Open Journal of Discrete Mathematics, 2013, 3, 93-96
http://dx.doi.org/10.4236/ojdm.2013.32018 Published Online April 2013 (http://www.scirp.org/journal/ojdm)

Scientific Research

Inverse Problems on Critical Number in Finite Groups

Qinghong Wang[1], Jujuan Zhuang[2]
[1]Colleage of Science, Tianjin University of Technology, Tianjin, China
[2]Department of Mathematics, Dalian Maritime University, Dalian, China
Email: wqh1208@yahoo.com.cn, jjzhuang1979@yahoo.com.cn

Received February 28, 2013; revised March 28, 2013; accepted April 20, 2013

ABSTRACT

Let G be a finite nilpotent group of odd order and S be a subset of $G\setminus\{0\}$. We say that S is **complete** if every element of G can be represented as a sum of different elements of S and **incomplete** otherwise. In this paper, we obtain the characterization of large incomplete sets.

Keywords: Critical Number; Incomplete Set; Finite Nilpotent Group

1. Introduction

Let G be a finite additively written group (not necessarily commutative). Let $S=\{a_1,\cdots,a_k\}$ be a subset of $G\setminus\{0\}$. Define $\Sigma(S)=\{a_{i_1}+\cdots+a_{i_l}\mid i_1,\cdots,i_l$ are distinct $1\le l\le k\}$. For technical reasons we define $\Sigma_0(S)=\Sigma(S)\cup\{0\}$. We call S an **additive basis** of G if $\Sigma(S)=G$. The critical number $\mathrm{cr}(G)$ of G is the smallest integer t such that every subset S of $G\setminus\{0\}$ with $|S|\ge t$ forms an additive basis of G. $\mathrm{cr}(G)$ was first introduced and studied by Erdős and Heilbronn in 1964 [1] for $G=\mathbb{Z}_p$ where p is a prime. This parameter has been studied for a long time and its exact value is known for a large number of groups (see [2-10]).

Following Erdős [1], we say that S is **complete** if $\Sigma(S)=G$ and **incomplete** otherwise.

In this paper, we would like to study the following question: What is the structure of a relatively large incomplete set? Technically speaking, we would like to have a characterization for incomplete sets of relatively large size. Such a characterization has been obtained recently for finite abelian groups (see [11-13]). In this paper, we shall prove the following result.

Theorem 1.1. Let G be a finite nilpotent group with order $n=ph$, where $p\ge 5$ is the smallest prime dividing n. Also assume that h is composite and $h\ge 7p+3$. Let S be a subset of $G\setminus\{0\}$ such that $|S|=h+p-3$. If S is incomplete, then there exist a subgroup H of order h and $g\notin H$ such that $(H\setminus\{0\})\subseteq S$ and $S\subseteq H\cup(g+H)\cup(-g+H)$.

2. Notations and Tools

If S be a subset of the group G, we shall denote by $|S|$ the cardinality of S, by $\langle S\rangle$ the subgroup generated by S. If $A_1,\cdots,A_n$ are subsets of G, let $A_1+\cdots+A_n$ denote the set of all sums $a_1+\cdots+a_n$, where $a_i\in A_i$. Recall the following well known result obtained by Cauchy and Davenport.

Lemma 2.1. Let p be a prime number. Let X and Y be non-empty subsets of $\mathbb{Z}_p$. Then

$$|X+Y|\ge\min\{p,|X|+|Y|-1\}.$$

We also use the following well known result.

Lemma 2.2 [14]. Let G be a finite group. Let X and Y be subsets of G such that $X+Y\ne G$. Then

$$|X|+|Y|\le|G|.$$

Lemma 2.3 [3]. Let G be a cyclic group of order pq, where p,q are primes. Then

$$p+q-2\le\mathrm{cr}(G)\le p+q-1.$$

Lemma 2.4 [8]. Let G be a non-abelian group of order $pq\ge 10$, where p,q are distinct primes. Then $\mathrm{cr}(G)=p+q-2$.

Lemma 2.5 [10]. Let G be a finite nilpotent group of odd order and let p be the smallest prime dividing $|G|$. If $|G|/p$ is a composite number then $\mathrm{cr}(G)=|G|/p+p-2$.

Lemma 2.6. Let G be a finite nilpotent group of odd order and let p be the smallest prime dividing $|G|$. If $|S|=|G|/p+p-1$ then $\Sigma(S)=G$.

Proof. Obviously, this follows from Lemmas 2.3-2.5.

Lemma 2.7 [15]. Let S be a subset of a finite group G of order n. If $|S| \ge 3\sqrt{n}$ then $0 \in \Sigma(S)$.

Lemma 2.8 [16]. Let G be a noncyclic group. Let S be a subset $G \setminus \{0\}$. Then $|\Sigma_0(S)| \ge \min\{|G|-1, 2|S|\}$.

Let $B \subseteq G$ and $x \in G$. As usual, we write $\lambda_B(x) = |(B+x) \setminus B|$. We have the following result obtained by Olson.

Lemma 2.9 [5]. Let S be a nonempty subset of $G \setminus \{0\}$ and $y \in S$. Let $B = \Sigma(S)$. Then

$$|\Sigma_0(S)| \ge |\Sigma_0(S \setminus y)| + \lambda_B(y).$$

We shall also use the following result of Olson.

Lemma 2.10. Let G be a finite group and let S be a generating subset of G such that $0 \notin S$. Let B be a subset of G such that $|B| \le |G|/2$. Then there is $x \in S$ such that

$$\lambda_B(x) \ge \min\left(\frac{|B|+1}{2}, \frac{|S \cup -S|+2}{4}\right).$$

This result follows by applying Lemma 3.1 of [15] to $S \cup -S$ Let x be a subset of G with cardinality k. Let $\{x_1, \cdots, x_k\}$ be an ordering of X. For $0 \le i \le k$, set $X_i = \{x_j \mid 1 \le j \le i\}$ and $B_i = \Sigma_0(X_i)$.

The ordering $\{x_1, \cdots, x_k\}$ is called a **resolving sequence** of X if, for each $i = 1, \cdots, k$, $\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) \mid 1 \le j \le i\}$.

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

We need the following basic property of resolving sequence which is implicit in [5].

Lemma 2.11. Let X be a generating subset of a finite group G such that

$$X \cap -X = \varnothing \text{ and } 2|\Sigma_0(X)| \le |G|.$$

Let the ordering $\{x_1, \cdots, x_k\}$ be a resolving sequence of X with critical index t. Then, there is a subset $V \subset X$ such that $|V| = t-1, \langle V \rangle \ne G$ and

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

Proof. This is essentially formula (4) of [5]. By Lemma 2.9 we have

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

By Lemma 2.10 we have $\lambda_{B_i}(x_i) \ge \left\lceil \frac{i+1}{2} \right\rceil$ for each $i \ge t$. On the other hand, by Lemma 2.8 we have $|B_{t-1}| \ge 2(t-1)$. By the definition of t, we have $|B_t| \ge |B_{t-1}| + |x_t + B_{t-1}| = 2|B_{t-1}| \ge 4(t-1)$. By taking $V = X_{t-1}$, we have the claimed inequality.

Lemma 2.12. Let G be a finite group with order $n = ph$, where $p \ge 5$ is the smallest prime dividing n and $h \ge 7p+3$. Let S be a subset of $G \setminus \{0\}$ such that $|S| = h+p-3$ and $\Sigma(S) \ne G$. Then there exists a set $X \subset S$ such that $|X| = (|S|-1)/2, X \cap -X = \varnothing$ and $2|\Sigma_0(X)| + \frac{|S|-1}{4} + 1 \le n.$

Proof. Since $h \ge 7p+3$ and p is the smallest prime dividing n, we have $|S|^2 > 9ph$. By Lemma 2.7, $\Sigma(S) = \Sigma_0(S)$.

Clearly, we may partition $S = U \cup V$ such that $|U| = |V| - 1$ and $U \cap -U = V \cap -V = \varnothing$.

We consider two cases.

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

Set $C = \Sigma_0(V)$. By Lemma 2.10, there is $y \in V$ such that

$$\lambda_C(y) \ge \frac{|S|-1}{4} + 1.$$

It follows $|\Sigma_0(V)| \ge |\Sigma_0(V \setminus \{y\})| + \frac{|S|-1}{4} + 1$ by Lemma 2.9.

Since $G \ne \Sigma_0(S) \supseteq \Sigma_0(U) + \Sigma_0(V)$ we have, by Lemma 2.2,

$$|\Sigma_0(U)| + |\Sigma_0(V \setminus \{y\})| + \frac{|S|-1}{4} + 1 \le n.$$

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

By Lemma 2.2, $|\Sigma_0(U)| \le \frac{n}{2}$. Put $E = \Sigma_0(U)$. By Lemma 2.10, there is $y \in V$, such that

$$\lambda_E(y) \ge \frac{|S|-1}{4} + 1.$$

Therefore,

$$|\Sigma_0(U \cup \{y\})| \ge |\Sigma_0(U)| + \lambda_E(y) \ge +1 + \frac{|S|-1}{4}.$$

By Lemma 2.2, $G \ne \Sigma_0(S) \supseteq \Sigma_0(U \cup \{y\}) + \Sigma_0(V \setminus \{y\})$ implies

$$|\Sigma_0(U)| + |\Sigma_0(V \setminus \{y\})| + \frac{|S|-1}{4} + 1 \le n.$$

In both cases, one of the sets $U, V \setminus \{y\}$ verifies the conclusion of the lemma. This completes the proof.

Lemma 2.13. Let $k = \frac{n+p^2}{2p} - 2$, where p is the smallest prime dividing n. If

$$8v-n+\frac{(k+v+5)(k-v-1)+k}{2}\le 0$$

and $n>7p^2$, then $v>\frac{n}{p^2}+p-2.$

Proof. Set

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

and $G(n)=F\left(\frac{n}{p^2}+p-2,n\right)$.

First, let us show that $v\ge 5$. Assume the contrary that $0\le v\le 4$. We have

$$\frac{\partial}{\partial n}F(v,n)=\frac{n-3p^2+p}{4p^2}>0.$$

Since $n>7p^2$, we have

$$F(v,n)\ge F(0,n)\ge F\left(0,7p^2\right)=p^2+2p-\frac{11}{2}>0,$$

a contradiction to $F(v,n)\le 0.$

Second, let us show that $v>\frac{n}{p^2}+p-2$.

Assume the contrary. Since $v\ge 5$, $\frac{\partial}{\partial v}F(v,n)=5-v\le 0$, we have

1) $G(n)\le F(v,n)\le 0.$

On the other hand, since $n\ge 7p^2$, we have

$$4p^4G'(n)=n\left(p^2-4\right)-p^2\left(3p^2+3p-28\right)$$
$$\ge p^3(4p-3)>0$$

Then, $G(n)\ge G\left(7p^2\right)=\frac{1}{2}\left(p^2+4p+14\right)>0,$

A contradiction to (1). Therefore, we have $v>\frac{n}{p^2}+p-2.$ This completes the proof.

Lemma 2.14. Let G be a finite group with order n. Let H be a proper subgroup of G and S a subset of $G\setminus\{0\}$. If $\Sigma_0(S\setminus H)+H\ne G$ and $|G|/|H|$ is a prime, then $|S\setminus H|\le\frac{|G|}{|H|}-2$.

Moreover, if $|S\setminus H|=\frac{|G|}{|H|}-2>0$ then there is $g\notin H$ such that $S\subseteq H\cup(g+H)\cup(-g+H).$

Proof. By $\bar{x}$ we shall mean $\phi(x)$, where $G\to G/H$ is the canonical morphism. Put $S\setminus H=\{a_1,\cdots,a_j\}$.

From our assumption we have $\Sigma_0\left(\overline{S\setminus H}\right)\ne G/H$.

By Lemma 2.1, we have

$$\left|\Sigma_0\left(\overline{S\setminus H}\right)\right|=\left|\{0,\bar{a}_1\}+\cdots+\{0,\bar{a}_j\}\right|\ge(q,j+1).$$

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

Assume now $j=q-2$. If there is i such that $\bar{a}_i\notin\{\bar{a}_1,-\bar{a}_1\}$, say $i=2$, then $\left|\{0,\bar{a}_1\}+\{0,\bar{a}_2\}\right|=4.$

By Lemma 2.1, we have

$$\left|\{0,\bar{a}_1\}+\cdots+\{0,\bar{a}_{q-2}\}\right|\ge 3+\min(q,q-3)=q,$$

a contradiction to $\Sigma_0(S\setminus H)+H\ne G.$ Then there is $g\notin H$ such that

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

3. Proof of Theorem 1.1

Proof. By Lemma 2.12 there exists a set $X\subset S$ such that $|X|=(|S|-1)/2$, $X\cap -X=\varnothing$ and

$$2|\Sigma_0(X)|+\frac{|S|-1}{4}+1\le n. \quad (2)$$

We have

$$|\langle X\rangle|\ge|X\cup -X\cup\{0\}|=\frac{n}{p}+p-3.$$

Therefore X generates G.

By Lemma 2.11, there is $V\subset X$ such that $\langle V\rangle\ne G$ verifying

$$|\Sigma_0(X)|\ge 4|V|+\frac{(|X|+|V|+5)(|X|-|V|-1)-2}{4}. \quad (3)$$

Let H be the subgroup generated by V and let p' be the smallest prime dividing $|H|$.

Put $v=|V|, k=\frac{n+p^2}{2p}-2.$ Set

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

By (2) and (3), we have $F(v,n)\le 0.$

By Lemma 2.13, we have

$$|V|>\frac{n}{p^2}+p-2\ge\frac{n}{pp'}+p'-2.$$

By Lemma 2.6, we get $\Sigma_0(V)=H.$

Since $|H|>\frac{n}{p^2}$, we see easily that $q=\frac{|G|}{|H|}$ is a prime. Since S is incomplete, we have $G\ne\Sigma_0(V)+\Sigma_0(S\setminus H)=H+\Sigma_0(S\setminus H).$ By Lemma 2.14, $|S\setminus H|\le q-2.$

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, $|S\setminus H|=p-2$. By Lemma 2.14, there exist a subgroup H of order h and $g\notin H$ such that

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

4. Acknowledgements

The authors would like to thank the referee for his/her very useful suggestions. This work has been supported by the National Science Foundation of China with grant No. 11226279 and 11001035.

REFERENCES

[1] P. Erdős and H. Heibronn, "On the Addition of Residue Classes Mod p," *Acta Arithmetica*, Vol. 9, 1964, pp. 149-159.

[2] J. A. Dias da Silva and Y. O. Hamidoune, "Cyclic Spaces for Grassmann Derivatives and Additive Theory," *Bulletin London Mathematical Society*, Vol. 26, No. 2, 1994, pp. 140-146. doi:10.1112/blms/26.2.140

[3] G. T. Diderrich, "An Addition Theorem for Abelian Groups of Order pq," *Journal of Number Theory*, Vol. 7, No. 1, 1975, pp. 33-48. doi:10.1016/0022-314X(75)90006-2

[4] J. E. Olson, "An Addition Theorem Mod p," *Journal of Combinatorial Theory*, Vol. 5, No. 1, 1968, pp. 45-52. doi:10.1016/S0021-9800(68)80027-4

[5] W. Gao and Y. O. Hamidoune, "On Additive Bases," *Acta Arithmetica*, Vol. 88, 1999, pp. 233-237.

[6] H. B. Mann and Y. F. Wou, "An Addition Theorem for the Elementary Abelian Group of Type (p,p)," *Monatshefte für Mathematik*, Vol. 102, No. 4, 1986, pp. 273-308. doi:10.1007/BF01304301

[7] M. Freeze, W. D. Gao and A. Geroldinger, "The Critical Number of Finite Abelian Groups," *Journal of Number Theory*, Vol. 129, No. 11, 2009, pp. 2766-2777. doi:10.1016/j.jnt.2009.05.016

[8] Q. H. Wang and J. J. Zhuang, "On the Critical Number of Finite Groups of Order pq," *International Journal of Number Theory*, Vol. 8, No. 5, 2012, pp. 1271-1280. doi:10.1142/S1793042112500741

[9] J. R. Griggs, "Spanning Subset Sums for Finite Abelian Groups," *Discrete Mathematics*, Vol. 229, No. 1-3, 2001, pp. 89-99. doi:10.1016/S0012-365X(00)00203-X

[10] Q. H. Wang and Y. K. Qu, "On the Critical Number of Finite Groups (II)," *Ars Combinatoria*, Accepted for Publication in December 2009, to Appear.

[11] W. Gao, Y. O. Hamidoune, A. Llad and O. Serra, "Covering a Finite Abelian Group by Subset Sums," *Combinatorica*, Vol. 23, No. 4, 2003, pp. 599-611. doi:10.1007/s00493-003-0036-x

[12] V. H. Vu, "Structure of Large Incomplete Sets in Finite Abelian Groups," *Combinatorica*, Vol. 30, No. 2, 2010, pp. 225-237. doi:10.1007/s00493-010-2336-2

[13] D. Guo, Y. K. Qu, G. Q. Wang and Q. H. Wang, "Extremal Incomplete Sets in Finite Abelian Groups," *Ars Combinatoria*, Accepted for Publication in December 2011, to Appear.

[14] H. B. Mann, "Addition Theorems," 2nd Edition, R. E. Krieger, New York, 1976.

[15] J. E. Olson, "Sum of Sets of Group Elements," *Acta Arithmetica*, Vol. 28, No. 76, 1975, pp. 147-156.

[16] Y. O. Hamidoune, "Adding Distinct Congruence Classes," *Combinatorics, Probability and Computing*, Vol. 7, No. 1, 1998, pp. 81-87. doi:10.1017/S0963548397003180