



HAL
open science

k-sums in abelian groups

Benjamin Girard, Simon Griffiths, Yahya Ould Hamidoune

► **To cite this version:**

Benjamin Girard, Simon Griffiths, Yahya Ould Hamidoune. k-sums in abelian groups. 2011. hal-00630441v1

HAL Id: hal-00630441

<https://hal.sorbonne-universite.fr/hal-00630441v1>

Preprint submitted on 10 Oct 2011 (v1), last revised 26 Jun 2012 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

k -sums in abelian groups

Benjamin Girard ^{*} Simon Griffiths [†] Yahyaould Hamidoune

Abstract

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 $|k \wedge A| \geq |A|$ for all $k \in \{2, \dots, |A| - 2\}$, unless $k \in \{2, |A| - 2\}$ and A is a coset of an elementary 2-subgroup of G . Furthermore, we characterise those finite sets $A \subseteq G$ for which $|k \wedge A| = |A|$ for some $k \in \{2, \dots, |A| - 2\}$. This result answers a question of Diderrich. Our proof relies on an elementary property of proper edge-colourings of the complete graph.

1 Introduction

Sumsets are a central object of study in the area of Additive Combinatorics. In particular, the sumset

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

and the k -fold sumset

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

of subsets A, B of an abelian group G have been extensively studied. For background and a selection of reference we refer the reader to the course of Ruzsa [18] and the book of Tao and Vu [19]. See also the recent results of Petridis [16, 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 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 [14] and the articles of Lev [13], Hamidoune, Lladó and Serra [11], and Gallardo, Grekos, Habsieger, Hennecart, Landreau and Plagne [9]. 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

^{*}IMJ, Équipe Combinatoire et Optimisation, Université Pierre et Marie Curie (Paris 6), 4 place Jussieu, 75005 Paris, France, email: bgirard@math.jussieu.fr.

[†]IMPA, Estrada Dona Castorina 110, Rio de Janeiro, Brasil, 22460-320, email: sgriff@impa.br. Research supported by CNPq Proc. 500016/2010-2.

is a k -sum, see the seminal article of Erdős, Ginzburg and Ziv [7], the article of Bollobás and Leader [2], the survey of Gao and Geroldinger [10] 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 [3, 4] that the inequality

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

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 [5] proved that the inequality

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

holds for each $k \in \mathbb{N}$ and subset $A \subseteq \mathbb{Z}_p$ (p prime). This result was proved by resolving a general problem on Grassmann spaces, and the case $k = 2$ confirmed a conjecture of Erdős and Heilbronn [8]. An alternative proof, using the Combinatorial Nullstellensatz, was then given by Alon, Nathanson and Ruzsa [1].

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

$$|k \wedge A| \geq |A|$$

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 2-cosets of order 2.*

Remark 1. The first part of Theorem 1.1 was first proved by Mann and Olson [15] in the case that $G = \mathbb{Z}_p$ (p prime), and by Diderrich [6] in the case that G has no 2-torsion. Wang [20] rediscovered the result of Diderrich and proved that equality occurs only if A is a coset of a subgroup of G .

Remark 2. Diderrich's proof is inductive and for this reason he actually proved a slightly more general result in which $|k \wedge A|$ and $|A|$ are replaced by $|\sigma(k \wedge A)|$ and $|\sigma(A)|$ where $\sigma : G \rightarrow G/H$ is a canonical homomorphism. Alternatively, this result may be viewed as a sequence version of the original result. 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

$$a_1 + \cdots + a_{k-2} + 2 \wedge B \subseteq k \wedge A \quad (2)$$

for any distinct elements a_1, \dots, 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 $|A| \geq 5$, then*

(i) *if $|2 \wedge A| \geq |A|$, there is a subset $B \subseteq A$ with $|B| = \lfloor (|A| + 3)/2 \rfloor$ such that $|2 \wedge B| \geq |A|$, and*

(ii) *if $|2 \wedge A| < |A|$, 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 (2), together with Proposition 1.2, the implication

$$|2 \wedge A| \geq |A| \quad \Rightarrow \quad |k \wedge A| \geq |A|$$

holds for all $k \in \{2, \dots, \lfloor |A|/2 \rfloor\}$. By considering also the symmetry $|k \wedge A| = |(|A| - k) \wedge A|$, we observe that the implication holds for all $k \in \{2, \dots, |A| - 2\}$. Except for the special case that 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 characterisation of the cases of the equality $|k \wedge A| = |A|$, again uses Proposition 1.2, however on this occasion we consider not only a single $(k - 2)$ -sum of $A \setminus B$ (as in (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.

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.

Proposition 1.3. *Let $n \geq 5$ be a natural number and let $c : E(K_n) \rightarrow \mathbb{N}$ be a proper edge-colouring of the complete graph on n vertices, then*

- (i) if at least n colours are used by c , there is a subset $U \subseteq V(K_n)$ with $|U| = \lfloor (n+3)/2 \rfloor$ on which c uses at least n colours, and
- (ii) if c uses less than n colours, there is a subset $U \subseteq A$ with $|U| = n/2 + 1$ on which c uses $n - 1$ colours.

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 $|2 \wedge A| < |A|$ 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. \square

We now characterise subsets of 2-cosets for which the inequality $|2 \wedge A| \leq |A|$ 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 $\{x_1, \dots, x_d\}$ is a minimal subset of A such that $H = \langle x_1, \dots, x_d \rangle$, and that $|H \setminus A| \geq 2$ (as there is nothing to prove if A is a 2-coset or almost 2-coset). Let $I \subseteq [d]$ be minimal such that $\sum_I x_i \notin A$, and let $J \subseteq [d]$ be minimal such that $J \neq I$ and $\sum_J x_j \notin A$. By minimality both $\sum_I x_i$ and $\sum_J x_j$ may be expressed as sums of two distinct elements of A . Thus,

$$2 \wedge A \supseteq (A \setminus \{0\}) \cup \left\{ \sum_I x_i, \sum_J x_j \right\},$$

and so $|2 \wedge A| > |A|$. □

We now establish two lemmas that will help us characterise 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*

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

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 $2x = y + z$.

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 $|2 \wedge A| \geq 2|C| - 1 \geq 2|A| - 3 > |A|$, 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 $|2 \wedge A| \geq 2|C| - 1 \geq 2|A| - 5$, which is a contradiction unless $|A| = 5$. In the case $|A| = 5$ we note that the subset C has cardinality

3, and so $|2 \wedge A| \geq 3 + 3 > |A|$, 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

$$y + z = y + y_2 + z - y_2 = x + u + z - y_2 = x + x + y_2 - y_2 = 2x.$$

□

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 2-cosets 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 $2y = 2z$, as required. □

3 Proof of Proposition 1.2

In this section we prove Proposition 1.2. Most of the work goes into proving Proposition 1.3. Let us note immediately that Proposition 1.2 follows from Proposition 1.3.

Proof of Proposition 1.2. Let $A \subseteq G$ be an additive set of cardinality $n \geq 5$. 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 $|2 \wedge A| \geq |A|$ then at least $n = |A|$ colours are used in the colouring described above. By Proposition 1.3 there exists a subset $B \subseteq A$ of cardinality $\lfloor (n+3)/2 \rfloor$ on which at least n colours are used. Translating back to additive language, this says precisely that $|2 \wedge B| \geq n = |A|$, as required.

(ii) If $|2 \wedge A| < |A|$ then fewer than $n = |A|$ colours are used in the colouring described above. By Proposition 1.3 there exists a subset $B \subseteq A$ of cardinality $n/2 + 1$ on which at least n colours are used. 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 U to be a uniformly random subset of the appropriate cardinality and prove a lower bound on the expected number of colours used in U . The following lemma will help us prove the required bound on the expectation.

Lemma 3.1. *Given a pair (a, n) of natural numbers, with $n \geq 5$ and $a \leq n/2$, let $p(a, n)$ be the probability that a uniformly random subset of $\{1, \dots, n\}$ of size $\lfloor (n+3)/2 \rfloor$ contains at least one of the pairs $\{1, 2\}, \dots, \{2a-1, 2a\}$. Then*

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

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

Remark 3. Since the pairs $\{1, 2\}, \dots, \{2a-1, 2a\}$ play no special role, $p(a, n)$ is also the probability that the random subset contains at least one of the pairs e_1, \dots, e_a , for any set of a disjoint pairs e_1, \dots, e_a .

Proof of Lemma 3.1. We observe immediately that the $p(a, n) = 1$ in the case that a is equal to $n/2$ (n even) or $(n-1)/2$ (n odd). Thus it remains to prove the bound for pairs (a, n) with $1 \leq a \leq (n-2)/2$. Since the bound can easily be verified for all such pairs with $n \leq 10$, it suffices to prove the following two claims.

Claim 1: The inequality $1 - p(a, n) \leq (\frac{3}{4})^a$ holds for all pairs (a, n) , with $1 \leq a \leq (n-2)/2$, and the stronger inequality $1 - p(a, n) \leq \frac{1}{2}(\frac{3}{4})^{a-1}$ holds for all pairs (a, n) , with $(n-3)/2 \leq a \leq (n-2)/2$.

Proof of Claim 1: The proof is straightforward, we simply observe that if none of the pairs $\{1, 2\}, \dots, \{2a-3, 2a-2\}$ lie in U then the conditional probability that $\{2a-1, 2a\} \subseteq U$ is at least $1/4$. Since the base case ($a = 1$) also holds, i.e.,

$$\mathbb{P}(\{1, 2\} \subseteq U) = \frac{\binom{\lfloor (n+3)/2 \rfloor}{2}}{\binom{n}{2}} \geq \frac{1}{4},$$

it follows immediately by induction on a that

$$1 - p(a, n) \leq \left(\frac{3}{4}\right)^a$$

holds for all pairs (a, n) , with $1 \leq a \leq (n-2)/2$.

For the second part, argue exactly as before and use the additional observation that the conditional probability that $\{2\lfloor (n-2)/2 \rfloor - 1, 2\lfloor (n-2)/2 \rfloor\} \subseteq U$ given that no previous pair is contained in U is at least $\binom{3}{2}/\binom{4}{2} = \frac{1}{2}$ (for n even) and $\binom{4}{2}/\binom{5}{2} \geq \frac{1}{2}$ (for n odd). The Claim is proved.

Claim 2: The inequality $1 - (\frac{3}{4})^a > 2a/n$ holds for all pairs (a, n) with $1 \leq a \leq (n-4)/2$ and $n \geq 11$, and the inequality $1 - \frac{1}{2}(\frac{3}{4})^{a-1} > 2a/n$ holds for all pairs (a, n) with $1 \leq a \leq (n-2)/2$ and $n \geq 11$.

Proof of Claim 2: We begin by proving the first part by induction. The base cases, $(a, n) = (1, 11), (2, 11), (3, 11), (1, 12), (2, 12), (3, 12), (4, 12)$, can be checked by hand. Since $2a/n$

is decreasing in n , it suffices to prove the induction step $(a, n) \rightarrow (a+1, n+2)$. By the induction hypothesis we have that

$$\left(\frac{3}{4}\right)^a < \frac{n-2a}{n},$$

and so

$$\left(\frac{3}{4}\right)^{a+1} < \frac{3n-6a}{4n} = \frac{3(n+2)}{4n} \left(1 - \frac{2(a+1)}{n+2}\right).$$

The induction step, and therefore the proof of the first part, is now completed since $(3n+6)/4n \leq 1$ for all $n \geq 6$.

The second part follows from the first for pairs (a, n) with $a \leq (n-4)/2$. Our proof of the remaining cases is identical to the above proof, except that now the base cases for the induction are $(a, n) = (4, 11), (5, 12)$. This completes the proof of Claim 2 and also the proof of the lemma. \square

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

Proof of Proposition 1.3. (i) Let U be a uniformly randomly selected vertex subset 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 U is

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

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 U is greater than $n - 1$. In particular, there exists a set U of $\lfloor (n+3)/2 \rfloor$ vertices on which n colours are used.

(ii) Since each colour may be used at most $n/2$ times (with equality only if the edges of the colour class form a matching) and fewer than n colours are used by c , it follows that n must be even, $n - 1$ colours are used and each colour class is a perfect matching. It is then easily observed that *every* set U of $n/2 + 1$ vertices contains an edge from each of the $n - 1$ colour classes. \square

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 $2 \leq k \leq |A| - 2$. Then the inequality*

$$|k \wedge A| \geq |A|$$

holds, 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 $2 \leq k \leq \lfloor |A|/2 \rfloor$. The $k = 2$ case is precisely Lemma 2.2. For $k \in \{3, \dots, \lfloor |A|/2 \rfloor\}$ we consider the following two cases. (Note that since $k \geq 3$ we may assume $|A| \geq 5$.)

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

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

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

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 the second part of Proposition 1.2, 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, \dots, c_{k-1} be distinct elements of $A \setminus B$ and note that the sets

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

are not identical, since $c_{k-1} - c_1 \notin \text{Stab}(2 \wedge B) = \{0\}$. Finally, since $k \wedge A$ contains both these sets we deduce that $|k \wedge A| \geq |A|$. \square

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 be a coset of a subgroup H of an abelian group G , and let $k \in \{1, \dots, |Q| - 1\}$. 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. \square

We now prove a lemma that will help us in characterising 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: $|A| \in C(A)$ 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 $k \in \{3, \dots, |A| - 3\}$.*

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 $|k \wedge A| \geq 3|A|/2$. 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.

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 $k \in \{3, \dots, \lfloor |A|/2 \rfloor\}$. We divide into 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

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

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

Case II: A is the union of two cosets Q_1, Q_2 of H and $k \geq 4$. Since $k \geq 4$ we may assume $|A| \geq 8$, and so $|H| \geq 4$. 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 that

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

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 $|k \wedge A| \geq 3|H| > |A|$, 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, $|k \wedge A| \geq 3|H| - 3$. If $|A| > 6$, then $3|H| - 3 > |A|$ and the proof is complete. If $|A| = 6$ then $|H| = 3$ (not a power of 2), so that Corollary 4.2 gives the stronger conclusion that each of the three sets mentioned above has cardinality at least $|H|$, and so $|k \wedge A| \geq 3|H| = 3|A|/2 > |A|$, and the proof is complete. \square

We are now ready to characterise 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 $k \in \{2, \dots, |A| - 2\}$. By Proposition 4.1, the inequality

$$|k \wedge A| \geq |A|$$

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

Now suppose that the equality $|k \wedge A| = |A|$ holds for some $k \in \{2, \dots, |A| - 2\}$. Then in particular the equality holds for some $k \in \{2, \dots, \lfloor |A|/2 \rfloor\}$. If $k = 2$, then either $|A| = 4$ and A is a union of two 2-cosets of order 2 by Lemma 2.5, or $|A| \geq 5$ and 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 $k \in \{3, \dots, \lfloor |A|/2 \rfloor\}$. 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 $|2 \wedge A| \geq |A|$ and (by Proposition 1.2) that $|2 \wedge B| \geq |A|$ 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 inequalities $|S + C| = |S|$ or $|S - C| = |S|$ holds. If $k = 3$, then $S + C$ is a subset of $k \wedge A$ and so

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

If $k \in \{4, \dots, \lfloor |A|/2 \rfloor\}$, we instead 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

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

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

It follows from the claim that $|H|$ divides $|S| = |A|$, and $|H| \geq |C| = \lfloor (|A| - 3)/2 \rfloor$. 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 so $|H| = |S| = |A|$ and we are in 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 $|A|/3 = |H| \geq \lceil (|A| - 3)/2 \rceil$, which implies that $|A| \leq 9$ 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. Implying $|3 \wedge A| \geq 10 > 9 = |A|$, 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. Implying $|3 \wedge A| \geq 10 > 9 = |A|$, a contradiction.

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

5 A sequence version of Theorem 1.1

In this section we prove that Theorem 1.1 holds when A is allowed to be a sequence (or multiset). We denote by $\text{Supp}(A)$ the support of the sequence A . Note that $|A|$ now denotes the number of elements in the sequence A . The following result is easily deduced from Theorem 1.1. In the case that $|A| = |\text{Supp}(A)|$ then $A = \text{Supp}(A)$ and one may refer directly to Theorem 1.1.

Theorem 5.1. *Let $A \subseteq G$ be a sequence with $|A| > |\text{Supp}(A)|$ and let $2 \leq k \leq |A| - 2$. Then*

$$|k \wedge A| \geq |\text{Supp}(A)|$$

in all cases. Furthermore

$$|k \wedge A| > |\text{Supp}(A)|$$

unless $\text{Supp}(A)$ is a coset of a subgroup of G .

Proof. As usual it suffices to prove the result for $k \in \{2, \dots, \lfloor |A|/2 \rfloor\}$.

If $k = 2$, then consider two cases. If $\text{Supp}(A)$ is not a 2-coset, almost 2-coset or union of two 2-cosets of order 2, then the required result follows immediately from Theorem 1.1. If, on the other hand, $\text{Supp}(A)$ is equal to one of these, then simply observe that in each of these cases any sequence A with $|A| > |\text{Supp}(A)|$ has at least one more 2-sum than $\text{Supp}(A)$. This completes the proof for the case $k = 2$.

If $3 \leq k \leq |\text{Supp}(A)| - 3$, then the result follows immediately from Theorem 1.1, simply observe that $|k \wedge A| \geq |k \wedge \text{Supp}(A)|$.

If $|\text{Supp}(A)| - 2 \leq k \leq \lfloor |A|/2 \rfloor$, then $|A| \geq k + 3$ and so

$$|A| - |\text{Supp}(A)| \geq k - (|\text{Supp}(A)| - 3).$$

Therefore, setting $\ell = |\text{Supp}(A)| - 3$, there is a subsequence $a_1, \dots, a_{k-\ell}$ of A such that $\text{Supp}(A \setminus \{a_1, \dots, a_{k-\ell}\}) = \text{Supp}(A)$. Now, since

$$k \wedge A \supseteq a_1 + \dots + a_{k-\ell} + \ell \wedge \text{Supp}(A),$$

it suffices to prove the claims in the theorem with $|\ell \wedge \text{Supp}(A)|$ in place of $|k \wedge A|$. Except for the special case that $|\text{Supp}(A)| = 5$ we have that $\ell = |\text{Supp}(A)| - 3 \notin \{2, |\text{Supp}(A)| - 2\}$ and so the claims follow from Theorem 1.1. The claims also follow in the case that $|\text{Supp}(A)| = 5$ since none of the special cases of Theorem 1.1 apply to sets of cardinality 5. \square

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) for additive subsets A of general abelian groups. Indeed, Alon, Nathanson and Ruzsa [1] asked this question for $G = \mathbb{Z}_n$, where n is not necessarily prime, and Hamidoune, Lladó and Serra [12] conjectured (1) still holds for sets of units modulo n .

Conjecture 6.1 ([12]). *Let A be a subset of \mathbb{Z}_n^* and let $k \in \mathbb{N}$. Then $|k \wedge A| \geq \min\{n, k(|A| - k) + 1\}$.*

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 $2 \wedge A = G$ whenever G is of odd order and $|A| \geq (|G| + 3)/2$. (In fact this is a special case of [9, Lemma 2.2].) One might expect that the condition $|A| \geq (|G| + 3)/2$ should be sufficient to guarantee that $k \wedge A = G$ for all $k \in \{2, \dots, |A| - 2\}$, 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 one has that $|A| = 6 = (|G| + 3)/2$, but $|3 \wedge A| = 7 < 9 = |G|$. However, 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 [13] 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 6.2. Determine $c_k := \limsup_{m \rightarrow \infty} c_k(2m+1)$ for each $k \in \mathbb{N}$, where

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

Acknowledgments

The present paper is the first part of a joint work with Yahyaould 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] N. ALON, M. B. NATHANSON AND I. RUZSA *The polynomial method and restricted sums of congruence classes*, J. Number Theory **56** (1996), 404-417.
- [2] B. BOLLOBÁS AND I. LEADER *The number of k -sums modulo k* , J. Number Theory **78** no. 1 (1999), 27-35.
- [3] A. CAUCHY *Recherches sur les nombres*, J. École Polytechnique **9** (1813), 99-116.
- [4] H. DAVENPORT *On the addition of residue classes*, J. Lond. Math. Soc. **10** (1935), 30-32.
- [5] J. A. DIAS DA SILVA AND Y. O. HAMIDOUNE *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc. **26** (1994), 140-146.
- [6] G. T. DIDERRICH *Sums of length t in abelian groups*, Israel J. Math. **14** (1973), 14-22.
- [7] P. ERDŐS, A. GINZBURG AND A. ZIV *Theorem in the additive number theory*, Bull. Res. Council Israel (F) **10** (1961), 41-43.
- [8] P. ERDŐS AND H. HEILBRONN *On the addition of residue classes mod p* , Acta Arith. **9** (1964), 149-159.
- [9] L. GALLARDO, G. GREKOS, L. HABSIEGER, F. HENNECART, B. LANDREAU AND A. PLAGNE *Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős-Ginzburg-Ziv problem*, J. London Math. Soc. **65** no. 2 (2002), 513-523.
- [10] W. GAO AND A. GEROLDINGER *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** no. 4 (2006), 337-369.
- [11] Y. O. HAMIDOUNE, A. S. LLADÓ AND O. SERRA *On restricted sums*, Combin. Probab. Comput. **9** no. 6 (2000), 513-518.

- [12] Y. O. HAMIDOUNE, A. S. LLADÓ AND O. SERRA *On complete subsets of the cyclic group*, J. Combin. Theory Ser. A **115** (2008), 1279-1285.
- [13] V. F. LEV *Three-fold restricted set addition in groups*, European J. Combin. **23** (2002), 613-617.
- [14] V. F. LEV *Restricted set addition in abelian groups: results and conjectures*, J. Théor. Nombres Bordeaux **17** (2005), 181-193.
- [15] H. B. MANN AND J. E. OLSON *Sums of sets in the elementary abelian group of type (p, p)* , J. Combinatorial Theory **2** (1967), 275-284.
- [16] G. PETRIDIS *New proofs of Plünnecke-type estimates for product sets in groups*, arXiv:1101.3507 [math.CO]
- [17] G. PETRIDIS *Upper bounds on the cardinality of higher sumsets*, arXiv:1101.5001 [math.CO]
- [18] I. RUZSA *Sumsets and structure*, In A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics, CRM Barcelona, Birkhäuser (2009), 87-210.
- [19] T. TAO AND V. VU *Additive Combinatorics*, Cambridge University Press (2006).
- [20] G. WANG *On restricted sumsets in abelian groups of odd order*, Integers **8** (2008), #A22.