Combinatorics, Probability and Computing (2000) 9, 513–518. Printed in the United Kingdom

On Restricted Sums

Y. O. HAMIDOUNE,[1] A. S. LLADÓ[2]† and O. SERRA[2]†

[1] UFR 921, E. Combinatoire , Université Pierre et Marie Curie,
4 Place Jussieu, 75005 Paris, France
(e-mail: yha@ccr.jussieu.fr)

[2] Dep. Matematica Aplicada i Telematica, Universitat Politècnica de Catalunya,
Jordi Girona, 1, 08034 Barcelona, Spain
(e-mail: allado@mat.upc.es, oserra@mat.upc.es)

Received 12 July 1999; revised 29 September 1999

Let G be an abelian group. For a subset $A \subset G$, denote by $2 \wedge A$ the set of sums of two *different* elements of A. A conjecture by Erdős and Heilbronn, first proved by Dias da Silva and Hamidoune, states that, when G has prime order, $|2 \wedge A| \geqslant \min(|G|, 2|A| - 3)$.

We prove that, for abelian groups of odd order (respectively, cyclic groups), the inequality $|2 \wedge A| \geqslant \min(|G|, 3|A|/2)$ holds when A is a generating set of G, $0 \in A$ and $|A| \geqslant 21$ (respectively, $|A| \geqslant 33$). The structure of the sets for which equality holds is also determined.

1. Introduction

Let p be a prime and let A be a subset of $\mathbf{Z}/p\mathbf{Z}$. It was conjectured by P. Erdős and H. Heilbronn that $|2 \wedge A| \geqslant \min(p, 2|A| - 3)$. This conjecture was proved by J. Dias da Silva and one of the authors in [2] using linear algebra. Another proof was obtained later by N. Alon, M. B. Nathanson and I. Z. Ruzsa [1] using the polynomial method.

We obtain in this paper lower bounds for $|2 \wedge A|$, where A is a finite subset of an abelian group. Clearly, $|2 \wedge A| = |2 \wedge (A - x)|$, for every $x \in A$. Therefore one may assume that $0 \in A$. Moreover, we can restrict ourselves to the group generated by A. Therefore, one can also assume without loss of generality that A generates G.

Let $\mathscr{E}$ denote the set of subsets of G that are of the form $H \cup x + H$, where H is a subgroup of G. Then, for a set $A \in \mathscr{E}$, we have $2 \wedge A \subset H \cup H + x \cup H + 2x$. In particular $|2 \wedge A| \leqslant 3|A|/2$.

Our main result shows that $|2 \wedge A| \geqslant \min(|G|, 3|A|/2)$, for any finite generating subset A, provided $|A|$ is large enough. As a corollary we obtain the following result.

† Supported by the Spanish Research Council, CICYT, under project TIC97-0963.

Let G be a cyclic group (respectively, an abelian group of odd order), and let A be a generating subset of G such that $0 \in A$. If $|A| \geqslant 21$ (respectively, $|A| \geqslant 33$), then

$$|2 \wedge A| \geqslant \min(|G|, 3|A|/2). \tag{1.1}$$

Moreover, we prove that the above bound can only be achieved by members of $\mathscr{E}$ when $|A| \geqslant 33$.

2. Preliminaries

We need the following well-known theorem of Kneser.

Theorem 2.1 (Kneser [5, 6]). *Let A, B be finite nonempty subsets of an abelian group G. Then there is a subgroup H such that $A+B+H = A+B$ and $|A+B| \geqslant |A+H|+|B+H|-|H|$.*

Corollary 2.2. *Let A be a finite generating subset of an abelian group G such that $0 \in A$. Then*

$$|2A| \geqslant \min(|G|, 3|A|/2). \tag{2.1}$$

Assume moreover that $|A| \geqslant 9$ and $A \notin \mathscr{E}$. Then

$$|2A| \geqslant \min(|G|, (3|A|+3)/2). \tag{2.2}$$

Proof. Assume $2A \neq G$. By Kneser's theorem (Theorem 2.1), there is a subgroup H such that $2A + H = 2A$ and $|2A| \geqslant 2|A+H| - |H|$. Since $H \neq G$, and A generates G, we have $|H + A| \geqslant 2|H|$. It follows that

$$|A|/2 \leqslant |H+A|/2 = |H+A| - |H+A|/2 \leqslant |H+A| - |H| \leqslant |2A| - |A|.$$

This proves inequality (2.1).

Assume now that $A \notin \mathscr{E}$.

Case 1. $|A+H| \geqslant 3|H|$. It follows that

$$2|A|/3 \leqslant 2|H+A|/3 = |H+A| - |H+A|/3 \leqslant |H+A| - |H| \leqslant |2A| - |A|.$$

Therefore $|2A| \geqslant 5|A|/3$.

Case 2. $|A+H| = 2|H|$. Since $A \notin \mathscr{E}$, we have $|A| \leqslant |A+H| - 1$. Therefore

$$\begin{aligned} |A|/2 \leqslant (|H+A|-1)/2 &= |H+A| - |H+A|/2 - 1/2 \\ &= |H+A| - |H| - 1/2 \leqslant |2A| - |A+H| - 1/2. \end{aligned}$$

Therefore $|2A| \geqslant 3(|A|+1)/2$. □

Inequality (2.1) in the above corollary was proved by J. E. Olson [7] for not necessarily abelian groups.

Let G be a finite abelian group and let S be a subset of G. For a pair of subsets A, B of G, we shall write

$$\Omega_S(A, B) = \{(x, y) \in A \times B : y \in x + S\},$$

https://doi.org/10.1017/S096354830000451X Published online by Cambridge University Press

and $\omega_S(A,B) = |\Omega_S(A,B)|$. When $A = B$ we shall write $e_S(A) = \omega_S(A,A)$. Note that e_S is invariant under translations: $e_S(X) = e_S(X+a)$ for every $a \in G$.

We shall also write

$$\Omega'_S(A,B) = \{(x,y) \in A \times B : y \in x + (S \setminus \{x\})\},$$

and $\omega'_S(A,B) = |\Omega'_S(A,B)|$. We shall omit the subscript S when the context is clear.

We clearly have

$$\omega(A,B) = \sum_{x\in A} |(x+S)\cap B| = \sum_{x\in B} |(x-S)\cap A|, \text{ and} \tag{2.3}$$

$$\omega'_S(A,B) \geqslant \omega(A,B) - |A \cap S|. \tag{2.4}$$

We need the following easy lemma.

Lemma 2.3. *Let G be an abelian group and let S be a finite subset of G such that $0 \notin S$. Let α be an integer such that $|S \cap -S| \leqslant \alpha - 1$. Put $|S| = s$. Then, for each finite $X \subset G$, the following inequalities hold:*

$$e(S) \leqslant s(s+\alpha-2)/2, \tag{2.5}$$

and

$$\omega(X, S\setminus X) + \omega(S\setminus X, X) \leqslant (s+\alpha-1-|X|)|X|. \tag{2.6}$$

Proof. Clearly

$$\begin{aligned} s(s-1) &= \sum_{x\in S} |S\setminus x| \\ &= \sum_{x\in S} |S\cap(x+(G\setminus 0))| \\ &\geqslant \sum_{x\in S} |S\cap(x+(S\cup -S))| \\ &= \sum_{x\in S} |S\cap(x+S)| + |S\cap(x-S)| - |S\cap(x+(S\cap(-S))| \\ &\geqslant 2e(S) - s(\alpha-1). \end{aligned}$$

On the other hand, using (2.3) we have

$$\begin{aligned} \omega(X,S\setminus X)+\omega(S\setminus X,X) &= \sum_{x\in X} |(x+S)\cap(S\setminus X)| + |(x-S)\cap(S\setminus X)| \\ &\leqslant \sum_{x\in X} (|(x+(S\cup -S))\cap(S\setminus X)| + |x+(S\cap -S)|) \\ &\leqslant |X|(|S\setminus X|+\alpha-1). \end{aligned}$$

□

https://doi.org/10.1017/S096354830000451X Published online by Cambridge University Press

3. The main result

Proposition 3.1. *Let $0 \in A$ be a finite generating subset of an abelian group G. Let α be an integer such that $\alpha \geqslant |A \cap -A|$, and let $a = |A|$. Then*

$$|2 \wedge A| \geqslant (3a-1)/2 + \frac{a^2 - (8\alpha+14)a - 5\alpha^2 + 9}{8(a-1)}, \text{ and} \tag{3.1}$$

$$|2 \wedge A| \geqslant (3a+2)/2 + \frac{a^2 - (8\alpha+26)a - 5\alpha^2 + 21}{8(a-1)}. \tag{3.2}$$

Proof. Set $S = A \setminus \{0\}$ and put $s = a-1$. By inequality (2.5), we have $e(S) \leqslant s(s+\alpha-2)/2$. Therefore there is an $x_0 \in S$ such that $|(x_0+S) \cap S| \leqslant (s+\alpha-2)/2$. Let $K_0 = (x_0+S) \setminus S$ and $K = K_0 - x_0$ and $|K| = k$. Notice that $e(K) = e(K_0)$ and $K \subset S$. We have

$$\omega(S, K_0) \leqslant \left(\sum_{x \in K_0} |x - S| \right) - e(K_0) = sk - e(K). \tag{3.3}$$

In particular,

$$k = |K_0| \geqslant \frac{s - \alpha + 2}{2}. \tag{3.4}$$

We have

$$\omega(S, K_0) + \omega(S, G \setminus (S \cup K_0)) + e(S) = s^2.$$

Therefore, using (2.6) and (3.3), we have

$$\begin{aligned}
&\omega(S, (G \setminus (K_0 \cup S)))\\
&\geqslant \left(\sum_{x \in S} |x + S| \right) - \omega(S,S) - \omega(S, K_0)\\
&= s^2 - \omega(K, S \setminus K) - \omega(S \setminus K, K) - e(S \setminus K) - e(K) - \omega(S, K_0)\\
&\geqslant s^2 - (s-k)(k+\alpha-1) - ((s-k)(s-k+\alpha-2)/2 - e(K_0)) - sk + e(K)\\
&= (s-k)(s-k-3\alpha+4)/2.
\end{aligned}$$

Hence, by inequality (2.4), we get

$$\begin{aligned}
\omega'(S \setminus \{x_0\}, (G \setminus (K_0 \cup S))) &\geqslant \omega(S \setminus \{x_0\}, (G \setminus (K \cup S)))) - s + 1\\
&\geqslant (s-k)(s-k-3\alpha+4)/2 - s + 1.
\end{aligned}$$

It follows that $|(2 \wedge A) \setminus (K_0 \cup S)| \geqslant ((s-k)(s-k-3\alpha+4)/2 - s + 1)/s$, which implies

$$\begin{aligned}
|2 \wedge A| &\geqslant |0 + S| + |(x_0 + (S \setminus \{x_0\}))| + (s-k)(s-k-3\alpha+4)/2s - 1 + 1/s\\
&= s + k - 1 + ((s-k)(s-k-3\alpha+4)/2 - s + 1)/s.
\end{aligned}$$

The above expression is an increasing function of k. Hence, using (3.4),

$$\begin{aligned}
|2 \wedge A| &\geqslant s + (s-\alpha+2)/2 - 1\\
&\quad + ((s - (s-\alpha+2)/2)(s - (s-\alpha+2)/2 - 3\alpha + 4)/2 - s + 1)/s\\
&= (3s-\alpha)/2 - 1 + \frac{8 + (s+\alpha-2)(s-5\alpha+6)}{8s}
\end{aligned}$$

https://doi.org/10.1017/S096354830000451X Published online by Cambridge University Press

$$= \quad (3a-1)/2 + \frac{a^2-(8\alpha+14)a-5\alpha^2+9}{8(a-1)}$$

$$= \quad (3a+2)/2 + \frac{a^2-(8\alpha+26)a-5\alpha^2+21}{8(a-1)}.$$

The proof is complete. □

We are now ready to prove our main result. For a finite abelian group G, we shall write $\mu(G) = |\{x \in G : 2x = 0\}|$.

Theorem 3.2. *Let G be an abelian group and let μ be an integer such that* $\mu \geqslant \mu(G)$. *Let A be a generating subset of G containing 0 such that* $|A| > 4\mu + 7 + \sqrt{21\mu^2 + 32\mu + 40}$. *Then*

$$|2 \wedge A| \geqslant \min(|G|, 3|A|/2).$$

Moreover, if $A \notin \mathscr{E}$ *and* $|A| > 4\mu + 13 + \sqrt{21\mu^2 + 80\mu + 148}$, *then*

$$|2 \wedge A| \geqslant \min(|G|, 3(|A|+1)/2).$$

Proof. Assume first that there is an $x \in A$ such that $|(x - A) \cap (-x + A)| \leqslant \mu$. Note that $A - x$ also generates G. Since $|2 \wedge A| = |2 \wedge (A - x)|$, we may assume without loss of generality that $x = 0$. Therefore $|A \cap -A| \leqslant \mu$. Put $a = |A|$. By (3.1),

$$|2 \wedge A| \geqslant (3a-1)/2 + \frac{a^2-(8\alpha+26)a-5\alpha^2+21}{8(a-1)}.$$

It follows that

$$|2 \wedge A| \geqslant 3a/2,$$

for $a > 4\mu + 7 + \sqrt{21\mu^2 + 32\mu + 40}$. Similarly, using (3.2) we have

$$|2 \wedge A| \geqslant 3(a+1)/2,$$

for $a > 4\mu + 13 + \sqrt{21\mu^2 + 80\mu + 148}$.

Assume now that, for every $x \in A$, we have $|(x - A) \cap (-x + A)| > \mu$. Let us show that $2A = 2 \wedge A$. Assuming the contrary, we may choose $y \in A$ such that $2y \notin 2 \wedge A$. Since the equation $2x = 0$ has at most μ solutions in G, there exists $z \in (y - A) \cap (-y + A)$ such that $2z \neq 0$. There exist $a_1, a_2 \in A$ such that $z = y - a_1 = -y + a_2$. It follows that $2y = a_1 + a_2$. We have $a_1 \neq a_2$, since otherwise $2z = 0$. Therefore $2y \notin 2 \wedge A$, a contradiction.

By Corollary 2.2, we have

$$|2 \wedge A| = |2A| \geqslant \min(|G|, 3|A|/2).$$

Moreover, if $A \notin \mathscr{E}$, then

$$|2 \wedge A| = |2A| \geqslant \min(|G|, 3(|A|+1)/2).$$

This completes the proof. □

https://doi.org/10.1017/S096354830000451X Published online by Cambridge University Press

When G is an abelian group of odd order, then the equation $2x = 0$ has only the trivial solution in G. Similarly, if G is a cyclic group, then there is at most one nontrivial solution of the equation. Therefore, the above theorem implies the following corollaries.

Corollary 3.3. *Let A be a generating set of an abelian group G of odd order with $0 \in A$. If $|A| \geqslant 21$ then*

$$|2 \wedge A| \geqslant \min(|G|, 3|A|/2).$$

Moreover, if $A \notin \mathscr{E}$ and $|A| \geqslant 33$ then

$$|2 \wedge A| \geqslant \min(|G|, 3(|A|+1)/2). \qquad \square$$

Corollary 3.4. *Let A be a generating set of a finite cyclic group G with $0 \in A$. If $|A| \geqslant 29$, then*

$$|2 \wedge A| \geqslant \min(|G|, 3|A|/2).$$

Moreover, if $A \notin \mathscr{E}$ and $|A| \geqslant 38$, then

$$|2 \wedge A| \geqslant \min(|G|, 3(|A|+1)/2). \qquad \square$$

Let G be an abelian group and let A be a finite subset of G. Note that we trivially have $|2 \wedge A| \geqslant |(A \setminus \{x\}) + x| = |A| - 1$. Equality holds when $A = G = \mathbf{Z}_2^n$. The following statement could hold.

Conjecture 3.5. *Let A be a finite generating subset of an abelian group G with $0 \in A$. If $|A| \geqslant 6$ then*

$$|2 \wedge A| \geqslant \min(|G| - 1, 3|A|/2).$$

If true, the inequality $|A| \geqslant 6$ is best possible, since for an arithmetic progression P with $|P| < 6$, we have $|2 \wedge P| = 2|P| - 3 < 3|P|/2$.

References

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

[2] Dias da Silva, J. A. and Hamidoune, Y. O. (1994) Cyclic subspaces of Grassmann derivations. *Bull. London Math. Soc.* **26** 140–146.

[3] Erdős, P. and Heilbronn, H. (1964) On the addition of residue classes mod *p*. *Acta Arith.* **9** 149–159.

[4] Erdős, P. and Graham, R. (1980) Old and new problems and results in combinatorial number theory. *L'Enseignement Mathématique* 1–128.

[5] Mann, H. B. (1976) *Addition Theorems*, 2nd edn, Krieger, New York.

[6] Nathanson, M. B. (1996) *Additive Number Theory, 1: Inverse Theorems and the Geometry of Sumsets*, Vol. 165 of *Graduate Texts in Mathematics*, Springer, New York.

[7] Olson, J. E. (1975) Sums of sets of group elements. *Acta Arith.* **28** 147–156.