ON A CONJECTURE OF ZHUANG AND GAO

YONGKE QU AND YUANLIN LI*

Abstract. Let $G$ be a multiplicatively written finite group. We denote by $E(G)$ the smallest integer $t$ such that every sequence of $t$ elements in $G$ contains a product-one subsequence of length $|G|$. In 1961, Erdős, Ginzburg and Ziv proved that $E(G) \leq 2|G| - 1$ for every finite abelian group $G$ and this result is known as the Erdős-Ginzburg-Ziv Theorem. In 2005, Zhuang and Gao conjectured that $E(G) = d(G) + |G|$, where $d(G)$ is the small Davenport constant. In this paper, we confirm the conjecture for the case when $G = \langle x, y | x^p = y^m = 1, x^{-1}y x = y^r \rangle$, where $p$ is the smallest prime divisor of $|G|$ and $\gcd(p(r-1), m) = 1$.

Keywords: Erdős-Ginzburg-Ziv theorem; Davenport constant; Product-one sequence; Metacyclic group

2020 Mathematics Subject Classifications: Primary 11B75; Secondary 11P70

1. Introduction and main results

Let $G$ be a finite group written multiplicatively. Let $S = g_1 \cdots g_\ell$ be a sequence over $G$ with length $\ell$. We use

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

to denote the set of products of $S$. We say that $S$ is a product-one sequence if $1 \in \pi(S)$. Let $d(G)$ be the small Davenport constant of $G$ (i.e., the maximal integer $\ell$ such that there is a sequence of length $\ell$ over $G$ which has no nontrivial product-one subsequence). We denote by $E(G)$ the smallest integer $t$ such that every sequence of length $t$ over $G$ contains a product-one subsequence of length $|G|$. The problem of finding the precise value of the Davenport constant and what is now known as the Erdős-Ginzburg-Ziv Theorem have become the starting points of zero-sum theory.

Theorem 1.1. (Theorem of Erdős-Ginzburg-Ziv) \[4\] Let $G$ be a finite abelian group. Then $E(G) \leq 2|G| - 1$.

Since that time (dating back to the early 1960s), zero-sum theory has developed into a flourishing branch of additive and combinatorial number theory. At the present moment, two conjectures on $E(G)$ can be found in the literature. We briefly discuss some history and the motivation for studying these conjectures. For more detailed information, the interested reader may refer to the surveys \[2\] \[7\] \[14\] or the monographs \[13\] \[15\]. Although the main focus of zero-sum theory has initially been on abelian groups, the research has never been restricted to the abelian setting alone. In 1976, Olson \[18\] showed that $E(G) \leq 2|G| - 1$ holds for all finite groups. In 1984, Yuster and Peterson \[20\] showed that

*Corresponding author: Yuanlin Li, E-mail: yli@brocku.ca.
E(G) ≤ 2|G| − 2 when G is a non-cyclic solvable group. Later Yuster \cite{19} improved the result to E(G) ≤ 2|G| − r provided that |G| ≥ 600((r − 1)!)². In 1996, Gao \cite{5} further improved the upper bound to E(G) ≤ \frac{11|G|}{6} − 1. More recently in 2010, Gao and Li \cite{8} proved that E(G) ≤ \frac{7|G|}{4} − 1 and they proposed the following conjecture.

**Conjecture 1.2.** Let G be any finite non-cyclic group. Then E(G) ≤ \frac{3|G|}{2}.

We remark that the above mentioned upper bound on E(G) is the best possible since E(G) = \frac{3|G|}{2} when G = D_{2n} is a dihedral group \cite[Theorem 8]{11}.

In 1996, Gao \cite{6} discovered the fundamental relationship between E(G) and d(G) for abelian groups, i.e., E(G) = d(G) + |G|. In 2005, Zhuang and Gao \cite{21} investigated this relation E(G) = d(G) + |G| for some non-abelian groups and proposed the following conjecture.

**Conjecture 1.3.** Let G be a finite group. Then E(G) = d(G) + |G|.

They confirmed Conjecture 1.3 for dihedral groups of order 2p where p ≥ 4001 is a prime. Gao and Lu \cite{11} then improved this result to dihedral groups of order 2n for all n ≥ 23. Bass \cite{11} extended the method used by Gao and Lu, and proved the conjecture for all dihedral groups, dicyclic groups, and groups C_p \rtimes C_q, where p, q are primes. Recently, in 2015 Han \cite{16} verified the conjecture for the case when G is a non-cyclic nilpotent group or when G ≅ C_p \rtimes C_{pm}, where p is a prime. Most recently, in 2019 Han and Zhang \cite{17} further extended Han’s early result and verified the conjecture for G ≅ C_m \rtimes C_{mn}. It is natural to extend this line of research to the class of metacyclic groups C_n \rtimes C_m where gcd(n, m) = 1. In this paper, we confirm Conjecture 1.3 for the following class of metacyclic groups and our main result is as follows.

**Theorem 1.4.** Let G = \langle x, y | x^p = y^m = 1, x^{-1}yx = y^r \rangle, where p is the smallest prime divisor of |G| and gcd(p(r − 1), m) = 1. Then d(G) = m + p − 2 and E(G) = d(G) + |G|.

We remark that the investigation of the above mentioned class of metacyclic groups is of special interest as it is closely related to solving Conjecture 1.2. Very recently, Gao, Li, and Qu \cite{10} made substantial progress on this conjecture and proved that E(G) ≤ \frac{3|G|}{2} holds for all non-cyclic groups of odd order by using the minimal counterexample method.

Our main result and some technical lemmas in Section 3 have been used in \cite{10} as the necessary ingredients to construct a minimal counterexample leading to a contradiction. In addition, the methods developed in this paper (such as applying a generalization of Kneser’s Additive Theorem to estimate a partial product of sets Π_m(A)) have been used repeatedly in \cite{10} to help simplify some complicated computations and to achieve the best possible upper bound on E(G).

### 2. Notation and Preliminaries

We follow the notation and conventions detailed in \cite{12}.

For real numbers a, b ∈ \mathbb{R}, we set [a, b] = \{x ∈ \mathbb{Z} : a ≤ x ≤ b\}. For integers m, n ∈ \mathbb{Z}, we denote by gcd(m, n) the greatest common divisor of m and n.
Let $G$ be a finite multiplicative group. If $A \subseteq G$ is a nonempty subset, then denote by $\langle A \rangle$ the subgroup of $G$ generated by $A$. If $A$ and $B$ are subsets of $G$, we define the product-set as $AB = \{ab : a \in A, b \in B\}$. Recall that by a sequence over a group $G$, we mean a finite, unordered sequence where repetition of elements is allowed. We view sequences over $G$ as elements of the free abelian monoid $\mathcal{F}(G)$, denote multiplication in $\mathcal{F}(G)$ by the bold symbol $\cdot$ rather than by juxtaposition, and use brackets for all exponentiation in $\mathcal{F}(G)$.

A sequence $S \in \mathcal{F}(G)$ can be written in the form $S = g_1 \cdots g_\ell$, where $|S| = \ell$ is the length of $S$. For $g \in G$, let $\nu_g(S) = |\{i \in [1, \ell] : g_i = g\}|$ denote the multiplicity of $g$ in $S$. A sequence $T \in \mathcal{F}(G)$ is called a subsequence of $S$ and is denoted by $T \mid S$ if $\nu_g(T) \leq \nu_g(S)$ for all $g \in G$. Denote by $S \cdot T^{[-1]}$ the subsequence of $S$ obtained by removing the terms of $T$ from $S$.

If $S_1, S_2 \in \mathcal{F}(G)$, then $S_1 \cdot S_2 \in \mathcal{F}(G)$ denotes the sequence satisfying $\nu_g(S_1 \cdot S_2) = \nu_g(S_1) + \nu_g(S_2)$ for all $g \in G$. For convenience, we write $g^{[k]} = \underbrace{g \cdot \ldots \cdot g}_{k} \in \mathcal{F}(G)$ for $g \in G$ and $k \in \mathbb{N}_0$.

Suppose $S = g_1 \cdots g_\ell \in \mathcal{F}(G)$. Let
\[ \pi(S) = \{g_{\tau(1)} \cdots g_{\tau(\ell)} : \tau \text{ a permutation of } [1, \ell] \} \subseteq G \]
denote the set of products of $S$. Let
\[ \Pi_n(S) = \bigcup_{|T| = n} \pi(T) \]
denote the set of all $n$-products of $S$. Let
\[ \Pi(S) = \bigcup_{1 \leq n \leq \ell} \Pi_n(S) \]
denote the set of all subsequence products of $S$. The sequence $S$ is called
- product-one if $1 \in \pi(S)$;
- product-one free if $1 \not\in \Pi(S)$;
- minimal product-one if $1 \in \pi(S)$ and $S$ has no proper product-one subsequence.

If $A = (A_1, \ldots, A_\ell)$ is a sequence of finite subsets of $G$, let $m \leq \ell$, we define
\[ \Pi^m(A) = \{a_{i_1} \cdots a_{i_m} : 1 \leq i_1 < \cdots < i_m \leq \ell \text{ and } a_{i_j} \in A_{i_j} \text{ for every } 1 \leq j \leq m\}. \]

Let $A$ be a subset of $G$ and $\text{stab}(A) = \{g \in G : gA = A\}$ its stabilizer. The following lemma is a generalization of Kneser’s Theorem which is crucial for our proof of the main result.

**Lemma 2.1.** [3 Theorem 1.3][13 Theorem 13.1] Let $A = (A_1, \ldots, A_\ell)$ be a sequence of finite subsets of an abelian group $G$, let $m \leq \ell$, and let $H = \text{stab}(\Pi^m(A))$. If $\Pi^m(A)$ is nonempty, then
\[ |\Pi^m(A)| \geq |H| \left(1 - m + \sum_{Q \in G/H} \min\{\ell, |\{i \in [1, \ell] : A_i \cap Q \neq \emptyset\}|\right). \]
We also need the following lemma about product-one free sequences.

**Lemma 2.2.** [9 Lemma 2.4] Let $S$ be a product-one free sequence over $G$. Then $|\Pi(S)| \geq |S|$.

### 3. Proof of Theorem 1.4

Throughout this section, let $G = \langle x, y | x^p = y^m = 1, x^{-1}yx = y^r \rangle \cong C_p \ltimes C_m$, where $p$ is the smallest prime divisor of $|G|$, and $\gcd(p(r-1), m) = 1$. Let $K = \langle x \rangle$ and $N = \langle y \rangle$. Then $C_m \cong N \triangleleft G$ and $K \cong G/N \cong C_p$. Let $\varphi$ be the canonical homomorphism from $G$ onto $G/N$. Then for each sequence $T$ over $G$, $\varphi(T)$ is a sequence over $G/N$. Note that if $\varphi(T)$ is a product-one sequence over $G/N$, then $\pi(T) \subseteq N$, as $\varphi(\pi(T)) = \pi(\varphi(T)) = 1$. We first prove a few useful lemmas.

**Lemma 3.1.** Let $M$ be any subgroup of $N = \langle y \rangle$, $u$ be an element of $N$ and $0 \leq s < s' \leq p-1$. Then

(i) If $u^s \in M$, then $\{u, u^r, \ldots, u^{r^{p-1}}\} \subseteq M$.

(ii) If both $u^s$ and $u^{s'}$ are in the same coset of $M$, then $\{u, u^r, \ldots, u^{r^{p-1}}\} \subseteq M$.

(iii) If $u \neq 1$, then $u^s \neq u^{s'}$.

**Proof.** (i) Since $\gcd(r, m) = 1$, we have $\gcd(r^s, m) = 1$. Therefore, there exist $k, e \in \mathbb{Z}$ such that $1 = r^sk + me$. From $u \in N$ we have $u^m = u^{[N]} = 1$. If $u^s \in M$, then $u = u^s + me = (u^s)^k \in M$. Thus $\{u, u^r, \ldots, u^{r^{p-1}}\} \subseteq M$.

(ii) Since both $u^s$ and $u^{s'}$ are in the same coset of $M$, $u^{s-r^s} \in M$, and thus $u^{1-r^s-s} \in M$. Since $u^{1-r^s-s} \in N$, by (i) we conclude that $u^{1-r^s-s} \in M$. Next we show that $\gcd(1-r^{s'-s}, m) = 1$. Assume to the contrary that $\gcd(1-r^{s'-s}, m) \neq 1$. Then there exists a prime divisor $q$ of $m$ such that $1-r^s-s \equiv 0 \pmod{q}$. Since $\gcd(r-1, m) = 1$, we have $r \equiv 1 \pmod{m}$. Since $r^p \equiv 1 \pmod{m}$, we have $r^p \equiv 1 \pmod{m}$, which together with $r \equiv 1 \pmod{m}$ gives $s' - s \equiv 0 \pmod{m}$. Thus $s = s'$, yielding a contradiction. Hence, we must have $\gcd(1-r^{s'-s}, m) = 1$. As in (i), we obtain $u \in M$, and thus $\{u, u^r, \ldots, u^{r^{p-1}}\} \subseteq M$.

(iii) Assume to the contrary that $u^s = u^{s'}$. Then both $u^s$ and $u^{s'}$ are in the same coset of the trivial subgroup $\{1\}$. By (ii), $u \in \{1\}$, so $u = 1$, yielding a contradiction. □

**Lemma 3.2.** Let $T = g_1 \cdots g_t$ be a sequence over $G$ such that $\varphi(T)$ is a minimal product-one sequence over $G/N$. Then for any $u \in \pi(T)$, we have $\pi(T) \supseteq \{u^{s_1}, u^{s_2}, \ldots, u^{s_t}\}$ for some subset $\{s_1, \ldots, s_t\} \subseteq [0, p-1]$. Moreover, if $u \neq 1$, then $u^{s_i} \neq u^{s_j}$ for all $1 \leq i < j \leq t \leq p$.

**Proof.** Without loss of generality, we may assume that $u = g_1 \cdots g_t$. Since $\varphi(T)$ is a minimal product-one sequence over $G/N \cong C_p$, we conclude that $t \leq p$ and $u = y^k \in \pi(T)$ for some $k \in [0, m-1]$. Let $g_1 \cdots g_t = x^{s_i} y^{c_i}$, where $1 \leq i \leq t$, $s_i \in [0, p-1]$ and $c_i \in [0, m-1]$. Since $u = x^{s_i} y^{c_i} = y^{k}$, we have $s_i = 0$ and $c_i = k$. Let $u_i = (g_1 \cdots g_t)^{-1} u (g_1 \cdots g_t)$, for
each \(i \in [1, t]\). Then \(u_t = u \in \pi(T)\) and \(u_i = g_{i+1}g_{i+2} \cdots g_{t}g_1 \cdots g_i \in \pi(T)\) for \(i \in [1, t-1]\). Therefore,

\[
u_i = (g_1 \cdots g_i)^{-1}u(g_1 \cdots g_i) = (x^{s_i}y^{c_i})^{-1}y^{(x^{s_i}y^{c_i})} = x^{-s_i}y^{x^{s_i}c_i} = u_i^{s_i}
\]

where \(i \in [1, t]\). Thus \(\pi(T) \supseteq \{u_i^{s_1}, u_i^{s_2}, \ldots, u_i^{s_t}\}\). We next prove \(s_i \neq s_j\) for all \(1 \leq i < j \leq t\). Assume to the contrary that \(s_i = s_j\) for some \(1 \leq i < j \leq t\). Then \(g_{i+1} \cdots g_j = (g_1 \cdots g_i)^{-1}(g_1 \cdots g_j) = (x^{s_i}y^{c_i})^{-1}x^{s_j}y^{c_j} = x^{s_j-s_i}y^{c_j-c_i} \in N\). Thus \(\varphi(g_{i+1} \cdots g_j) = 1\), yielding a contradiction to the proposition that \(\varphi(T)\) is a minimal product-one sequence over \(G/N\). This proves the first result of the lemma. The final statement follows immediately from Lemma 3.3 (iii). 

We remark that the following lemma is a slight generalization of [1, Lemma 16] and the same proof for [1, Lemma 16] carries over. Let \(N_i = x^iN\) be the \(i\)th coset of \(N\) in \(G\) for \(0 \leq i \leq p - 1\).

**Lemma 3.3.** Let \(T_0\) be a sequence of \(p\) elements in \(N_i\) for some \(i \in [1, p - 1]\). For every \(j \in [1, \ell]\), let \(T_j\) be a sequence over \(G\) such that \(\pi(T_j) \cap N \neq \emptyset\), and let \(u_j \in \pi(T_j) \cap N\). Then, for every \(t \in [1, \ell]\), \(\pi(T_0 \cdot T_1 \cdot \ldots \cdot T_t)\) contains the product set \(\pi(T_0)\{u_1, u_1', \ldots, u_t' \cdot u_1, u_1', \ldots, u_t'\}\).

**Remark 3.4.** \(m \equiv 1 \pmod{p}\).

**Proof.** Since \(r^p \equiv 1 \pmod{m}\), we have \(r^p \equiv 1 \pmod{q}\) for every prime \(q|m\). Since \(\gcd(r - 1, m) = 1\), we have \(r \not\equiv 1 \pmod{q}\). Therefore, \(r\) has order \(p\) modulo \(q\) and thus \(p|q - 1\) for every prime \(q|m\). Now, clearly \(m \equiv 1 \pmod{p}\). 

The next result gives the exact value of the small Davenport constant \(d(G)\).

**Proposition 3.5.** \(d(G) = m + p - 2\).

**Proof.** Let \(S_0 = x^{[p-1]} \cdot y^{[m-1]}\) be a sequence over \(G\) with length \(m + p - 2\). Then \(1 \not\in \Pi(S_0)\), so we have \(d(G) \geq m + p - 2\). Next, let \(S\) be any sequence over \(G\) of length \(m + p - 1\). We show that \(1 \in \Pi(S)\). Assume to the contrary that \(1 \not\in \Pi(S)\). Then \(1 \not\in \Pi(S_N)\). This together with Lemma 2.2 implies that \(m - 1 \geq |\Pi(S_N)| \geq |S_N|\). Let \(T = S \cdot S_N^{-1}\). Then \(|T| = |S| - |S_N| \geq p\). Since \(|\varphi(T)| = |T| \geq p\) and \(d(G/N) = d(C_{p^2}) = p - 1\), there exists a subsequence \(T_1 \mid T\) such that \(\varphi(T_1)\) is a minimal product-one sequence over \(G/N\). Let \(t\) be the maximal integer such that \(T_1 \cdot \ldots \cdot T_t \mid T\) and \(\varphi(T_i)\) is a minimal product-one subsequence over \(G/N\). Since \(\varphi(T \cdot (T_1 \cdot \ldots \cdot T_t)^{-1})\) is product-one free and \(d(G/N) = p - 1\), we have \(|T \cdot (T_1 \cdot \ldots \cdot T_t)^{-1}| = |\varphi(T \cdot (T_1 \cdot \ldots \cdot T_t)^{-1})| \leq p - 1\).

Let \(u_i \in \pi(T_i)\) for all \(i \in [1, t]\). Since \(1 \not\in \Pi(S)\), we have \(1 \not\in \pi(T_i)\) and thus

\[
u_i \neq 1 \mbox{ for all } i \in [1, t]. \quad (\Delta)
\]

By Lemma 3.2,

\[
\pi(T_i) \supseteq \{u_i^{s_{i1}}, u_i^{s_{i2}}, \ldots, u_i^{s_{ik}}\}
\]

for all \(i \in [1, t]\), \(t_i = |T_i|\), and moreover, \(u_i^{s_{ik}} \neq u_i^{s_{ik}}\) for \(1 \leq j < k \leq t_i\). Let \(S_N = u_{t+1} \cdot \ldots \cdot u_\ell\) where \(u_i \in N, i \in [t + 1, \ell], \ell = t + |S_N|\). Since \(1 \not\in \Pi(S_N)\), \(u_i \neq 1\) for
all \(i \in [t + 1, \ell]\). This, together with (\(\Delta\)), gives that \(u_i \neq 1\) for all \(i \in [1, \ell]\). Let \(A_1 = \{u_1^{r_1i_1}, u_1^{r_1i_2}, \ldots, u_1^{r_1i_t}\}\), \(A_i = \{1, u_i^{r_i}, u_i^{r_i2}, \ldots, u_i^{r_i}\}\) where \(i \in [2, t]\), and \(A_i = \{1, u_i\}\) where \(i \in [t + 1, \ell]\). By Lemma 3.2, we have

\[
|A_i| = \begin{cases} |T_1|, & i = 1; \\ |T_i| + 1, & i \in [2, t]; \\ 2, & i \in [t + 1, \ell]. \end{cases}
\]

Thus

\[
\sum_{i=1}^{\ell} |A_i| = \sum_{i=1}^{t} |T_i| + t - 1 + 2(\ell - t) \\
\geq (|T| - p + 1) + \ell + |S_N| - 1 \quad (\text{as } |S_N| = \ell - t) \\
= |S| + \ell - p \quad (\text{as } |S| = |T| + |S_N|) \\
= m + \ell - 1 \quad (\text{as } |S| = m + p - 1).
\]

Let \(A = (A_1, \ldots, A_\ell)\) and \(M = \text{stab}(\Pi^\ell(A))\). Since \(A_i \subseteq N\) for all \(i \in [1, \ell]\), we have \(\Pi^\ell(A) \subseteq N\) and \(M \subseteq N\). By Lemma 2.1

\[
|\Pi^\ell(A)| \geq |M| \left( 1 - \ell + \sum_{Q \in N/M} \min\{|i \in [1, \ell] : A_i \cap Q \neq \emptyset\} \right) \\
= |M| \left( 1 - \ell + \sum_{Q \in N/M} |\{i \in [1, \ell] : A_i \cap Q \neq \emptyset\}| \right) \\
= |M| \left( 1 - \ell + \sum_{Q \in N/M} \sum_{i \in [1, \ell], A_i \cap Q \neq \emptyset} 1 \right) \\
= |M| \left( 1 - \ell + \sum_{i \in [1, \ell]} \sum_{Q \in N/M, A_i \cap Q \neq \emptyset} 1 \right).
\]

Let \(I_M\) be the subset of \([1, \ell]\) such that \(i \in I_M\) if and only if \(A_i \subseteq M\). Since \(M\) is a cyclic subgroup of \(N\), if \(|I_M| \geq |M|\), then there exists a subset \(\{i_1, \ldots, i_v\} \subseteq I_M\) such that \(1 = u_{i_1} \ldots u_{i_v} \in \pi(T_{i_1} \cdot \ldots \cdot T_{i_v})\), yielding a contradiction. So we may always assume that \(|I_M| \leq |M| - 1\). We now show \(1 \in \Pi^\ell(A)\). Clearly, if \(M = N\), then \(\Pi^\ell(A) = N\) and thus \(1 \in \Pi^\ell(A)\) as desired. We may always assume that \(M \subseteq N\). By Lemma 3.1 (i) and (ii), if any two elements of \(A_i\) are contained in the same coset of \(M\), then \(A_i \subseteq M\) where \(i \in [1, \ell]\); i.e., \(i \in I_M\). This means if \(i \notin I_M\), then all the elements of \(A_i\) are in \(|A_i|\)
different cosets of $M$. Therefore,

$$|\Pi^\ell(A)| \geq |M| \left(1 - \ell + \sum_{i \in I_M} |A_i| + |I_M| \right)$$

$$= |M|(1 - \ell + \sum_{i \in I_M} |A_i|)$$

$$= |M|(1 - \ell + \sum_{i=1}^\ell |A_i| - \sum_{i \in I_M} |A_i| + |I_M|)$$

$$\geq |M|(1 - \ell + \sum_{i=1}^\ell |A_i| - p|I_M|)$$

$$\geq |M|(m - p(|M| - 1))$$

$$= (|M| - 1)(m - p|M|) + m$$

$$\geq m \quad \text{(as } M \leq N, \text{ and thus } m > p|M|).$$

Thus $1 \in N = \Pi^\ell(A)$. Then there exists $u'_i \in A_i$ for each $i \in [1, \ell]$ such that $u'_1 \ldots u'_\ell = 1$. Let $I = \{i \in [1, \ell] : u'_i \neq 1\} = \{i_1, \ldots, i_k\}$, where $1 \leq i_1 < \ldots < i_k \leq \ell$ and $k = |I|$. Then $i_1 = 1 \in I$ and thus $1 = u'_1 \ldots u'_k \in \pi(T_{i_1} \ldots T_{i_k}) \subseteq \Pi(S)$, yielding a contradiction. This completes the proof of the lemma. \hfill $\square$

We are now in a position to prove our main result.

**Proof of Theorem 1.4**

It follows from Proposition 3.3 that $d(G) = m + p - 2$. By [21] Lemma 4, $E(G) \geq |G| + d(G) = pm + m + p - 2$. Let $S$ be a sequence over $G$ with length $pm + m + p - 2$. To prove our result, it is sufficient to show that $1 \in \Pi_{pm}(S)$. We divide the proof into the following two cases.

**Case 1** $|S_{N_i}| \geq p$ for some $i \in [1, p - 1]$.

Then there exists a subsequence $T_0 \mid S_{N_i}$ with $|T_0| = p$. Clearly, $\varphi(T_0)$ is a minimal product-one subsequence over $G/N$. Let $\ell$ be the maximal integer such that

$$T_0 \cdot T_1 \cdot \ldots \cdot T_\ell \mid S,$$

where $\varphi(T_j)$ is a product-one subsequence over $G/N$ with $|T_j| = p$ for every $j \in [1, \ell]$. By rearranging the order of $T_1, T_2, \ldots, T_\ell$ if necessary, we may assume that $\pi(T_j) \neq \{1\}$ for all $j \in [1, v]$ and $\pi(T_j) = \{1\}$ for $j \in [v + 1, \ell]$. Since $G/N \cong C_p$, by the maximality of $\ell$ and Theorem 1.1 we have $|S \cdot (T_0 \cdot T_1 \cdot \ldots \cdot T_\ell)^{-1}| = |\varphi(S)| - |\varphi(T_0 \cdot T_1 \cdot \ldots \cdot T_\ell)| \leq E(G/N) - 1 = 2p - 2$. Therefore, $p\ell = |\varphi(T_0 \cdot T_1 \cdot \ldots \cdot T_\ell)| - p \geq |S| - 2p - 2 - p \geq mp + m - 2p$. By Remark 3.4 $m \equiv 1 \pmod{p}$. Thus $\ell \geq m + (m - 1)p - 1$. Let $1 \neq u_j \in \pi(T_j)$ for all $j \in [1, v]$ and $1 = u_j \in \pi(T_j)$ for $j \in [v + 1, \ell]$. By Lemma 3.3

$$\pi(T_0 \cdot T_1 \cdot \ldots \cdot T_\ell) \supseteq \pi(T_0)\{u_1, u'_1, \ldots, u_1^{p-1}\} \ldots \{u_\ell, u'_\ell, \ldots, u_\ell^{p-1}\}.$$
Let $A_0 = \pi(T_0)$, $A_j = \{u_j, u_j', \ldots, u_j^{p-1}\}$ for $j \in [1, v]$, and $A_j = \{1\}$ for $j \in [v+1, \ell]$. Let $A = (A_1, \ldots, A_\ell)$. Then

$$\Pi_{pm}(S) \supseteq A_0\Pi^{m-1}(A).$$

Let $M = \text{stab}(\Pi^{m-1}(A))$. By Lemma 2.7,

$$|\Pi^{m-1}(A)| \geq |M|(2 - m + \sum_{Q \in N/M} \min \{m - 1, |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}|\}).$$

Let $I_M$ be the subset of $[1, \ell]$ such that $j \in I_M$ if and only if $A_j \subseteq M$. Since $M$ is a cyclic subgroup of $N$, if $|I_M| \geq (m/|M|)|M| + |M| - 1 = m + |M| - 1$, then by using Theorem 1.1 repeatedly for $m/|M|$ times, we can find a subset $\{j_1, \ldots, j_m\} \subseteq I_M$ such that $1 \in \pi(T_{j_1} \cdot \ldots \cdot T_{j_m})$. Since $|T_{j_1} \cdot \ldots \cdot T_{j_m}| = pm$, $1 \in \Pi_{pm}(S)$ and we are done. We only need to consider the case when $|I_M| \leq m + |M| - 2$.

We now show $|\Pi^{m-1}(A)| \geq m$. Note that if $M = N$, then $\Pi^{m-1}(A) = N$ and thus $|\Pi^{m-1}(A)| \geq m$ as desired. We may always assume that $M \subseteq N$. Let $Q \in N/M$ and $V_Q = \{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}$. Clearly, $V_M \supseteq I_M$, and by Lemma 3.1 (i) we have $V_M \subseteq I_M$, whence $V_M = I_M$. Moreover, if $Q \neq M$, then $V_Q \cap V_M = V_Q \cap I_M = \emptyset$. By Lemma 3.1 (ii), if $j \in V_Q$ for $Q \neq M$, then all the elements of $A_j$ are in $p$ different cosets of $M$.

Let

$$\mu = |\{Q \in N/M : |V_Q| \geq m\}|.$$

If $\mu = 0$, then as in the proof of Proposition 3.5 we have

$$|\Pi^{m-1}(A)| \geq |M|(2 - m + \sum_{i \in [1, \ell] \setminus I_M} \sum_{Q \in N/M, A_i \cap Q \neq \emptyset} 1 + \sum_{i \in I_M} \sum_{Q \in N/M, A_i \cap Q \neq \emptyset} 1) \geq |M|(2 - m + p(\ell - |I_M|) + |I_M|) = 2 - m + p\ell - (p - 1)|I_M| \geq 2 - m + (pm + m - p - 1) - (p - 1)(m - 1) \geq m.$$

If $\mu \geq 2$, then

$$|\Pi^{m-1}(A)| \geq |M|(2 - m + 2(m - 1)) \geq m.$$

If $\mu = 1$, then let $R \in N/M$ be the unique coset of $M$ such that $|V_R| \geq m$. Assume that $R \neq M$. Then $R = \alpha M$ for some $\alpha \in N \setminus M$. Let $\alpha_j \in A_j \cap R = A_j \cap \alpha M$ for all $j \in V_R$. Since $\alpha_j \in A_j = \{u_j, u_j', \ldots, u_j^{p-1}\}$, $\alpha_j^* \in A_j$. Thus $\alpha_j^* \in A_j \cap \alpha^* M$ for all $j \in V_R$. Impling that for all $j \in V_R$, $j \in V_{\alpha^* M}$ and thus $|V_{\alpha^* M}| \geq |V_R|$. Since $\alpha \notin M$, by Lemma 3.1 (ii), $\alpha M \neq \alpha^* M$. So we have found another coset $\alpha^* M(\neq R)$ such that $|V_{\alpha^* M}| \geq |V_R| \geq m$, yielding a contradiction to $\mu = 1$. Thus we must have $R = M$. Since
Therefore, \( V_1 \subseteq I(1) \subseteq m - 1 \) and \( V_M = |V_R| \geq m > |V_1| \), we have \( M \neq \{1\} \). By Lemma 2.1

\[
|\Pi^{m-1}(A)| \geq |M| \left( 2 - m + \sum_{Q \in N/M} \min \{m - 1, |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}| \} \right)
\]

\[
= |M| \left( 2 - m + \sum_{Q \in N/M, Q \neq M} |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}| + m - 1 \right)
\]

\[
= |M| \left( 1 + \sum_{Q \in N/M} |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}| - |V_M| \right)
\]

\[
= |M| \left( 1 + \sum_{Q \in N/M} \sum_{j \in [1, \ell], A_j \cap Q \neq \emptyset} 1 - |I_M| \right)
\]

\[
= |M| \left( 1 + \sum_{Q \in N/M, A_j \cap Q \neq \emptyset} 1 - |I_M| \right)
\]

\[
= |M| \left( 1 + \sum_{j \in [1, \ell]} \sum_{I_M \subseteq Q \subseteq N/M, A_j \cap Q \neq \emptyset} 1 + \sum_{j \in I_M, Q \subseteq N/M, A_j \cap Q \neq \emptyset} 1 - |I_M| \right)
\]

\[
= |M| \left( 1 + p(\ell - |I_M|) \right)
\]

\[
\geq |M| \left( pm + m - p - p(m + |M| - 2) \right)
\]

(as \( \ell \geq m + (m - 1)/p - 1 \) and \( |I_M| \leq m + |M| - 2 \))

\[
= |M| \left( m - p(|M| - 1) \right)
\]

\[
= (|M| - 1)(m - p|M|) + m
\]

\[
\geq m \quad \text{(as \( M \leq N \), and thus \( m > p|M| \)).}
\]

So in all the cases, we have shown \( |\Pi^{m-1}(A)| \geq m \). Thus \( 1 \in N = \Pi^{m-1}(A) = A_0 \Pi^{m-1}(A) \subseteq \Pi_{pm}(S) \). This completes the proof of Case 1.

**Case 2** \( |S_{N_i}| < p \) for all \( i \in [1, p - 1] \).

Then \( |S \cdot S_N^{[-1]}| = |S_{N_1} \cdot \ldots \cdot S_{N_{p-1}}| \leq (p - 1)^2 \). Let \( n = v_1(S) \), i.e., the number of times 1 occurs in \( S \). If \( n \geq p + m - 2 \), then let \( S' = S \cdot 1^{-(m + p - 2)} \) be the subsequence of \( S \) obtained by removing \( m + p - 2 \) terms of 1 from \( S \). By Proposition 3.5, \( d(G) = m + p - 2 \). Since \( |S'| = |S| - (m + p - 2) = pm \geq d(G) + 1 \), we can find a product-one subsequence \( T_1 \) of \( S' \). Let \( t \) be the maximal integer such that \( T_1 \cdot \ldots \cdot T_t \mid S' \) and \( T_i \) is product-one for \( i \in [1, t] \). Then \( |S' \cdot (T_1 \cdot \ldots \cdot T_t)^{[-1]}| \leq m + p - 2 \). Hence \( pm - (m + p - 2) \leq d \leq pm \) where \( d = |T_1 \cdot \ldots \cdot T_t| \), and thus \( 0 \leq pm - d \leq m + p - 2 \).

Therefore, \( 1 \in \pi(T_1 \cdot \ldots \cdot T_t) = \pi(T_1 \cdot \ldots \cdot T_t \cdot 1^{[pm-d]}) \). Since \( |T_1 \cdot \ldots \cdot T_t \cdot 1^{[pm-d]}| = pm \), \( 1 \in \Pi_{pm}(S) \). Next we may always assume that \( n \leq p + m - 3 \). Again we divide the rest of the proof of Case 2 into the following two subcases.

**Subcase 2.1** \( p \leq |S \cdot S_N^{[-1]}| \leq (p - 1)^2 \).
Since $d(G/N) = d(C_p) = p - 1$ and $|S \cdot S_N^{[-1]}| \geq p$, we can find a factorization 

$$S \cdot S_N^{[-1]} = W_1 \cdot \ldots \cdot W_k \cdot W'$$

with $k \geq 1$, where $\varphi(W_i)$ is a minimal product-one subsequence over $G/N$ for $i \in [1, k]$ and $\varphi(W')$ is product-one free over $G/N$. Since $d(G/N) = d(C_p) = p - 1$, we have $|W_k| \leq p$ and $|W'| \leq p - 1$. Let $W_k = w_1 \cdot \ldots \cdot w_e$ and $w_e = x^iy^j$, where $e = |W_k|, 1 \leq i \leq p - 1$ and $0 \leq j \leq m - 1$. Let $S_N = u_1 \cdot \ldots \cdot u_t$ such that $u_t \neq 1$ for $t \in [1, \ell - n]$ and $u_t = 1$ for $t \in [\ell - n + 1, \ell]$, where $\ell = |S_N|$. Then

$$pm + m + p - 2 - (p - 1)^2 \leq \ell = |S_N| = |S| - |S \cdot S_N^{[-1]}| \leq pm + m - 2.$$ 

We insert each $u_t$ into the product $w_1 \ldots w_e$, either before or after $w_e$, where $t \in [1, \ell - n]$. If we put $u_t$ after $w_e$ then it multiplies the product by $u_t$; putting it before $w_e$ multiplies the product by $u_t^{-i}$. Therefore, we have

$$\pi(W_k \cdot u_1 \cdot \ldots \cdot u_{\ell - n}) \supseteq (w_1 \ldots w_e)\{u_1, u_1^{r_1}\} \ldots \{u_{\ell - n}, u_{\ell - n}^{r_{\ell - n}}\}.$$ 

Let $A_0 = \{w_1 \ldots w_e\}, A_t = \{u_t, u_t^{r_i}\}$ for $t \in [1, \ell - n]$ and $A_t = \{1\}$ for $t \in [\ell - n + 1, \ell]$. Let $A = (A_1, \ldots, A_\ell), s = pm - |W_1 \cdot \ldots \cdot W_k|$ and $M = \text{stab}(\Pi^*(A))$. Since $pm - (p - 1)^2 \leq pm - |W_1 \cdot \ldots \cdot W_k| = pm - (|S| - \ell - |W'|) \leq \ell - m + 1$, we have

$$m + p - 3 \leq pm - (p - 1)^2 \leq s \leq \ell - m + 1 \leq pm - 1.$$ 

By Lemma 2.1

$$|\Pi^*(A)| \geq |M| \left(1 - s + \sum_{Q \subseteq N/M} \min\{s, |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}|\right).$$

Recall that $I_M$ is the subset of $[1, \ell]$ such that $j \in I_M$ if and only if $A_j \subseteq M$. As before, if $|I_M| \geq pm + |M| - 1$, then there exists a product-one subsequence of $S_M$ with length $pm$ and we are done. We only need to consider the case when $|I_M| \leq \min\{\ell, pm + |M| - 2\}$.

We first prove $|\Pi^*(A)| \geq m$. As before, we may always assume that $M \leq N$. Recall that $V_Q = \{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}$ where $Q \subseteq N/M$. Clearly, $V_Q \supseteq I_M$, and by Lemma 3.1 (i) we have $V_M \subseteq I_M$, so $V_M = I_M$. Moreover, if $Q \neq M$, then $V_Q \cap V_M = V_Q \cap I_M = \emptyset$. By Lemma 3.1 (ii), if $j \in V_Q$ for $Q \neq M$, then the two elements of $A_j$ are in 2 different cosets of $M$. Let

$$\mu = \{|Q \subseteq N/M : |V_Q| \geq s + 1\}|.$$ 

If $\mu = 0$, then as in Case 1, we have

$$|\Pi^*(A)| \geq |M| \left(1 - s + \sum_{i \in [1, \ell]} \sum_{|I_M \cap Q| \neq \emptyset} \sum_{Q \subseteq N/M, A_i \cap Q \neq \emptyset} 1 + \sum_{i \in I_M} \sum_{Q \subseteq N/M, A_i \cap Q \neq \emptyset} 1 \right) \geq |M|(1 - s + 2(\ell - |I_M|)) \geq |M|(1 + 2(\ell - s)) \quad \text{(as } |I_M| = |V_M| \leq s) \geq |M|(1 + 2(m - 1)) \quad \text{(as } s \leq \ell - m + 1) \geq m.$$
If \( \mu \geq 2 \), then

\[
|\Pi^*(A)| \geq |M|(1 - s + 2s) \geq m \quad (\text{as } s \geq m).
\]

If \( \mu = 1 \), then let \( R \in N/M \) be the unique coset of \( M \) such that \( |V_R| \geq s + 1 \). If \( R = M \), then \( V_R = I_M \). Note that since \( |I_{[1]}| \leq m + p - 3 \leq s \), we have \( M = R \neq \{1\} \). Since \( M \leq N \), we have \( |I_M| \leq \min\{\ell, pm + |M| - 2\} = pm + |M| - 2 \). As in Case 1, we have

\[
|\Pi^*(A)| \geq |M| \left(1 + \sum_{j \in [1, \ell] \setminus I_M} \sum_{Q \in N/M, A_j \cap Q \neq \emptyset} 1 + \sum_{j \in I_M} \sum_{Q \in N/M, A_j \cap Q \neq \emptyset} 1 - |I_M|\right)
\]

\[
= |M|(1 + 2(\ell - |I_M|))
\]

\[
\geq |M|(1 + 2((pm + m + p - 2 - (p - 1)^2) - (pm + |M| - 2))
\]

(as \( \ell \geq pm + m + p - 2 - (p - 1)^2 \) and \( |I_M| \leq pm + |M| - 2 \)

\[
= |M|(1 + 2(m + p - (p - 1)^2 - |M|))
\]

\[
= (2|M| - 1)(m - |M| + p - (p - 1)^2) - (p - 1)^2 + p + m
\]

\[
\geq (2p + 1)(p(p + 1) + p - (p - 1)^2) - (p - 1)^2 + p + m
\]

(as \( |M| \geq p + 1 \) and \( m \geq (p + 1)|M| \)

\[
\geq m.
\]

If \( R \neq M \), then \( V_R \cap I_M = \emptyset \), so \( |I_M| + |V_R| \leq \ell \). Therefore, by Lemma 2.1

\[
|\Pi^*(A)| \geq |M| \left(1 - s + \sum_{Q \in N/M} \min\{s, |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}|\right)
\]

\[
= |M| \left(1 - s + \sum_{Q \in N/M, Q \neq R} |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}| + s\right)
\]

\[
= |M| \left(1 + \sum_{Q \in N/M} |\{j \in [1, \ell] : A_j \cap Q \neq \emptyset\}| - |V_R|\right)
\]

\[
= |M| \left(1 + \sum_{Q \in N/M} \sum_{j \in [1, \ell], A_j \cap Q \neq \emptyset} 1 - |V_R|\right)
\]

\[
= |M| \left(1 + \sum_{j \in [1, \ell]} \sum_{Q \in N/M, A_j \cap Q \neq \emptyset} 1 - |V_R|\right)
\]

\[
= |M| \left(1 + 2(\ell - |I_M|) + |I_M| - |V_R|\right)
\]

\[
\geq |M|(\ell + 1) \quad (\text{as } |I_M| + |V_R| \leq \ell)
\]

\[
\geq m \quad (\text{as } s \leq \ell - m + 1).
\]

In all the cases, we have shown \( |\Pi^*(A)| \geq m \), whence \( A_0 \Pi^*(A) = \Pi^*(A) = N \). Hence, we can find a subsequence \( U = u_1 \ldots u_\ell \) with length \( |U| = s \) such that \( 1 \in \pi(W_1 \ldots W_k \cdot U) \).
Since $|W_1 \cdots W_k U| = pm$, we have $1 \in \Pi_{pm}(S)$. This completes the proof of Subcase 2.1.

**Subcase 2.2** $|S \cdot S_N^{[-1]}| \leq p - 1$.

Note that $|S_N| = |S| - |S \cdot S_N^{[-1]}| \geq pm + m + p - 2 - (p - 1) = pm + m - 1$. By using Theorem [1] repeatedly for $p$ times, we can find $p$ disjoint product-one subsequences $T_1, \ldots, T_p$ of $S_N$ with length $|T_j| = m$ for all $j \in [1, p]$. Therefore, $T_1 \cdots T_p$ is a product-one subsequence of $S$ with length $pm$. This completes the proof of Subcase 2.2. □

**Acknowledgements.** This work was carried out during a visit of the first author to Brock University as an international visiting scholar. He would like to sincerely thank the host institution for its hospitality and for providing an excellent atmosphere for research. This work was supported in part by the National Science Foundation of China (No. 11701256, 11871258), the Youth Backbone Teacher Foundation of Henan’s University (No. 2019GGJS196), the China Scholarship Council (Grant No. 201908410132), and it was also supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (Grant No. RGPIN 2017-03903).

**References**

[1] J. Bass, *Improving the Erdős-Ginzburg-Ziv theorem for some non-abelian groups*, J. Number Theory 126 (2007) 217-236.

[2] Y. Caro, *Zero-sum problems - a survey*, Discrete Math. 152 (1996) 93-113.

[3] M. DeVos, L. Goddyn, B. Mohar, *A generalization of Kneser’s Addition Theorem*, Adv. Math. 220 (2009) 1531-1548.

[4] P. Erdős, A. Ginzburg, A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel 10F (1961) 41-43.

[5] W. Gao, *An improvement of Erdős-Ginzburg-Ziv theorem*, Acta Math. Sinica 39 (1996) 514-523.

[6] W. Gao, *A combinatorial problem on finite abelian groups*, J. Number Theory 58 (1996) 100-103.

[7] W. Gao, A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. 24 (2006) 337-369.

[8] W. Gao, Y. Li, *The Erdős-Ginzburg-Ziv theorem for finite solvable groups*, J. Pure Appl. Algebra 214 (2010) 898-909.

[9] W. Gao, Y. Li, J. Peng, *An upper bound for the Davenport constant of finite groups*, J. Pure Appl. Algebra 218 (2014) 1838-1844.

[10] W. Gao, Y. Li, Y. Qu, *On the invariant $E(G)$ for groups of odd order*, Acta Arith., Accepted, May 2021.

[11] W. Gao, Z. Lu, *The Erdős-Ginzburg-Ziv theorem for dihedral groups*, J. Pure Appl. Algebra 212 (2008) 311-319.

[12] A. Geroldinger, D. Grynkiewicz, *The large Davenport constant I: groups with a cyclic, index 2 subgroup*, J. Pure Appl. Algebra 217 (2013) 863-885.

[13] A. Geroldinger, F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[14] A. Geroldinger and I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory, Advanced Courses in Mathematics. CRM Barcelona*, Birkhäuser Verlag, Basel, 2009.

[15] D. Grynkiewicz, *Structural Additive Theory*, Developments in Mathematics 30, Springer, Cham, 2013.
[16] D. Han, The Erdős-Ginzburg-Ziv theorem for finite nilpotent groups, Arch. Math. (Basel) 104 (2015) 325-332.
[17] D. Han, H. Zhang, Erdős-Ginzburg-Ziv theorem and Noether number for $C_m \ltimes \varphi C_{mn}$, J. Number Theory 198 (2019) 159-175.
[18] J. Olson, On a combinatorial problem of Erdős, Ginzburg and Ziv, J. Number Theory 8 (1976) 52-57.
[19] T. Yuster, Bounds for counter-example to an addition theorem in solvable groups, Arch. Math. (Basel) 51 (1988) 223-231.
[20] T. Yuster, B. Peterson, A generalization of an addition theorem for solvable groups, Canad. J. Math. 36 (1984) 529-536.
[21] J. Zhuang, W. Gao, Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index, European J. Combin. 26 (2005) 1053-1059.

Department of Mathematics, Luoyang Normal University, LuoYang 471934, P.R. CHINA
Email address: yongke1239@163.com

Department of Mathematics and Statistics, Brock University, St. Catharines, ON L2S 3A1, Canada
Email address: yli@brock.ca