The Minimum Size of Signed Sumsets

Béla Bajnok
Department of Mathematics
Gettysburg College
U.S.A.
bbajnok@gettysburg.edu

Ryan Matzke
School of Mathematics
University of Minnesota
U.S.A.
matzk053@umn.edu

Submitted: Dec 6, 2014; Accepted: May 27, 2015; Published: XX
Mathematics Subject Classifications: 11B75, 05D99

Abstract

For a finite abelian group G and positive integers m and h, we let

$$\rho(G,m,h) = \min\{|hA| \ : \ A \subseteq G, |A| = m\}$$

and

$$\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \subseteq G, |A| = m\},$$

where hA and $h_{\pm}A$ denote the h-fold sumset and the h-fold signed sumset of A, respectively. The study of $\rho(G,m,h)$ has a 200-year-old history and is now known for all G, m, and h. Here we prove that $\rho_{\pm}(G,m,h)$ equals $\rho(G,m,h)$ when G is cyclic, and establish an upper bound for $\rho_{\pm}(G,m,h)$ that we believe gives the exact value for all G, m, and h.

1 Introduction

Let G be a finite abelian group written with additive notation. For a nonnegative integer h and a nonempty subset A of G, we let hA and $h_{\pm}A$ denote the h-fold *sumset* and the h-fold *signed sumset* of A, respectively; that is, for an m-subset $A = \{a_1, \ldots, a_m\}$ of G, we let

$$hA = \{\Sigma_{i=1}^m \lambda_i a_i \ : \ (\lambda_1, \ldots, \lambda_m) \in \mathbb{N}_0^m, \ \Sigma_{i=1}^m \lambda_i = h\}$$

and

$$h_{\pm}A = \{\Sigma_{i=1}^m \lambda_i a_i \ : \ (\lambda_1, \ldots, \lambda_m) \in \mathbb{Z}^m, \ \Sigma_{i=1}^m |\lambda_i| = h\}.$$

While signed sumsets are less well-studied in the literature than sumsets are, they come up naturally: For example, in [4], the first author and Ruzsa investigated the *independence number* of a subset A of G, defined as the maximum value of $t \in \mathbb{N}$ for which

$$0 \notin \cup_{h=1}^t h_{\pm}A$$

(see also [1] and [2]); and in [12], Klopsch and Lev discussed the *diameter* of G with respect to A, defined as the minimum value of $s \in \mathbb{N}$ for which

$$\cup_{h=0}^{s} h_{\pm} A = G$$

(see also [13]). The independence number of A in G quantifies the "degree" to which A is linearly independent in G (no subset is "completely" independent), while the diameter of G with respect to A measures how "effectively" A generates G (if at all). Note that $h_{\pm}A$ is always contained in $h(A \cup -A)$, but this may be a proper containment when $h \geqslant 2$.

For a positive integer $m \leqslant |G|$, we let

$$\rho(G, m, h) = \min\{|hA| \ : \ A \subseteq G, |A| = m\}$$

and

$$\rho_{\pm}(G, m, h) = \min\{|h_{\pm}A| \ : \ A \subseteq G, |A| = m\}$$

(as usual, $|S|$ denotes the size of the finite set S). The value of $\rho(G, m, h)$ has a long and distinguished history and has been determined for all G, m, and h; in this paper we attempt to find $\rho_{\pm}(G, m, h)$.

We start by a brief review of the case of sumsets. In 1813, for prime values of p, Cauchy [5] found the minimum possible size of

$$A + B = \{a + b \ : \ a \in A, \ b \in B\}$$

among subsets A and B of given sizes in the cyclic group $\mathbb{Z}_p$. In 1935, Davenport [6] rediscovered Cauchy's result, which is now known as the Cauchy–Davenport Theorem. (Davenport was unaware of Cauchy's work until twelve years later; see [7].)

Theorem 1 (Cauchy–Davenport Theorem) *If A and B are nonempty subsets of the group $\mathbb{Z}_p$ of prime order p, then*

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}.$$

It can easily be seen that the bound is tight for all values of $|A|$ and $|B|$, and thus

$$\rho(\mathbb{Z}_p, m, 2) = \min\{p, 2m - 1\}.$$

After various partial results, the general case was finally solved in 2006 by Plagne [15] (see also [14], [9], and [10]). To state the result, we introduce the function

$$u(n, m, h) = \min\{f_d(m, h) \ : \ d \in D(n)\},$$

where n, m, and h are positive integers, $D(n)$ is the set of positive divisors of n, and

$$f_d(m, h) = (h \lceil m/d \rceil - h + 1) \cdot d.$$

(Here $u(n, m, h)$ is a relative of the Hopf–Stiefel function used also in topology and bilinear algebra; see, for example, [8], [11], [14], and [16].)

Theorem 2 (Plagne; cf. [15]) *Let n, m, and h be positive integers with $m \leqslant n$. For any abelian group G of order n we have*

$$\rho(G, m, h) = u(n, m, h).$$

Turning now to $\rho_{\pm}(G, m, h)$, we start by observing that

$$\rho_{\pm}(G, m, 0) = 1$$

and

$$\rho_{\pm}(G, m, 1) = m$$

for all G and m. To see the latter equality, it suffices to verify that one can always find a *symmetric* subset of size m in G, that is, an m-subset A of G for which $A = -A$. Therefore, from now on, we assume that $h \geqslant 2$.

We must admit that our study of $\rho_{\pm}(G, m, h)$ resulted in quite a few surprises. For a start, we noticed that, in spite of the fact that $h_{\pm}A$ is usually much larger than hA is, the equality

$$\rho_{\pm}(G, m, h) = \rho(G, m, h)$$

holds quite often; it is an easy exercise to verify that, among groups of order 24 or less, equality holds with only one exception: $\rho_{\pm}(\mathbb{Z}_3^2, 4, 2) = 8$ while $\rho(\mathbb{Z}_3^2, 4, 2) = 7$. In fact, we can prove that $\rho_{\pm}(G, m, h)$ agrees with $\rho(G, m, h)$ for all cyclic groups G and all m and h (see Theorem 4 below).

However, in contrast to $\rho(G, m, h)$, the value of $\rho_{\pm}(G, m, h)$ depends on the structure of G rather than just the order n of G. Suppose that G is of type $(n_1, \ldots, n_r)$, that is,

$$G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_1 \geqslant 2$ and n_i divides n_{i+1} for each $i \in \{1, \ldots, r-1\}$. We exhibit a specific subset $D(G, m)$ of $D(n)$ with which the quantity

$$u_{\pm}(G, m, h) = \min\{f_d(m, h) \ : \ d \in D(G, m)\}$$

provides an upper bound for $\rho_{\pm}(G, m, h)$ (see Theorem 5 below). Therefore, to get lower and upper bounds for $\rho_{\pm}(G, m, h)$, we minimize $f_d(m, h)$ for all $d \in D(n)$ and for $d \in D(G, m)$, respectively:

$$\min\{f_d(m, h) \ : \ d \in D(n)\} \leqslant \rho_{\pm}(G, m, h) \leqslant \min\{f_d(m, h) \ : \ d \in D(G, m)\}.$$

In fact, we also conjecture that

$$\rho_{\pm}(G, m, h) = u_{\pm}(G, m, h)$$

holds always except for one very special situation (see Conjecture 10 below).

Further surprises come from the inverse problem of trying to classify subsets that yield the minimum signed sumset size. To start with, we point out that it is not always

symmetric sets that work best. As an example, consider $\rho_{\pm}(\mathbb{Z}_5^2, 9, 2)$. One can see that for any 9 elements of $\pm a + H$, where H is any subgroup of size 5 and $a \notin H$, we have

$$2_{\pm}A = H \cup (\pm 2a + H),$$

so

$$\rho_{\pm}(\mathbb{Z}_5^2, 9, 2) = \rho(\mathbb{Z}_5^2, 9, 2) = 15.$$

Here A is not symmetric but is *near-symmetric*: it becomes symmetric once one of its elements is removed. However, we can verify that for any symmetric subset A of size 9, $2_{\pm}A$ must have size 17 or more, as follows: If A contains a subgroup H of size 5, then with any $a \in A \setminus H$, the 2-fold signed sumset of A will contain the 17 distinct elements of H, $\pm a + H$, and $\{\pm 2a\}$; while if A contains no subgroup of size 5, then

$$A \cap \{2a \ : \ a \in A\} = \{0\},$$

so

$$|2_{\pm}A| \geqslant |A| + |\{2a \ : \ a \in A\}| - 1 = 17.$$

And that is not all: sometimes it is best to take an *asymmetric* set, a set A where A and $-A$ are disjoint. It is easy to check that, in the example of $\rho_{\pm}(\mathbb{Z}_3^2, 4, 2) = 8$ mentioned above, with a 4-subset A of $\mathbb{Z}_3^2$ we get $2_{\pm}A = \mathbb{Z}_3^2 \setminus \{0\}$ when A is asymmetric, and $2_{\pm}A = \mathbb{Z}_3^2$ in all other cases.

We have thus seen that sets that minimize signed sumset size may be symmetric, near-symmetric, or asymmetric—we can prove, however, that there is always a set that is of one of these three types (see Theorem 3 below).

With this paper we aim to introduce the question of finding the minimum size of signed sumsets. Our approach here is entirely elementary. In the follow-up paper [3], we investigate the question in elementary abelian groups, where, using deeper results from additive combinatorics, we are able to assert more.

2 The role of symmetry

Given a group G and a positive integer $m \leqslant |G|$, we define a certain collection $\mathcal{A}(G, m)$ of m-subsets of G. We let

- $\mathrm{Sym}(G, m)$ be the collection of *symmetric* m-subsets of G, that is, m-subsets A of G for which $A = -A$;
- $\mathrm{Nsym}(G, m)$ be the collection of *near-symmetric* m-subsets of G, that is, m-subsets A of G that are not symmetric, but for which $A \setminus \{a\}$ is symmetric for some $a \in A$;
- $\mathrm{Asym}(G, m)$ be the collection of *asymmetric* m-subsets of G, that is, m-subsets A of G for which $A \cap (-A) = \emptyset$.

We then let

$$\mathcal{A}(G,m) = \mathrm{Sym}(G,m) \cup \mathrm{Nsym}(G,m) \cup \mathrm{Asym}(G,m).$$

In other words, $\mathcal{A}(G,m)$ consists of those m-subsets of G that have exactly m, $m-1$, or 0 elements whose inverse is also in the set.

Theorem 3 *For every G, m, and h, we have*

$$\rho_{\pm}(G,m,h) = \min\{|h_{\pm}A| \ : \ A \in \mathcal{A}(G,m)\}.$$

Proof: Since our claim is trivial when $m \leqslant 2$, we assume that $m \geqslant 3$.

For a subset S of G, let us define its *degree of symmetry*, denoted by $\mathrm{sdeg}(S)$, as the number of elements of S that are also elements of $-S$. We shall prove that for any m-subset B of G with

$$1 \leqslant \mathrm{sdeg}(B) \leqslant m-2,$$

there is an m-subset B' of G with

$$\mathrm{sdeg}(B') = \mathrm{sdeg}(B) + 2$$

and $|h_{\pm}B'| \leqslant |h_{\pm}B|$; repeated application of this results in a subset $A \in \mathcal{A}(G,m)$ with $|h_{\pm}A| \leqslant |h_{\pm}B|$, from which our result follows.

Let

$$B = \{b_1, b_2, b_3, \ldots, b_m\}$$

be an m-subset of G, and suppose that $-b_1 \notin B$, $-b_2 \notin B$, but $-b_3 \in B$. Note that we may have $b_3 = -b_3$; furthermore, the sets $\{\pm b_1\}$, $\{\pm b_2\}$, and $\{\pm b_3\}$ are pairwise disjoint. Replacing b_1 by $-b_2$ in B, we let

$$B' = \{-b_2, b_2, b_3, \ldots, b_m\}.$$

Then B' has size m, and its degree of symmetry is exactly two more than that of B; we need to show that $|h_{\pm}B'| \leqslant |h_{\pm}B|$. We shall, in fact, show that $h_{\pm}B' \subseteq h_{\pm}B$.

By definition, $h_{\pm}B'$ is the collection of all elements of the form

$$g = \lambda_1(-b_2) + \lambda_2 b_2 + \lambda_3 b_3 + \cdots + \lambda_m b_m$$

where $\sum_{i=1}^{m} |\lambda_i| = h$. Clearly, if λ_1 and λ_2 are of opposite sign or either one is zero, then

$$|\lambda_2 - \lambda_1| = |\lambda_1| + |\lambda_2|,$$

so

$$g = (\lambda_2 - \lambda_1)b_2 + \lambda_3 b_3 + \cdots + \lambda_m b_m \in h_{\pm}B.$$

Suppose now that λ_1 and λ_2 are both positive; the case when they are both negative can be handled similarly. Furthermore, we assume that $\lambda_1 \geqslant \lambda_2$; again, the reverse case is analogous.

Assume first that $2b_3 = 0$; in this case we have $\lambda_3 b_3 = -\lambda_3 b_3$, and thus we may assume that $\lambda_3 \geqslant 0$. Observe that

$$g = (\lambda_2 - \lambda_1)b_2 + (2\lambda_1 + \lambda_3)b_3 + \lambda_4 b_4 + \cdots + \lambda_m b_m,$$

and

$$|\lambda_2 - \lambda_1| + |2\lambda_1 + \lambda_3| + |\lambda_4| + \cdots + |\lambda_m| = h,$$

thus $g \in h_\pm B$.

Finally, suppose that $2b_3 \neq 0$; since $-b_3 \in B$, we must have $m \geqslant 4$, and without loss of generality we can assume that $b_4 = -b_3$. We can rewrite g as follows:

$$g = \begin{cases} (\lambda_2 - \lambda_1)b_2 + (\lambda_1 + \lambda_3)b_3 + (\lambda_1 + \lambda_4)b_4 + \lambda_5 b_5 + \cdots + \lambda_m b_m & \text{if } \lambda_3 \geqslant 0, \lambda_4 \geqslant 0; \\ (\lambda_2 - \lambda_1)b_2 + (\lambda_1 + \lambda_3 - \lambda_4)b_3 + \lambda_1 b_4 + \lambda_5 b_5 + \cdots + \lambda_m b_m & \text{if } \lambda_3 \geqslant 0, \lambda_4 \leqslant 0; \\ (\lambda_2 - \lambda_1)b_2 + \lambda_1 b_3 + (\lambda_1 - \lambda_3 + \lambda_4)b_4 + \lambda_5 b_5 + \cdots + \lambda_m b_m & \text{if } \lambda_3 \leqslant 0, \lambda_4 \geqslant 0; \\ (\lambda_2 - \lambda_1)b_2 + (\lambda_1 - \lambda_4)b_3 + (\lambda_1 - \lambda_3)b_4 + \lambda_5 b_5 + \cdots + \lambda_m b_m & \text{if } \lambda_3 \leqslant 0, \lambda_4 \leqslant 0. \end{cases}$$

Since the expressions above show that $g \in h_\pm B$ in each case, our proof is complete. □

3 Cyclic groups

In this section we prove that, when G is cyclic, then $\rho_\pm(G, m, h)$ agrees with $\rho(G, m, h)$ for all m and h.

Theorem 4 *For all positive integers n, m, and h, we have*

$$\rho_\pm(\mathbb{Z}_n, m, h) = \rho(\mathbb{Z}_n, m, h).$$

Proof: Since the reverse inequality is obvious, it suffices to prove that

$$\rho_\pm(\mathbb{Z}_n, m, h) \leqslant \rho(\mathbb{Z}_n, m, h).$$

Recall that

$$\rho(\mathbb{Z}_n, m, h) = \min\{f_d(m, h) \ : \ d \in D(n)\}.$$

Observe that, for any symmetric subset R of G (that is, for every subset R for which $R = -R$), we have $h_\pm R = hR$. Our strategy is to find, for each $d \in D(n)$, a symmetric subset $R = R_d(n, m)$ of $\mathbb{Z}_n$ so that $|R| \geqslant m$ and $|hR| \leqslant f_d(m, h)$; this will then imply that

$$\rho_\pm(\mathbb{Z}_n, m, h) \leqslant \min\{f_d(m, h) \ : \ d \in D(n)\} = \rho(\mathbb{Z}_n, m, h).$$

We introduce some notations. We write $n = 2^a n_0$, $d = 2^b d_0$, and $\lceil m/d \rceil = 2^c m_0$, where a, b, and c are nonnegative integers and n_0, d_0, and m_0 are odd positive integers. Our explicit construction of R depends on whether $b + c \leqslant a$ or not.

Suppose first that $b + c \leqslant a$. In this case, let H be the subgroup of G that has order $2^c d$, and set

$$R = \bigcup_{i=-\lfloor m_0/2 \rfloor}^{\lfloor m_0/2 \rfloor} (i + H).$$

Clearly, R is symmetric; to see that R has size at least m, note that for the index of H in G we have

$$|G : H| = n/(2^c d) \geqslant \lceil m/d \rceil / 2^c = m_0 = 2 \lfloor m_0/2 \rfloor + 1,$$

hence

$$|R| = (2 \lfloor m_0/2 \rfloor + 1) \cdot |H| = d \lceil m/d \rceil \geqslant m.$$

To verify that $|hR| \leqslant f_d(m, h)$, note that

$$hR = \bigcup_{i=-h\lfloor m_0/2 \rfloor}^{h\lfloor m_0/2 \rfloor} (i + H),$$

so

$$\begin{aligned} |hR| &= \min\{n, (2h \lfloor m_0/2 \rfloor + 1) \cdot |H|\} \\ &\leqslant (2h \lfloor m_0/2 \rfloor + 1) \cdot |H| \\ &= (hm_0 - h + 1) \cdot 2^c d \\ &\leqslant (2^c h m_0 - h + 1) d \\ &= f_d(m, h). \end{aligned}$$

In the case when $b + c \geqslant a + 1$, we let H be the subgroup of G that has order $2^a d_0$, and set

$$R = \bigcup_{i=1}^{2^{b+c-a-1} m_0} (\lfloor e/2 \rfloor + i + H) \cup (-\lfloor e/2 \rfloor - i + H),$$

where $e = n_0/d_0$. We see that R is symmetric; in order to estimate $|R|$ and $|hR|$, we rewrite R as follows.

Note that e is an odd integer, and thus

$$-\lfloor e/2 \rfloor = \lfloor e/2 \rfloor + 1 - e;$$

furthermore, $e = n/|H|$ and thus e is an element (in fact, a generator) of H, and so

$$-\lfloor e/2 \rfloor - i + H = \lfloor e/2 \rfloor + 1 - i + H$$

for every integer i. With this, we have

$$R = \bigcup_{i=-2^{b+c-a-1} m_0 + 1}^{2^{b+c-a-1} m_0} (\lfloor e/2 \rfloor + i + H).$$

To show that R has size at least m, we see that, for the index of H in G, we have

$$|G:H| = n/(2^a d_0) = 2^{b-a} n/d \geqslant 2^{b-a} \lceil m/d \rceil = 2^{b+c-a} m_0,$$

hence

$$|R| = \left(2^{b+c-a} m_0\right) \cdot |H| = d \lceil m/d \rceil \geqslant m.$$

Finally,

$$hR = \bigcup_{i=-2^{b+c-a-1}hm_0+h}^{2^{b+c-a-1}hm_0} (H + h\lfloor e/2 \rfloor + i),$$

so for $|hR|$ we get

$$\begin{aligned} |hR| &= \min\{n, \left(2^{b+c-a} hm_0 - h + 1\right) \cdot |H|\} \\ &\leqslant \left(2^{b+c-a} hm_0 - h + 1\right) \cdot |H| \\ &= \left(2^{b+c-a} hm_0 - h + 1\right) \cdot 2^a d_0 \\ &\leqslant (2^c hm_0 - h + 1)d \\ &= f_d(m,h), \end{aligned}$$

with which our proof is complete. □

4 Noncyclic groups

Let us now turn to noncyclic groups. We say that a finite abelian group G has type $(n_1, \ldots, n_r)$ if it is isomorphic to the invariant product

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

where $n_1 \geqslant 2$ and n_i divides n_{i+1} for each $i \in \{1, \ldots, r-1\}$. Here r is the rank of G, n_r is the exponent of G, and we still use the notation $n = \Pi_{i=1}^r n_i$ for the order of G.

Recall that for the minimum size of the h-fold sumset of an m-subset of a group of order n we have

$$\rho(G,m,h) = \min\{f_d(m,h) \ : \ d \in D(n)\}.$$

This, of course, implies that for signed sumsets we have the lower bound

$$\rho_\pm(G,m,h) \geqslant \min\{f_d(m,h) \ : \ d \in D(n)\}.$$

It turns out that we can get an upper bound for $\rho_\pm(G,m,h)$ by minimizing $f_d(m,h)$ for a certain subset of $D(n)$; more precisely, we establish the following result:

Theorem 5 *The minimum size of the h-fold signed sumset of an m-subset of a group G of type $(n_1, \ldots, n_r)$ satisfies*

$$\rho_\pm(G,m,h) \leqslant \min\{f_d(m,h) \ : \ d \in D(G,m)\},$$

where

$$D(G,m) = \{d \in D(n) \ : \ d = d_1 \cdots d_r, d_1 \in D(n_1), \ldots, d_r \in D(n_r), dn_r \geqslant d_r m\}.$$

Observe that, for cyclic groups of order n, $D(G,m)$ is simply $D(n)$.

Theorem 5 will be the immediate consequence of Propositions 6 and 7 below.

Proposition 6 *For every group G of type $(n_1,\ldots,n_r)$ and order n, $m \leqslant n$, and $h \in \mathbb{N}$ we have*

$$\rho_{\pm}(G,m,h) \leqslant u_{\pm}(G,m,h),$$

where

$$u_{\pm}(G,m,h) = \min\left\{\Pi_{i=1}^{r} u(n_i,m_i,h) \ : \ m_1 \leqslant n_1,\ldots,m_r \leqslant n_r, \Pi_{i=1}^{r} m_i \geqslant m\right\}.$$

Proof: For each $i = 1,2,\ldots,r$, let m_i be an integer so that $m_i \leqslant n_i$ but $m_1\cdots m_r \geqslant m$. According to the proof of Theorem 4, for each i we can find symmetric sets $A_i \subseteq \mathbb{Z}_{n_i}$ of size at least m_i for which

$$|h_{\pm}A_i| = |hA_i| = u(n_i,m_i,h).$$

Therefore, $A_1\times\cdots\times A_r$ is a symmetric subset of $Z_{n_1}\times\cdots\times Z_{n_r}$ of size at least $m_1\cdots m_r$, so we have

$$\begin{aligned}
\rho_{\pm}(\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_r},m,h) &\leqslant \rho_{\pm}(\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_r},m_1\cdots m_r,h)\\
&\leqslant |h_{\pm}(A_1\times\cdots\times A_r)|\\
&= |h(A_1\times\cdots\times A_r)|\\
&\leqslant |hA_1\times\cdots\times hA_r|\\
&= u(n_1,m_1,h)\cdots u(n_r,m_r,h),
\end{aligned}$$

as claimed. □

Proposition 7 *With the notations as introduced above, we have*

$$u_{\pm}(G,m,h) = \min\{f_d(m,h) \ : \ d \in D(G,m)\}.$$

Proof: First, we prove that

$$u_{\pm}(G,m,h) \leqslant \min\{f_d(m,h) \ : \ d \in D(G,m)\}.$$

Suppose that $d_1,\ldots,d_r$ are positive integers so that $d_1 \in D(n_1),\ldots,d_r \in D(n_r)$, and $dn_r \geqslant d_r m$, where $d = d_1\cdots d_r$. Let $m_1 = d_1,\ldots,m_{r-1} = d_{r-1}$, and $m_r = \lceil d_r m/d\rceil$. By assumption, $m_i \leqslant n_i$ for all $1 \leqslant i \leqslant r$, and we also have $m_1\cdots m_r \geqslant m$; we will establish our claim by showing that

$$u_{\pm}(G,m,h) \leqslant f_d(m,h).$$

Observe that, for each $1 \leqslant i \leqslant r-1$,

$$f_{d_i}(m_i,h) = f_{d_i}(d_i,h) = (h\lceil d_i/d_i\rceil - h + 1)\, d_i = d_i,$$

and

$$f_{d_r}(m_r,h) = f_{d_r}(\lceil d_r m/d\rceil, h) = (h\lceil\lceil d_r m/d\rceil/d_r\rceil - h + 1)\, d_r,$$

which, according to an identity for the ceiling function, equals

$$(h\lceil m/d\rceil - h + 1)\, d_r.$$

Therefore,

$$f_{d_1}(m_1,h)\cdots f_{d_r}(m_r,h) = (h\lceil m/d\rceil - h + 1)\, d = f_d(m,h).$$

Our claim now follows, since

$$u_{\pm}(G,m,h) \leqslant u(n_1,m_1,h)\cdots u(n_r,m_r,h) \leqslant f_{d_1}(m_1,h)\cdots f_{d_r}(m_r,h).$$

Conversely, we need to prove that

$$u_{\pm}(G,m,h) \geqslant \min\{f_d(m,h) \ : \ d \in D(G,m)\}. \tag{1}$$

As we have already mentioned, this holds for cyclic groups. We will now prove that the inequality also holds for $r = 2$; that is, for a group of type (n_1,n_2) we have

$$u_{\pm}(G,m,h) \geqslant \min\{f_{d_1d_2}(m,h) \ : \ d_1 \in D(n_1), d_2 \in D(n_2), d_1n_2 \geqslant m\}. \tag{2}$$

Suppose that positive integers m_1 and m_2 are selected so that $m_1 \leqslant n_1$, $m_2 \leqslant n_2$, $m_1m_2 \geqslant m$, and

$$u_{\pm}(G,m,h) = u(n_1,m_1,h)\cdot u(n_2,m_2,h);$$

furthermore, suppose that integers δ_1 and δ_2 are chosen so that $\delta_1 \in D(n_1)$, $\delta_2 \in D(n_2)$, $u(n_1,m_1,h) = f_{\delta_1}(m_1,h)$, and $u(m_2,h) = f_{\delta_2}(m_2,h)$. We need to prove that there are integers d_1 and d_2, so that $d_1 \in D(n_1)$, $d_2 \in D(n_2)$, $d_1n_2 \geqslant m$, and

$$f_{d_1d_2}(m,h) \ \leqslant \ f_{\delta_1}(m_1,h)\cdot f_{\delta_2}(m_2,h). \tag{3}$$

We will separate two cases depending on whether $\delta_1n_2 \geqslant m$ or not.

In the case when $\delta_1n_2 \geqslant m$, we show that $d_1 = \delta_1$ and $d_2 = \delta_2$ are appropriate choices. Clearly, $d_1 \in D(n_1)$, $d_2 \in D(n_2)$, and $d_1n_2 \geqslant m$, so we just need to show that

$$f_{d_1d_2}(m,h) \leqslant f_{d_1}(m_1,h)\cdot f_{d_2}(m_2,h).$$

Since $m \leqslant m_1m_2$ and the function f is nondecreasing in m, it suffices to prove that

$$f_{d_1d_2}(m_1m_2,h) \leqslant f_{d_1}(m_1,h)\cdot f_{d_2}(m_2,h),$$

or, equivalently, that

$$h\lceil(m_1m_2)/(d_1d_2)\rceil - h + 1 \leqslant (h\lceil m_1/d_1\rceil - h + 1)\cdot(h\lceil m_2/d_2\rceil - h + 1).$$

Note that

$$\lceil(m_1m_2)/(d_1d_2)\rceil \leqslant \lceil m_1/d_1\rceil\cdot\lceil m_2/d_2\rceil,$$

so our inequality will follow once we prove that

$$h\lceil m_1/d_1\rceil \cdot \lceil m_2/d_2\rceil - h + 1 \leqslant (h\lceil m_1/d_1\rceil - h + 1)\cdot(h\lceil m_2/d_2\rceil - h + 1)\,.$$

But this indeed holds as subtracting the left-hand side from the right-hand side yields

$$h(h-1)\left(\lceil m_1/d_1\rceil - 1\right)\left(\lceil m_2/d_2\rceil - 1\right),$$

which is clearly nonnegative.

Suppose now that $\delta_1 n_2 < m$; we consider two subcases: when $m_2 \leqslant \delta_2$ and when $m_2 > \delta_2$.

When $\delta_1 n_2 < m$ and $m_2 \leqslant \delta_2$, we set $d_1 = \gcd(n_1, \delta_2)$ and $d_2 = \delta_1\delta_2/\gcd(n_1,\delta_2)$. Then, clearly, $d_1 \in D(n_1)$; to see that $d_2 \in D(n_2)$, note that n_1/d_1 and δ_2/d_1 are relatively prime integers that both divide n_2/d_1, so their product $n_1\delta_2/d_1^2$ divides n_2/d_1 as well, and therefore $n_1\delta_2/d_1$, and thus its divisor d_2, divide n_2. Furthermore, since $n_1\delta_2/d_1$ divides n_2, we have

$$d_1 n_2 \geqslant n_1\delta_2 \geqslant m_1 m_2 \geqslant m.$$

It remains to be shown that (3) holds, but since $d_1 d_2 = \delta_1\delta_2$, this follows as in the previous case.

Finally, suppose that $\delta_1 n_2 < m$ and $m_2 > \delta_2$; we now set $d_1 = n_1$ and $d_2 = \delta_1 n_2/n_1$. We see that $d_1 \in D(n_1)$, $d_2 \in D(n_2)$, and $d_1 n_2 \geqslant m$; we need to show that (3) holds.

Let us denote $\lceil m_1/\delta_1\rceil$ and $\lceil m_2/\delta_2\rceil$ by k_1 and k_2, respectively; note that $m_2 > \delta_2$ implies that $k_2 \geqslant 2$, and $\delta_1 n_2 < m$ implies that $k_1 \geqslant 2$ as well, since

$$m_1 \geqslant m/m_2 > \delta_1 n_2/m_2 \geqslant \delta_1.$$

Therefore,

$$2(k_1-1)(k_2-1) = (k_1-2)(k_2-2) + (k_1k_2-2) \geqslant k_1k_2 - 2,$$

so, since $h \geqslant 2$, we get

$$h(h-1)(k_1-1)(k_2-1) \geqslant k_1k_2 - 2,$$

or, equivalently,

$$(hk_1 - h + 1)\cdot(hk_2 - h + 1) \geqslant (h+1)(k_1k_2 - 1).$$

Multiplying by $\delta_1\delta_2$ yields exactly

$$f_{\delta_1}(m_1, h)\cdot f_{\delta_2}(m_2, h)$$

on the left hand side; therefore, to prove (3), it is enough to verify that

$$f_{d_1d_2}(m,h) \leqslant (h+1)(k_1k_2-1)\delta_1\delta_2. \tag{4}$$

By definition,

$$f_{d_1d_2}(m,h) = f_{\delta_1 n_2}(m,h) = (h\lceil m/(\delta_1 n_2)\rceil - h + 1)\,\delta_1 n_2.$$

But

$$\left\lceil \frac{m}{\delta_1 n_2} \right\rceil \leqslant \left\lceil \frac{m_1 m_2}{\delta_1 n_2} \right\rceil \leqslant \left\lceil \frac{k_1 k_2 \delta_1 \delta_2}{\delta_1 n_2} \right\rceil = \left\lceil \frac{k_1 k_2}{n_2/\delta_2} \right\rceil \leqslant \frac{k_1 k_2 + n_2/\delta_2 - 1}{n_2/\delta_2},$$

hence

$$f_{d_1 d_2}(m,h) \leqslant (h(k_1k_2 - 1) + n_2/\delta_2)\,\delta_1\delta_2. \tag{5}$$

Since we are under the assumption that $\delta_1 n_2 < m$, we have

$$\frac{n_2}{\delta_2} < \frac{m}{\delta_1\delta_2} \leqslant \frac{m_1 m_2}{\delta_1\delta_2} \leqslant k_1 k_2,$$

so the integer n_2/δ_2 can be at most $k_1k_2 - 1$, and thus (5) implies (4), completing the proof of (2).

In order to prove that (1) holds for any fixed $r > 2$, we suppose that positive integers $m_1, \ldots, m_r$ are selected so that $m_i \leqslant n_i$ for each $1 \leqslant i \leqslant r$, $m_1 \cdots m_r \geqslant m$, and

$$u_{\pm}(G, m, h) = u(n_1, m_1, h) \cdots u(n_r, m_r, h).$$

Furthermore, we suppose that integers $\delta_1, \ldots, \delta_r$ are chosen so that for each $1 \leqslant i \leqslant r$, $\delta_i \in D(n_i)$ and $u(n_i, m_i, h) = f_{\delta_i}(m_i, h)$. We will prove that there are integers $d_1, \ldots, d_r$, so that, for each $1 \leqslant i \leqslant r$, $d_i \in D(n_i)$,

$$d_1 \cdots d_{r-1} n_r \;\; \geqslant \;\; m, \tag{6}$$

and

$$f_{d_1 \cdots d_r}(m,h) \;\; \leqslant \;\; u_{\pm}(G,m,h) = f_{\delta_1}(m_1,h)\cdots f_{\delta_r}(m_r,h). \tag{7}$$

We proceed by induction, and assume that (1) holds for $r-1$ terms and for $m' = m_2 \cdots m_r$; in particular, for a group G of rank $r-1$ and of type $(n_2, \ldots, n_r)$ we have

$$u_{\pm}(G, m', h) \geqslant \min\{f_d(m', h) \;:\; d \in D(G, m')\}.$$

Therefore, we are able to find integers $\mu_2, \ldots, \mu_r$ so that $\mu_i \in D(n_i)$ for each $2 \leqslant i \leqslant r$,

$$\mu_2 \cdots \mu_{r-1} n_r \;\; \geqslant \;\; m', \tag{8}$$

and

$$f_{\mu_2 \cdots \mu_r}(m', h) \;\; \leqslant \;\; u_{\pm}(G, m', h) \leqslant f_{\delta_2}(m_2, h) \cdots f_{\delta_r}(m_r, h). \tag{9}$$

Furthermore, observing that by (8), $m'' = \lceil m'/(\mu_2 \cdots \mu_{r-1})\rceil$ is at most n_r, from (2), for a group of rank 2 and of type (n_1, n_r) we have

$$u_{\pm}(G, m_1 m'', h) \geqslant \min\{f_d(m_1 m'', h) \;:\; d \in D(G, m_1 m'')\},$$

and so there are integers $\nu_1 \in D(n_1)$ and $\nu_r \in D(n_r)$ for which

$$\nu_1 n_r \;\geqslant\; m_1 m'', \tag{10}$$

and

$$f_{\nu_1\nu_r}(m_1m'', h) \;\leqslant\; u_{\pm}(G, m_1m'', h) \leqslant f_{\delta_1}(m_1, h) \cdot f_{\mu_r}(m'', h). \tag{11}$$

Now let $d_1 = \nu_1$, $d_r = \nu_r$, and $d_i = \mu_i$ for $2 \leqslant i \leqslant r-1$. We immediately see that, with these notations, (6) holds, since, by (10),

$$d_1 \cdots d_{r-1} n_r = \nu_1 \mu_2 \cdots \mu_{r-1} n_r \geqslant m_1 \mu_2 \cdots \mu_{r-1} m'' \geqslant m_1 m' = m_1 \cdots m_r \geqslant m.$$

To see that (7) holds, note that, for the left-hand side we have

$$\begin{aligned} f_{d_1\cdots d_r}(m, h) &= f_{\nu_1\nu_r\mu_2\cdots\mu_{r-1}}(m, h) \\ &\leqslant f_{\nu_1\nu_r\mu_2\cdots\mu_{r-1}}(m_1m''\mu_2\cdots\mu_{r-1}, h) \\ &= (h\,\lceil (m_1m'')/(\nu_1\nu_r)\rceil - h + 1)\,\nu_1\nu_r\mu_2\cdots\mu_{r-1} \\ &= f_{\nu_1\nu_r}(m_1m'', h)\mu_2\cdots\mu_{r-1}; \end{aligned}$$

and, for the right-hand side of (7), using (9), we see that

$$\begin{aligned} f_{\delta_1}(m_1, h)\cdots f_{\delta_r}(m_r, h) &\geqslant f_{\delta_1}(m_1, h) f_{\mu_2\cdots\mu_r}(m', h) \\ &= f_{\delta_1}(m_1, h)\,(h\,\lceil m'/(\mu_2\cdots\mu_r)\rceil - h + 1)\,\mu_2\cdots\mu_r \\ &= f_{\delta_1}(m_1, h)\,(h\,\lceil m''/\mu_r\rceil - h + 1)\,\mu_2\cdots\mu_r \\ &= f_{\delta_1}(m_1, h) f_{\mu_r}(m'', h)\mu_2\cdots\mu_{r-1}. \end{aligned}$$

Therefore, (7) follows from (11). With this, the proof of (1), and thus of Proposition 7, is complete. □

Our next result exhibits a situation where the upper bound of Proposition 6, and thus of Theorem 5, is not tight:

Proposition 8 *If G is a noncyclic group of odd order n and type $(n_1, \ldots, n_r)$, then*

$$\rho_{\pm}\,(G, (n-1)/2, 2) \leqslant n-1,$$

but

$$u_{\pm}(G, (n-1)/2, 2) = n.$$

Proof: Note that every element of $G \setminus \{0\}$ has order at least 3, thus there is a subset A of $G \setminus \{0\}$ with which $G \setminus \{0\}$ can be partitioned into A and $-A$. Since $|A| = (n-1)/2$ and $0 \notin 2_{\pm}A$, we have

$$\rho_{\pm}\,(G, (n-1)/2, 2) \leqslant n-1.$$

To prove our second claim, note that for each $i \in \{1, \ldots, r\}$,

$$n/n_i \cdot (n_i - 1)/2 < (n-1)/2.$$

Therefore, if positive integers $m_1, \ldots, m_r$ satisfy $m_i \leqslant n_i$ for each $i \in \{1, \ldots, r\}$ and

$$m_1 \cdots m_r \geqslant (n-1)/2,$$

then we must have $m_i \geqslant (n_i+1)/2$, and thus $u(n_i, m_i, 2) = n_i$, for each $i \in \{1, \ldots, r\}$, from which our claim follows. □

A bit more generally, if d is an odd element of $D(n)$ so that $d \geqslant 2m+1$, then the same argument yields

$$\rho_{\pm}(G, m, 2) \leqslant d-1,$$

and therefore we have the following:

Corollary 9 *Suppose that G is an abelian group of order n and type $(n_1, \ldots, n_r)$. Let $m \leqslant n$, and let d_m be the smallest odd element of $D(n)$ that is at least $2m+1$; if no such element exists, set $d_m = \infty$. We then have*

$$\rho_{\pm}(G, m, 2) \leqslant \min\{u_{\pm}(G, m, 2), d_m - 1\}.$$

We are not aware of any subsets with smaller signed sumset size, and we believe that the following holds:

Conjecture 10 *Suppose that G is an abelian group of order n and type $(n_1, \ldots, n_r)$. Let $m \leqslant n$ and $h \geqslant 2$.*

If $h \geqslant 3$, then

$$\rho_{\pm}(G, m, h) = u_{\pm}(G, m, h).$$

If each odd divisor of n is less than $2m$, then

$$\rho_{\pm}(G, m, 2) = u_{\pm}(G, m, 2).$$

If there are odd divisors of n greater than $2m$, let d_m be the smallest one. We then have

$$\rho_{\pm}(G, m, 2) = \min\{u_{\pm}(G, m, 2), d_m - 1\}.$$

5 An example

Trivially, if G is an elementary abelian 2-group, then $\rho_{\pm}(G, m, h)$ agrees with $\rho(G, m, h)$, and it is not hard to see that this is also true if G is any 2-group. More generally still, as an application to Theorem 5, we prove the following:

Proposition 11 *If there is no odd prime p for which $\mathbb{Z}_p^2$ is isomorphic to a subgroup of G, then*

$$\rho_{\pm}(G, m, h) = \rho(G, m, h).$$

Proof: Suppose that G is of order n and of type $(n_1, \ldots, n_r)$; by Theorem 4, we may assume that $r \geqslant 2$.

Let $d \in D(n)$ be such that

$$\rho\,(G, m, h) = u(n, m, h) = f_d(m, h).$$

By Theorem 5, it suffices to prove that $d \in D(G, m)$.

Our assumption that there is no odd prime p for which $\mathbb{Z}_p^2$ is isomorphic to a subgroup of G is equivalent to saying that $n_1 \cdots n_{r-1}$ is a power of 2; let

$$n_1 \cdots n_{r-1} = 2^{k_1}.$$

Furthermore, we write

$$n_r = 2^{k_2} \cdot c_2$$

and

$$d = 2^{k_3} \cdot c_3,$$

where k_2 and k_3 are nonnegative integers, and c_2 and c_3 are odd. Note that

$$k_1 + k_2 \;\;\geqslant\;\; k_3, \tag{12}$$

and c_2 must be divisible by c_3.

Now if $m \leqslant n_r$, then clearly $d \in D(G, m)$, so assume that $m \geqslant n_r + 1$, and thus there is a nonnegative integer k for which

$$2^k \cdot n_r + 1 \leqslant m \leqslant 2^{k+1} \cdot n_r.$$

Note that we must then have

$$k_1 \;\;\geqslant\;\; k + 1. \tag{13}$$

We claim that we also have

$$k_3 \;\;\geqslant\;\; k_2 + k + 1. \tag{14}$$

Indeed,

$$\begin{aligned} u(n, m, h) &= f_d(m, h) \\ &= (h \cdot \lceil m/d \rceil - h + 1) \cdot d \\ &\geqslant \left(h \cdot \left\lceil \frac{2^k \cdot n_r + 1}{d} \right\rceil - h + 1 \right) \cdot d. \end{aligned}$$

On the other hand, from (13) we see that G contains a subgroup of order $2^{k+1} \cdot n_r$, and thus

$$\begin{aligned} u(n, m, h) &\leqslant 2^{k+1} \cdot n_r \\ &< h \cdot 2^k \cdot n_r + d \\ &= \left(h \cdot \frac{2^k \cdot n_r + d}{d} - h + 1 \right) \cdot d. \end{aligned}$$

Therefore,

$$\left\lceil \frac{2^k \cdot n_r + 1}{d} \right\rceil < \frac{2^k \cdot n_r + d}{d},$$

which yields that $2^k \cdot n_r$ cannot be divisible by d, that is, $2^{k+k_2} \cdot c_2$ cannot be divisible by $2^{k_3} \cdot c_3$, proving (14).

Now let

$$d_r = 2^{k_2} \cdot c_3.$$

Then d_r is a divisor of n_r; furthermore, by (14), $d/d_r = 2^{k_3 - k_2}$ is an integer, and by (12), it is a divisor of $n_1 \cdots n_{r-1}$. Using (14) again, we have

$$d \cdot n_r = 2^{k_3} \cdot c_3 \cdot n_r \geqslant 2^{k_2+k+1} \cdot c_3 \cdot n_r = d_r \cdot 2^{k+1} \cdot n_r \geqslant d_r \cdot m,$$

so $d \in D(G, m)$, as claimed. □

Having a subgroup that is isomorphic to $\mathbb{Z}_p^2$ for an odd prime p is thus a necessary condition for $\rho_{\pm}(G, m, h)$ to be greater than $\rho(G, m, h)$. We study $\mathbb{Z}_p^2$, and, more generally, elementary abelian groups, in the upcoming paper [3].

References

[1] B. Bajnok, Spherical Designs and Generalized Sum-Free Sets in Abelian Groups. Special issue dedicated to Dr. Jaap Seidel on the occasion of his 80th birthday (Oisterwijk, 1999). *Des. Codes Cryptogr.* **21** (2000), no. 1–3, 11-18.

[2] B. Bajnok, The Spanning Number and the Independence Number of a Subset of an Abelian Group. In *Number Theory,* D. Chudnovsky, G. Chudnovsky, and M. Nathalson (Ed.), Springer-Verlag (2004), 1-16.

[3] B. Bajnok and R. Matzke, On the Minimum Size of Signed Sumsets in Elementary Abelian Groups, Preprint, http://arxiv.org/abs/1412.1609 (2014).

[4] B. Bajnok and I. Ruzsa, The Independence Number of a Subset of an Abelian Group. *Integers* **3** (2003), Paper No. A2, 23 pp.

[5] A.-L. Cauchy, Recherches sur les nombres, *J. École Polytechnique* **9** (1813), 99–123.

[6] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[7] H. Davenport, A historical note, *J. London Math. Soc.* **22** (1947), 100–101.

[8] S. Eliahou and M. Kervaire, Old and new formulas for the Hopf–Stiefel and related functions, *Expo. Math.*, **23** (2005), no. 2, 127–145.

[9] S. Eliahou and M. Kervaire, Some extensions of the Cauchy–Davenport Theorem, *Electron. Notes in Discrete Math.*, **28** (2007) 557–564.

[10] S. Eliahou, M. Kervaire, and A. Plagne, Optimally small sumsets in finite abelian groups, *J. Number Theory*, **101** (2003), 338–348.

[11] Gy. Károlyi, A note on the Hopf–Stiefel function. *European J. Combin.*, **27** (2006), 1135–1137.

[12] B. Klopsch and V. F. Lev, How long does it take to generate a group? *J. Algebra*, **261** (2003), 145–171.

[13] B. Klopsch and V. F. Lev, Generating abelian groups by addition only. *Forum Math.*, **21** (2009), no. 1, 23–41.

[14] A. Plagne, Additive number theory sheds extra light on the Hopf–Stiefel ∘ function, *Enseign. Math., II Sér*, **49**(2003), no. 1–2, 109–116.

[15] A. Plagne, Optimally small sumsets in groups, I. The supersmall sumset property, the $\mu_G^{(k)}$ and the $\nu_G^{(k)}$ functions, *Unif. Distrib. Theory*, **1** (2006), no. 1, 27–44.

[16] D. Shapiro, Products of sums of squares, *Expo. Math.*, **2** (1984), 235–261.