Available online at www.sciencedirect.com
ScienceDirect
Journal of Pure and Applied Algebra 212 (2008) 311–319
JOURNAL OF PURE AND APPLIED ALGEBRA
www.elsevier.com/locate/jpaa

The Erdős–Ginzburg–Ziv theorem for dihedral groups

Weidong Gao*, Zaiping Lu

Center for Combinatorics, Nankai University, Tianjin 300071, PR China

Received 10 January 2007; received in revised form 26 February 2007; accepted 13 April 2007
Available online 23 May 2007

Communicated by J. Walker

Abstract

Let $n \geq 23$ be an integer and let D_{2n} be the dihedral group of order $2n$. It is proved that, if $g_1, g_2, \ldots, g_{3n}$ is a sequence of $3n$ elements in D_{2n}, then there exist $2n$ distinct indices $i_1, i_2, \ldots, i_{2n}$ such that $g_{i_1} g_{i_2} \cdots g_{i_{2n}} = 1$. This result is a sharpening of the famous Erdős–Ginzburg–Ziv theorem for $G = D_{2n}$.

MSC: Primary: 20D60; secondary: 05A15

Let G be a finite group of order n, and let $S = (a_1, \ldots, a_k)$ be a sequence of k elements in G (repetition allowed). We call S *a* 1-*product sequence* if $1 = \prod_{i=1}^{k} a_{\tau(i)}$ holds for some permutation τ of $\{1, \ldots, k\}$. We denote by $\prod(S)$ the product $\prod_{i=1}^{k} a_i$. We call $T = (a_{i_1}, \ldots, a_{i_\ell})$ *a subsequence* of S if $1 \leq i_j \leq k$ for each j and $i_j \neq i_t$ when $j \neq t$. Furthermore, if $1 \leq i_1 < \cdots < i_\ell \leq k$, we call T *a main subsequence* of S. Clearly, every subsequence of S can be reordered to form a unique main subsequence of S. For example, the subsequence (a_2, a_1) of S can be reordered to a main subsequence (a_1, a_2) of S. We denote by I_T the index set $I_T = \{i_1, \ldots, i_\ell\}$ of T and by ST^{-1} the main subsequence obtained by deleting the terms of T from S. If $T_1 = (a_{j_1}, \ldots, a_{j_u})$ and $T_2 = (a_{h_1}, \ldots, a_{h_v})$ are two subsequences of S, we denote by $T_1 \cap T_2$ the main subsequence X of S such that $I_X = I_{T_1} \cap I_{T_2}$. Let $T_2 T_1^{-1}$ be the subsequence obtained by deleting the terms of $T_2 \cap T_1$ from T_2. Furthermore, if T_1 and T_2 are disjoint (i.e. $I_{T_1} \cap I_{T_2} = \emptyset$), we denote by $T_1 T_2$ the sequence $(a_{j_1}, \ldots, a_{j_u}, a_{h_1}, \ldots, a_{h_v})$. For each $\ell \in \{1, \ldots, k\}$, we denote by $\sum_\ell(S)$ the set consisting of all elements which can be expressed as a product of a subsequence T of S with $|T| = \ell$. In particular,

$$\sum_{\ell}(S) = \{a_{i_1} \cdots a_{i_\ell} \mid 1 \leq i_j \leq k \text{ for each } j, \text{ and } i_j \neq i_t \text{ when } j \neq t\}.$$

Set $\sum_{\leq \ell}(S) = \cup_{j=1}^{\ell} \sum_j(S)$ and set $\sum(S) = \cup_{j=1}^{k} \sum_j(S)$. For each $g \in G$, we denote by $v_g(S)$ the number of times that g occurs in S.

Let $D(G)$ be Davenport's constant of G (i.e. the smallest integer d such that every sequence of d elements in G contains a non-empty 1-product subsequence). We denote by $s(G)$ the smallest integer t such that every sequence

* Corresponding author.
E-mail addresses: wdgao1963@yahoo.com.cn (W. Gao), lu@nankai.edu.cn (Z. Lu).

0022-4049/$ - see front matter
doi:10.1016/j.jpaa.2007.04.012

of t elements in G contains a 1-product subsequence of length n. In 1961, Erdős, Ginzburg and Ziv [2] proved that $s(G) \leq 2n-1$ for every finite solvable group G, and this result is well known as the Erdős–Ginzburg–Ziv theorem. In 1976, Olson [8] showed that $s(G) \leq 2n-1$ holds for every finite group G. He also conjectured the following stronger result.

Conjecture 1 ([8]). *If $a_1, \cdots, a_{2n-1}$ is a sequence of $2n-1$ elements in a finite group G of order n, then $1 = a_{i_1} a_{i_2} \cdots a_{i_n}$ for some $1 \leq i_1 < i_2 < \cdots < i_n \leq 2n-1$.*

Olson [8] pointed out that Conjecture 1 is open even for solvable groups.

Let G be a finite non-cyclic solvable group of order n. In 1984, Yuster and Peterson [10] proved that $s(G) \leq 2n-2$; in 1988, with the restriction that $n \geq 600((r-1)!)^2$, Yuster [11] proved that $s(G) \leq 2n-r$; and in 1996, the first author [5] proved that $s(G) \leq \frac{11}{6}n - 1$. For some recent related work, we refer the reader to [6].

For a finite abelian group G of order n, the first author [4] showed that $s(G) = n - 1 + D(G)$. We note that $s(G) \geq n - 1 + D(G)$ for any group G of order n (see [12]). It is plausible to suggest the following.

Conjecture 2 ([12]). *$s(G) = n - 1 + D(G)$ holds for every finite group G of order n.*

Zhuang and the first author [12] proved that the equality in Conjecture 2 is true for $G = D_{2p}$ with prime $p \geq 4001$. If Conjecture 2 were true, then it, together with Lemma 4, would imply that $s(G) \leq 3n/2$ for any non-cyclic group G of order n. In this paper we shall confirm Conjecture 2 for the dihedral group D_{2n} with $n \geq 23$.

Theorem 3. *Let $n \geq 23$ be an integer and let D_{2n} be the dihedral group of order $2n$. Then*

$$s(D_{2n}) = |D_{2n}| - 1 + D(D_{2n}) = 3n.$$

To prove Theorem 3, we need some preliminaries. It is well known that, if G is the cyclic group of order n, then $D(G) = n$. Recently, Dimitrov [1] obtained an upper bound of $D(G)$ for a finite non-abelian p-group G. In 1977, Olson and White [9] obtained the following result for $D(G)$ when G is not cyclic.

Lemma 4 ([9]). *If G is a finite non-cyclic group of order n, then $D(G) \leq \lceil \frac{n+1}{2} \rceil$, where $\lceil x \rceil$ denotes the smallest integer not less than x.*

Lemma 5 ([12]). *If D_{2n} is the dihedral group of order $2n$, then $D(D_{2n}) = n + 1$.*

Lemma 6 ([4]). *Let G be a finite abelian group of order n, and let S be a sequence of n elements in G. Let $k = \max\{v_g(S) | g \in G\}$ be the maximal value of repetition of an element occurring in S. Then $1 \in \sum_{\leq k}(S)$.*

The following technical result is crucial in the proof of Theorem 3.

Lemma 7. *Let G be a finite abelian group of order n and let $r \geq 2$ be an integer. Let S be a sequence of $n + r - 2$ elements in G. If $1 \notin \sum_n(S)$, then $|\sum_{n-2}(S)| = |\sum_r(S)| \geq r - 1$.*

Proof. Since G is abelian and $(n-2) + r = |S|$, we have $|\sum_{n-2}(S)| = |\sum_r(S)|$. So, it suffices to prove that

$$\left| \sum_r (S) \right| \geq r - 1.$$

Set $k = \max\{v_g(S) | g \in G\}$. Let $g \in G$ with $v_g(S) = k$. We multiply every term of S by g^{-1} and denote the resulting sequence by S'. Since G is abelian, we have that

$$g^{-r} \sum_r (S) \stackrel{\text{def}}{=} g^{-r} \left\{ h : h \in \sum_r (S) \right\} = \sum_r (S')$$

and

$$g^{-n} \sum_n (S) \stackrel{\text{def}}{=} g^{-n} \left\{ h : h \in \sum_n (S) \right\} = \sum_n (S').$$

Therefore, $|\sum_r(S)| = |\sum_r(S')|$ and $\sum_n(S) = \sum_n(S')$. Hence, $1 \notin \sum_n(S') = \sum_n(S)$. Then, replacing S by S', we may assume that $g = 1$. Furthermore, by rearranging the subscripts (if necessary), we may assume that

$$S = (g_1, \ldots, g_{n+r-2-k}, \underbrace{1, \ldots, 1}_{k})$$

with $g_i \neq 1$ for every $i \in \{1, \ldots, n+r-2-k\}$.
Set

$$T = (g_1, \ldots, g_{n+r-2-k}).$$

Since $1 \notin \sum_n(S)$, we have $k \leq n-1$. We distinguish two cases:
Case 1. $n-1 \geq k \geq r-1$. Then

$$r - 1 \leq n + r - 2 - k = |T| \leq n - 1.$$

Let W be the maximal (in length) 1-product main subsequence of T (if T contains no 1-product subsequence, then let W be the empty sequence). If $|W| \geq n-k$, then $W(\underbrace{1, \ldots, 1}_{n-|W|})$ is a 1-product subsequence of S with length n, a contradiction. Therefore, $|W| \leq n-k-1$ and $|TW^{-1}| \geq r-1$. By the choice of W we infer that $1 \notin \sum(TW^{-1})$. Let $X = (x_1, \ldots, x_{r-1})$ be any $(r-1)$-term subsequence of TW^{-1}. Then $x_1, x_1x_2, \ldots, x_1x_2\cdots x_{r-1}$ are pairwise distinct. Let $i \in \{1, \ldots, r-1\}$. Since $k \geq r-1$, we infer that $x_1 \cdots x_i = x_1 \cdots x_i 1^{r-i} \in \sum_r(X(\underbrace{1, \ldots, 1}_{k})) \subseteq \sum_r(S)$.
Therefore, $|\sum_r(S)| \geq r-1$.
Case 2. $k \leq r-2$. Then $|T| \geq n$. By using Lemma 6 on T repeatedly, we can find some disjoint 1-product subsequences $T_1, \cdots, T_u$ of T such that $1 \leq |T_i| \leq k$ for every $i \in \{1, \ldots, u\}$, and $|T(T_1 \cdots T_u)^{-1}| \leq n-1$, where $u \geq 1$. Therefore,

$$|T_1| + \cdots + |T_u| = |T| - |T(T_1 \cdots T_u)^{-1}| \geq (n + r - 2 - k) - (n - 1) = r - 1 - k.$$

This gives that

$$|T_1| + \cdots + |T_u| + k \geq r - 1. \tag{1}$$

Let W_0 be the maximal 1-product main subsequence of $T(T_1 \cdots T_u)^{-1}$ (if $T(T_1 \cdots T_u)^{-1}$ contains no 1-product subsequence, then let W_0 be the empty sequence). If $|W_0T_1 \cdots T_u| \geq n-k$, then either $|W_0T_1 \cdots T_u| \leq n-1$ and $W_0T_1 \cdots T_u(\underbrace{1, \ldots, 1}_{n-|W_0T_1\cdots T_u|})$ is a 1-product subsequence of S with length n, which is a contradiction, or

$$|W_0T_1 \cdots T_u| \geq n.$$

For the latter case, since $|W_0| \leq |T(T_1 \cdots T_u)^{-1}| \leq n-1$, there exists $v \in \{0, 1, \ldots, u-1\}$ such that $|W_0T_1 \cdots T_v| \leq n-1$ and $|W_0T_1 \cdots T_vT_{v+1}| \geq n$ (if $v = 0$, then let $W_0T_1 \cdots T_v = W_0$). It follows from $|T_{v+1}| \leq k$ that

$$n - k \leq n - |T_{v+1}| \leq |W_0T_1 \cdots T_v| \leq n - 1.$$

Therefore, $W_0T_1 \cdots T_v(\underbrace{1, \ldots, 1}_{n-|W_0T_1\cdots T_v|})$ is a 1-product subsequence of S of length n, also a contradiction. So, we may assume that

$$|W_0T_1 \cdots T_u| \leq n - k - 1.$$

It follows that

$$|T(T_1 \cdots T_u)^{-1}W_0^{-1}| = |T| - |W_0T_1 \cdots T_u| \geq r - 1.$$

By the choice of W_0 we infer that $1 \notin \sum(T(T_1 \cdots T_u)^{-1}W_0^{-1})$. Let $X = (x_1, \ldots, x_{r-1})$ be any $(r-1)$-term subsequence of $T(T_1 \cdots T_u)^{-1}W_0^{-1}$. Then $x_1, x_1x_2, \ldots, x_1x_2\cdots x_{r-1}$ are pairwise distinct. We show next that

$$\{x_1, x_1x_2, \ldots, x_1x_2\cdots x_{r-1}\} \subseteq \sum_r(X(\underbrace{1, \ldots, 1}_{k})T_1 \cdots T_u) \subseteq \sum_r(S). \tag{2}$$

Let $i \in \{1, \ldots, r-1\}$. If $i \geq r-k$, then

$$x_1 x_2 \cdots x_i \in \sum_r (X(\underbrace{1, \ldots, 1}_{k})) \subseteq \sum_r (X(\underbrace{1, \ldots, 1}_{k}) T_1 \cdots T_u) \subseteq \sum_r (S).$$

Now assume $i \leq r-k-1$. By (1) we have $i \geq 1 \geq r-k-|T_1|-\cdots-|T_u|$, and there is an integer $m \in \{1, \ldots, u\}$ such that

$$i \geq r-k-|T_1|-\cdots-|T_m|$$

and

$$i \leq r-1-k-|T_1|-\cdots-|T_{m-1}| \quad (\text{if } m=1, \text{ then let } |T_1|+\cdots+|T_{m-1}|=0).$$

Therefore,

$$r-k \leq i+|T_1|+\cdots+|T_{m-1}|+|T_m| \leq r-1-k+|T_m| \leq r-1.$$

Thus,

$$\begin{aligned} x_1 x_2 \cdots x_i &= x_1 x_2 \cdots x_i \prod (T_1 \cdots T_m) \in \sum_r (X(\underbrace{1, \ldots, 1}_{k}) T_1 \cdots T_m) \\ &\subseteq \sum_r (X(\underbrace{1, \ldots, 1}_{k}) T_1 \cdots T_u) \subseteq \sum_r (S). \end{aligned}$$

This proves (2) and the lemma follows. □

For every positive integer n, we denote by $\mathbb{Z}_n$ the cyclic group of n elements. Recall that $\mathbb{Z}_n$ (as a group) is written multiplicatively in this paper.

Lemma 8. *Let $n \geq 8$, and let S be a sequence of elements in $\mathbb{Z}_n$ with $|S| \geq 2\lfloor \log_2 n \rfloor$, where $\lfloor x \rfloor$ denotes the largest integer not exceeding x. Then* (1) *there are two disjoint non-empty subsequences S_1 and S_2 of S such that $\prod(S_1) = \prod(S_2)$ and $|S_1| = |S_2| \leq \lfloor \log_2 n \rfloor$; and* (2) *there are two disjoint subsequences C and D of S such that $\prod(C) = \prod(D)$ and $|C| = |D| \geq \frac{|S|-2\lfloor \log_2 n \rfloor+1}{2}$ (for the definition of $\prod(S)$, see the first paragraph of this paper).*

Proof. (1) Let $k = 2\lfloor \log_2 n \rfloor$, and let T be a main subsequence of S with $|T| = k$. We denote by $T^{\lfloor k/2 \rfloor}$ the family that consists of all main subsequences of T of length $\lfloor k/2 \rfloor$. Then

$$|T^{\lfloor k/2 \rfloor}| = \frac{k(k-1)\cdots(\lfloor k/2 \rfloor+1)}{\lfloor k/2 \rfloor} \geq 2^{k/2+1} > n.$$

Therefore, there are two distinct main subsequences T_1 and T_2 of T such that

$$\prod(T_1) = \prod(T_2) \quad \text{and} \quad |T_1| = |T_2| = \lfloor k/2 \rfloor.$$

Setting $S_1 = T_1 T_2^{-1} = T_1(T_1 \cap T_2)^{-1}$ and $S_2 = T_2 T_1^{-1} = T_2(T_1 \cap T_2)^{-1}$, we get the desired result.

(2) By using (1) repeatedly, we can find some disjoint non-empty subsequences

$$U_1, V_1, U_2, V_2, \ldots, U_m, V_m$$

of S such that $\prod(U_i) = \prod(V_i)$ and $|U_i| = |V_i| \leq \lfloor \log_2 n \rfloor$ for every $i \in \{1, 2, \ldots, m\}$, and such that $|S(U_1 V_1 U_2 V_2 \cdots U_m V_m)^{-1}| \leq 2\lfloor \log_2 n \rfloor - 1$. Now set $C = U_1 U_2 \cdots U_m$ and $D = V_1 V_2 \cdots V_m$. Then $\prod(C) = \prod(D)$ and $|C| = |D| \geq \frac{|S|-2\lfloor \log_2 n \rfloor+1}{2}$. □

It is well known that the dihedral group D_{2n} has a unique cyclic subgroup H of order n. Setting $N = G \setminus H$ yields that $N^2 \subseteq H$ and each $x \in N$ has order 2 in D_{2n}. Let S be a sequence of elements in D_{2n}. We denote by $S \cap H$ (respectively $S \cap N$) the main subsequence of S that consists of the terms in H (respectively N). The following lemma will be used repeatedly in the proof of Theorem 3.

Lemma 9. *Let S be a sequence of $3n$ elements in D_{2n}. If one of the following conditions holds, then S contains a 1-product subsequence of length $2n$.*

(I) *There are two disjoint 1-product subsequences T_1 and T_2 of S such that $|T_1| = |T_2| = n$.*

(II) *There are two disjoint subsequences U and V of S satisfying (1) $|U| = |V| \leq n$ and $\prod(U) = \prod(V) \in N$; and (2) $q + w + |U| \geq n$, where q is the maximal non-negative integer such that $(S \cap N)(UV)^{-1}$ has a subsequence of the type $(a_1, a_1) \cdots (a_q, a_q)$, and $w \geq 0$ is the maximal non-negative integer such that $(S \cap H)(UV)^{-1}$ has a subsequence of the type $(b_1, b_1) \cdots (b_w, b_w)$.*

Proof. If (I) holds, then T_1T_2 is a 1-product subsequence of S of length $2n$.

Suppose that (II) holds. If $|U| = |V| = n$, then $|UV| = 2n$ and $\prod(UV) = \prod(U)\prod(V) = 1$.

Assume that $|U| = |V| < n$ and $q + |U| = q + |V| \geq n$. Setting $k = n - |U| = n - |V|$, then $1 \leq k \leq q$ and $UV(a_1, a_1) \cdots (a_k, a_k)$ is a 1-product sequence of length $2n$.

Now, $q + |U| = q + |V| < n$. Setting $\ell = n - |U| - q = n - |V| - q$, then $1 \leq \ell \leq w$ and $U(b_1, \ldots, b_\ell)V(b_1, \ldots, b_\ell)(a_1, a_1) \cdots (a_q, a_q)$ is a 1-product sequence of length $2n$. So the proof is completed. □

The following lemmas will also be used in the proof of Theorem 3.

Lemma 10 (*[7], Lemma 2.2*). *Let A, B be two subsets of a finite group G. If $|A| + |B| > |G|$, then $A + B = G$, where $A + B = \{ab | a \in A, b \in B\}$.*

Lemma 11 (*[3]*). *Let n, u be integers with $2 \leq u \leq \frac{n}{4} + 2$. Let S be a sequence of $2n - u$ elements in $\mathbb{Z}_n$. If $1 \notin \sum_n(S)$, then there are two elements $a, b \in \mathbb{Z}_n$ such that $v_a(S) \geq v_b(S) \geq n - 2u + 3$ and ab^{-1} generates $\mathbb{Z}_n$.*

Proof of Theorem 3. Since $s(D_{2n}) \geq |D_{2n}| + D(D_{2n}) - 1 = 3n$ (the last equality follows from Lemma 4), it suffices to prove that $s(D_{2n}) \leq 3n$. Let $n \geq 3$, and let S be a sequence of $3n$ elements in D_{2n}. We have to prove that S contains a 1-product subsequence of length $2n$. Let H, N, $S \cap N$ and $S \cap H$ be defined as prior to Lemma 9.

It is well known that D_{2n} is generated by two elements x and y with $\operatorname{ord}(x) = 2$, $\operatorname{ord}(y) = n$ and $yx = xy^{-1}$. Then

$$H = \{1 = y^n, y, y^2, \ldots, y^{n-1}\}, \qquad N = \{x, xy, \ldots, xy^{n-1}\}, \quad \text{and} \quad (xy^i)(xy^j) = y^{j-i}$$

holds for any two indices $i, j \in \{0, 1, \ldots, n-1\}$.

By rearranging the subscripts, we may assume that

$$S \cap N = (a_1, a_1)(a_2, a_2) \cdots (a_r, a_r)(c_1, c_2, \ldots, c_u),$$

where $c_1, c_2, \ldots, c_u$ are pairwise distinct, $0 \leq r \leq \frac{|S \cap N|}{2}$ and $2r + u = |S \cap N|$.

Further, assume that

$$S \cap H = (b_1, b_1)(b_2, b_2) \cdots (b_t, b_t)(d_1, d_2, \ldots, d_v),$$

where $d_1, d_2, \ldots, d_v$ are pairwise distinct and $0 \leq t \leq \frac{|S \cap H|}{2}$ with $2t + v = |S \cap H|$.

We shall prove the theorem by showing that at least one of (I) and (II) in Lemma 9 holds for S. Set

$$c_i = xy^{m_i}, \quad i = 1, \ldots, u,$$

where $1 \leq m_i \leq n$. Now we distinguish two cases in terms of whether or not $r = 0$.

Case 1. $r = 0$. Then $|S \cap N| = 2r + u = u \leq n$ and $|S \cap H| \geq 2n$. By the Erdős–Ginzburg–Ziv theorem, $S \cap H$ contains a 1-product subsequence T_1 with $|T_1| = n$. If $u \leq 1$, then

$$|(S \cap H)T_1^{-1}| = |S \cap H| - n = 3n - |S \cap N| - n = 2n - u \geq 2n - 1,$$

and again by using the Erdős–Ginzburg–Ziv theorem we can find a 1-product subsequence T_2 of $(S \cap H)T_1^{-1}$ with $|T_2| = n$ and the theorem follows from Lemma 9(I). Therefore, we may assume that $u \geq 2$. Noting that $c_1c_2, \ldots, c_1c_u$ are pairwise distinct, we have $|\sum_2(c_1, c_2, \ldots, c_u)| \geq u - 1$. We distinguish two subcases.

Subcase 1.1. $|\sum_2(c_1, c_2, \ldots, c_u)| \geq u$. Note that

$$|(S \cap H)T_1^{-1}| = |S \cap H| - n = 3n - |S \cap N| - n = 2n - u.$$

If $1 \in \sum_n((S \cap H)T_1^{-1})$, then the theorem follows from Lemma 9(I) and we are done. Assume that $1 \notin \sum_n((S \cap H)T_1^{-1})$. It follows from Lemma 7 that $|\sum_{n-2}((S \cap H)T_1^{-1})| \geq n - u + 1$, and therefore,

$$\left|\sum_{n-2}(S \cap H)T_1^{-1}\right| + \left|\sum_{2}(c_1, c_2, \ldots, c_u)\right| \geq (n - u + 1) + u > n.$$

It follows from Lemma 10 that

$$1 \in H = \sum_{n-2}((S \cap H)T_1^{-1}) + \sum_{2}(c_1, c_2, \ldots, c_u) \subseteq \sum_{n}(ST_1^{-1}),$$

and thus the theorem follows again from Lemma 9(I).

Subcase 1.2. $|\sum_2(c_1, c_2, \ldots, c_u)| = u - 1$. Then

$$\{c_1c_2, c_1c_3, \ldots, c_1c_u\} = \sum_{2}(c_1, c_2, \ldots, c_u) = \{c_2c_1, c_2c_3, \ldots, c_2c_u\}.$$

By a straightforward calculation, we have

$$\{c_1c_2, c_1c_3, \ldots, c_1c_u\} = \{y^{m_2-m_1}, y^{m_3-m_1}, \ldots, y^{m_u-m_1}\},$$

and

$$\{c_2c_1, c_2c_3, \ldots, c_2c_u\} = \{y^{m_1-m_2}, y^{m_3-m_2}, \ldots, y^{m_u-m_2}\}.$$

Hence,

$$\{y^{m_2-m_1}, y^{m_3-m_1}, \ldots, y^{m_u-m_1}\} = \{y^{m_1-m_2}, y^{m_3-m_2}, \ldots, y^{m_u-m_2}\}.$$

In particular,

$$y^{m_2-m_1}y^{m_3-m_1}\cdots y^{m_u-m_1} = y^{m_1-m_2}y^{m_3-m_2}\cdots y^{m_u-m_2}.$$

Hence,

$$m_2 - m_1 + m_3 - m_1 + \cdots + m_u - m_1 \equiv m_1 - m_2 + m_3 - m_2 + \cdots + m_u - m_2 \pmod{n}.$$

This gives that $u(m_1 - m_2) \equiv 0 \pmod{n}$. Similarly, $u(m_j - m_k) \equiv 0 \pmod{n}$ holds for every pair of j, k with $1 \leq j \neq k \leq u$. Therefore, $y^{m_j-m_k}$ are all in the subgroup M of H with $|M| = \gcd(u, n)$, the greatest common divisor of u and n. Therefore,

$$u \geq \gcd(u, n) = |M| \geq |\{1, y^{m_2-m_1}, y^{m_3-m_1}, \ldots, y^{m_u-m_1}\}| = u.$$

Hence, $|M| = u$, $u|n$ and

$$\begin{aligned}\sum_{2}(c_1, c_2, \ldots, c_u) &= \{y^{m_2-m_1}, y^{m_3-m_1}, \ldots, y^{m_u-m_1}\} = M \setminus \{1\} \\ &= \{y^{\frac{n}{u}}, y^{2\frac{n}{u}}, \ldots, y^{(u-1)\frac{n}{u}}\}.\end{aligned}$$

Thus,

$$\{c_1, c_2, \ldots, c_u\} = \{xy^{m_1}, xy^{m_1+\frac{n}{u}}, xy^{m_1+2\frac{n}{u}}, \ldots, xy^{m_1+(u-1)\frac{n}{u}}\}.$$

Suppose first that $u \geq 7$. Then $u - 1 \geq 6$. We may assume that

$$c_2 = xy^{m_1+2\frac{n}{u}}, \qquad c_3 = xy^{m_1+4\frac{n}{u}}, \qquad c_4 = xy^{m_1+3\frac{n}{u}}, \qquad c_5 = xy^{m_1+6\frac{n}{u}}, \qquad c_6 = xy^{m_1+5\frac{n}{u}}.$$

Then $c_1c_2c_3 = xy^{m_1+2\frac{n}{u}} = c_4c_5c_6$. Set $\ell = \lfloor \frac{u-7}{4} \rfloor$. Let

$$A = (c_1, c_2, c_3, xy^{m_1+7\frac{n}{u}}, \ldots, xy^{m_1+(6+2\ell)\frac{n}{u}})$$

and

$$B = (c_4, c_5, c_6, xy^{m_1+(7+2\ell)\frac{n}{u}}, \ldots, xy^{m_1+(6+4\ell)\frac{n}{u}}).$$

Clearly, A and B are two disjoint subsequences of $S \cap N$ such that $|A| = |B| = 3 + 2\ell$ and $\prod(A) = \prod(B) = xy^{m_1+(2+\ell)\frac{n}{u}} \in N$.

Recall that $S \cap H = (b_1, b_1)\cdots(b_t, b_t)(d_1, \ldots, d_v)$, where $d_1, \ldots, d_v$ are pairwise distinct. Now by Lemma 8 there exist two disjoint subsequences C and D of $(d_1, \ldots, d_v)$ such that $\prod(C) = \prod(D)$ and $|C| = |D| \geq \frac{v-2\lfloor\log_2 n\rfloor+1}{2}$ (if $v \leq 2\lfloor\log_2 n\rfloor - 1$, then let C and D be the empty sequence and $\prod(C) = \prod(D) = 1$). Therefore, $\prod(AC) = \prod(BD) = xh \in N$ and $|AC| = |BD|$, where $h = y^{m_1+(2+\ell)\frac{n}{u}}\prod(C) \in H$. Note That

$$n \geq \frac{u}{2} + \frac{v}{2} > |AC| = |BD| \geq \frac{v - 2\lfloor\log_2 n\rfloor + 1}{2} + 3 + 2\ell$$
$$\geq \frac{v - 2\lfloor\log_2 n\rfloor + 1}{2} + 3 + 2\left(\frac{u-7}{4} - \frac{3}{4}\right) \geq \frac{u + v - 2\lfloor\log_2 n\rfloor - 3}{2}.$$

Therefore,

$$t + |AC| = t + |BD| \geq t + \frac{u + v - 2\lfloor\log_2 n\rfloor - 3}{2} = \frac{2t + u + v - 2\lfloor\log_2 n\rfloor - 3}{2}$$
$$= \frac{3n - 2\lfloor\log_2 n\rfloor - 3}{2} \geq n \quad (\text{since } n \geq 23).$$

Now the theorem follows from Lemma 9(II) with $U = AC$ and $V = BD$. This completes the proof of this subcase with $u \geq 7$.

Next suppose that $2 \leq u \leq 6$. If $1 \in \sum_n((S \cap H)T_1^{-1})$, then the theorem follows from Lemma 9(I). Assume that $1 \notin \sum_n((S \cap H)T_1^{-1})$. Since $|(S \cap H)T_1^{-1}| = 2n - u$ and $2 \leq u \leq 6 \leq \frac{n}{4} + 2$, then, by Lemma 11, $(S \cap H)T_1^{-1}$ has a subsequence $(\underbrace{a, \ldots, a}_{n-2u+3}, \underbrace{b, \ldots, b}_{n-2u+3})$ where ab^{-1} generates H. It follows from $n - 2u + 3 \geq \frac{n}{u} = D(H/M)$ that the sequence $(\underbrace{ab^{-1}, \ldots, ab^{-1}}_{n-2u+3})$ contains a non-empty subsequence T such that $\prod(T) \in M$ and $|T| \leq \frac{n}{u}$. If $k = |T|$, then $a^k b^{-k} = (ab^{-1})^k = \prod(T) \in M$. Note that ab^{-1} generates H and $k < n$; we must have $a^k b^{-k} \neq 1$. So, $a^k b^{-k} \in M \setminus \{1\} = \sum_2(c_1, c_2, \ldots, c_u)$. Without loss of generality, we may assume that $a^k b^{-k} = c_1 c_2$. Therefore,

$$xy^{m_1}a^k = c_1 a^k = c_2 b^k = xy^{m_2}b^k.$$

Again, without loss of generality, we may assume that

$$(S \cap H)(\underbrace{a, \ldots, a}_{k}, \underbrace{b, \ldots, b}_{k})^{-1} = (b_1, b_1)\cdots(b_{t-k}, b_{t-k})(d_1, \ldots, d_v).$$

By Lemma 8 there exist two disjoint subsequences C and D of $(d_1, \ldots, d_{v-1})$ such that

$$\prod(C) = \prod(D) \quad \text{and} \quad \left\lfloor \frac{v-1}{2} \right\rfloor \geq |C| = |D| \geq \frac{v - 1 - 2\lfloor\log_2 n\rfloor + 1}{2}.$$

Therefore,

$$\prod((c_1, \underbrace{a, \ldots, a}_{k})C) = \prod((c_2, \underbrace{b, \ldots, b}_{k})D) = xh,$$

where $h = y^{m_1}a^k\prod(C) = y^{m_2}b^k\prod(D) \in H$ and $|(c_1, \underbrace{a, \ldots, a}_{k})C| = |(c_2, \underbrace{b, \ldots, b}_{k})D|$.

Note that

$$n \geq 1 + \frac{n}{u} + \left\lfloor \frac{v-1}{2} \right\rfloor \geq |(c_1, \underbrace{a, \ldots, a}_{k})C| = |(c_2, \underbrace{b, \ldots, b}_{k})D|$$
$$\geq 1 + k + \frac{v - 1 - 2\lfloor\log_2 n\rfloor + 1}{2} = k + \frac{v - 2\lfloor\log_2 n\rfloor + 2}{2}.$$

Therefore,

$$\begin{aligned} t-k+|(c_1,\underbrace{a,\dots,a}_{k})C| &= t-k+|(c_2,\underbrace{b,\dots,b}_{k})D| \ge t+\frac{v-2\lfloor\log_2 n\rfloor+2}{2} \\ &= \frac{2t+v+u-2\lfloor\log_2 n\rfloor+2-u}{2} = \frac{3n-2\lfloor\log_2 n\rfloor+2-u}{2} \\ &\ge \frac{3n-2\lfloor\log_2 n\rfloor-4}{2} \ge n \quad (\text{since } n\ge 23). \end{aligned}$$

Now the theorem follows again from Lemma 9(II) with $U=(c_1,\underbrace{a,\dots,a}_{k})C$ and $V=(c_2,\underbrace{b,\dots,b}_{k})D$.

Case 2. $r\ge 1$. By Lemma 8 there exist two disjoint subsequences C and D of $(d_1,\dots,d_v)$ such that $\prod(C)=\prod(D)$ and $|C|=|D|\ge \frac{v-2\lfloor\log_2 n\rfloor+1}{2}$. Let $\ell=\lfloor\frac{u-1}{2}\rfloor$. Since

$$\{c_1c_2,c_3c_4,\dots,c_{2\ell-1}c_{2\ell}\}\subseteq H,$$

again by Lemma 8 there exist two disjoint subsequences A' and B' of $(c_1c_2,c_3c_4,\dots,c_{2\ell-1}c_{2\ell})$ such that $\prod(A')=\prod(B')\in H$ and $|A'|=|B'|\ge\frac{\ell-2\lfloor\log_2 n\rfloor+1}{2}$. Therefore, there exist two disjoint subsequences A and B of $(c_1,c_2,\dots,c_{2\ell})$ such that

$$\prod(A)=\prod(A')=\prod(B')=\prod(B)\in H$$

and

$$|A|=|B|=2|A'|=2|B'|\ge \ell-2\lfloor\log_2 n\rfloor+1.$$

Now we have

$$\prod((a_1)AC)=\prod((a_1)BD)=xh\quad\text{for some } h\in H$$

and

$$|(a_1)AC|=|(a_1)BD|=|D|+|B|+1\ge\frac{v-2\lfloor\log_2 n\rfloor+1}{2}+\ell-2\lfloor\log_2 n\rfloor+1+1.$$

Thus,

$$\begin{aligned} n &\ge 1+\left\lfloor\frac{v}{2}\right\rfloor+\left\lfloor\frac{u-1}{2}\right\rfloor\ge|(a_1)AC|=|(a_1)BD|\ge\frac{v-2\lfloor\log_2 n\rfloor+1}{2}+\ell-2\lfloor\log_2 n\rfloor+2 \\ &\ge \frac{v-2\lfloor\log_2 n\rfloor+1}{2}+\frac{u-1}{2}-\frac{1}{2}-2\lfloor\log_2 n\rfloor+2=\frac{u+v-6\lfloor\log_2 n\rfloor+3}{2}. \end{aligned}$$

Therefore,

$$\begin{aligned} r-1+t+|(a_1)AC| &= r-1+t+|(a_1)BD|\ge r-1+t+\frac{u+v-6\lfloor\log_2 n\rfloor+3}{2} \\ &= \frac{2r+2t+u+v-6\lfloor\log_2 n\rfloor+1}{2}=\frac{3n-6\lfloor\log_2 n\rfloor+1}{2} \\ &\ge n\quad(\text{since } n\ge 23). \end{aligned}$$

The theorem now follows from Lemma 9(II) with $U=(a_1)AC$ and $V=(a_1)BD$. □

Acknowledgements

The authors would like to thank the referee and professor Yuanlin Li for several suggestions for preparing the revised version of the manuscript. This work was performed under the auspices of the 973 program with grant no. 2006CB805900, the Ministry of Education, the Ministry of Science and Technology, the National Science Foundation of China, the Foundation of Nankai University, and the Doctoral Program Foundation of Institutions of Higher Education of China.

References

[1] V. Dimitrov, On the strong davenport constant of nonabelian finite p-groups, Math. Balkanica (N.S.) 18 (2004) 129–140.
[2] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel 10F (1961) 41–43.
[3] W.D. Gao, An addition theorem for finite cyclic groups, Discrete Math. 163 (1997) 257–265.
[4] W.D. Gao, A combinatorial problem on finite abelian groups, J. Number Theory 58 (1996) 100–103.
[5] W.D. Gao, An improvement of Erdős–Ginzburg–Ziv theorem, Acta Math. Sinca 39 (1996) 514–523.
[6] Y.O. Hamidoune, D. Quiroz, On subsequence weighted products, Combin. Probab. Comput. 14 (2005) 485–489.
[7] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, 1996.
[8] J.E. Olson, On a combinatorial problem of Erdős, Ginzburg and Ziv, J. Number Theory 8 (1976) 52–57.
[9] J.E. Olson, E.T. White, Sums from a sequences of group elements, in: Number Theory and Algebra, Academic Press, New York, 1977, pp. 215–222.
[10] T. Yuster, B. Peterson, A generalization of an addition theorem for sovable groups, Canad. J. Math. 36 (1984) 529–536.
[11] T. Yuster, Bounds for counter-example to an addition theorem in solvable groups, Arch. Math. (Basel) 51 (1988) 223–231.
[12] J.J. Zhuang, W.D. Gao, Erdős–Ginzburg–Ziv theorem for dihedral groups of large prime index, European J. Combin. 26 (2005) 1053–1059.