Combinatorics, Probability and Computing (1999) 8, 461–466. Printed in the United Kingdom
© 1999 Cambridge University Press

On Sets with a Small Subset Sum

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

[1] E. Combinatoire, Univ. Pierre et Marie Curie, 4 Place Jussieu,
75230 Paris Cedex 05, France
(e-mail: yha@ccr.jussieu.fr)

[2] Dep. Matemàtica Aplicada i Telemàtica, Univ. Politècnica de Catalunya,
Jordi Girona, 1, 08034 Barcelona, Spain
(e-mail: {allado, oriol}@mat.upc.es)

Received 27 November 1997; revised 18 May 1998

Let A be a subset of an abelian group G. The subset sum of A is the set $\Sigma(A) = \{\sum_{x\in T} | T \subset A\}$. We prove the following result. Let S be a generating subset of an abelian group G such that $0 \notin S$ and $14 \leqslant |S|$. Then one of the following conditions holds.

(i) $|\Sigma(S)| \geqslant \min(|G| - 3, 3|S| - 3)$.
(ii) There is an $x \in S$ such that $S \setminus \{x\}$ generates a proper subgroup of order less than $(3|S| - 3)/2$.

As a consequence, we obtain the following open case of an old conjecture of Diderrich. Let q be a composite odd number and let G be an abelian group of order $3q$. Let S be a subset of G with cardinality $q + 1$. Then every element of G is the sum of some subset of S.

1. Introduction

Let G be an abelian group and let A be a finite subset of $G \setminus \{0\}$. We write

$$\Sigma(A) = \left\{ \sum_{x\in T} x \quad \middle| \quad T \subset A \right\}.$$

Thus, setting $A = \{a_1, \ldots, a_j\}$, we have $\Sigma(A) = \{0, a_1\} + \cdots + \{0, a_j\}$, where, for two subsets $B, C \subset G$, we write $B + C = \{b + c \,|b \in B, c \in C\}$.

Let $c(G)$ be the minimal t such that, for every subset S with cardinality t not containing 0, we have $\Sigma(S) = G$. The problem of determining $c(G)$ has received a lot of attention, and the reader may refer to [2, 3, 6] for more details on the existing results.

† Supported by the Spanish Ministry of Education under grant SAB95-0573
‡ Supported by the Spanish Research Council, CICYT, under project TIC97-0963

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press

Actually, most of the authors deal with $c^*(G)$, defined as the minimal t such that, for every subset S with cardinality t not containing 0, $\Sigma(S) = G$ and 0 is the sum of some non-empty subset of S. However, it follows from the main result in [11] that $c^*(G) = c(G)$, for $|G|$ non-prime. One can use a result in [8] to show that $c^*(G) = c(G)$ for $|G|$ a prime as well.

Estimation of $|\Sigma(A)|$ has received some interest in the literature. The known results assert the existence of a constant c such that $|\Sigma(A)| \geqslant c|A|^2$ provided that 0 is not a sum of a non-empty sequence of distinct elements from S. The existence of c was first proved by Szemerédi [12]. The value of c was improved by Olson [11] and by the authors of [8].

As far as we are aware, the first lower bound not assuming that 0 is not a non-empty subset sum is the relation $|\Sigma(S)| \geqslant \min(|G'| - 1, 2|S| - 1)$, where G' is the subgroup generated by S, obtained by one of the authors in [7].

In this paper, we shall describe the sets S such that $|\Sigma(S)| < 3|S| - 3$. More precisely, we obtain the following result. Let S be a generating subset of an abelian group G such that $0 \notin S$ and $14 \leqslant |S|$. Then one of the following conditions holds.

(i) $|\Sigma(S)| \geqslant \min(|G| - 3, 3|S| - 3)$.
(ii) There is an $x \in S$ such that $S \setminus x$ generates a subgroup of order less than $(3|S|-3)/2$.

As a corollary, we shall show the following result. Let q be a composite odd number and let G be an abelian group of order $3q$. Let S be a subset of G with cardinality $q + 1$. Then every element of G is the sum of some subset of S.

This result is one of the few open cases of an old conjecture of Diderrich [2], which we will state below for the benefit of the reader.

Let p be the smallest prime dividing the order of an abelian group G. For $|G| = p$, it was proved by Erdős and Heilbronn [5] that $c(G) \leqslant \sqrt{54p}$. Olson proved in [10] that $c(G) \leqslant \sqrt{4p - 3} + 1$. The authors of [1] obtained $c(G) \leqslant \sqrt{4p - 7} + 1$.

The case where $|G|$ is composite is of a different nature and $c(G)$ has a relatively large lower bound. Let H be a subgroup of G of order $|G|/p$, and let $x \in G \setminus H$. Let $h_1, h_2, \ldots, h_{p-3}$ be distinct nonzero elements of H. Put $S = (H \setminus \{0\}) \cup \{x, x + h_1, \ldots, x + h_{p-3}\}$. The reader may check easily that $\Sigma(S) \neq G$. In particular,

$$c(G) \geqslant |G|/p + p - 2.$$

Suppose $p \geqslant 3$. When $|G|/p$ is a prime, Diderrich proved that $|G|/p + p - 2 \leqslant c(G) \leqslant |G|/p + p - 1$. The two bounds are attained. When $|G|/p$ is a composite number, Diderrich conjectured that $c(G) = |G|/p + p - 2$.

This conjecture has been proved by Gao [6] for $p \geqslant 43$. But the methods used by Gao based on Theorem 2.3 are not suitable for small primes. In contrast, our main result applies to all subsets of G and it coincides with the Diderrich conjecture only for large sets.

2. Preliminaries

Recall the following well-known and easy lemma.

Lemma 2.1. *Let G be a finite group. Let X and Y be subsets of G such that $|X|+|Y| > |G|$. Then $X + Y = G$.*

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press

Proof. Suppose on the contrary that $x \in G \setminus (X+Y)$. Then $x - X \cap Y = \emptyset$, contradicting $|x-X| + |Y| = |X| + |Y| > |G|$. □

Let G be an abelian group containing a subset $B \subset G$ and an element x. Following Olson, we write

$$\lambda_B(x) = |(B+x) \cap \overline{B}|,$$

where $\overline{B}$ denotes the complement of B in G.

We use the following lemma.

Lemma 2.2 ([10]). *Let G be a finite abelian group. Let S be a subset of G such that $0 \notin S$. Then, for every $y \in S$ we have*

$$|\Sigma(S)| \geqslant |\Sigma(S \setminus y)| + \lambda_B(y), \tag{2.1}$$

where $B = \Sigma(S)$. □

As a main tool we use the following result of Olson.

Theorem 2.3 (Olson [11]). *Let B and S be subsets of G such that $0 \notin S$ and $G = \langle S \rangle$. Then there is an $x \in S$ such that*

$$\lambda_B(x) \geqslant \min((|B|+1)/2, (|G \setminus B|+1)/2, (|S|+2)/4) \tag{2.2}$$

□

This result is exactly Lemma 3.1 of [11] combined with the equality $\lambda_B(x) = \lambda_{\overline{B}}(x)$, proved in [10, 11].

We use the following result.

Theorem 2.4 ([7]). *Let S be a generating subset of an abelian group G such that $0 \notin S$. Then*

$$|\Sigma(S)| \geqslant \min(|G|-1, 2|S| - \epsilon), \tag{2.3}$$

where $\epsilon = 1$ for $|S| \leqslant 4$ and $\epsilon = 0$ for $|S| \geqslant 5$. □

We use also the following obvious consequence of the above result, which may be easily deduced from a result by Diderrich and Mann [3].

Corollary 2.5. *Let S be a subset of an abelian group G such that $0 \notin S$ and $|S| \geqslant |G|/2+1$. Then $\Sigma(S) = G$.*

Proof. Let $x \in S$ and set $S' = S \setminus x$. Clearly S' generates G. By (2.3), $|\Sigma(S')| \geqslant |G| - 1$. By Lemma 2.1, $\Sigma(S) = \Sigma(S') + \{0, x\} = G$. □

Later we shall use the following consequence of the above two results.

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press

Corollary 2.6. *Let S be a subset of an abelian group G such that $0 \notin S$ and $3|S|/2 \leqslant |G|$. Then $|\Sigma(S)| \geqslant 3|S|/2$.*

Proof. The result holds by (2.3) if $3|S|/2 \leqslant |G| - 1$ and by Corollary 2.5 when $3|S|/2 > |G| - 1$. □

3. The result

Let S be a subset of an abelian group G. We shall say that S is *regular* if, for each $x \in S$, the subgroup generated by $S \setminus x$ has order at least $\min(|G|, 3(|S| - 1)/2)$.

Lemma 3.1. *Let S be a regular generating subset of an abelian group G such that $0 \notin S$ and $|S| \geqslant 6$. Then either $|\Sigma(S)| \geqslant \min(|G|, 3|S| - 3)$ or $S \setminus \{x\}$ is a regular generating subset of G for each $x \in S$.*

Proof. Suppose first that $S_1 = S \setminus \{x\}$ generates a proper subgroup H for some $x \in S$. By the regularity of S we have $3(|S| - 1)/2 \leqslant |H|$. By Corollary 2.6, we have $|\Sigma(S_1)| \geqslant 3(|S| - 1)/2$. Clearly $|\Sigma(S)| = |\Sigma(S_1) \cup (x + \Sigma(S_1))| = 2|\Sigma(S_1)| \geqslant 3|S| - 3$.

Suppose now that there is an $x \in S$ such that $S_1 = S \setminus \{x\}$ is a nonregular generating subset of G. Let $y \in S_1$ such that $S_1 \setminus y$ generates a proper subgroup H with cardinality less than $(3|S_1| - 3)/2$.

By Corollary 2.5, we have $\Sigma(S_2) = H$. Since S is regular, $x \notin H$. Therefore, $|\Sigma(S)| \geqslant |H \cup H + x \cup H + y \cup H + x + y|$. Suppose now $|\Sigma(S)| < 3|S| - 3$. Since $|H| \geqslant |S_2 \cup \{0\}| \geqslant |S| - 1$ we have $|\Sigma(S)| < 3|H|$. It follows that $H + x = H + y$ and $H + x + y = H$. Since S generates G we would have $|G| = 2|H| = |\Sigma(S)|$. □

We need first to deal with subsets with a small cardinality.

Lemma 3.2. *Let S be a regular generating subset of an abelian group G such that $0 \notin S$. Then*

(i) *If $|S| \geqslant 6$ then $|\Sigma(S)| \geqslant \min(|G| - 3, 3|S| - 6)$.*
(ii) *If $|S| \geqslant 10$ then $|\Sigma(S)| \geqslant \min(|G| - 5, 4|S| - 16)$.*

Proof. Set $B = \Sigma(S)$. Choose $x \in S$ such that $\lambda_B(x) = \max\{\lambda_B(y); y \in S\}$. By Lemma 3.1 we may assume that $S' = S \setminus \{x\}$ is a regular generating subset of G. Notice that $|\Sigma(S')| \leqslant |B|$.

(i) The proof is by induction on $|S|$. By (2.3), the result holds for $|S| = 6$. Suppose that $|S| \geqslant 7$ and $|B| \leqslant |G| - 4$. By (2.2), $\lambda_B(x) > 2$. By the induction hypothesis and by (2.1), $|B| \geqslant |\Sigma(S')| + \lambda_B(x) \geqslant 3|S'| - 6 + 3 = 3|S| - 6$.

(ii) The proof is again by induction on $|S|$, the result being true for $|S| = 10$ by (i). Suppose that $|S| \geqslant 11$ and $|B| \leqslant |G| - 6$. Now (2.2) implies that $\lambda_B(x) > 3$. Therefore, using the induction hypothesis and (2.1) we get $|B| \geqslant |\Sigma(S')| + \lambda_B(x) \geqslant 4|S| - 16$. □

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press

Theorem 3.3. *Let S be a regular generating subset of an abelian group G such that $0 \notin S$ and $14 \leqslant |S|$. Then*

$$|\Sigma(S)| \geqslant \min(|G| - 3, 3|S| - 3).$$

Proof. Put $B = \Sigma(S)$. Suppose that $|S| \geqslant 14$ and $|B| \leqslant |G| - 4$. By (2.2), there is an $x \in S$ such that $\lambda_B(x) > 2$. By Lemma 3.1 we may assume that $S' = S \setminus \{x\}$ is a regular generating subset of G. Clearly, $|\Sigma(S')| \leqslant |B|$. By equation (2.1) $|B| \geqslant |\Sigma(S')| + 3$. Now the result holds for $|S| = 14$ by Lemma 3.2(ii) and for $|S| > 14$ by induction on $|S|$. □

The above result can be restated in the following form.

Corollary 3.4. *Let S be a generating subset of an abelian group G such that $0 \notin S$ and $14 \leqslant |S|$. Then one of the following conditions holds.*

(i) $|\Sigma(S)| \geqslant \min(|G| - 3, 3|S| - 3)$.

(ii) *There is an $x \in S$ such that $S \setminus x$ generates a subgroup of order $< 3(|S| - 1)/2$.* □

Corollary 3.5. *Let $q > 13$ be an odd number. Let G be an abelian group of order $3q$. Let A be subset of $G \setminus \{0\}$ such that $|A| = q + 1$. Then $\Sigma(A) = G$.*

Proof. Choose $a, b \in A$ with $a \notin \{b, -b\}$. Clearly $|\Sigma\{a, b\}| = 4$. Set $S = A \setminus \{a, b\}$. Consider first the case where there is a $c \in S$ such that $S' = S \setminus \{c\}$ generates a proper subgroup H. Since $|S'| = q - 2$, we have $|H| = q$. By Corollary 2.5, $\Sigma(S') = H$. There are $u, v \in A \setminus S'$ such that $u, v \notin H$. One may see easily that $|H \cup H + u \cup H + v \cup H + u + v| \geqslant 3|H|$. It follows that $|\Sigma(A)| \geqslant 3|H| = |G|$.

Assume now that for every $c \in S$, $S \setminus \{c\}$ generates G. By Theorem 3.3, $|\Sigma(S)| \geqslant 3q - 3$. Hence, by Lemma 2.1, $\Sigma(A) = \Sigma(S) + \Sigma(\{a, b\}) = G$. □

Notice that the condition q odd can not be removed, since any subset S of a subgroup H of index 2 in a group G with even order has $\Sigma(S) \neq G$.

Corollary 3.5 shows the validity of the Diderrich conjecture mentioned in the Introduction when $p = 3$ and $|G| \neq 27$. On the other hand, it is not difficult to check it directly for $|G| = 27$. Therefore the Diderrich conjecture holds for $p = 3$.

References

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

[2] Diderrich, G. T. (1975) An addition theorem for abelian groups of order pq. *J. Number Theory* **7** 33–48.

[3] Diderrich, G. T. and Mann, H. B. (1973) Combinatorial problems in finite abelian groups. In *3A survey of Combinatorial Theory* (J. L. Srivasta *et al.*, eds), North-Holland, Amsterdam, pp. 95–100.

[4] Eggleton, R. B. and Erdős, P. (1972) Two combinatorial problems in group theory. *Acta Arith.* **21** 112–116.

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press

[5] Erdős, P. and Heilbronn, H. (1964) On the addition of residue classes mod *p*. *Acta Arith.* **9** 149–159.
[6] Gao, W. (1997) On the size of additive bases of finite groups. Preprint.
[7] Hamidoune, Y. O. (1998) Adding distinct congruence classes. *Combinatorics, Probability and Computing* **7** 81–87.
[8] Hamidoune, Y. O. and Zémor, G. (1996) On zero-free subset sums. *Acta Arith.* **LXXVIII** 143–152.
[9] Mann, H. B. (1976) *Addition Theorems*, 2nd edn, R. E. Krieger, New York.
[10] Olson, J. E. (1968) An addition theorem mod *p*. *J. Combin. Theory* **5** 45–52.
[11] Olson, J. E. (1975) Sum of sets of group elements. *Acta Arith.* **28** 147–156.
[12] Szemerédi, E. (1970) On a conjecture of Erdős and H. Heilbronn. *Acta Arith.* **17** 227–229.
[13] White, E. T. (1978) Ordered sums of group elements. *J. Combin. Theory Ser. A* **24** 118–121.

https://doi.org/10.1017/S0963548399003922 Published online by Cambridge University Press