Astérisque

JOHN STEINIG

# On Freiman's theorems concerning the sum of two finite sets of integers

*Astérisque*, tome 258 (1999), p. 129-140
<http://www.numdam.org/item?id=AST_1999__258__129_0>

*Astérisque* **258**, 1999, p. 129–140

# ON FREIMAN'S THEOREMS CONCERNING THE SUM OF TWO FINITE SETS OF INTEGERS

*by*

John Steinig

***Abstract.*** — Details are provided for a proof of Freiman's theorems [1] which bound $|M+N|$ from below, where $M$ and $N$ are finite subsets of $\mathbb{Z}$.

## 1. Introduction

If $M$ and $N$ are subsets of $\mathbb{Z}$, their sum $M+N$ is the set

$$M+N := \{x \in \mathbb{Z} : x = b+c,\ b \in M,\ c \in N\}.$$

If a set $E \subset \mathbb{Z}$ is finite and non-empty, its cardinality will be denoted by $|E|$, and its largest and smallest element by $\max(E)$ and $\min(E)$, respectively. If $A$ is some collection of integers, say $a_1, \ldots, a_k$, not all zero, their greatest common divisor will be denoted by $(a_1, \ldots, a_k)$, or by $\gcd(A)$.

Now let $M$ and $N$ be finite sets of non-negative integers, such that $0 \in M \cap N$, say

$$M = \{b_0, \ldots, b_{m-1}\} \quad \text{with} \quad b_0 = 0 \quad \text{and} \quad b_i < b_{i+1} \quad (\text{all } i) \tag{1.1}$$

and

$$N = \{c_0, \ldots, c_{n-1}\} \quad \text{with} \quad c_0 = 0 \quad \text{and} \quad c_i < c_{i+1} \quad (\text{all } i). \tag{1.2}$$

It is easily seen that

$$|M+N| \geq |M| + |N| - 1 \tag{1.3}$$

(consider $b_0, \ldots, b_{m-1}, b_{m-1}+c_1, \ldots, b_{m-1}+c_{n-1}$).

The following two theorems of Freiman's [**1**] give a better lower bound for $|M+N|$, when additional conditions are imposed on $M$ and $N$.

**Theorem X.** *Let $M$ and $N$ be finite sets of non-negative integers with $0 \in M \cap N$, as in (1.1) and (1.2). If*

$$c_{n-1} \leq b_{m-1} \leq m+n-3 \tag{1.4}$$

*or*

$$c_{n-1} < b_{m-1} = m+n-2, \tag{1.5}$$

**1991** ***Mathematics Subject Classification.*** — 11 B 13.
***Key words and phrases.*** — Inverse theorems, sumsets of integers.

*then*

$$|M+N| \geq b_{m-1} + n\,. \tag{1.6}$$

*If*

$$c_{n-1} = b_{m-1} \leq m+n-3\,, \tag{1.7}$$

*then*

$$|M+N| \geq b_{m-1} + \max(m,n)\,. \tag{1.8}$$

**Theorem XI.** *Let $M$ and $N$ be finite sets of non-negative integers with $0 \in M \cap N$, as in (1.1) and (1.2). If*

$$\max(b_{m-1}, c_{n-1}) \geq m+n-2 \tag{1.9}$$

*and*

$$(b_1, \ldots, b_{m-1}, c_1, \ldots, c_{n-1}) = 1\,, \tag{1.10}$$

*then*

$$|M+N| \geq m+n-3+\min(m,n)\,. \tag{1.11}$$

We remark here that if $\min(m,n) \geq 2$, then any sets $M$ and $N$ which satisfy (1.4) or (1.5) also satisfy (1.10). In fact, either of these conditions implies that $\gcd(M) = 1$ or $\gcd(N) = 1$. For if $\gcd(M) > 1$, then $M$ contains neither 1, nor any pair of consecutive positive integers; that is, $b_\nu - b_{\nu-1} \geq 2$ for $\nu = 1, \ldots, m-1$. Hence, by summing up, $b_{m-1} \geq 2m-2$. Similarly, $c_{n-1} \geq 2n-2$ if $\gcd(N) > 1$. And these two lower bounds are incompatible if (1.4) or (1.5) holds.

Interesting applications of these two theorems to the study of sum-free sets of positive integers are given in **[2]** and **[3]**.

The proof of Theorem XI in **[1]** is presented very succinctly, but divides the argument into many cases and is in fact quite long once the necessary details are provided. The aim of this paper is to give a detailed proof, separated into fewer cases than in **[1]**. As in **[1]**, one proceeds by induction on $m+n$ and distinguishes two situations (called here, and there, Cases (I) and (II)), essentially according to the size of $\max(b_{m-2}, c_{n-2})$.

Inequality (2.11) and Theorem 2.1 (below) are essential tools, here and in **[1]**. Case (I) requires fewer subcases here than in **[1]**, and uses an argument which is applied again at the end of Case (II). Case (II) has been simplified by avoiding consideration of the sign of $b_p - c_p$ (cf. **[1]**, after (26)), and of $m - p_1 - p_1^*$ (**[1]**, after (29)).

For completeness, Theorem X is also proved, since it is used to prove Theorem XI. We follow **[1]** here, but the formulation of Theorem X given above differs from Freiman's in including (1.5) and (1.7), which in **[1]** are embodied in the proof of Theorem XI.

I am grateful to Felix Albrecht, who helped me by translating **[1]** into English.

## 2. Preliminaries

We now introduce some more notation and three auxiliary results.

Part of the proof of Theorem XI exploits a certain symmetry between $M$ and $N$ and the sets

$$M^* := \{b_{m-1} - b_\nu\}_{\nu=0}^{m-1}\,, \tag{2.1}$$

and

$$N^* := \{c_{n-1} - c_\nu\}_{\nu=0}^{n-1}\,, \tag{2.2}$$

which we also write as

$$M^* = \{x_0,\, x_1, \dots, x_{m-1}\}, \qquad \text{with} \qquad x_\nu = b_{m-1} - b_{m-1-\nu}\,, \tag{2.3}$$

and

$$N^* = \{y_0,\, y_1, \dots, y_{n-1}\}, \qquad \text{with} \qquad y_\nu = c_{n-1} - c_{n-1-\nu} \tag{2.4}$$

($x_0 = 0$, $x_{m-1} = b_{m-1}$ and $x_i < x_{i+1}$ for all $i$; $y_0 = 0$, $y_{n-1} = c_{n-1}$ and $y_i < y_{i+1}$ for all $i$).

The hypotheses of Theorem XI are met by $M^*$ and $N^*$ if they are by $M$ and $N$, because

$$(b_{m-1} - b_{m-2}, \dots, b_{m-1} - b_1, b_{m-1}) = (b_1, \dots, b_{m-1})\,, \tag{2.5}$$

$|M^*| = |M|$, $|N^*| = |N|$ and $\max(x_{m-1},\, y_{n-1}) = \max(b_{m-1},\, c_{n-1})$. And the theorem's conclusion holds for $|M+N|$ if it does for $|M^* + N^*|$, since the two are equal.

For any $r$ and $s$ with $0 \le r \le m$ and $0 \le s \le n$, let

$$M'_r := \{b_i \in M : i \le r-1\}\,,\ N'_s := \{c_i \in N : i \le s-1\}\,, \tag{2.6}$$

and

$$(M^*)'_r := \{x_i \in M^* : i \le r-1\}\,,\ (N^*)'_s := \{y_i \in N^* : i \le s-1\}\,.$$

Theorem XI is proved by induction. Typically, one writes $M = M'_r \cup (M \backslash M'_r)$, then subtracts from each element of $M \backslash M'_r$ its smallest element, $b_r$, in order to obtain a set with the same cardinality, which contains 0. This set is, for $0 \le r \le m-1$,

$$M''_{m-r} := \{0,\, b_{r+1} - b_r, \dots, b_{m-1} - b_r\} = \{b_\nu - b_r\}_{\nu=r}^{m-1}\,, \tag{2.7}$$

and the corresponding set for $N \backslash N'_s$ is

$$N''_{n-s} := \{0,\, c_{s+1} - c_s, \dots, c_{n-1} - c_s\} = \{c_\nu - c_s\}_{\nu=s}^{n-1}\,. \tag{2.8}$$

For any $r$ and $s$ with $0 \le r < m$ and $0 \le s < n$, we have

$$|M''_{m-r}| = m - r \qquad \text{and} \qquad |N''_{n-s}| = n - s\,. \tag{2.9}$$

Many of the estimates involving these sets will be combined with the following elementary inequality: if $E_1$ and $E_2$ are subsets of the finite set $E$, then

$$|E| \ge |E_1| + |E_2| - |E_1 \cap E_2|\,. \tag{2.10}$$

We shall use the following form of (2.10): if $k \le r \le m-1$ and $\ell \le s \le n-1$, then

$$|M+N| \ge |M'_r + N'_s| + |M''_{m-k} + N''_{n-\ell}| - |(M'_r + N'_s) \cap ((M \backslash M'_k) + (N \backslash N'_\ell))|\,. \tag{2.11}$$

To obtain (2.11), set $E = M + N$, $E_1 = M'_r + N'_s$ and $E_2 = (M \backslash M'_k) + (N \backslash N'_\ell)$ in (2.10), and observe that

$$M''_{m-k} + N''_{n-\ell} = \{x \in \mathbb{Z} : x = b_u + c_v - (b_k + c_\ell),\ k \le u \le m-1,\ \ell \le v \le n-1\}\,,$$

so that if $x$ runs through the elements of $M''_{m-k} + N''_{n-\ell}$, then $x + (b_k + c_\ell)$ runs through those of $E_2$; consequently

$$|M''_{m-k} + N''_{n-\ell}| = |\{x \in \mathbb{Z} : x = b_u + c_v,\ k \le u \le m-1\,,\ \ell \le v \le n-1\}|\,. \quad (2.12)$$

From (2.10) and (2.12) we get (2.11).

The following property of the counting functions

$$B(s) := |\{b_i \in M : 1 \le b_i \le s\}|\,,\ C(s) := |\{c_i \in N : 1 \le c_i \le s\}| \quad (2.13)$$

follows from Mann's inequality ([**4**], Chap. I.4; [**5**]); we will apply it to choose the parameters in (2.11).

**Theorem 2.1.** *If* $B(s) + C(s) \ge s$ *for* $s = 1, \dots, k$, *then* $\{0, 1, \dots, k\} \subset M + N$.

We will use the following proposition in establishing Case (II) of Theorem XI. Its proof is suggested by an argument of Freiman's ([**1**], p. 152). There is an arithmetical hypothesis, different from (1.10), but no condition on the size of $\max(M \cup N)$. The conclusion is stronger than (1.11).

**Proposition 2.2.** *If $M$ and $N$ are finite subsets of* $\mathbb{Z}$, *such that* $0 \in M \cap N$, $|M| \ge 2$, $|N| \ge 2$ *and* $\gcd(N) \nmid \gcd(M)$, *then*

$$|M + N| \ge |M| + 2|N| - 2\,. \quad (2.14)$$

*Proof.* — Set $d := \gcd(N)$, and $N_0 := N\backslash\{0\}$. Since $0 \in M$ and $d \nmid \gcd(M)$, some, but not all elements of $M$ are divisible by $d$. Let $b_r$ and $b_s$ be the largest integers in $M$ such that, respectively, $b_r \equiv 0$ and $b_s \not\equiv 0 \pmod d$. Then $M$, $\{b_r\} + N_0$ and $\{b_s\} + N_0$ are pairwise disjoint subsets of $M + N$ (for instance, $b = b_r + c$ for some $b \in M$ and $c \in N_0$ would imply both $b \equiv 0 \pmod d$ and $b \ge b_r + 1$). This proves (2.14).

**Corollary 2.3.** *Let $M$ and $N$ be as in (1.1) and (1.2), and such that (1.10) holds. Assume also that* $\min(m, n) \ge 3$. *Then (1.11) is true, if any one of the following conditions is satisfied*:

$$\gcd(M) > 1\,, \quad (2.15)$$

$$\gcd(M'_{m-1}) > 1\,, \quad (2.16)$$

$$\gcd((M^*)'_{m-1}) > 1\,. \quad (2.17)$$

*Proof.* — Because of (1.10), $\gcd(M) \nmid \gcd(N)$ if $\gcd(M) > 1$; and then $|M + N| \ge m + n - 2 + \min(m, n)$, by (2.14). Thus (1.11) follows from (1.10) and (2.15).

Now suppose that (2.16) is verified. We may assume that $\gcd(N) = 1$, for if not, (1.11) is true (exchange $M$ and $N$ in Proposition 2.2 and argue as above). Then, $\gcd(M'_{m-1}) \nmid \gcd(N)$ and by Proposition 2.2,

$$|M'_{m-1} + N| \ge 2\,(m-1) + n - 2 \ge m + n - 4 + \min(m, n)\,.$$

This implies (1.11), since $b_{m-1} + c_{n-1} \notin M'_{m-1} + N$.

Finally, (1.10) and (2.5) imply that $(x_1, \dots, x_{m-1}, y_1, \dots, y_{n-1}) = 1$. The preceding arguments then show that (2.17) implies (1.11) for $M^*$ and $N^*$, hence also for $M$ and $N$.