group commutators,

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

except that the bracket now refers to the Lie algebra operation rather than the group commutator.

The reason for introducing *basic* commutators becomes clear in this context: by a theorem of Witt [**10**, Chapter 11] the elements $X_1, \dots, X_t$ form a basis for $\mathfrak{n}_{k,s}$ as a vector space over $\mathbb{C}$. We call this an *adapted basis* for $\mathfrak{n}_{k,s}$.

Definition 2.1 (free nilboxes). Let $k, s \geqslant 1$ be integers, and let $X_1, \dots, X_k$ be generators for the free nilpotent Lie algebra $\mathfrak{n}_{k,s}$. Let $L = (L_1, \dots, L_k)$ be a vector of positive integer lengths. Then the free s-step nilbox with lengths L is the set $\mathfrak{B}(X_1, \dots, X_k; L) \subseteq \mathfrak{n}_{k,s}$ defined by

$$\mathfrak{B}(X_1, \dots, X_k; L) = \{l_1 X_1 + \cdots + l_t X_t : |l_j| \leqslant L^{\chi(j)}\},$$

where $X_1, \dots, X_t$ is an adapted basis for $\mathfrak{n}_{k,s}$.

Definition 2.2 (nilboxes). Let $\mathfrak{g}$ be an s-step nilpotent Lie algebra and suppose that $x_1, \dots, x_k \in \mathfrak{g}$. Let $L = (L_1, \dots, L_k)$ be a vector of positive integer lengths. Then we define the nilbox $\mathfrak{B}(x_1, \dots, x_k; L)$ to be the image $\pi(\mathfrak{B}(X_1, \dots, X_k; L))$, where $\pi : \mathfrak{n}_{k,s} \to \mathfrak{g}$ is the Lie algebra homomorphism induced by mapping X_i to x_i, $i = 1, \dots, k$. It is convenient to write $x_i := \pi(X_i)$ for $i = k+1, \dots, t$ also.

As we remarked, it suffices to prove Theorem 1.5 when Γ is a subgroup of a simply connected s-step nilpotent Lie group G. We may now divide this task into the task of proving the following two propositions.

Proposition 2.3 (control by nilboxes). *Suppose that G is an s-step simply connected nilpotent Lie group with Lie algebra $\mathfrak{g}$, and that $A \subseteq G$ is a K-approximate group. Then there are $x_1, \dots, x_k \in \mathfrak{g}$ such that*

(i) $k \leqslant K^{C_s}$;

(ii) $\exp(x_1), \dots, \exp(x_t)$ *lie in the group $\langle A \rangle$ generated by A;*

(iii) *there is a nilbox $\mathfrak{B}(x_1, \dots, x_k; L)$ such that $\exp(\mathfrak{B}(x_1, \dots, x_k; L))$ $\mathrm{e}^{K^{C_s}}$-controls A.*

Proposition 2.4 (nilpotent progressions control nilboxes). *Suppose that G is an s-step simply connected nilpotent Lie group with Lie algebra $\mathfrak{g}$. Suppose that $x_1, \dots, x_k \in G$, and write $u_i := \exp(x_i)$. Let $L = (L_1, \dots, L_k)$ be a vector of positive integer lengths. Then the nilpotent progression $P(u_1, \dots, u_k; L)$ $\mathrm{e}^{k^{C_s}}$-controls $\exp(\mathfrak{B}(x_1, \dots, x_k; L))$.*

Theorem 1.5 clearly follows from the combination of the last two propositions after we observe that the nilpotent progression $P(u_1, \dots, u_k; L)$ obtained in Proposition 2.4 entirely lies in Γ and that if A and B are two subsets of the subgroup Γ and A is K-controlled by B in G, then A must also be K-controlled by B in Γ.

Either proposition is conceivably of independent interest. For example it seems to be easier to study nilboxes than nilpotent progressions. The proof of Proposition 2.3 is essentially additive–combinatorial and occupies the next four sections. The proof of Proposition 2.4 requires a certain amount of material on coordinates in nilpotent Lie

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

groups: this material is summarized in Appendix B and the proposition itself is confirmed in § 7.

To conclude this section let us note that there is a certain arbitrariness in the definitions of nilpotent progression and nilbox, coming from the non-canonical choice of an ordering for the basic commutators (or indeed for the basic commutators themselves, which are defined in different ways by different authors). This is not a serious matter and any other choice would lead to completely equivalent theorems.

3. Preliminaries from multiplicative combinatorics

We take the opportunity to record some basic facts about noncommutative product sets, and in particular concerning the notions of K-approximate group and K-control defined in the introduction. This material is all due to Tao [**18**]; in turn some of that is based on earlier work of Ruzsa in the abelian setting. See also the book of Tao and Vu [**20**], especially § 2.7.

Proposition 3.1 (approximate groups and control). *Let $K \geqslant 1$ be a parameter and let A be a set in some ambient group G. If $n \geqslant 1$ is an integer we write $A^n = \{a_1 \cdots a_n : a_1, \dots, a_n \in A\}$ and $A^{\pm n} = \{a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n} : a_1, \dots, a_n \in A,\ \varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}\}$.*

(i) *If $\pi : G \to H$ is a homomorphism and if $A \subseteq G$ is a K-approximate group, then $\pi(A)$ is a K-approximate subgroup of H.*

(ii) *If A is a K-approximate group, then $|A^{\pm n}| = |A^n| \leqslant K^{n-1}|A|$ and A^n is K^{n+1}-controlled by A.*

(iii) *If B, C are further subsets of G and if A is K-controlled by B and B is K-controlled by C, then A is K^2-controlled by C.*

(iv) *If A and B are K-approximate groups and A is K-controlled by B, then B is K^4-controlled by A.*

(v) *If the doubling constant $|A^2|/|A|$ is at most K, then there is an $f_1(K)$-approximate group $B \subseteq A^{\pm 3}$ which $f_2(K)$-controls A. If the tripling constant $|A^3|/|A|$ is at most K, then we may take $B = A^{\pm 3}$.*

(vi) *If A is a K-approximate group and if $A' \subseteq A$ is a subset with $|A'| \geqslant |A|/K$, then $A'^{\pm 3}$ is an $f_3(K)$-approximate group which $f_4(K)$-controls A. The same is in fact true under the essentially weaker assumption that $|A^3| \leqslant K|A|$.*

All of the quantities $f_1(K), \dots, f_4(K)$ can be taken to be polynomial in K.

Proof. Part (i) follows immediately from the definition. To prove (ii), suppose that X is a symmetric set such that $|X| \leqslant K$ and $A \cdot A \subseteq X \cdot A$. Then, since A is symmetric, we also have $A \cdot A \subseteq A \cdot X$ and hence $A^n \subseteq X^{n-1} \cdot A$ and $A^n \subseteq A \cdot X^{n-1}$ for all $n \geqslant 1$ by an easy induction, from which the result follows immediately.

Part (iii) is very easy and follows straight from the definitions. Part (iv) follows from the non-abelian Ruzsa covering lemma [**18**, Lemma 3.6]. Parts (v) and (vi) may be

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

found in [**18**]: (v) is Theorem 4.6 and Corollary 3.10 of that paper, while (vi) follows from Lemma 3.6 and Corollary 3.10. □

4. Generalized arithmetic progressions in Lie algebras

Let $\mathfrak{g}$ be an s-step nilpotent Lie algebra and let $\mathfrak{p} \subseteq \mathfrak{g}$ be a progression, thus

$$\mathfrak{p} = \{l_1x_1 + \cdots + l_kx_k : |l_i| \leqslant L_i\}$$

for some lengths $L_1, \ldots, L_k$ and some $x_1, \ldots, x_k \in \mathfrak{g}$. Our aim is to understand ways in which $\mathfrak{p}$ can interact with the bracket operation $[\cdot\,,\cdot]$.

We begin with a definition.

Definition 4.1 (nilcompletion). Suppose that $\mathfrak{b} \subseteq \mathfrak{g}$ is a set. Then by the *nilcompletion* $\bar{\mathfrak{b}}$ of $\mathfrak{b}$ we mean the set $\mathfrak{b} + [\mathfrak{b},\mathfrak{b}] + [\mathfrak{b},[\mathfrak{b},\mathfrak{b}]] + \cdots + [[\mathfrak{b},\mathfrak{b}],[\mathfrak{b},[\mathfrak{b},\mathfrak{b}]]] + \cdots$, where the sum is over all* commutators.

Now it is known from standard Lie theory that if $\mathfrak{g}_i := \log(G_i)$ then $[\mathfrak{g}_i,\mathfrak{g}_j] \subseteq \mathfrak{g}_{i+j}$, and so any commutator with more than s copies of $\mathfrak{b}$ vanishes identically. The number of commutators of order $k+1$ is the kth Catalan number

$$C_k = \frac{1}{k+1}\binom{2k}{k}.$$

We easily see that the total number of such up to order s can be bounded above by 4^s.

Lemma 4.2 (properties of the nilcompletion). *Let $\mathfrak{b} \subseteq \mathfrak{g}$ be a set. Then*

(i) *for any integer $m \geqslant 1$ we have $\overline{m\mathfrak{b}} \subseteq m^s\bar{\mathfrak{b}}$;*

(ii) $[\bar{\mathfrak{b}},\bar{\mathfrak{b}}] \subseteq \bar{\mathfrak{b}}$.

Proof. The first inclusion is a consequence of the fact that an s-fold commutator is s-multilinear. For example (when $m = 2$), $[b_1 + b_1', b_2 + b_2']$ may be written as a sum of four commutators involving only elements of $\mathfrak{b}$. The second is also immediate, and it is the main reason for introducing this definition of nilcompletion. □

Now if $\mathfrak{p}$ is a progression then its nilcompletion $\bar{\mathfrak{p}}$ need not be in general. Proposition 4.4 below is a good substitute for the failure of this statement, however. Before stating it we record a simple number-theoretic lemma that we will use several times in the sequel.

Lemma 4.3. *Suppose that $L_1, \ldots, L_k$ are integers. Then every non-negative integer less than or equal to $L_1 \cdots L_k$ can be written as the sum of at most 2^{k-1} numbers of the form $l_1 \cdots l_k$ with $1 \leqslant l_i \leqslant L_i$ for $i = 1, \ldots, k$.*

Proof. This may be established by induction on k from the base case $k = 2$: to prove that case, write a given m as $qL_2 + r$, where $0 \leqslant q < L_1$ and $1 \leqslant r \leqslant L_2$. □

* In this paper we are not concerned with the dependence of our estimates on the step parameter s. If we were, it might be more efficient at this point to take only *nested* commutators into account in making this definition.

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Proposition 4.4. *Suppose that* $\mathfrak{p} \subseteq \mathfrak{g}$ *is a* progression *of dimension* k *and that* $\bar{\mathfrak{p}}$ *is its nilcompletion. Then there is a* progression $\mathfrak{q}$ *of dimension at most* $(4k)^s$ *such that* $[\mathfrak{q},\mathfrak{q}] \subseteq (2k)^{2s}\mathfrak{q}$ *and* $\bar{\mathfrak{p}} \subseteq \mathfrak{q} \subseteq (2k)^s\bar{\mathfrak{p}}$.

Proof. Suppose as usual that $\mathfrak{p}$ has generators $x_1,\dots,x_k$. Then

$$\mathfrak{b} \subseteq \mathfrak{p} \subseteq k\mathfrak{b}, \tag{4.1}$$

where

$$\mathfrak{b} := \bigcup_{i=1}^{k} \{l_i x_i : |l_i| \leqslant L_i\}.$$

Let $\mathcal{C}$ be the set of all commutators in the x_is, such as $[[x_1,x_7],[x_3,x_5]]$. To each $c \in \mathcal{C}$ we may assign a weight vector $\chi(c) \in \mathbb{N}_0^k$ much as described in the introduction; for this example, $\chi = (1,0,1,0,1,0,1,0,0,\dots)$. We first claim that

$$\bar{\mathfrak{b}} \subseteq \mathfrak{r} \subseteq 2^{s-1}\bar{\mathfrak{b}}, \tag{4.2}$$

where $\mathfrak{r}$ is the progression defined by

$$\mathfrak{r} = \Big\{ \sum_{c\in\mathcal{C}} l_c c : |l_c| \leqslant L^{\chi(c)} \Big\},$$

where

$$L^{\chi(s)} := \prod_{i=1}^{k} L_i^{(\chi(s))_i}.$$

The first inclusion is clear. To see the second, we invoke Lemma 4.3. Now $\bar{\mathfrak{b}}$ contains all elements of the form $l^{\chi(c)}c$, provided $|l_i| \leqslant L_i$ for all $i = 1,\dots,k$. Hence by our observation we must have $\mathfrak{r} \subseteq n\bar{\mathfrak{b}}$ where $n = 2^{s-1}$. This proves (4.2).

Now from (4.1), (4.2) and Lemma 4.2 (i) we have $\bar{\mathfrak{p}} \subseteq k^s\bar{\mathfrak{b}} \subseteq k^s\mathfrak{r}$. This last set $k^s\mathfrak{r}$ is another progression, and this we take to be $\mathfrak{q}$. Specifically,

$$\mathfrak{q} = k^s\mathfrak{r} = \Big\{ \sum_{c\in\mathcal{C}} l_c c : |l_c| \leqslant k^s L^{\chi(c)} \Big\}.$$

The dimension of $\mathfrak{q}$ is $|\mathcal{C}|$, which is less than or equal to $(4k)^s$, since as we observed earlier, the total number of bracketing patterns of length at most s is less than or equal to 4^s. Now by construction we have $\bar{\mathfrak{p}} \subseteq \mathfrak{q}$. Finally, (4.1) and (4.2) yield $\mathfrak{q} = k^s\mathfrak{r} \subseteq (2k)^s\bar{\mathfrak{b}} \subseteq (2k)^s\bar{\mathfrak{p}}$, as required.

It remains to show that $[\mathfrak{q},\mathfrak{q}]$ is contained in an appropriate multiple of $\mathfrak{q}$. This now follows from the fact that $[m\mathfrak{b},m\mathfrak{b}] \subseteq m^2[\mathfrak{b},\mathfrak{b}]$ for any set $\mathfrak{b} \subseteq \mathfrak{g}$ and from Lemma 4.2. □

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

5. Some nilpotent algebra

In this section we establish some results about nilpotent Lie groups and their interaction with their Lie algebras via the exponential map. Throughout this section, then, G is a simply connected s-step nilpotent Lie group.

One of the key tools in this paper is a theorem of Lazard [**11**, **12**], given in Lemma 5.2 below, stating that both addition and the bracket operation on $\mathfrak{g}$ may be expressed using words in G of length C_s. This consequence of the Baker–Campbell–Hausdorff formula was discussed in detail in the 1969 thesis of Ian Stewart (see also [**17**]). Results of this type were first exploited in the additive–combinatorial setting by Fisher *et al.* [**6**].

We shall also need the following lemma on rational powers in nilpotent Lie groups.

Lemma 5.1 (rational powers of products). *Suppose that G is an s-step nilpotent Lie group and that $x_1, \dots, x_t \in G$. Let $\eta \in \mathbb{Q}$. Then there is an integer t' and for $j \in \{1, \dots, t'\}$ there are polynomials $P_j(\eta) \in \mathbb{Q}[\eta]$ drawn from a finite list depending only on s such that $(x_1 \cdots x_t)^\eta = x_{i_1}^{P_1(\eta)} \cdots x_{i_{t'}}^{P_{t'}(\eta)}$ for some indices $i_j \in \{1, \dots, t\}$.*

Proof. This follows from the Hall–Petresco formula as presented, for example, in [**10**, Theorem 12.3.1] or [**5**, Appendix A]. This formula states (for an arbitrary s-step nilpotent group) that there are words $w_2(x_1, x_2, \dots, x_t), \dots, w_s(x_1, x_2, \dots, x_t)$ such that $w_j \in G_j$ and

$$(x_1 \cdots x_t)^n = x_1^n x_2^n \cdots x_t^n w_2(x_1, \dots, x_t)^{\binom{n}{2}} \cdots w_s(x_1, \dots, x_t)^{\binom{n}{s}}$$

for all positive integers n. By induction on the step of G, this implies that there are polynomials $P_j(n)$ with coefficients in $\mathbb{Q}$ depending only on s such that $(x_1 \cdots x_t)^n = \prod_{1 \leqslant j \leqslant t'} x_{i_j}^{P_j(n)}$, where $i_j \in \{1, \dots, t\}$ for $j = 1, \dots, t'$. If G is a Lie group then by Ado's theorem one can embed G into a group of upper triangular matrices, in which setting the matrix entries of both sides of the preceding formula are polynomials. It follows that this formula is in fact valid with n replaced by an arbitrary real number η. □

Lemma 5.2 (Lazard). *There is a sequence of rational numbers $\alpha_1, \beta_1, \dots, \alpha_m, \beta_m$, depending only on s, such that, for all $x, y \in G$,*

$$\exp(\log x + \log y) = x^{\alpha_1} y^{\beta_1} \cdots x^{\alpha_m} y^{\beta_m}.$$

Similarly there is a sequence of rational numbers $\gamma_1, \delta_1, \dots, \gamma_m, \delta_m$ such that, for all $x, y \in G$,

$$\exp([\log x, \log y]) = x^{\gamma_1} y^{\delta_1} \cdots x^{\gamma_m} y^{\delta_m}.$$

Proof. This is not quite the result stated in [**17**], for example, where the expressions obtained are of the form $w_1(x, y)^{\eta_1} w_2(x, y)^{\eta_2} \cdots w_m(x, y)^{\eta_m}$ with each w_i a word in x and y (and x^{-1}, y^{-1}) and the η_i rational numbers. However, it follows immediately from that formulation and Lemma 5.1. □

It follows immediately from the last two lemmas that there is a similar expression for $\exp(\log x_1 + \cdots + \log x_n)$. In order to get the right bound for the last part of Theorem 1.5 we will require a certain amount of control over what this expression is.

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Lemma 5.3 (expansion of sums). *Let G be an s-step nilpotent Lie group and suppose that $x_1, \dots, x_n \in G$, where $n \geqslant 2$. Then there is a sequence of rational numbers $\alpha_1, \dots, \alpha_m$ depending on n, all of which may be put over a common denominator of size bounded by n^{C_s}, and a collection of indices $i_1, \dots, i_m \in \{1, \dots, n\}$ such that*

$$\exp(\log x_1 + \cdots + \log x_n) = x_{i_1}^{\alpha_1} \cdots x_{i_m}^{\alpha_m}.$$

Proof. It clearly suffices to establish this when n is a power of two: if n is not a power of two, let n'^r be the least power of two greater than n and take $x_{n+1} = \cdots = x_{n'} = \mathrm{id}_G$. To establish this case we proceed inductively, relating the expansion for $n = k$ to that for $n = 2k$. We have

$$\exp(\log x_1 + \cdots + \log x_k) = x_{i_1}^{\alpha_1} \cdots x_{i_m}^{\alpha_m}$$

and

$$\exp(\log x_{k+1} + \cdots + \log x_{2k}) = x_{j_1}^{\alpha_1} \cdots x_{j_m}^{\alpha_m},$$

where the α_i may all be put over some denominator Q. Applying the first of Lazard's expansions we may expand $\exp(\log x_1 + \cdots + \log x_{2k})$ as a product of terms of the preceding type, each to some rational power over some fixed denominator q_s depending only on s. Now expand each of *those* using Lemma 5.1: this results in an expansion of $\exp(\log x_1 + \cdots + \log x_{2k})$ as a product of terms $x_{i_j}^{\beta_j}$, where all of the β_j may be put over denominator Qq_s' for some integer q_s' depending only on s. The result follows immediately by induction. □

6. Control by a nilbox

In this section we prove Proposition 2.3, the statement that an approximate subgroup of an s-step nilpotent Lie group G is controlled by a nilbox. Recall that this, together with Proposition 2.4, implies our main result.

Throughout this section G is a simply connected nilpotent Lie group and $A \subseteq G$ is a K-approximate group. We write $\mathfrak{a} = \log A = \{\log x : x \in A\}$ for the corresponding subset of the Lie algebra $\mathfrak{g}$. Fisher *et al.* [**6**] used results close to those of the previous section to prove that $\mathfrak{a}$ is close to invariant under both addition and Lie bracket. We essentially recover this result in Lemma 6.1 below. In their paper it was also remarked that one might apply the Freĭman–Ruzsa theorem in this setting, and we shall see how this suggestion may be realized and used to prove Proposition 2.3. Some of the ideas here were also anticipated by the foundational work of Tao [**18**]: in the last part of this paper he described sets of small tripling in the Heisenberg group as being precisely the sets that are roughly closed under both addition and commutation, a fact he deduced by applying what amounts to the Baker–Campbell–Hausdorff formula in this case.

Lemma 6.1 ($\mathfrak{a}$ is almost invariant under nilcompletion). *Let $\bar{\mathfrak{a}}$ be the nilcompletion of $\mathfrak{a}$. Then $|\mathfrak{a} + \bar{\mathfrak{a}}| \leqslant K^{C_s}|\mathfrak{a}|$. More generally, $|m\bar{\mathfrak{a}}| \leqslant K^{mC_s}|\mathfrak{a}|$ for all $m \in \mathbb{N}$.*

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Proof. It follows from Lemmas 5.2 and 5.1 that, for any $x_1, x_2, \ldots \in G$, we have

$$\exp(\log x_1 + \log x_2 + [\log x_3, \log x_4] + [\log x_5, [\log x_6, \log x_7]] + \cdots) = x_1^{\eta_1} x_2^{\eta_2} \cdots x_M^{\eta_M}$$

for some rationals $\eta_1, \eta_2, \ldots, \eta_M$ and $M = C_s$. Here, all of the commutators appearing in the definition of nilcompletion are featured. Choose some integer $Q = C_s$ such that all of the rationals η_i may be put over the common denominator Q, and set $B := \{a^Q, a^{Q^2}, \ldots, a^{Q^s} : a \in A\}$ and $\mathfrak{b} = \log B$. Then every element of $\exp(\mathfrak{b} + \bar{\mathfrak{b}})$ lies in A^{C_s}, and hence by the iterated product set estimate (see Proposition 3.1) we have $|\mathfrak{b} + \bar{\mathfrak{b}}| \leqslant K^{C_s}|A|$.

Now suppose that $x \in \mathfrak{a}$. Then, noting that $\log(g^t) = t \log g$, we see that all of $Qx, Q^2x, \ldots, Q^sx$ lie in $\mathfrak{b}$. Hence if $x_1, x_2, x_3, \ldots \in \mathfrak{a}$ then

$$\begin{aligned} Q^s(x_1 + x_2 + [x_3 + x_4] + [x_5, [x_6, x_7]] + \cdots) \\ = Q^s x_1 + Q^s x_2 + [Q^{s-1} x_3, Q x_4] + [Q^{s-2} x_5, [Q x_6, Q x_7]] + \cdots \end{aligned}$$

lies in $\mathfrak{b} + \bar{\mathfrak{b}}$, that is to say $Q^s(\mathfrak{a} + \bar{\mathfrak{a}}) \subseteq (\mathfrak{b} + \bar{\mathfrak{b}})$. The dilation map $Q^s : \mathfrak{g} \to \mathfrak{g}$ is, of course, a bijection and so the result follows immediately. The last claim follows immediately from the Ruzsa triangle inequality [**20**, (2.6)] and its associated sum-set estimates [**20**, Corollary 2.23]. □

At this point we apply the Freĭman–Ruzsa theorem, stated as Theorem 1.3 in the introduction. We will need a slightly stronger version of this theorem than is commonly stated in the literature.

Theorem 1.3′. *Suppose that X is a K-approximate subgroup of $\mathbb{R}^m$. Then there is a progression*

$$P = \{l_1 x_1 + \cdots + l_k x_k : |l_i| \leqslant L_i\}$$

with $k \leqslant K^C$ such that $X \subseteq P \subseteq K^C X$.

Remarks on the proof. There are two slight novelties here. The first is minor and it is that the Freĭman–Ruzsa theorem is normally only stated for subsets of $\mathbb{Z}$, not of $\mathbb{R}^m$. This is certainly addressed by the more general result of the second author and Ruzsa [**8**], which is valid in an arbitrary abelian group (very likely a more direct reduction to the $\mathbb{Z}$-case is also possible). More seriously, the containment $P \subseteq K^C X$ is not normally stated as part of the theorem and indeed we know of no reference in the literature where it is explicitly mentioned. It may, however, be read without difficulty out of [**8**]. There one finds a proof that $2X - 2X$ contains a progression P_0 of size at least $\exp(-K^C)|X|$ and dimension at most K^C. This is a standard ingredient in 'Ruzsa-style' proofs of the Freĭman–Ruzsa theorem and may also be found in Ruzsa's original paper [**15**] for subsets of $\mathbb{Z}$. To proceed from such a statement to the Freĭman–Ruzsa theorem one applies a 'covering lemma', and the most efficient one in this context is implicit in Chang [**3**]. It is explicitly stated in [**20**, Lemma 5.31], and using that result one obtains

$$X \subseteq P_0 - P_0 + \{-1, 0, 1\}^d \cdot (v_1, \ldots, v_d) + x_0,$$

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

for some $x_0 \in X$, $v_1, \dots, v_d \in X - X = 2X$ and where $d \leqslant K^C$. Let P be the set on the right. It is a progression of dimension at most K^C, and it is fairly clearly contained in $(9+2d)X$. Also observe that the x_is all lie in $4X$. □

Putting the tools we have assembled so far together, we obtain the next result, which is the key to our main result.

Corollary 6.2. *Suppose that $A \subseteq G$ is a K-approximate group and let $\mathfrak{a} = \log A$. Then $\mathfrak{a}$ is contained in a* progression $\mathfrak{p}$ *of dimension at most K^{C_s} whose nilcompletion $\bar{\mathfrak{p}}$ is contained in $K^{C_s}\bar{\mathfrak{a}}$.*

Proof. Recall Lemma 6.1. Since $\mathfrak{a} \subseteq \bar{\mathfrak{a}}$, the upper bound on $|\mathfrak{a}+\bar{\mathfrak{a}}|$ certainly tells us that $|\mathfrak{a}+\mathfrak{a}| \leqslant K^{C_s}|\mathfrak{a}|$. Applying Chang's version of the Freĭman–Ruzsa theorem we obtain a progression $\mathfrak{p} \subseteq K^{C_s}\mathfrak{a}$ of dimension at most K^{C_s} such that $\mathfrak{a} \subseteq \mathfrak{p}$. The fact that $\bar{\mathfrak{p}} \subseteq K^{C_s}\bar{\mathfrak{a}}$ follows from Lemma 4.2 (i). □

Now given the progression $\mathfrak{p} = \{l_1x_1 + \dots + l_kx_k : |l_i| \leqslant L_i\}$ it is very tempting to consider the nilbox $\mathfrak{B}(x_1, \dots, x_k; L)$. One cannot quite use this to prove Proposition 2.3, however, since it is not necessarily the case that $\exp(x_i) \in \langle A \rangle$ for $i = k+1, \dots, t$. This may be rectified by the simple expedient of taking suitable dilates $M \cdot x_i$ of the generators x_i, $i = 1, \dots, k$. For $i = k+1, \dots, t$ write $x_i^{(M)} := M^{\chi(i)} \cdot x_i$ and note that there is a Lie algebra homomorphism $\pi_M : \mathfrak{n}_{k,s} \to \mathfrak{g}$ such that $\pi_M(x_i) = x_i^{(M)}$ for $i = 1, \dots, t$ (this being the one induced by mapping X_i to $M \cdot x_i$ for $i = 1, \dots, k$).

Lemma 6.3. *Suppose that $A \subseteq G$ and that $\mathfrak{a} := \log A$. Suppose that $\mathfrak{p}$ is a generalized progression as above, that $\mathfrak{p}$ contains $\mathfrak{a}$ and that $\bar{\mathfrak{p}}$ is contained in $m\bar{\mathfrak{a}}$. Let $M \geqslant 1$ be an integer. Then*

(i) *the nilbox $\mathfrak{B}(x_1, \dots, x_k; L)$ contains $\mathfrak{a}$ and is contained in $(4k)^s m\bar{\mathfrak{a}}$;*

(ii) *there is some $M \leqslant (2mk)^{C_s}$ for which the elements $\exp(x_i^{(M)})$, $i = 1, \dots, t$, all lie in the group $\langle A \rangle$ generated by A.*

Proof. The first part of (i) is totally obvious since $\mathfrak{p}$ contains $\mathfrak{a}$. To establish part (ii) we employ an argument identical to the one in the proof of Proposition 4.4 to obtain the inclusions $\mathfrak{B}(x_1, \dots, x_k; L) \subseteq (4k)^s\bar{\mathfrak{p}} \subseteq (4k)^s m\bar{\mathfrak{a}}$, as required.

Let us turn to (ii). We take M to have the special form R^s for some integer $R \geqslant 1$ to be specified. Then for each $i = 1, \dots, t$ the element $x_i^{(M)} = M^{\chi(i)} \cdot x_i$ may be written as the sum of at most $4^s m$ elements of the form $M^r[a_1, [a_2, [\cdots]]]$, where the a_i lie in $\mathfrak{a}$ and $r \geqslant 1$. We may each such element as $[b_1, [b_2, [\cdots]]]$ where the commutator has the same shape and each b_i is $R^{u_i}a_i$ for some $u_i \geqslant 1$.

Now we simply expand $\exp(x_i^{(M)})$ using Lemmas 5.1, 5.2 and 5.3, obtaining a finite product $y_{i_1}^{\eta_1}y_{i_2}^{\eta_2} \cdots$ with $y_i := \exp(b_i)$ in which, it may be confirmed, the rationals η_j may all be put over some common denominator of size at most $(2ks)^{C_s}$. Taking R to be this common denominator it follows that each $y_{i_j}^{\eta_j}$ lies in the group generated by A, which is what we wanted to prove. □

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

We are at last in a position to conclude the proof of Proposition 2.3, at least given a small result on nilboxes and their dilations from the next section.

Proof of Proposition 2.3. As ever $A \subseteq G$ is a K-approximate group and $\mathfrak{a} := \log A$. Applying Corollary 6.2 we obtain a progression $\mathfrak{p}$ of dimension K^{C_s} whose nilcompletion $\bar{\mathfrak{p}}$ is contained in $K^{C_s}\bar{\mathfrak{a}}$. Applying Lemma 6.3 (i) we obtain a nilbox $\mathfrak{B}(x_1, \dots, x_k; L)$ of dimension $k \leqslant K^{C_s}$ which contains $\mathfrak{a}$ and is contained in $K^{C_s}\bar{\mathfrak{a}}$. It follows from this last inclusion and Lemma 6.1 that $|\mathfrak{B}(x_1, \dots, x_k; L)| \leqslant \mathrm{e}^{K^{C_s}}|A|$, and hence $\exp(\mathfrak{B}(x_1, \dots, x_k; L))$ $\mathrm{e}^{K^{C_s}}$-controls A. Finally, we may apply Lemma 6.3 (ii) to find an $M = K^{C_s}$ such that the generators $\exp(x_i^{(M)})$, $i = 1, \dots, t$, all lie in $\langle A \rangle$. By Corollary 7.3, $\exp(\mathfrak{B}(x_1^{(M)}, \dots, x_k^{(M)}; L))$ also $\mathrm{e}^{K^{C_s}}$-controls A. This concludes the proof of Proposition 2.3. □

7. Nilboxes, nilpotent progressions and control

To conclude the proof of our main theorem we must establish Proposition 2.4, which asserts that the exponential of a nilbox is efficiently controlled by a nilpotent progression. We use the need for this as an excuse to develop the relationship of nilboxes and nilpotent progressions more generally.

Let us recall the statement of Proposition 2.4.

Proposition 2.4 (nilpotent progressions control nilboxes). *Suppose that G is an s-step simply connected nilpotent Lie group with Lie algebra $\mathfrak{g}$. Suppose that $x_1, \dots, x_k \in G$, and write $u_i := \exp(x_i)$. Let $L = (L_1, \dots, L_k)$ be a vector of positive integer lengths. Then the nilpotent progression $P(u_1, \dots, u_k; L)$ $\mathrm{e}^{k^{C_s}}$-controls $\exp(\mathfrak{B}(x_1, \dots, x_k; L))$.*

In fact we shall show that $\exp(\mathfrak{B}(x_1, \dots, x_k; L))$ $\mathrm{e}^{k^{C_s}}$-controls $P(u_1, \dots, u_k; L)$ as well. This notion of *mutual control*, where two sets A and B in some group K-control one another, is very useful since if π is a group homomorphism then $\pi(A)$ and $\pi(B)$ also K-control one another. Indeed the inclusions $A \subseteq (X \cdot B) \cap (B \cdot X)$ and $B \subseteq (X' \cdot A) \cap (A \cdot X')$ imply $\pi(A) \subseteq (\pi(X) \cdot \pi(B)) \cap (\pi(B) \cdot \pi(X))$ and $\pi(B) \subseteq (\pi(X') \cdot \pi(A)) \cap (\pi(A) \cdot \pi(X'))$, conditions which automatically imply that $|\pi(A)| \leqslant K|\pi(B)|$ and $|\pi(B)| \leqslant K|\pi(A)|$. In our setting, the upshot of this together with the commutativity of the diagram

$$\begin{array}{ccc} \mathfrak{n}_{k,s} & \xrightarrow{\exp} & N_{k,s} \\ \downarrow & & \downarrow \\ \mathfrak{g} & \xrightarrow{\exp} & G \end{array} \tag{7.1}$$

is that we need only establish Proposition 2.4 in the free setting.

Suppose then that $X_1, \dots, X_k, X_{k+1}, \dots, X_t$ is an adapted basis for the free s-step nilpotent Lie algebra $\mathfrak{n}_{k,s}$, as described in § 2. Let us introduce the shorthand

$$\mathfrak{B}(k, s; L) := \mathfrak{B}(X_1, \dots, X_k; L) := \{l_1X_1 + \cdots + l_tX_t : |l_i| \leqslant L^{\chi(i)}\}$$

for the free nilbox on k generators. We will require the variants

$$\mathfrak{B}(k, s; L, Q) := \{l_1X_1 + \cdots + l_tX_t : |l_i| \leqslant L^{\chi(i)},\ Q \mid l_i\}$$

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

for integers $Q \geqslant 1$. Write $u_i = \exp(X_i)$, $i = 1, \dots, k$, and suppose that $u_{k+1}, \dots, u_t$ is the ordered list of basic commutators in the u_i described in the introduction. We also introduce shorthands for the nilpotent progressions based on the u_i, thus

$$P(k, s; L) := P(u_1, \dots, u_k; L) := \{u_1^{l_1} \cdots u_t^{l_t} : |l_i| \leqslant L^{\chi(i)}\}.$$

Finally, we introduce the variant

$$P(k, s; L, Q) := \{u_1^{l_1} \cdots u_t^{l_t} : |l_i| \leqslant L^{\chi(i)},\ Q \mid l_i\}.$$

The key proposition linking these two types of object is the following proposition, which we will establish in the appendix after developing some basic theory of 'coordinates' on the free nilpotent group. Those results ultimately rest on the Baker–Campbell–Hausdorff formula.

Proposition 7.1. *There is some integer Q_s and constants $c = c_s$, $C = C_s$ such that for any positive integer Q divisible by Q_s we have*

$$\exp(\mathfrak{B}(k, s; cL, Q)) \subseteq P(k, s; L),$$
$$P(k, s; cL, Q) \subseteq \exp(\mathfrak{B}(k, s; L))$$

and such that uniformly in $\rho, \rho' < 10$, we have

$$\exp(\mathfrak{B}(k, s; \rho L, Q)) \cdot \exp(\mathfrak{B}(k, s; \rho' L, Q)) \subseteq \exp(\mathfrak{B}(k, s; (\rho + \rho' + C\rho\rho')L; Q))$$

and

$$P(k, s; \rho L, Q) \cdot P(k, s; \rho' L, Q) \subseteq P(k, s; (\rho + \rho' + C\rho\rho')L, Q).$$

In fact,

$$P(k, s, \rho L) \cdot P(k, s, \rho' L) \subseteq P(k, s; (\rho + \rho' + C\rho\rho')L).$$

Remark. The final inclusion here easily implies that if we set $X_\rho := P(k, s; (\rho - C'\rho^2)L)$ for an appropriate C' then $X_\rho \cdot X_{\rho'} \subseteq X_{\rho+\rho'}$. Furthermore, Proposition 7.2 below together with a little calculation implies that $X_{2\rho}$ is $\exp(C_s k^s)$-controlled by X_ρ. These two facts imply that the system $(X_\rho)_{\rho \leqslant 4}$ forms a *Bourgain system* in the sense of [**9**, **16**], thereby providing a link between our work and that of Sanders.

Proposition 2.4 follows immediately from Proposition 7.1 and the next result.

Proposition 7.2. *Let $k, s \geqslant 1$ be integers and let $Q, Q' \geqslant 1$ be two integers with $Q|Q'$ and $Q_s|Q'$, where Q_s is the quantity appearing the previous proposition. Let $\lambda < 1$ be a positive real number. Then $\exp(\mathfrak{B}(k, s, L; Q))$ and $\exp(\mathfrak{B}(k, s, \lambda L; Q'))$ mutually γ-control one another, as do $P(k, s, L; Q)$ and $P(k, s, \lambda L; Q')$, where we may take $\gamma = (1 + (Q'/\lambda Q))^{C_s k^s}$.*

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Proof. In view of the third inclusion of Proposition 7.1, there is some $\lambda' \geqslant c_s\lambda$ such that $\exp(\mathfrak{B}(k,s,\lambda' L;Q'^3)) \subseteq \exp(\mathfrak{B}(k,s,\lambda L,Q'))$. Hence to conclude the proof it suffices to show, in view of Proposition 3.1, the bound

$$\frac{|\mathfrak{B}(k,s,\lambda' L;Q')|}{|\mathfrak{B}(k,s,L;Q)|} \geqslant \left(1+\frac{Q'}{\lambda Q}\right)^{-C_s k^s}.$$

However, one has

$$|\mathfrak{B}(k,s,\lambda' L;Q')| = \prod_{j=1}^{t}\left(2\left\lfloor\frac{(\lambda' L)^{\chi(j)}}{Q'}\right\rfloor+1\right) \geqslant \prod_{j=1}^{t}\left(2\left\lfloor\frac{\lambda'^s}{Q'}L^{\chi(j)}\right\rfloor+1\right),$$

whereas

$$|\mathfrak{B}(k,s,L;Q)| = \prod_{j=1}^{t}\left(2\left\lfloor\frac{L^{\chi(j)}}{Q}\right\rfloor+1\right).$$

Note, however, the inequality

$$2\lfloor x\rfloor+1 \leqslant 2x+1 \leqslant \frac{2}{\alpha}(\lfloor\alpha x\rfloor+1)+1 \leqslant \left(1+\frac{1}{\alpha}\right)(2\lfloor\alpha x\rfloor+1),$$

valid for any $\alpha, x \geqslant 0$. It follows that

$$\frac{|\mathfrak{B}(k,s,\lambda' L;Q')|}{|\mathfrak{B}(k,s,L;Q)|} \geqslant \left(1+\frac{Q'}{\lambda' Q}\right)^{-t}.$$

Finally, note, as remarked in the introduction, that $t \leqslant (4k)^s$.

The proof for the nilprogressions $P(k,s;L)$ is essentially identical. □

Let us record a particular application of this that we used in § 5.

Corollary 7.3 (control by dilated balls). *Let G be a simply connected s-step nilpotent Lie group with Lie algebra $\mathfrak{g}$. Let $x_1,\dots,x_k \in \mathfrak{g}$, and suppose that $M, M' \geqslant 1$ are integers. Then $\exp(\mathfrak{B}(Mx_1,\dots,Mx_k;L))$ and $\exp(\mathfrak{B}(M'x_1,\dots,M'x_k;L))$ mutually $(MM')^{C_s k^s}$-control one another.*

Proof. The introduction of M' is merely to make the statement look symmetric. We only needed the corollary in the case $M'=1$, and in fact the general case clearly follows from this special one using the transitivity of control. Suppose, then, that $M'=1$. Since we are dealing with *mutual* control, a notion which persists under homomorphisms by the remarks at the beginning of the section, it suffices to work in the free setting.

One may easily check the inclusions

$$\mathfrak{B}(MX_1,\dots,MX_k;M^{-s}L,Q) \subseteq \mathfrak{B}(X_1,\dots,X_k;L,Q)$$

and

$$\mathfrak{B}(X_1,\dots,X_k;L,M^sQ) \subseteq \mathfrak{B}(MX_1,\dots,MX_k;L,Q)$$

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

for any integer $Q \geqslant 1$. Thus

$$\mathfrak{B}(MX_1, \dots, MX_k; L) \supseteq \mathfrak{B}(X_1, \dots, X_k; L, M^s) \supseteq \mathfrak{B}(MX_1, \dots, MX_k; M^{-s}L, M^s),$$

which implies by Proposition 7.2 that

$$\exp(\mathfrak{B}(MX_1, \dots, MX_k; L))$$

$M^{C_s k^s}$-controls

$$\exp(\mathfrak{B}(X_1, \dots, X_k; L, M^s)).$$

By another application of Proposition 7.2 this, in turn, $M^{C_s k^s}$-controls

$$\exp(\mathfrak{B}(X_1, \dots, X_k; L)).$$

The inverse relationship may be obtained very similarly. □

Appendix A. Freĭman invariance of nilpotent progressions

In this section we show that nilpotent progressions are preserved under *Freĭman homomorphisms* if the side lengths L are sufficiently large. Thus, in a sense, they are well-defined multiplicative–combinatorial objects. We recall the definition of Freĭman homomorphism. Suppose that A and B are two sets in ambient groups and that $\phi : A \to B$ is a map. We say that ϕ is a Freĭman k-homomorphism provided that for all $a_1, \dots, a_k \in A$ and all choices of $\varepsilon_1, \dots, \varepsilon_k \in \{-1, 0, 1\}$ the conditions $a_1^{\varepsilon_1} \cdots a_k^{\varepsilon_k} = \mathrm{id}$ implies that $\phi(a_1)^{\varepsilon_1} \cdots \phi(a_k)^{\varepsilon_k} = \mathrm{id}$.

Proposition A.1 (invariance under Freĭman isomorphism). *Suppose G and H are two groups and $s \in \mathbb{N}$. There is a constant $C_s \geqslant 1$ such that the following holds. Let A be an s-step nilpotent progression with k generators in G and side lengths $L = (L_1, \dots, L_k)$ with $L_i \geqslant C_{k,s}$ for $i = 1, \dots, k$. Let ϕ be a Freĭman 3-homomorphism from A onto a subset B of H. Then B is also an s-step nilpotent progression with k generators.*

Proof. Every nilpotent progression has the form

$$A = \{u_1^{l_1} \cdots u_t^{l_t} : |l_j| \leqslant L^{\chi(j)}\} \tag{A.1}$$

for some elements $u_1, \dots, u_t$. However, not every set of this form is a nilpotent progression: indeed $u_{k+1}, \dots, u_t$ are specific commutators involving $u_1, \dots, u_k$, and in particular there are words w_i, $i = k+1, \dots, t$, independent of the underlying group, such that $u_i = w_i(u_1, \dots, u_k)$. Moreover, it is not hard to see that *if* the u_i satisfy these conditions and if all $(s+1)$-fold commutators of the u_i equal the identity then the object (A.1) does define a nilpotent progression.

Now if the lengths $L = (L_1, \dots, L_k)$ are sufficiently great then all initial segments of all these words w_j lie in the nilpotent progression $P(u_1, \dots, u_k; L)$. This follows from the fifth inclusion of Proposition 7.1, or else it may be verified more explicitly by taking each initial segment $u_{i_1}, \dots, u_{i_m}$ and commutating until all copies of u_1 are at the left, then repeating this process for u_2 and so on.

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

Now let $\phi : A \to B$ be a map. Observe that if $a_1, \dots, a_m$ are elements of A or A^{-1} such that each initial segment $a_1 \cdots a_i$ belongs to A for all $i = 1, \dots, m$, then $\phi(a_1 \cdots a_m) = \phi(a_1) \cdots \phi(a_m)$. Also, by an easy induction, we have $\phi(a^j) = \phi(a)^j$ whenever all the powers $a, a^2, \dots, a^j$ lie in A. Writing $v_i := \phi(u_i)$ for $i = 1, \dots, t$, it follows from these observations and the analysis of the preceding paragraph that the v_i satisfy the same words $v_i = w_i(v_1, \dots, v_k)$, and also that all $(s+1)$-fold commutators of the v_i equal the identity.

It follows that

$$\{v_1^{l_1} \cdots v_t^{l_t} : |l_j| \leqslant L^{\chi(j)}\}$$

is a nilpotent progression in H. Furthermore, several more applications of the observation we made in the last paragraph confirm that

$$\phi(u_1^{l_1} \cdots u_t^{l_t}) = v_1^{l_1} \cdots v_t^{l_t},$$

and so this nilpotent progression is precisely equal to B. □

Appendix B. On coordinates in the free nilpotent Lie group

Throughout this appendix we will be working in the free s-step nilpotent Lie algebra $\mathfrak{n}_{k,s}$ on k generators and with the corresponding free nilpotent Lie group $N_{k,s}$. We suppose that an adapted basis (see the introduction for definitions) $X_1, \dots, X_t$ for $\mathfrak{n}_{k,s}$ has been chosen, and that $u_1, \dots, u_t$ is the corresponding ordered list of group commutators in $N_{k,s}$. We will also use the weight function $\chi : [t] \to \mathbb{N}_0^k$ introduced in § 1.

Our aim in this section is to establish Proposition 7.1, which the reader may care to recall now. We shall be quite brief in our treatment, which depends on a study of *coordinates* in the following sense.

Definition B.1 (coordinates). Suppose that $x \in N_{k,s}$. Then we define the group coordinates $\psi_{\mathrm{gp}}(x)$ to be $(x_1, \dots, x_t)$, where $x_1, \dots, x_t$ are the unique complex numbers such that $x = u_1^{x_1} \cdots u_t^{x_t}$. We define the algebra coordinates $\psi_{\mathrm{alg}}(x)$ to be $(x'_1, \dots, x'_t)$, where $x'_1, \dots, x'_t$ are the unique complex numbers such that $x = \exp(x'_1 X_1 + \cdots + x'_t X_t)$.

Remarks. The existence and uniqueness of the group coordinates is not obvious, and it will be a byproduct of our analysis. The algebra coordinates are the same thing as 'exponential coordinates of type I', as featured for example in [**4**] (hence the notation, with a single dash). The group coordinates are *not* quite the same thing as exponential coordinates of type II. If $x \in N_{k,s}$ then to find the type II coordinates $(x''_1, \dots, x''_t)$ one expresses x as $\exp(x''_1 X_1) \cdots \exp(x''_t X_t)$. We will encounter type II coordinates again in a short while.

Everything will follow from the Baker–Campbell–Hausdorff formula, which states that

$$\exp(X)\exp(Y) = \exp(X + Y + \tfrac{1}{2}[X,Y] + \tfrac{1}{12}[X,[X,Y]] + \cdots).$$

It is not important to know what the rational numbers here are, and indeed they are rather complicated to describe. All that is important is that the series on the right is finite in an s-step nilpotent group, and that all the rationals occurring have complexity $O_s(1)$.

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

With a little thought, this leads directly to the following description of multiplication in algebra coordinates.

Lemma B.2 (multiplication in algebra coordinates). *Suppose that $x, y \in N_{k,s}$ and that $\psi_{\mathrm{alg}}(x) = (x_1, \dots, x_t)$ while $\psi_{\mathrm{alg}}(y) = (y_1, \dots, y_t)$. Then*

$$\psi_{\mathrm{alg}}(xy) = (P_1(x_i, y_i), \dots, P_t(x_i, y_i)).$$

Here, each P_j is a polynomial of the form

$$x_j + y_j + \sum_{\alpha,\beta \neq 0} C^{(j)}_{\alpha,\beta} x^\alpha y^\beta,$$

where the $C^{(j)}_{\alpha,\beta}$ are rationals with complexity $O_s(1)$, $\alpha = (\alpha_1, \dots, \alpha_t)$ and $\beta = (\beta_1, \dots, \beta_t) \in \mathbb{N}_0^t$ are multi-indices and x^α means $x_1^{\alpha_1} \cdots x_t^{\alpha_t}$. Furthermore, $C^{(j)}_{\alpha,\beta}$ is only non-zero if $\sum_{l \in [t]} \chi(l)(\alpha_l + \beta_l) = \chi(j)$.

The third inclusion of Proposition 7.1 follows quickly from this, taking Q_s to be the least common multiple of the denominators of all the $C^{(j)}_{\alpha,\beta}$.

We may also say something about the transformation which takes the group coordinates of a point $x \in N_{k,s}$ and outputs the algebra coordinates. Before doing this it is convenient to set up a notion of *degree*. Suppose that $(x_1, \dots, x_t)$ are variables, to be thought of as coordinates. Now let $z_1, \dots, z_k$ be further variables, and substitute $x_j = z^{\chi(j)} = z_1^{\chi(j)_1} \cdots z_k^{\chi(j)_k}$. When we speak of the *degree* $\deg(P)$ of a polynomial $P = P(x_1, \dots, x_t)$ involving the x_i, we shall mean the total degree in the z_i of $P(z_1, \dots, z_k)$ after this substitution has been made. We shall also write $\deg_i$ for the degree with respect to z_i.

Definition B.3 (privileged coordinate change). Let $\phi : \mathbb{C}^t \to \mathbb{C}^t$ be a polynomial map. We say that ϕ is a *privileged coordinate change* if $(\phi(x))_j = x_j + P_j(x_1, \dots, x_t)$, where $\deg_i(P_j(x)) \leqslant \deg_i(x_j)$ for all $i = 1, \dots, k$ and P_j depends only on those variables x_l with $\deg(x_l) < \deg(x_j)$.

The inverse of a privileged coordinate change is another privileged coordinate change, as is the composition of two such coordinate changes. We leave the proof as an exercise. If all the coefficients of the P_j are rationals with complexity $O_s(1)$ then we say that ϕ is of *bounded complexity*; the inverse and composition of privileged coordinate changes of bounded complexity are also privileged coordinate changes of bounded complexity, albeit with worsenings of the unspecified constants $O_s(1)$.

Lemma B.4 (group coordinates to algebra coordinates). *Suppose that $x \in N_{k,s}$ and that $\psi_{\mathrm{gp}}(x) = (x_1, \dots, x_t)$ and $\psi_{\mathrm{alg}}(x) = (x'_1, \dots, x'_t)$. Then the mapping $(x_j) \to (x'_j)$ and its inverse are privileged coordinate changes of bounded complexity.*

Proof. Write $Y_i := \log(u_i)$ for $i = 1, \dots, t$. We claim that the relation between the Y_i and the X_i is a rather special one: we have

$$Y_j = X_j + \sum_m \mu_{jm} X_m,$$

https://doi.org/10.1017/S1474748010000150 Published online by Cambridge University Press

where the sum is restricted to those m for which $\chi(m) \geqslant \chi(j)$ pointwise but $\chi(m) \neq \chi(j)$. This may be established by induction on the order of the commutator u_i using the Baker–Campbell–Hausdorff formula: we leave the details to the reader. Suppose that $\psi_{\mathrm{alg}}(x) = (x'_1, \dots, x'_t)$, that is to say $\log x = x'_1 X_1 + \cdots + x'_t X_t$. We may also represent $\log x$ as $y_1 Y_1 + \cdots + y_t Y_t$ in 'exponential coordinates of type I' relative to the basis Y_i, and it is not hard to check that the change of coordinates map $(x'_i) \to (y_i)$ is a privileged coordinate change of bounded complexity.

In view of the group closure properties of the notion of privileged coordinate change it suffices to show that the map $(x_i) \to (y_i)$ is a privileged coordinate change of bounded complexity. Note that $x = \exp(x_1 Y_1) \cdots \exp(x_t Y_t)$ (so the group coordinates $\psi_{\mathrm{gp}}(x) = (x_i)$ are actually the same thing as the 'exponential coordinates of type II' relative to the basis $Y_1, \dots, Y_t$). The desired property follows from repeated application of the Baker–Campbell–Hausdorff formula: once again we leave the precise details to the reader. □

Remark. The existence and uniqueness of group coordinates follows from (the proof of) this lemma.

The first and second inclusions of Proposition 7.1 follow very quickly from this lemma. To establish the fourth and fifth inclusions of that proposition, it suffices to prove the following 'group' variant of Lemma B.2.

Lemma B.5 (multiplication in group coordinates). *Suppose that $x, y \in N_{k,s}$ and that $\psi_{\mathrm{gp}}(x) = (x_1, \dots, x_t)$ while $\psi_{\mathrm{gp}}(y) = (y_1, \dots, y_t)$. Then*

$$\psi_{\mathrm{gp}}(xy) = (P_1(x_i, y_i), \dots, P_t(x_i, y_i)).$$

Here, each P_j is a polynomial mapping $\mathbb{Z}^t \times \mathbb{Z}^t$ to $\mathbb{Z}$ of the form

$$x_j + y_j + \sum_{\alpha,\beta \neq 0} C^{(j)}_{\alpha,\beta} x^\alpha y^\beta,$$

where the $C^{(j)}_{\alpha,\beta}$ are rationals with complexity $O_s(1)$, $\alpha = (\alpha_1, \dots, \alpha_t)$ and $\beta = (\beta_1, \dots, \beta_t) \in \mathbb{N}_0^t$ are multi-indices, and x^α means $x_1^{\alpha_1} \cdots x_t^{\alpha_t}$. Furthermore, $C^{(j)}_{\alpha,\beta}$ is only non-zero if $\sum_{l \in [t]} \chi(l)(\alpha_l + \beta_l) = \chi(j)$.

Proof. Combine Lemma B.4 with Lemma B.2. The fact that each P_i maps $\mathbb{Z}^t \times \mathbb{Z}^t$ to $\mathbb{Z}$ follows from the fact that the set $\{u_1^{n_1} \cdots u_t^{n_t} : n_1, \dots, n_t \in \mathbb{Z}\}$ is a group (the free s-step nilpotent group $\Gamma_{k,s}$ on k generators). This may be verified by repeated commutation, taking the product of two such elements and moving all copies of u_1 to the left, then all copies of u_2, and so on. □

Remark. Similar issues to those addressed by the last lemma are discussed in [**13**].

Acknowledgements. It is a pleasure to thank Elon Lindenstrauss, Tom Sanders and Terry Tao for a number of helpful conversations.

References

1. N. Bourbaki, Éléments de mathématique, XXVI, in *Groupes et algèbres de Lie, Chapitre 1: Algèbres de Lie*, Actualités Scientifiques et Industrielles, No. 1285 (Hermann, Paris, 1960).
2. E. Breuillard and B. J. Green, Approximate subgroups of solvable Lie groups, *Q. J. Math. (Oxford)*, in press.
3. M. C. Chang, A polynomial bound in Freĭman's theorem, *Duke Math. J.* **113**(3) (2002), 399–419.
4. L. J. Corwin and F. P. Greenleaf, *Representations of nilpotent Lie groups and applications*, Volume I, Cambridge Studies in Advanced Mathematics, Volume 18 (Cambridge University Press, 1990).
5. J. D. Dixon, M. P. F. du Sautoy, A. Mann and D. Segal, *Analytic pro-p groups*, 2nd edn, Cambridge Studies in Advanced Mathematics, Volume 61 (Cambridge University Press, 1999).
6. D. Fisher, N. H. Katz and I. Peng, On Freĭman's theorem in nilpotent groups, preprint (arXiv:0901.1409; 2009).
7. G. A. Freĭman, *Foundations of a structural theory of set addition* (transl. from Russian), Translations of Mathematical Monographs, Volume 37 (American Mathematical Society, Providence, RI, 1973).
8. B. J. Green and I. Z. Ruzsa, Freiman's theorem in an arbitrary abelian group, *J. Lond. Math. Soc.* **75**(1) (2007), 163–175.
9. B. J. Green and T. Sanders, A quantitative version of the idempotent theorem in harmonic analysis, *Annals Math.* **168**(3) (2008), 1025–1054.
10. M. Hall, *Theory of groups* (American Mathematical Society/Chelsea, Providence, RI, 1999).
11. M. Lazard, Problémes d'extension concernant les N-groupes; inversion de la formule de Hausdorff, *C. R. Acad. Sci. Paris Sér. I* **237** (1953), 1377–1379.
12. M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, *Annales Scient. Éc. Norm. Sup.* **71**(2) (1954), 101–190.
13. A. Leibman, Polynomial sequences in groups, *J. Alg.* **201**(1) (1998), 189–206.
14. M. S. Raghunathan, *Discrete subgroups of Lie groups* (Springer, 1972).
15. I. Z. Ruzsa, Generalized arithmetical progressions and sumsets, *Acta Math. Hungar.* **65**(4) (1994), 379–388.
16. T. Sanders, From polynomial growth to metric balls in monomial groups, preprint (arXiv:0912.0305; 2009).
17. I. Stewart, An algebraic treatment of Mal'cev's theorems concerning nilpotent Lie groups and their Lie algebras, *Compositio Math.* **22** (1970), 289–312.
18. T. C. Tao, Product set estimates for non-commutative groups, *Combinatorica* **28**(5) (2008), 547–594.
19. T. C. Tao, Freiman's theorem for solvable groups, *Contrib. Disc. Math.*, in press.
20. T. C. Tao and V. H. Vu, *Additive combinatorics* (Cambridge University Press, 2006).