COMBINATORICA
Bolyai Society – Springer-Verlag

COMBINATORICA **23** (4) (2003) 599–611

COVERING A FINITE ABELIAN GROUP BY SUBSET SUMS

W. GAO, Y. O. HAMIDOUNE, A. LLADÓ*, O. SERRA†

Received May 16, 2000

Let G be an abelian group of order n. The critical number $c(G)$ of G is the smallest s such that the subset sums set $\Sigma(S)$ covers all G for each subset $S \subset G \setminus \{0\}$ of cardinality $|S| \geq s$. It has been recently proved that, if p is the smallest prime dividing n and n/p is composite, then $c(G) = |G|/p + p - 2$, thus establishing a conjecture of Diderrich.

We characterize the critical sets with $|S| = |G|/p + p - 3$ and $\Sigma(S) = G$, where $p \geq 3$ is the smallest prime dividing n, n/p is composite and $n \geq 7p^2 + 3p$.

We also extend a result of Diderrich and Mann by proving that, for $n \geq 67$, $|S| \geq n/3+2$ and $\langle S \rangle = G$ imply $\Sigma(S) = G$. Sets of cardinality $|S| \geq \frac{n+11}{4}$ for which $\Sigma(S) \neq G$ are also characterized when $n \geq 183$, the smallest prime p dividing n is odd and n/p is composite. Finally we obtain a necessary and sufficient condition for the equality $\Sigma(G) = G$ to hold when $|S| \geq n/(p+2) + p$, where $p \geq 5$, n/p is composite and $n \geq 15p^2$.

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

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

for the set of all subset sums of S.

Mathematics Subject Classification (2000): 11A75, 20K01

* Work partially supported by the Spanish Research Council under grant TIC2000-1017
† Work partially supported by the Catalan Research Council under grant 2000SGR00079

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 subgroup generated by a subset S of G will be denoted $\langle S\rangle$. The additive group of integers modulo n will be denoted by $\mathbb{Z}_n$ and the letter p will always denote a prime number.

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

Theorem A. *If p is an odd prime then*

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

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 inequalities 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 present authors [5,9].

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*

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

In this paper we extend and complement the results mentioned above by giving conditions for the equality (1) to hold when $|S|$ is smaller than $c(G)$.

Let G be an abelian group of order n. In Section 3 we show that, for $n\geq 67$ and $|S|\geq\frac{n}{3}+2$, $\Sigma(S)=G$ if and only if S generates G. This extends a result of Diderrich and Mann [3], also obtained by Griggs and Poonen [7] which states that, for n even and at least 10, $c(G)\leq n/2$.

For groups with odd order, we shall prove sharper results. Let G be an abelian group of odd order $n=ph$, where $p\geq 3$ is the smallest prime dividing n and h is composite. In Section 3 we characterize the sets S with $|S|\geq\frac{n+11}{4}$ and $\Sigma(S)\neq G$ when $n\geq 183$. In section 4 we characterize the sets with the critical cardinality

$$|S| = h + p - 3 \text{ and } \Sigma(S) \neq G$$

when $p\geq 5$ and $n\geq 7p^2$.

In section 5, we obtain a corresponding result if

$$|S| \geq \frac{n}{p+2} + p,$$

when $p\geq 5$ and $n\geq 15p^2$.

2. Some tools

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 $X+Y \neq G$. Then $|X|+|Y| \leq |G|$.*

We use also the Cauchy–Davenport Theorem, see for instance [11, Corollary 1.2.3].

Theorem 2.2 (Cauchy-Davenport). *Let p be a prime number. Let X and Y be non-empty subsets of $\mathbb{Z}_p$. Then $|X+Y| \geq \min(p, |X|+|Y|-1)$.*

For convenience we summarize the Theorems stated in the Introduction in the following result.

Lemma 2.3. *Let G be an abelian group with order $n=ph$, where p is the smallest prime dividing n and $h \geq 1$. Let S be a subset of $G \setminus \{0\}$ such that $|S| = h+p-2+\delta(h)$, where $\delta(h)=1$ if h is a prime or $h=4$ and $\delta(h)=0$ otherwise. Then $\Sigma(S)=G$.*

Proof. If h is a prime, the result follows from Theorem D. If h is composite, it follows from Theorem E. ∎

Let G be an abelian group and $S \subset G \setminus \{0\}$. For technical reasons we shall deal with

$$\Sigma_0(S) = \Big\{ \sum_{x \in T} x \quad | \quad T \subset S \Big\},$$

so that $\Sigma_0(S) = \Sigma(S) \cup \{0\}$. The following result proved by Olson [15] shows that $\Sigma_0(S)=\Sigma(S)$ for $|S| \geq 3\sqrt{|G|}$.

Lemma 2.4 (Olson [15]). *Let S be a subset of an abelian group G of order n. If $|S| \geq 3\sqrt{n}$ then $0 \in \Sigma(S)$.*

Let $B \subseteq G$ and $x \in G$. As usual, we write

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

Let S be a nonempty subset of $G \setminus \{0\}$ and $y \in S$. Put $B=\Sigma(S)$. Olson [14] proved:

$$|\Sigma_0(S)| \geq |\Sigma_0(S \setminus y)| + \lambda_B(y). \tag{2}$$

We shall use also the following result of Olson.

Lemma 2.5 (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*

$$\lambda_B(x) \geq \min\Big(\frac{|B|+1}{2}, \frac{|S \cup -S|+2}{4} \Big). \tag{3}$$

This result follows by applying Lemma 3.1 of [15] to $S\cup -S$.

We use the following lemmas:

Lemma 2.6 **([8]).** *Let S be a subset of an abelian group G with $0\notin S$. Then*

$$|\Sigma_0(S)| \geq \min(|G|-1, 2|S|-1).$$

Moreover, if $S\cap -S=\emptyset$, then $|\Sigma_0(S)|\geq 2|S|$.

Lemma 2.7 **([9]).** *Let S be a subset of an abelian group G such that $0\notin S$ and $14\leq |S|$. Then one of the following conditions holds:*

(i) $|\Sigma_0(S)|\geq \min(|G|-3, 3|S|-3)$.

(ii) There is a subgroup $H\neq G$ such that $|S\cap H|\geq |S|-1$.

Let X be a subset of G with cardinality k. Let $\{x_1,\dots,x_k\}$ be an ordering of X. For $0\leq i\leq k$, set

$$X_i = \{x_j \mid 1\leq j\leq i\} \text{ and } B_i = \Sigma_0(X_i).$$

The ordering $\{x_1,\dots,x_k\}$ is called a *resolving sequence* of X if, for each $i=1,\dots,k$,

$$\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) \mid 1\leq j\leq i\}.$$

The *critical index* of the resolving sequence is the largest integer $t\in [1,k+1]$ such that X_{t-1} generates a proper subgroup of G. Clearly, every nonempty subset S has a resolving sequence.

We need the following basic property of resolving sequences which is implicit in [6].

Lemma 2.8. *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 $\{x_1,\dots,x_k\}$ be a resolving sequence of X with critical index t. Then, there is a subset $V\subset X$ such that $|V|=t-1$, $\langle V\rangle\neq G$ and*

$$|\Sigma_0(X)| \geq 4|V| + \frac{(|X|+|V|+5)(|X|-|V|-1)-2}{4} \tag{4}$$

Proof. This is essentially formula (4) of [6]. By using inequality (2) we have

$$|\Sigma_0(X)| \geq \lambda_{B_k}(x_k)+\cdots+\lambda_{B_{t+1}}(x_{t+1})+|B_t|.$$

By Lemma 3 we have $\lambda_{B_i}(x_i)\geq \lceil\frac{i+1}{2}\rceil$ for each $i\geq t$. On the other hand, by Lemma 2.6, we have $|B_{t-1}|\geq 2(t-1)$. By the definition of t, we then have $|B_t|\geq |B_{t-1}|+|x_t+B_{t-1}|=2|B_{t-1}|\geq 4(t-1)$. By taking $V=X_{t-1}$, we have the claimed inequality. ∎

The following Lemma provides a class of sets whose subset sums do not cover the host group.

Lemma 2.9. *Let G be a finite abelian group with order n. Let H be a proper subgroup of G and S a subset of $G\setminus\{0\}$.*

If $\Sigma_0(S\setminus H)+H\neq G$ then

(i) $\Sigma_0(S)\neq G$.

(ii) If $|G|/|H|$ is a prime, then

$$|S\setminus H|\leq\frac{|G|}{|H|}-2.$$

Moreover, if $|S\setminus H|=\frac{|G|}{|H|}-2>0$, then there is $y\notin H$ such that

$$S\subseteq H\cup(y+H)\cup(-y+H).$$

Proof. We have $\Sigma_0(S)\neq G$, since otherwise

$$G=\Sigma_0(S)=\Sigma_0(S\cap H)+\Sigma_0(S\setminus H)\subseteq H+\Sigma_0(S\setminus H).$$

Assume now that $q=|G|/|H|$ is a prime and $S\not\subset H$.

By $\overline{x}$ we shall mean $\phi(x)$, where $\phi:G\to G/H$ is the canonical morphism. Put $S\setminus H=\{a_1,\dots,a_j\}$. From our assumption we have $\Sigma_0(\overline{S\setminus H})\neq G/H$. By the Cauchy–Davenport Theorem,

$$|\Sigma_0(\overline{S\setminus H})|=|\{0,\overline{a_1})\}+\cdots+\{0,\overline{a_j}\}|\geq\min(q,j+1).$$

It follows that $j\leq q-2$.

Assume now $j=q-2$. If there is i such that $\overline{a_i}\notin\{\overline{a_1},-\overline{a_1}\}$, say $i=2$, then $|\{0,\overline{a_1}\}+\{0,\overline{a_2}\}|=4$. By the Cauchy–Davenport Theorem, $|\{0,\overline{a_1}\}+\cdots+\{0,\overline{a_{q-2}}\}|\geq 3+\min(q,q-3)$. This contradiction proves the last part of the Lemma. ∎

3. Subsets with cardinality $\geq|G|/4$

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 $\Sigma(S)=G$. We next show that these results can be extended to all abelian groups of order $n\geq 67$.

Theorem 3.1. *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 $\langle S\rangle=G$.*

Proof. Suppose first $\Sigma(S)=G$. Since $\Sigma(S)\subseteq\langle S\rangle$, we have $\langle S\rangle=G$.

Suppose now $\langle S\rangle=G$.

Assume first that there is a subgroup $H\neq G$ such that $|H\cap S|\geq|S|-3$. Since $|H|\geq n/3$ we have $|G|=q|H|$ with $q\in\{2,3\}$. Choose $a\in(S\cap H)$ and set $S_1=(S\cap H)\setminus\{a\}$. Since $n\geq 24$ we have $|S_1|\geq(n/2)/2\geq|H|/2$. By Lemma 2.6, $|\Sigma_0(S_1)|\geq|H|-1$ and, by Lemma 2.1,

$$\Sigma_0(S\cap H)=\Sigma_0(S_1)+\{0,a\}=H.$$

Since S generates G we have $|S\setminus H|\geq 1$ and, if $q=3$, then $|S\setminus H|\geq 2$. By Lemma 2.9 (ii) we have $G=\Sigma_0(S\setminus H)+H=\Sigma_0(S\setminus H)+\Sigma_0(S\cap H)$, a contradiction.

So we may assume that, for every subgroup $H\neq G$, $|H\cap S|\leq|S|-4$. We may choose distinct elements $x,x'\in S$, such that $x\neq -x'$. By Lemma 2.7, $|\Sigma_0(S\setminus\{x,x'\})|\geq\min(n-3,3|S|-9)=n-3$. By Lemma 2.1, we have again $\Sigma_0(S)=\Sigma_0(S\setminus\{x,x'\})+\{0,x,x',x+x'\}=G$.

Since $n\geq 67$, Lemma 2.4 implies $\Sigma_0(S)=\Sigma(S)$. This completes the proof. ∎

The next result improves Theorem 3.1 for groups with odd order.

Theorem 3.2. *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 $|S\setminus H|\leq 1$.

Proof. Obviously, (ii) implies (i).

Suppose $\Sigma(S)\neq G$. Since $n\geq 121$ we have $|S|\geq 3\sqrt{n}$ and, by Lemma 2.4, $\Sigma(S)=\Sigma_0(S)$.

Set $k=\lfloor\frac{|S|}{2}\rfloor$. We shall show that there is $X\subset S$ such that $|X|=k$, $X\cap -X=\emptyset$ and

$$2|\Sigma_0(X)|\leq n. \tag{5}$$

Let S' be a subset of S such that $|S'|=2k$. Clearly we may partition $S'=X\cup Z$ such that $|X|=|Z|=k$ and $X\cap -X=Z\cap -Z=\emptyset$. Since $\Sigma_0(S)\neq G$, we have by Lemma 2.1, $|\Sigma_0(X)|+|\Sigma_0(Z)|\leq n$. Therefore, we may assume that X verifies (5).

Suppose that $\langle X\rangle=G$. By Corollary 2.8 there is $V\subset X$ such that $\langle V\rangle\neq G$ verifying (4). Put $v=|V|$.

By (5) and (4), we have

$$16v+(k-v-1)(k+v+5)-2n-2\leq 0.$$

Since $k \geq \frac{|S|-1}{2} \geq \frac{n}{8}$, we have $16v+(\frac{n}{8}-v-1)(\frac{n}{8}+v+5)-2n-2 \leq 0$. Therefore

$$v^2 - 10v - (1/64)n^2 + (3/2)n + 7 \geq 0$$

It follows that either $v \leq 5 - \frac{1}{8}\sqrt{n^2-96n+1152}$ or $v \geq 5 + \frac{1}{8}\sqrt{n^2-96n+1152}$. Since $v \geq 0$ and $n \geq 184$, we have $v \geq 5 + \frac{1}{8}\sqrt{n^2-96n+1152} > \frac{n}{9}+1$.

Let H be the subgroup generated by V. Since $|H| \geq 2|V|+1 > 2n/9$ and n is odd, then $|G|/|H|=3$. Let p' be the smallest prime dividing $|H|$. We have $|V| > \frac{n}{9}+1$. Hence, $|V| \geq \frac{n}{pp'}+p'-1 \geq \frac{|H|}{p'}+p'-1$. By Lemma 2.3, $\Sigma(V)=H$.

We have $\Sigma_0(S\setminus H)+H \neq G$, since otherwise $G=\Sigma_0(V)+\Sigma_0(S\setminus H) \subseteq \Sigma_0(S)=\Sigma(S)$. By Lemma 2.9, $|S\setminus H| \leq 1$. This proves (ii) in this case.

Suppose that X generates a proper subgroup H of G. Since $|H| \geq 2|X|+1 > n/4$ and n is odd we have $|H|=n/3$. Let p' be the smallest prime dividing $|H|$. We have $|X| \geq (|S|-1)/2 > n/8 \geq \frac{n}{pp'}+p'-1$. By Lemma 2.3, $\Sigma_0(X)=H$. By Lemma 2.9, $|S\setminus H| \geq 1$. This completes the proof. ∎

4. Extremal sets

In this Section we shall determine the structure of the sets $S \subset G\setminus\{0\}$ for which $\Sigma(S) \neq G$ and S has the critical cardinality $h+p-3$, where $|G|=ph$ and p is the smallest prime dividing $|G|$. By Theorem 3.2 we only need to consider the case when $p \geq 5$.

Theorem 4.1. *Let G be a finite abelian group with order $n=ph$, where $p \geq 5$ is the smallest prime dividing n. Also assume that h is composite and $h \geq 7p+3$. Let S be a subset of $G\setminus\{0\}$ such that $|S|=h+p-3$. Then the following conditions are equivalent.*

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

(ii) There are a subgroup H of order h and $y \notin H$ such that

$$(H \setminus \{0\}) \subseteq S \text{ and } S \subseteq H \cup (y+H) \cup (-y+H).$$

Proof. Obviously, (ii) implies (i).

Suppose $\Sigma(S) \neq G$. By Lemma 2.4, $|S|^2 > 9ph$ implies $\Sigma(S)=\Sigma_0(S)$.

Set $k(n)=(|S|-1)/2=\frac{n+p^2}{2p}-2$. We shall write sometimes k instead of $k(n)$.

We shall show that there is $X \subset S$ such that $|X|=k$, $X \cap -X=\emptyset$ and

$$2|\Sigma_0(X)|+\frac{k}{2}+1 \leq n. \tag{6}$$

Clearly, we may partition $S = U \cup V$ such that $|U| = |V| - 1 = k$ and $U \cap -U = V \cap -V = \emptyset$. We consider two cases.

Case 1. $|\Sigma(V)| \leq \frac{n}{2}$.

Put $C = \Sigma_0(V)$. By (3), there is $y \in V$ such that $\lambda_C(y) \geq \frac{k+2}{2}$. Then (2) implies $|\Sigma_0(V)| \geq |\Sigma_0(V \setminus \{y\})| + \frac{k}{2} + 1$.

Since $G \neq \Sigma_0(S) = \Sigma_0(U) + \Sigma_0(V)$ we have, by Lemma 2.1, $|\Sigma_0(U)| + |\Sigma_0(V \setminus \{y\})| + \frac{k}{2} + 1 \leq n$.

Case 2. $|\Sigma_0(V)| > \frac{n}{2}$.

By Lemma 2.1, $|\Sigma_0(U)| \leq \frac{n}{2}$. Put $E = \Sigma_0(U)$. By (3), there is $y \in V$, such that $\lambda_E(y) \geq \frac{k+2}{2}$. Therefore, $|\Sigma_0(U \cup \{y\})| = |\Sigma_0(U)| + \lambda_E(y) \geq |\Sigma_0(U)| + \frac{k}{2} + 1$.

By Lemma 2.1, $G \neq \Sigma_0(S) = \Sigma_0(U \cup \{y\}) + \Sigma_0(V \setminus \{y\})$ implies $|\Sigma_0(U)| + |\Sigma(V \setminus \{y\})| + \frac{k}{2} + 1 \leq n$.

In both cases, one of the sets $U, V \setminus \{y\}$, verifies (6). Let us denote this set by X.

We have $|\langle X \rangle| \geq |X \cup -X \cup \{0\}| = 2k+1 = \frac{n}{p} + p - 3$. Therefore X generates G.

By Corollary 2.8, there is $V \subset G$ such that $\langle V \rangle \neq G$ verifying (4). Put $v = |V|$.

Set

$$F(v,n) = 8v - n + \frac{(k(n)+v+5)(k(n)-v-1)+k(n)}{2}$$
$$= \frac{1}{2}(-v^2 + 10v + k^2(n) + 5k(n) - 2n - 5).$$

By (6) and (4), we have

$$F(v,n) \leq 0. \tag{7}$$

Let us show that $v \geq 5$. Suppose on the contrary that $0 \leq v \leq 4$. We have $\frac{\partial}{\partial n} F(v,n) = \frac{n - 3p^2 + p}{4p^2} > 0$. Therefore, since $n > 7p^2$, we have $0 \geq F(v,n) \geq F(0,n) > F(0, 7p^2) = p^2 + 2p - \frac{11}{2} > 0$, a contradiction.

Let us show that

$$v > \frac{n}{p^2} + p - 2. \tag{8}$$

Assume the contrary. Since $v \geq 5$, $\frac{\partial}{\partial v} F(v,n) = 5 - v \geq 0$, then $G(n) = F(\frac{n}{p^2} + p - 2, n) \leq F(v,n)$. By (7) we have

$$G(n) \leq 0. \tag{9}$$

Using $n \geq 7p^2$, we have $4p^2 G'(n) = n(p^2 - 4) - p^2(3p^2 + 3p - 28) \geq p^3(4p - 3) > 0$. Then, $G(n) \geq G(7p^2) = \frac{1}{2}(p^2 + 4p + 14) > 0$ contradicting (9).

Let H be the subgroup generated by V and let p' be the smallest prime dividing $|H|$. By (8), $|V|>\frac{n}{p^2}+p-2\geq\frac{n}{pp'}+p'-2$. By Lemma 2.3, $\Sigma_0(V)=H$.

Since $|H|>\frac{n}{p^2}$, we see easily that $q=\frac{|G|}{|H|}$ is a prime. Since $G\neq\Sigma_0(V)+\Sigma_0(S\setminus H)$, we have $G\neq H+\Sigma_0(S\setminus H)$. By Lemma 2.9, $|S\setminus H|\leq q-2$.

We have

$$\frac{n}{q}=|H|\geq|S\cap H|+1\geq\frac{n}{p}+p-3-(q-2)+1=\frac{n}{p}+p-q,$$

which implies $p=q$ and $\frac{n}{p}=|H|=|S\cap H|+1$. Hence, $|S\setminus H|=p-2$. Then Lemma 2.9 implies (ii). ∎

5. Large sets

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 with some additional restrictions on n and its smaller prime divisor. More precisely, we prove the following Theorem.

Theorem 5.1. *Let G be a finite abelian group with order $n=ph$, where $p\geq 5$ is the smallest prime dividing n. Assume that $n\geq 15p^2$ and that h is 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 h such that

$$|S\setminus H|\leq p-2 \text{ and } \Sigma(S\setminus H)+H\neq G.$$

Proof. Obviously (ii) implies (i).

Suppose $\Sigma(S)\neq G$. By lemma 2.4, $n\geq 15p^2$ implies $\Sigma(S)=\Sigma_0(S)$.

Put $k_0=\lfloor|S|/2\rfloor$. Let S' be a subset of S with cardinality $2k_0$ and partition S' into two sets $S'=X\cup Z$ such that $|X|=|Z|=k_0$ and $X\cap -X=Z\cap -Z=\emptyset$. Since $G\neq\Sigma_0(S')=\Sigma_0(X)+\Sigma_0(Y)$ we have, by Lemma 2.1, $|\Sigma_0(X)|+|\Sigma_0(Z)|\leq n$. Therefore we may assume that

$$2|\Sigma_0(X)|\leq n. \tag{10}$$

Suppose that X generates a proper subgroup H of G. Since $|H|\geq 2|X|+1\geq\frac{n}{p+2}+p$ and n is odd, we have $|H|=n/p$.

Let p' be the smallest prime dividing $|H|$. Since $|X| \geq \frac{n}{pp'} + p' - 1$, we have $\Sigma(X) = H$. We have $\Sigma_0(S \backslash H) + H \neq G$, since otherwise $G = \Sigma(X) + \Sigma_0(S \backslash H) \subseteq \Sigma_0(S) = \Sigma(S)$. By Lemma 2.9,

$$|S \setminus H| \leq p - 2.$$

This proves (ii) when $\langle X \rangle \neq G$.

Suppose now that $\langle X \rangle = G$. By Corollary 2.8 there is $V \subset G$ such that $\langle V \rangle \neq G$ verifying (4). Put $v = |V|$ and let $F_0(v, n, r) = 16v + (r - v - 1)(r + v + 5) - 2n - 2$. By (10) and (4), we have

$$F_0(v, n, k_0(n)) = 16v + (k_0 - v - 1)(k_0 + v + 5) - 2n - 2 \leq 0.$$

Set $k(n) = \frac{n + p^2 + p + 1}{2(p+2)}$. We have $k(n) < k_0(n)$. We shall write sometimes k instead of $k(n)$. We clearly have $F(v, n) = F_0(v, n, k(n)) \leq F_0(v, n, k_0(n))$. Therefore

$$0 \geq F(v, n) = -v^2 + 10v + k^2(n) + 4k(n) - 2n - 7. \tag{11}$$

We shall show that $v \geq 5$. Suppose on the contrary that $0 \leq v \leq 4$. We have $\frac{\partial}{\partial n} F(v, n) = 2k(n)k'(n) + 4k'(n) - 2 > 0$ for $n \geq 15p^2$, and $\frac{\partial}{\partial v} F(v, n) = 10 - 2v > 0$. Now, by (11), we have

$$0 \geq F(v, n) \geq F(0, n) \geq F(0, 15p^2) = \frac{136p^4 - 320p^3 - 211p^2 - 86p - 95}{4(p+2)^2}.$$

Using $p \geq 3$ we easily see that the right hand size is positive, a contradiction.

Let us now show that

$$v > \frac{n}{p^2} + p - 2. \tag{12}$$

Assume the contrary and set $G(n) = F(\frac{n}{p^2} + p - 2, n)$. Since $5 \leq v \leq \frac{n}{p^2} + p - 2$ and $\frac{\partial}{\partial v} F(v, n) = 10 - 2v$, (11) implies

$$G(n) \leq 0. \tag{13}$$

We have $2(p+2)^2 p^4 G'(n) = n(p^4 - 4p^2 - 16p - 16) - p^2(3p^4 - 15p^3 + 5p^2 + 96p + 112)$. Using $p \geq 5$ and $n \geq 15p^2$, $2(p+2)^2 p^4 G'(n) \geq 2(p+2)^2 p^4 G'(15p^2) = p^2(12p^4 + 15p^3 - 65p^2 - 144p + 352) > 0$. It follows that

$$0 \geq G(n) \geq G(15p^2) = \frac{132p^4 - 400p^3 - 639p^2 - 966p - 719}{4(p+2)^2} > 0,$$

a contradiction.

Let H be the subgroup generated by V and let p' be the smallest prime dividing $|H|$. By (12), $|V| > \frac{n}{p^2} + p - 2 \geq \frac{n}{pp'} + p' - 2$. By Lemma 2.3, $\Sigma(V) = H$.

Since $|H|>\frac{n}{p^2}$, we see easily that $q=\frac{|G|}{|H|}$ is a prime. We have $\Sigma(S\backslash H)+H\neq G$, since otherwise $G=\Sigma(V)+\Sigma(S\setminus H)\subseteq\Sigma(S)$. By Lemma 2.9,

$$|S\setminus H|\leq q-2.$$

We have $q=p$, since otherwise,

$$|S|\leq\frac{n}{q}+q-3\leq\frac{n}{p+2}+p-1,$$

a contradiction. This completes the proof. ∎

Acknowledgements

The authors are grateful to the anonymous referees for their helpful suggestions and remarks which led to an improved version of the paper.

References

[1] 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.
[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(3)** (1999), 233–237.
[7] J. R. Griggs and B. Poonen: *Subset Sums for Finite Abelian Groups*, Preprint.
[8] Y. O. Hamidoune: Adding distinct congruence classes, *Combinatorics, Probability and Computing* **7** (1998), 81–87.
[9] Y. O. Hamidoune, A. S. Lladó and O. Serra: On sets with a small subset sum, *Combinatorics, Probability and Computing* **8** (1999), 461–466.
[10] E. Lipkin: Subset sums of sets of residues, *Structure Theory of Set Addition, Astérisque* **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 for 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.

W. Gao

Department of Computer Science and Technology
University of Petroleum
Beijing
102200, China
wdgao@public.fhnet.cn.net

Y. O. Hamidoune

Université P. et M. Curie
E. Combinatoire
Case 189, 4 Place Jussieu
75005 Paris
France
yha@ccr.jussiev.fr

A. Lladó

Universitat Politècnica de Catalunya
Dept. of Applied Mathematics
Jordi Girona, 1
E-08034 Barcelona
Spain
allado@mat.upc.es

O. Serra

Universitat Politècnica de Catalunya
Dept. of Applied Mathematics
Jordi Girona, 1
E-08034 Barcelona
Spain
oserra@mat.upc.es