Inverse Problems on Critical Number in Finite Groups

Qinghong Wang¹, Jujuan Zhuang²
¹College of Science, Tianjin University of Technology, Tianjin, China
²Department 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

Copyright © 2013 Qinghong Wang, Jujuan Zhuang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

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 $S = \{a_1, \ldots, a_n\}$ be a subset of $G \setminus \{0\}$. Define $S(S) = \{a_1 + \cdots + a_k | a_1, \ldots, a_k \text{ are distinct } 1 \leq l \leq k \}$. For technical reasons we define $\Sigma(S) = \{ \sum(S) \cup \{0\} \}$. We call $S$ an additive basis of $G$ if $\Sigma(S) = G$. The critical number $\text{cr}(G)$ of $G$ is the smallest integer $t$ such that every subset $S$ of $G \setminus \{0\}$ with $|S| > t$ forms an additive basis of $G$. The critical number $\text{cr}(G)$ 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 $p \geq 5$ 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 $|S| = h/p - 3$. If $S$ is incomplete, then there exist a subgroup $H$ of order $h$ and $g \in H$ 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 $A_1, \ldots, A_n$ 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

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

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 $X + Y \neq G$. Then

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

Lemma 2.3 [3]. Let $G$ be a cyclic group of order $pq$, where $p,q$ are primes. Then $p + q + 1 \leq \text{cr}(G) \leq p + q - 1$.

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

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 $\text{cr}(G) = |G|/p + p - 2$.

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 \( |S| \geq 3\sqrt{n} \) then \( 0 \in \Sigma(S) \).

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

Let \( B \subseteq G \) and \( x \in G \). As usual, we write \( \lambda_g(x) = \mid \langle B + x \rangle \setminus B \mid \). 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

\[
\Sigma_0(S) \geq \Sigma_0(S \setminus y) + \lambda_g(y).
\]

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 \( |B| \leq |G|/2 \). Then there is \( x \in S \) such that

\[
\lambda_g(x) \geq \min\left( \frac{|B| + 1}{2}, \frac{|S \cup \{x\} - 2 + 4}{4} \right).
\]

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

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

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

The **critical index** of the resolving sequence is the largest \( t \in [1, k + 1] \) such that \( X_{t \cdots} \) 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

\( X \cap -X = \emptyset \) and \( 2\mid \Sigma_0(X) \mid \leq \mid G \mid \).

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

\[
\mid \Sigma_0(V) \mid \geq 4|V| + \left( \frac{|X| + |V| + 5}{4} \right) \frac{|X| - |V| - 1}{2} - 2.
\]

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

\[
\mid \Sigma_0(X) \mid \geq \sum_{i \leq t} \lambda_{x_i}(x_i) + \lambda_{B_t}(x_t).
\]

By Lemma 2.10 we have \( \lambda_{x_i}(x_i) \geq \frac{i + 1}{2} \) for each \( i \leq t \). On the other hand, by Lemma 2.8 we have

\[ |B_{t - 1}| \geq 2(t - 1). \]

By the definition of \( t \), we have

\[ |B_t| \geq |B_{t - 1}| + |x_t + B_{t - 1}| = 2|B_{t - 1}| \geq 4(t - 1). \]

By taking

\[ V = X_{t \cdots} \]

we have the claimed inequality.

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

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

Clearly, we may partition \( S = U \cup V \) such that \( |U| = |V| - 1 \) and \( U \cap -V = V \cap -V = \emptyset \).

We consider two cases.

**Case 1.** \( |(U \cup V)| < \frac{n}{2} \).

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

\[ \lambda_y(y) \geq \frac{|S| - 1}{4} + 1. \]

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

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

\[ |\Sigma_0(U)| + |\Sigma_0(V \setminus \{y\})| + \frac{|S| - 1}{4} + 1 \leq k \]

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

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

\[ \lambda_{y}(y) \geq \frac{|S| - 1}{4} + 1. \]

Therefore,

\[ |\Sigma_0(U \cup \{y\})| \geq |\Sigma_0(U)| + \lambda_{y}(y) \geq \frac{|S| - 1}{4} + 1. \]

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

\[ |\Sigma_0(U)| + |\Sigma_0(V \setminus \{y\})| + \frac{|S| - 1}{4} + 1 \leq k \]

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
\[
8v-n + \frac{(k+v+5)(k-v-1)+k}{2} \leq 0
\]
and \(n > 7p^2\), then \(v > \frac{n}{p^2} + p - 2\).

**Proof.** Set

\[
F(v,n) = 8v-n + \frac{(k+v+5)(k-v-1)+k}{2} = \frac{1}{2}(k^2+5k-2n-v^2+10v-5)
\]
and \(G(n) = F\left(\frac{n}{p^2} + p-2,n\right)\).

First, let us show that \(v \geq 5\). Assume the contrary that \(0 < v < 4\). We have

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

Since \(n > 7p^2\), we have

\[
F(v,n) \geq F(0,n) \geq F(0,7p^2) = p^2 + 2p - 11 > 0,
\]
a contradiction to \(F(v,n) \leq 0\).

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

Assume the contrary. Since \(v \geq 5\),

\[
\frac{\partial}{\partial v} F(v,n) = 5 - v \leq 0,
\]
we have

1. \(G(n) \leq F(v,n) \leq 0\).

On the other hand, since \(n > 7p^2\), we have

\[
4p^2G'(n) = n(p^2-4) - p^2(3p^2+3p-28) \\
\geq p^3(4p-3) > 0
\]
Then, \(G(n) \geq G(7p^2) = \frac{1}{2}(p^2+4p+14) > 0\),

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 \(\Sigma_0(S \setminus H) + H \neq G\) and \(|G|/|H|\) is a prime, then \(|S \setminus H| \leq \left\lfloor \frac{|G|}{|H|} \right\rfloor - 2\).

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

**Proof.** By \(\overline{S}\) we shall mean \(\phi(x)\), where \(G \rightarrow G/H\) is the canonical morphism. Put \(S \setminus H = \{a_1, \ldots, a_j\}\).

From our assumption we have \(\Sigma_0(S \setminus H) \neq G/H\).

By Lemma 2.1, we have

\[
\left|\Sigma_0(S \setminus H)\right| = \left|\{0, a_1\} + \cdots + \{0, a_j\}\right| \geq (q, j + 1).
\]
It follows that \(j \leq q - 2\).

Assume now \(j = q - 2\). If there is \(i\) such that \(\overline{a_i} \notin \{\overline{a_1}, \ldots, \overline{a_j}\}\), say \(i = 2\), then \(\left|\{0, \overline{a_1}\} + \{0, \overline{a_2}\}\right| = 4\).

By Lemma 2.1, we have

\[
\left|\{0, \overline{a_1}\} + \cdots + \{0, \overline{a_{q-2}}\}\right| \geq 3 + \min(q, q - 3) = q,
\]
a contradiction to \(\Sigma_0(S \setminus H) + H \neq G\).

Therefore \(g \notin H\) such that \(S \subset H \cup (g + H) \cup (-g + H)\).
\[ \frac{n}{q} = \left| H \right| \geq \left| S \cap H \right| + 1 \geq \frac{n}{p} + p - 3(q - 2) + 1 = \frac{n}{p} + p - q, \]

which implies \( p = q \) and \( \frac{n}{p} = \left| H \right| = \left| S \cap H \right| + 1 \). Hence, \( \left| S \setminus H \right| = p - 2 \). By Lemma 2.14, there exist a subgroup \( H \) of order \( h \) and \( g \not\in H \) such that \( \left( H \setminus \{0\} \right) \subseteq S \) 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


