ON THE CRITICAL NUMBER OF FINITE GROUPS (II)

QINGHONG WANG AND YONGKE QU

Abstract. Let G be a finite group and S a subset of $G \setminus \{0\}$. We call S an *additive basis of* G if every element of G can be expressed as a sum over a nonempty subset in some order. Let $cr(G)$ be the smallest integer t such that every subset of $G \setminus \{0\}$ of cardinality t is an additive basis of G. In this paper, we determine $cr(G)$ for the following cases: (i) G is a finite nilpotent group; (ii) G is a group of even order which possesses a subgroup of index 2.

1. Introduction and Main Results

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 $\sum(S) = \{a_{i_1} + \cdots + a_{i_l} | i_1, \cdots, i_l$ are distinct and $1 \le l \le k\}$, and for any $1 \le r \le k$, define $\sum_r(S) = \{a_{i_1} + \cdots + a_{i_r} | i_1, \cdots, i_r$ are distinct$\}$. We call S an *additive basis of* G if $\sum(S) = G$. The critical number $cr(G)$ 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.

Let Z_n be the cyclic group of n elements. $cr(G)$ was first introduced and studied by Erdős and Heilbronn in 1964 for $G = Z_p$ where p is a prime. With many mathematicians' efforts, after nearly half a century, $cr(G)$ has been determined for all finite abelian groups recently (see [3][5][7][10][11][13]).

However, the problem to determine $cr(G)$ for G non-abelian is widely open. So far, we only have the following results in this direction.

Theorem 1.1. *([8], [14]) Let G be a finite group of order n and p be the smallest prime divisor of n. Then, $cr(G) = n/p + p - 2$ providing one of the following conditions holds,*

(i) G is nilpotent, $p \ge 149$ and $n \ge 120p^2$;

AMS 2010: 11B13, 11P50, 20D15. Key Words: critical number, nilpotent group, additive basis.

*Corresponding author: Qinghong Wang, Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China.
E-mail addresses: wqh1208@yahoo.com.cn (Qinghong Wang).

January 3, 2010.

(*ii*) *There exists a subgroup of* G *with index* p *and the other prime divisor of* n *(if exists) is larger than* $6p$, $p \geq 149$ *and* $n \geq 120p^2$*;*

(*iii*) G *be a non-abelian group of order* $pq \geq 10$ *where* q *is a prime.*

In this paper we shall determine $cr(G)$ for all groups G as stated in the abstract by showing the following two results.

Theorem 1.2. *Let* G *be a finite nilpotent group of odd order and let* p *be the smallest prime dividing* $|G|$*. If* $\frac{|G|}{p}$ *is a composite number then* $cr(G) = |G|/p + p - 2$.

Theorem 1.3. *Let* G *be a finite non-abelian group of even order* n *which possesses a subgroup of index* 2*. Then,*

(*i*) *if* $n = 6$ *then* $cr(G) = cr(S_3) = 4$, *where* S_3 *denotes the symmetric group of six elements;*

(*ii*) $cr(G) = n/2$, *otherwise.*

Remark 1.4. *The proofs of Theorem 1.2 and 1.3 will be heavily based on the ideas contained in* [10] *and* [11] *respectively.*

Remark 1.5. *From Theorem 1.1, Theorem 1.2, Theorem 1.3, and the fact that* $cr(G)$ *has been determined for all finite abelian groups we know that, the critical number* $cr(G)$ *also has been determined for all finite nilpotent groups and all finite groups of even order which possesses a subgroup of index two. However, for finite groups which contains no subgroup with index* p *(*p *is the smallest prime divisor of the order of* G*), we even can't guess the exact value of* $cr(G)$.

2. Notation and Preliminary Lemmas

Lemma 2.1. *(*[12]*) Let* G *be a finite group. Let* A *and* B *be subsets of* G *such that* $|A| + |B| > |G|$*. Then* $A + B = G$, *where* $A + B = \{a + b | a \in A, b \in B\}$.

M. B. Nathanson([12], Lemma 2.1) stated the conclusion of Lemma 2.1 for abelian groups, but the method used there does work for the nonabelian groups. For convenience, we repeat the proof here.

Proof of Lemma 2.1. For $g \in G$, let $g - B = \{g - b : b \in B\}$. Since

$$\begin{aligned} |G| &\geq |A \cup (g - B)| \\ &= |A| + |g - B| - |A \cap (g - B)| \\ &= |A| + |B| - |A \cap (g - B)|, \end{aligned}$$

it follows that

$$|A \cap (g - B)| \geq |A| + |B| - |G| \geq 1,$$

and so there exist a element $a \in A$ and $b \in B$ such that $g = a + b$. This completes the proof of the lemma. □

Lemma 2.2. *([5]) Let p, q be two primes and G be a finite abelian group of order pq. Let S be a subset of G such that $0 \notin S$ and $|S| = p + q - 1$. Then $\sum(S) = G$.*

Let G be a finite group. Let $B \subset G$ and $x \in G$. As usual, we write $\lambda_B(x) = |(B + x) \setminus B|$. For any B, x, Olson proved in [2]

$$\lambda_B(x) = \lambda_B(-x) \tag{2.1}$$

and

$$\lambda_B(x) = \lambda_{G \setminus B}(x). \tag{2.2}$$

We use the following property which is implicit in [2]: Let G be a finite group. Let S be a subset of G such that $0 \notin S$. Put $B = \sum(S)$. For every $y \in S$, we have

$$\begin{aligned} \lambda_B(y) &= |(\textstyle\sum(S) + y) \setminus \sum(S)| \\ &\leq |(\textstyle\sum(S) + y) \setminus (\sum(S \setminus y) + y)| \\ &= |\textstyle\sum(S) \setminus \sum(S \setminus y)| \\ &= |\textstyle\sum(S)| - |\sum(S \setminus y)|. \end{aligned}$$

By above analysis we get the following inequality

$$|\sum(S)| \geq |\sum(S \setminus y)| + \lambda_B(y). \tag{2.3}$$

We also use the following result of Olson.

Lemma 2.3. *([4]) 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 $|B| \leq |G|/2$. Then there is a $x \in S$ such that*

$$\lambda_B(x) \geq min((|B| + 1)/2, (|S \cup -S| + 2)/4).$$

Lemma 2.4. *Let G be a finite group of odd order. Let S be a subset of G such that $S \cap -S = \emptyset$ and $|S| \geq 3$. Then $|\sum(S)| \geq 2|S|$.*

Proof. We proceed by induction on $|S|$. For $|S| = 3$, set $S = \{a, b, c\}$. In order to prove $|\sum(S)| \geq 6$, we distinguish three cases.

Case 1. $a+b = c$. We consider the sequence $(a, b, c, a+c, c+b, a+b+c)$. If $a + c = b$, then $2a = 0$, a contradiction. If $c + b = a$, then $2b = 0$, a contradiction. If $c+b = a+c$, then $b = a$, a contradiction. If $c+b = a+b+c$, then $b = c$, a contradiction. If $b = a+b+c$, then $a+c = 0$, a contradiction. By above analysis we have that $\{a, b, c, a + c, c + b, a + b + c\}$ is a set, then $|\sum(S)| \geq 6$.

Case 2. $a + c = b$. The proof is similar to Case 1.

Case 3. $b + c = a$. The proof is similar to Case 1.

Case 4. $a+b \neq c$, $a+c \neq b$, $b+c \neq a$. Now we have that either $a, b, c, a+b, a+c, b+c$ or $a, b, c, a+b, a+c, a+b+c$ are pairwise distinct. This proves the lemma for $|S| = 3$.

Now assume that the lemma is true for smaller $|S|$. Set $B = \sum(S)$. Applying Lemma 2.3 to B or $G \setminus B$ and using (2.2), there exists a $y \in S$ such that $\lambda_B(y) \geq 2$. By (2.3), $|B| \geq |\sum(S \setminus y)| + 2 \geq 2|S|$. This completes the proof. □

Let X be a subset of G with cardinality k. Let $\{x_i, 1 \leq i \leq k\}$ be an ordering of X. For $0 \leq i \leq k$, set $X_i = \{x_j | 1 \leq j \leq i\}$ and $B_i = \sum(X_i)$. The ordering $\{x_1, \cdots, x_k\}$ will be called a *resolving sequence* of X if for all i, $\lambda_{B_i}(x_i) = max\{\lambda_{B_i}(x_j); 1 \leq j \leq i\}$. The *critical index* of the resolving sequence is the maximal integer t such that X_{t-1} generates a proper subgroup of G.

Clearly, every nonempty subset S not containing 0 admits a resolving sequence. Moreover, the critical index is ≥ 1.

We shall write $\lambda_i = \lambda_{B_i}(x_i)$. By induction we have using (2.3) for all $1 \leq j \leq k$,

$$|\sum(X)| \geq \lambda_k + \cdots + \lambda_j + |B_{j-1}|.$$

Put $\delta(m) = 0$ if m is odd and $= 1$ otherwise. If $\sum(X) < n/2$, by Lemma 2.3, $\lambda_i \geq (i + 1 + \delta(i))/2$ for all $i \geq t$. In particular for all $s \geq t$, we have

$$|\sum(X)| \geq (k+s+3)(k-s+1)/4 - 1/2 + |B_{s-1}|. \tag{2.4}$$

Lemma 2.5. *Let G be a finite group of order 9, and let A, B be two subsets of G.*

(i) If $|A| = 3$ and A is zero-sum free then $|\sum(A)| \geq 6$.
(ii) If $|A| = 3$ and $0 \notin A$ then $|\sum(A)| \geq 5$.
(iii) If $|A| = 4$ and $0 \notin A$ then $|\sum(A)| \geq 7$.
(iv) If $|A| = 4$ then $|\sum_2(A)| \geq 5$.
(v) If $|A| = 4$ and $|B| \geq 2$ then $|A + B| \geq 5$.

Proof. By the basic knowledge of group theory we know that G is abelian.

(i) One can find a proof in [9].

(ii) Let $A = \{a_1, a_2, a_3\}$. Assume to the contrary that

$$|\sum(A)| \leq 4.$$

It follows that $|\{a_1, a_2, a_3\} \cap \{a_1+a_2, a_1+a_3, a_2+a_3\}| \geq 2$. Without loss of generality we may assume that $a_1 = a_2 + a_3$ and $a_2 = a_1 + a_3$. Therefore, $a_1 + a_2 = a_2 + a_3 + a_1 + a_3$. Hence, $2a_3 = 0$. Thus, $a_3 = 0$ for $|G| = 9$, a contradiction with $A \subset G \setminus \{0\}$.

(iii) Let $A = \{a_1, a_2, a_3, a_4\}$. Assume to the contrary that

$$|\sum(A)| \leq 6.$$

If A is zero-sum free then $a_1 + a_2 + a_3 + a_4 \notin \sum(\{a_1, a_2, a_3\})$. By (i) we obtain that $|\sum(A)| \geq |\{a_1 + a_2 + a_3 + a_4\} \cup \sum(\{a_1, a_2, a_3\})| = 1 + |\sum(\{a_1, a_2, a_3\})| \geq 7$, a contradiction. Hence,

$$0 \in \sum(A).$$

Therefore,

$$|\sum(A) \setminus \{0\}| \leq 5.$$

This together with (i) implies that

(*) A contains no zero-sum free sequence of length 3.

By rearranging if necessary we may assume that $a_1 + a_2 + a_3 \neq 0$. By (*) we may assume that $a_1 + a_2 = 0$ (by rearranging if necessary). Since $a_1 \neq a_2$, either $a_1 + a_3 + a_4 \neq 0$ or $a_2 + a_3 + a_4 \neq 0$. Without loss of generality we assume that $a_1 + a_3 + a_4 \neq 0$. It follows from (*) and $a_1 + a_2 = 0$ that $a_3 + a_4 = 0$. Now we have

$$A = \{a_1, -a_1, a_3, -a_3\}.$$

Since $\{0\} \cup A = \{0, a_1, -a_1, a_3, -a_3\} \subset \sum(A)$, by the contrary hypothesis we infer that $\{a_1 + a_3, -(a_1 + a_3)\} \cap A \neq \emptyset$. By the symmetry of A we may assume that $a_1 + a_3 \in A$. Therefore, $a_1 + a_3 = -a_1$ or $a_1 + a_3 = -a_3$. Again by the symmetry of A we may assume that $a_1 + a_3 = -a_1$. Thus, $a_3 = -2a_1$. Now we have $A = \{a_1, -a_1, 2a_1, -2a_1\}$. Since $|G| = 9$ and $a_1 \neq -2a_1$, it is easy to see that $0, a_1, -a_1, 2a_1, -2a_1, 3a_1, -3a_1$ are 7 distinct elements from $\sum(A)$, a contradiction.

(iv) Let $A = \{a_1, a_2, a_3, a_4\}$. Assume to the contrary that $|\sum_2(A)| \leq 4$. It follows that $|\{a_1 + a_2, a_1 + a_3, a_1 + a_4\} \cap \{a_2 + a_3, a_2 + a_4, a_3 + a_4\}| \geq 2$. By rearranging if necessary we assume that $a_1 + a_2 = a_3 + a_4$ and $a_1 + a_3 = a_2 + a_4$. Thus, $a_1 + a_2 + a_1 + a_3 = a_3 + a_4 + a_2 + a_4$. It follows that $a_1 = a_4$, a contradiction.

(v) Let $B = \{b_1, b_2\}$. Assume to the contrary that $|A + B| \leq 4$. It follows that $|A + B| = 4$, and $b_1 + A = b_2 + A = A + B$. Therefore, $\sum_{a \in A}(b_1 + a) = \sum_{a \in A}(b_2 + a)$. Hence, $|A|b_1 + \sum_{a \in A} a = |A|b_2 + \sum_{a \in A} a$. Thus, $4b_1 = 4b_2$ and $b_1 = b_2$, a contradiction. □

Lemma 2.6. *If* $|G| = 27$ *then* $cr(G) = 10$.

Proof. We only need to check the case that G is non-abelian. Since G is a nilpotent group, G possesses a normal subgroup K of index 3. Suppose $G/K = \langle 1 + K \rangle$. Let $x \in 1 + K$ and $T = (K \setminus \{0\}) \cup \{x\}$. It is easy to see that $-1 + K \not\subset \sum(T)$. This shows that $cr(G) \geq 10$. So it suffices to prove that $cr(G) \leq 10$. Let $S \subset G \setminus \{0\}$ and $|S| = 10$. We want to show that $\sum(S) = G$.

From the basic knowledge on p-groups (see [6]) we know that there exist exactly four distinct maximal subgroups of G and each is a normal subgroup of order 9, and G equals to the union of these maximal subgroups. Since $|S| = 10 = 2 \times 4 + 2$, there exists a maximal subgroup H of G such that

$$|S \cap H| \geq 3.$$

Now we fix $a \in G \setminus H$. Then, $G = H \cup (a + H) \cup (2a + H)$. It suffices to prove the following inclusions hold simultaneously:

$$H \subset \sum(S), \quad a + H \subset \sum(S), \quad 2a + H \subset \sum(S).$$

Let $A = (a + H) \cap S$ and $B = (2a + H) \cap S$. Suppose

$$A = \{a + a_1, \cdots, a + a_r\}, \quad B = \{2a + b_1, \cdots, 2a + b_t\},$$

where $r \geq t \geq 0$, $r + t = 10 - |S \cap H|$, and $a_i, b_j \in H$.

Since H is a normal subgroup of G, we also have that

$$a + a_i = a'_i + a, \quad 2a + b_j = b'_j + 2a,$$

where $a'_i, b'_j \in H$.

We distinguish three cases.

Case 1. $|S \cap H| \geq 5$. By Lemma 2.2 we get

$$H = \sum(S \cap H) \subset \sum(S).$$

Since $|S \cap H| \leq |H \setminus \{0\}| = 8$, $|S \cap (G \setminus H)| \geq 2$. Therefore, $(\sum(S \cap (G \setminus H))) \cap (a + H) \neq \emptyset$ and $(\sum(S \cap (G \setminus H))) \cap (2a + H) \neq \emptyset$. It follows from $H = \sum(S \cap H)$ that $a + H \subset \sum(S)$ and $2a + H \subset \sum(S)$.

Case 2. $|S \cap H| = 4$. Now we have

$$r + t = 6.$$

By Lemma 2.5(iii) we obtain that

$$|\sum(S \cap H)| \geq 7.$$

Subcase 2.1. $r = t = 3$. Note that $(2a+b_i)+(a+a_i) = b'_i+2a+a+a_i = b'_i+3a+a_i = h+a_i$, where $h = b'_i+3a \in H$. By Lemma 2.1 $\sum(S\cap H)+\{h+a_1, h+a_2, h+a_3\} = H$. Therefore $H \subset \sum(S\cap H)+(2a+b_1)+A \subset \sum(S)$. Again by Lemma 2.1 we have that $a + H \subset A + \sum(S \cap H) \subset \sum(S)$ and $2a + H \subset B + \sum(S \cap H) \subset \sum(S)$.

Subcase 2.2. $r \geq 4$ and $t \geq 1$. Similar to Subcase 2.1 we know that $H \subset \sum(S)$ and $a + H \subset \sum(S)$. Note that $\sum_2(A) \supset \{a + a_1 + a + a_2, a + a_1 + a + a_3, a + a_1 + a + a_4\}$. Therefore, $\sum_2(A) = 2a + C$ with $C \subset H$ and $|C| \geq 3$. By Lemma 2.1, we have $2a + H = 2a + C + \sum(S \cap H) = \sum_2(A) + \sum(S \cap H) \subset \sum(S)$.

Subcase 2.3. $r = 6$. Similarly to Subcase 2.2 one can prove that $a + H \subset \sum(S)$ and $2a + H \subset \sum(S)$. Since $\{a + a_1 + a + a_2 + a + a_3, a + a_1 + a + a_2 + a + a_4, a + a_1 + a + a_2 + a + a_5\} \subset \sum_3(A)$, we infer that $|\sum_3(A)| \geq 3$. Note that $\sum_3(A) \subset H$. By Lemma 2.1, we have $H = \sum_3(A) + \sum(S \cap H) \subset \sum(S)$.

Case 3. $|S \cap H| = 3$. By Lemma 2.5 we get

$$|\sum(S \cap H)| \geq 5.$$

In this case we have

$$r + t = 7.$$

Subcase 3.1. $r = 4$ and $t = 3$. Note that $A + B = \{a'_1 + a, a'_2 + a, a'_3 + a, a'_4 + a\} + \{2a + b_1, 2a + b_2, 2a + b_3\} = \{a'_1 + 3a, a'_2 + 3a, a'_3 + 3a, a'_4 + 3a\} + \{b_1, b_2, b_3\} \subset H$. Since $3a \in H$, by Lemma 2.5(v), $|A + B| \geq 5$. It follows from Lemma 2.1 that $H = (A+B) + \sum(S \cap H) \subset \sum(S)$. Note that $a + a_i + (2a + b_1) + (a + a_j) = a + a_i + (b'_1 + 2a) + (a + a_j) = a + a_i + (b'_1 + 3a + a_j) = a + b'_1 + 3a + a_i + a_j$. Therefore, $a + b'_1 + 3a + \sum_2\{a_1, a_2, a_3, a_4\} \subset \sum_3(A \cup B)$. By Lemma 2.5($iv$), $|\sum_2\{a_1, a_2, a_3, a_4\}| \geq 5$. It follows from Lemma 2.1 that $a + H = a + b'_1 + 3a + \sum_2(A) + \sum(S \cap H) \subset \sum_3(A \cup B) + \sum(S \cap H) \subset \sum(S)$. Note that $2a + b_i + (a + a_k) + (2a + b_j) = 2a + b_i + (a'_k + a) + (2a + b_j) = 2a + a'_k + 3a + b_j + b_i = 2a + 3a + a'_k + b_j + b_i$. Therefore, $2a + 3a + \{a'_1, a'_2, a'_3, a'_4\} + \sum_2\{b_1, b_2, b_3\} \subset \sum_3(A \cup B)$. By Lemma 2.5, $|\{a'_1, a'_2, a'_3, a'_4\} + \sum_2\{b_1, b_2, b_3\}| \geq 5$. Again by Lemma 2.1 we have $2a + H = 2a + 3a + \{a'_1 + a'_2 + a'_3 + a'_4\} + \sum_2\{b_1, b_2, b_3\} + \sum(S \cap H) \subset \sum(S)$.

Subcase 3.2. $r = 5$ and $t = 2$. Similarly to above one can prove that $H \subset \sum(S)$ and $a + H \subset \sum(S)$. Since $A + (2a + b_1) + (2a + b_2) \subset 2a + H$, by Lemma 2.1 we infer that $2a + H = A + (2a + b_1) + (2a + b_2) + \sum(S \cap H) \subset \sum(S)$.

Subcase 3.3. $r = 6$ and $t = 1$. Similarly to above one can prove that $H \subset \sum(S)$ and $a + H \subset \sum(S)$. Note that $\{a + a_1\} + \{a + a_2, \cdots, a + a_6\} \subset \sum_2(A)$. Therefore, $|\sum_2(A)| \geq 5$. Now by Lemma 2.1 and $\sum_2(A) \subset 2a + H$ we obtain that $2a + H = \sum_2(A) + \sum(S \cap H) \subset \sum(S)$.

Subcase 3.4. $r = 7$ and $t = 0$. Similarly to above one can prove $a + H \subset \sum(S)$ and $2a + H \subset \sum(S)$. Note that $(a + a_1) + (a + a_2) + \{(a + a_3), \cdots, (a + a_7)\} \subset \sum_3(A) \subset H$. Therefore, $|\sum_3(A)| \geq 5$. Again by Lemma 2.1, $H = \sum_3(A) + \sum(S \cap H) \subset \sum(S)$. □

3. The Proofs of The Main Results

Proof of Theorem 1.2.

Set $|G| = n$. Since G is a nilpotent group, G possesses a normal subgroup K of index p. Suppose $G/K = \langle 1 + K \rangle$. Let B be any subset of $p - 2$ elements in $1 + K$ and $T = (K \setminus \{0\}) \cup B$. It is easy to see that $-1 + K \not\subset \sum(T)$. This shows that $cr(G) \geq n/p + p - 2$. So it suffices to prove that $cr(G) \leq n/p + p - 2$.

Let S be any subset of $G \setminus \{0\}$ with cardinality $|S| = n/p + p - 2$. We need to show $\sum(S) = G$. We proceed by induction on the number of prime divisors of n (counted with multiplicity). By the hypothesis we know that $n = 27$ or $n \geq 45$. By Lemma 2.6 we may assume that $n \geq 45$. Set $k(n) = (n/p+p-2)/2$. We shall write sometimes k instead of $k(n)$. Clearly we may partition $S = X \cup Y$ so that $|X| = |Y| = k$, $X \cap -X = Y \cap -Y = \emptyset$ and $|\sum(X)| \leq |\sum(Y)|$.

The result holds by Lemma 2.1 if $|\sum(X)| > n/2$. Suppose the contrary. Since n is odd, we have

$$|\sum(X)| \leq (n-1)/2. \tag{3.1}$$

Let $\{x_i; 1 \leq i \leq k\}$ be a resolving sequence for X with critical index t.

By Lemma 2.4 and note that $n \geq 45$, in a similar way to the proof of Theorem 3.1 in [10] we can prove that

$$t \geq n/p^2 + p. \tag{3.2}$$

Let H be the proper subgroup generate by X_{t-1}. Let p' be the smallest prime divisor of n/p. By (3.2), $|H \cap S| \geq n/(pp') + p' - 1$. If n/p is the product of more than two primes, then by the induction hypothesis, $\sum(S \cap H) = H$. If n/p is the product of two primes, then by Theorem 1.1 and Lemma 2.2, $\sum(S \cap H) = H$.

Since $|H| > n/(pp')$, we see easily that $q = |G/H|$ is a prime. Since G is nilpotent, H is a normal subgroup of G. Clearly $|S \setminus H| \geq q - 1$. Let $a_1, \cdots, a_{q-1}$ be distinct elements from $S \setminus H$. We denote by $\bar{a}_i$ the image of a_i in G/H under the canonical morphism.

By the Cauchy-Davenport Theorem(cf.[12]), $\{0, \bar{a}_1\} + \cdots + \{0, \bar{a}_{q-1}\} = G/H$. It follows that $\sum(a_1, \cdots, a_{q-1}) + H = G$. The theorem now follows since $\sum(S \cap H) = H$. □

Proof of Theorem 1.3.

Since G possesses a subgroup of index 2, in a similar way to the proof of Theorem 1.2 we can show that $cr(G) \geq n/2$. So, it suffices to prove that $cr(G) \leq n/2$. In a similar way to the proof of Lemma 2.6 we can checked the theorem for $n \leq 14$(one can find the structures of nonabelian groups for the case in [6]). Now assume that $n \geq 16$. Let S be a subset of $G \setminus \{0\}$ of size $n/2$. Let $T = S \cup \{0\}$.

Now fix a subgroup H of index 2. Then, for any $g \in G$, $H + 2g = H$, so that $2g \in H$. Also the sets T and $g - T$ cannot be disjoint, because of their sizes, so g has a representation as $t_1 + t_2$ with $t_i \in T$. If $g \notin H$, since $2g \in H$, it means that $t_1 \neq t_2$ in its representation $g = t_1 + t_2$. Tossing away 0, if it is one of t_i's, we have express g as a subset sum in S.

So from now on, we assume $g \in H$, and split the proof into three cases according to $k =: |T \cap H|$.

Case 1. $k \geq (n/2) - 1$. obviously.

Case 2. $3 \leq k \leq (n/2) - 2$. Consider the collection of sums $h + j$ with $h \in T \cap H$ and $j \in T \cap (G \setminus H)$. These $k(|T| - k)$ sums belong to $G \setminus H$, so some element v occurs in this collection with multiplicity at least

$$\lceil \tfrac{k(|T|-k)}{|G \setminus H|} \rceil = \lceil \tfrac{k(n/2+1-k)}{n/2} \rceil \geq \lceil \tfrac{3(n/2-2)}{n/2} \rceil = 3.$$

In other words, we can write $v = h_i + j_i$, for $i = 1, 2, 3$, such that the $h_i(resp., j_i)$ are distinct elements of $T \cap H(resp., T \cap (G \setminus H))$. Since $g - v \notin H$, and since as above T and $(g - v) - T$ are not disjoint, we can write $g - v = h + j$ or $g - v = j' + h'$ with $h, h' \in H$ and $j, j' \in T \cap (G \setminus H)$. Pick i so that $h_i \neq h$ and $j_i \neq j$ or $h_i \neq h'$ and $j_i \neq j'$(which is possible since there are three choice for i). Then we have $g = h + j + h_i + j_i$ or $g = j' + h' + h_i + j_i$, which is a sum of distinct elements of T. Omitting 0 as one of the terms, if present, gives a subset from S.

Case 3. $k \leq 2$. Now T contains $G \setminus H$, with the possible exception of a single element r. Fix $v \in T \setminus H$. The $\frac{n}{2}(n/2 - 1)^2$ sums $x_1 + x_2 + x_3$ with $x_1, x_2 \in G \setminus (H \cup \{r\})$ and $x_3 \in G \setminus H$. In particular, $g - v$ can be represented $(n/2 - 1)^2$ ways as such a sum. Exactly $n/2 - 1$ of these sums have $x_1 = x_2$, $n/2 - 1$ have $x_2 = x_3$, and $n/2 - 1$ have $x_1 = x_3$. Also, $n/2 - 1$ of these sums have $x_1 = v$, $n/2 - 1$ sums have $x_2 = v$, and $n/2 - 1$ sums have $x_3 = v$. Similar $n/2 - 1$ of these sums have $x_3 = r$. There exists a form $g - v = v + v + x_3$. Thus there remain at least

$$(n/2)^2 - 7(n/2 - 1) + 1 = \tfrac{(n-2)(n-16)}{4} + 1 > 0.$$

sums $x_1 + x_2 + x_3$ equaling $g - v$ with distinct $x_i \in G \setminus H$ not equal either v or r. So there exists a subset sum representation $g = x_1 + x_2 + x_3 + v$. This completes the proof of the theorem. □

ACKNOWLEDGEMENTS

The authors would like to express sincere thanks to the referees for their many helpful suggestions and also wish to thank their advisor W.Gao for his constructive comments.

References

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

[2] J.E. Olson, *An addition theorem modulo p*, J. Combin. Theory 5 (1968) 45-52.

[3] G.T. Diderrich and H.B. Mann, *combinatorial problems in finite Abelian groups, In "A survey of Combinatorial Theory" (J.N.Srivastava et al., Erdös.)* pp. 95–100. North-Holland, Amsterdam, 1973.

[4] J.E.Olson, *Sums of sets of group elements*, Acta Arith. 28 (1975) 147-156.
[5] G.T. Diderrich, *An Addition Theorem for Abelian Groups of Order pq*, Journal of Number Theory, 7 (1975), 33–48.
[6] Thomas W. Hungerford, Algebra, 1980.
[7] J.A. Dias da Silva and Y.O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. Lond. Math. Soc. 26 (1994) 140-146.
[8] W.Gao, *A combinatorial problem on finite groups*, Acta Math SINCA. 38 (1995) 395-399.
[9] A. Geroldinger, F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
[10] W. Gao and Y.O. Hamidoune, *On additive bases*, Acta Arith. 88 (1999), 233–237.
[11] J.R. Griggs, *Spanning subset sums for finite abelian groups*, Discrete Math. 229 (2001), 89–99.
[12] M. B. Nathanson, Additive Number Theory, GTM 165, Springer, 1996.
[13] Michael Freeze, Weidong Gao and Alfred Geroldinger, *The critical number of finite abelian groups*, J. Number Theory. 129 (2009), 2766-2777.
[14] Qinghong Wang and Yongke Qu, *On the critical number of finite groups of order pq*, Submitted.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: wqh1208@yahoo.com.cn

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China
E-mail address: quyongke@sohu.com