Combinatorics, Probability and Computing (2012) 21, 582–596. © Cambridge University Press 2012
doi:10.1017/S0963548312000168

k-Sums in Abelian Groups

BENJAMIN GIRARD[1], SIMON GRIFFITHS[2†]
and YAHYA OULD HAMIDOUNE

[1]IMJ, Équipe Combinatoire et Optimisation, Université Pierre et Marie Curie (Paris 6),
4 Place Jussieu, 75005 Paris, France
(e-mail: bgirard@math.jussieu.fr)
[2]IMPA, Estrada Dona Castorina 110, Rio de Janeiro, Brasil 22460-320
(e-mail: sgriff@impa.br)

Received 10 October 2011; revised 1 March 2012; first published online 23 April 2012

Given a finite subset A of an abelian group G, we study the set $k \wedge A$ of all sums of k distinct elements of A. In this paper, we prove that $|k \wedge A| \geqslant |A|$ for all $k \in \{2, \ldots, |A| - 2\}$, unless $k \in \{2, |A| - 2\}$ and A is a coset of an elementary 2-subgroup of G. Furthermore, we characterize those finite sets $A \subseteq G$ for which $|k \wedge A| = |A|$ for some $k \in \{2, \ldots, |A| - 2\}$. This result answers a question of Diderrich. Our proof relies on an elementary property of proper edge-colourings of the complete graph.

AMS 2010 *Mathematics subject classification*: Primary 05E15, 11B13, 11P70, 05C15

1. Introduction

Sumsets are the central object of study in additive combinatorics. In particular, the sumset

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

and the k-fold sumset

$$kA := \{a_1 + \cdots + a_k : a_i \in A\}$$

of subsets A, B of an abelian group G have been extensively studied. For background and references we refer the reader to the course of Ruzsa [18] and the book of Tao and Vu [19]. See also recent results of Petridis [17].

In this paper, we consider sums of k *distinct elements* of A, which we will call *k-sums*. Given an abelian group G (not necessarily finite), any finite subset A of G will be referred

† Research supported by CNPq Proc. 500016/2010-2.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

to as an *additive set*, and

$$k \wedge A := \left\{ \sum_{a \in B} a : B \subseteq A, |B| = k \right\}$$

will denote the set of k-sums of A. Many results concerning k-sums of subsets of abelian groups focus on the cases $k = 2$ and $k = 3$. See for example the survey of Lev [15] and the papers of Lev [14], Hamidoune, Lladó and Serra [13], and Gallardo, Grekos, Habsieger, Hennecart, Landreau and Plagne [10]. On the other hand, k-sums for general k have been studied more extensively for sequences than for sets, with a particular emphasis on determining whether 0 is a k-sum; see the seminal article of Erdős, Ginzburg and Ziv [8], the article of Bollobás and Leader [3], the survey of Gao and Geroldinger [11] and the references contained therein.

It is often more tricky to prove results about the set of k-sums $k \wedge A$ than the k-fold sumset kA. For example, it is a straightforward consequence of the Cauchy–Davenport theorem [4, 5] that the inequality

$$|kA| \geqslant \min\{p, k|A| - (k-1)\}$$

holds for each $k \in \mathbb{N}$ and subset A of $\mathbb{Z}_p$, the integers modulo a prime p. Establishing the analogous result for k-sums is significantly more difficult. Indeed, it was a major breakthrough when Dias da Silva and Hamidoune [6] proved that the inequality

$$|k \wedge A| \geqslant \min\{p, k(|A| - k) + 1\} \tag{1.1}$$

holds for each $k \in \mathbb{N}$ and subset A of $\mathbb{Z}_p$ (p prime). This result was proved by studying a general problem on Grassmann spaces, and the case $k = 2$ confirmed a conjecture of Erdős and Heilbronn [9]. An alternative proof, using the Combinatorial Nullstellensatz [1], was then given by Alon, Nathanson and Ruzsa [2].

Our aim in this paper is to prove a much more modest estimate but in the more general setting of an *arbitrary* abelian group G. In the case of k-fold sums it is trivial that $|kA| \geqslant |A|$, and easily proved that equality occurs if and only if A is a coset of a subgroup of G (provided $k \geqslant 2$). We prove the analogous result for k-sums.

We require the following definitions. An *elementary 2-subgroup* is a finite subgroup of G in which all non-identity elements have order 2 (equivalently, a subgroup isomorphic to $\mathbb{Z}_2^d$, for some $d \in \mathbb{N}$). We call an additive set $A \subseteq G$ a *2-coset* if it is a coset of an elementary 2-subgroup and an *almost 2-coset* if A may be obtained from a 2-coset by removing a single element.

Theorem 1.1. *Let $A \subseteq G$ be an additive set and let $2 \leqslant k \leqslant |A| - 2$. Then*

$$|k \wedge A| \geqslant |A|$$

unless $k \in \{2, |A| - 2\}$ and A is a 2-coset. Furthermore

$$|k \wedge A| > |A|$$

unless A is a coset of a subgroup of G or $k \in \{2, |A| - 2\}$ and

(i) *A is an almost 2-coset, or*
(ii) *$|A| = 4$ and A is the union of two cosets of a subgroup of order 2.*

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Remarks. **(1)** The first assertion of Theorem 1.1 was first proved by Mann and Olson [16] in the case that $G = \mathbb{Z}_p$ (p prime), and by Diderrich [7] in the case that G has no 2-torsion. Wang [20] rediscovered the result of Diderrich and proved that equality occurs if and only if A is a coset of a subgroup of G.

(2) Diderrich's proof is inductive and for this reason he actually proved a slightly more general result stating that $|\sigma(k \wedge A)| \geqslant |\sigma(A)|$ for any canonical homomorphism $\sigma : G \to G/H$. Alternatively, this result may be viewed as a sequence version of the inequality $|k \wedge A| \geqslant |A|$. In Section 5, we sketch the proof of a sequence version of Theorem 1.1 which extends Diderrich's result.

Our proof of Theorem 1.1 proceeds in two steps. In the first, we focus on 2-sums and prove detailed results concerning this case. In the second, we relate the k-sums of a set A to the 2-sums of a subset $B \subseteq A$ using the observation that

$$a_1 + \cdots + a_{k-2} + 2 \wedge B \subseteq k \wedge A \tag{1.2}$$

for any distinct elements $a_1, \ldots, a_{k-2}$ of $A \setminus B$. Thus, our proof relies on proving bounds on $|2 \wedge B|$ for subsets $B \subseteq A$.

Proposition 1.2. *Let $A \subseteq G$ be an additive set of cardinality $|A| \geqslant 5$.*

(i) *If $|2 \wedge A| \geqslant |A|$ then there is a subset $B \subseteq A$ with $|B| = \lfloor (|A|+3)/2 \rfloor$ such that $|2 \wedge B| \geqslant |A|$.*
(ii) *If $|2 \wedge A| < |A|$ then there is a subset $B \subseteq A$ with $|B| = |A|/2 + 1$ such that $|2 \wedge B| = |A| - 1$.*

□

The reader will observe that by (1.2), together with Proposition 1.2, the implication

$$|2 \wedge A| \geqslant |A| \Rightarrow |k \wedge A| \geqslant |A|$$

holds for all $k \in \{2, \ldots, \lfloor |A|/2 \rfloor\}$. Taking into account the symmetry $|k \wedge A| = |(|A| - k) \wedge A|$, we observe that the implication holds for all $k \in \{2, \ldots, |A| - 2\}$. Except for the special case when A is a 2-coset, this is precisely our proof of the first part of Theorem 1.1 (see Proposition 4.1 and its proof). The proof of the second part of Theorem 1.1, the characterization of the cases where the equality $|k \wedge A| = |A|$ holds, again uses Proposition 1.2, but in this case we consider not only a single $(k-2)$-sum of $A \setminus B$ (as in (1.2)) but all of them:

$$(k-2) \wedge (A \setminus B) + 2 \wedge B \subseteq k \wedge A.$$

The outline of the paper is as follows. We complete the introduction by stating the graph-theoretic analogue of Proposition 1.2. In Section 2 we prove results concerning $|2 \wedge A|$, the number of 2-sums of A. In Section 3 we prove Proposition 1.2, and in Section 4 we bring together the two strands to prove Theorem 1.1. In Section 5, we state and prove a sequence version of Theorem 1.1. Finally, in Section 6, we mention some open problems and make some concluding remarks.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

We remark that Proposition 1.2 will be deduced from the following graph-theoretic statement, which we state here in case it may be of independent interest. We denote by K_n the complete graph on n vertices. The vertex set and edge set of K_n are denoted by $V(K_n)$ and $E(K_n)$ respectively. Given a graph G and a vertex subset U, we denote by $G[U]$ the subgraph of G induced by U. Finally, we recall that a proper edge-colouring of a graph is one in which any two edges that share an endpoint receive different colours.

Proposition 1.3. *Let $n \geqslant 5$ be an integer and let $c : E(K_n) \to \mathbb{N}$ be a proper edge-colouring of the complete graph on n vertices.*

(i) *If at least n colours are used by c then there is a subset $U \subseteq V(K_n)$ with $|U| = \lfloor (n+3)/2 \rfloor$ and such that c uses at least n colours on the edges of $K_n[U]$.*

(ii) *If c uses $n-1$ colours then there is a subset $U \subseteq V(K_n)$ with $|U| = n/2 + 1$ and such that c uses $n-1$ colours on the edges of $K_n[U]$.*

□

The proof of Proposition 1.3, given in Section 3, is a straightforward application of the probabilistic method, namely the first moment method.

2. The number of 2-sums

In this section we prove some lemmas on the number of 2-sums of an additive set A. Before doing so, we recall the following well-known fact (see [19, Proposition 2.2] for example).

Lemma 2.1. *Let $A, B \subseteq G$ be additive sets. Then $|A+B| = |A|$ if and only if A is a union of cosets of a subgroup H of G and B is contained in a coset of H. In particular, $|A+A| = |A|$ if and only if A is a coset of a subgroup of G.*

We now establish the key lemmas on the set of 2-sums of A. To do so, the following notation will be used. We say that a 2-sum g of an additive set A is *represented* at an element $a \in A$ if there is an element $b \in A \setminus \{a\}$ such that $a + b = g$.

Lemma 2.2. *Let $A \subseteq G$ be an additive set of cardinality at least 3. Then $|2 \wedge A| < |A|$ if and only if A is a 2-coset.*

Proof. In the case that A is a 2-coset then it is easily observed that $|2 \wedge A| = |A| - 1 < |A|$. Now, suppose that A is an additive set for which $|2 \wedge A| < |A|$. Since $|2 \wedge A|$ is invariant under translation we may assume also that $0 \in A$. We shall prove that $2y = 0$ for every $y \in A$. Observe that this is sufficient to complete the proof of the lemma. Indeed, by Lemma 2.1 it suffices to prove that A is contained in an elementary 2-subgroup of G and that $|A+A| = |A|$, and both these facts follow easily once we prove that $2y = 0$ for every $y \in A$ (for the latter, observe that $A + A = (2 \wedge A) \cup \{2y : y \in A\}$).

In proving that $2y = 0$ for every $y \in A$ we shall use the following observation: since $|A| - 1$ distinct 2-sums are represented at each element of A, the inequality $|2 \wedge A| < |A|$

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

may occur only if $|2 \wedge A| = |A| - 1$. In this case every 2-sum is represented at every element of A.

Now, let $y \in A$ be fixed; we prove that $2y = 0$. We argue as follows. Let z be an arbitrary element of $A \setminus \{0, y\}$. Then we may deduce from the above observation that the sum $y + z$ is represented at 0 and the sum $0 + z$ is represented at y. It follows that

$$y + z,\ z - y \in A.$$

If these elements are distinct, then $2z = (y + z) + (z - y)$ would be a 2-sum not represented at z, a contradiction. It follows that $y + z = z - y$, and so $2y = 0$, as required. □

We now characterize subsets of 2-cosets for which the inequality $|2 \wedge A| \leqslant |A|$ holds. Recall that an almost 2-coset is an additive set A that may be obtained from a 2-coset by removing a single element.

Lemma 2.3. *Let $A \subseteq G$ be a subset of a 2-coset. Then $|2 \wedge A| > |A|$ unless A is either a 2-coset or an almost 2-coset.*

Proof. Without loss of generality we may assume that $0 \in A$, so that A is contained in some elementary 2-subgroup H of G. We may further assume that H is minimal such that $A \subseteq H$, that $\{x_1, \ldots, x_d\}$ is a minimal subset of A such that $H = \langle x_1, \ldots, x_d \rangle$, and that $|H \setminus A| \geqslant 2$ (as there is nothing to prove if A is a 2-coset or almost 2-coset). Let $I \subseteq \{1, \ldots, d\}$ be minimal such that $\sum_{i \in I} x_i \notin A$, and let $J \subseteq \{1, \ldots, d\}$ be minimal such that $J \neq I$ and $\sum_{j \in J} x_j \notin A$. By minimality both $\sum_{i \in I} x_i$ and $\sum_{j \in J} x_j$ may be expressed as sums of two distinct elements of A. Thus,

$$2 \wedge A \supseteq (A \setminus \{0\}) \cup \left\{ \sum_{i \in I} x_i, \sum_{j \in J} x_j \right\},$$

and so $|2 \wedge A| > |A|$. □

We now establish two lemmas that will help us characterize those additive sets A for which $|2 \wedge A| = |A|$.

Lemma 2.4. *Let $A \subseteq G$ be an additive set of cardinality at least 5, and suppose that A is not an almost 2-coset. Then*

$$|2 \wedge A| \leqslant |A| \quad \Leftrightarrow \quad |A + A| = |A|.$$

Proof. Since $2 \wedge A$ is a subset of $A + A$, one direction of the implication is trivial. Also, we remark that if A is a 2-coset then $|A + A| = |A|$. In particular, by Lemma 2.2, this deals with the case that $|2 \wedge A| < |A|$.

Thus, we may suppose that A is an additive set of cardinality at least 5, that A is not an almost 2-coset and that $|2 \wedge A| = |A|$. We shall prove that in this case $A + A = 2 \wedge A$. To do so, it suffices to prove that for each element $x \in A$ there exists a pair of distinct elements $y, z \in A$ such that $2x = y + z$.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Fix $x \in A$. We first claim that there are three elements y_1, y_2, y_3 of A such that $2x \neq 2y_i$ for $i = 1, 2, 3$. Observe that if this were not the case then A would contain a subset C of cardinality $|A|, |A| - 1$ or $|A| - 2$ such that $2c = 2c'$ for all $c, c' \in C$. In fact each of these three possibilities contradicts the equality $|2 \wedge A| = |A|$. If $|C| = |A|$ then A is a subset of a 2-coset and so $|2 \wedge A| > |A|$ by Lemma 2.3, a contradiction. If $|C| = |A| - 1$ then there is an element $a \in A$ such that $A = C \cup \{a\}$, where C is a subset of a 2-coset and a is not an element of this coset. It follows that $2 \wedge C$ and $a + C$ are disjoint subsets of $2 \wedge A$, and so $|2 \wedge A| \geqslant 2|C| - 1 \geqslant 2|A| - 3 > |A|$, a contradiction. Finally, if $|C| = |A| - 2$ then there exist elements $a, a' \in A$ such that $A = C \cup \{a, a'\}$, where C is a subset of a 2-coset and a, a' do not belong to this coset. Arguing as above we obtain that $|2 \wedge A| \geqslant 2|C| - 1 \geqslant 2|A| - 5$, which is a contradiction unless $|A| = 5$. In the case $|A| = 5$ we note that the subset C has cardinality 3, and so $|2 \wedge A| \geqslant 3 + 3 > |A|$, as $|2 \wedge C| = 3$ for all additive sets of cardinality 3, again a contradiction.

Having established the claim we may now assume that there are three elements y_1, y_2, y_3 of A such that $2x \neq 2y_i$ for $i = 1, 2, 3$. Since at most one 2-sum is not represented at x, one of the sums $y_1 + y_2, y_1 + y_3$ is represented at x, without loss of generality $y_1 + y_2$. Let $u \in A$ be such that $x + u = y_1 + y_2$. Arguing as before, at least one of the sums $x + y_1, x + y_2$ is represented at u, without loss of generality $x + y_2$. Let $z \in A$ be such that $u + z = x + y_2$, and set $y = y_1$. We claim that $y + z = 2x$. Indeed

$$y + z = y + y_2 + z - y_2 = x + u + z - y_2 = x + x + y_2 - y_2 = 2x. \qquad \square$$

In the case that $|A| = 4$ we have the following.

Lemma 2.5. *Let $A \subseteq G$ be an additive set of cardinality 4 for which $|2 \wedge A| = |A|$. Then A is the union of two cosets of a subgroup of order 2.*

Proof. Since there are six pairs of elements of A and only 4 distinct sums, two sums are repeated. It follows that the elements of A may be labelled x, y, z, u in such a way that

$$x + y = z + u \quad \text{and} \quad x + z = y + u.$$

Hence

$$2x = (x + y) + (x + z) - y - z = (z + u) + (y + u) - y - z = 2u,$$

and similarly $2y = 2z$. Thus, A is the union of two cosets of the subgroup $\{0, (x - u)\} = \{0, (z - y)\}$, as required. $\square$

3. Proof of Proposition 1.2

We first give a proof of Proposition 1.2 assuming the graph-theoretic Proposition 1.3. The rest of the section will then be dedicated to proving Proposition 1.3.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Proof of Proposition 1.2. Let $A \subseteq G$ be an additive set of cardinality $n \geqslant 5$. Define an edge-colouring of the complete graph on vertex set A by assigning colour $x+y$ to the edge $\{x,y\}$ (for each pair of elements $x, y \in A$). Since $x+y \neq x+z$ when y,z are distinct, this edge-colouring is proper.

(i) If $|2 \wedge A| \geqslant |A|$ then at least $n = |A|$ colours are used in this colouring. By Proposition 1.3 there exists a subset $B \subseteq A$ of cardinality $\lfloor (n+3)/2 \rfloor$ such that c uses at least n colours on the edges of $K_n[B]$. Translating back to additive language, this says precisely that $|2 \wedge B| \geqslant n = |A|$, as required.

(ii) If $|2 \wedge A| < |A|$ then $n-1 = |A|-1$ colours are used in this colouring. By Proposition 1.3 there exists a subset $B \subseteq A$ of cardinality $n/2+1$ such that c uses $n-1$ colours on the edges of $K_n[B]$. Translating back to additive language, this says precisely that $|2 \wedge B| = |A|-1$, as required. □

Our approach to proving Proposition 1.3 is to select the vertex subset U uniformly at random from the collection of subsets of the appropriate cardinality and prove a lower bound on the expected number of colours used in $K_n[U]$. The following lemma will help us prove the required bound on the expectation.

Given two positive integers a, n such that $n \geqslant 5$ and $a \leqslant n/2$, we define the probability $p(a,n) \in [0,1]$ as follows. Let $p(a,n)$ be the probability that a subset $U \subseteq \{1,\dots,n\}$ selected uniformly at random from the collection of subsets of cardinality $\lfloor (n+3)/2 \rfloor$ covers at least one of the pairs $\{1,2\},\dots,\{2a-1,2a\}$. Note that the same probability $p(a,n)$ applies if the pairs $\{1,2\},\dots,\{2a-1,2a\}$ are replaced by any a disjoint pairs $e_1,\dots,e_a$ of elements of $\{1,\dots,n\}$.

Lemma 3.1. *Let a, n be two positive integers such that $n \geqslant 5$ and $a \leqslant n/2$. Then*

$$p(a,n) \geqslant \frac{2a}{n},$$

with equality if and only if $a = n/2$.

Proof. Let F be a set of $\lfloor n/2 \rfloor$ disjoint pairs of elements of $\{1,\dots,n\}$. For each subset $E \subseteq F$ of cardinality $|E| = a$, let X_E be the indicator random variable for U covering at least one pair of E. On the one hand, the pigeonhole principle implies that every subset $U \subseteq \{1,\dots,n\}$ of cardinality $\lfloor (n+3)/2 \rfloor$ covers at least one pair of F. Thus, we obtain

$$\sum_{\substack{E \subseteq F \\ |E|=a}} X_E \geqslant \binom{\lfloor n/2 \rfloor - 1}{a-1}.$$

On the other hand, it follows from the above discussion that for every $E \subseteq F$ of cardinality $|E| = a$, one has $p(a,n) = \mathbb{P}(X_E = 1)$. Therefore, linearity of expectation yields

$$p(a,n) \geqslant \binom{\lfloor n/2 \rfloor - 1}{a-1} \Big/ \binom{\lfloor n/2 \rfloor}{a} = \frac{a}{\lfloor n/2 \rfloor} \geqslant \frac{2a}{n}.$$

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Now, for equality to hold, n must be even. In particular, $n \geqslant 6$ and $\lfloor (n+3)/2 \rfloor = n/2 + 1$. Moreover, there is a subset $U_0 \subseteq \{1, \ldots, n\}$ of cardinality $n/2+1$ covering at least two pairs of F. Hence the number of subsets $E \subseteq F$ of cardinality $|E| = a$ such that U_0 covers at least one pair of E strictly exceeds $\binom{n/2-1}{a-1}$ whenever $a < n/2$. Therefore, the equality $p(a,n) = 2a/n$ can only occur when $a = n/2$, and it is easily seen that $p(a,n) = 1$ holds in this case. □

We now complete our proof of Proposition 1.2 by proving Proposition 1.3.

Proof of Proposition 1.3. **(i)** Let U be selected uniformly at random from the collection of vertex subsets of cardinality $\lfloor (n+3)/2 \rfloor$. For each $i \in \mathbb{N}$, let a_i denote the number of times colour i is used in the colouring c. Now, by Lemma 3.1, the expected number of colours used in $K_n[U]$ is

$$\sum_{i \in \mathbb{N}} p(a_i, n) \geqslant \sum_{i \in \mathbb{N}} \frac{2a_i}{n} = n - 1.$$

Furthermore, since at least n colours are used in the colouring c, some a_i must lie strictly between 0 and $n/2$. Thus, the above inequality is strict, and the expected number of colours used in $K_n[U]$ is at least n. In particular, there exists a subset U of $\lfloor (n+3)/2 \rfloor$ vertices such that at least n colours are used in $K_n[U]$.

(ii) Since each colour may be used at most $n/2$ times and c uses $n-1$ colours, each colour class is a perfect matching. It is then easily observed that for *every* subset U of $n/2+1$ vertices, $K_n[U]$ contains an edge from each of the $n-1$ colour classes. □

4. Proof of Theorem 1.1

In this section we bring together the results of the previous sections to prove Theorem 1.1. We note that the results of Section 2 together establish the $k = 2$ case of Theorem 1.1. We may immediately complete the proof of the first part of Theorem 1.1.

Proposition 4.1. *Let $A \subseteq G$ be an additive set and let $2 \leqslant k \leqslant |A| - 2$. Then*

$$|k \wedge A| \geqslant |A|$$

unless $k \in \{2, |A| - 2\}$ and A is a 2-coset. □

Proof. By the symmetry $|(|A| - k) \wedge A| = |k \wedge A|$ it suffices to prove the proposition for $2 \leqslant k \leqslant \lfloor |A|/2 \rfloor$. The $k = 2$ case is precisely Lemma 2.2. For $k \in \{3, \ldots, \lfloor |A|/2 \rfloor\}$, we may assume $|A| \geqslant 5$. We now consider the following two cases.

Case I. If $|2 \wedge A| \geqslant |A|$, then, by Proposition 1.2(i), there exists a subset $B \subseteq A$ of cardinality $\lfloor (|A|+3)/2 \rfloor$ such that $|2 \wedge B| \geqslant |A|$. Now simply choose a sequence $c_1, \ldots, c_{k-2}$ of $k - 2 \leqslant |A|/2 - 2$ distinct elements of $A \setminus B$ and observe that

$$k \wedge A \supseteq (c_1 + \cdots + c_{k-2}) + 2 \wedge B,$$

and so $|k \wedge A| \geqslant |2 \wedge B| \geqslant |A|$, as required.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Case II. If $|2 \wedge A| < |A|$, then, by Lemma 2.2, A is a 2-coset, and one easily observes that $2 \wedge A$ is an almost 2-coset. Also, by Proposition 1.2(ii), there exists a subset $B \subseteq A$ of cardinality $|A|/2 + 1$ such that $|2 \wedge B| = |A| - 1$. Of course $2 \wedge B$ must be precisely $2 \wedge A$, and so is also an almost 2-coset. Now, let $c_1, \ldots, c_{k-1}$ be distinct elements of $A \setminus B$ and note that the sets

$$c_1 + \cdots + c_{k-2} + 2 \wedge B \quad \text{and} \quad c_2 + \cdots + c_{k-1} + 2 \wedge B$$

are not identical, since $c_{k-1} - c_1$ does not belong to the stabilizer of $2 \wedge B$, which is trivial. Finally, since $k \wedge A$ contains both these sets we deduce that $|k \wedge A| \geqslant |A|$. □

For convenience we read out an immediate corollary of the above proposition, corresponding to the case that A is a coset of a subgroup of G, that will be useful in our proof of Theorem 1.1.

Corollary 4.2. *Let Q denote a coset of a subgroup H of an abelian group G, and let $k \in \{1, \ldots, |Q| - 1\}$. Then $k \wedge Q$ contains exactly those elements of the coset kQ, unless $k \in \{2, |Q| - 2\}$ and Q is a 2-coset, in which case $k \wedge Q$ contains all but one element of kQ.*

Proof. It is elementary that $k \wedge Q$ is contained in the coset kQ in all cases. Since kQ is also a coset of H its cardinality is equal to that of Q. The corollary now follows immediately from Proposition 4.1 together with the observation that $|2 \wedge Q| = |Q| - 1$ whenever Q is a 2-coset. □

We now prove a lemma that will help us characterize the cases for which the equality $|k \wedge A| = |A|$ holds. Given an additive set $A \subseteq G$, we write $C(A)$ for the set of sizes of cosets contained in A, *i.e.*, $h \in C(A)$ if and only if there is a subgroup H of G of order h such that $Q \subseteq A$ for some coset Q of H. Note that $|A| \in C(A)$ if and only if A itself is a coset of a subgroup of G.

Lemma 4.3. *Let $A \subseteq G$ be an additive set of even cardinality at least 6. If $|A|/2 \in C(A)$ but $|A| \notin C(A)$, then $|k \wedge A| > |A|$ for all $k \in \{3, \ldots, |A| - 3\}$.*

We must prove a certain *expansion* in the set of sums relative to the original set A. In fact in almost all cases it is easy to prove (using Corollary 4.2) that at least three cosets of H lie in $k \wedge A$ (where H is a subgroup with $|H| = |A|/2$ and such that a coset of H is contained in A), implying $|k \wedge A| \geqslant 3|A|/2$. To deal with the few exceptional cases of Corollary 4.2 we use the following observation.

Observation 4.4. *Let H be a subgroup of G, let Q, R be cosets of H and let $X \subseteq Q, Y \subseteq R$ be subsets such that $|X| + |Y| > |H|$. Then $X + Y = Q + R$.*

This observation is simply a variant of the 'prehistoric lemma' which states that $X + Y = G$ whenever $X, Y \subseteq G$ are such that $|X| + |Y| > |G|$. We now prove Lemma 4.3.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Proof of Lemma 4.3. Let H be a subgroup of cardinality $|A|/2$ such that some coset Q of H is contained in A. By the usual symmetry argument, it suffices to prove the result for $k \in \{3, \ldots, \lfloor |A|/2 \rfloor\}$. We consider the following three cases.

Case I. A is the union of two cosets Q_1, Q_2 of H and $k = 3$. Observe first that $2Q_1 \neq 2Q_2$ in G/H, as A itself is not a coset of a subgroup of G. It follows that the cosets $3Q_1, 2Q_1 + Q_2$ and $Q_1 + 2Q_2$ are distinct, and therefore the sets

$$3 \wedge Q_1,\ 2 \wedge Q_1 + Q_2 \quad \text{and} \quad Q_1 + 2 \wedge Q_2 \tag{4.1}$$

are disjoint subsets of $3 \wedge A$. If $|H| = 3$ then it is easily observed that these sets have cardinalities $1, 3, 3$ respectively, which implies that $|3 \wedge A| \geqslant 7 > 6 = |A|$. If $|H| \geqslant 4$ then it follows from Corollary 4.2 that each of the sets $j \wedge Q_1, j \wedge Q_2$, where $j \in \{1, 2, 3\}$, has cardinality at least $|H| - 1 > |H|/2$, and so, using Observation 4.4, we obtain that the sets mentioned in (4.1) have cardinalities at least $|H| - 1, |H|, |H|$ respectively, and so $|3 \wedge A| \geqslant 3|H| - 1 > |A|$, as required.

Case II. A is the union of two cosets Q_1, Q_2 of H and $k \geqslant 4$. Since $k \geqslant 4$ we may assume $|A| \geqslant 8$, and so $|H| \geqslant 4$. It follows from Corollary 4.2 that each of the sets

$$(k - j) \wedge Q_1,\ j \wedge Q_2 \quad j \in \{1, 2, 3\}$$

has cardinality at least $|H| - 1 > |H|/2$. Observation 4.4 then yields

$$|(k - j) \wedge Q_1 + j \wedge Q_2| = |H| \quad \text{for each } j \in \{1, 2, 3\}.$$

These three sets are disjoint (since, as argued in Case I, $2Q_1 \neq 2Q_2$ in G/H) and are contained in $k \wedge A$. It follows that $|k \wedge A| \geqslant 3|H| > |A|$, as required.

Case III. A contains a coset Q_1 of H and meets at least two other cosets of H, say Q_2 and Q_3. By translation we may assume that $Q_1 = H$. Let $x \in A \cap Q_2$ and $y \in A \cap Q_3$. The sets

$$x + (k - 1) \wedge Q_1,\ y + (k - 1) \wedge Q_1 \quad \text{and} \quad x + y + (k - 2) \wedge Q_1$$

are disjoint subsets of $k \wedge A$. By Corollary 4.2, each of the three sets mentioned above has cardinality at least $|H| - 1$. Thus $|k \wedge A| \geqslant 3|H| - 3$. If $|A| > 6$, then $3|H| - 3 > |A|$ and the proof is complete. If $|A| = 6$ then $|H| = 3$ is not a power of 2, so Corollary 4.2 gives the stronger conclusion that each of the three sets mentioned above has cardinality at least $|H|$, so that $|k \wedge A| \geqslant 3|H| = 3|A|/2 > |A|$, and the proof is complete. □

We are now ready to characterize the cases in which the equality $|k \wedge A| = |A|$ holds, completing the proof of our main theorem.

Proof of Theorem 1.1. Let $A \subseteq G$ be an additive set and let $k \in \{2, \ldots, |A| - 2\}$. By Proposition 4.1, the inequality

$$|k \wedge A| \geqslant |A|$$

holds, unless $k \in \{2, |A| - 2\}$ and A is a 2-coset.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Now suppose that the equality $|k \wedge A| = |A|$ holds for some $k \in \{2, \ldots, |A| - 2\}$. Then in particular the equality holds for some $k \in \{2, \ldots, \lfloor |A|/2 \rfloor\}$. If $k = 2$, then either $|A| = 4$, in which case A is a union of two cosets of a subgroup of order 2 by Lemma 2.5, or $|A| \geqslant 5$, in which case A is either an almost 2-coset or a coset of a subgroup of G by Lemmas 2.1 and 2.4.

Suppose now that the equality $|k \wedge A| = |A|$ holds for some $k \in \{3, \ldots, \lfloor |A|/2 \rfloor\}$. We prove that A is a coset of a subgroup of G. If A is a 2-coset then we are done immediately. Hence we may assume that A is not a 2-coset. In particular this implies (by Lemma 2.2) that $|2 \wedge A| \geqslant |A|$ and (by Proposition 1.2) that $|2 \wedge B| \geqslant |A|$ for some subset $B \subseteq A$ with $|B| = \lfloor (|A| + 3)/2 \rfloor$.

Set

$$S = 2 \wedge B \quad \text{and} \quad C = A \setminus B.$$

Claim. *There is a subgroup H of G such that S is a union of cosets of H and C is contained in a coset of H.*

Proof of Claim. By Lemma 2.1 it suffices to prove that one of the equalities $|S + C| = |S|$ or $|S - C| = |S|$ holds. If $k = 3$, then $S + C$ is a subset of $k \wedge A$, and so

$$|S + C| \leqslant |k \wedge A| = |A| = |S|.$$

If $k \in \{4, \ldots, \lfloor |A|/2 \rfloor\}$, we shall prove that every subset C' of C of cardinality $k - 1$ is contained in a coset of H. Since the subset C' is arbitrary, this certainly implies that C is contained in a coset of H. Given a subset C' of C of cardinality $k - 1$, we denote by $\sigma_{C'}$ the sum $\sum_{a \in C'} a$. Now, since $k \wedge A$ contains $S + (k - 2) \wedge C' = S + \sigma_{C'} - C'$ we have that

$$|S + \sigma_{C'} - C'| \leqslant |k \wedge A| = |A| = |S|.$$

Thus $|S - C'| = |S|$, completing the proof of the claim.

It follows from the claim that $|H|$ divides $|S| = |A|$, and $|H| \geqslant |C| = \lceil (|A| - 3)/2 \rceil$. There are three cases to consider.

Case I. $|H| = |A|$. In this case S is equal to a coset of H, implying that B is contained in a coset Q of H. We claim that C is also contained in Q, which implies that $A = B \cup C$ is indeed a coset of a subgroup of G. Indeed, if C were not contained in Q then $k \wedge A$ would contain the $|A|$ elements in $S + (k - 2) \wedge C$ and at least $|B| = \lfloor (|A| + 3)/2 \rfloor$ elements in $B + (k - 1) \wedge C$, implying $|k \wedge A| > |A|$, a contradiction.

Case II. $|H| = |A|/2$. For this case to occur, A must have even cardinality at least 6, and S is the union of two cosets of H. Note that if B met at least three cosets of H then at least three cosets of H would be represented in S. Thus, B meets exactly two cosets Q_1, Q_2 of H. Likewise, if B has at least two elements in each of Q_1 and Q_2 then at least three cosets of H would be represented in S (the equality $2Q_1 = 2Q_2$ may not hold, as in this case B, and therefore S, would be contained in a coset of a subgroup of G, and

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

so $|H| = |S| = |A|$, which brings us back to Case I). The only remaining case is that B contains a coset Q_1 of H and a single element of Q_2. In particular $|A|/2 = |H| \in C(A)$. If $|A| \in C(A)$ then A is a coset of a subgroup of G, as required. If $|A| \notin C(A)$ then it follows from Lemma 4.3 that $|k \wedge A| > |A|$, a contradiction.

Case III. $|H| = |A|/3$. In this case $|A|/3 = |H| \geqslant \lceil (|A| - 3)/2 \rceil$, which implies that $|A| \leqslant 9$ and that $|A|$ is a multiple of 3, and so $|A| \in \{6, 9\}$. If $|A| = 9$, then we have that $|B| = 6$, $|S| = 9$, $|C| = |H| = 3$ and $k \in \{3, 4\}$. We consider first the case $k = 3$, so that $|3 \wedge A| = |A|$. By considering the sizes of C and S we see that C is equal to a coset Q_0 of H and S is a union of three cosets of H. If B meets at least three cosets of H, say elements $b_1, b_2, b_3 \in B$ belong to distinct cosets of H. Then

$$2 \wedge Q_0 + b_1,\ 2 \wedge Q_0 + b_2,\ 2 \wedge Q_0 + b_3 \quad \text{and} \quad 3 \wedge Q_0$$

are disjoint subsets of $3 \wedge A$ with cardinalities $3, 3, 3, 1$ respectively, so that $|3 \wedge A| \geqslant 10 > 9 = |A|$, a contradiction. On the other hand, if B meets only two cosets Q_1, Q_2 of H, then $B = Q_1 \cup Q_2$, and $A = Q_0 \cup Q_1 \cup Q_2$. If $Q_0 \cup Q_1 \cup Q_2$ is a coset of a subgroup of G then we are done, so we may suppose (by relabelling if necessary) that $2Q_1 \neq Q_0 + Q_2$. In this case

$$Q_0 + Q_1 + Q_2,\ Q_0 + 2 \wedge Q_1,\ 2 \wedge Q_1 + Q_2 \quad \text{and} \quad 3 \wedge Q_1$$

are disjoint subsets of $3 \wedge A$ with cardinalities $3, 3, 3, 1$, so that $|3 \wedge A| \geqslant 10 > 9 = |A|$, a contradiction.

Since the arguments for the case $|A| = 9$ and $k = 4$ and the case $|A| = 6$ are similar to those given above we do not give them in full here, but they may be easily verified by the reader. □

5. A sequence version of Theorem 1.1

In this section we prove an analogue of Theorem 1.1 for sequences (or multisets). We denote by $S(A)$ the support of the sequence A. Note that $|A|$ now denotes the number of elements in the sequence A. The following result is mainly an easy consequence of Theorem 1.1. However, a few special cases do need to be considered separately. In the case that $|A| = |S(A)|$ then $A = S(A)$, and one may refer directly to Theorem 1.1.

Given a sequence A, we write $S_j(A)$ for the set of elements that appear at least j times in A.

Theorem 5.1. *Let A be a sequence over G with $|A| > |S(A)|$ and let $2 \leqslant k \leqslant |A| - 2$. Then*

$$|k \wedge A| \geqslant |S(A)|$$

with equality if and only if one of the following holds.

(i) *$S(A)$ is a coset of a subgroup of G.*
(ii) *$|S(A)| = 2$ and $|S_2(A)| = 1$.*
(iii) *$S(A)$ is an arithmetic progression of length three, and $S_2(A)$ contains only the middle term of the progression.*

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

Proof. As usual it suffices to prove the result for $k \in \{2, \ldots, \lfloor |A|/2 \rfloor\}$. We first deal with the cases where $|S(A)|$ is small. If $|S(A)| = 1$ then the inequality trivially holds as an equality and $S(A)$ is a coset of the trivial subgroup.

If $|S(A)| = 2$, say $S(A) = \{x, y\}$, then without loss of generality the sequence A contains a subsequence $A' = x, x, y$. Then, either $k = 2$ and we readily obtain $|2 \wedge A| \geqslant |2 \wedge A'| = 2$, or $k \geqslant 3$ and there is a subsequence $a_1, \ldots, a_{k-2}$ of A which is disjoint from A' and yields $|k \wedge A| \geqslant |2 \wedge A'| = 2$. If $S(A)$ is not a coset of a subgroup and $|S_2(A)| = 2$, then A contains a subsequence $A' = x, x, y, y$ and, arguing as above, $|k \wedge A| \geqslant |2 \wedge A'| = 3$. Reciprocally, it can easily be checked that $|k \wedge A| = 2$ whenever $|S_2(A)| = 1$ or $S(A)$ is a coset of a subgroup.

If $|S(A)| = 3$, say $S(A) = \{x, y, z\}$, then A contains a subsequence $A' = x, y, z$. Now, either $k = 2$ and we have $|2 \wedge A| \geqslant |2 \wedge A'| = 3$, or $k \geqslant 3$ and there is a subsequence $a_1, \ldots, a_{k-2}$ of A which is disjoint from A' and gives $|k \wedge A| \geqslant |2 \wedge A'| = 3$. In addition, if $S(A)$ is not an arithmetic progression of length three then A contains a subsequence of the form $A' = x, y, y, z$ and, arguing as above, $|k \wedge A| \geqslant |2 \wedge A'| = 4$. If $S(A)$ is not a coset of a subgroup but an arithmetic progression of length three such that an element other than the middle term is represented at least twice in A, say A contains $A' = x, x, y, z$, then $|k \wedge A| \geqslant |2 \wedge A'| = 4$. Reciprocally, it can easily be checked that $|k \wedge A| = 3$ whenever $S(A)$ is a coset of a subgroup or an arithmetic progression of length three such that $S_2(A)$ contains only the middle term of the progression.

From now on, we assume $|S(A)| \geqslant 4$. When $k = 2$, we consider two cases. If $S(A)$ is a 2-coset, an almost 2-coset or a union of two cosets of a subgroup of order 2, then it is easily seen that, since $|A| > |S(A)|$, the sequence A has at least one more 2-sum than $S(A)$, which gives the required result for these cases. Otherwise, the desired result follows immediately from Theorem 1.1.

Now suppose $3 \leqslant k \leqslant \lfloor |A|/2 \rfloor$. If $|S(A)| = 4$, say $S(A) = \{w, x, y, z\}$, then A contains a subsequence $A' = w, x, y, z$. First, one can readily notice that if $S(A)$ is a coset of a subgroup then the desired inequality holds as an equality. Therefore, we now assume that $S(A)$ is not a coset of a subgroup and consider the following two cases. If $S(A)$ is not the union of two cosets of a subgroup of order 2 then there is a subsequence $a_1, \ldots, a_{k-2}$ of A which is disjoint from A', and it follows from Theorem 1.1 that $|k \wedge A| \geqslant |2 \wedge A'| \geqslant 5$. If $S(A)$ is the union of two cosets of a subgroup of order 2, then without loss of generality A contains a subsequence $A' = w, w, x, y, z$. Now, either $k = 3$ and we readily obtain $|3 \wedge A| \geqslant |3 \wedge A'| = |2 \wedge A'| \geqslant 5$, or $k \geqslant 4$ and there is a subsequence $a_1, \ldots, a_{k-3}$ of A which is disjoint from A'. Therefore, $k \wedge A$ contains a translate of $3 \wedge A'$, so that $|k \wedge A| \geqslant |3 \wedge A'| = |2 \wedge A'| \geqslant 5$.

We now consider the remaining case where $|S(A)| \geqslant 5$. If $3 \leqslant k \leqslant |S(A)| - 3$, then the result follows immediately from Theorem 1.1, by simply observing that $|k \wedge A| \geqslant |k \wedge S(A)|$.

If $|S(A)| - 2 \leqslant k \leqslant \lfloor |A|/2 \rfloor$, let A' be a subsequence of A with $A' = S(A') = S(A)$. Since $|A| - |S(A)| \geqslant 2k - |S(A)| \geqslant k - 2$, there is a subsequence $a_1, \ldots, a_{k-3}$ of A which is disjoint from A'. Thus, it follows from Theorem 1.1 that $|k \wedge A| \geqslant |3 \wedge A'| \geqslant |S(A)|$. Furthermore, if $S(A)$ is not a coset of a subgroup then Theorem 1.1 gives a strict inequality. □

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

6. Concluding remarks

The results of this paper establish that an additive set A has at least $|A|$ k-sums unless $k \in \{2, |A|-2\}$ and A is a 2-coset, and strictly more than $|A|$ k-sums except in a few specific cases. Though these results are precise in the cases they deal with, we expect that stronger bounds are true in general. For example, one might hope to prove an analogue of (1.1) for additive subsets A of general abelian groups. Indeed, Alon, Nathanson and Ruzsa [2] asked this question for $G = \mathbb{Z}_n$, where n is not necessarily prime.

In another direction one might ask what cardinality of a subset A of an abelian group G ensures that A covers G with its k-sums. For example, it is easily observed that if G is of odd order and $|A| \geqslant (|G|+3)/2$, then $2 \wedge A = G$ (see [10, Lemma 2.2] or [12, Lemma 3.2]). One might expect that the condition $|A| \geqslant (|G|+3)/2$ should be sufficient to guarantee that $k \wedge A = G$ for all $k \in \{2, \ldots, |A|-2\}$, and in any abelian group G of odd order. However, this is not the case in $G = \mathbb{Z}_3^2$, where, taking A to be the union of two cosets of a subgroup of order 3, we have that $|A| = 6 = (|G|+3)/2$, but $|3 \wedge A| = 7 < 9 = |G|$. Yet, we believe this result should hold in all abelian groups of sufficiently large odd order.

In the case that $k > 2$ one might even expect that weaker conditions also imply that $k \wedge A = G$. For example, Lev [14] proved that if G has sufficiently large odd order and $|A| > 2|G|/5$ then $3 \wedge A = G$. Furthermore, the condition $|A| > 2|G|/5$ may be weakened to $|A| > 5|G|/13$ provided that A is not a union of two cosets of a subgroup of order 5. This suggests the following general problem.

Problem 6.1. *Determine* $c_k := \limsup_{m\to\infty} c_k(2m+1)$ *for each* $k \in \mathbb{N}$, *where*

$$c_k(n) := \inf\{c : A \subseteq G, |G| = n, |A| > c|G| \Rightarrow k \wedge A = G\}.$$

Acknowledgements

The present paper is the first part of a joint work with Yahya ould Hamidoune. Our research project was ongoing when he passed away in March 2011. He will keep on being a living source of inspiration to us, and we would like to express all our gratitude for his constant mathematical enthusiasm.

References

[1] Alon, N. (1999) Combinatorial Nullstellensatz. *Combin. Probab. Comput.* **8** 7–29.
[2] Alon, N., Nathanson, M. B. and Ruzsa, I. (1996) The polynomial method and restricted sums of congruence classes. *J. Number Theory* **56** 404–417.
[3] Bollobás, B. and Leader, I. (1999) The number of k-sums modulo k. *J. Number Theory* **78** 27–35.
[4] Cauchy, A. (1813) Recherches sur les nombres. *J. École Polytechnique* **9** 99–116.
[5] Davenport, H. (1935) On the addition of residue classes. *J. London Math. Soc.* **10** 30–32.
[6] Dias da Silva, J. A. and Hamidoune, Y. O. (1994) Cyclic spaces for Grassmann derivatives and additive theory. *Bull. London Math. Soc.* **26** 140–146.
[7] Diderrich, G. T. (1973) Sums of length t in abelian groups. *Israel J. Math.* **14** 14–22.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press

[8] Erdős, P., Ginzburg, A. and Ziv, A. (1961) Theorem in the additive number theory. *Bull. Res. Council Israel* (F) **10** 41–43.
[9] Erdős, P. and Heilbronn, H. (1964) On the addition of residue classes mod p. *Acta Arith.* **9** 149–159.
[10] Gallardo, L., Grekos, G., Habsieger, L., Hennecart, F., Landreau, B. and Plagne, A. (2002) Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős–Ginzburg–Ziv problem. *J. London Math. Soc.* **65** 513–523.
[11] Gao, W. and Geroldinger, A. (2006) Zero-sum problems in finite abelian groups: A survey. *Expo. Math.* **24** 337–369.
[12] Hamidoune, Y. O. (1998) Adding distinct congruence classes. *Combin. Probab. Comput.* **7** 81–87.
[13] Hamidoune, Y. O., Lladó, A. S. and Serra, O. (2000) On restricted sums. *Combin. Probab. Comput.* **9** 513–518.
[14] Lev, V. F. (2002) Three-fold restricted set addition in groups. *European J. Combin.* **23** 613–617.
[15] Lev, V. F. (2005) Restricted set addition in abelian groups: Results and conjectures. *J. Théor. Nombres Bordeaux* **17** 181–193.
[16] Mann, H. B. and Olson, J. E. (1967) Sums of sets in the elementary abelian group of type (p, p). *J. Combin. Theory* **2** 275–284.
[17] Petridis, G. New proofs of Plünnecke-type estimates for product sets in groups. `arXiv:1101.3507 [math.CO]`
[18] Ruzsa, I. (2009) Sumsets and structure. In *Combinatorial Number Theory and Additive Group Theory* (A. Geroldinger and I. Ruzsa, eds), Birkhäuser, pp. 87–210.
[19] Tao, T. and Vu, V. (2006) *Additive Combinatorics*, Cambridge University Press.
[20] Wang, G. (2008) On restricted sumsets in abelian groups of odd order. *Integers* **8** #A22.

https://doi.org/10.1017/S0963548312000168 Published online by Cambridge University Press