https://doi.org/10.1016/j.ejc.2013.05.020

LARGE RESTRICTED SUMSETS IN GENERAL ABELIAN GROUPS

Y. O. HAMIDOUNE, S. C. LÓPEZ, AND A. PLAGNE

Shortly after this work was started, the first-named author and main inspirator of this article passed away unexpectedly. The two other authors dedicate the paper to his memory.

Abstract. Let A, B and S be subsets of a finite Abelian group G. The restricted sumset of A and B with respect to S is defined as $A \wedge^S B = \{a + b : a \in A, b \in B \text{ and } a - b \notin S\}$. Let $L_S = \max_{z \in G} |\{(x, y) : \ x, y \in G, \ x + y = z \text{ and } x - y \in S\}|$. A simple application of the pigeonhole principle shows that $|A| + |B| > |G| + L_S$ implies $A \wedge^S B = G$. We then prove that if $|A| + |B| = |G| + L_S$ then $|A \wedge^S B| \geq |G| - 2|S|$. We also characterize the triples of sets (A, B, S) such that $|A| + |B| = |G| + L_S$ and $|A \wedge^S B| = |G| - 2|S|$. Moreover, in this case, we also provide the structure of the set $G \setminus (A \wedge^S B)$.

1. Introduction

Let G be a finite Abelian group. Given two subsets A and B of G, the *sumset* and the *restricted sumset* of A and B are defined, respectively, by

$$A + B = \{a + b : a \in A, b \in B\} \quad \text{and} \quad A \wedge B = \{a + b : a \in A, b \in B \text{ and } a \neq b\}.$$

We shall write $A + b$ or $A - b$ instead of $A + \{b\}$ and $A + \{-b\}$.

To give lower bounds for the cardinality of sumsets is probably the most central problem of additive number theory (see [11] for a general overview). A historical result in this area is the famous Cauchy-Davenport theorem [2, 3].

Theorem A (Cauchy, Davenport). *Let A and B be non-empty subsets of the group of prime order p. Then*

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

For restricted sumsets, the most famous result is due to Dias da Silva and Hamidoune [5] who, in the beginning of the 1990s, solved an Erdős-Heilbronn conjecture which remained open since 1964:

Theorem B (Dias da Silva and Hamidoune). *Let A and B be non-empty sets of the group of prime order p. Then*

$$|A \wedge B| \geq \min\{p, |A| + |B| - 3\}.$$

Several years later, Alon, Nathanson and Rusza [1] proposed an alternative proof using the so-called polynomial method, a powerful method which has then inspired a lot of new results in additive combinatorics.

Another important set of problems in the area is known under the name of *Critical Pair Theory.* Having found a general lower bound for the cardinality of sumsets, the problem is now to achieve the description of pairs of sets, the sum of which attains the lower bound. For instance, Vosper's Theorem describe precisely the pairs of subsets (A, B) in a group of prime order such that $|A+B| = |A|+|B|-1$.

We now introduce some notation and tools needed in the sequel and formulate a few basic remarks.

Let G_0 denote the subgroup of G composed of elements of order 2 or less, that is,

$$G_0 = \{x \in G : \ 2x = 0\}.$$

We write $L(G) = |G_0|$, the *doubling constant* introduced by Lev in [10]. Notice that if $|G|$ is odd, then $L(G) = 1$ whereas if $|G|$ is even, $L(G)$ is a power of 2. It is immediate to notice that $L(G)$ is the maximal number of pairwise distinct elements of a group G that can share a common doubling, in other words

$$L(G) = \max_{t \in G} |\{x \in G : \ 2x = t\}|.$$

If two sets A and B of G are given, we denote for any $x \in G$,

$$\nu(x) = |\{(a, b) : \ a \in A, \ b \in B, \ a + b = x\}|,$$

the *number of representations function*. When the context will not make it obvious, we may denote $\nu_{A,B}$ instead of simply ν. Notice that if $|A| + |B| > |G| + L(G)$, then for any $x \in G$ we have

$$\nu(x) = |A \cap (x - B)| = |A| + |x - B| - |A \cup (x - B)| \geq |A| + |B| - |G| > L(G),$$

whence $A \wedge B = G$.

Finally, for a set $A \subset G$ and $t \in \mathbb{Z}$, we shall denote

$$t \cdot A = \{ta : a \in A\},$$

and $-A = (-1) \cdot A$. We define the *half* of a set $T \subset G$ as $\mathcal{H}(T) = \{g \in G : \ 2g \in T\}$ and the *subgroup of doubles* in G as

$$2 \cdot G = \{2x : \ x \in G\}.$$

Notice that $|2 \cdot G| = |G|/L(G)$.

In a recent paper, Guo [7] studied the problem of restricted sumsets in Abelian groups in the case when the cardinality of the sets is large and proved the following result.

Theorem C (Guo)**.** *Let A and B be subsets of a finite Abelian group G satisfying $|A| + |B| = |G| + L(G)$. Then $|A \wedge B| \geq |G| - 2$.*

In the same paper [7], Guo also gave a complete description of the pairs of subsets (A, B) such that $|A| + |B| = |G| + L(G)$ and $|A \wedge B| = |G| - 2$. This is the content of the next theorem.

Theorem D (Guo)**.** *Let A and B be subsets of a finite Abelian group G. Then, $|A|+|B| = |G|+L(G)$ and $|A \wedge B| = |G| - 2$ if and only if there exist two distinct elements $a, b \in A \cap B$ satisfying*

(i) *the order d of the subgroup $H = \langle 2(b - a)\rangle$ is an odd integer greater than 1;*
(ii) *there exist distinct elements $x_1, \ldots, x_k, x_{k+1}, \ldots, x_l, x_{l+1}, \ldots, x_m$ in $G \setminus (G_0 + H)$, where*

$$m = \frac{|G|/d - |G_0|}{2}$$

and $0 \leq k, l \leq m$, such that

$$G \setminus (G_0 + H) = \bigcup_{i=1}^{m} ((a + x_i + H) \cup (a - x_i + H)),$$
$$A = a + ((\{0, b - a, 3(b - a), \ldots, (d - 2)(b - a)\} + G_0) \cup (\{x_1, \ldots, x_k, \pm x_{k+1}, \ldots, \pm x_l\} + H)),$$
$$B = a + ((\{0, b - a, 3(b - a), \ldots, (d - 2)(b - a)\} + G_0) \cup (\{x_1, \ldots, x_k, \pm x_{l+1}, \ldots, \pm x_m\} + H)).$$

We want to point out that, as it was proved in [7], if two sets A and B are of the form described in Theorem D, then the two $A \wedge B$*-exceptions* – by which we mean elements of $(A + B) \setminus (A \wedge B)$ – are precisely $2a$ and $2b$.

In this article, we deal with a generalization of restricted sumsets (introduced in [14]) in which a new set appears. Let A, B and S be non-empty subsets of G. The *restricted sumset of A and B with respect to S* is defined by

$$A \wedge^S B = \{a + b : \; a \in A, \; b \in B \text{ and } a - b \notin S\}.$$

Notice that, when $S = \{0\}$, this sumset corresponds to the classical restricted sumset of two sets. Partial results to the problem of estimating $|A \wedge^S B|$ from below are given recently in [8, 12, 13]. In particular, Pan and Sun used the polynomial method to study a conjecture of Lev. As a corollary they proved [13] the following result.

Theorem E (Pan and Sun)**.** *Let G be an Abelian group and let A, B and S be finite non-empty subsets of G such that $A \wedge^S B$ is not empty.*

(i) *If G is torsion-free or elementary Abelian, then*

$$|A \wedge^S B| \geq |A| + |B| - |S| - \min_{z \in A \wedge^S B} \nu(z).$$

(ii) *If the torsion part of G is cyclic, then*

$$|A \wedge^S B| \geq |A| + |B| - 2|S| - \min_{z \in A \wedge^S B} \nu(z).$$

In [8], Guo and Sun used a variation of Tao's method [15] in harmonic analysis to prove the next theorem, which is a generalization of Theorem B.

Theorem F (Guo and Sun)**.** *Let A, B and S be non-empty subsets of the group of prime order p. Then*

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

In this paper, applying techniques similar to those used in [4, 6] and [7], we study the restricted sumset of two large sets A and B with respect to a set S, in general finite Abelian groups. Given non-empty sets A, B and S, we first introduce a generalization of the doubling constant $L(G)$ which depends on the set S, that we denote L_S. It is easy to see that if $|A| + |B| > |G| + L_S$ then $A \wedge^S B = G$ (Lemma 2) and as our first principal result we show that if $|A| + |B| = |G| + L_S$ then $|A \wedge^S B| \geq |G| - 2|S|$ (Theorem 12). We also characterize the triples of sets (A, B, S) such that $|A| + |B| = |G| + L_S$ and $|A \wedge^S B| = |G| - 2|S|$ (Theorems 18 and 23). Moreover, in this case, we also provide the structure of the set $G \setminus (A \wedge^S B)$.

The organization the paper is the following. In Section 2, we introduce the terminology and some preliminary results. The key-point in this section is Lemma 6. Section 3 is devoted to the proof of the lower bound. We also give some examples in order to show that our bound is tight. In Section 4, we characterize the critical sets in the important special case $L_S = |S| \; L(G)$. In particular, this gives the characterization the critical sets for Abelian groups of odd order. Finally, in Section 5, we extend the characterization to the case $L_S < |S| \; L(G)$, provided some restriction holds.

2. Terminology and preliminaries

We first start with two basic results. The first one was baptised Prehistorical lemma by the first-named author.

Lemma G (Folkloric prehistorical lemma)**.** *Let A and B be subsets of a finite group G. If $|A|+|B| > |G|$ then $A + B = G$.*

The second result we shall need is Kneser's Theorem [9], see also [11]. It has a lot of applications in additive and combinatorial number theory. We will use it as a key-tool in the characterization of critical sets in groups of even order.

Theorem H (Kneser)**.** *Let G be an Abelian group and let A and B be finite, non-empty subsets of G. Let $H = H(A+B) = \{g \in G : \ g + A + B = A + B\}$ be the stabilizer of $A+B$. If $|A+B| < |A| + |B|$ then $|A+B| = |A+H| + |B+H| - |H|$.*

Given $z \in G$ and a non-empty subset $S \subset G$, we define

$$L_S(z) = |\{(x,y) : \ x, y \in G, \ x+y = z \text{ and } x - y \in S\}|$$

and

$$L_S = \max_{z \in G} L_S(z).$$

The mean-value of $L_S(z)$ on G is easy to compute since

$$\begin{aligned} \frac{1}{|G|} \sum_{z \in G} L_S(z) &= \frac{1}{|G|} \sum_{z \in G} |\{(x,y) : \ x,y \in G, \ x+y = z \text{ and } x-y \in S\}| \\ &= \frac{1}{|G|} |\{(x,y) : \ x,y \in G, \text{ such that } \ x-y \in S\}| \\ &= \frac{1}{|G|} \ |S||G| = |S|. \end{aligned}$$

Therefore, we must have $L_S \geq |S| \geq 1$.

The next lemma will be useful for further reference. Notice that $L_S(z) = |\{y : \ z - 2y \in S\}|$.

Lemma 1. *Let S be a finite non-empty subset of an Abelian group G and let $z \in G$. Then*

(i) *We have*
$$L_S(z) = |S \cap (z + 2 \cdot G)| \ L(G).$$
(ii) *In particular, $L_S(z)$ is a multiple of $L(G)$, less than or equal to $|S|L(G)$.*
(iii) *In particular, $L_S(0) = |S \cap 2 \cdot G| \ L(G)$.*
(iv) *In particular,*
$$L_S = m \ L(G),$$
for some integer m satisfying $1 \leq m \leq |S|$.
(v) *If $L_S = |S| \ L(G)$, then S is included in a coset modulo $2 \cdot G$.*
(vi) *If $L_S(0) = L_S = |S| \ L(G)$, then S is included in $2 \cdot G$.*

The next result can be thought as a generalization of Lemma G:

Lemma 2. *Let A, B and S be non-empty subsets of a finite Abelian group G. If $|A|+|B| > |G|+L_S$ then $A \wedge^S B = G$.*

Proof. For any $z \in G$ we have

$$\nu(z) = |A \cap (z - B)| = |A| + |z - B| - |A \cup (z - B)| \geq |A| + |B| - |G| > L_S.$$

Thus, by definition of L_S, one at least among the $\nu(z)$ pairs $(a,b) \in A \times B$ such that $z = a + b$ must satisfy $a - b \notin S$. Therefore $z \in A \wedge^S B$. □

Similarly, we obtain the following:

Lemma 3. *Let A, B and S be non-empty subsets of a finite Abelian group G and assume that $|A| + |B| = |G| + L_S$, in particular $A + B = G$. Then*

(i) *For each $z \in G$, $\nu(z) \geq L_S$.*
(ii) *If $z \notin A \wedge^S B$ then $\nu(z) = L_S(z) = L_S$. That is, there are exactly L_S pairs $(a,b) \in A \times B$ such that $z = a + b$. Moreover, for each sum $z = a + b$ with $a \in A$ and $b \in B$ we have $a - b \in S$.*

Proof. For any $z \in G$ we have $\nu(z) = |A \cap (z-B)| = |A|+|z-B|-|A\cup(z-B)| \geq |A|+|B|-|G| = L_S$. This proves (i).

For the proof of (ii), by definition, if $z = a+b$ with $a \in A$ and $b \in B$ then $a-b \in S$. Thus, $\nu(z) \leq L_S(z) \leq L_S$. Hence, by (i), we must have $\nu(z) = L_S(z) = L_S$. □

Generalizing an earlier notation, we say that z is an $A \wedge^S B$*-exception* if $z \in (A+B) \setminus (A \wedge^S B)$.

A useful reduction is given by the following lemma.

Lemma 4. *Let A, B and S be non-empty subsets of a given Abelian group G. Let z be an $A \wedge^S B$-exception.*

(i) *There exist $s \in S$ and $b \in (A-s) \cap B$ such that $z = 2b+s$.*
(ii) *For any $s \in S$ and $b \in (A-s)\cap B$ with $z = 2b+s$, letting $A' = A-b-s$, $B' = B-b$ and $S' = S-s$, we have*
  (a) $0 \in A' \cap B' \cap S'$,
  (b) $A' \wedge^{S'} B' = A \wedge^S B - (2b+s)$, *and*
  (c) 0 *is an* $A' \wedge^{S'} B'$*-exception.*
(iii) *If $|A|+|B| = |G|+L_S$ then*

$$\nu_{A',B'}(0) = L_{S'}(0) = L_{S'} = L_S.$$

(iv) *If $|A|+|B| = |G|+L_S$ and $L_S = |S|\ L(G)$ both hold, then (i), (ii) and (iii) are valid for any $s \in S$.*

Proof. Since z is in $A+B$, it can be written $a+b$ for some $a \in A$ and $b \in B$. But, being an $A \wedge^S B$-exception, we must have $a-b \in S$, say $a-b = s$, for an $s \in S$. It follows that $b \in A-s$ and $z = a+b = 2b+s$. This proves (i).

To prove (ii), one first observes that $A' = A-a$ and thus (a) is immediate. Assertion (b) follows from

$$\begin{aligned} A' \wedge^{S'} B' &= \{a'+b' : a' \in A',\ b' \in B' \text{ and } a'-b' \notin S'\} \\ &= \{(\alpha-a)+(\beta-b) :\ \alpha \in A,\ \beta \in B \text{ and } (\alpha-a)-(\beta-b) \notin S-s\} \\ &= \{\alpha+\beta-(a+b) :\ \alpha \in A,\ \beta \in B \text{ and } \alpha-\beta \notin S\} \\ &= A \wedge^S B - (a+b) \\ &= A \wedge^S B - (2b+s). \end{aligned}$$

Finally (c) follows from the fact that if 0 (which belongs to $A'+B'$) was not an $A' \wedge^{S'} B'$-exception, then $0 = a'+b'$ with $a' \in A'$, $b' \in B'$ and $a'-b' \notin S'$ from which we would derive that z is not an $A \wedge^S B$-exception, a contradiction.

Point (iii) is an immediate consequence of Lemma 3 (ii) applied to the sets A', B' and S' and the $A' \wedge^{S'} B'$-exception $z = 0$, on recalling that $|A'| = |A|$, $|B'| = |B|$, $|S'| = |S|$ and $L_{S'} = L_S$.

For the proof of (iv), let us write $k = |S|$, $S = \{s_1, \ldots, s_k\}$ and consider z an $A \wedge^S B$-exception. By Lemma 3 (ii) again, we know that there are exactly L_S pairs $(a,b) \in A \times B$ such that $z = a+b$ and, for each such sum, we have $a-b \in S$ or, equivalently $a-b = s_i$ for some i in $\{1,\ldots,k\}$. But for each $1 \leq i \leq k$, there are at most $L(G)$ solutions to the system $a+b = z,\ a-b = s_i$, since it is equivalent to the equation $z = 2b+s_i$. Since $L_S = |S|\ L(G)$, the only possibility is that for all i in $\{1,\ldots,k\}$, there are exactly $L(G)$ corresponding solutions. In particular, this implies that there is at least one solution $(a,b) \in A \times B$ to $a+b = z$ and $a-b = s_i$, for each $i \in \{1,\ldots,k\}$. □

Corollary 5. *Let A, B and S be non-empty subsets of a given Abelian group G. We assume that $0 \in S$ and that both equalities $|A|+|B| = |G|+L_S$ and $L_S = |S|\ L(G)$ hold, then*

$$G \setminus (A \wedge^S B) \subset 2 \cdot (A \cap B).$$

Proof. This follows from (iv) in the preceding lemma: one may therefore apply (i) with any prechosen element s in S. Selecting $s = 0$, it follows that any $A \wedge^S B$-exception z can be written $2b$ for some $b \in A \cap B$. □

The next lemma is a technical result which will be central to give a lower bound for $|A \wedge^S B|$.

We shall use the standard notation

$$S\Delta - S = (S \setminus -S) \cup (-S \setminus S)$$

for any set S of G. Notice that

$$(S \cap -S) \cup (S\Delta - S) = (S \cap -S) \cup (S \setminus -S) \cup (-S \setminus S)$$

is a partition of $S \cup -S$.

Lemma 6. *Suppose that A, B and S are subsets of a finite Abelian group such that $|A| + |B| = |G| + L_S$, $L_S = |S|\ L(G)$ and $0 \in A \cap B \cap S$. If $b \in A \cap B$ and $0, 2b \notin A \wedge^S B$, then for any $x \in G$ we have*

$$|A \cap \{b - x, b + x\}| + |B \cap \{b - x, b + x\}| = \begin{cases} 2 & \text{if } 2x \notin S \cup -S, \\ 3 & \text{if } 2x \in S\Delta - S, \\ 4 & \text{if } 2x \in S \cap -S,\ 2x \neq 0 \\ 2 & \text{if } 2x = 0 \end{cases}$$

Proof. We shall denote by LHS(x) and RHS(x), respectively, the left-hand side and the right-hand side of the equality to prove. From $2b \notin A \wedge^S B$ we easily get LHS$(x) \le$ RHS(x), for any $x \in G$. On the other hand, if $\sum_x^*$ denotes the summation over all elements $x \in G$, with every value x with $2x = 0$ attained twice, then

$$\sum_x{}^* \mathrm{LHS}(x) = 2|A| + 2|B|.$$

Furthermore, by Lemma 1 (vi) we have $S \cup (-S) \subset 2 \cdot G$, implying:

$$\begin{aligned} \sum_x{}^* \mathrm{RHS}(x) &= 2|G| + |\{x \in G :\ 2x \in S\Delta - S\}| + 2|\{x \in G :\ 2x \in S \cap -S\}| \\ &= 2|G| + |\{x \in G :\ 2x \in S \cup -S\}| + |\{x \in G :\ 2x \in S \cap -S\}| \\ &= 2|G| + |S \cup -S|L(G) + |S \cap -S|L(G) \\ &= 2|G| + 2|S|L(G) \\ &= 2|G| + 2L_S \\ &= 2|A| + 2|B|. \end{aligned}$$

□

From Lemma 6 we derive the following corollary.

Corollary 7. *Suppose that A, B and S are subsets of a finite Abelian group G such that $|A| + |B| = |G| + L_S$, $L_S = |S|\ L(G)$, and $0 \in A \cap B \cap S$. If $b \in A \cap B$ and $0, 2b \notin A \wedge^S B$, then there exist partitions*

$$G \setminus \mathcal{H}(S \cup -S) = X_0 \cup -X_0 \cup X_1 \cup -X_1 \cup X_2 \cup -X_2$$

and

$$\mathcal{H}(S\Delta - S) = Y_1 \cup -Y_1 \cup Y_2 \cup -Y_2$$

such that

$$\begin{aligned} A - b &= \mathcal{H}(S \cap -S) \cup X_0 \cup X_1 \cup -X_1 \cup Y_1 \cup -Y_1 \cup Y_2, \\ B - b &= \mathcal{H}(S \cap -S) \cup X_0 \cup X_2 \cup -X_2 \cup Y_1 \cup Y_2 \cup -Y_2. \end{aligned}$$

3. The lower bound

We start this section with a lemma that contains the central part of the main result.

Lemma 8. *Let A, B and S be subsets, containing 0, of a finite Abelian group G. Assume that $|A| + |B| = |G| + L_S$, that 0 is an $A \wedge^S B$-exception and that $L_S = |S|\ L(G)$. Let z be an $A \wedge^S B$-exception not contained in $S \cup -S$.*

(i) *If z' is another $A \wedge^S B$-exception, then we have $z' - z \in A \cap B$,*
(ii) *Moreover, if $z' \notin S \cup -S$ then $z' - z \in S \cap -S$.*

Proof. By Corollary 5, we may assume that $z = 2b$ and $z' = 2b'$ for some $b, b' \in A \cap B$.

Clearly $2b \notin A \cup B$, otherwise since $0 \in A \cap B$ and $2b$ is an $A \wedge^S B$-exception, we would have that either $2b \in S$ or $-2b \in S$ that is, $2b \in S \cup -S$, a contradiction. Defining $r = 2b - b'$, this can be reformulated as $b' + r \notin A \cup B$. Therefore, since $2b'$ is an $A \wedge^S B$-exception, by Lemma 6, we must have $b' - r \in A \cap B$, or equivalently $2b' - 2b \in A \cap B$. This proves (i).

Suppose now that $2b' \notin S \cup -S$. By symmetry, applying what we just proved, we also have $2b - 2b' \in A \cap B$.

But then, using the fact that 0 is an $A \wedge^S B$-exception, the equalities (giving two representations of 0 as an element of $A + B$)

$$(2b - 2b') + (2b' - 2b) = (2b' - 2b) + (2b - 2b') = 0$$

imply that both $4b - 4b'$ and $4b' - 4b$ are in S, that is $2(2b' - 2b) \in S \cap -S$.

Now, Lemma 6 implies that $2b' - b = b + (2b' - 2b) \in A \cap B$. Using this and $b \in B$, we deduce from $2b' = (2b' - b) + b \in A + B$ and the fact that $2b'$ is an $A \wedge^S B$-exception, that $2b' - 2b = (2b' - b) - b \in S$. By symmetry, $2b - 2b' \in S$, therefore $2b' - 2b \in S \cap -S$, which proves assertion (ii). □

Corollary 9. *Let A, B and S be subsets, containing 0, of a finite Abelian group G. Assume that $|A| + |B| = |G| + L_S$, that 0 is an $A \wedge^S B$-exception and that $L_S = |S|\ L(G)$. Then, for any $A \wedge^S B$-exception z not contained in $S \cup -S$, we have*

$$G \setminus (A \wedge^S B) \subset S \cup -S \cup (z + S \cap -S).$$

In the special case $S = -S$, we obtain $G \setminus (A \wedge^S B) \subset S \cup (z + S)$.

Proof. Since, by assumption, z is not in $S \cup -S$, we may then apply the preceding lemma. Consider another $A \wedge^S B$-exception z'. By Lemma 8 (ii), it is either in $S \cup -S$, or in $z + S \cap -S$. □

The next theorem gives us the lower bound for restricted sumsets with respect to a set S, in the case $L_S = |S|\ L(G)$. It is a direct application of Lemma 8.

Theorem 10. *Let A, B and S be non-empty subsets of a finite Abelian group G. If $|A| + |B| = |G| + L_S$ and $L_S = |S|\ L(G)$, then*

$$|A \wedge^S B| \geq |G| - 2|S|.$$

Proof. Since $L_S \geq 1$, Lemma G implies that $A + B = G$. Assume that the set of exceptions $G \setminus (A \wedge^S B)$ is not empty, otherwise there is nothing to prove. Let z be an $A \wedge^S B$-exception.

Lemma 4 gives the existence of $s \in S$ and $b \in (A - s) \cap B$ such that $z = 2b + s$ and if we put $A' = A - b - s$, $B' = B - b$ and $S' = S - s$, we have that $|A'| + |B'| = |G| + L_S$, $0 \in A' \cap B' \cap S'$, 0 is an $A' \wedge^{S'} B'$-exception and that $L_S = L_{S'} = L_{S'}(0)$.

If there is no $A' \wedge^{S'} B'$-exception outside $S' \cup -S'$, then

$$|G \setminus (A \wedge^S B)| = |G \setminus (A' \wedge^{S'} B')| \leq |S' \cup -S'| \leq 2|S'| = 2|S|$$

and thus the result holds.

Suppose now that there is at least one $A' \wedge^{S'} B'$-exception outside $S' \cup -S'$. By applying Corollary 9, we obtain

$$\begin{aligned} |G \setminus (A \wedge^S B)| &= |G \setminus (A' \wedge^{S'} B')| \\ &\leq |S' \cup -S'| + |S' \cap -S'| \\ &= 2|S'| \\ &= 2|S| \end{aligned}$$

which proves the theorem. □

We introduce another lemma.

Lemma 11. *Let A, B and S be subsets, containing 0, of a finite Abelian group G. Assume that $|A| + |B| = |G| + L_S$ and that 0 is an $A \wedge^S B$-exception. Let $\Sigma = S \cap 2 \cdot G$. Then*

(i) $L_S = |\Sigma|\ L(G) = L_\Sigma(0) = L_\Sigma$,
(ii) $|A \wedge^\Sigma B| \geq |G| - 2|\Sigma|$, *and*
(iii) *the set of $A \wedge^S B$-exceptions can be partitioned as follows:*

$$G \setminus (A \wedge^S B) = (G \setminus (A \wedge^\Sigma B)) \cup (G \setminus (A \wedge^{(S \setminus \Sigma)} B)).$$

Proof. By Lemmas 1 and 3, since 0 is an $A \wedge^S B$-exception, we have that

$$L_S = |\Sigma|\ L(G).$$

By applying Lemma 1 (iii), we check that $L_\Sigma(0) = |\Sigma|\ L(G)$ and by definition of L_Σ and Lemma 1 (iv), we have $L_\Sigma(0) \leq L_\Sigma \leq |\Sigma|\ L(G)$, therefore

$$|\Sigma|\ L(G) = L_\Sigma(0) = L_\Sigma$$

and (i) is proved.

In view of (i), Theorem 10 applied to the sets A, B and Σ implies that

$$|A \wedge^\Sigma B| \geq |G| - 2|\Sigma|,$$

that is (ii).

To prove (iii), first notice that it is immediate that the right-hand side is included in the left-hand side. Let us see now that the other inclusion holds. Assume that z is an $A \wedge^S B$-exception. By Lemma 4 (i), there are $s \in S$ and $b \in (A - s) \cap B$ such that $z = 2b + s$. Assume that there exists a different $s' \in S$ such that $z = 2b' + s'$, where $b' \in (A - s') \cap B$. Thus, we obtain that $s = s' + 2(b' - b) \in s' + 2 \cdot G$. That is, if $s \in 2 \cdot G$ then $s' \in 2 \cdot G$, and viceversa. Hence, $s \in \Sigma$ if and only if, $s' \in \Sigma$. Therefore, if z is an $A \wedge^S B$-exception and there exist $a, a' \in A$ and $b, b' \in B$ such that $z = a + b = a' + b'$ either $a - b, a' - b' \in \Sigma$ or $a - b, a' - b' \in S \setminus \Sigma$. □

We are now ready for our next theorem which is a generalization of Theorem C.

Theorem 12. *Let A, B and S be non-empty subsets of a finite Abelian group G. If $|A| + |B| = |G| + L_S$ then $|A \wedge^S B| \geq |G| - 2|S|$.*

Notice that, for the sake of clarity, (the first step of the induction in) the forthcoming proof relies on Theorem C, but it would be no problem – to be more precise, the very same proof, but in a drastically simplified way – to keep the paper self-contained and prove Theorem 12 without invoking it.

Proof. We shall prove the result by (finite) induction on the cardinality of S.

If $|S| = 1$, then $L_S = L(G)$ and the result holds by Theorem C.

Assume now that the result is proved for any set of cardinality $< \sigma$ for some integer $\sigma \leq |G|$ and let us consider a set S of cardinality σ.

We start by recalling that in the present situation, $A + B = G$. We may also assume that there is at least one $A \wedge^S B$-exception, say z, otherwise $A \wedge^S B = G$ and there is nothing more to prove.

By Lemma 4 (i), we can assume that $z = 2b + s$ for some $s \in S$ and $b \in (A - s) \cap B$. By replacing A, B and S respectively by $A' = A - b - s$, $B' = B - b$ and $S' = S - s$ we have that $0 \in A' \cap B' \cap S'$, 0 is an $A' \wedge^{S'} B'$-exception and that $L_S = L_{S'}(0) = L_{S'}$. Moreover we also have $A' + B' = G$.

We denote $\Sigma = S' \cap 2 \cdot G$ and notice that $0 \in \Sigma$. We distinguish three cases.

If $\Sigma = S'$, then by Lemma 11 (i), we can apply Theorem 10, which gives the result. From now on, assume $\Sigma \neq S'$.

If $A' \wedge^{(S' \setminus \Sigma)} B' = G$ then, by Lemma 11 (iii), we obtain that

$$G \setminus (A' \wedge^{S'} B') = G \setminus (A' \wedge^{\Sigma} B').$$

Lemmas 4 and 11 (ii) now yield

$$|A \wedge^S B| = |A' \wedge^{S'} B'| = |A' \wedge^{\Sigma} B'| \geq |G| - 2|\Sigma| \geq |G| - 2|S'| = |G| - 2|S|,$$

and the result is proved.

Or, there exists an exception $z' \in G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')$. We first check that

$$L_{S' \setminus \Sigma} = L_{S'}. \tag{1}$$

Indeed, by Lemma 11 (iii) z' is an $A' \wedge^{S'} B'$-exception, and by Lemma 3 (ii), $\nu(z') = L_{S'} = L_{S'}(z')$. But, since $z' \notin A' \wedge^{S' \setminus \Sigma} B'$, for any $a \in A'$, $b \in B'$ such that $z' = a + b$, we have $a - b \in S' \setminus \Sigma$. Thus $\nu(z) \leq L_{S' \setminus \Sigma}(z') \leq L_{S' \setminus \Sigma} \leq L_{S'}$ which implies equality (1).

By (1), we have $|A'| + |B'| = |G| + L_{S' \setminus \Sigma}$. Since $0 \in \Sigma \subsetneq S'$, we have $1 \leq |S' \setminus \Sigma| < \sigma = |S'|$, and we may use the induction hypothesis which implies that

$$|G \setminus (A' \wedge^{S' \setminus \Sigma} B')| \leq 2|S' \setminus \Sigma|.$$

Thus, using Lemma 11 (iii) and (ii), we obtain that

$$\begin{aligned} |G \setminus (A \wedge^S B)| &= |G \setminus (A' \wedge^{S'} B')| \\ &= |G \setminus (A' \wedge^{\Sigma} B')| + |G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')| \\ &\leq 2|\Sigma| + 2|S' \setminus \Sigma| \\ &= 2|S'| \\ &= 2|S| \end{aligned}$$

which finishes the induction step and the proof. □

Examples. *From the characterization given in* [7], *we construct the first example. By a slight modification we can then generate the two other examples, which show that the bound of Theorem 12 is tight.*

(1) *Let* $G = \mathbb{Z}/15\mathbb{Z}$, *we have that* $G_0 = 0$. *If* $S = \{0\}$ *then* $L_S = L(G) = 1$. *Let us consider* $H = \langle 5 \rangle$, $A = A_0 \cup (2 + H)$ *and* $B = B_0 \cup (2 + H) \cup (4 + H) \cup (1 + H)$, *where* $A_0 = B_0 = \{0, 5\}$.

In particular, $|A|+|B|=|G|+L_S$. *Then*

$$\nu_{A+B}(u)=\begin{cases}|A_0|+|H|, & \text{if } u\in 1+H;\\ 2|A_0|, & \text{if } u\in 2+H;\\ |H|, & \text{if } u\in 3+H;\\ |A_0|+|H|, & \text{if } u\in 4+H;\end{cases}\qquad \text{and } A_0\wedge^S B_0=\{5\}.$$

Thus, the set of $A\wedge^S B$*-exceptions is* $\{0,10\}$.

(2) *Let* $G=\mathbb{Z}/30\mathbb{Z}$, *we have that* $G_0=\{0,15\}$. *If* $S=\{0,15\}$ *then* $L_S=L(G)$. *Let us consider* $H=\langle 5\rangle$, $A=A_0\cup(2+H)$ *and* $B=B_0\cup(2+H)\cup(4+H)\cup(1+H)$, *where* $A_0=B_0=\{0,5,15,20\}$. *In particular,* $|A|+|B|=|G|+L_S$. *Then* $\nu_{A+B}(u)>L_S$ *for* $u\notin H$ *and*

$$A_0\wedge^S B_0=\{5,20\}.$$

Thus, the set of $A\wedge^S B$*-exceptions is* $\{0,10,15,25\}$.

(3) *Let* $G=\mathbb{Z}/45\mathbb{Z}$, *we have that* $G_0=0$. *If* $S=\{0,15,30\}$ *then* $L_S=3|G_0|$ *(clearly, since* $3|G_0|\geq L_S\geq L_S(0)=3$*). Let us consider* $H=\langle 5\rangle$, $A=A_0\cup(2+H)$ *and* $B=B_0\cup(2+H)\cup(4+H)\cup(1+H)$, *where* $A_0=B_0=\{0,5,15,20,30,35\}$. *In particular,* $|A|+|B|=|G|+L_S$. *Then* $\nu_{A+B}(u)>L_S$ *for* $u\notin H$ *and*

$$A_0\wedge^S B_0=\{5,20,35\}.$$

Thus, the set of $A\wedge^S B$*-exceptions is* $\{0,10,15,25,30,40\}$.

4. The critical sets for Abelian groups. Case $L_S=|S|\ L(G)$.

In what follows, instead of G_0 we will write $K(G)$. That is, $K(G)=\{g\in G:\ 2g=0\}$. We start with a lemma.

Lemma 13. *Let* A,B *and* S *be subsets, containing* 0, *of a finite Abelian group* G. *Assume that* $|A|+|B|=|G|+L_S$, *that* 0 *is an* $A\wedge^S B$*-exception and that* $L_S=|S|\ L(G)$. *Let* z *and* z' *be two* $A\wedge^S B$*-exceptions such that* $z\notin S\cup -S$, $z'\in S\Delta-S$ *and* $z'-z\notin S\cap -S$. *Then,* $2z-2z'\in(S\Delta-S)\cap(A\wedge^S B)$.

Proof. Slightly more precisely, we shall in fact prove that if $\epsilon=-1$ or 1 and $z'\in\epsilon(S\setminus -S)$, then $2z-2z'\in\epsilon(S\setminus -S)\cap(A\wedge^S B)$.

By Corollary 5, we may assume that $z=2b$ and $z'=2b'$ for some $b,b'\in A\cap B$. Recall first that, by Lemma 8, we have

$$z'-z=2b'-2b\in A\cap B. \tag{2}$$

For all this proof, we define $r=2b'-b$.

We first prove that

$$z'\in A\cup B. \tag{3}$$

Indeed, suppose to the contrary that $b+r\notin A\cup B$, therefore since $2b$ is an $A\wedge^S B$-exception, Lemma 6 implies that $b-r=2b-2b'\in A\cap B$. But then, the equalities

$$(2b-2b')+(2b'-2b)=(2b'-2b)+(2b-2b')=0$$

giving two ways to write 0 as an element of $A+B$, by using (2), imply, since 0 is an $A\wedge^S B$-exception, that $4b-4b'$ and $4b'-4b$ are in S, that is $2(2b'-2b)\in S\cap -S$. Thus, by Lemma 6, we obtain $2b'-b=b+(2b'-2b)\in A\cap B$. This implies in turn, in view of the writing of the $A\wedge^S B$-exception $2b'$ as an element of $A+B$ in the form $(2b'-b)+b$, that $2b'-2b\in S$. In a similar fashion, we obtain $2b-2b'\in S$. Therefore, $z-z'\in S\cap -S$. Since this is a contradiction with an assumption of our statement, (3) is proved.

We are now reduced to study two cases.

Case 1: $z' \in A$.

Writing $2b' = 2b' + 0 \in A + B$ and since $2b'$ is an $A \wedge^S B$-exception, we obtain that $2b' \in S$ and thus

$$z' \in S \setminus -S$$

(recall that in all this proof, we assume that $z' \in S\Delta - S$). This implies that

$$b + r = 2b' = z' \notin B,$$

since otherwise it follows from the writing of the $A \wedge^S B$-exception $2b' = 0 + 2b' \in A + B$ that $2b' \in -S$, a contradiction to $2b' \in S \setminus -S$.

By Lemma 6,

$$|A \cap \{b - r, b + r\}| + |B \cap \{b - r\}| = |A \cap \{b - r, b + r\}| + |B \cap \{b - r, b + r\}| \in \{2, 3\}. \tag{4}$$

Note that, $b - r \neq b + r$ since otherwise we would have $b - r = b + r \notin B$ and the left-hand side of the preceding formula would be equal to 1. In particular, by Lemma 6, we obtain that

$$r \notin \mathcal{H}(S \cap -S). \tag{5}$$

We now prove that

$$z - z' \notin B. \tag{6}$$

Indeed if, to the contrary, $2b - 2b' \in B$ then the writing $2b$ as the sum $2b' + (2b - 2b')$ in $A + B$ implies, since $2b$ is an $A \wedge^S B$-exception, that $2r = 4b' - 2b \in S$. In view of (5), we obtain that $2r = s$ for some $s \in S \setminus -S$. By Lemma 6, we derive

$$|A \cap \{b - r, b + r\}| + |B \cap \{b - r, b + r\}| = 3$$

hence, since $b+r \notin B$, we obtain that $2b-2b' = b-r \in A\cap B$. We are now back to the situation of the proof of assertion (3). Proceeding in a similar way, we obtain consecutively that $2z - 2z' \in S \cap -S$, $2b' - b \in A \cap B$, $2b' \in A + B$ and finally $2b' - 2b \in S$. With $2b - 2b' \in S$, which holds by symmetry, the contradiction $z - z' \in S \cap -S$ follows and (6) is proved.

Relation (6) can be rewritten as $b - r = 2b - 2b' \notin B$. Using $b + r \notin B$, we see that the left-hand side of (4) must be equal to 2 and we obtain, by Lemma 6, that

$$2b - 2b' = b - r \in A \setminus B. \tag{7}$$

Thus, using this, (2) and the writing $(2b-2b')+(2b'-2b) = 0$ yields, since 0 is an $A\wedge^S B$-exception,

$$4b - 4b' \in S.$$

Hence, we must have

$$2z - 2z' = 4b - 4b' \in S \setminus -S,$$

otherwise $4b - 4b' \in S \cap -S$, that is $2(2b - 2b') \in S \cap -S$. Therefore, using that 0 is an $A \wedge^S B$-exception, Lemma 6 implies that $2b - 2b' \in A \cap B$, a contradiction with (7).

Note that, in the present case, if $2z - 2z'$ is an $A \wedge^S B$-exception, then by Corollary 5, it is of the form $2b''$ for some $b'' \in A \cap B$. Thus, using Lemma 6, it follows that $2b - 2b' \in b'' + K(G) \subset A \cap B$, a contradiction.

Case 2: $z' \in B$. This case is analogous.

Finally, the study of these two cases implies the result.

□

The next proposition gives more information on the structure of S and the set of $A\wedge^S B$-exceptions when $|A \wedge^S B| = |G| - 2|S|$.

Proposition 14. *Let A, B and S be non-empty subsets of a finite Abelian group G with $|A|+|B| = |G| + L_S$ and $L_S = |S|\ L(G)$. If $|A \wedge^S B| = |G| - 2|S|$ then*

(i) $S - S \subset 2 \cdot G$

Moreover, for any s in S,

(ii) *we have $-(S - s) = S - s$ and*
(iii) *the set of $A \wedge^S B$-exceptions can be partitioned in the form $(z_1 + S) \cup (z_2 + S)$, for some $z_1, z_2 \in G$.*

Proof. Let us choose an arbitrary s in S. Since $A + B = G$, the cardinality condition implies that there are exactly $2|S|$ $A \wedge^S B$-exceptions. Let w be one of them. By Lemma 4 (iv), w can be written as $2b + s$ for some $b \in (A - s) \cap B$. Let $A' = A - b - s$, $B' = B - b$ and $S' = S - s$. By Lemma 4 (iii), $L_S = L_{S'}(0)$ and since we are assuming that $L_S = |S|\ L(G)$, Lemma 1 (vi) implies that $S - s = S' \subset 2 \cdot G$. Taking the union over all possible s implies (i).

In order to prove the equality (ii), notice first that the set of $A' \wedge^{S'} B'$-exceptions cannot be included in $S' \cup -S'$ since in this case its cardinality would be at most $|S' \cup -S'| < 2|S'|$, a contradiction.

Let z be an $A' \wedge^{S'} B'$-exception outside $S' \cup -S'$. By Corollary 9,

$$G \setminus (A' \wedge^{S'} B') \subset S' \cup -S' \cup (z + S' \cap -S').$$

But since the right-hand side has a cardinality at most $|S' \cup -S'| + |S' \cap -S'| = 2|S'|$ we obtain, using the assumption on the cardinality of the set of $A' \wedge^{S'} B'$-exceptions, the equality

$$G \setminus (A' \wedge^{S'} B') = S' \cup -S' \cup (z + S' \cap -S')$$

and that this union is disjoint. It follows that we can partition the set of $A' \wedge^{S'} B'$-exceptions as

$$G \setminus (A' \wedge^{S'} B') = (S' \cap -S') \cup (S' \Delta - S') \cup (z + S' \cap -S'). \tag{8}$$

If $S' \Delta - S'$ is empty then $S' = -S'$ and the result is proved. Otherwise let $z' \in S' \Delta - S'$. By partition (8), it is not in $z + S' \cap -S'$ and we may apply Lemma 13 which implies that $2z - 2z'$ is an element of $S' \Delta - S'$ not in the set of $A' \wedge^{S'} B'$-exceptions, contrarily to the partition (8). This proves (ii).

With (ii), Corollary 9 and the assumption $|G \setminus (A' \wedge^{S'} B')| = 2|S|$ yield

$$G \setminus (A' \wedge^{S'} B') = S' \cup (z + S').$$

Thus

$$G \setminus (A \wedge^S B) = G \setminus (A' \wedge^{S'} B') + w = (S' \cup (z + S')) + w = (2b + S) \cup (2b + z + S),$$

on recalling that $w = 2b + s$. □

The next lemma will be useful.

Lemma 15. *Let G be a finite Abelian group. Let S be a subset of G such that, for each $s \in S$, $S - s = -(S - s)$. Then one of the following happens:*

(i) *S is a coset.*
(ii) *$S - S$ is contained in $K(G)$.*
(iii) *There exists a group $H \leq G$ such that $S = (s_1 + H) \cup (s_2 + H) \cup \ldots \cup (s_k + H)$ and for any $i, j \in \{1, \ldots, k\}$ we have $2(s_i - s_j) \in H$.*

Proof. First, notice that the assumption is equivalent to the fact that for any $s \in S$, $S = -S + 2s$, in other words

$$S = -S + 2 \cdot S. \tag{9}$$

Assume first that $|2 \cdot S| = |S|$. In this case, (9) implies for any $s \in S$, that $-s + 2 \cdot S \subset S$. By the assumption on the cardinalities of these two sets, we then obtain $2 \cdot S = S + s$ and finally $2 \cdot S = 2S$. Choose any s in S and write $S' = S - s$ so that 0 is in S', we get $S' = -S'$ and $2S' = 2 \cdot S' = S'$. Therefore, S' is a subgroup of G and S is a coset.

Suppose now that $|2 \cdot S| < |S|$, in particular $K(G) \neq 0$. The trivial inequality $|S| \leq |2 \cdot S| + |S| - 1$ implies, by Theorem H, that there exists a group H (namely the stabilizer of S) such that

$$|S| = |-S + 2 \cdot S| = |2 \cdot S + H| + |-S + H| - |H| = |2 \cdot S + H| + |S + H| - |H|.$$

In other words, the sum of two non-negative terms $(|2 \cdot S + H| - |H|) + (|S + H| - |S|)$ is equal to 0. Hence, we obtain that $|2 \cdot S + H| = |H|$ and $|S + H| = |S|$, in particular, this means that S is composed of (full) cosets modulo H.

If $H = \{0\}$, then for any $s \in S$, we get $2 \cdot (S - s) = \{0\}$ and thus $S - s \subset K(G)$ which implies $S - S \subset K(G)$.

Suppose now $H \neq \{0\}$. Let $S = (s_1 + H) \cup (s_2 + H) \cup \cdots \cup (s_k + H)$ be the decomposition of S into H-cosets (H-tiling). We have $2 \cdot S = (2s_1 + H) \cup (2s_2 + H) \cup \cdots \cup (2s_k + H)$. Using now $|2 \cdot S + H| = |H|$, we deduce that

$$(2s_1 + H) = (2s_2 + H) = \cdots = (2s_k + H),$$

that is, $2(s_i - s_j) \in H$ for any pair $i, j \in \{1, \ldots, k\}$. □

The next example shows that a set S that verifies the hypothesis of Lemma 15 it is not necessarily a coset.

Example. *Let $G = \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with generators a, b and relations $4a = 2b = 0$. Note that $K(G) = \{0, 2a, b, 2a + b\}$. Let us now consider the set $S = H_0 \cup (a + H_0) \cup (a + b + H_0) = H_0 \cup (a + K(G))$, where $H_0 = \langle 2a \rangle = \{0, 2a\}$. Then we may check that, for each $s \in S$, we have $-(S - s) = S - s$ (or, equivalently, $S = -S + 2 \cdot S$) while S is not a coset.*

We are now ready to study the critical sets S of Theorem 10.

Theorem 16. *Let A, B and S be non-empty subsets of a finite Abelian group G. Assume that $|A| + |B| = |G| + L_S$, where $L_S = |S|\ L(G)$ and that $|A \wedge^S B| = |G| - 2|S|$. Then*

(i) *there exists a subgroup H of $2 \cdot G$ such that S is a coset modulo H, and*
(ii) *$G \setminus (A \wedge^S B)$ is a union of two cosets modulo H.*

Proof. Let z be an $A \wedge^S B$-exception, which exists since $|A \wedge^S B| = |G| - 2|S|$. By Lemma 4, for each $s \in S$ we may find $b \in (A - s) \cap B$ and define the sets $A' = A - b - s$, $B' = B - b$ and $S' = S - s$. In particular, we have that $0 \in A' \cap B' \cap S'$ and $G \setminus (A' \wedge^{S'} B') = G \setminus (A \wedge^S B) - z$.

Assume that we have proved that $S - s$ is a subgroup H of G. Then $H \subset S - S \subset 2 \cdot G$ by Proposition 14 (i). Statement (i) of the Theorem follows. By Proposition 14 (iii), we obtain that the set of $A \wedge^S B$-exceptions can be partitioned into two translates of S, that is, two H-cosets and (ii) is proved.

What remains to be proved is that $S' = S - s$ is a group. Suppose the contrary. By Proposition 14 (ii), we can apply Lemma 15. Two cases may happen.

<u>Case 1</u>. $S - S \subset K(G)$.

Let $s_1', s_2' \in S'$. As shown in the course of the proof of Proposition 14, in the present situation: $S' \subset G \setminus (A' \wedge^{S'} B')$. By Corollary 5, there exists $y \in A' \cap B'$ such that $s_1' = 2y$. Notice that since we have that $S' \subset S - S \subset K(G)$ and $K(G)$ is a group, we have that $s_1' + s_2' \in K(G)$.

Since $2y \in S'$ is an $A' \wedge^{S'} B'$-exception, and $0 \in S' \cap -S'$, Lemma 6 implies $y + K(G) = y + \mathcal{H}(\{0\}) \subset A' \cap B'$. Therefore $y + s_1' + s_2' \in A' \cap B'$. Writing s_2' as the sum $s_2' = (y + s_1' + s_2') + y$ in $A' + B'$, we deduce from the fact that s_2' is an $A' \wedge^{S'} B'$-exception that $s_1' + s_2' = (y + s_1' + s_2') - y \in S'$. This proves $S' + S' \subset S'$.

This and the facts that $0 \in S'$ and S' is finite implies that S' is a subgroup of G, a contradiction.

Case 2. We now suppose that there exists a group J such that $S = (s_1 + J) \cup (s_2 + J) \cup \ldots \cup (s_k + J)$ and for each pair $i, j \in \{1, \ldots, k\}$ we have $2(s_i - s_j) \in J$.

Notice that $J \subset S - s_1 \subset S - S \subset 2 \cdot G$ which shows $J \subset 2 \cdot G$.

Let $\pi : G \to G/J$. We first prove that

$$|\pi(A')| + |\pi(B')| = |G/J| + L_{\pi(S')}, \quad L_{\pi(S')} = |\pi(S')|\ L(G/J) \quad \text{and} \quad \pi(S') \subset K(G/J). \tag{10}$$

Indeed, since by Proposition 14 (iii) the set of $A \wedge^S B$-exceptions can be partitioned into two translates of S and since S is a union of J-cosets, the equality $|A \wedge^S B| = |G| - 2|S|$ implies that

$$|\pi(A') \wedge^{\pi(S')} \pi(B')| = |G/J| - 2|\pi(S')|.$$

Thus, by Lemma 2 and Lemma 1 (iv), we obtain that:

$$|\pi(A')| + |\pi(B')| \leq |G/J| + L_{\pi(S')} \leq |G/J| + |\pi(S')||K(G/J)|. \tag{11}$$

Let us see now that $|K(G/J)| = L(G)$. Since J is a subgroup of $2 \cdot G$, the set $Y = \{y \in G : \ 2y \in J\}$ itself is a group. Moreover, we have that $Y + K(G) = Y$ and $Y + J = Y$ and we obtain that $|K(G/J)| = |Y/J| = L(G)$. Hence, we should have $|\pi(A')| + |\pi(B')| = |G/J| + |\pi(S')||K(G/J)|$, otherwise, using (11), we derive the inequalities

$$|G| + |S'|\ L(G) = |J|(|G/J| + |\pi(S')||K(G/J)|) > |J|(|\pi(A')| + |\pi(B')|) \geq |A'| + |B'|,$$

which gives us a contradiction with $|A| + |B| = |G| + |S|\ L(G)$. Clearly, the inclusion $\pi(S') \subset K(G/J)$ holds. This proves (10).

Notice that, from (10) we also conclude that $\pi(S') - \pi(S') \subset K(G/J)$. Therefore, by the same reasoning as in Case 1, applied to $\pi(A'), \pi(B')$ and $\pi(S')$, we obtain that $\pi(S')$ is a subgroup in G/J. Which implies, since S' is union of cosets modulo J, that S' is a subgroup of G, a contradiction. □

Theorem 17. *Let A, B and S be non-empty subsets of a finite Abelian group G with $|A| + |B| = |G| + L_S$ and $L_S = |S|\ L(G)$. Let $2b_s + s$ be an $A \wedge^S B$-exception, with $s \in S$, $b_s \in (A - s) \cap B$. Then, the following assertions are equivalent*

(i) $|A \wedge^S B| = |G| - 2|S|$.

(ii) (a) *the set $\Sigma = S - s$ is a subgroup of $2 \cdot G$,*

(b) *if $\pi : G \to G/\Sigma$ denotes the natural projection, $A' = \pi(A - b_s - s)$, $B' = \pi(B - b_s)$,*

$$|A'| + |B'| = |G/\Sigma| + L(G/\Sigma) \text{ and } |A' \wedge B'| = |G/\Sigma| - 2.$$

Proof. Suppose first that the equality $|A \wedge^S B| = |G| - 2|S|$ holds. By Theorem 16, Σ is a subgroup of $2 \cdot G$ and the set of $A \wedge^S B$-exceptions is a union of two cosets modulo Σ. Hence, since $A \wedge^S B - (2b_s + s) = (A - b_s - s) \wedge^\Sigma (B - b_s)$, we have that $|A' \wedge B'| = |G/\Sigma| - 2$. This implies, by Lemma 2, in case $S = \{0\}$, that $|A'| + |B'| \leq |G/\Sigma| + L(G/\Sigma)$.

Let us see now that $L(G/\Sigma) = L(G)$. Since Σ is a subgroup of $2\cdot G$, the set $Y = \{y \in G : \; 2y \in \Sigma\}$ itself is a group. Moreover, we have that $Y + K(G) = Y$ and $Y + \Sigma = Y$. Thus we obtain that $L(G/\Sigma) = |Y/\Sigma| = L(G)$. Hence, we should have $|A'| + |B'| = |G/\Sigma| + L(G/\Sigma)$, otherwise

$$|G| + |S| \; L(G) = |S|(|G/\Sigma| + L(G/\Sigma)) > |S|(|A'| + |B'|) \geq |A| + |B|,$$

a contradiction with $|A| + |B| = |G| + |S| \; L(G)$. Note that, we also conclude that A and B are unions of cosets modulo Σ.

For the converse statement, assume that Σ is a subgroup of $2\cdot G$ and that the equalities $|A'|+|B'| = |G/\Sigma| + L(G/\Sigma)$ and $|A' \wedge B'| = |G/\Sigma| - 2$ hold. The condition $|A| + |B| = |G| + L_S$, with $L_S = |S| \; L(G)$ implies that A and B are unions of cosets modulo Σ, since, as it is easy to check, $L(G/\Sigma) = L(G)$. Hence, the set of $A' \wedge B'$-exceptions is a union of two cosets modulo Σ. Therefore, we have $|A \wedge^S B| = |G| - 2|S|$. □

From the previous result together with Theorem D (in case $a = 0$) we obtain the characterization of the critical sets A, B and S of Theorem 10.

Theorem 18. *Let A, B and S be non-empty subsets of a finite Abelian group G with $|A| + |B| = |G| + L_S$ and $L_S = |S| \; L(G)$. Let $2b_s + s$ be an $A \wedge^S B$-exception with $s \in S$ and $b_s \in (A - s) \cap B$. Then, the equality $|A \wedge^S B| = |G| - 2|S|$ holds, if and only if the following conditions hold true:*

(i) *$\Sigma = S - s$ is a subgroup.*

Let $\pi : G \to G/\Sigma$ be the natural projection and let $A' = \pi(A - b_s - s)$ and $B' = \pi(B - b_s)$.

(ii) *There exists $b \in A' \cap B'$ such that $H = \langle 2b \rangle$ is a subgroup in G/Σ of odd order d greater than 1.*
(iii) *There exists $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_l, x_{l+1}, \ldots, x_m\} \subset (G/\Sigma) \setminus (K(G/\Sigma) + H)$, where $m = (|G/\Sigma|/d - L(G/\Sigma))/2$ and $0 \leq k, l \leq m$, such that*

$$(G/\Sigma) \setminus (K(G/\Sigma) + H) = \bigcup_{i=1}^{m} ((x_i + H) \cup (-x_i + H)),$$
$$A' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/\Sigma) \cup (\{x_1, \ldots, x_k, \pm x_{k+1}, \ldots, \pm x_l\} + H),$$
$$B' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/\Sigma) \cup (\{x_1, \ldots, x_k, \pm x_{l+1}, \ldots, \pm x_m\} + H),$$

(iv) *And $A = b_s + s + \pi^{-1}(A')$ and $B = b_s + \pi^{-1}(B')$.*

Note that, under the assumptions of the previous theorem, we can determine the set of $A \wedge^S B$-exceptions. Let $Y = \{y \in G : \; 2y \in \Sigma\}$ then $\pi^{-1}(K(G/\Sigma)) = Y$ and the set $G \setminus (A \wedge^S B) = (2b_s + S) \cup (2b^* + 2b_s + S)$, where $b^* \in G$ and $\pi(b^*) = b$.

5. The critical sets for Abelian groups. Case $L_S < |S| \; L(G)$.

As an immediate consequence of Theorem 12, we obtain the following result.

Theorem 19. *Let A, B and S be non-empty subsets of a finite Abelian group G with $|A|+|B| = |G| + L_S$. If the equality $|A \wedge^S B| = |G| - 2|S|$ holds then there exists a decomposition $S = S_1 \cup S_2 \cup \ldots \cup S_k$ of S modulo $2 \cdot G$ such that*

(i) *$|S_i| = L_S/L(G)$ for each $i \in \{1, 2, \ldots, k\}$,*
(ii) *$|A \wedge^{S_i} B| = |G| - 2|S_i|$ and $|A \wedge^{(S \setminus S_i)} B| = |G| - 2|S \setminus S_i|$ for each $i \in \{1, 2, \ldots, k\}$. Moreover, the set of $A \wedge^S B$-exceptions can be partitioned in the form:*

$$G \setminus (A \wedge^S B) = \cup_{i=1}^{k} (G \setminus (A \wedge^{S_i} B)).$$

Proof. Let $L_S = mL(G)$, for some $m \leq |S|$. We will prove the result by induction on $|S|$. We have $A + B = G$. Let z be an $A \wedge^S B$-exception. We write $z = 2b + s$ for some $s \in S$ and $b \in (A - s) \cap B$ and define $A' = A - b - s$, $B' = B - b$ and $S' = S - s$. Again, $0 \in A' \cap B' \cap S'$, $G \setminus (A \wedge^S B) - (2b + s) = G \setminus (A' \wedge^{S'} B')$ (in particular, 0 is an $A' \wedge^{S'} B'$-exception), $L_S = L_{S'}(0) = L_{S'}$ and $A' + B' = G$.

We denote $\Sigma = S' \cap 2 \cdot G$. Notice that $0 \in \Sigma$, and also by Lemma 11 (i) that $m = |\Sigma|$. If $|S'| = m$ then the result holds with $k = 1$. Suppose now that $|S'| > m$.

By Lemma 11 (iii), we obtain that the set of $A' \wedge^{S'} B'$-exceptions can be partitioned as follows

$$G \setminus (A' \wedge^{S'} B') \quad = \quad (G \setminus (A' \wedge^{\Sigma} B')) \cup (G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')) \tag{12}$$

Now, using Lemma 11 (ii), we have that $|G \setminus (A' \wedge^{\Sigma} B')| \leq 2|\Sigma|$. In particular, since $|S'| > |\Sigma|$, there exists and exception $z' \in G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')$. Thus, (1) is still valid and we have $L_{S' \setminus \Sigma} = L_S$, hence $|A'| + |B'| = |G| + L_{S' \setminus \Sigma}$. By Theorem 12, we obtain that $|G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')| \leq 2|S' \setminus \Sigma|$. Therefore, using $|G \setminus (A \wedge^S B)| = 2|S|$ and the partition (12), we conclude that $|G \setminus (A' \wedge^{\Sigma} B')| = 2|\Sigma|$ and $|G \setminus (A' \wedge^{(S' \setminus \Sigma)} B')| = 2|S' \setminus \Sigma|$.

The inductive process applied to $S' \setminus \Sigma$ completes the result.

□

We now introduce some results that allow us to be more precise about the structure of the sets S and $G \setminus (A \wedge^S B)$ in the case $L_S < |S|\ L(G)$, provided some restriction holds.

Proposition 20. *Let A and B be subsets of a finite Abelian group G. Suppose that there exists an element $b \in A \cap B$ such that:*

(i) *The order d of the subgroup $H = \langle 2b \rangle$ is an odd integer greater than $2L(G) - 1$.*
(ii) *There exists a subset $\{x_1, \dots, x_k, x_{k+1}, \dots, x_l, x_{l+1}, \dots, x_m\} \subset G \setminus (K(G) + H)$, where $m = (|G|/d - |K(G)|)/2$ and $0 \leq k, l \leq m$, such that*

$$G \setminus (K(G) + H) = \bigcup_{i=1}^{m} ((x_i + H) \cup (-x_i + H)),$$
$$A = (\{0, b, 3b, \dots, (d-2)b\} + K(G)) \cup (\{x_1, \dots, x_k, \pm x_{k+1}, \dots, \pm x_l\} + H),$$
$$B = (\{0, b, 3b, \dots, (d-2)b)\} + K(G)) \cup (\{x_1, \dots, x_k, \pm x_{l+1}, \dots, \pm x_m\} + H).$$

Then, for each $z \in G \setminus (K(G) \cup (2b + K(G)))$ we have $\nu(z) > L(G)$. In particular, if $\nu(z) = L(G)$ then $z \in K(G) \cup (2b + K(G))$.

Proof. Let P, Q and R be the subsets defined as follows:

$$P \quad = \quad \{0, b, 3b, \dots, (d-2)b\} + K(G),$$
$$Q \quad = \quad \{x_1, \dots, x_k, \pm x_{k+1}, \dots, \pm x_l\} + H,$$
$$R \quad = \quad \{x_1, \dots, x_k, \pm x_{l+1}, \dots, \pm x_m\} + H.$$

Then $A = P \cup Q$, $B = P \cup R$ and $A + B = (P + P) \cup (P + R) \cup (P + Q) \cup (Q + R)$. Notice that, since $|H| = d$ is odd, we can prove that $|H + K(G)| = dL(G)$ and thus $|A| + |B| = |G| + L(G)$ (see [7]). In particular, $A + B = G$. Let us see now how $\nu(z)$ is lower bounded according to which part of the sum it belongs to.

For the sum $P + P$, clearly, $P + P \subset K(G) + H$ and since d is odd, we have that $db + K(G) = K(G)$. Thus, by a direct computation, it follows that $\nu(z) > L(G)$ unless $z \in K(G) \cup (2b + K(G))$.

Concerning the sum $P + R$, we have that $P + R \subset G \setminus (K(G) + H)$. Since $\{0, b, 3b, \dots, (d-2)b\} \subset H$, it is clear that $P + R$ is a union of $(H + K(G))$-cosets. Moreover, for each $z \in P + R$ we have

$\nu(z) \geq (d+1)/2$. Hence, since we are assuming that $(d+1)/2 > L(G)$, we conclude that $\nu(z) > L(G)$, for each $z \in P+R$.

The case of the sum $P+Q$ is similar to the previous one. (Here we have that $P+Q \subset G \setminus (K(G)+H)$).

Finally, it follows that $Q+R$ is a union of H cosets, none of which is H, hence $0, 2b \notin Q+R$. Moreover, for each $z \in Q+R$, $\nu(z) \geq |H| > L(G)$. □

With the notation and assumptions of the preceding proposition, we can state the following two corollaries:

Corollary 21. *Let $z \in G$. If $\nu(z) = L(G)$ then $z \in (K(G) \cup (2b + K(G))) \setminus (Q+R)$.*

Corollary 22. *Let A, B be non-empty subsets of a finite Abelian group G and T be a subgroup of $2 \cdot G$ such that $|A|+|B| = |G|+|T|\ L(G)$. Let $\pi : G \to G/T$ be the natural projection. Denote $A' = \pi(A)$ and $B' = \pi(B)$. Suppose that*

(i) *there exists $b \in A' \cap B'$ such that $H = \langle 2b \rangle$ is a subgroup in G/T of odd order d greater than $2L(G/T) - 1$,*
(ii) *there exists $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_l, x_{l+1}, \ldots, x_m\} \subset (G/T) \setminus (K(G/T)+H)$, where $m = (|G/T|/d - L(G/T))/2$ and $0 \leq k, l \leq m$, such that*

$$(G/T) \setminus (K(G/T)+H) = \bigcup_{i=1}^{m} ((x_i + H) \cup (-x_i + H)),$$
$$A' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/T) \cup (\{x_1, \ldots, x_k, \pm x_{k+1}, \ldots, \pm x_l\} + H),$$
$$B' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/T) \cup (\{x_1, \ldots, x_k, \pm x_{l+1}, \ldots, \pm x_m\} + H).$$

Then, for each $z \in G \setminus \pi^{-1}(K(G/T) \cup (2b + K(G/T)))$ we have $\nu(z) > L(G)\ |T|$. In particular, if $\nu(z) = L(G)\ |T|$ then $z \in \pi^{-1}(K(G/T) \cup (2b + K(G/T)))$.

The next theorem gives a characterization of the critical sets of Theorem 12, provided a restriction holds.

Theorem 23. *Let A, B and S be non-empty subsets of a finite Abelian group G with $|A|+|B| = |G| + L_S$. Assume that 0 is an $A \wedge^S B$-exception with $0 \in A \cap B \cap S$ and that $|A \wedge^S B| = |G| - 2|S|$. The following conditions hold true:*

(i) *There exists a decomposition $S = S_1 \cup S_2 \cup \ldots \cup S_k$ of S modulo $2 \cdot G$ such that $|S_i| = L_S/L(G)$ for each $i \in \{1, 2, \ldots, k\}$ and $|A \wedge^{S_i} B| = |G| - 2|S_i|$ for each $i \in \{1, 2, \ldots, k\}$. Moreover, the set of $A \wedge^S B$-exceptions can be partitioned in the form $G \setminus (A \wedge^S B) = \cup_{i=1}^{k} (G \setminus (A \wedge^{S_i} B))$.*

Without loss of generality, we can assume that $0 \in S_1$.

(ii) *S_1 is a group.*

Let $\pi : G \to G/S_1$ be the natural projection and let $A' = \pi(A)$ and $B' = \pi(B)$.

(iii) *There exists $b \in A' \cap B'$ such that $H = \langle 2b \rangle$ is a subgroup of G/S_1 of odd order d greater than 1.*
(iv) *There exists $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_l, x_{l+1}, \ldots, x_m\} \subset (G/S_1) \setminus (K(G/S_1)+H)$, where $m = (|G/S_1|/d - L(G/S_1))/2$ and $0 \leq k, l \leq m$, such that*

$$G/S_1 \setminus (K(G/S_1)+H) = \bigcup_{i=1}^{m} ((x_i + H) \cup (-x_i + H)),$$
$$A' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/S_1)) \cup (\{x_1, \ldots, x_k, \pm x_{k+1}, \ldots, \pm x_l\} + H),$$
$$B' = \{0, b, 3b, \ldots, (d-2)b\} + K(G/S_1)) \cup (\{x_1, \ldots, x_k, \pm x_{l+1}, \ldots, \pm x_m\} + H).$$

Moreover, if we suppose that $(d+1)/2 > L(G/S_1)$ *then*

(v) $S_i = y_i + S_1$, *for each* $i = 1, \ldots, k$, *where* $Y = \{y \in G : 2y \in S_1\}$ *and* $Y = \cup_{i=1}^{r}(y_i + S_1)$, $r \geq k$, *is a decomposition modulo* S_1. *In particular,* $2 \cdot S \subset S_1$,

(vi) *The set of* $A \wedge^S B$*-exceptions is* $\{0, 2b^*\} + S$, *where* $b^* \in \pi^{-1}(b)$, *and*

(vii) $(\{0, 2b\} + \{\pi(y_1), \pi(y_2), \ldots, \pi(y_k)\}) \cap (Q + R) = \emptyset$, *where* $Q = \{x_1, \ldots, x_k, \pm x_{k+1}, \ldots, \pm x_l\} + H$ *and* $R = \{x_1, \ldots, x_k, \pm x_{l+1}, \ldots, \pm x_m\} + H$.

Proof. (i) holds by Theorem 19. Theorem 18 implies (ii), (iii) and (iv). Finally, by Proposition 20, Corollary 21 and Corollary 22 we obtain (v), (vi) and (vii). □

Acknowledgements

The authors want to thank the anonymous referee for his/her careful reading of the paper, and for the useful comments that he/she made, which helped to increase the quality of the paper.

Research done when the second author was visiting Université Pierre et Marie Curie, E. Combinatoire, Paris, supported by the Ministry of Education, Spain, under the National Mobility Programme of Human Resources, Spanish National Programme I-D-I 2008–2011.

References

[1] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* **56** (1996), 404–417.

[2] A.-L. Cauchy, Recherches sur les nombres, J. École polytechnique (1813), 99–123.

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

[4] G. Chiaselotti, On additive bases with two elements, *Acta Arith* **101.2** (2002), 115–119.

[5] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivates and additive theory, *Bull. London Math. Soc.* **26** (1994), 140–146.

[6] L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau, A. Plagne, Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős-Ginzburg-Ziv problem, *J. London Math. Soc.* **65** (2) (2002), 513–523.

[7] S.G. Guo, Restricted sumsets in a finite Abelian group, *Discrete Math.* **309** (2009), 6530–6534.

[8] S. Guo, Z.W. Sun, A variant of Tao's method with application to restricted sumsets, *J. Number Theory* **129** (2009), 434–438.

[9] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.

[10] V.F. Lev, Restricted set addition in groups I: The classical setting, *J. London Math. Soc.* **62** (2) (2000), 27–40.

[11] M.B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Grad. Texts in Math. 165, Springer, 1996.

[12] H. Pan, Z.W. Sun, A lower bound $|\{a + b : a \in A, b \in B, P(a, b) \neq 0\}|$, *J. Combin. Theory Ser. A* **100** (2002), 387–393.

[13] H. Pan, Z.W. Sun, Restricted sumsets and a conjecture of Lev, *Israel J. Math.* **154** (2006), 21–28.

[14] Z.W. Sun, Restricted sums of subsets of $\mathbb{Z}$, *Acta Arith.* **99** (2001), 41–60.

[15] T. Tao, An uncertainty principle for cyclic groups of prime order, *Math. Res. Lett.* **12** (2005), 121–127.

E-mail address: susana@ma4.upc.edu

E-mail address: plagne@math.polytechnique.fr

Universitat Politècnica de Catalunya. BarcelonaTech, Dept. Matemàtica Apl. IV; C/Esteve Terrades, 5, Castelldefels, Spain.

École polytechnique, Centre de Mathématiques Laurent Schwartz, UMR 7640 du CNRS, 91128 Palaiseau cedex, France.