A Conjecture by Diderrich on subset sums[1]

O. Serra[2]

Resumen

Sea G un grupo abeliano de orden n. El número crítico $c(G)$ de G es el menor k tal que, para cualquier subconjunto $S = \{s_1, \cdots, s_k\}$, la ecuación

$$x = \epsilon_1 s_1 + \cdots + \epsilon_k s_k, \quad \epsilon_i \in \{0, 1\},$$

tiene solución para cada $x \in G$.

El problema del cálculo de $c(G)$, planteado por Erdős y Heilbronn en 1964, ha sido recientemente completado con la resolución del último caso abierto constituído por la conjetura que Diderrich formuló en 1975.

En esta nota se describe la historia del problema hasta su resolución y se identifican los conjuntos críticos para la conjetura de Diderrich, lo que permite mejorar sensiblemente el valor de $c(G)$.

1 Introduction

Let G be a finite Abelian group of order $|G| \geq 3$, and let S be a subset of non-zero elements of G. A *subset sum* is the sum of distinct elements of a non-empty subset of S. As usual, we write

$$\Sigma(S) = \{\sum_{x \in A} x \;\Big|\; A \subseteq S,\ A \neq \emptyset\},$$

for the set of all subset sums of S.

If $|S| = |G| - 1$ then clearly

$$\Sigma(S) = G, \tag{1}$$

that is, the subset sums of S *cover* G. The *critical number* of G, denoted by $c(G)$, is the smallest s such that (1) holds for every subset $S \subseteq G \setminus 0$ with cardinality $|S| = s$.

The study of the parameter $c(G)$ stems from the 1964 work of Erdős and Heilbronn [4] on the case $G = \mathbb{Z}_p$. They showed that if S is a set of non-zero elements of $\mathbb{Z}_p$ with $|S| \geq 3\sqrt{6p}$, then the subset sums of S, together with 0, cover $\mathbb{Z}_p$. In that paper they introduced an average technique which has proved to be useful for the complete computation of $c(G)$.

Olson [14] improved the result to $c(\mathbb{Z}_p) \leq \sqrt{4p-3} + 1$ by a refinement of the same techniques. Much later, in 1994, Dias da Silva and Hamidoune [1] obtained the following result using Grassmann derivations, which is essentially best possible:

Theorem A *If p is an odd prime then*

$$c(\mathbb{Z}_p) \leq \sqrt{4p-7}.$$

[1] This work has been supported by the Catalan Resarrch Council under grant 2000SGR00079.

[2] Universitat Politècnica de Catalunya

The evaluation of $c(G)$ for groups with composite order was first considered in 1967 by Mann and Olson. They obtained the inequality $c(\mathbb{Z}_p \oplus \mathbb{Z}_p) \leq 2p-1$ in [12]. Mann and Wou [13] give the exact value for this case.

Theorem B *If p is an odd prime then*

$$c(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p-2.$$

In 1971 Diderrich and Mann [3] obtained the following theorem which determines $c(G)$ when $|G|$ is an even composite number.

Theorem C *Let G be an Abelian group of order $2h$, where $h > 1$. Then*

$$c(G) = \begin{cases} h & \text{if } h \geq 5 \text{ or } G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \\ h+1 & \text{otherwise} \end{cases}$$

Diderrich [2] proved in 1975 the following inequality when $|G|$ is the product of two primes.

Theorem D *Let G be an Abelian group of order pq, where p and $q \geq p$ are primes. Then*

$$p+q-2 \leq c(G) \leq p+q-1,$$

For $|G|$ composite, let p be the smallest prime dividing $|G|$ and write $|G| = ph$. In Theorems B, C and D above, the smallest of the possible values of $c(G)$ is $p+h-2$. The only case not covered by these theorems is when $p > 2$ and h is composite. Diderrich conjectured in the same paper [2] that in this case we must have $c(G) = p+h-2$. This conjecture was studied by Peng [16] and, more recently, by Lipkin [10] and by various combinations of the authors Gao, Hamidoune, Lladó and Serra [5, 7, 9].

Finally, in 1999, Gao and Hamidoune [6] proved Diderrich's conjecture for all odd primes. Combining this result with Theorem C we have the following theorem.

Theorem E *Let G be an Abelian group of order ph, where p is the smallest prime dividing $|G|$ and h is composite. If $p = 2$, $h = 4$ and $G \neq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, then $c(G) = 5$. In all other cases we have*

$$c(G) = p+h-2.$$

The techniques used in the final solution of Diderrich's conjecture essentially go back to the original ones introduced by Erdős and Heilbronn and refined by Olson. The same techniques allow to identify the structure of critical sets showing that, behind them, the value of $c(G)$ can be considerably improved.

2 The averaging technique for $\Sigma(S)$.

Throughout the paper G denotes an abelian group of order n. Erdős and Heilbronn introduced in [4] the function

$$\lambda_B(x) = |(B+x) \setminus B|.$$

for each $B \subseteq G$ and $x \in G$. From the subadditivity of λ_B, an average technique allows to show that $\max_{x \in X} \lambda_B(x) \geq |X|/6$ in $\mathbb{Z}_p$. Olson generalized the result to arbitrary abelian groups. His result implies the following.

Lemma 2.1 *(Olson [15]) Let G be an abelian group and let S be a generating subset of G such that $0 \notin S$. Let B be a subset of G such that $|B| \leq \frac{|G|}{2}$. Then there is $x \in S$ such that*

$$\lambda_B(x) \geq \min(\frac{|B|+1}{2}, \frac{|S \cup -S|+2}{4}).\square \tag{2}$$

One of the consequences of this Lemma is the following key tool.

Lemma 2.2 *Let X be a generating subset of an abelian group G such that $X \cap -X = \emptyset$ and $2|\Sigma_0(X)| \leq |G|$. Let the ordering $\{x_1, \ldots, x_k\}$ such that $\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j); 1 \leq j \leq i\}$, where $B_i = \Sigma(x_1, \ldots, x_i)$. Let t be the largest integer such that $\{x_1, \cdots, x_t\}$ generates a proper subgroup of G. Then, there is a subset $V \subset X$ such that $|V| = t-1$, $\langle V \rangle \neq G$ and*

$$|\Sigma(X)| \geq 4|V| + \frac{(|X|+|V|+5)(|X|-|V|-1)-2}{4} \tag{3}$$

This inequality is often sufficient to prove the following extensions to the computation of $c(G)$. First of all, the trivial examples for the value $c(G) = (n/p)+p-2$ in Diderrich conjecture consist of a proper subgroup of largest order and a transversal with two elements deleted. These are in fact the only examples.

Theorem 2.3 ([7]) *Let G be a finite abelian group with order $n \geq 6p^2$, where $p \geq 5$ is the smallest prime dividing n. Also assume $\frac{n}{p}$ composite. Let S be a subset of $G \setminus 0$ such that $|S| = \frac{n}{p} + p - 3$. Then the following conditions are equivalent.*

(i) $\Sigma(S) \neq G$.

(ii) There are a subgroup H of order $\frac{n}{p}$ and $y \notin H$ such that $(H \setminus 0) \subseteq S$ and $S \subseteq H \cup (y+H) \cup (-y+H)$.

Suppose that G is an abelian group of order $n > 3$ and let $S \subset G \setminus \{0\}$ with $|S| \geq n/3+2$. If n is a prime number then $|S| \geq \lfloor\sqrt{4n-7}\rfloor$ and, by Theorem A, $\Sigma(S) = G$. If n is composite with smallest prime divisor $p \geq 3$, then $|S| \geq n/p+p-1$ and, by Theorems D and E, we also have $\Sigma(S) = G$. These results can be extended to all abelian groups of order $n \geq 67$.

Theorem 2.4 ([7]) *Let G be an abelian group of order $n \geq 67$ and let S be a subset of $G \setminus \{0\}$ such that $|S| \geq \frac{n}{3} + 2$. Then $\Sigma(S) = G$ if and only if $\langle S \rangle = G$.*

The next result improves Theorem 2.4 for groups with odd order.

Theorem 2.5 ([7]) *Let G be a finite Abelian group of order $n \geq 183$. Assume $\frac{n}{p}$ composite, where $p \geq 3$ is the smallest prime dividing n. Let S be a subset of $G \setminus \{0\}$ such that $|S| \geq \frac{n+11}{4}$. Then the following conditions are equivalent.*

(i) $\Sigma(S) \neq G$.

(ii) There is a subgroup H of order $\frac{n}{3}$ such that $|S \setminus H| \leq 1$.

The characterization of large sets $S \subset G \setminus 0$ for which $\Sigma(S) \neq G$ can be accomplished in a similar way to the above results whith some additional restrictions on n and its smaller prime divisor.

Theorem 2.6 *Let G be a finite abelian group with order n. Assume $n \geq 15p^2$, where $p \geq 5$ is the smallest prime dividing n. Also assume $\frac{n}{p}$ composite. Let S be a subset of $G \setminus 0$ such that $|S| \geq \frac{n}{p+2} + p$. Then the following conditions are equivalent.*

(i) $\Sigma(S) \neq G$.

(ii) There is a subgroup H of order $\frac{n}{p}$ such that $|S \setminus H| \leq p-2$ and $\Sigma(S \setminus H) + H \neq G$.

Referencias

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

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

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

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

[5] W. Gao, *On the size of additive bases of finite groups* Preprint, October 1997.

[6] W. Gao and Y.O. Hamidoune, *On additive bases* Acta Arith. **88** (1999), 3, 233-237.

[7] W. Gao, Y.O. Hamidoune, A. Lladó and O. Serra, Covering a finite abelian group by subset sums, *Combinatorica,* to appear.

[8] Y. O. Hamidoune, *Adding distinct congruence classes* , Combinatorics, Computing and Probability (1998) 7, 81-87.

[9] Y.O. Hamidoune A. S. Lladó and O. Serra, On sets with a small subset sum , Combinatorics, Probability and Computing (1999) 8, 461–466.

[10] E. Lipkin, *Subset sums of sets of residues.* Structure Theory of Set Addition, Astérique 258(1999), 187-192.

[11] H.B. Mann, *Addition Theorems,* R.E. Krieger, New York, 1976.

[12] H.B. Mann and J. E. Olson, *Sums of sets of elements in the elementary abelian group of type (p,p),* J. Comb. Theory 2(1967), 275- 284.

[13] H.B. Mann and Y. F. Wou, *Addition theorem fot the elementary abelian group of type (p,p),* Mh. Math. 102(1986), 273- 308.

[14] J. E. Olson, *An addition theorem mod p,* J. Comb. Theory 5(1968), 45-52.

[15] J. E. Olson, *Sum of sets of group elements,* Acta Arith. 28 (1975), 147-156.

[16] C. Peng, *An addition theorems in elementary abelian groups,* J. Number Theory 27 (1987), 58-62.