ACTA ARITHMETICA
Online First version

On additive bases of finite groups

by

YONGKE QU (Luoyang) and WEIDONG GAO (Tianjin)

Abstract. Let G be a multiplicatively written finite group. The critical number $\mathsf{cr}(G)$ of G is the smallest integer t such that for every subset S of $G \setminus \{1\}$ with $|S| \geq t$ the following holds: every element of G can be written as a non-empty product of distinct elements from S. We prove that $\mathsf{cr}(G) \leq |G|/p + p - 2$ for all finite non-abelian groups G with $|G| \neq 6$, where p is the smallest prime divisor of $|G|$. Moreover, equality holds if and only if G has a subgroup of index p.

1. Introduction and main results. Let G be a multiplicatively written finite group (not necessarily commutative). For any two subsets X, Y of G, we define their product set as

$$XY = \{xy : x \in X \text{ and } y \in Y\}.$$

Of course, we use the abbreviations $Xg = \{xg : x \in X\}$ and $gY = \{gy : y \in Y\}$ when dealing with a single element g. For any subset S of G, we define the *inverse set* as

$$S^{-1} = \{g^{-1} : g \in S\}.$$

Let S be a subset of G with $|S| = \ell$, and $S_H = S \cap H$ for any subgroup H of G. Write

$$\pi(S) = \{g_{\tau(1)} \cdot \ldots \cdot g_{\tau(\ell)} : \tau \text{ a permutation of } [1, \ell]\} \subset G$$

to denote the set of products of S. Furthermore, for every integer $n \in [1, \ell]$, define

$$\Pi_n(S) = \bigcup_{T \subset S,\, |T|=n} \pi(T),$$

and set

$$\Pi(S) = \bigcup_{1 \leq n \leq \ell} \Pi_n(S), \qquad \Pi^*(S) = \Pi(S) \cup \{1\}.$$

2020 *Mathematics Subject Classification*: Primary 11B75; Secondary 11P70.
Key words and phrases: critical number, finite group, subset.
Received 23 March 2023; revised 28 March 2024.
Published online *.

DOI: 10.4064/aa230323-10-4

The *critical number* $\mathsf{cr}(G)$ of G is the smallest integer t such that $\Pi(S) = G$ for every subset S of $G \setminus \{1\}$ with $|S| \geq t$.

The problem of determining $\mathsf{cr}(G)$ was first proposed and studied by Erdős and Heilbronn [4] for $G = C_p$, where p is a prime. They proved that $\mathsf{cr}(C_p) \leq 3(6p)^{1/2}$. Since then, there has been a lot of research on the critical number $\mathsf{cr}(G)$ (see [1, 2, 3, 6, 7, 10, 14, 15]). In 2009, Freeze, the second author and Geroldinger [5] settled the last case and determined the precise value of $\mathsf{cr}(G)$ for all finite abelian groups. Meanwhile, there has been a lot of related research on the complete and incomplete sets with large cardinality (see [8, 11, 19]).

However, the research on $\mathsf{cr}(G)$ has never been restricted to the abelian setting alone. In 1973, Diderrich and Mann [3] proved that $|G|/2 \leq \mathsf{cr}(G) \leq |G|/2 + 1$ for every finite group which has a subgroup of index 2. Let p be the smallest prime divisor of $|G|$. In 1995, the second author [6] proved that $\mathsf{cr}(G) = |G|/p + p - 2$ for the following groups G with $p \geq 149$ and $|G| \geq 120p^2$: (i) finite nilpotent groups; (ii) finite groups which have a subgroup with index p and any other prime divisor of $|G|$ (if exists) is $> 6p$. In 2012, Wang and Zhuang [21] proved that $\mathsf{cr}(G) = |G|/p+p-2$ for finite non-abelian groups of order $|G| = pq \geq 10$, where p, q are distinct primes. In 2014, Wang and the first author [20] proved that $\mathsf{cr}(G) = |G|/p + p - 2$ for all finite nilpotent groups of odd order with at least three prime divisors and for all finite groups with $|G| > 6$ which have a subgroup of index 2. In this paper, we extend the proof given by the second author and Hamidoune [7] to prove a tight upper bound for the critical number of non-abelian groups. The main result is as follows.

Theorem 1.1. *Let G be a finite non-abelian group with $|G| \neq 6$ and let p be the smallest prime divisor of $|G|$. Then*

$$\mathsf{cr}(G) \leq |G|/p + p - 2.$$

Moreover, equality holds if and only if G has a subgroup of index p.

2. Preliminaries

Lemma 2.1 ([12, Theorem 1.1]). *Let G be a finite group. Let X and Y be subsets of G such that $XY \neq G$. Then $|X| + |Y| \leq |G|$.*

Lemma 2.2 ([16, Lemma 4]). *Suppose A and B are finite subsets of an arbitrary group and $1 \in A \cap B$. If $ab = 1$ (for $a \in A$, $b \in B$) has no solution except $a = b = 1$, then $|AB| \geq |A| + |B| - 1$.*

Let G be a finite group, $B \subset G$ and $x \in G$. As usual, we write $\lambda_B(x) = |Bx \setminus B|$. We need the following result, which is an improvement of a result of Olson [15, Lemma 3.1].

LEMMA 2.3 ([20, Lemma 2.3]). *Let G be a finite group and let T be a generating subset of G such that $1 \notin T$. Let B be a subset of G such that $|B| \leq |G|/2$. Then there is an $x \in T$ such that*

$$\lambda_B(x) \geq \min\{(|B|+1)/2, (|T \cup T^{-1}|+2)/4\}.$$

With the following property (see [20]) which was implicit in [14] already, Lemma 2.3 can be applied to estimate the cardinality of $\Pi(S)$ effectively.

Let S be a subset of a finite group G such that $1 \notin S$. Then for every $y \in S$, we have $\lambda_B(y) = |\Pi^*(S)y \setminus \Pi^*(S)| \leq |\Pi^*(S)y \setminus \Pi^*(S \setminus \{y\})y| = |\Pi^*(S) \setminus \Pi^*(S \setminus \{y\})| = |\Pi^*(S)| - |\Pi^*(S \setminus \{y\})|$, where $B = \Pi^*(S)$. Therefore,

$$|\Pi^*(S)| \geq |\Pi^*(S \setminus \{y\})| + \lambda_B(y). \tag{2.1}$$

Let X be a subset of G with cardinality k. Let $(x_i)_{i=1}^k$ be an ordering of X. For $0 \leq i \leq k$, set $X_i = \{x_j : 1 \leq j \leq i\}$ and $B_i = \Pi^*(X_i)$. The ordering $(x_i)_{i=1}^k$ will be called a *resolving sequence* of X if for all i, $\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) : 1 \leq j \leq i\}$. We claim that every non-empty subset X with $|X| = k$ admits a resolving sequence. Let $g \in X$ be such that $\lambda_B(g) = \max\{\lambda_B(x) : x \in X\}$, where $B = \Pi^*(X)$. Then we have an ordering of X with $x_k = g$. Similarly, we can find an x_i such that $\lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x) : x \in X_i\}$, where $X_i = X \setminus \{x_{i+1}, \ldots, x_k\}$ for $i = k-1, k-2, \ldots, 1$. Finally, $(x_i)_{i=1}^k$ is a resolving sequence of X.

The *critical index* of a resolving sequence is the maximal integer t such that X_{t-1} generates a proper subgroup of G. Clearly, the critical index of every resolving sequence of any non-empty subset X is ≥ 1.

Let $(x_i)_{i=1}^k$ be a resolving sequence of X. Define X_i, B_i and $\lambda_{B_i}(x_i)$ as above. We shall write $\lambda_i = \lambda_{B_i}(x_i)$. By induction we have, using (2.1), for all $1 \leq j \leq k$,

$$|\Pi^*(X)| \geq \lambda_k + \cdots + \lambda_j + |B_{j-1}|. \tag{2.2}$$

If $1 \notin X$ and $|B_j| \leq |G|/2$, then we can apply Lemma 2.3 to estimate λ_j for $j \geq t$, where t is the critical index of $(x_i)_{i=1}^k$, and thus a lower bound of $|\Pi^*(X)|$ and $|\Pi(X)|$.

3. Proof of the main result. We begin by collecting some known results on the critical number and on finite groups, which will be used later.

LEMMA 3.1. *Let G be a finite group with $|G| \geq 3$ and let p be the smallest prime divisor of $|G|$.*

(i) *If G is of even order and has a subgroup of index 2, then $\mathsf{cr}(G) = |G|/2+1$ for $G \cong C_4$, $C_2 \otimes C_2$, C_6, S_3, C_8 or $C_2 \otimes C_4$, and $\mathsf{cr}(G) = |G|/2$ otherwise.*

(ii) *If G is a nilpotent group and $|G|/p$ is a composite number with $p \geq 3$, then* $\mathsf{cr}(G) = |G|/p + p - 2$.
(iii) *If G is of order pq for primes p and q, then* $\mathsf{cr}(G) \leq p+q-1$. *Moreover, if G is non-abelian and $|G| = pq \neq 6$, then* $\mathsf{cr}(G) = q + p - 2$.

Proof. (i) See [20, Theorem 1.3] and [5, Theorem 1.2(2,3)].

(ii) See [20, Theorem 1.2].

(iii) See [21, Theorem 1.2] and [5, Theorem 1.2(2, 3)]. ■

LEMMA 3.2. *Let G be a finite group and let H be a subgroup of G.*

(i) *Suppose $|G| = p^r$ for some prime p. Then G is nilpotent and has a subgroup of index p.*
(ii) *If $|G| = 2n$ with n odd, then G has a subgroup of index* 2.
(iii) *If the index $|G : H|$ is the smallest prime divisor of $|G|$, then H is a normal subgroup of G.*
(iv) *If* $\gcd(|G|, \varphi(|G|)) = 1$, *where φ is the Euler function, then G is cyclic.*
(v) *Suppose $|G| = p^2q$, where p, q are distinct primes. If* $p \not\equiv \pm 1 \pmod q$ *and* $q \not\equiv 1 \pmod p$, *then G is abelian.*
(vi) *If H is normal and G/H has a subgroup of index 2, then G has a subgroup of index* 2.
(vii) *Suppose $|G| = 4p$ with p a prime. If G has no subgroup of index 2, then $p = 3$ and $G \cong A_4$, the alternating group of degree* 4.

Proof. (i) See [18, p. 88, Corollary 1.6].

(ii) See [18, p. 309, Exercise 10(i)].

(iii) See [18, p. 34, Exercise 3(b)].

(iv) See [22, p. 125, Theorem 6.8] or [18, p. 113, Exercise 8].

(v) By the Sylow Theorem (see [22, p. 55, The Third Sylow Theorem] and [18, p. 95, Theorem 2.2]), we see that both the Sylow p-subgroup S_p and the Sylow q-subgroup S_q of G are normal. Since both S_p and S_q are abelian, G is abelian.

(vi) This result follows from the Generalized Correspondence Theorem (see [18, p. 40, Theorem 5.5]).

(vii) By (i), $p \neq 2$. If $p \geq 5$, then by the Sylow Theorem we deduce that the Sylow p-subgroup S_p is normal. Since $|G/S_p| = 4$, G/S_p has a subgroup of index 2. By (vi), G has a subgroup of index 2, a contradiction. Therefore, $p = 3$ and thus $|G| = 12$. By the classification of groups of order 12, we have $G \cong A_4$. ■

LEMMA 3.3. *Let G be a finite group and let H be a normal subgroup of G of prime index q. If S is a subset of G such that $\mathit{\Pi}(S_H) = H$ and $|S \setminus H| \geq q - 1$, then $\mathit{\Pi}(S) = G$.*

Proof. Let $a_1, \dots, a_{q-1}$ be distinct elements from $S \setminus H$. We denote by $\bar{a}_i$ the image of a_i in G/H under the canonical homomorphism. By the Cauchy–Davenport Theorem (see [12, Corollary 1.2.3], [13, Theorem 2.2]),

$$\{1, \bar{a}_1\} \cdot \ldots \cdot \{1, \bar{a}_{q-1}\} = G/H.$$

It follows that $\Pi(\{a_1, \dots, a_{q-1}\})H = G$. Since $\Pi(S_H) = H$, we have $\Pi(S) \supset \Pi(\{a_1, \dots, a_{q-1}\})\Pi(S_H) = G$. ∎

Lemma 3.4. *Let G be a non-abelian group of order $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$, where $5 \le p_1 < p_2 < \cdots < p_r$ and $\alpha_i \ge 1$ for $i \in [1, r]$. If $r \ge 2$ and $\alpha_1 + \alpha_2 + \cdots + \alpha_r \ge 3$, then $n(p_2^2 - p_1^2) \ge 6p_1^2 p_2^2$.*

Proof. If $\alpha_1 + \alpha_2 + \cdots + \alpha_r \ge 4$, then $n \ge p_1^3 p_2$. Note that $p_2 - p_1 \ge 2$. We have $n(p_2^2 - p_1^2) \ge 2p_1^3 p_2(p_2 + p_1) > (2p_1)p_1^2 p_2^2 > 6p_1^2 p_2^2$. Next, assume

$$\alpha_1 + \alpha_2 + \cdots + \alpha_r = 3.$$

If $p_2 - p_1 \ge 4$, then $p_2 \ge p_1 + 4 \ge 9$. Now we have $n(p_2^2 - p_1^2) \ge n(p_2^2 - (p_2 - 4)^2) = n(8p_2 - 16) > 6np_2 \ge 6p_1^2 p_2^2$ and we are done. So, we may assume that

$$p_2 = p_1 + 2.$$

Case 1: $n = p_1 p_2 p_3$. If $p_3 \ge \frac{7}{4} p_1$, then

$$n(p_2^2 - p_1^2) = p_3 p_2 p_1 (p_2^2 - (p_2 - 2)^2) = 4p_1^2 p_2^2 \frac{p_3}{p_1} \frac{p_2 - 1}{p_2} \ge 4p_1^2 p_2^2 \frac{7}{4} \frac{6}{7} = 6p_1^2 p_2^2$$

and we are done. So, we may assume that

$$p_3 < \frac{7}{4} p_1.$$

Then $\gcd(n, \varphi(n)) = 1$. By Lemma 3.2(iv), G is cyclic, a contradiction.

Case 2: $n = p_1^2 p_2$ *or* $n = p_1 p_2^2$. Since $p_2 = p_1 + 2$ and $p_1 \ge 5$, we see that $p_1 \not\equiv \pm 1 \pmod{p_2}$ and $p_2 \not\equiv \pm 1 \pmod{p_1}$. By Lemma 3.2(v), G is abelian, a contradiction. ∎

By [20, Lemma 2.4], we have the following.

Lemma 3.5. *Let G be a finite group of odd order. Let S be a subset of G such that $S \cap S^{-1} = \emptyset$. Then $|\Pi^*(S)| \ge 2|S|$.*

We now show the upper bound of the critical number for groups of odd order which has at least three prime divisors.

Lemma 3.6. *Let G be a finite group and $p \ge 3$ be the smallest prime divisor of $|G|$. If $|G|/p$ is a composite number, then $\mathsf{cr}(G) \le |G|/p + p - 2$. Moreover, equality holds if and only if G has a subgroup of index p.*

Proof. Set $|G| = n$. By Lemma 3.1(ii), we may assume that G is not nilpotent. So, by Lemma 3.2(i), n is not a power of one prime and thus $n \ge p^2 q$, where q is the second smallest prime divisor of n. If $|G| = 45$, then by Lemma 3.2(v), G is abelian, yielding a contradiction. Therefore, we may assume that $n \geq 63$. Let X be a subset of $G \setminus \{1\}$ with $k = |X|$ and $X \cap X^{-1} = \emptyset$. We claim the following:

Claim. *If $k = (n/p + p - 4)/2$ and $|\Pi^*(X)| \leq (n-1)/2$, then G has a subgroup H of index p. Moreover,*

$$|X_H| \geq n/(pp') + p' - 1,$$

where p' is the smallest prime divisor of $|H|$.

Proof of Claim. Note that G is of odd order and $X \cap X^{-1} = \emptyset$. If $\langle X \rangle \neq G$, then $|\langle X \rangle| \geq 2|X| + 1 \geq n/p$. Thus, $\langle X \rangle$ is a subgroup of index p. Let $H = \langle X \rangle$. Since $n \geq 63$, we have $|X_H| = |X| = k = (n/p + p - 4)/2 \geq n/(3p) + 3 - 1 \geq n/(pp') + p' - 1$.

Next we assume that $\langle X \rangle = G$. Let $(x_i)_{i=1}^k$ be a resolving sequence for X with critical index t. As before (2.2), denote $X_i = \{x_j : 1 \leq j \leq i\}$, $B_i = \Pi^*(X_i)$ and $\lambda_i = \lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) : 1 \leq j \leq i\}$. Since $X \cap X^{-1} = \emptyset$, by Lemma 2.3 we have

$$\lambda_i \geq (i + 1 + \delta(i))/2$$

for all $i \geq t$, where $\delta(m) = 0$ if m is odd and $\delta(m) = 1$ otherwise.

Since $|\Pi^*(X)| \leq (n-1)/2$, by (2.2) we have

$$(n-1)/2 \geq |\Pi^*(X)| \geq (k + s + 3)(k - s + 1)/4 - 1/2 + |B_{s-1}| \tag{3.1}$$

for all $s \geq t$. By Lemma 3.5 we deduce that $|B_{t-1}| \geq 2(t-1)$. Obviously $|B_t| = |B_{t-1}| + |B_{t-1}x_t| = 2|B_{t-1}| \geq 4(t-1)$. By (3.1), applied with $s = t+1$, we have

$$4t - 4 + (k + t + 4)(k - t)/4 - n/2 \leq 0. \tag{3.2}$$

Set $F(t, n) = 4t - 4 + (k + t + 4)(k - t)/4 - n/2 = n^2/(16p^2) - 3n/8 + p^2/16 - t^2/4 + 3t - 5$. Let us show that $t \geq 6$. Since G is non-abelian, we have $t \geq 2$. Since $\frac{\partial F(t,n)}{\partial t} = 3 - t/2 > 0$ when $2 \leq t \leq 5$, we have $F(t, n) \geq F(2, n)$. Similarly, since $F(2, n)$ is an increasing function of n on the interval $[p^2 q, \infty)$, we obtain $F(2, n) \geq F(2, 63) = 63^2/144 - 189/8 + 9/16 > 0$. Thus $F(t, n) \geq F(2, n) > 0$, a contradiction to (3.2). Therefore, $t \geq 6$.

Let

$$m = \max\{n/p^2 + p, (n/q - 1)/2 + 2\}.$$

We next show that $t \geq m$. Assume to the contrary that $t \leq m - 1$. Then $F(t, n) > 0$, yielding a contradiction to (3.2). Set $G(n) = F(m - 1, n)$.

Case 1: $m = n/p^2 + p$. Since $n/p^2 + p - 1 \geq 6$ (we recall that $n \geq 63$), we have $F(t, n) \geq F(m - 1, n) = G(n)$ for $6 \leq t \leq m - 1$. Thus, by (3.2),

$$G(n) \leq F(t, n) \leq 0.$$

Note that $G(n) = 7n/(2p^2) + 7p/2 + n^2/(16p^2) - 3n/8 - n/2p - 3p^2/16 - n^2/(4p^4) - 33/4$. Observe that $G'(n) = 7/(2p^2) + n/(8p^2) - 1/(2p) - n/(2p^4) - 3/8 \geq 0$. In particular, $G(n)$ is an increasing function. Since $n \geq p^2 q \geq p^2(p+2)$, we have $\frac{1}{16}(p^4 - 2p^3 - 23p^2 + 80p - 36) = G(p^2(p+2)) \leq G(n) \leq 0$. On the other hand, it is easy to prove that $p^4 - 2p^3 - 23p^2 + 80p - 36 > 0$ for all $p \geq 3$, a contradiction.

CASE 2: $m = (n/q - 1)/2 + 2$. Then $(n/q-1)/2+2 \geq n/p^2 + p$ and thus $p \geq 5$. Since $n \geq p^2 q$ and $p \geq 5$, we have $(n/q - 1)/2 + 1 \geq 6$. As in Case 1, by (3.2),

$$G(n) \leq 0.$$

Note that $G(n) = n^2(q^2 - p^2)/(16p^2q^2) + p^2/16 + 11n/(8q) - 3n/8 - 57/16$. By Lemma 3.4, $G(n) \geq p^2/16 + 11n/(8q) - 57/16 > 0$, a contradiction. This proves that

$$t \geq m = \max\{n/p^2 + p, (n/q - 1)/2 + 2\}.$$

Let H be the proper subgroup generated by X_{t-1}. Noting that $X \cap X^{-1} = \emptyset$, we have $(|H| - 1)/2 \geq t - 1$. Thus $|H| \geq 2t - 1 > \max\{n/p^2, n/q\}$. Therefore, H is a subgroup of index p. Moreover, $|X_H| \geq t - 1 \geq n/(pp') + p' - 1$. This completes the proof of the Claim. ∎

Now, we prove that $\mathsf{cr}(G) \leq n/p + p - 2$. Let S be a subset of $G \setminus \{1\}$ with $|S| = n/p + p - 2$. Let $X \subset S$ and $Y = S \setminus X$ be such that $|X| = |Y|$, $X \cap X^{-1} = Y \cap Y^{-1} = \emptyset$ and $|\Pi(X)| \leq |\Pi(Y)|$. If $|\Pi(X)| > n/2$, then the result follows from Lemma 2.1.

Assume that $|\Pi(X)| \leq n/2$. Since n is odd, we have $|\Pi(X)| \leq (n-1)/2$. Let X' be a subset of X with $|X'| = (n/p + p - 4)/2$. If $|\Pi(X')| < |\Pi(X)|$, then $|\Pi^*(X')| \leq |\Pi(X)| \leq (n-1)/2$. If $|\Pi(X')| = |\Pi(X)|$, then $\Pi(X') = \Pi(X)$. Suppose $\{g\} = X \setminus X'$ and $K = \langle g \rangle$. Then $\Pi(X')g \subset \Pi(X)$ and $|\Pi(X')g| = |\Pi(X')| = |\Pi(X)|$. Thus $\Pi(X')g = \Pi(X) = \Pi(X')$. Moreover, $\Pi(X')K = \Pi(X')$. Since $g \in K$ and $g \in \Pi(X)$, we have $1 \in K \subset \Pi(X)K = \Pi(X')K = \Pi(X')$ and thus $|\Pi^*(X')| = |\Pi(X')| = |\Pi(X)| \leq (n-1)/2$. In both cases, we have $|\Pi^*(X')| \leq (n-1)/2$. Note that $X' \cap X'^{-1} = \emptyset$. By the Claim, there exists a subgroup H of G of index p such that $|S_H| \geq |X'_H| \geq n/(pp') + p' - 1$, where p' is the smallest prime divisor of n/p.

Since p is the smallest prime divisor of $|G|$, by Lemma 3.2(iii) we find that H is a normal subgroup of order n/p of G. Note that n/p is a composite number. If n/p is the product of two primes, then by Lemma 3.1(iii), $\mathsf{cr}(H) \leq |H|/p' + p' - 1$. If n/p is the product of more than two primes, then $|H|/p' = n/pp'$ is a composite number. By the induction hypothesis, we have $\mathsf{cr}(H) \leq |H|/p' + p - 2$. In both cases, we conclude that $\mathsf{cr}(H) \leq |H|/p' + p' - 1 = n/(pp') + p' - 1 \leq |S_H|$. Thus $\Pi(S_H) = H$. Clearly, $|S \setminus S_H| \geq p - 1$. By Lemma 3.3, $\Pi(S) = G$. Therefore, $\mathsf{cr}(G) \leq n/p + p - 2$.

Next, assume that G does not have any subgroup of index p. We show that $\mathsf{cr}(G) \le n/p+p-3$. Let S be a subset of $G\setminus\{1\}$ with $|S| = n/p+p-3$. Let $X \subset S$ and $Y = S \setminus X$ be such that $|X| = (n/p+p-4)/2 = |Y|-1$, $X \cap X^{-1} = Y \cap Y^{-1} = \emptyset$ and $|\Pi^*(X)| \le |\Pi(Y)|$ (as $|\Pi(Y)| \ge |\Pi^*(Y\setminus\{y\})|$ for each $y \in Y$). If $|\Pi^*(X)| \le (n-1)/2$, then by the Claim, there exists a subgroup of index p, a contradiction. Thus, $|\Pi^*(X)| \ge (n+1)/2$ and $|\Pi(Y)| \ge (n+1)/2$. By Lemma 2.1, $\Pi(S) \supset \Pi^*(X)\Pi(Y) = G$. Therefore, $\mathsf{cr}(G) \le n/p+p-3$.

Finally, we show that if G has a subgroup H of index p, then $\mathsf{cr}(G) = n/p+p-2$. Since $\mathsf{cr}(G) \le n/p+p-2$, it suffices to construct a subset S of $G\setminus\{1\}$ with $|S| = n/p+p-3$ such that $\Pi(S) \ne G$. Let $S = (H\setminus\{1\}) \cup S'$, where S' is a subset of aH for some $a \notin H$ with $|S'| = p-2$. By Lemma 3.2(iii), H is a normal subgroup of G. Then $\Pi(S) \cap (a^{p-1}H) = \emptyset$. Thus $\Pi(S) \ne G$.

Next, we consider the groups of even order, and begin with the critical number $\mathsf{cr}(G)$ of non-abelian groups G of order 12.

Lemma 3.7. *Let G be a finite non-abelian group of order* 12*. Then* $\mathsf{cr}(G) \le |G|/2 = 6$*. Moreover, equality holds if and only if G has a subgroup of index* 2*.*

Proof. By Lemma 3.1(i), if G has a subgroup of index 2, then $\mathsf{cr}(G) = 6$. Now, assume that G does not have any subgroup of index 2. It suffices to prove that $\mathsf{cr}(G) \le 5$. By Lemma 3.2(vii), we have $G \cong A_4$, the alternating group of degree 4. Let H be the normal subgroup of order 4. Then $H \cong C_2 \otimes C_2$ and $gH = Hg$ for any $g \in G$. Let $H_a = aH$ and $A \subset H_a$ for some $a \in G\setminus H$. We have the following observations:

(i) If $|A| = 2$, then $|\Pi_2(A)| = 2$ and $|A \cup hA \cup Ah| \ge 3$ for $h \in H\setminus\{1\}$.
(ii) If $|A| = 3$, then $\Pi_3(A) = H$.
(iii) If $|A| = 3$, then $\Pi_2(A) = a^2H$.

Since G has no subgroup of index 2, we infer that every proper subgroup of G has order in $\{2,3,4\}$ and every non-zero element in G has order in $\{2,3,4\}$. It follows that every element in $G\setminus H$ has order 3. Therefore, for any $g \in G\setminus H$ and any $h \in H\setminus\{1\}$ we have $\langle g,h\rangle = G$ and

$$gh \ne hg. \tag{3.3}$$

Let

$$H = \{1, h_1, h_2, h_3\}.$$

From (3.3) we have $ah_ia^{-1} \ne h_i$ for each $i = 1,2,3$ and $a \in G\setminus H$. This implies that, by renumbering if necessary,

$$ah_1a^{-1} = h_2, \quad ah_2a^{-1} = h_3 \quad \text{and} \quad ah_3a^{-1} = h_1. \tag{3.4}$$

To prove observation (i), let $A = \{ax, ay\}$ with distinct $x, y \in H = C_2 \otimes C_2$. We need to prove $(ax)(ay) \neq (ay)(ax)$. Assume to the contrary that $(ax)(ay) = (ay)(ax)$; then $xay = yax$ and $y^{-1}xa = axy^{-1}$ follows. Note that $x = x^{-1}$ and $y = y^{-1}$; we obtain $(yx)a = a(xy)$, but $yx = xy \neq 1$, which contradicts (3.3). This proves $|\Pi_2(A)| = 2$. If $|A \cup hA \cup Ah| \leq 2$ for some $h \in H \setminus \{1\}$, then $A = hA = Ah$. Thus $h(ax) = ay = (ax)h$, contrary to (3.3). This proves observation (i).

To prove observation (ii), let $A = \{ax, ay, az\}$ with distinct $x, y, z \in H$. We have the following four possibilities: $\{x, y, z\} = \{h_1, h_2, h_3\}$, $\{x, y, z\} = \{h_1, h_2, 1\}$, $\{x, y, z\} = \{h_1, 1, h_3\}$ and $\{x, y, z\} = \{1, h_2, h_3\}$. If $\{x, y, z\} = \{h_1, h_2, h_3\}$, then from (3.4) we obtain $(ah_3)(ah_1)(ah_2) = h_1a^2h_1ah_2 = h_1a^3(a^{-1}h_1a)h_2 = h_1h_3h_2 = 1$. This proves that $1 \in \Pi_3(A)$. Again from (3.4) we obtain $(ah_2)(ah_1)(ah_3) = h_3a^2h_1ah_3 = h_3h_3h_3 = h_3$. Similarly, $(ah_3)(ah_2)(ah_1) = h_1$ and $(ah_1)(ah_3)(ah_2) = h_2$. Therefore, $\Pi_3(A) = H$. If $\{x, y, z\} = \{1, h_2, h_3\}$, then similar to the above, from (3.4) we obtain $(ah_3)a(ah_1) = 1, (ah_1)a(ah_3) = h_2h_3 = h_1, (ah_3)a(ah_2) = h_1h_2 = h_3$ and $(ah_2)a(ah_1) = h_3h_1 = h_2$. Therefore, $\Pi_3(A) = H$. If $\{x, y, z\} = \{h_1, h_2, 1\}$ or $\{x, y, z\} = \{h_1, 1, h_3\}$, then in a similar way to the above we can prove that $\Pi_3(A) = H$. This proves observation (ii).

To prove observation (iii), let $A = \{ax, ay, az\}$ with distinct $x, y, z \in H$. Again we have the four possibilities as above. If $\{x, y, z\} = \{h_1, h_2, h_3\}$, then from (3.4) we obtain $(ah_1)(ah_2) = a^2(a^{-1}h_1a)h_2 = a^2h_3h_2 = a^2h_1$, $(ah_1)(ah_3) = a^2h_3h_3 = a^2$, $(ah_2)(ah_3) = a^2h_2$ and $(ah_3)(ah_1) = a^2h_3$. Hence, $\Pi_2(A) = a^2H$. If $\{x, y, z\} = \{1, h_2, h_3\}$, then similar to the above, from (3.4) we obtain $(ah_3)(ah_2) = a^2$, $a(ah_2) = a^2h_2$, $a(ah_3) = a^2h_3$, $(ah_2)a = a^2h_1$. Therefore, $\Pi_2(A) = a^2H$. If $\{x, y, z\} = \{h_1, h_2, 1\}$ or $\{x, y, z\} = \{h_1, 1, h_3\}$, then in a similar way to the above we can prove that $\Pi_2(A) = a^2H$. This proves observation (iii).

Let S be a subset of $G \setminus \{1\}$ with $|S| = |G|/2 - 1 = 5$. It suffices to prove that $\Pi(S) = G$. Recall that $S_H = S \cap H$. Denote $S_a = S \cap H_a$ and $S_{a^2} = S \cap H_{a^2}$. We have

$$|S_H| + |S_a| + |S_{a^2}| = |S| = 5. \tag{3.5}$$

Without loss of generality, we assume that

$$|S_a| \geq |S_{a^2}|. \tag{3.6}$$

Case 1: $|S_a| = 3$ or 4. By observations (ii) and (iii), we have $\Pi(S) \supset \Pi_3(S_a) \supset H$ and $\Pi(S) \supset \Pi_2(S_a) \supset a^2H$. If $|S_{a^2}| \geq 1$, then $\Pi(S) \supset \Pi_2(S_a)S_{a^2} \supset aH$. Now suppose that $|S_{a^2}| = 0$. If $|S_a| = 3$, then by (3.5) we have $|S_H| = 2$. Thus $\Pi(S) \supset \Pi^*(S_H)S_a \supset aH$. If $|S_a| = 4$, then $S_a = aH$. Therefore,

$$\Pi(S) \supset H \cup a^2H \cup aH = G,$$

and $\Pi(S) = G$ follows.

Case 2: $|S_a| = 2$. By (3.5) and (3.6) we derive that $1 \leq |S_H| \leq 3$.

If $|S_H|=3$, then $\Pi(S_H)=H$ and $|S \setminus S_H|=2$. By Lemma 3.3, $\Pi(S)=G$.

If $|S_H| = 2$, then $|S_{a^2}| = 1$. Clearly, $\Pi^*(S_H) = H$. Then $\Pi(S) \supset \Pi^*(S_H)S_a \supset aH$, $\Pi(S) \supset \Pi^*(S_H)S_aS_{a^2} \supset H$ and $\Pi(S) \supset \Pi^*(S_H)S_{a^2} \supset a^2H$. Therefore, $\Pi(S) \supset aH \cup H \cup a^2H = G$, and $\Pi(S) = G$ follows.

If $|S_H| = 1$, then $|S_{a^2}| = 2$. Let $S_H = \{h\}$. By observation (i), we have $|\Pi_2(S_a) \cup h\Pi_2(S_a) \cup \Pi_2(S_a)h| \geq 3$ and $|\Pi_2(S_{a^2}) \cup h\Pi_2(S_{a^2}) \cup \Pi_2(S_{a^2})h| \geq 3$. By Lemma 2.1, $\Pi(S) \supset (\Pi_2(S_a) \cup h\Pi_2(S_a) \cup \Pi_2(S_a)h)S_{a^2} \supset aH$, $\Pi(S) \supset (\Pi_2(S_{a^2}) \cup h\Pi_2(S_{a^2}) \cup \Pi_2(S_{a^2})h)S_a \supset a^2H$ and $\Pi(S) \supset (\Pi_2(S_a) \cup h\Pi_2(S_a) \cup \Pi_2(S_a)h)\Pi_2(S_{a^2}) \supset H$. Therefore, $\Pi(S) \supset aH \cup a^2H \cup H = G$, and $\Pi(S) = G$ follows.

Case 3: $|S_a| = 1$. Since $|S_H| \leq 3$, by (3.5) and (3.6) we derive that $|S_H| = 3$ and $|S_{a^2}| = 1$. Clearly, $\Pi(S_H) = H$. Since $|S \setminus S_H| = 2$, by Lemma 3.3 we find that $\Pi(S) = G$. ■

By [9, Proposition 5.3.2], we have the following lemma.

Lemma 3.8. *Let S be a subset of a finite abelian group G with $1 \notin \Pi(S)$. If $|S| \geq 2$, then $|\Pi^*(S)| \geq |S| + 2$. If $|S| \geq 4$, then $|\Pi^*(S)| \geq 2|S| + 1$.*

Lemma 3.9. *Let S be a subset of a finite non-abelian group G. If $1 \notin \Pi(S)$, $G = \langle S \rangle$ and $|S| \leq |G|/2 - 2$, then $|\Pi^*(S)| \geq 2|S| + 1$.*

Proof. We proceed by induction on $k = |S|$. Note that $G = \langle S \rangle$ is non-abelian. If $k = 2$, then $|\Pi^*(S)| = 5 = 2|S| + 1$. Assume that the result is true for $k \geq 2$. We next prove the result is also true for $k + 1$.

If $\langle S \setminus \{g\} \rangle$ is abelian for some $g \in S$, then by Lemma 3.8, $|\Pi^*(S \setminus \{g\})| \geq |S \setminus \{g\}| + 2 = k + 2$. Since G is non-abelian, we deduce that $|\Pi^*(S)| \geq 2|\Pi^*(S \setminus \{g\})| \geq 2(k + 2) \geq 2|S| + 1$.

Now assume that $\langle S \setminus \{g\} \rangle$ is non-abelian for every $g \in S$. If $\langle S \setminus \{g\} \rangle \neq G$ for some $g \in S$, then $|\Pi^*(S)| \geq 2|\Pi^*(S \setminus \{g\})|$. Since $\langle S \setminus \{g\} \rangle$ is non-abelian, there exist $g_1, g_2 \in S \setminus \{g\}$ such that $g_1g_2 \neq g_2g_1$. Since $1 \notin \Pi(S)$, we conclude that $ab = 1$ has no solution except $a = 1$ and $b = 1$, where $a \in \Pi^*(S \setminus \{g, g_1, g_2\})$ and $b \in \Pi^*(\{g_1, g_2\}) = \{1, g_1, g_2, g_1g_2, g_2g_1\}$. By Lemma 2.2,

$$\begin{aligned}
|\Pi^*(S \setminus \{g\})| &\geq |\Pi^*(S \setminus \{g, g_1, g_2\})\Pi^*(\{g_1, g_2\})| \\
&\geq |\Pi^*(S \setminus \{g, g_1, g_2\})| + |\Pi^*(\{g_1, g_2\})| - 1 \\
&\geq |S \setminus \{g, g_1, g_2\}| + 1 + |\Pi^*(\{g_1, g_2\})| - 1 \\
&= k - 1 + 5 - 1 = k + 3.
\end{aligned}$$

Therefore, $|\Pi^*(S)| \geq 2|\Pi^*(S \setminus \{g\})| \geq 2(k + 3) \geq 2(k + 1) + 1 = 2|S| + 1$.

Suppose $\langle S \setminus \{g\} \rangle = G$ for every $g \in S$. Clearly, $|S \setminus \{g\}| \leq |G|/2 - 2$. By the induction hypothesis, we have $|\Pi^*(S \setminus \{g\})| \geq 2|S \setminus \{g\}| + 1 = 2k + 1$.

Let $B = \Pi^*(S)$. Then $|B| \geq k+2$. If $|B| \geq |G|-2$, then clearly $|B| > 2|S|+1$. If $|B| \leq |G|/2$, then by Lemma 2.3, applied with B and $T = S$, there is a $g \in S$ such that $\lambda_B(g) \geq \min\{(|B|+1)/2, (|S \cup S^{-1}|+2)/4\}$. Since $|S| = k+1$, we have

$$\lambda_B(g) \geq \lceil \min\{(k+3)/2, (k+3)/4\} \rceil \geq 2.$$

Therefore, $|\Pi^*(S)| \geq |\Pi^*(S \setminus \{g\})| + \lambda_B(g) \geq 2k+1+2 = 2|S|+1$.

Now, assume that $|G|/2 < |B| \leq |G|-3$. Then $3 \leq |G \setminus B| \leq |G|/2$. By Lemma 2.3, applied with $G \setminus B$ and $T = S$, there is a $g \in S$ such that $\lambda_{G\setminus B}(g) \geq \min\{(|G \setminus B|+1)/2, (|S \cup S^{-1}|+2)/4\}$. Thus

$$\lambda_{G\setminus B}(g) \geq \lceil \min\{(3+1)/2, (k+3)/4\} \rceil = 2.$$

Since $\lambda_{G\setminus B}(g) = |(G\setminus B)g \setminus (G \setminus B)| = |(G \setminus Bg) \cap B| = |B \setminus Bg| = |Bg \setminus B| = \lambda_B(g)$, we have $|\Pi^*(S)| \geq |\Pi^*(S \setminus \{g\})| + \lambda_B(g) = |\Pi^*(S \setminus \{g\})| + \lambda_{G\setminus B}(g) \geq 2k+1+2 = 2|S|+1$. ■

LEMMA 3.10. *Let G be a finite non-abelian group of order $n \geq 24$ with $4 \,|\, n$ and let $S \subset G \setminus \{1\}$ be a subset with $|S| = n/2-1$. Let $X \subset S$ be a subset with $|X| = n/4-1$ such that $|\Pi^*(X)|$ is minimal and let $Y = S \setminus X$. Suppose $\langle X \rangle = \langle Y \rangle = G$. If either $|\Pi^*(X)| \geq (15n-7)/32$ or $|\Pi^*(X \setminus \{x_0\})| \geq (6n-5)/16$ for some $x_0 \in X$, then $\Pi(S) = G$.*

Proof. If $|\Pi^*(X)| \geq n/2+1$, then $|\Pi^*(Y)| \geq |\Pi^*(X)| \geq n/2+1$. Thus $|\Pi(Y)| \geq n/2$. Therefore, $|\Pi^*(X)| + |\Pi(Y)| > n$. By Lemma 2.1, $\Pi(S) \supset \Pi^*(X)\Pi(Y) = G$. Next assume that $|\Pi^*(X)| \leq n/2$. We first prove the following

CLAIM. *We have $1 \in \Pi(S)$.*

Proof of Claim. Let $(x_i)_{i=1}^{n/4-1}$ be a resolving sequence of X. As before (2.2), denote $X_i = \{x_j : 1 \leq j \leq i \leq n/4-1\}$, $B_i = \Pi^*(X_i)$ and $\lambda_i = \lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) : 1 \leq j \leq i \leq n/4-1\}$. Assume to the contrary that $1 \notin \Pi(S)$. Then $1 \notin \Pi(X)$ and $1 \notin \Pi(X \setminus \{x_{n/4-1}\})$. By Lemma 3.9, $|\Pi^*(X)| \geq n/2-1$. Let $H = \langle X \setminus \{x_{n/4-1}\} \rangle$; then $|H| \geq n/4-1$. Since $n \geq 24$, we conclude that $|H| \in \{n, n/2, n/3, n/4\}$ and $|X_{n/4-2}| = n/4-2 \geq 4$. Next we show that $|B_{n/4-2}| \geq n/2-3$. If H is abelian, then by Lemma 3.8, $|\Pi^*(X \setminus \{x_{n/4-1}\})| \geq 2|X \setminus \{x_{n/4-1}\}|+1 = n/2-3$.

Assume that H is non-abelian. Note that $n \geq 24$. If $|H| = n/4$, then by [17, Theorem 1.1], we have $|X_{n/4-2}| = n/4-2 > n/8 = |H|/2+2-2 \geq |H|/q+q-2 \geq \mathsf{d}(H)$, where $\mathsf{d}(H)$ is the small Davenport constant of H, and q is the smallest prime divisor of $|H|$. Therefore, $1 \in \Pi(X_{n/4-2})$, yielding a contradiction.

Similarly, if $|H| = n/3$ and $n > 24$, then $|X_{n/4-2}| > |H|/2 \geq \mathsf{d}(H)$. Then $1 \in \Pi(X_{n/4-2})$, yielding a contradiction. If $|H| = n/3$ and $n = 24$, then $|H| = 8$ and $|X_H| \geq |X_{n/4-2}| = 4 = |H|/2$. By Lemma 3.2(i), H has a subgroup of index 2. Since H is non-abelian, by Lemma 3.1(i) we have $|X_{n/4-2}| = 4 = \mathsf{cr}(H)$. Thus $1 \in \Pi(X_{n/4-2}) = H$, yielding a contradiction.

If $|H| \in \{n/2, n\}$, then $|X_{n/4-2}| \le |H|/2 - 2$. By Lemma 3.9, $|B_{n/4-2}| \ge n/2 - 3$. Therefore, in each case we have $|B_{n/4-2}| \ge n/2 - 3$. Let

$$\lambda = \min\{(|\Pi^*(X)| + 1)/2, (|S \cup S^{-1}| + 2)/4\}.$$

Then $\lambda \ge (n+2)/8$. By Lemma 2.3, applied with $B = \Pi^*(X)$ and $T = S$, there is a $g \in X \cup Y$ such that $\lambda_{\Pi^*(X)}(g) \ge \lambda$. If $g \in X$, then $\lambda_{n/4-1} \ge \lambda \ge (n+2)/8$. Thus $|\Pi^*(X)| \ge |B_{n/4-2}| + \lambda_{n/4-1} > n/2$, a contradiction. Therefore, $g \in Y$. Clearly, $|\Pi^*(X \cup \{g\})| \ge |\Pi^*(X)| + \lambda$. Since $|Y \setminus \{g\}| = n/4 - 1$, we have $|\Pi(Y \setminus \{g\})| \ge |\Pi^*(Y \setminus \{g\})| - 1 \ge |\Pi^*(X)| - 1$. Thus

$$\begin{aligned}|\Pi^*(X \cup \{g\})| + |\Pi(Y \setminus \{g\})| &\ge 2|\Pi^*(X)| + \lambda - 1 \\ &\ge 2(n/2 - 1) + (n+2)/8 - 1 > n = |G|.\end{aligned}$$

By Lemma 2.1, $\Pi(S) \supset \Pi^*(X \cup \{g\})\Pi(Y \setminus \{g\}) = G$, a contradiction to $1 \notin \Pi(S)$. This completes the proof of the Claim. ∎

We now show that if $|\Pi^*(X)| \ge (15n - 7)/32$, then $\Pi(S) = G$. Let

$$\lambda' = \min\{(|\Pi^*(X)| + 1)/2, (|Y \cup Y^{-1}| + 2)/4\}.$$

Then $\lambda' \ge (n+8)/16$. By Lemma 2.3, applied with $B = \Pi^*(X)$ and $T = Y$, there exists a $y \in Y$ such that $\lambda_{\Pi^*(X)}(y) \ge \lambda'$. Clearly, $|\Pi^*(X \cup \{y\})| \ge |\Pi^*(X)| + \lambda'$. Since $|Y \setminus \{y\}| = n/4 - 1$, we have $|\Pi^*(Y \setminus \{y\})| \ge |\Pi^*(X)|$. Thus $|\Pi^*(X \cup \{y\})| + |\Pi^*(Y \setminus \{y\})| \ge 2|\Pi^*(X)| + \lambda' > |G|$. By the Claim, $1 \in \Pi(S)$. Therefore, $\Pi(S) = \Pi^*(S) = \Pi^*(X \cup \{y\})\Pi^*(Y \setminus \{y\}) = G$ by Lemma 2.1.

Finally, we will show that if $|\Pi^*(X)| < (15n - 7)/32$ and $|B_{n/4-2}| \ge (6n-5)/16$, then $\Pi(S) = G$. By Lemma 2.3, we have $\lambda_{n/4-1} \ge (n+4)/16$ and thus $|\Pi^*(X)| \ge |B_{n/4-2}| + \lambda_{n/4-1} \ge (7n - 1)/16$. As before, by Lemma 2.3, applied with $B = \Pi^*(X)$ and $T = S$, there is a $g \in X \cup Y$ such that $\lambda_{\Pi^*(X)}(g) \ge \lambda$. If $g \in X$, then $\lambda_{n/4-1} \ge \lambda \ge (n+2)/8$. Thus $|\Pi^*(X)| \ge |B_{n/4-2}| + \lambda_{n/4-1} \ge (6n-5)/16 + (n+2)/8 \ge (15n-7)/32$, a contradiction. Therefore, $g \in Y$. As above, $|\Pi^*(X \cup \{g\})| + |\Pi^*(Y \setminus \{g\})| \ge 2|\Pi^*(X)| + \lambda \ge 2(7n - 1)/16 + (n+2)/8 > n = |G|$. By Lemma 2.1, $\Pi(S) = \Pi^*(S) = \Pi^*(X \cup \{g\})\Pi^*(Y \setminus \{g\}) = G$.

Lemma 3.11. *Let G be a finite non-abelian group of even order $n \ne 6$. Then $\mathsf{cr}(G) \le n/2$. Moreover, equality holds if and only if G has a subgroup of index 2.*

Proof. By Lemma 3.1(i), if G has a subgroup of index 2, then $\mathsf{cr}(G) = n/2$. It suffices to prove that if G does not have any subgroup of index 2, then $\mathsf{cr}(G) \le n/2 - 1$. Now, assume that G does not have any subgroup of index 2. By Lemma 3.2(ii), $4 \mid n$. Moreover, by Lemma 3.2(i, vii), $n \notin \{16, 20\}$. By

Lemma 3.7, we may assume that $n > 12$ and thus $n \geq 24$. Let S be a subset of $G \setminus \{1\}$ with cardinality $|S| = n/2 - 1$. It suffices to show that $\Pi(S) = G$. Let $X \subset S$ with $|X| = n/4 - 1$ be a subset such that $|\Pi^*(X)|$ is minimal and let $Y = S \setminus X$.

Case 1: $\langle X\rangle \neq G$ or $\langle Y\rangle \neq G$. Assume that $\langle X\rangle \neq G$. Let $H = \langle X\rangle$. Since $|X| = n/4 - 1$, we have $|H| \geq n/4$. Thus, $|H| = n/4$ or $n/3$. Since G does not have any subgroup of index 2, if $|H| = n/4$, then by Lemma 3.2(vi), H is not normal. Moreover, $\mathrm{Core}(H) \neq H$ and $G/\mathrm{Core}(H)$ is isomorphic to a subgroup of S_4, where $\mathrm{Core}(H)$ is the core of H and S_4 is the symmetric group of degree 4. By Lemma 3.2(vi), $G/\mathrm{Core}(H)$ contains no subgroup of index 2. Since $4 \mid |G/\mathrm{Core}(H)|$, we conclude that $G/\mathrm{Core}(H) \cong A_4$. By Lemma 3.7, $\mathsf{cr}(G/\mathrm{Core}(H)) \leq 5$. Let $\varphi : G \to G/\mathrm{Core}(H)$ be the natural epimorphism. Since $\lceil |S|/|\mathrm{Core}(H)|\rceil \geq 6$, we conclude that $\varphi(S \setminus \mathrm{Core}(H))$ contains a subset $\bar{X}$ of $G/\mathrm{Core}(H)$ with $|\bar{X}| \geq 5$. Thus $\varphi(\Pi(S\setminus\mathrm{Core}(H))) = \Pi(\varphi(S \setminus \mathrm{Core}(H))) \supset \Pi(\bar{X}) = G/\mathrm{Core}(H)$. Note that $X = H \setminus \{1\}$. Then $\mathrm{Core}(H) = X_{\mathrm{Core}(H)} \cup \{1\} = \Pi^*(X_{\mathrm{Core}(H)}) = \Pi^*(S_{\mathrm{Core}(H)})$. Therefore, $\Pi(S) \supset \Pi^*(S_{\mathrm{Core}(H)})\Pi(S \setminus \mathrm{Core}(H)) = G$.

If $|H| = n/3$ and H is not normal, then $\mathrm{Core}(H) \neq H$ and $G/\mathrm{Core}(H)$ is isomorphic to a subgroup of S_3, where S_3 is the symmetric group of degree 3. Since $3 \mid |G/\mathrm{Core}(H)|$, we conclude that $G/\mathrm{Core}(H)$ has a subgroup of index 2. By Lemma 3.2(vi), G has a subgroup of index 2, a contradiction.

Now assume that $|H| = n/3$ and H is normal. Note that $|H| = n/3 \geq 8$ and $2 \mid |H|$. If H has a subgroup of index 2, then by Lemma 3.1(i) we have $\mathsf{cr}(H) \leq |H|/2 + 1$. If H does not have any subgroup of index 2, then H is non-abelian. Since $|H| \neq 6$, by the induction hypothesis we have $\mathsf{cr}(H) \leq |H|/2 - 1$. In both cases, $\mathsf{cr}(H) \leq |H|/2 + 1 = n/6 + 1 \leq n/4 - 1 = |X|$. Thus $\Pi(S_H) \supset \Pi(X) = H$. Moreover, $|S \setminus S_H| \geq |S| - |H| + 1 \geq 2$. By Lemma 3.3, $\Pi(S) = G$.

If $\langle Y\rangle \neq G$, then as above, we conclude that $|\langle Y\rangle| = n/3$ and $\Pi(S) = G$.

Case 2: $\langle X\rangle = G$ and $\langle Y\rangle = G$. Let $(x_i)_{i=1}^{n/4-1}$ be a resolving sequence for X with critical index t and $H = \langle X_{t-1}\rangle$. As before (2.2), denote $X_i = \{x_j : 1 \leq j \leq i \leq n/4 - 1\}$, $B_i = \Pi^*(X_i)$ and $\lambda_i = \lambda_{B_i}(x_i) = \max\{\lambda_{B_i}(x_j) : 1 \leq j \leq i \leq n/4 - 1\}$. By Lemma 3.10, if $|\Pi^*(X)| \geq (15n - 7)/32$ or $|B_{n/4-2}| \geq (6n - 3)/16$, then $\Pi(S) = G$. Next, we assume that

$$|\Pi^*(X)| < (15n - 7)/32 \quad \text{and} \quad |B_{n/4-2}| < (6n - 5)/16.$$

Subcase 2.1: $t > n/5$. Since H is a proper subgroup of G, we have $|H| \geq t > n/5$. Note that G has no subgroups of index 2. Thus $|H| = n/4$ or $n/3$.

If $|H| = n/4$, then H is not normal. Since $n \geq 24$, by Lemma 3.2(vii), we know that H is not of prime order. Suppose H is of even order. If H has a subgroup of index 2, then by Lemma 3.1(i), $\mathsf{cr}(H) \le |H|/2 + 1$. If H does not have any subgroup of index 2, then H is non-abelian. By the induction hypothesis, $\mathsf{cr}(H) \le |H|/2$. Now, suppose H is of odd order. If $|H|$ has at least three prime divisors, then by Lemma 3.6, $\mathsf{cr}(H) \le |H|/q+q-2 \le |H|/2$, where q is the smallest prime divisor of $|H|$. If $|H|$ has two prime divisors, then by Lemma 3.1(iii), $\mathsf{cr}(H) \le |H|/q + q - 1 \le |H|/2 + 1$. In all cases, $\mathsf{cr}(H) \le |H|/2+1 = n/8+1 \le \lfloor n/5 \rfloor \le t-1$. Thus $\Pi(X_{t-1}) = H$. Therefore,

$$|\Pi^*(X)| \ge |\Pi(X)| \ge |\Pi(X_t)| \ge 2|\Pi(X_{t-1})| \ge n/2,$$

a contradiction.

If $|H| = n/3$, then as in Case 1, H is normal. Note that H is of even order and $|H| \ge 8$. If $|H| = 8$, then $|G| = 24$. Since G does not contain any subgroup of index 2, we conclude that every subgroup of order 4 is not normal and thus is not a characteristic subgroup of H. By the subgroup structure of groups of order 8, we deduce that only C_2^3 and Q_8 have no characteristic subgroup of order 4 and hence either $H \cong C_2^3$ or $H \cong Q_8$. By Lemma 3.1(i), $\mathsf{cr}(H) = |H|/2$. Now suppose that $|H| > 8$. If H has a subgroup of index 2, then by Lemma 3.1(i), $\mathsf{cr}(H) = |H|/2$. If H does not have any subgroup of index 2, then H is non-abelian. By the induction hypothesis, we have $\mathsf{cr}(H) \le |H|/2 - 1$. In each case, we have $\mathsf{cr}(H) \le |H|/2 = n/6 \le \lfloor n/5 \rfloor \le t - 1$. Thus $\Pi(X_{t-1}) = H$. Therefore, $|\Pi^*(X)| \ge |\Pi(X)| \ge |\Pi(X_t)| \ge 2|\Pi(X_{t-1})| \ge 2n/3 > n/2$, a contradiction.

Subcase 2.2: $t \le n/5$. We will compute the cardinality of $B_{n/4-2}$, which will lead to a contradiction with $|B_{n/4-2}| < (6n-5)/16$, and complete the proof. Note that $|\Pi^*(X)| < (15n-7)/32$ and $\langle X \rangle = G$. By Lemma 2.3, $\lambda_i \ge (i + 2 + \mu(i))/4$ for all $i \ge t$, where $\mu(i) = a$ for $i \equiv 2 - a \bmod 4$ and $a \in [0, 3]$. By (2.2), for all $n/4 - 2 \ge s \ge t$, we have

$$(6n-5)/16 > |B_{n/4-2}| \ge (n/4+s+5)(n/4-s-1)/8-1/2+|B_{s-1}|. \tag{3.7}$$

Note that $|B_i| \ge i + 1$ for $i \ge 1$. Therefore, $|B_t| = |B_{t-1}| + |B_{t-1}x_t| = 2|B_{t-1}| \ge 2t$. By (3.7), applied with $s = t + 1$, we have

$$2t + (n/4 + t + 6)(n/4 - t - 2)/8 - 1/2 - (6n - 5)/16 < 0. \tag{3.8}$$

Set $F(t, n) = 2t+(n/4+t+6)(n/4-t-2)/8-3/16-3n/8$. Notice that $\frac{\partial F(t,n)}{\partial t} = 1 - t/4$. Since G is non-abelian, we have $t \ge 2$. Thus $2 \le t \le n/5$. Therefore, $F(t, n) \ge \min\{F(2, n), F(n/5, n)\}$. Let

$$G_1(n) = F(2, n) = (n/4 + 8)(n/4 - 4)/8 + 61/16 - 3n/8,$$
$$G_2(n) = F(n/5, n) = 2n/5 + (9n/20 + 6)(n/20 - 2)/8 - 3/16 - 3n/8.$$

If $n \ge 36$, then $G_1'(n) = (n/2 + 4)/32 - 3/8 \ge 0$ and $G_2'(n) = 9n/1600 - 1/20 \ge 0$. Therefore,

$$G_1(n) \ge G_1(36) = (9 + 8)(9 - 4)/8 + 61/16 - 27/2 > 0,$$

and

$$G_2(n) \geq G_2(36) = 72/5 + (81/5 + 6)(9/5 - 2)/8 - 3/16 - 27/2 > 0.$$

Thus $F(t, n) > 0$, a contradiction to (3.8).

Now assume that $24 \leq n \leq 35$. Since $4 \mid n$ and G does not contain any subgroup of index 2, by Lemma 3.2(vii, i), we conclude that $n \notin \{28, 32\}$. Then $n = 24$, $2 \leq t \leq 4$ and $|B_4| \leq 8$.

SUBSUBCASE 2.2.1: $t = 4$. If $|B_3| \geq 5$, then $|B_4| \geq 2|B_3| \geq 10$, a contradiction.

Note that $B_3 = \Pi^*(\{x_1, x_2, x_3\}) \supset \{1, x_1, x_2, x_3\}$. If $|B_3| \leq 4$, then $|B_3| = 4$ and thus $B_3 = \{1, x_1, x_2, x_3\}$. We now show that B_3 is a subgroup of order 4. If $x_1x_2 = 1$, then $x_1x_3 = x_3x_1 = x_2$ and $x_2x_3 = x_3x_2 = x_1$. Thus $x_1^2 = x_2^2 = x_3$ and $x_3^2 = 1$. Therefore, $B_3 \cong C_4$. Similarly, if $x_1x_3 = 1$ or $x_2x_3 = 1$, then $B_3 \cong C_4$. Suppose that $x_ix_j \neq 1$ for distinct $i, j \in [1, 3]$. Then $x_1x_2 = x_2x_1 = x_3$, $x_1x_3 = x_3x_1 = x_2$ and $x_2x_3 = x_3x_2 = x_1$. Thus $x_1^2 = x_2^2 = x_3^2 = 1$. Therefore, $B_3 \cong C_2 \otimes C_2$. So, G has a subgroup $M = B_3$ of order 4. If M is normal, then $|G/M| = 6$. Therefore, G/M has a subgroup of index 2 and so does G, a contradiction. So M is not normal. Note that $\langle M, x_4 \rangle = G$. Then $x_4 \notin N_G(M)$. Therefore, $x_4Mx_4^{-1} \neq M$ and $|x_4Mx_4^{-1} \cap M| \leq 2$. Thus $|x_4M \cap Mx_4| \leq 2$. Since $B_4 \supset M \cup x_4M \cup Mx_4$, we have $|B_4| \geq 2|M| + 2 \geq 10$, a contradiction.

SUBSUBCASE 2.2.2: $t = 3$. If $|B_2| \geq 4$, then $|B_3| \geq 2|B_2| \geq 8$. Since $\lambda_4 \geq 2$, we have $|B_4| \geq |B_3| + 2 \geq 10$, a contradiction.

If $|B_2| \leq 3$, then $|B_2| = 3$ and $x_1 = x_2^{-1}$. Let $M = \langle x_1 \rangle$. Then $|M| = 3, 4, 6$, or 8. Now we show that M is not normal. Assume to the contrary that M is normal. If $|M| \in \{3, 4, 6\}$, then G/M has a subgroup of index 2. By Lemma 3.2(vi), G has a subgroup of index 2, a contradiction. If $|M| = 8$, then M has a characteristic subgroup M_1 of order 4 since M is cyclic, whence M_1 is a normal subgroup of G. Since G/M_1 has a subgroup of index 2, we deduce that G has a subgroup of index 2, a contradiction. Therefore, M is not normal in each case. Note that $\langle M, x_3 \rangle = G$ and M is cyclic. As in Subsubcase 2.2.1, we have

$$|x_3B_2x_3^{-1} \cap B_2| = 1 \quad \text{and} \quad |x_3B_2 \cap B_2x_3| = 1.$$

As above, $|B_3| \geq 2|B_2| + 2 \geq 8$ and $|B_4| \geq |B_3| + 2 \geq 10$, a contradiction.

SUBSUBCASE 2.2.3: $t = 2$. Since $\langle x_1, x_2 \rangle = G$ is not abelian, we have $x_1x_2 \neq x_2x_1$, whence $|B_2| = |\{1, x_1, x_2, x_1x_2, x_2x_1\}| = 5$. Since $\lambda_3 \geq 2$ and $\lambda_4 \geq 2$, we have $|B_4| \geq |B_2| + 2 + 2 \geq 9$, a contradiction. ■

Proof of Theorem 1.1. If G is of odd order, then the result follows from Lemmas 3.6 and 3.1(iii). If G is of even order, then the result follows from Lemma 3.11. ■

Acknowledgements. We would like to thank the referees for their valuable suggestions which helped improve the readability of the paper.

This work was supported in part by the National Natural Science Foundation of China (Nos. 11701256, 12071344), the Natural Science Foundation of Henan (No. 242300421393) and the Foundation of Henan Educational Committee (No. 23A110012).

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. N. Srivastava et al. (eds.), North-Holland, Amsterdan, 1973, 95–100.
[4] P. Erdős and H. Heilbronn, *On the additon of residue classes mod p*, Acta Arith. 9 (1964), 149–159.
[5] M. Freeze, W. Gao and A. Geroldinger, *The critical number of finite abelian groups*, J. Number Theory 129 (2009), 2766–2777; Corrigendum 152 (2015), 205–207.
[6] W. Gao, *A combinatorial problem on finite groups*, Acta Math. Sinica 38 (1995), 395–399 (in Chinese).
[7] W. Gao and Y. O. Hamidoune, *On additive bases*, Acta Arith. 88 (1999), 233–237.
[8] W. Gao, Y. O. Hamidoune, A. Lladó and O. Serra, *Covering a finite abelian group by subset sums*, Combinatorica 23 (2003), 599–611.
[9] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.
[10] J. R. Griggs, *Spanning subset sums for finite abelian groups*, Discrete Math. 229 (2001), 89–99.
[11] Y. O. Hamidoune, A. S. Lladó and O. Serra, *On complete subsets of the cyclic group*, J. Combin. Theory Ser. A 115 (2008), 1279–1285.
[12] H. B. Mann, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory*, Interscience, New York, 1965.
[13] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, New York, 1996.
[14] J. E. Olson, *An addition theorem modulo p*, J. Combin. Theory 5 (1968), 45–52.
[15] J. E. Olson, *Sums of sets of group elements*, Acta Arith. 28 (1975), 147–156.
[16] J. E. Olson and E. T. White, *Sums from a sequence of group elements*, in: Number Theory and Algebra, H. Zassenhaus (ed.), Academic Press, 1977, 215-222.
[17] Y. Qu, Y. Li and D. Teeuwsen, *On a conjecture of the small Davenport constant for finite groups*, J. Combin. Theory Ser. A 189 (2022), art. 105617, 14 pp.
[18] M. Suzuki, *Group Theory*, Vol. I, Springer, Berlin, 1982.
[19] V. H. Vu, *Structure of large incomplete sets in abelian groups*, Combinatorica 30 (2010), 225–237.
[20] Q. Wang and Y. Qu, *On the critical number of finite groups (II)*, Ars Combin. 113A (2014), 321–330.

[21] Q. Wang and J. Zhuang, *On the critical number of finite groups of order pq*, Int. J. Number Theory 8 (2012), 1271–1279.

[22] M. Y. Xu, *An Introduction to Finite Group Theory I*, Sci. Press, Beijing, 1999 (in Chinese).

Yongke Qu
Department of Mathematics
Luoyang Normal University
Luoyang 471934, P.R. China
E-mail: yongke1239@163.com

Weidong Gao
Center for Applied Mathematics
Tianjin University
Tianjin 300072, P.R. China
E-mail: wdgao@nankai.edu.cn
weidong.gao@tju.edu.cn