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

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

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 $\nu = 1, \dots, m-1$. 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

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

and

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

($x_0 = 0$, $x_{m-1} = b_{m-1}$ 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

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

$|M^*| = |M|$, $|N^*| = |N|$ 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 $0 \le r \le m-1$,

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

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

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

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

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

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

The following property of the counting functions

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

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* $s = 1, \ldots, k$, *then* $\{0, 1, \ldots, k\} \subset M + N$.

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*

$$|M + N| \ge |M| + 2|N| - 2\,. \tag{2.14}$$

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*:

$$\gcd(M) > 1\,, \tag{2.15}$$

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

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

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

3. Freiman's Theorems

3.1. Proof of Theorem X. — Consider the sets

$$A := \{b_0, \ldots, b_{m-1}, b_{m-1} + c_1, \ldots, b_{m-1} + c_{n-1}\}$$

and

$$B := \{g \in \mathbb{Z} : 1 \leq g < b_{m-1}, g \notin M\}.$$

Since $A \subset (M + N)$ and $|A| + |B| = b_{m-1} + n$, (1.6) is true if $B = \phi$. If $B \neq \phi$, (1.6) is proved by constructing an injective mapping, say f, of B into $(M + N)\backslash A$, as follows. Let $g \in B$.

If $g \in N$, then $g \in M + N$; $g \notin A$, since $A \cap B = \phi$. In this case, set $f(g) = g$.

If $g \notin N$, if $c_{n-1} < b_{m-1}$ and $c_{n-1} < g < b_{m-1}$, then the n integers

$$g - c_0, \ g - c_1, \ldots, \ g - c_{n-1} \tag{3.1}$$

are in the interval $[1, b_{m-1})$. Since $|B| = b_{m-1} - (m - 1) \leq n - 1$, some integer in (3.1) belongs to M, say $g - c_s = b_r$, whence $g = b_r + c_s \in M + N$. As before, $g \notin A$. Here also, set $f(g) = g$.

If $g \notin N$ and $g < c_{n-1}$, let $i\,(0 \leq i \leq n - 2)$ be such that $c_i < g < c_{i+1}$. The $n - 1$ integers

$$g + b_{m-1} - c_\nu \ (\nu = i + 1, \ldots, n - 2), \ g - c_\nu \ (\nu = 0, \ldots, i) \tag{3.2}$$

are distinct ($g + b_{m-1} - c_{n-2} > g = g - c_0$), and in $[1, b_{m-1})$. If $b_{m-1} - (m-1) \leq n-2$, as in (1.4), one of them must belong to M. If $b_{m-1} - (m-1) = n-1$ and $c_{n-1} < b_{m-1}$ as in (1.5), we may include $g + b_{m-1} - c_{n-1}$ in (3.2) since $g + b_{m-1} - c_{n-1} > g$ in this case, and reach the same conclusion. Hence g or $g + b_{m-1}$ is in $M + N$. Neither is in A; $g \notin A$ as before, and $g + b_{m-1} \notin A$ since $g + b_{m-1} > b_{m-1}$ and $g \notin N$. We set $f(g) = g$, or $f(g) = g + b_{m-1}$, so as to have $f(g) \in M + N$.

This f is injective. Indeed, $f(g) = g$ or $f(g) = g + b_{m-1}$ for each $g \in B$; and if $g < g' < b_{m-1}$ then $g < g' < g + b_{m-1} < g' + b_{m-1}$.

This concludes the proof of (1.6). And (1.8) now follows on observing that if $b_{m-1} = c_{n-1}$ in (1.4), the roles of M and N may be exchanged.

3.2. Proof of Theorem XI. — The proof proceeds by induction on $m + n$. Since (1.3) implies (1.11) if $\min(m, n) \leq 2$, we may assume that $\min(m, n) \geq 3$. We shall show that (1.11) is true for M and N, if it is true for all finite sets A and B of non-negative integers which are such that

$$|A| + |B| < m + n, \tag{3.3}$$

$$0 \in A \cap B, \tag{3.4}$$

$$\gcd(A \cup B) = 1, \tag{3.5}$$

and

$$\max(A \cup B) \geq |A| + |B| - 2. \tag{3.6}$$

We consider separately the two cases

(I) $$\max(b_{m-2}, \ c_{n-2}) < m + n - 4, \tag{3.7}$$

(II) $$\max(b_{m-2}, \ c_{n-2}) \geq m + n - 4. \tag{3.8}$$

We first deal with

Case (I). Clearly, (3.7) implies that $M \cap N \neq \{0\}$. We proceed to make this remark more precise.

Let B and C be the counting functions defined in (2.13). Because of (3.7), we have

$$B(m+n-4) + C(m+n-4) \geq m+n-4 \tag{3.9}$$

and

$$B(m+n-5) + C(m+n-5) > m+n-5\,. \tag{3.10}$$

It follows from Theorem 2.1 that (1.11) is true, if also

$$B(s) + C(s) \geq s \quad \text{for} \quad s = 1, \ldots, m+n-6\,. \tag{3.11}$$

Indeed, Theorem 2.1 and (3.9) through (3.11) ensure that $\{0, 1, \ldots, m+n-4\} \subset M+N$. And if $b_{m-1} \geq c_{n-1}$, then the n integers $b_{m-1} + c_\nu$ $(\nu = 0, \ldots, n-1)$ are in the set $(M+N)\backslash\{0, 1, \ldots, m+n-4\}$, because of (1.9); if $c_{n-1} > b_{m-1}$ we can find m integers in this set. Hence, $|M+N| \geq (m+n-3) + \min(m,n)$ if (3.7) and (3.11) are true.

It therefore suffices to consider the possibility that (3.11) fails to hold, say that

$$B(s_o) + C(s_o) < s_o \tag{3.12}$$

for some s_o, $1 \leq s_o \leq m+n-6$. Then,

$$B(s_o+1) + C(s_o+1) \leq s_o + 1\,. \tag{3.13}$$

It follows from (3.10), (3.12) and (3.13) that there is an integer i, with $s_o + 2 \leq i \leq m+n-5$, such that

$$B(s) + C(s) \leq s \quad \text{for} \quad s_o \leq s \leq i-1 \tag{3.14}$$

and $B(i) + C(i) > i$.

Then,

$$B(i-1) + C(i-1) = i-1 \tag{3.15}$$

and

$$B(i) + C(i) = i+1, \tag{3.16}$$

whence $i \in M \cap N$. And $i - 2 \geq s_o$ by definition, hence from (3.14),

$$B(i-2) + C(i-2) \leq i-2\,. \tag{3.17}$$

With (3.15), this implies that $i - 1 \in M \cup N$.

We now define q_1 and q_2 $(1 \leq q_1 \leq m-2$ and $1 \leq q_2 \leq n-2)$ by setting

$$b_{q_1} = i = c_{q_2}\;; \tag{3.18}$$

then $\max(b_{q_1-1}, c_{q_2-1}) = i-1$.

From (3.16) and (3.18) we have

$$i = q_1 + q_2 - 1\,; \tag{3.19}$$

hence $q_1 + q_2 \geq 4$, since $i \geq 3$. And from (3.18) and (3.19),

$$b_{q_1} = c_{q_2} = q_1 + q_2 - 1\,. \tag{3.20}$$

We may invoke the induction hypothesis to obtain the following estimates:
if $b_{q_1-1} = i-1$, then

$$|M''_{m-q_1+1} + N''_{n-q_2}| \geq m+n-(q_1+q_2)-2+\min(m-q_1+1\,,\, n-q_2); \quad (3.21)$$

if $c_{q_2-1} = i-1$, then

$$|M''_{m-q_1} + N''_{n-q_2+1}| \geq m+n-(q_1+q_2)-2+\min(m-q_1\,,\, n-q_2+1)\,; \quad (3.22)$$

and in both cases,

$$|M''_{m-q_1+1} + N''_{n-q_2+1}| \geq m+n-(q_1+q_2)+\min(m-q_1\,,\, n-q_2)\,. \quad (3.23)$$

Indeed, (3.3) is verified each time because of (2.9) and since $q_1+q_2 \geq 4$. Condition (3.4) is met, since $0 \in M''_{m-r} \cap N''_{n-s}$ by (2.7) and (2.8). Condition (3.5) is satisfied because by (3.18) we have $1 = b_{q_1} - b_{q_1-1} \in M''_{m-q_1+1}$ if $b_{q_1-1} = i-1$, and $1 \in N''_{n-q_2+1}$ if $c_{q_2-1} = i-1$. To verify (3.6) we observe that by (2.7) and (1.9),

$$\begin{aligned}\max(M''_{m-r} \cup N''_{n-s}) &= \max(b_{m-1}-b_r,\, c_{n-1}-c_s)\\ &\geq (m+n-2)-\max(b_r, c_s),\end{aligned}$$

from which (3.6) follows in each case.

We shall also need two consequences of Theorem X, namely

$$|M'_{q_1+1} + N'_{q_2+1}| \geq q_1+q_2+\max(q_1\,,\, q_2\,) \quad (3.24)$$

and

$$|M'_{q_1} + N'_{q_2+1}| \geq 2q_1+q_2-1\,. \quad (3.25)$$

To obtain (3.24) we observe that because of (3.20) the sets M'_{q_1+1} and N'_{q_2+1} satisfy (1.7) since

$$|M'_{q_1+1}| + |N'_{q_2+1}| - 3 = q_1+q_2-1\,;$$

(3.24) is (1.8) for these sets.
For (3.25), we note that M'_{q_1} and N'_{q_2+1} verify (1.5) since by (1.1) and (3.20),

$$b_{q_1-1} < c_{q_2} = q_1+q_2-1 = |M'_{q_1}| + |N'_{q_2+1}| - 2.$$

By (1.6) then,

$$|M'_{q_1} + N'_{q_2+1}| \geq c_{q_2} + q_1\,,$$

and this is (3.25).

We proceed to apply (3.21) through (3.25). The argument in Case (I) is now separated into two subcases,

$$\begin{aligned}&\text{(Ia)} \qquad b_{q_1-1} = c_{q_2-1}\,, \qquad (3.26)\\ &\text{(Ib)} \qquad b_{q_1-1} \neq c_{q_2-1}\,.\end{aligned}$$

Case (Ia). In this case,

$$|M+N| \geq |M'_{q_1+1} + N'_{q_2+1}| + |M''_{m-q_1+1} + N''_{n-q_2+1}| - 3\,. \quad (3.27)$$

To prove (3.27) we use (2.11) with $r = q_1+1$, $s = q_2+1$, $k = q_1-1$, $\ell = q_2-1$. For simplicity of notation, set $M_1 = M'_{q_1+1}$, $N_1 = N'_{q_2+1}$, $M_2 = M \backslash M'_{q_1-1}$ and $N_2 = N \backslash N'_{q_2-1}$. We must show that $|(M_1+N_1) \cap (M_2+N_2)| = 3$ in order to get (3.27) from (2.11). Indeed, $b_{q_1-1}+c_{q_2-1}$, $b_{q_1}+c_{q_2-1}$, $b_{q_1-1}+c_{q_2}$ and $b_{q_1}+c_{q_2}$ are in

$(M_1+N_1)\cap(M_2+N_2)$, and $b_{q_1}+c_{q_2-1}=b_{q_1-1}+c_{q_2}$ by (3.18) and (3.26). These are the only elements of $(M_1+N_1)\cap(M_2+N_2)$. For consider some $x\in M_1+N_1$, say $x=b_u+c_v$, with $u<q_1-1$ or $v<q_2-1$; then $x<b_{q_1-1}+c_{q_2}$, hence $x\in M_2+N_2$ only if $x=b_{q_1-1}+c_{q_2-1}$.
Return now to (3.27). On combining (3.27), (3.23) and (3.24) we have

$$|M+N|\geq m+n-3+\max(q_1,q_2)+\min(m-q_1,n-q_2),$$

and this implies (1.11). This concludes the proof in Case (Ia).

Case (Ib). The argument when $b_{q_1-1}<c_{q_2-1}$ is typical. Then, we have

$$|M+N|\geq|M'_{q_1+1}+N'_{q_2+1}|+|M''_{m-q_1}+N''_{n-q_2+1}|-2 \tag{3.28}$$

and

$$|M+N|\geq|M'_{q_1}+N'_{q_2+1}|+|M''_{m-q_1}+N''_{n-q_2+1}|\,. \tag{3.29}$$

To verify (3.28), set $r=q_1+1$, $s=q_2+1$, $k=q_1$, $\ell=q_2-1$ in (2.11) and observe that if $u\leq q_1-1$ and $v\leq q_2$, then $b_u+c_v\in M'_{q_1+1}+N'_{q_2+1}$ but $b_u+c_v\leq b_{q_1-1}+c_{q_2}<b_{q_1}+c_{q_2-1}=\min(M\backslash M'_{q_1})+(N\backslash N'_{q_2-1})$. Hence $b_{q_1}+c_{q_2-1}$ and $b_{q_1}+c_{q_2}$ are the only elements of $(M'_{q_1+1}+N'_{q_2+1})\cap((M\backslash M'_{q_1})+(N\backslash N'_{q_2-1}))$. And (3.29) follows from (2.11) with $r=q_1$, $s=q_2+1$, $k=q_1$, $\ell=q_2-1$, since $b_{q_1-1}+c_{q_2}<b_{q_1}+c_{q_2-1}$ that is, $\max(M'_{q_1}+N'_{q_2+1})<\min((M\backslash M'_{q_1})+(N\backslash N'_{q_2-1}))$.

From (3.28), (3.22) and (3.24),

$$|M+N|\geq m+n-4+\max(q_1,q_2)+\min(m-q_1\,,\,n-q_2+1),$$

from which (1.11) follows if $q_2>q_1$.

If $q_1\geq q_2$ we use (3.29), (3.22) and (3.25) which together yield

$$|M+N|\geq m+n-3+q_1+\min(m-q_1\,,\,n-q_2+1),$$

and (1.11) follows.

This settles Case (Ib) when $b_{q_1-1}<c_{q_2-1}$. If $b_{q_1-1}>c_{q_2-1}$ the argument goes through as above on replacing (3.22) by (3.21) and similarly interchanging the roles of M and N in (3.25), (3.28) and (3.29).

This disposes of Case (I).

Case (II). This case is determined by condition (3.8). We may also assume that

$$\max(b_{m-1}-b_1,\ c_{n-1}-c_1)\geq m+n-4\,, \tag{3.30}$$

for otherwise, by Case (I), the conclusion of Theorem XI holds for M^* and N^*, since $b_{m-1}-b_1=x_{m-2}$ and $c_{n-1}-c_1=y_{n-2}$.

Because of Corollary 2.3, it suffices to consider sets M and N such that

$$\gcd(M)=\gcd(N)=1\,, \tag{3.31}$$

$$\gcd((M^*)'_{m-1})=1\,, \tag{3.32}$$

and

$$\gcd(M'_{m-1})=1\,. \tag{3.33}$$

In Case (II), we may further assume that

$$b_1=c_1=1 \tag{3.34}$$

and that

$$b_{m-1} - b_{m-2} = c_{n-1} - c_{n-2} = 1\,, \tag{3.35}$$

as we proceed to show. Consider (3.34) first. If $b_1 \neq c_1$ then 0, b_1, c_1 are distinct elements of $M + N$, not in $M_0 + N_0$ (in the notation of Proposition 2.2). Hence if $b_1 \neq c_1$,

$$|M + N| \geq |M_0 + N_0| + 3 = |(M^*)'_{m-1} + (N^*)'_{n-1}| + 3 \tag{3.36}$$

($b_{m-1} + c_{n-1} - x$ runs through $(M^*)'_{m-1} + (N^*)'_{n-1}$, if x runs through $M_0 + N_0$).

Inequality (3.36) also holds if $b_1 = c_1 \geq 2$. For if $b_1 = c_1 \geq 2$, let b_u and c_v be the smallest integers in M and N, respectively, such that $b_1 \nmid b_u$ and $b_1 \nmid c_v$ (they are well-defined, because of (3.31)). Then $u \geq 2$ and $v \geq 2$, whence

$$b_0 + c_0 < b_1 + c_0 < \min(b_u,\, c_v)\,. \tag{3.37}$$

And $\min(b_u,\, c_v) \notin M_0 + N_0$. Indeed, say $b_u \leq c_v$, and suppose that $b_u = b_k + c_\ell$ for some $k \geq 1$ and $\ell \geq 1$. Then $b_u > b_k$ and $c_v \geq b_u > c_\ell$, whence $b_k \equiv c_\ell \equiv 0 \pmod{b_1}$. This is impossible since $b_1 \nmid b_u$. Hence with (3.37), we have (3.36) again.

Now the induction hypothesis applies to $(M^*)'_{m-1}$ and $(N^*)'_{n-1}$ because of (3.30) and (3.32). With it, (3.36) yields (1.11). This justifies assumption (3.34).

To justify (3.35), we use M^* and N^*; note that (3.35) is equivalent to $x_1 = y_1 = 1$. By (2.5) and (3.31), $\gcd(M^*) = \gcd(N^*) = 1$. By reasoning as for (3.34) we see that

$$|M^* + N^*| \geq |M'_{m-1} + N'_{n-1}| + 3\,, \tag{3.38}$$

except perhaps if $x_1 = y_1 = 1$. And because of (3.8) and (3.33), we may apply the induction hypothesis to M'_{m-1} and N'_{n-1}; (1.11) then follows from (3.38).

Another restriction is possible in Case (II): we may assume that $m = n$. Indeed, suppose $m < n$. The induction hypothesis applies to M and N'_{n-1}: (3.5) is satisfied because of (3.31); so is (3.6) since by (1.9) and (3.35),

$$\max\,(M \cup N'_{n-1}) = \max\,(b_{m-1},\, c_{n-1} - 1) \geq m + n - 3 = |M| + |N'_{n-1}| - 2\,.$$

From the induction hypothesis we get

$$|M + N'_{n-1}| \geq m + (n-1) - 3 + \min\,(m, n-1) = m + n - 4 + \min\,(m, n),$$

and (1.11) follows. If $m > n$ we can reason in the same manner with M'_{m-1} and N.

Finally, since Theorem XI is symmetric in M and N, and since we have made no assumptions distinguishing M from N, we may assume that $b_{m-1} \geq c_{n-1}$.

We again consider the function $B(s) + C(s) - s$, where B and C are as in (2.13). It is ultimately negative, since M and N are finite. In fact, since now $b_{m-1} \geq c_{n-1}$ and consequently $b_{m-1} \geq m + n - 2$,

$$B(s) + C(s) < s \quad \text{for} \quad s > b_{m-1}\,. \tag{3.39}$$

On the other hand, because of (3.34), we have $B(1) + C(1) > 1$, and $B(2) + C(2) \geq 2$. Hence there is an integer j, with $2 \leq j \leq b_{m-1}$, such that $B(s) + C(s) \geq s$ for $1 \leq s \leq j$ and $B(j+1) + C(j+1) < j+1$. Then $B(j) + C(j) = j = B(j+1) + C(j+1)$, whence $j + 1 \notin M \cup N$. And by Theorem 2.1,

$$\{0, 1, \ldots, j\} \subset M + N\,. \tag{3.40}$$

If $j \geq m+n-4$ then (1.11) is true, by the argument developed after (3.11). We may therefore assume that $j \leq m+n-5$; then, $j+1 < b_{m-1}$ by (1.9). With this assumption, let p_1 be such that $b_{p_1-1} < j+1 < b_{p_1}$. By (3.34) and (3.35), $2 \leq p_1 \leq m-2$. Then, either $c_{n-1} < j+1 < b_{p_1}$ or $j+1 < c_{n-1}$.

If $c_{n-1} < j+1 < b_{p_1}$ then $B(j+1)+C(j+1)=j$ yields

$$j = n + p_1 - 2\ . \tag{3.41}$$

The integers in (3.40), the b_i with $p_1 \leq i \leq m-1$ and the $b_{m-1}+c_k$ with $1 \leq k \leq n-1$ are distinct, and in $M+N$. By (3.41) they are $(j+1)+(m-p_1)+(n-1) = m+2n-2$ in number; this implies (1.11).

If $j+1 < c_{n-1}$, let $p_2\,(2 \leq p_2 \leq n-2)$ be such that $c_{p_2-1} < j+1 < c_{p_2}$. Then (3.41) is replaced by

$$j = p_1 + p_2 - 2\ . \tag{3.42}$$

We now distinguish three subcases, according to the sign of $p_1 - p_2$. Suppose first that $p_1 = p_2 = p$, say. Then by arguing as for (3.27), we have

$$|M+N| \geq |M'_{p+1} + N'_{p+1}| + |M''_{m-p+1} + N''_{n-p+1}| - a\,, \tag{3.43}$$

where

$$a = \begin{cases} 4 & \text{if} \quad b_{p-1}+c_p \neq b_p + c_{p-1} \qquad (3.44)\\ 3 & \text{else.} \qquad (3.45)\end{cases}$$

For the first member on the right side of (3.43), we have

$$|M'_{p+1}+N'_{p+1}| \geq \begin{cases} 3p+1 & \text{if} \quad b_{p-1}+c_p \neq b_p + c_{p-1} \qquad (3.46)\\ 3p & \text{else.} \qquad (3.47)\end{cases}$$

Indeed, $\{0,1,\ldots,j\} \subset M'_{p+1} + N'_{p+1}$ because of (3.40) and since

$$b_u + c_v > \min(b_p,\, c_p) > j$$

if $u > p$ or $v > p$. And if $b_p + c_{p-1} < b_{p-1} + c_p$, then the $p+2$ integers $b_p + c_\nu$ $(\nu = 0,1,\ldots,p)$ and $b_{p-1}+c_p$ are distinct, in $M'_{p+1} + N'_{p+1}$, and larger than j. This proves (3.46), since $(j+1)+p+2 = 3p+1$. (If $b_p + c_{p-1} > b_{p-1}+c_p$, use the $b_\nu + c_p$ with $0 \leq \nu \leq p$, and $b_p + c_{p-1}$.) To prove (3.47), use the same integers as for (3.46), except $b_{p-1}+c_p$ (or $b_p + c_{p-1}$, as the case may be).

For the second member on the right side of (3.43), we have

$$|M''_{m-p+1} + N''_{n-p+1}| \geq 3\,(m-p+1) - 3 \tag{3.48}$$

by the induction hypothesis: condition (3.5) is verified since $b_{m-1} - b_{p-1}$ and $b_{m-2} - b_{p-1}$ are consecutive integers, by (3.35); and (3.6) is met, since

$$\begin{aligned}&\max(b_{m-1} - b_{p-1}\,,\, c_{n-1} - c_{p-1})\\ &\quad\geq \max(b_{m-1},\, c_{n-1}) - \max(b_{p-1},\, c_{p-1})\\ &\quad\geq (m+n-2) - j = (m-p+1) + (n-p+1) - 2\,.\end{aligned}$$

Now (3.43) through (3.48) imply (1.11). This settles the subcase in which $p_1 = p_2$.

Suppose now that $p_1 > p_2$ in (3.42). Because of (3.40) and since $c_{p_2} > j$,

$$|M+N| \geq (j+1) + |M + \{c_{p_2},\, c_{p_2+1}, \ldots,\, c_{n-1}\}|, \tag{3.49}$$

whence with (2.12),

$$|M+N| \geq (j+1) + |M + N''_{n-p_2}|\,. \tag{3.50}$$

The induction hypothesis applies to M and N''_{n-p_2}, by (3.31) and (1.9), and since $b_{m-1} > c_{n-1} - c_{p_2}$ and $p_2 \geq 2$. With it and (3.42), (3.50) yields

$$|M+N| \geq (p_1 + p_2 - 1) + m + 2(m - p_2) - 3 = 3m - 4 + (p_1 - p_2)\,,$$

whence $|M+N| \geq 3m-3$.

We must still treat the subcase in which

$$p_1 < p_2\,. \tag{3.51}$$

Arguing as for (3.50), we see that (3.40) and $b_{p_1} > j$ imply that

$$|M+N| \geq (j+1) + |M''_{m-p_1} + N|\,. \tag{3.52}$$

If $\max\,(M''_{m-p_1} \cup N) \geq |M''_{m-p_1}| + |N| - 2$, that is, if

$$\max\,(b_{m-1} - b_{p_1}\,, c_{n-1}) \geq 2m - p_1 - 2\,, \tag{3.53}$$

then by the induction hypothesis,

$$|M''_{m-p_1} + N| \geq 3(m-1) - 2p_1\,. \tag{3.54}$$

With (3.54), (1.11) follows from (3.52), (3.42) and (3.51).

In order to conclude the proof of Theorem XI, we must consider subcase (3.51) when, instead of (3.53),

$$\max\,(b_{m-1} - b_{p_1}, c_{n-1}) \leq 2m - p_1 - 3\,. \tag{3.55}$$

For this we use the sets M^* and N^*, as defined in (2.3) and (2.4). In analogy to (2.13), let B^* and C^* denote the counting functions of the positive elements of M^* and N^*, respectively. By (1.9) and (3.35) there is an integer j^* with $2 \leq j^* \leq b_{m-1}$, such that $B^*(s) + C^*(s) \geq s$ for $1 \leq s \leq j^*$ and $B^*(j^*+1) + C^*(j^*+1) < j^*+1$. Then $j^*+1 \notin M^* \cup N^*$, $j^* = B^*(j^*+1) + C^*(j^*+1)$, and by Theorem 2.1,

$$\{0, 1, \ldots, j^*\} \subset M^* + N^*\,. \tag{3.56}$$

By a previous assumption, $y_{n-1} := c_{n-1} \leq b_{m-1} =: x_{m-1}$. By the argument applied after (3.40), we may assume that $j^*+1 < x_{m-1}$. Then define p_1^* $(1 < p_1^* < m)$ by

$$x_{p_1^*-1} < j^* + 1 < x_{p_1^*}\,. \tag{3.57}$$

If $y_{n-1} < j^*+1 < x_{p_1^*}$, we can prove (1.11) by reasoning as when $c_{n-1} < j+1 < b_{p_1}$ (use (3.56), and replace (3.41) by $j^* = n + p_1^* - 2$). Accordingly, let us assume that

$$j^* + 1 < c_{n-1}\,. \tag{3.58}$$

Because of (3.55), and since $b_{m-1} - b_{p_1} = x_{m-p_1-1}$ and $c_{n-1} = y_{m-1}$, we have

$$B^*(2m - p_1 - 3) + C^*(2m - p_1 - 3) \geq (m - p_1 - 1) + (m-1) > 2m - p_1 - 3\,.$$

And $2m - p_1 - 3 \geq c_{n-1} > j^* + 1$ by (3.55) and (3.58). Thus, if (3.55) and (3.58) hold, then

$$B^*(s) + C^*(s) > s \qquad \text{for some} \quad s > j^* + 1\,.$$

Now

$$B^*(j^*+1) + C^*(j^*+1) < j^* + 1\,. \tag{3.59}$$

Hence (3.55) and (3.58) imply the existence of an integer g such that

$$B^*(s) + C^*(s) \leq s \qquad \text{for} \qquad j^* + 1 \leq s \leq g - 1 \tag{3.60}$$

and

$$B^*(g) + C^*(g) > g\,.$$

Then,

$$B^*(g-1) + C^*(g-1) = g - 1, \tag{3.61}$$

$$B^*(g) + C^*(g) = g + 1\,, \tag{3.62}$$

and therefore $g \in M^* \cap N^*$. Furthermore, $g \geq j^* + 2$ by definition, and $g = j^* + 2$ is excluded by comparing (3.59) and (3.61). Thus $g - 2 \geq j^* + 1$, and from (3.60),

$$B^*(g-2) + C^*(g-2) \leq g - 2\,; \tag{3.63}$$

with (3.61) this implies that $g - 1 \in M^* \cup N^*$.

Now define r_1 and r_2 by setting

$$x_{r_1} = g = y_{r_2}\,; \tag{3.64}$$

then $x_{r_1 - 1} = g - 1$ or $y_{r_2 - 1} = g - 1$. And from (3.62) and (3.64),

$$g = r_1 + r_2 - 1\,. \tag{3.65}$$

We now have a situation entirely similar to the one encountered in Case (I): compare (3.61) through (3.65) with (3.15) through (3.19).

To complete the proof of (1.11) when (3.51) holds, it suffices to proceed as in Case (I). On replacing there M and N by M^* and N^*, respectively, q_i by r_i $(i = 1, 2)$, each b by x and each c by y, and remembering that $|M^* + N^*| = |M + N|$, we dispose of this last subcase.

This concludes the proof of Theorem XI.

References

[1] Freiman G.A., *Inverse Problems in Additive Number Theory*, VI. On the Addition of Finite Sets, III (in Russian). Izv. Vyss. Ucebn. Zaved. Matematika, **3 (28)**, 1962, 151–157.

[2] Freiman G.A., *On the Structure and the Number of Sum-Free Sets*, Journées Arithmétiques de Genève 1991, Astérisque **209**, 195–203.

[3] Deshouillers J.-M., Sós V., Freiman G.A. and Temkin M., *On the Structure of Sum-Free Sets, 2*, this volume.

[4] Halberstam H. and Roth K.F., *Sequences* (second edition), Springer-Verlag, New York, Berlin, 1983.

[5] Mann H.B., *A Proof of the Fundamental Theorem on the Density of Sums of Sets of Positive Integers*, Ann. Math., **43**, 1942, 523–527.

J. Steinig, Section de Mathématiques, Université de Genève, C.P. 240, 1211 Genève 24, Suisse
E-mail : Peterman@ibm.unige.ch (qui transmettra)