A NOTE ON FREIMAN MODELS

1. Introduction

Let G be a group (not necessarily abelian), and let $s \geqslant 2$ be an integer. Let $A \subseteq G$ be a set, and let $\pi : A \to G'$ be a map. We say that π is a Freiman s-homomorphism if, for every choice of signs $\varepsilon_1, \dots, \varepsilon_s \in \{-1, 1\}$, and for all choices of $x_1, \dots, x_s, y_1, \dots, y_s$ with

$$x_1^{\varepsilon_1} \dots x_s^{\varepsilon_s} = y_1^{\varepsilon_1} \dots y_s^{\varepsilon_s},$$

we have

$$\pi(x_1)^{\varepsilon_1} \dots \pi(x_s)^{\varepsilon_s} = \pi(y_1)^{\varepsilon_1} \dots \pi(y_s)^{\varepsilon_s}.$$

In words, a map π is a Freiman s-homomorphism is a map which preserves those properties of G that can be specified with at most s multiplications with elements of A. If π is injective and if the inverse $\pi^{-1} : \pi(A) \to G$ is also a Freiman k-homomorphism, we say that π is a Freiman isomorphism of order k onto its image.

In the paper [2] I. Z. Ruzsa and the author established a structural result concerning sets A in an *abelian* group G with the "small doubling property", namely that $|A+A| \leqslant K|A|$. A crucial ingredient of the argument was the following result.

Proposition 1.1 ([2], Proposition 1.2)**.** *Suppose that G is abelian, and that $|A + A| \leqslant K|A|$. Let $s \geqslant 2$. Then there is an abelian group G' with $|G'| \leqslant (10sK)^{10K^2}|A|$ such that A is Freiman s-isomorphic to a subset of G'.*

An isomorphic copy of A which is economically contained inside some group G' is called a *good Freiman s-model* for A. In this note we give an example showing that there need not exist good models in the nonabelian setting, at least if one demands that s be large. In fact, our example shows that even a much weaker requirement cannot be satisfied in general, making it almost certain that a radically different approach to questions of Freiman type needs to be found in the nonabelian setting.

Theorem 1.2. *Suppose that $s \geqslant 64$. Then for any n there is a group G and a set $A \subseteq G$ with $|A| > n$ and $|A \cdot A| < 2|A|$ such that if $A' \subseteq A$ is any set with $|A'| \geqslant |A|^{22/23}$, and if $\pi : A' \to G'$ is a Freiman s-isomorphism onto its image, then $|G'| \geqslant \frac{1}{32}|A'|^{23/22}$.*

We note that our example also has $|A \cdot A \cdot A| < 3|A|$. In the nonabelian setting a "small tripling" property such as this does not follow automatically from the small doubling condition, as is shown by simple examples (cf. [4, p. 94]). The number 64 could probably be reduced somewhat, but new ideas would certainly be required if one wanted to take $s = 2$.

Acknowledgement. A previous version of Theorem 1.2 was privately circulated by the author, but Elon Lindenstrauss and Zhiren Wang indicated a flaw in the argument. I thank them for drawing this serious oversight to our attention, and for subsequent helpful communications.

2. The counterexample

In this section we prove Theorem 1.2. The set A is not hard to describe; set $G = \begin{pmatrix} 1 & \mathbb{Z}/p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} \\ 0 & 1 & \mathbb{Z}/p\mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$, the Heisenberg group over $\mathbb{Z}/p\mathbb{Z}$, and define

$$A := \{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : |x| \leqslant p^{7/8} \}.$$

It is clear that $|A \cdot A| < 2|A|$. It is much less clear that no large subset of A is Freiman-isomorphic to a subset of a smallish group, and this will be our task in the rest of this section. Suppose that $A' \subseteq A$ has size at least $|A|^{22/23}$ and that $\pi : A' \to G'$ is a Freiman s-isomorphism onto its image, where $s \geqslant 64$. Note in particular that $|A'| > p^{11/4}$.

We start with some basic remarks about Freiman homomorphisms. Suppose that A is any set and that $\pi : A \to B$ is a Freiman s-homomorphism. If $s' \leqslant s$ and if $\varepsilon_1, \dots, \varepsilon_{s'}$ is any choice of signs in $\{-1, 1\}$ then π induces a well-defined map from $A^{\varepsilon_1} \cdots A^{\varepsilon_{s'}}$ to B via

$$\tilde{\pi}(a_1^{\varepsilon_1} \cdots a_{s'}^{\varepsilon_{s'}}) := \pi(a_1)^{\varepsilon_1} \cdots \pi(a_{s'})^{\varepsilon_{s'}}.$$

We will abuse notation by referring to this map as π. Note that π is a Freiman $\lfloor s/s' \rfloor$-homomorphism. All of these remarks apply, of course, to isomorphisms.

Now for economy of notation write $[x, y, z]$ for the matrix $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$ and $*$ for the operation of matrix multiplication. Thus

$$[x_1, y_1, z_1] * [x_2, y_2, z_2] = [x_1 + x_2, y_1 + y_2, z_1 + z_2 + x_1 y_2].$$

Suppose that $\pi : A' \to G'$ is a Freiman s-homomorphism onto its image, and that our aim is to show that G' is significantly larger than A'. We may assume, without any loss of generality, that G' is the group generated by the $\pi(a)$, $a \in A'$. Now G is 2-step nilpotent, that is to say the triple commutator $[a_1, [a_2, a_3]]$ is equal to the identity for all $a_1, a_2, a_3 \in G$. This may be expanded as

$$a_1 a_2 a_3 a_2^{-1} a_3^{-1} a_1^{-1} a_3 a_2 a_3^{-1} a_2^{-1} = \mathrm{id}_G = tttt^{-1}t^{-1}t^{-1}ttt^{-1}t^{-1},$$

where $t \in G$ is arbitrary. Suppose that $s \geqslant 10$ and that $a_1, a_2, a_3, t \in A$. Then this relation is preserved under π and we obtain $[\pi(a_1), [\pi(a_2), \pi(a_3)]] = \mathrm{id}_{G'}$.

Now it seems to be a reasonably standard fact in group theory that if generators $x_1, \dots, x_n$ of some finite group Γ satisfy the commutation relations

$$[x_i, [x_j, x_k]] = \mathrm{id} \tag{2.1}$$

for all i, j, k then the group is 2-step nilpotent. In fact a result of this type holds for higher commutators as well, and has to do with specifying bases for free nilpotent groups (see, for example, [3, Chapter 11]). In the 2-step case one may proceed quite directly using the commutator relation

$$[ab, c] = [a, [b, c]] \cdot [b, c] \cdot [a, c]. \tag{2.2}$$

Suppose, without loss of generality, that the set $X = \{x_1, \dots, x_n\}$ is a maximal subset of Γ for which (2.1) is always satisfied. Then two applications of (2.2) imply that $[[x_1x_2, x_j], x_k] = \mathrm{id}$ for all j and k. A further application gives $[x_1x_2, [x_1x_2, x_i]] = \mathrm{id}$, and so we see that $x_1x_2 \in X$, that is to say X is closed under multiplication. Since Γ is finite it follows immediately that $X = \Gamma$.

Returning to our argument, it follows that G' is 2-step nilpotent. From further general results in group theory (see, for example, [3, Theorem 10.3.4]) G' is the direct product of its Sylow subgroups. A special rôle will be played in our argument by the Sylow p-subgroup, which we denote by G'_p. Our first task is to show that G'_p must be nontrivial.

Lemma 2.1. *Suppose that $B \subseteq G$ is any set of size at least $p^{11/4}$. Then $B^4 \cdot B^{-4} \cdot B^4 \cdot B^{-4}$ contains the subgroup $[0, 0, \mathbb{Z}/p\mathbb{Z}]$.*

Proof. Write $\psi : G \to (\mathbb{Z}/p\mathbb{Z})^2$ for projection onto the first two coordinates. Clearly $\psi(B)$ has size at least $p^{7/4}$, and hence it contains horizontal and vertical fibres of size at least $p^{3/4}$. It follows that $\psi(B^2) = \psi(B) + \psi(B)$ contains a product set $X \times Y$ with $|X|, |Y| \geqslant p^{3/4}$. Using the fact that the commutator of the elements $[x_1, y_1, z_1]$ and $[x_2, y_2, z_2]$ is $[0, 0, x_1y_2 - x_2y_1]$, we see that $B^4 \cdot B^{-4} \cdot B^4 \cdot B^{-4}$ contains $[0, 0, S]$, where

$$S := \{x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 : x_1, x_2, x_3, x_4 \in X, y_1, y_2, y_3, y_4 \in Y\}.$$

We claim that $S = \mathbb{Z}/p\mathbb{Z}$. To prove this, we use a simple and well-known lemma of Vinogradov [5, Lemma 10a], which tells us that

$$|\sum_{x \in X} \sum_{y \in Y} e(rxy/p)| \leqslant \sqrt{p|X||Y|}$$

when $r \neq 0$. Now the number of solutions Σ_t to $x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 = t$ is

$$\frac{1}{p} \sum_{r \in \mathbb{Z}/p\mathbb{Z}} \sum_{\substack{x_1,x_2,x_3,x_4 \in X \\ y_1,y_2,y_3,y_4 \in Y}} e\Big(\frac{r(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 - t)}{p}\Big).$$

This may be split into the $r = 0$ term, which has size $|X|^4|Y|^4$, plus $p - 1$ terms with $r \neq 0$, each of which has magnitude at most $p^2|X|^2|Y|^2$ by Vinogradov's inequality. It follows that $\Sigma_t > |X|^2|Y|^2(|X|^2|Y|^2 - p^3) \geqslant 0$, and the result follows. □

Apply the preceding lemma with $B = A'$, and set $A_1 := B^4 \cdot B^{-4} \cdot B^4 \cdot B^{-4}$. Thus A_1 contains $[0, 0, \mathbb{Z}/p\mathbb{Z}]$. If $s \geqslant 64$ then π induces a map on $A_1 \cdot A_1 \cdot A_1 \cdot A_1$ with the property that

$$\pi(ab) = \pi(a)\pi(b) \qquad \text{whenever } a, b \in A_1 \cdot A_1. \tag{2.3}$$

In particular, G' contains a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

We divide into cases according to the size of the Sylow p-subgroup G'_p, which we now know to be nontrivial.

Case 1. $|G'_p| \geqslant p^3$. Then of course $|G'| \geqslant p^3$ and we are done.

Case 2. $|G'_p| = p^2$. Then G'_p is abelian. Suppose that $G' \cong G'_p \times H$, and write π_H for the composition of π with projection onto H. Note that $|H| \leqslant p^{1-c_0+\eta}$. Write $A_1(t) := \{a \in A_1 : \pi_2(a) = t\}$. Since every pair of elements in $G'_p \times \{t\}$ commutes, the same is true of $A_1(t)$. However it is not hard to see that any subset of G with this property is contained in some set of the form $\{[x,y,z] : \lambda x = \mu y\}$, where λ, μ are not both zero. If $\mu \neq 0$ then such a set has intersection at most $16|A|/p$ with A_1. Since the set $\{[x,y,z] : x = 0\}$ has size p^2, we have the bound

$$|A'| \leqslant |A_1| = \sum_{t \in H} |A_1(t)| \leqslant p^2 + \frac{16|A||H|}{p}.$$

Since $|A'| \geqslant 2p^2$ this implies that $16|A||H| \geqslant p|A'|$ and hence that $|G'| = p^2|H| \geqslant p^3|A'|/16|A| \geqslant \frac{1}{32}p^{1/8}|A'| \geqslant \frac{1}{32}|A'|^{23/22}$, as required.

Case 3. $G'_p \cong \mathbb{Z}/p\mathbb{Z}$. Then $G' \cong \mathbb{Z}/p\mathbb{Z} \times H$ for some group H whose order has no factor of p. Write $\pi_1 : A_1 \cdot A_1 \to \mathbb{Z}/p\mathbb{Z}$ for the composition of π with projection onto the first factor. Since $\pi([0,0,1])$ has order p, we may assume without loss of generality that $\pi_1([0,0,1]) = 1$. Now by (2.3) we have

$$\begin{aligned} \pi_1([x,y,z+z']) &= \pi_1([x,y,z] * [0,0,z']) \\ &= \pi_1([x,y,z]) + \pi_1([0,0,z']) \\ &= \pi_1([x,y,z]) + z', \end{aligned}$$

and so π_1 has the form

$$\pi_1([x,y,z]) = \rho(x,y) + z$$

for some map $\rho : (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$ (for all $[x,y,z] \in A_1 \cdot A_1$).

Suppose that $[x_1,y_1,z_1],[x_2,y_2,z_2] \in A_1$. Then the relation $\pi_1([x_1,y_1,z_1]\cdot[x_2,y_2,z_2]) = \pi_1([x_1,y_1,z_1]) + \pi([x_2,y_2,z_2])$ tells us that

$$\rho(x_1,y_1) + \rho(x_2,y_2) = \rho(x_1+x_2, y_1+y_2) + x_1y_2.$$

By symmetry we clearly also have

$$\rho(x_1,y_1) + \rho(x_2,y_2) = \rho(x_1+x_2, y_1+y_2) + x_2y_1$$

and so $x_1y_2 = x_2y_1$. This implies that A_1 lies inside some set $\{[x,y,z] : \lambda x + \mu y = 0\}$, and so $|A_1| \leqslant p^2$. This is obviously a contradiction. $\square$

References

[1] A. A. Glibichuk, *Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem,* Math. Notes, **79** (2006), 356–365.
[2] B. J. Green and I. Z. Ruzsa, *Freiman's theorem in an arbitrary abelian group,* Jour. London Math. Soc. **75** (2007), no. 1, 163–175.
[3] P. Hall, Theory of Groups.
[4] T. C. Tao and V. H. Vu, *Additive Combinatorics,* Cambridge University Press 2006.
[5] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers,* Dover.