PRODUCT ONE SUBSEQUENCES OVER SUBGROUPS OF A FINITE GROUP

WEIDONG GAO, YUANLIN LI, CHAO LIU, AND YONGKE QU

Abstract. Let G be a finite group, and let $\mathsf{D}^{(1)}(G)$ be the smallest integer t such that, every sequence S over G with length $|S| \geq t$ has a nonempty subsequence T over a cyclic subgroup of G with the product of all terms in T in some order equaling to one, the identity element of G. In this paper, among other results, we prove that $\mathsf{D}^{(1)}(G) \geq |G|$ holds for all finite groups G and characterize all nilpotent finite groups such that the above equality holds. When G is abelian, we also provide a computation formula of $\mathsf{D}^{(1)}(G)$ involving Möbius function.

1. Introduction

As in recent papers [10], [14] and [15], we write a finite group G multiplicatively. We say that S is a product-one sequence if its terms can be ordered so that their product equals 1, the identity element of the group.

Let G be a multiplicatively written, finite cyclic group and $g \in G$ with $\mathrm{ord}(g) = |G| = n$. For a sequence

$$S = (g^{n_1}) \cdot \ldots \cdot (g^{n_l}) \quad \text{over } G, \quad \text{where } l \in \mathbb{N}_0 \quad \text{and} \quad n_1, \ldots, n_l \in [1, n],$$

we set

$$\|S\|_g = \frac{n_1 + \ldots + n_l}{n},$$

and then denote by

$$\mathrm{ind}(S) = \min\{\|S\|_h \mid h \in G \text{ with } \mathrm{ord}(h) = n\} \in \mathbb{Q}_{\geq 0}$$

the *index* of S. The index of a sequence is a crucial invariant in the investigation of (minimal) product-one sequences (resp. of product-one free sequences) over cyclic groups. It was first addressed by Lemke and Kleitman ([19]), used as key tool by Geroldinger ([13, page 736]), and then investigated by Gao [7] in a systematical way. Since then it has attracted a great deal of attention from researchers in combinatoric and additive number theory and related areas (see, for example, [7, 11, 20, 21, 27]).

2010 *Mathematics Subject Classification.* Primary 20D60; Secondary 11B75.

Key words and phrases. Product-one sequence, maximal cyclic subgroup, cyclic simple group.

A possible way to generalize the concept of index of sequences from cyclic groups to finite groups is as follows. For any finite (not necessarily abelian) group G, we say that a sequence S over G has index 1 if S is a sequence over a cyclic subgroup of G and $\mathrm{ind}(S) = 1$. Let $\mathsf{t}(G)$ be the smallest positive integer ℓ such that, every sequence S over G with length $|S| \geq \ell$ has a subsequence of index 1.

For any positive integer n, let C_n denote the cyclic group of n elements. Lemke and Kleitman made the following conjecture [19].

Conjecture 1.1. *Let p be a prime. Then $\mathsf{t}(C_p) = p$.*

In fact, Lemke and Kleitman conjectured that $\mathsf{t}(C_n) = n$ for all positive integers n, but it was shown recently that $t(C_n) > n$ for infinitely many composite integers n (see [11, 20, 21, 27]). By now we still do not know any good upper bound on $\mathsf{t}(G)$. Note also that Conjecture 1.1 is widely open. Thus, to determine $\mathsf{t}(G)$ for all finite groups seems to be very difficult. Here we will consider a related problem and determine the invariant $\mathsf{D}^{(1)}(G)$, which is defined as the smallest integer t, such that every sequence S over G with length $|S| \geq t$ has a product-one subsequence over a cyclic subgroup of G.

One reason that we consider here all finite groups (instead of restricting on finite abelian groups) is, in recent years, product-one problems (or zero-sum problems) for non-abelian groups have attracted more and more attention (see, for example, [1, 2, 14, 15, 10, 18]). It has been shown that the Davenport constant $\mathsf{D}(G)$ for any finite (not necessarily commutative) group G has some close connection with the Noether number of G, an invariant from the algebraic representation theory. In the history, the investigation on product-one problems can be tracked back to 1960's. The celebrated Erdős-Ginzburg-Ziv theorem was first proved for any finite solvable group by Erdős, Ginzburg and Ziv in [3], and then was generalized to any finite group by Olson in [23]. The Davenport constant of any finite group was first investigated by Olson and White in [24].

In this paper, among other results, we will prove the following main results.

Theorem 1.2. *For every finite group G we have,*

$$\mathsf{D}^{(1)}(G) \geq |G|.$$

Theorem 1.3. *Let G be a finite nilpotent group. Then, $\mathsf{D}^{(1)}(G) = |G|$ if and only if one of the following holds.*

(1) G is cyclic.
(2) G is a p-group of exponent p, where p is a prime.
(3) G is a dihedral 2-group of order at least 8, i.e., $G = D_{2n}$ with $n = 2^s$ for some integer $s \geq 2$.

Theorem 1.4. *Let G be a finite abelian group such that $G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ with $1 < n_1|n_2|\cdots|n_r$. Then,*

$$\mathsf{D}^{(1)}(G) = 1 + \sum_{n|n_r}\sum_{d|n}\sum_{q|n_r} \frac{(n-1)\mu(d)\mu(q)}{\phi(n)} \prod_{i=1}^{r} \left(\frac{n}{d}, \frac{n_i}{(n_i, q)}\right)$$

where $\phi(n)$ is the Euler's totient function, and $\mu(d)$ is the classical Möbius function.

The rest of this paper is organized as follows. Section 2 provides some notations and concepts which will be used in the sequel. Section 3 deals with $\mathsf{D}^{(1)}(G)$ and provides the proofs of Theorem 1.2 and Theorem 1.3. In Section 4 we give a proof for Theorem 1.4. Some related results will be given in the final section.

2. Preliminaries

We adopt the notations and conventions described in detail in [14].

Let G be a finite multiplicative group. The exponent of G is the least common multiple of the orders of all elements of G, denote by $\exp(G)$. Denote by $\langle A\rangle$ the subgroup of G generated by A, where A is a nonempty subset G. Recall that by a sequence over a group G, we mean a finite, unordered sequence where the repetition of elements is allowed. We view sequences over G as elements of the free abelian monoid $\mathcal{F}(G)$ and we denote multiplication in $\mathcal{F}(G)$ by the bold symbol $\boldsymbol{\cdot}$ 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 $S = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$, where $|S| = \ell$ is the *length* of S. For $g \in G$, let

- $\mathsf{v}_g(S) = |\{i \in [1,\ell] : g_i = g\}|$ 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 $\mathsf{v}_g(T) \le \mathsf{v}_g(S)$ for all $g \in G$. Denote by $T^{[-1]} \boldsymbol{\cdot} S$ or $S \boldsymbol{\cdot} T^{[-1]}$ the subsequence of S obtained by removing the terms of T from S.

If $S_1, S_2 \in \mathcal{F}(G)$, then $S_1 \boldsymbol{\cdot} S_2 \in \mathcal{F}(G)$ denotes the sequence satisfying that $\mathsf{v}_g(S_1 \boldsymbol{\cdot} S_2) = \mathsf{v}_g(S_1) + \mathsf{v}_g(S_2)$ for all $g \in G$. For convenience we write

$$g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k} \in \mathcal{F}(G) \quad \text{and} \quad T^{[k]} = \underbrace{T \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} T}_{k} \in \mathcal{F}(G),$$

for $g \in G$, $T \in \mathcal{F}(G)$ and $k \in \mathbb{N}_0$. Let $T^{[-k]} = (T^{[k]})^{[-1]}$.

Suppose $S = g_1 \boldsymbol{\cdot} g_2 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell \in \mathcal{F}(G)$. Let

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

denote the *set of products* of S. Let

$$\Pi(S) = \cup_{1\le i\le \ell} \cup_{T|S,\ |T|=i} \pi(T)$$

denote the *set of all subsequence products* of S. The sequence S is called

- *squarefree* if $\mathsf{v}_g(S) \le 1$ for all $g \in G$;
- *product-one* if $1 \in \pi(S)$;
- *product-one free* if $1 \notin \Pi(S)$;
- *minimal product-one* if $1 \in \pi(S)$ and S cannot be factored into two nonempty, product-one subsequences.

Let $\mathsf{B}(G)$ be the set of all nonempty product-one sequences over G. For any subset $\Omega \subset \mathsf{B}(G)$, let $d_\Omega(G)$ be the smallest integer t such that every sequence S over G with length $|S| \ge t$ has a product-one subsequence in Ω. The invariant $d_\Omega(G)$ was first introduced recently in [12] for abelian groups.

Let $r(G)$ be the smallest integer r such that G can be generated by r elements. For $\Omega = \cup_{H\le G, r(H)\le k}\mathcal{B}(H)$, let $\mathsf{D}^{(k)}(G) = d_\Omega(G)$. Clearly, we have

$$\mathsf{D}^{(1)}(G) \ge \mathsf{D}^{(2)}(G) \ge \cdots \ge \mathsf{D}^{(r)}(G) = \mathsf{D}(G).$$

We need the following well known result ([17, Theorem 5.1.10]).

Lemma 2.1. *Let $n > 1$ be an integer, and let S be a product-one free sequence over C_n with $|S| = n-1$. Then, $S = g^{[n-1]}$ for some generator $g \in C_n$.*

3. On $\mathsf{D}^{(1)}(G) = |G|$

We say that a cyclic subgroup H of G is *a maximal cyclic subgroup* if there is no cyclic subgroup K of G with $H \subsetneq K$. We need the following result.

Theorem 3.1. *Let G be a finite group, and let $H_1, H_2, \cdots, H_m$ be all distinct maximal cyclic subgroups of G. Then,*

$$\mathsf{D}^{(1)}(G) = 1 + \sum_{i=1}^{m}(|H_i| - 1).$$

Furthermore, if S is a sequence over G with length $|S| = \mathsf{D}^{(1)}(G) - 1$ such that S has no nonempty product-one subsequence T with $\langle T\rangle$ being cyclic, then

$$S = g_1^{[|H_1|-1]} \cdot \ldots \cdot g_m^{[|H_m|-1]}$$

where $\langle g_i\rangle = H_i$ for each $i \in [1, m]$.

Proof. For every $g \in G$, the subgroup $\langle g \rangle$ generated by g is contained in some maximal cyclic subgroup of G. It follows that

$$\cup_{i=1}^{m} H_i = G.$$

Let S be an arbitrary sequence over G of length $|S| \geq 1 + \sum_{i=1}^{m}(|H_i| - 1)$. For every subgroup H of G, let S_H denote the subsequence of S consisting of all terms in H. Since $\cup_{i=1}^{m} H_i = G$, we infer that $\sum_{i=1}^{m} |S_{H_i}| \geq |S| \geq 1 + \sum_{i=1}^{m}(|H_i| - 1)$. It follows that $|S_i| \geq |H_k| = \mathsf{D}(H_k)$ for some $k \in [1, m]$. Hence, S_k has a nonempty product-one subsequence over H_k and so does S. This proves that

$$\mathsf{D}^{(1)}(G) \leq 1 + \sum_{i=1}^{m}(|H_i| - 1).$$

To prove $\mathsf{D}^{(1)}(G) \geq 1 + \sum_{i=1}^{m}(|H_i| - 1)$, for every $i \in [1, m]$, take a generator $g_i \in H_i$. Let

$$T = \prod_{i=1}^{m} g_i^{[|H_i|-1]} = \prod_{i=1}^{m} g_i^{[\mathrm{ord}(g_i)-1]}.$$

Clearly, T has no nonempty product-one subsequence with its spanning subgroup being cyclic. This proves the above inequality, completing the proof of the first part of the theorem.

Let S be a sequence over G with $|S| = \mathsf{D}^{(1)}(G) - 1 = \sum_{i=1}^{m}(|H_i| - 1)$. Suppose that S has no nonempty product-one subsequence with its spanning subgroup being cyclic. It follows that S_{H_i} is product-one free for each $i \in [1, m]$. Therefore,

$$|S_{H_i}| \leq |H_i| - 1 \text{ for each } i \in [1, m].$$

It follows from $\sum_{i=1}^{m} |S_{H_i}| \geq |S| = \sum_{i=1}^{m}(|H_i| - 1)$ that

$$|S_{H_i}| = |H_i| - 1 \text{ for each } i \in [1, m].$$

This together with S_{H_i} being product-one free implies that $S_{H_i} = g_i^{[|H_i|-1]}$ for some generator g_i of H_i by Lemma 2.1, completing the proof.

□

Remark 3.2. *We can simplify the formulation on $\mathsf{D}^{(1)}(G)$ in Theorem 1.4 for some special groups. For the groups listed in Theorem 1.3 we have $\mathsf{D}^{(1)}(G) = |G|$. Let p be a prime, and let $G = C_{p^a} \oplus C_{p^b}$ with $1 \leq a \leq b$. From Theorem 1.4, or Theorem 3.1 we can obtain that $\mathsf{D}^{(1)}(G) = 1 + p^{a-1}(p^{b+1} + p^b + pa - pb - p - a + b - 1)$.*

A finite (not necessarily abelian) group G is called cyclic simple if any two maximal cyclic subgroups H and K of G have only the trivial intersection, i.e., $H \cap K = \{1\}$. Our first main result follows from the following theorem.

Theorem 3.3. *Let G be a finite group. Then $\mathsf{D}^{(1)}(G) \geq |G|$. Moreover, the equality $\mathsf{D}^{(1)}(G) = |G|$ holds if and only if G is cyclic simple.*

Proof. Let $H_1, H_2, \cdots, H_k$ be all distinct maximum cyclic subgroups of G. Then

$$H_1 \cup H_2 \cup \ldots \cup H_k = G.$$

It follows from Theorem 3.1 that

$$\begin{aligned} \mathsf{D}^{(1)}(G) &= 1 + |H_1 \backslash \{1\}| + |H_2 \backslash \{1\}| + \ldots + |H_k \backslash \{1\}| \\ &\geq 1 + |H_1 \cup H_2 \cup \ldots \cup H_k \backslash \{1\}|, \end{aligned}$$

so we have

$$\mathsf{D}^{(1)}(G) \geq |G|.$$

Moreover, the above equality holds if and only if $H_i \cap H_j = \{1\}$ for any two distinct $i, j \in [1, k]$, i.e., if and only if G is cyclic simple.

□

Theorem 3.4. *If a finite group G is cyclic simple, then every subgroup H of G is also cyclic simple.*

Proof. Assume to the contrary that H is not cyclic simple. By the definition of a cyclic simple group, there exist two distinct maximal cyclic subgroups H_1 and H_2 of H such that $\{1\} \subsetneq H_1 \cap H_2$. Let K_1 and K_2 be the maximal cyclic subgroups of G which contain H_1 and H_2 respectively. Then $\{1\} \subsetneq H_1 \cap H_2 \subset K_1 \cap K_2$. Since G is cyclic simple, we must have $K_1 = K_2 = K$. Therefore, $H_1 \subset K \cap H$ and $H_2 \subset K \cap H$. By the maximality of H_1 and H_2, we infer that $H_1 = K \cap H = H_2$, a contradiction. Thus H must be cyclic simple, completing the proof. □

Corollary 3.5. *Let G be a finite abelian group. If G is cyclic simple, then either G is cyclic, or G is an elementary abelian p-group for some prime p.*

Proof. Assume to the contrary that, G is neither cyclic nor an elementary abelian p-group. Then, $G = C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$ with $1 < n_1 \mid n_2 \mid \cdots \mid n_r$, $r \geq 2$ and n_r composite. By Theorem 3.4, the subgroup $H = C_{n_1} \times C_{n_r}$ is cyclic simple. Let $x \in C_{n_1}$ with $\mathrm{ord}(x)$ being a prime and let $y \in C_{n_r}$ with $\mathrm{ord}(y) = n_r$. Now the two different cyclic subgroups $\langle y \rangle$ and $\langle xy \rangle$ both have order n_r, the maximal value of the order of a cyclic subgroup of G. Therefore, both $\langle y \rangle$ and $\langle xy \rangle$ are maximal cyclic subgroups of G. But $1 \neq y^{\mathrm{ord}(x)} \in \langle y \rangle \cap \langle xy \rangle$, a contradiction.

□

Corollary 3.6. *Let G be a finite group with non-trivial center $Z(G)$, i.e., $|Z(G)| > 1$. If G is cyclic simple and G has some element of composite order, then*

(1) G has exactly one maximal cyclic subgroup H of composite order.
(2) $Z(G) \subset H$.
(3) H is a normal subgroup of G.

Proof. Let H be a maximal cyclic subgroup of composite order. Take an arbitrary element $x \in Z(G)$. Consider the abelian subgroup $\langle x, H\rangle$ of G, generated by x and H. Clearly, this subgroup is not an elementary abelian p-group for any prime p as H is a cyclic group of composite order. By Corollary 3.5, $\langle x, H\rangle$ is cyclic. Hence, $\langle x, H\rangle = H$ and thus $\langle x\rangle \subset H$. Therefore, $Z(G) \subset H$, proving Conclusion 2, and Conclusion 1 follows from the assumption that G is cyclic simple. It remains to prove H is normal. Let $g \in G$, and let y be an generator of H. Then, $\mathrm{ord}(gyg^{-1}) = \mathrm{ord}(y)$ is composite. Since H is the unique maximal cyclic subgroup of G with composite order $|H|$, it forces that $gyg^{-1} \in H$. This proves that H is normal. □

Lemma 3.7. *Let G be a finite non-cyclic p-group for some prime p. Suppose that G has exponent larger than p. If G is cyclic simple, then $p = 2$ and G is the dihedral 2-group D_{2n} with $n = 2^s$ and $s \geq 2$.*

Proof. It is well know that $|Z(G)| > 1$ as G is a nontrivial p-group. Since G is cyclic simple and has exponent larger than p, by Corollary 3.6 we conclude that G has exactly one maximal cyclic subgroup H with order $|H| > p$, $G \setminus H \neq \emptyset$ and every element in $G \setminus H$ is of order p. Let a be a generator of H and let

$$p^m = \mathrm{ord}(a) = |H|.$$

Take an element $b \in G \setminus H$. Since H is a normal subgroup of G by Corollary 3.6, we have $bab^{-1} \in H$, and thus, $bab^{-1} = a^k$. Now we have

$$b^p = 1, (ba)^p = (ab)^p = 1, \text{ and } ba = a^k b. \tag{3.1}$$

From $ba = a^k b$, we infer that

$$ba^\ell = a^{\ell k} b. \tag{3.2}$$

Since $Z(G) \subset H$ and $|Z(G)| > 1$, we obtain that $a^{p^{m-1}} \in Z(G)$. Therefore, $ba^{p^{m-1}} b^{-1} = a^{p^{m-1}}$. On the other hand, by $bab^{-1} = a^k$, we deduce that $ba^{p^{m-1}} b^{-1} = a^{kp^{m-1}}$. Hence, $a^{p^{m-1}} = a^{kp^{m-1}}$. This implies that

$$p^{m-1} \equiv kp^{m-1} \pmod{p^m}.$$

So, equivalently, we have that

$$k \equiv 1 \pmod{p}. \tag{3.3}$$

By induction on $t \geq 2$ and $ba^\ell = a^{\ell k} b$ we can deduce that

$$(ab)^t = a^{1+k+k^2+\cdots+k^{t-1}} b^t. \tag{3.4}$$

Especially, we have

$$1 = (ab)^p = a^{1+k+k^2+\cdots+k^{p-1}} b^p = a^{1+k+k^2+\cdots+k^{p-1}}.$$

This gives that

$$\frac{k^p - 1}{k - 1} = 1 + k + k^2 + \cdots + k^{p-1} \equiv 0 \pmod{p^m}. \tag{3.5}$$

By (3.3) we know that $k = sp + 1$ for some integer s. This together with (3.5) gives that

$$\frac{\sum_{i=0}^{p-1} \binom{p}{i} (sp)^{p-i}}{sp} \equiv 0 \pmod{p^m}. \tag{3.6}$$

If $p \geq 3$, then the left side of (3.6) is equal to $p^2\alpha + p \not\equiv 0 \pmod{p^m}$ as $m > 1$, where $\alpha = \frac{\sum_{i=0}^{p-2} \binom{p}{i} (sp)^{p-i}}{sp}$ is an integer, giving a contradiction. Thus we must have $p = 2$ and $k = 2s + 1 \equiv -1 \pmod{2^m}$ by (3.6). Therefore,

$$bab^{-1} = a^{-1}.$$

We show next that

$$G = \langle a, b \rangle.$$

Assume to the contrary that, $G \setminus \langle a, b \rangle \neq \emptyset$. Take any $c \in G \setminus \langle a, b \rangle$. As above, we can prove that

$$cac^{-1} = a^{-1}.$$

Therefore,

$$(bc)a(bc)^{-1} = b(cac^{-1})b^{-1} = ba^{-1}b^{-1} = a.$$

So, the subgroup $\langle bc, a \rangle$ generated by bc and a is abelian. By Corollary 3.5 we have that $\langle bc, a \rangle$ is cyclic. Since H is a maximal cyclic subgroup of G, we obtain that $\langle bc, a \rangle = H = \langle a \rangle$. So, $bc \in \langle bc, a \rangle = H \subset \langle b, a \rangle$ giving a contradiction to the choice of $c \in G \setminus \langle a, b \rangle$. This proves that $G = \langle a, b \rangle$, and $G = D_{2n}$ with $n = \frac{|G|}{2} = 2^s$ and $s \geq 2$. □

As a consequence, we obtain the following result.

Theorem 3.8. *If G is a finite cyclic simple group, then for every odd prime divisor p of $|G|$, each Sylow p-subgroup of G is either a p-group of exponent p or a cyclic group. Moreover, if $2 \mid |G|$, then each Sylow 2-subgroup is either an elementary abelian 2-group, or a cyclic group, or a dihedral 2-group of order at least 8.*

We are now ready to provide a proof for the second main result.

Proof of Theorem 1.3. If G is a finite p-group for some prime p, then the result follows from Lemma 3.7. Now assume that $|G|$ has at least two distinct prime divisors. We first assume that the Sylow p-subgroup of G is not cyclic for some prime $p \mid |G|$. Let H be the Sylow p-subgroup of G, and let K be the Sylow q-subgroup of G for a prime $q \mid |G|$ with $q \neq p$. Since G is nilpotent, the group $H \times K$ is a subgroup of G. It follows from Theorem 3.4 that $HK = H \times K$ is cyclic simple.

Take $x \in K$ with $\operatorname{ord}(x)$ being maximal. Since H is not cyclic, we can take two elements a, b in H with $\langle a \rangle$ and $\langle b \rangle$ are two different maximal cyclic subgroups of H. Note that for any $c \in H$ and $z \in K$ we have $cz = zc$ and $\operatorname{ord}(cz) = \operatorname{ord}(c)\operatorname{ord}(z)$. By the maximality of orders of x, a, b, we know that both $\langle ax \rangle$ and $\langle bx \rangle$ are maximal cyclic subgroups of $HK = H \times K$. However, $1 \neq x^{|H|} = (ax)^{|H|} = (bx)^{|H|} \in \langle ax \rangle \cap \langle bx \rangle$, yielding a contradiction to HK being cyclic simple. Thus we must have that for every prime $p \mid |G|$, the Sylow p-subgroup of G is cyclic. Thus G is cyclic and we are done. □

4. Proof of Theorem 1.4

Proof of Theorem 1.4. We say an element $g \in G$ is irreducible if the subgroup $\langle g \rangle$ is a maximal cyclic subgroup of G. For any positive factor d of $n_r = \exp(G)$, let

$$w(d) = |\{g \in G, \operatorname{ord}(g) = d \text{ and } g \text{ is irreducible }\}|.$$

By Theorem 3.1, we have

$$\mathsf{D}^{(1)}(G) = 1 + \sum_{d \mid n_r} \frac{w(d)}{\phi(d)}(d-1). \tag{4.1}$$

For every positive factor n of n_r, let

$$f(n) = |\{g \in G, ng = 0 \text{ and } g \text{ is irreducible }\}|.$$

Then,

$$\sum_{d \mid n} w(d) = f(n).$$

By the Möbius inversion theorem, we obtain that

$$w(n) = \sum_{d \mid n} \mu(d) f(\frac{n}{d}). \tag{4.2}$$

So, it remains to compute $f(n)$. For every factor $q \mid n_r$, let

$$h(n, q) = |\{g \in G, ng = 0, g \in qG\}|.$$

Let

$$n_r = p_1^{u_1} \cdots p_l^{u_l}$$

with $p_1, \cdots, p_l$ being distinct primes.

By the Inclusion-Exclusion Principle we get

$$f(n) = h(n,1) - \sum_{i=1}^{l} h(n, p_i) + \sum_{1\le i<j\le l} h(n, p_i p_j) - \cdots + (-1)^l h(n, p_1 p_2 \cdots p_l).$$

Since $\mu(d) = 0$ if d is not square-free, we obtain that

$$f(n) = \sum_{q \mid n_r} \mu(q) h(n, q). \tag{4.3}$$

Note that

$$qG = C_{\frac{n_1}{(n_1,q)}} \oplus C_{\frac{n_2}{(n_2,q)}} \oplus \cdots \oplus C_{\frac{n_r}{(n_r,q)}}.$$

with $1 \le \frac{n_1}{(n_1,q)} | \frac{n_2}{(n_2,q)} | \cdots | \frac{n_r}{(n_r,q)}$.

Write

$$qG = \langle e_1 \rangle \oplus \langle e_2 \rangle \oplus \cdots \oplus \langle e_r \rangle$$

with $\mathrm{ord}(e_i) = \frac{n_i}{(n_i,q)}$ for every $i \in [1, r]$. An element $g = m_1e_1 + m_2e_2 + \cdots + m_re_r \in qG$ satisfies $ng = 0$ if and only if

$$nm_i \equiv 0 \pmod{\frac{n_i}{(n_i, q)}}$$

for every $i \in [1, r]$.

Note that the number of solutions for the congruence $ax \equiv 0 \pmod{v}$ is (a, v). We infer that $h(n, q) = \prod_{i=1}^{r} \left(n, \frac{n_i}{(n_i,q)}\right)$. Now the desired result follows from (4.1), (4.2) and (4.3).

□

5. Some Related Results

In this section, we present some related results. Let $\mathscr{F}$ be a set of some subgroups of a finite group G and let $\Omega_{\mathscr{F}} = \cup_{H\in\mathscr{F}} B(H)$. We first recall a result from [12].

Lemma 5.1. *(*[12, Proposition 3.1]*) Let G be a finite group, and let $\Omega \subset \mathcal{B}(G)$. Then, $d_\Omega(G) < \infty$ if and only if for every element $g \in G$, $g^{k\,\mathrm{ord}(g)} \in \Omega$ for some positive integer $k = k(g)$.*

We remark that the above lemma was proved only for the case when G is abelian in [12]. However, the same proof works for the general case.

The following result regarding $d_{\Omega_{\mathscr{F}}}$ follows immediately from Lemma 5.1.

Theorem 5.2. *$d_{\Omega_{\mathscr{F}}} < \infty$ if and only if $\cup_{H\in\mathscr{F}} H = G$.*

By the definitions of $\mathsf{t}(G)$ and $\mathsf{D}^{(1)}(G)$, we can easily deduce the following inequality

$$\mathsf{t}(G) \geq \mathsf{D}^{(1)}(G) \tag{5.1}$$

where G is any finite group.

The following proposition presents some special groups for which the equality in (5.1) holds.

Proposition 5.3. *Let G be a finite group. If $\exp(G) \leq 7$ then $\mathsf{t}(G) = \mathsf{D}^{(1)}(G)$.*

Proof. In terms of (5.1), it suffices to prove that $\mathsf{t}(G) \leq \mathsf{D}^{(1)}(G)$. And this follows from the fact that every minimal product-one sequence over C_n with $n \leq 7$ has index 1 and we are done. □

In terms of the proof of Theorem 3.1, we conclude that Conjecture 1.1 is equivalent to the following one.

Conjecture 5.4. *Let G be a finite p-group with $\exp(G) = p$ for some prime p. Then, $\mathsf{t}(G) = |G| = \mathsf{D}^{(1)}(G)$.*

We next compute $\mathsf{D}^{(2)}(G)$ for a finite elementary abelian 2-group G and we have the following main result.

Theorem 5.5. *Let $G = C_2^r$ with $r \geq 1$ be an elementary abelian 2-group. Then we have*

$$\mathsf{D}^{(2)}(G) = 2^{r-1} + 1.$$

Let G be a finite abelian group. For each positive integer $k \geq \exp(G)$, let $\mathsf{s}_{\leq k}(G)$ be the smallest positive integer t such that every sequence S over G of length $|S| \geq t$ has a nonempty product-one subsequence T with $|T| \leq k$. The invariant $\mathsf{s}_{\leq k}(G)$ was studied recently in [22] and [26]. By the definitions of $D^{(k)}(G)$ and $\mathsf{s}_{\leq t}(G)$, we can easily obtain the following result.

Lemma 5.6. *For any finite abelian G and any positive integer $\ell \leq r(G)$, we have*

$$\mathsf{D}^{(\ell)}(G) \leq \mathsf{s}_{\leq \ell+1}(G).$$

Proof. Let S be an arbitrary sequence over G with length $|S| = \mathsf{s}_{\leq \ell+1}(G)$. By the definition of $\mathsf{s}_{\leq \ell+1}(G)$, we obtain that there is a nonempty product-one subsequence T with length $|T| \leq \ell + 1$. Since T is product-one, it follows that $r(\langle T \rangle) \leq |T| - 1 \leq \ell$, completing the proof. □

We need the following well known result (see [17, Theorem 5.5.9] for a proof).

Lemma 5.7. *Let* $G = C_{p^{e_1}} \times C_{p^{e_2}} \times \cdots \times C_{p^{e_r}}$ *be a finite abelian* p*-group for some prime* p*. Then,* $\mathsf{D}(G) = 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$.

We now prove the following main lemma.

Lemma 5.8. *For every positive integer* r *and* $\ell \le r$*, we have*

$$\mathsf{D}^{(\ell)}(C_2^r) = \mathsf{s}_{\le \ell+1}(C_2^r).$$

Proof. By Lemma 5.6, it suffices to prove that $\mathsf{s}_{\le \ell+1}(C_2^r) \le \mathsf{D}^{(\ell)}(C_2^r)$. Let S be a sequence over C_2^r with length $|S| = \mathsf{D}^{(\ell)}(C_2^r)$. We need to prove that S has a nonempty product-one subsequence with length not exceeding $\ell + 1$. By the definition of $\mathsf{D}^{(\ell)}(C_2^r)$, S has a nonempty product-one subsequence T with $r(\langle T \rangle) \le \ell$. By Lemma 5.7 we obtain that $\mathsf{D}(\langle T \rangle) = \mathsf{D}(C_2^{r(\langle T \rangle)}) = r(\langle T \rangle) + 1$, and thus it follows that T has a nonempty product-one subsequence W with length $|W| \le r(\langle T \rangle) + 1 \le \ell + 1$, completing the proof.

□

Proof of Theorem 5.5. By Lemma 5.8, we have that $\mathsf{D}^{(2)}(C_2^r) = \mathsf{s}_{\le 3}(C_2^r)$. Since $\mathsf{s}_{\le 3}(C_2^r) = 2^{r-1} + 1$, (which is a known result (see [5, Theorem 7.2])), we obtain the desired result. □

Remark 5.9. *A subset* A *of* G *is said to be* sum-free *if* $A \cap (A + A) = \emptyset$*. When* $G = C_2^r$, $\mathsf{D}^{(2)}(G) = \mathsf{s}_{\le 3}(G)$ *which is equal to one plus the maximal cardinality of a sum-free subset of* G*. Sum-free sets have been studied since 1960's. It was proved in* [25] *that if* $G = C_p^r$ *for some prime* $p = 3k \pm 1$ *then the maximal cardinality of a sum-free set of* G *is equal to* kp^{r-1}*. In particular, when* $p = 2$*, the above result implies that* $\mathsf{D}^{(2)}(G) = 2^{r-1} + 1$*, which admits a very direct proof.*

Acknowledgements

We would like to thank the referee for his/her very useful suggestion. The research was carried out during a visit by the first author to Brock University as an international visiting scholar. He would like to gratefully thank the host institution for its hospitality and for providing an excellent atmosphere for research.

This research was supported in part by the 973 Program of China (Grant No. 2013CB834204), the PCSIRT Project of the Ministry of Science and Technology, the National Science Foundation of China with grant no.11671218 and grant no.11701256, and was also supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

References

[1] K. Cziszter and M. Domokos, *Groups with large Noether bound* , Ann. Inst. Fourier (Grenoble) **64** (2014) 909-944.

[2] K. Cziszter and M. Domokos, *The Noether number for the groups with a cyclic subgroup of index two* , J. Algebra **399** (2014) 546-560.

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

[4] Y. Fan, W. Gao, L. Wang and Q. Zhong, *Two zero-sum invariants on finite abelian groups*, European J. Combin. **34** (2013) 1331-1337.

[5] M. Freeze and W. Schmid, *Remarks on a generalization of the Davenport constant*, Discrete Math. **310** (2012) 3373-3389.

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

[7] W. Gao, *Zero sums in finite cyclic groups*, Integers **0** (2000), Paper A14, 9 pp.

[8] W. Gao, *On zero-sum subsequences of restricted size. II*, Discrete Math. **271** (2003) 51-59.

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

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

[11] W. Gao, Y. Li, J. Peng, C. Plyley and G. Wang, *On the Index of Sequences over Cyclic Groups*, Acta Arith. **148** (2011) 119-134.

[12] W. Gao, Y. Li, J. Peng and G. Wang, *A unifying look at zero-sum invariants*, International J. Number Theory, Accepted 2017.

[13] A. Geroldinger, *On non-unique factorizations into irreducible elements. II*, Number Theory, Vol. II Budapest 1987, Colloquia Mathematica Societatis Janos Bolyai, vol. 51, North Holland, 1990, pp. 723-757.

[14] A. Geroldinger and D. J. Grynkiewicz, *The Large Davenport Constant I: Groups with a Cyclic, Index 2 Subgroup*, J. Pure and Appl. Algebra. **217** (2013) 863-885.

[15] D.J. Grynkiewicz, *The Large Davenport Constant II: General upper bounds*, J. Pure and Appl. Algebra. **217** (2013) 2221-2246.

[16] A. Geroldinger, D. Grynkiewicz and W. Schmid, *Zero-sum problems with congruence conditions*, Acta Math. Hungarica. **131** (2011) 323-345.

[17] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. vol. 278, Chapman & Hall/CRC, 2006.

[18] D. Han and H. Zhang, *Erdős-Ginzburg-Ziv theorem and Noether number for* $C_m \ltimes_{\varphi} C_{mn}$, arxiv:1707.03639.

[19] P. Lemke and D. Kleitman, *An addition theorem on the integers modulo n*, J. Number Theory **31** (1989) 335- 345.

[20] Y. Li, C. Plyley, P. Yuan, and X. Zeng, *Minimal zero-sum sequences of length four over finite cyclic groups*, J. Number Theory **130** (2010) 2033- 2048.

[21] C. Liu, *On the index-r-free sequences over finite cyclic groups*, International J. Number Theory, **14** (2018) 1627-1636.

[22] A. Plagne and W. Schmid, *An application of coding theory to estimating Davenport constants*, Des. Codes Cryptogr. **61** (2011) 105-118.

[23] J. Olson, *On a combinatorial problem of Erdős, Ginzburg and Ziv*, J. Number Theory **8** (1976) 52-57.

[24] J.E. Olson and E.T. White, *Sums from a sequence of group elements*, Number Theory and Algebra (H. Zassenhaus, ed.), Academic Press, 1977, pp. 215-222.

[25] A. Rhemtulla and A. Street, *Maximal sum-free sets in finite abelian groups*, Bull. Aust. Math. Soc. **2** (1970) 289-297.

[26] C. Wang and K. Zhao, *On zero-sum subsequences of length not exceeding a given number*, J. Number Theory **176** (2017) 365-374.

[27] X. Zeng, P. Yuan, and Y. Li, *On a conjecture of Lemke and Kleitman*, Acta Arith. **168** (2015) 289-299.

Center for Combinatorics, LPMC-TJKLC, Nankai University, Tianjin 300071 P.R. China
E-mail address: wdgao@nankai.edu.cn

Department of Mathematics and Statistics, Brock University, St. Catharines, Ontario, Canada L2S 3A1
E-mail address: yli@brocku.ca

Center for Combinatorics, LPMC-TJKLC, Nankai University, Tianjin 300071 P.R. China
E-mail address: math@chaoliu.science

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