ON FREIMAN'S $3K - 4$ THEOREM

Prem Prakash Pandey
Department of Mathematics, IISER Berhampur, Berhampur, Odisha, India
premshivaganga@gmail.com

Received: 5/17/17, Revised: 9/28/17, Accepted: 2/7/18, Published: 2/19/18

Abstract

In this article we establish Freiman's $3k - 4$ Theorem, under some restrictions, for the groups $\mathbb{Z} \times G$, where G is any abelian group. Some consequences are also derived. Furthermore, the arguments of the article extend to cover the cases when G is non-abelian.

1. Introduction

Let G be an abelian group (written additively), and let A and B be finite subsets of G. The sumset of A and B is defined as $A + B := \{a + b : a \in A, b \in B\}$. If $G = \mathbb{Z}$, the group of integers, then it is well known that

$$|A + B| \geq |A| + |B| - 1. \tag{1}$$

The size of the cardinality $|A+B|$ has bearing on the structure of the sets A and B. In relation (1) equality holds if and only if A and B are arithmetic progressions with the same common differences. For the cyclic group $G = \mathbb{Z}/p\mathbb{Z}$ of prime order, the analogue of (1) is given by the classical theorem of Cauchy-Davenport (see for example [14] or [12]). For subsets A and B of $\mathbb{Z}/p\mathbb{Z}$ one has

$$|A + B| \geq \min\{p, |A| + |B| - 1\}. \tag{2}$$

In [15], Vosper proved that if $|A| + |B| - 1 < p$, then equality in (2) holds if and only if A and B are arithmetic progressions with the same common differences.

In [5], Freiman considered the group $G = \mathbb{Z}$ and proved the following structure theorem.

Theorem 1 ($3k - 4$ Theorem)**.** *If A is a set of integers of cardinality $k \geq 2$ and the inequality $|A + A| \leq 3k - 4$ holds, then A is a subset of an arithmetic progression of length $k + b$. Here b is given by $|A + A| = 2k - 1 + b$.*

Extending this theorem to other groups is a well-pursued problem (see the $3k-4$ conjecture in [11] or see [2, 6, 7, 8, 9, 10, 13]). In this article we consider groups of the form $\mathbb{Z} \times G$, where G is any abelian group, and prove the following theorem.

Theorem 2. *Let $k \geq 3$ be any integer and G be an abelian group. Consider a subset $\mathcal{A} = \{(a_i, x_i) : 1 \leq i \leq k\}$ of $\mathbb{Z} \times G$ such that the projection to the first coordinate, restricted to $\mathcal{A}$, is injective. If $|\mathcal{A} + \mathcal{A}| \leq 3k-4$, then $\mathcal{A}$ is a subset of an arithmetic progression of length $k+b$, where $|\mathcal{A}+\mathcal{A}| = 2k-1+b$.*

It is expected that the assumption "the projection to the first coordinate, restricted to $\mathcal{A}$, is injective" in Theorem 2 may be dropped (see [11] or [3]). In this direction we mention the works of Deshouillers and Freiman [4], where they prove a structure theorem (Theorem 2 in [4]) for subsets $\mathcal{A}$ of $\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$, without any assumption on the projection to the first coordinate, but under a stronger assumption on the sumset $|\mathcal{A}+\mathcal{A}|$. In [1] (see Theorem 1), authors have improved the result of Deshouillers and Freiman to cover all subsets $\mathcal{A}$ of $\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$ with $|\mathcal{A}+\mathcal{A}| < 2.5|\mathcal{A}|$. It seems that the method of [1] can be improved to cover sets with doubling constant more than 2.5. But, to us, it seems that it will be very lengthy and it is not clear if one can obtain a $3k-4$ type theorem along those lines.

2. Proof of Theorem 2

Before proceeding with the proofs we make some simplifications. Without loss of generality (as 2-isomorphisms take arithmetic progressions to arithmetic progressions, and translations and multiplications by a constant are 2-isomorphisms), we assume that $a_1 = 0 < a_2 < \ldots < a_k$ and the greatest common divisor of $a_1, \ldots, a_k$ is 1. We put $A = \{a_1, \ldots, a_k\}$, and $R = min\{k, a_k - k + 3\}$. We shall continue with these notations and assumptions throughout the article.

To prove Theorem 2 we introduce the concept of "structured sets". For a pair (X, A) of subsets of $\mathbb{Z}$ with $X \subset A$, we use the notation $X^{(1)} = (X + X - X) \cap A$ and for $i > 1$ we shall write $X^{(i)} = (X^{(i-1)})^{(1)}$. We define $X^{(\infty)} = \cup_{i \geq 1} X^{(i)}$. Note that the definition of $X^{(\infty)}$ depends on the pair (X, A).

A subset A of $\mathbb{Z}$ is called a *structured set* if there is a two element subset $X = \{g_1, g_2\} \subset A$ such that $g_2 - g_1 = 1$ and $A = X^{(\infty)}$. A subset $\mathcal{A} \subset \mathbb{Z} \times G$ is said to be *structured* if the image $\pi_1(\mathcal{A})$ of the first projection is a structured subset of $\mathbb{Z}$ and there are $x, y \in G$ satisfying $x_i = a_i x + y$. The motivation for this definition is based on the following.

Consider a subset $\mathcal{A} = \{(a_i, x_i) : 1 \leq i \leq s\}$ of $\mathbb{Z} \times G$, with small doubling, so that the implication $a_i + a_j = a_k + a_l \Longrightarrow x_i + x_j = x_k + x_l$ is true. It is natural to expect that there are elements $x, y \in G$ such that $x_i = a_i x + y$, for all i. Along the lines of the work of the author [13], we prove that the sets with small doubling are structured sets. In this direction we prove the following theorem.

Theorem 3. *Let $k \geq 3$ be any integer and G be an abelian group. Consider a subset $\mathcal{A} = \{(a_i, x_i) : 1 \leq i \leq k\}$ of $\mathbb{Z} \times G$ such that the projection to the first coordinate, restricted to $\mathcal{A}$, is injective. If $|\mathcal{A}+\mathcal{A}| \leq 3k-4$, then $\mathcal{A}$ is 2-isomorphic to a structured set.*

We will use Theorem 3 to prove Theorem 2. We begin with the following elementary lemma.

Lemma 1. *We have $|A + A| \geq 2k + R - 3$.*

Proof. Note that $R \leq k$. If the lemma does not hold then we have $|A + A| < 2k + R - 3 \leq 3k - 3$. Thus $|A + A| = 2k - 1 + b$ with $b < k - 2$. Now by Theorem 1 we see that A is contained in an arithmetic progression of length $k+b$. Hence we have $a_k \leq k+b-1$ and consequently $R \leq b+2$. This gives $2k+R-3 \leq 2k-1+b = |A+A|$, which is a contradiction to our assumption $|A + A| < 2k + R - 3$. □

We have one more elementary lemma.

Lemma 2. *If a_{k-1} and a_k are not successive terms of any arithmetic progression containing A, then, for $B = \{a_1, a_2, \ldots, a_{k-1}\}$, we have $|A + A| \geq |B + B| + 3$.*

Proof. Note that $a_k + a_k, \ldots, a_k + a_1$ are k distinct elements in $A + A$. Clearly $a_k + a_k, a_k + a_{k-1}$ are not in $B + B$. We claim that there is $i < k - 1$ such that $a_k + a_i$ is not in $B + B$, this will prove the lemma.

We consider the decreasing arithmetic progression $c_1 = a_k$, $c_2 = a_{k-1}, c_3 = a_k - 2(a_k - a_{k-1}), \ldots$. Then A is not contained in the arithmetic progression $c_1, c_2, \ldots$. If $a_k + a_{k-2} \in B+B$ then $a_k+a_{k-2} = 2a_{k-1}$ and consequently $a_{k-2} = c_3$. Thus, either $a_k+a_{k-2} \notin B+B$ or $a_{k-2} = c_3$. If former is the case then the claim is established. In the latter case, i.e. $a_{k-2} = c_3$, the element a_{k-2} lies in the arithmetic progression $c_1, c_2, \ldots$. Continuing this way we conclude that either there is some $i < k - 1$ such that $a_k + a_i$ is not in $B + B$ or A is contained in the arithmetic progression $c_1, c_2, \ldots$. Since A is not contained in the arithmetic progression $c_1, c_2, \ldots$, the claim is established. □

Proof. (Theorem 3) We use induction on k. For $k = 3$, we have $|A + A| \geq 5$ and $3k - 4 = 5$. Thus

$$|\mathcal{A} + \mathcal{A}| = |A + A| = 3k - 4. \tag{3}$$

Since $\min(A) = 0$ and $gcd(A) = 1$, by Equation (3) we have $A = \{0, 1, 2\}$. Also, Equation (3) forces $x_i+x_j = x_k+x_l$, whenever $a_i+a_j = a_k+a_l$. Let $x, y \in G$ be such that $x_1 = a_1x+y$ and $x_2 = a_2x+y$. If $x_3 \neq a_3x+y$, then $|\mathcal{A}+\mathcal{A}| > |A+A| = 3k-4$, which is a contradiction. Thus $\mathcal{A}$ is a structured set.

Now we assume that $k > 3$ and put $\mathcal{B} = \{(a_i, x_i) : 1 \le i \le k-1\}$. We consider following two cases.

`Case 1`: $\mathcal{B}$ is a structured set. Since $\mathcal{B}$ is structured, $\pi_1(\mathcal{B})$ is structured and there exist $x, y \in G$ such that $x_i = a_i x + y$ for all $i \le k-1$. If $(\mathcal{B}+\mathcal{B}) \cap ((a_k, x_k)+\mathcal{B}) \ne \emptyset$ then there are indices $u, v, w \le k-1$ such that

$$(a_k, x_k) + (a_u, x_u) = (a_v, x_v) + (a_w, x_w).$$

From this we see that $a_k = a_v + a_w - a_u$ and $x_k = x_v + x_w - x_u$. Now it immediately follows that $\mathcal{A}$ is structured. We may now assume that $(\mathcal{B}+\mathcal{B}) \cap ((a_k, x_k)+\mathcal{B}) = \emptyset$, so that $|\mathcal{A}+\mathcal{A}| \ge |\mathcal{B}+\mathcal{B}| + |\mathcal{B}|$; the consideration of $(a_k, x_k) + (a_k, x_k)$ leads to

$$|\mathcal{A}+\mathcal{A}| \ge |\mathcal{B}+\mathcal{B}| + |\mathcal{B}| + 1. \tag{4}$$

Using the trivial lower bound on the first coordinate we find

$$|\mathcal{B}+\mathcal{B}| \ge 2|\mathcal{B}| - 1. \tag{5}$$

Using this in (4) we get

$$|\mathcal{A}+\mathcal{A}| \ge 3|\mathcal{B}| = 3k-3,$$

which is a contradiction. This contradiction proves the theorem in this case.

`Case 2`: $\mathcal{B}$ is not structured. By the induction hypothesis we get $|\mathcal{B}+\mathcal{B}| \ge 3(k-1)-3$. If $a_{k-1} \ne a_k - 1$, then using Lemma 2, with $A = \pi_1(\mathcal{A})$ and $B = \pi_1(\mathcal{B})$, one immediately obtains $|\mathcal{A}+\mathcal{A}| \ge |\mathcal{B}+\mathcal{B}| + 3 \ge 3k-3$, which is a contradiction.

When $a_{k-1} = a_k - 1$, one can solve for $x, y \in G$ satisfying $x_k = a_k x + y$ and $x_{k-1} = a_{k-1}x + y$. Observe that, by considering first coordinates, the two elements (a_k+a_k, x_k+x_k) and $(a_k+a_{k-1}, x_k+x_{k-1})$ are in $\mathcal{A}+\mathcal{A}$ but not in $\mathcal{B}+\mathcal{B}$. If there is an $i < k-1$ such that $(a_k+a_i, x_k+x_i) \notin \mathcal{B}+\mathcal{B}$ then we get $|\mathcal{A}+\mathcal{A}| \ge |\mathcal{B}+\mathcal{B}|+3 \ge 3k-3$, which is a contradiction. Hence $(a_k+a_i, x_k+x_i) \in \mathcal{B}+\mathcal{B}$ holds for all $i < k-1$. Since $(a_k+a_{k-2}, x_k+x_{k-2}) \in \mathcal{B}+\mathcal{B}$, using order relation of $\mathbb{Z}$, we obtain $a_k+a_{k-2} = 2a_{k-1}$ and $x_k + x_{k-2} = 2x_{k-1}$. As a consequence $x_{k-2} = a_{k-2}x + y$. This proves that the set $\{(a_{k-2}, x_{k-2}), (a_{k-1}, x_{k-1}), (a_k, x_k)\}$ is a structured set. Continuing this way we see that $\mathcal{A}$ is a structured set. □

We now deduce Theorem 2 from Theorem 3. We have $|A + A| \le 3|A| - 4$. By Lemma 1 $2k + R - 3 \le 3k - 4$. Thus, $R \le k-1$ and $a_k = k + R - 3$. Consequently, A is contained in the interval $[0, k+R-3]$ and lies in an arithmetic progression of length $k+R-2$.

By Theorem 3, there exist $x, y \in G$ such that $x_i = a_i x + y$, for all i. Thus $\mathcal{A}$ is contained in an arithmetic progression of length $k + R - 2$.

We have $|A + A| = |\mathcal{A} + \mathcal{A}| = 2k - 1 + b$. From Lemma 1 one has $2k + R - 3 \le$

$2k-1+b$, that is, $R-2 \le b$. Consequently, $\mathcal{A}$ is contained in an arithmetic progression of length $k+b$.

Next we give some consequences of Theorem 3. We have not seen these results in literature, and these are easily deduced from Theorem 3.

Corollary 1. *Let A be a subset of $k \ge 3$ integers with $\min(A) = 0$ and the greatest common divisor of the elements of A is 1. If A is not a structured set, then $|A+A| > 3|A|-4$.*

Proof. Let G be any finite abelian group. Consider the subset $\mathcal{A} = \{(a,0) : a \in A\}$ of $\mathbb{Z} \times G$. If $|A+A| \le 3|A|-4$, then Theorem 2 will give that $\mathcal{A}$ is a structured set, and by definition, so is A. □

The following corollary gives a sufficient condition for a subset of $\mathbb{Z}$ to be a structured set.

Corollary 2. *Let $N \ge 2$, and $A \subset [0, N-1]$. If $|A| \ge 2N/3+1$, then A is a structured set.*

Proof. For $N \le 4$, it is easy to see that A is structured. So assume $N \ge 5$. It is clear that the greatest common divisor of elements of A is 1. With a translation, we can assume that $\min(A) = 0$.

Here, $A+A \subset [0, 2N-2]$ and hence $|A+A| \le 2N-1$. Since $2N/3+1 \le |A|$, we get $2N-1 \le 3|A|-4$. Thus, A satisfies the hypothesis of Corollary 1, and it follows that, up to a translation, A is a structured set. Since translates of structured sets are structured, it follows that, A is structured. □

The set $A = [0, N-1] \setminus \{a < N : a \equiv 2 \pmod 3\}$ is not a structured set, though $|A| \ge 2N/3$. But in this case we note that the sumset $A+A$ has cardinality bigger than $3|A|-4$.

3. Non-abelian Groups

In this section we briefly mention how Theorem 3 (and hence Theorem 2) can be proved when G is a non-abelian group (in which case we use multiplication as operation of G). We continue with the notations of Section 2. In this case we define a subset $\mathcal{A} \subset \mathbb{Z} \times G$ to be a *structured set* if the image $\pi_1(\mathcal{A})$ of the first projection is a structured subset of $\mathbb{Z}$, and there are commuting elements $x, y \in G$ satisfying $x_i = x^{a_i} y$.

Proof. (Theorem 3, when G is non-abelian) We use induction on k. For $k = 3$, we have $|A+A| \ge 5$ and $3k-4 = 5$. Thus

$$|\mathcal{A}+\mathcal{A}| = |A+A| = 3k-4. \tag{6}$$

Since $\min(A) = 0$ and $gcd(A) = 1$, by Equation (6) we have $A = \{0, 1, 2\}$. Also, Equation (6) forces $x_i x_j = x_k x_l$, whenever $a_i + a_j = a_k + a_l$. Let $x, y \in G$ be such that $x_1 = x^{a_1} y$ and $x_2 = x^{a_2} y$ (which is always possible, as $a_1 = 0, a_2 = 1$). From Equation (6) it follows that $x_1 x_2 = x_2 x_1$. From this it is clear that x and y commute. As $a_1 + a_3 = 2a_2$, we have $x_1 x_3 = x_2^2$. From which it follows that $x_3 = x^{a_3} y$. Thus $\mathcal{A}$ is a structured set.

Now we assume that $k > 3$ and put $\mathcal{B} = \{(a_i, x_i) : 1 \le i \le k-1\}$.

`Case 1:` $\mathcal{B}$ is a structured set. Since $\mathcal{B}$ is structured, $\pi_1(\mathcal{B})$ is structured and there exist commuting elements $x, y \in G$ such that $x_i = x^{a_i} y$ for all $i \le k-1$. If $(\mathcal{B} + \mathcal{B}) \cap ((a_k, x_k) + \mathcal{B}) \neq \emptyset$ then there are indices $u, v, w \le k-1$ such that

$$(a_k, x_k) + (a_u, x_u) = (a_v, x_v) + (a_w, x_w).$$

From this we see that $a_k = a_v + a_w - a_u$ and $x_k = x_v x_w x_u^{-1}$. Now it immediately follows that $\mathcal{A}$ is structured.

We may now assume that $(\mathcal{B} + \mathcal{B}) \cap ((a_k, x_k) + \mathcal{B}) = \emptyset$, so that $|\mathcal{A} + \mathcal{A}| \ge |\mathcal{B} + \mathcal{B}| + |\mathcal{B}|$; the consideration of $(a_k, x_k) + (a_k, x_k)$ leads to

$$|\mathcal{A} + \mathcal{A}| \ge |\mathcal{B} + \mathcal{B}| + |\mathcal{B}| + 1. \tag{7}$$

Using the trivial lower bound on the first coordinate we find

$$|\mathcal{B} + \mathcal{B}| \ge 2|\mathcal{B}| - 1. \tag{8}$$

Using this in (7) we get

$$|\mathcal{A} + \mathcal{A}| \ge 3|\mathcal{B}| = 3k - 3,$$

which is a contradiction. This contradiction proves the theorem in this case.

`Case 2:` $\mathcal{B}$ is not structured. By induction hypothesis we get $|\mathcal{B}+\mathcal{B}| \ge 3(k-1)-3$. If $a_{k-1} \neq a_k - 1$, then using Lemma 2, with $A = \pi_1(\mathcal{A})$ and $B = \pi_1(\mathcal{B})$, one immediately obtains $|\mathcal{A} + \mathcal{A}| \ge |\mathcal{B} + \mathcal{B}| + 3 \ge 3k - 3$, which is a contradiction. Similarly we otain a contradiction if $x_k x_{k-1} = x_{k-1} x_k$. Thus, we assume that $x_k x_{k-1} = x_{k-1} x_k$ and $a_{k-1} = a_k - 1$. One can solve for $x, y \in G$ satisfying $x_k = x^{a_k} y$ and $x_{k-1} = x^{a_{k-1}} y$. Since x_k and x_{k-1} commute, it follows that x and y commute. Observe that, by considering first coordinate, the two elements $(a_k + a_k, x_k x_k)$ and $(a_k + a_{k-1}, x_k x_{k-1})$ are in $\mathcal{A}+\mathcal{A}$ but not in $\mathcal{B}+\mathcal{B}$. If there is an $i < k-1$ such that $(a_k + a_i, x_k x_i) \notin \mathcal{B}+\mathcal{B}$ then we get $|\mathcal{A}+\mathcal{A}| \ge |\mathcal{B}+\mathcal{B}|+3 \ge 3k-3$, which is a contradiction. Hence $(a_k + a_i, x_k x_i) \in \mathcal{B}+\mathcal{B}$ holds for all $i < k-1$. Since $(a_k + a_{k-2}, x_k x_{k-2}) \in \mathcal{B}+\mathcal{B}$, using order relation of $\mathbb{Z}$, we obtain $a_k + a_{k-2} = 2a_{k-1}$ and $x_k x_{k-2} = x_{k-1}^2$. As a consequence $x_{k-2} = x^{a_{k-2}} y$. This proves that the set $\{(a_{k-2}, x_{k-2}), (a_{k-1}, x_{k-1}), (a_k, x_k)\}$ is a structured set. Continuing this way we see that $\mathcal{A}$ is a structured set. $\square$

Acknowledgements. We would like to thank the anonymous referee for improving the presentation of the article.

References

[1] R. Balasubramanian, P. P. Pandey, On a theorem of Deshouillers and Freiman, *European J. Comb.*, to appear.

[2] Y. Bilu, Structure of sets with small sumsets, *Asterique* **258** (1999), 77-108.

[3] Y. F. Bilu, V. F. Lev and I. Z. Ruzsa, Rectification principles in additive number theory, *Discrete Comput. Geom.* **19** (1998), 343-353.

[4] Jean-Marc Deshouillers, G. Freiman, A step beyong Kneser's theorem for finite abelian groups, *Proc. London Math. Soc.* **86** (2003), no. 1, 1-28.

[5] G. Freiman, On the addition of finite sets. I. *Izv. Vyss. Ucebn. Zaved. Matematika 6* **13** (1959), 202-213.

[6] G. Freiman, Inverse problems of the additive theory of numbers. On the addition of sets of residues with respect to a prime modulus, *Dokl. Akad. Nauk SSSR* **141** (1961) 571-573 (Russian), *Soviet Math. Dokl.* **2** (1961) 1520-1522 (English).

[7] G. Freiman, *Foundations of a Structural Theory of set Addition, Translations of Mathematical Monographs 37*, American Mathematical Society, Providence, RI, 1973.

[8] G. Freiman, Structure theory of set addition, *Asterisque* **258** (1999) 1-33.

[9] G. A. Freiman, M. Herzog, P. Longobardi, M. Maj, Small doubling in ordered groups, *J. Aust. Math. Soc.* **96** (2014), no. 3, 316-325.

[10] Y. Hamidoune, A. Llado, O. Sera, On subsets with small product in torsion free groups, *Combinatorica* **18** (4) (1998), 529-540.

[11] Y. Hamidoune, O. Serra, G. Zemor, t On the critical pair theory in $\mathbb{Z}/p\mathbb{Z}$, *Acta Arithmetica*, **121.2** (2006), 99-115.

[12] M. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets, Graduate Texts in Mathematics 165*, Springer-Verlan, New York, 1996.

[13] P. P. Pandey, The $3k-4$ Theorem for ordered groups, to appear in *Bulletin of Aust. Math. Soc.*

[14] T. Tao, V. Vu, *Additive Combinatorics*, Cambridge Studies in Mathematics 105, Cambridge, 2006.

[15] A. G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* **31** (1956) 200-205.