An alternative approach to Freiman's theorem in p-groups

Matthew C. H. Tointon*

Department of Pure Mathematics and Mathematical Statistics, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, United Kingdom
email: M.Tointon@dpmms.cam.ac.uk

Abstract

We prove a Freiman–Ruzsa-type theorem valid in a p-group of nilpotency class 2 when p is at least 3. The method is similar to that used by E. Breuillard and B. Green to prove their analogous result in the case of a torsion-free nilpotent group, with Mal'cev's embedding theorem replaced by the Lazard correspondence.

Disclaimer

This note is intended as an addendum to [6]. We therefore assume familiarity with all definitions, notation and motivation from that paper, and reference results from it directly, without restating them here.

This note is for interest only and is not intended for peer review or publication. As such, it is not as polished or carefully proof read as a published paper would be.

1 Introduction

The author has proved a structure theorem for approximate subgroups of an arbitrary nilpotent group [6]. This generalised earlier work of a number of authors, most recently E. Breuillard and B. Green [1], who had previously established the corresponding result in the special case of a torsion-free nilpotent group.

The approach taken in [6] is somewhat different to that used by Breuillard and Green. Their argument relies on an embedding theorem of Mal'cev, which essentially allows them to reduce the study of approximate subgroups of an arbitrary torsion-free nilpotent group to the study of approximate subgroups of a simply connected nilpotent Lie group. This in turn allows them to study the image of an approximate group in the Lie algebra associated to the Lie group, in which setting they are able appeal to abelian approximate group theory.

It is likely that one could prove a structure theorem for approximate subgroups of certain p-groups using a fairly direct adaptation of this argument. Specifically, it appears that such an approach should work if G is a p-group of nilpotency class less than p. Indeed, in that case a correspondence theorem of Lazard allows one to associate to G an additive abelian p-group $\mathfrak{g}$, called a *Lie ring*, that plays a role analogous to that of the Lie algebra of a Lie group; this should then allow one to apply arguments similar to those used by Breuillard and Green.

The purpose of this note is to illustrate this principle. We do so by proving the following version of [6, Theorem 1.5], valid in the simple case in which G is a 2-step p-group with $p > 2$. We do not consider the higher-step case, as even the most general result obtainable by this method would already be superseded by the results of [6].

*The author is a Junior Research Fellow of Homerton College, Cambridge. When this research was carried out he was supported by an EPSRC doctoral training grant, awarded by the Department of Pure Mathematics and Mathematical Statistics in Cambridge, and a Bye-Fellowship from Magdalene College, Cambridge.

Theorem 1.1. *Let p be an odd prime and let G be a p-group of nilpotency class 2. Suppose that $A \subset G$ is a K-approximate group. Then there exists a nilpotent progression $P = P(x_1, \dots, x_k; L)$ of rank $k \ll_K 1$ and a subgroup H of G, normalised by A, such that $|HP| \ll_K |A|$ and $A \subset HP$.*

In Section 2 we describe the Lazard correspondence and record its relevant properties, and then we briefly summarise the resultant notation in Section 3. We prove Theorem 1.1 in Sections 4 and 5.

Remark 1.2. The bounds in Theorem 1.1 are all effective and reasonable, but since [6, Theorem 1.5] is both stronger and more general than Theorem 1.1 we suppress the details.

Remark 1.3. In the 2-step setting a nilpotent progression has a fairly explicit form, as follows.

$$P(x_1, \dots, x_k; L) := \left\{ x_1^{l_1} \dots x_k^{l_k} \prod_{i<j} [x_i, x_j]^{l_{ij}} : |l_i| \leq L_i, |l_{ij}| \leq L_i L_j \right\}.$$

Acknowledgements

The author is indebted to Ben Green for helpful conversations, and to Emmanuel Breuillard and Tom Sanders for comments on an earlier version of this note.

2 The Lazard correspondence

Let G be a finite p-group of nilpotency class at most $p-1$. Then [3, Example 10.24] and the preceding discussion indicate that it is possible to define operations $+$ and $[\ ,\ ]$ on G that make it into a so-called *Lie ring* that plays a role similar to that of the Lie algebra of a Lie group. See also [4, §3]. This Lie ring is an additive abelian group under $+$ and the bracket is bilinear and anticommutative (meaning that $[x, x]$ is always trivial) and satisfies the Jacobi identity. We shall review briefly in this section the relevant properties of this construction.

The descriptions in [3, 4] define the operations $+$ and $[\ ,\ ]$ on the underlying set G itself. However, in order to emphasise the analogy with Lie groups and Lie algebras we shall view the Lie ring as a different set $\mathfrak{g}$ and define a map $\log : G \to \mathfrak{g}$ that takes an element x of G to its corresponding element in $\mathfrak{g}$, writing $\exp : \mathfrak{g} \to G$ for its inverse.

The first property that we highlight is that if $x \in G$ and $X := \log x \in \mathfrak{g}$ then the order of X in the additive group $\mathfrak{g}$ is equal to the order of x in the multiplicative group G [3].

The second property we describe relates to a well known feature of the exponential map to a Lie group from its Lie algebra, which is that it satisfies the Baker–Campbell–Hausdorff formula. In its 2-step incarnation this states that for X, Y belonging to the Lie algebra we have

$$\exp X \exp Y = \exp(X + Y + \tfrac{1}{2}[X, Y]). \tag{2.1}$$

In order for this formula and its consequences to make sense in the context of p-groups and their associated Lie rings it would be necessary at the very least to be able to define what $\frac{1}{2}[X, Y]$ should mean.

Definition 2.1. Let S be a set of primes. Then we shall say that a group Γ is *uniquely S-divisible* if for every $x \in \Gamma$ and every $n \in \mathbb{N}$ whose prime factors all lie in S there exists a unique $y \in \Gamma$ such that $y^n = x$. By uniqueness we may, in this situation, denote $x^{1/n} := y$.

Lemma 2.2. *Let p be a prime, let G be a p-group and write S_p for the set of primes distinct from p. Then G is uniquely S_p-divisible. Furthermore, if $x \in G$ and n is coprime to p then the element $x^{1/n}$ lies in the cyclic group generated by x.*

Proof. [3] Let n be a product of primes from S_p and let $x \in G$. The cyclic group generated by x has order p^m for some m. Clearly we may take y to be x^{n^*}, where n^* is the multiplicative inverse of n modulo p^m. Now suppose that z also satisfies $z^n = x$. Then $z^{nn^*} = y$, and so x, y and z lie in a common cyclic group. Hence $y = z$ by the uniqueness of multiplicative inverses of numbers coprime to p in $\mathbb{Z}/p^r\mathbb{Z}$. □

In particular, if p is odd then in any p-group we may take square roots or, if the group is abelian, halves, and so (2.1) is well defined. It turns out that if p is odd and G is a p-group of nilpotency class 2 with associated Lie ring $\mathfrak{g}$ then the exponential map does indeed satisfy the Baker–Campbell–Hausdorff formula[1] [3], and it is from this that a large part of our argument will follow.

Finally, we note some specialisations of the results in [1, Section 5] to 2-step p-groups.

Lemma 2.3. *Let p be an odd prime and let G be a 2-step p-group with associated Lie ring $\mathfrak{g}$. Suppose $x_1, x_2, \ldots \in G$ and write $X_i := \log x_i$. Then the following identities hold.*

(i) $\exp(X_1 + \ldots + X_n) = x_n^{1/2} x_{n-1}^{1/2} \ldots x_2^{1/2} x_1 x_2^{1/2} \ldots x_{n-1}^{1/2} x_n^{1/2}$.

(ii) $\exp([X_1, X_2]) = x_1 x_2 x_1^{-1} x_2^{-1}$.

(iii) $\exp(X_1 + X_2 + [X_3, X_4]) = x_2^{1/2} x_1 x_2^{1/2} x_3 x_4 x_3^{-1} x_4^{-1}$.

Proof. Statement (i) is true for $n = 1$ by definition and more or less immediate from the Baker–Campbell–Hausdorff formula when $n = 2$. For larger n it may be verified by iterating the $n = 2$ statement.

Statement (ii) is immediate from the Baker–Campbell–Hausdorff formula and statement (iii) follows from (i) and (ii) and the Baker–Campbell–Hausdorff formula. □

3 Notation

For the remainder of this note p will be an odd prime and G will be a 2-step nilpotent p-group with associated Lie ring $\mathfrak{g}$. We shall in general denote subsets of G by capital Roman letters $A, B \ldots$ and subsets of $\mathfrak{g}$ by lower-case Fraktur letters $\mathfrak{a}, \mathfrak{b}, \ldots$. We shall denote elements in G by lower-case Roman letters $x, y, \ldots$ and their corresponding elements in $\mathfrak{g}$ by the corresponding upper-case Roman letters $X, Y, \ldots$.

If $B \subset G$ is a set then we shall write $\log B := \{\log x : x \in B\}$. If $\mathfrak{b} \subset \mathfrak{g}$ is a set then we shall write $[\mathfrak{b}, \mathfrak{b}] := \{[X, Y] : X, Y \in \mathfrak{b}\}$. If $X_1, \ldots, X_k \in \mathfrak{g}$ then we shall denote by $\mathfrak{p}(X_1, \ldots, X_k; L)$ the abelian progression $P(X_1, \ldots, X_k; L)$ so as to emphasise its containment in $\mathfrak{g}$.

4 Nilcompletions and abelian coset progressions

In this section we recall some definitions from [1] and recast some of the arguments from that work in the setting of finite p-groups. Some of the arguments can be simplified in this setting, and we shall include remarks noting where simplification has been possible. On the other hand, there is a need for some additional work in order to cope with the possible appearance of the subgroup H in the conclusion of Theorem 1.1. Again, we shall include remarks to indicate exactly where these additional arguments are required.

We begin with a definition from [1].

Definition 4.1 (2-step nilcompletion [1, Definition 4.1])**.** Let $\mathfrak{b} \subset \mathfrak{g}$ be a set. We define the *nilcompletion* $\overline{\mathfrak{b}}$ of $\mathfrak{b}$ to be the set $\mathfrak{b} + [\mathfrak{b}, \mathfrak{b}]$.

The fact that the bracket operation is bilinear implies that, for elements $b_i, b'_j \in \mathfrak{b}$, we have

$$[b_1 + \ldots + b_m, b'_1 + \ldots + b'_m] = \sum_{i,j \leq m} [b_i, b'_j],$$

and so we have the inclusion

$$\overline{m\mathfrak{b}} \subset m^2 \overline{\mathfrak{b}} \tag{4.1}$$

[1] In fact, the general Baker–Campbell–Hausdorff formula holds whenever the step of the group is less than p.

from [1, Lemma 4.2]. The second inclusion from that lemma, namely

$$[\overline{\mathfrak{b}}, \overline{\mathfrak{b}}] \subset \overline{\mathfrak{b}}, \tag{4.2}$$

is immediate from the definition of nilcompletion.

We now come onto one of the key observations of [1], which implies that if A is an approximate subgroup of G then both $\log A$ and its nilcompletion are approximate additive subgroups of $\mathfrak{g}$.

Proposition 4.2 ([1, Lemma 6.1])**.** *Let $A \subset G$ be a K-approximate subgroup and write $\mathfrak{a} := \log A$. Then we have $|\mathfrak{a} + \overline{\mathfrak{a}}| \leq K^{23}|\mathfrak{a}|$ and $|m\overline{\mathfrak{a}}| \leq K^{O(m)}|\mathfrak{a}|$ for all $m \in \mathbb{N}$.*

Proof. The argument is essentially identical to that used in [1]. Set

$$B := \{x^2, x^4 : x \in A\} \qquad \text{and} \qquad \mathfrak{b} := \log B = \{2X, 4X : X \in \mathfrak{a}\},$$

and note that

$$\mathfrak{b} + \overline{\mathfrak{b}} = \{r_1X_1 + r_2X_2 + [r_3X_3, r_4X_4] : X_i \in A, r_i \in \{2, 4\}\}.$$

By Lemma 2.3, for any $r_i \in \{2, 4\}$ we have

$$\exp(r_1X_1 + r_2X_2 + [r_3X_3, r_4X_4]) = x_2^{r_2/2}x_1^{r_1}x_2^{r_2/2}x_3^{r_3}x_4^{r_4}x_3^{-r_3}x_4^{-r_4} \in A^{24},$$

and so by [6, Lemma 2.1] we have

$$|\mathfrak{b} + \overline{\mathfrak{b}}| \leq K^{23}|A| = K^{23}|\mathfrak{a}|. \tag{4.3}$$

Now $\mathfrak{a} + \overline{\mathfrak{a}} = \{X_1 + X_2 + [X_3, X_4] : X_i \in \mathfrak{a}\}$, and for $X_1, X_2, X_3, X_4 \in \mathfrak{a}$ we have

$$4(X_1 + X_2 + [X_3, X_4]) = 4X_1 + 4X_2 + [2X_3, 2X_4] \subset \mathfrak{b} + \overline{\mathfrak{b}},$$

and so

$$4 \cdot (\mathfrak{a} + \overline{\mathfrak{a}}) \subset \mathfrak{b} + \overline{\mathfrak{b}}. \tag{4.4}$$

However, since $\mathfrak{g}$ is an additive p-group, Lemma 2.2 implies that the map $X \mapsto 4X$ is a bijection $\mathfrak{g} \to \mathfrak{g}$, and so combining (4.3) and (4.4) we obtain

$$|\mathfrak{a} + \overline{\mathfrak{a}}| = |4 \cdot (\mathfrak{a} + \overline{\mathfrak{a}})| \leq |\mathfrak{b} + \overline{\mathfrak{b}}| \leq K^{23}|\mathfrak{a}|,$$

which was the first desired conclusion of the proposition. The second desired conclusion then follows from the Ruzsa triangle inequality [5, (2.6)] and its associated sum-set estimates [5, Corollary 2.23]. □

Now, in a spirit similar to that of [1, Corollary 6.2], we use the fact that $\mathfrak{a}$ is an approximate additive subgroup of $\mathfrak{g}$ to place $\mathfrak{a}$ efficiently inside a coset progression $\mathfrak{h} + \mathfrak{p}$. The key difficulties arise because we will also need to ensure that $\exp \mathfrak{h}$ is a genuine subgroup of G and that it is normalised by $\exp \mathfrak{p}$.

Proposition 4.3. *Let $A \subset G$ be a K-approximate subgroup and write $\mathfrak{a} := \log A$. Then there exist an additive subgroup $\mathfrak{h}$ of $\mathfrak{g}$ and a progression $\mathfrak{p} = \mathfrak{p}(X_1, \dots, X_k; L)$ in $\mathfrak{g}$ of dimension $k \ll_K 1$ satisfying the following conditions.*

(i) The set $\exp \mathfrak{h}$ is a subgroup of G.

(ii) For every $Y \in \mathfrak{h}$ and every X_i we have $[Y, X_i] \in \mathfrak{h}$.

(iii) $\mathfrak{a} \subset \mathfrak{h} + \mathfrak{p}$.

(iv) $\mathfrak{h} + \overline{\mathfrak{p}} \subset O_K(1)\overline{\mathfrak{a}}$.

It will be helpful to be able to apply Chang's covering argument in a slightly different form to that stated in [6].

Proposition 4.4 (Chang [2, Proposition 5.1])**.** *Suppose that X is a subset of an abelian group with doubling constant K and that $2X-2X$ contains a proper coset progression $H+Q$ of size $\eta|X|$ and dimension d. Then there exists a progression P of dimension at most $d+K^{O(1)}/\eta$ such that $X \subset H+P \subset K^{O(1)}X$.*

Proof of Proposition 4.3. It follows from Proposition 4.2 that $\mathfrak{a}$ has doubling constant at most $K^{O(1)}$, and so we can conclude from [6, Theorem 2.2] that there exists a proper coset progression $\mathfrak{h}_0+\mathfrak{q}$ with dimension at most $O(K^{O(1)})$ satisfying

$$|\mathfrak{h}_0+\mathfrak{q}| \geq \exp(-O(K^{O(1)}))|\mathfrak{a}| \tag{4.5}$$

and

$$\mathfrak{h}_0+\mathfrak{q} \subset 4\mathfrak{a}. \tag{4.6}$$

We can then apply Chang's covering argument in the form of Proposition 4.4 to conclude that there is a progression $\mathfrak{p}=\mathfrak{p}(X_1,\dots,X_k;L)$ of dimension

$$k \ll_K 1 \tag{4.7}$$

such that $\mathfrak{a} \subset \mathfrak{h}_0+\mathfrak{p} \subset O_K(1)\mathfrak{a}$, and hence by (4.1) that

$$\mathfrak{a} \subset \mathfrak{h}_0+\mathfrak{p} \subset \overline{\mathfrak{h}_0+\mathfrak{p}} \subset O_K(1)\overline{\mathfrak{a}}. \tag{4.8}$$

Set $\mathfrak{h} := \mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{h}_0]\rangle+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle$. Condition (ii) required by the lemma follows immediately from the linearity of the bracket in the first co-ordinate (and the fact that the nilpotency class of G is 2), whilst condition (iii) is a weaker statement than the first inclusion of (4.8).

Conditions (i) and (iv) require a bit more work. Let us verify condition (i), which is that $\exp\mathfrak{h}$ is a (genuine) subgroup of G. We start by noting that if Z_j are elements of $\mathfrak{h}_0$ and l_j are integers then

$$\sum_j [Z_j, l_jX_i] = \left[\sum_j l_jZ_j, X_i\right]$$

by the bilinearity of the bracket operator, and so

$$\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle = \left\{\sum_{i=1}^k [Z_i,X_i] : Z_i \in \mathfrak{h}_0\right\} = \sum_{i=1}^k [\mathfrak{h}_0,X_i]. \tag{4.9}$$

The set $\mathfrak{h}$ therefore consists of all elements of the form

$$Y+\sum_{j=1}^m [V_j,W_j]+\sum_{i=1}^k [Z_i,X_i], \tag{4.10}$$

with $m \in \mathbb{N}$ and $Y,V_j,W_j,Z_i \in \mathfrak{h}_0$. The Baker–Campbell–Hausdorff formula (2.1) then gives

$$\begin{aligned}\log\left(\exp\left(Y+\textstyle\sum_{j=1}^m[V_j,W_j]+\sum_{i=1}^k[Z_i,X_i]\right)\exp\left(Y'+\sum_{j=1}^m[V_j',W_j']+\sum_{i=1}^k[Z_i',X_i]\right)\right)\\ = Y+Y'+[\tfrac{1}{2}Y,Y']+\textstyle\sum_{j=1}^m[V_j,W_j]+\sum_{j=1}^m[V_j',W_j']+\sum_{i=1}^k[Z_i+Z_i',X_i],\end{aligned}$$

which is also of the form (4.10) by Lemma 2.2, and so $\exp\mathfrak{h}$ is a closed subset in a torsion group and hence a subgroup, as claimed.

We now turn to condition (iv). The final inclusion of (4.8) implies that $2(\overline{\mathfrak{h}_0+\mathfrak{p}}) \subset O_K(1)\overline{\mathfrak{a}}$, and so Proposition 4.2 and the first inclusion of (4.8) combine to imply that $|2(\overline{\mathfrak{h}_0+\mathfrak{p}})| \ll_K \overline{\mathfrak{h}_0+\mathfrak{p}}$.

Furthermore, it follows from (4.6) and (4.8) that $2(\overline{\mathfrak{h}_0+\mathfrak{p}})-2(\overline{\mathfrak{h}_0+\mathfrak{p}})$ contains the proper coset progression $\mathfrak{h}_0+\mathfrak{q}$, and from (4.5), (4.8) and Proposition 4.2 that $|\mathfrak{h}_0+\mathfrak{q}| \gg_K |\overline{\mathfrak{h}_0+\mathfrak{p}}|$, and so applying Proposition 4.4 again there is a progression $\mathfrak{p}'$ such that

$$\overline{\mathfrak{h}_0+\mathfrak{p}} \subset \mathfrak{h}_0+\mathfrak{p}' \tag{4.11}$$

and

$$\dim \mathfrak{p}' \ll_K 1. \tag{4.12}$$

It is clear that $\mathfrak{h}$ is contained in the group generated by $\overline{\mathfrak{h}_0+\mathfrak{p}}$, and so (4.11) and (4.12) imply that $\mathfrak{h}/\mathfrak{h}_0$, and in particular the further quotient $\mathfrak{h}/(\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle)$, have rank at most $O_K(1)$. Now $\mathfrak{h}/(\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle)$ is generated by elements of the form $\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle+[Y,Y']$, with $Y,Y'\in\mathfrak{h}_0$, and so the rank bound and [6, Lemmas D.1 & D.2] show that there must be some set $S=\{[Y_i,Y_i']:i\in[n]\}$ with $Y_i,Y_i'\in\mathfrak{h}_0$ and

$$n \ll_K 1 \tag{4.13}$$

such that $(\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle+S)$ generates $\mathfrak{h}/(\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle)$.

This implies in particular that

$$\mathfrak{h}=\mathfrak{h}_0+\langle[\mathfrak{h}_0,\mathfrak{p}]\rangle+\langle S\rangle \tag{4.14}$$

However, $l[Y_i,Y_i']=[lY_i,Y_i']\in[\mathfrak{h}_0,Y_i']$, and so, by a similar argument to that leading to (4.9), we have

$$\langle S\rangle=\sum_{i=1}^{n}[\mathfrak{h}_0,Y_i']. \tag{4.15}$$

Thus (4.9), (4.14) and (4.15) combine to show that $\mathfrak{h}\subset(k+n)(\overline{\mathfrak{h}_0+\mathfrak{p}})$, which then gives $\mathfrak{h}+\overline{\mathfrak{p}}\subset(1+k+n)(\overline{\mathfrak{h}_0+\mathfrak{p}})$. The bounds (4.7) and (4.13) and the last inclusion of (4.8) therefore imply that $\mathfrak{h}+\overline{\mathfrak{p}}\subset O_K(1)\overline{\mathfrak{a}}$, which is condition (iv) of the proposition. □

5 Nilboxes and nilpotent coset progressions

The purpose of this section is to complete the proof of Theorem 1.1. We begin by recalling from [1] the definition of a nilbox.

Definition 5.1 (Nilbox)**.** Suppose that $X_1,\dots,X_k\in\mathfrak{g}$ and that $L=(L_1,\dots,L_k)\in\mathbb{N}^k$. Then we define the *nilbox* $\mathfrak{B}(X_1,\dots,X_k;L)$ by

$$\mathfrak{B}(X_1,\dots,X_k;L):=\left\{\textstyle\sum_{i=1}^k l_iX_i+\sum_{i<j}l_{ij}[X_i,X_j]:|l_i|\le L_i,|l_{ij}|\le L_iL_j\right\}.$$

It is immediate from the definitions that for any $X_1,\dots,X_k\in\mathfrak{g}$ and any $L\in\mathbb{N}^k$ we have

$$\overline{\mathfrak{p}(X_1,\dots,X_k;L)}\subset\mathfrak{B}(X_1,\dots,X_k;L). \tag{5.1}$$

The following lemma shows that the reverse containment is also approximately true.

Lemma 5.2. *Let $X_1,\dots,X_k\in\mathfrak{g}$ and let $L\in\mathbb{N}^k$. Then*

$$\mathfrak{B}(X_1,\dots,X_k;L)\subset k(k-1)\overline{\mathfrak{p}(X_1,\dots,X_k;L)}.$$

Proof. Abbreviate $\mathfrak{p}:=\mathfrak{p}(X_1,\dots,X_k;L)$. By [1, Lemma 4.3] any integer l_{ij} satisfying $|l_{ij}|\le L_iL_j$ can be written in the form $l_{ij}=l_il_j+l_i'l_j'$ with $|l_i|,|l_i'|\le L_i$ and $|l_j|,|l_j'|\le L_i$. This implies in particular that $l_{ij}[X_i,X_j]=[l_iX_i,l_jX_j]+[l_i'X_i,l_j'X_j]$ lies in $2\overline{\mathfrak{p}}$, and so every element of the form

$$l_1X_1+\ldots+l_kX_k+\sum_{i<j}l_{ij}[X_i,X_j]$$

with $|l_i|\le L_i$ and $|l_{ij}|\le L_iL_j$ lies in $k(k-1)\overline{\mathfrak{p}}$, as required. □

It was established in [1] that nilboxes are also closely related to nilpotent progressions. In the present setting we have the following straightforward relationship.

Lemma 5.3. *Let $X_1, \dots, X_k \in \mathfrak{g}$ and write $x_i := \exp X_i$. Let $L \in \mathbb{N}^k$. Then*

$$\exp(\mathfrak{B}(X_1, \dots, X_k; L)) \subset P(x_1^{1/2}, \dots, x_k^{1/2}; \sqrt{6}L)$$

and

$$P(x_1, \dots, x_k; L) \subset \exp(\mathfrak{B}(\tfrac{1}{2}X_1, \dots, \tfrac{1}{2}X_k; \sqrt{6}L)).$$

Proof. For $l_1X_1 + \dots + l_kX_k + \sum_{i<j} l_{ij}[X_i, X_j] \in \mathfrak{B}(X_1, \dots, X_k; L)$ the Baker–Campbell–Hausdorff formula gives

$$\exp\left(l_1X_1 + \dots + l_kX_k + \textstyle\sum_{i<j} l_{ij}[X_i, X_j]\right) = x_1^{l_1} \dots x_k^{l_k} \prod_{i<j} [x_i, x_j]^{l_{ij} - \frac{1}{2}l_il_j}.$$

To see that this lies in $P(x_1^{1/2}, \dots, x_k^{1/2}; \sqrt{6}L)$ note simply that

$$[x_i, x_j]^{l_{ij} - \frac{1}{2}l_il_j} = [x_i^{1/2}, x_j^{1/2}]^{4l_{ij} - 2l_il_j}.$$

On the other hand, we have

$$\log\left(x_1^{l_1} \dots x_k^{l_k} \prod_{i<j} [x_i, x_j]^{l_{ij}}\right) = l_1X_1 + \dots + l_kX_k + \textstyle\sum_{i<j} (l_{ij} + \frac{1}{2}l_il_j)[X_i, X_j],$$

and so we have similarly that $P(x_1, \dots, x_k; L) \subset \exp(\mathfrak{B}(\frac{1}{2}X_1, \dots, \frac{1}{2}X_k; \sqrt{6}L))$. □

The first conclusion of Lemma 5.3 shows that if $\mathfrak{B}$ is a nilbox of dimension k and H is a subgroup of G normalised by $\mathfrak{B}$ such that $A \subset H(\exp \mathfrak{B})$ then there exists a nilpotent progression P of dimension k normalising H such that $A \subset HP$. However, this would be of little use without some control over the size of HP in relation to the size of $A \subset H(\exp \mathfrak{B})$, and so we now establish this.

Lemma 5.4. *Suppose that $x_1, \dots, x_k$ be elements of a 2-divisible abelian group and that $L_1, \dots, L_k \in \mathbb{N}$. Let $r \in \mathbb{N}$ and let*

$$\begin{aligned} P &= P(x_1, \dots, x_k; L_1, \dots, L_k); \\ P' &= P(\tfrac{1}{2}x_1, x_2 \dots, x_k; 2L_1, L_2 \dots, L_k); \\ P'' &= P(x_1, x_2 \dots, x_k; rL_1, L_2 \dots, L_k) \end{aligned}$$

Then P' lies in the union of 2 translates of P and P'' lies in the union of r translates of P.

Proof. We can express the required unions explicitly. Indeed, $P' \subset \{0, \frac{1}{2}x_1\} + P$ and $P'' \subset \{(-r + 1 + 2i)L_1x_1 : i = 0, \dots, r-1\} + P$. □

Lemma 5.5. *Suppose that $X_1, \dots, X_k \in \mathfrak{g}$ and that $L \in \mathbb{N}^k$. Let $r \in \mathbb{N}$. Then*

$$\mathfrak{B}(\tfrac{1}{2}X_1, \dots, \tfrac{1}{2}X_k; 2rL)$$

lies in the union of at most $O(r)^{O(k^2)}$ translates of $\mathfrak{B}(X_1, \dots, X_k; L)$.

Proof. This follows by iterating Lemma 5.4 if we rewrite $\mathfrak{B}(X_1, \dots, X_k; L)$ as

$$\mathfrak{p}(X_1, \dots, X_k, [X_1, X_2], \dots, [X_{k-1}, X_k]; L_1, \dots, L_k, L_1L_2, \dots, L_{k-1}L_k).$$

□

Proof of Theorem 1.1. Writing $\mathfrak{a} := \log A$, Proposition 4.3 implies that there exist an additive subgroup $\mathfrak{h}$ of $\mathfrak{g}$ and a progression $\mathfrak{p} = \mathfrak{p}(X_1, \dots, X_k; L)$ in $\mathfrak{g}$ such that

$$[\mathfrak{h}, X_i] \subset \mathfrak{h} \text{ for every } i, \tag{5.2}$$

such that $H := \exp \mathfrak{h}$ is a subgroup of G, and satisfying

$$\mathfrak{a} \subset \mathfrak{h} + \overline{\mathfrak{p}} \subset O_K(1)\overline{\mathfrak{a}} \tag{5.3}$$

and

$$k \ll_K 1. \tag{5.4}$$

Writing $\mathfrak{B} := \mathfrak{B}(X_1, \dots, X_k; L)$, we may conclude from (5.1), Lemma 5.2, (5.3) and (5.4) that

$$\mathfrak{a} \subset \mathfrak{h} + \mathfrak{B} \subset O_K(1)\overline{\mathfrak{a}}. \tag{5.5}$$

Condition (5.2) implies that

$$\exp(\mathfrak{h} + \mathfrak{B}) = H(\exp \mathfrak{B}), \tag{5.6}$$

and so the first inclusion of (5.5) implies that $A \subset H(\exp \mathfrak{B})$. Writing $x_i := \log(\frac{1}{2}X_i)$ and $P := P(x_1, \dots, x_k; 4L)$, Lemma 5.3 therefore yields $A \subset HP$. The fact that H is normalised by P follows from (5.2), and so all that remains is to show that $|HP| \ll_K |A|$. However, this follows readily from the second inclusion of (5.5), Proposition 4.2 and Lemmas 5.3 and 5.5. □

Remarks 5.6. Note that here we have containment of A inside HP, rather than the slightly weaker notion of *control* that is needed in [1]. This appears to be largely due to the fact that in [1] the group G is first embedded in a Lie group, and so there is no guarantee that the progressions constructed using the arguments seen here will yield progressions that are contained within the original group G.

To circumnavigate this issue the authors of [1] at various points take dilates of the objects under consideration that place them back into the span of A, and in so doing sacrifice containment but maintain control.

The main difficulty in applying arguments of the type found in [1] to torsion groups comes from the fact that whilst the subgroup $\mathfrak{h}_0$ of $\mathfrak{g}$ given by the Green–Ruzsa theorem in the proof of Proposition 4.3 is automatically a normal subgroup of $\mathfrak{g}$, its counterpart $\exp \mathfrak{h}_0$ is neither normal nor even a subgroup in G. In that sense, the key additional arguments of this note, as compared to [1], are contained in the remainder of the proof of Proposition 4.3.

References

[1] E. Breuillard and B. J. Green. Approximate groups. I. The torsion-free nilpotent case, *J. Inst. Math. Jussieu* **10**(1) (2011), 37-57.

[2] B. J. Green and I. Z. Ruzsa. Freiman's theorem in an arbitrary abelian group, *J. Lond. Math. Soc.* **75**(1) (2007), 163-175.

[3] E. I. Khukhro. p-automorphisms of finite p-groups, *London Math. Soc. Lecture Note Ser.* **246**, Cambridge Univ. Press (1998).

[4] N. Mazza. *Finite p-groups in representation theory*, notes available at `http://sma.epfl.ch/~dietler/Lecture_Notes_Mazza.pdf`.

[5] T. C. Tao and V. H. Vu. Additive combinatorics, *Cambridge studies in advanced mathematics* **105**, Cambridge Univ. Press (2006).

[6] M. C. H. Tointon. Freiman's theorem in an arbitrary nilpotent group, to appear in *Proc. London Math. Soc.*. `arXiv:1211.3989`.