THE ERDŐS-GINZBURG-ZIV THEOREM FOR FINITE SOLVABLE GROUPS

WEIDONG GAO AND YUANLIN LI*

Abstract. Let G be a non-cyclic finite solvable group of order n, and let $S = (g_1, \cdots, g_k)$ be a sequence of k elements (repetition allowed) in G. In this paper we prove that if $k \geq \frac{7}{4}n - 1$, then there exist some distinct indices $i_1, i_2, \cdots, i_n$ such that the product $g_{i_1} g_{i_2} \cdots g_{i_n} = 1$. This result substantially improves the Erdős-Ginzburg-Ziv Theorem and other existing results.

1. Introduction and Notations

Let G be a finite group of order n, and let $S = (g_1, \cdots, g_k)$ be a sequence of k elements in G (repetition allowed). We call S *a 1-product sequence* if $1 = \prod_{i=1}^{k} g_{\tau(i)}$ holds for some permutation τ of $\{1, \cdots, k\}$. We denote by $\prod(S)$ the product $\prod_{i=1}^{k} g_i$. We call $T = (g_{i_1}, \cdots, g_{i_\ell})$ *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 (g_2, g_1) of S can be reordered to a main subsequence (g_1, g_2) of S. We denote by I_T the index set $I_T = \{i_1, \cdots, i_\ell\}$ of T. If $T_1 = (g_{j_1}, \cdots, g_{j_u})$ and $T_2 = (g_{h_1}, \cdots, g_{h_v})$ are two disjoint subsequences of S (i.e., $I_{T_1} \cap I_{T_2} = \emptyset$), we denote by T_1T_2 the sequence $(g_{j_1}, \cdots, g_{j_u}, g_{h_1}, \cdots, g_{h_v})$ and call it the concatenation of T_1 and T_2. Similarly, we can define the concatenation of any finite number of disjointed subsequences of S. For every $g \in G$, let $o(g)$ denote the order of g. Let H be a normal subgroup of G, and let ϕ be the natural homomorphism from G onto G/H. Denote by $\phi(S)$ the sequence $(\phi(g_1), \cdots, \phi(g_k))$ of elements in G/H.

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 nonempty 1-product subsequence). We denote by $s(G)$ the smallest integer t such that every sequence of t elements in G contains a 1-product subsequence of length n. In 1961, Erdős, Ginzburg and Ziv [4] 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 [13] showed that $s(G) \leq 2n - 1$ holds for every finite group G. Davenport's constant and the Erdős-Ginzburg-Ziv Theorem have received a greater amount of attention in the recent twenty years, and more information regarding these topics can be found in [7, 8, 12, 18] and their references.

For a finite abelian group G of order n, the first author [5] 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 [21]). It is plausible to suggest the following.

Conjecture 1. [21] *$s(G) = n - 1 + D(G)$ holds for every finite group G of order n.*

2000 *Mathematics Subject Classification.* Primary 20D60; Secondary 11B75. Key Words: Erdos-Ginzburg-Ziv Theorem; Finite solvable groups; 1-product sequences; Davenport constant.

*Corresponding author: Yuanlin Li, Department of Mathematics, Brock University, St. Catharines, Ontario Canada L2S 3A1. E-mail addresses: yli@brocku.ca (Y. Li),

April 3, 2009.

Recently, this conjecture has been verified for Dihedral groups, dicyclic groups and all non-cyclic groups of order pq with p and q primes ([1], [9]).

Let G be a finite non-cyclic solvable group of order n. In 1984, Yuster and Peterson [19] proved that $s(G) \leq 2n-2$. In 1988, Yuster [20] proved that $s(G) \leq 2n-r$ with the restriction that $n \geq 600((r-1)!)^2$, and in 1996, the first author [6] proved that $s(G) \leq \frac{11}{6}n-1$. For some related recent work, we refer the reader to [11]. In this paper, using some new techniques we are able to provide a much better upper bound for $s(G)$, and our main result is the following.

Theorem 2. *If G is a non-cyclic solvable group of order n, then $s(G) \leq \frac{7}{4}n-1$.*

Conjecture 3. *The best upper bound for $s(G)$ is $\frac{3}{2}n$.*

2. Preliminaries

In order to prove Theorem 2, we need some preliminaries.

Lemma 4. [13] *If G is a finite group of order n, then $s(G) \leq 2n-1$.*

Lemma 5. [6] *Let $c \in (1,2]$ be a constant. Let H be a normal subgroup of a finite group G. If $s(H) \leq c|H|-1$, then $s(G) \leq c|G|-1$.*

Since the original proof of Lemma 5 in [6] was written in Chinese, we include a simplified English version of the proof here for the convenience of the reader.

Proof. Let $s = \lfloor c|G|-1 \rfloor$, and let $t = \lfloor c|H|-1 \rfloor$, where for any real number x, $\lfloor x \rfloor$ denotes the largest integer not exceeding x . Let $S = (g_1, \cdots, g_s)$ be any sequence of s elements in G. We want to prove that S contains a nonempty 1-product subsequence of length n.

Let ϕ be the natural homomorphism from G onto G/H and let $f = |G/H|$.

Note that

$$s-(t-1)f = \lfloor c|G| \rfloor - 1 - (\lfloor c|H|-2 \rfloor)f = 2f-1+\lfloor c|G| \rfloor - \lfloor c|H| \rfloor \frac{|G|}{|H|} \geq 2f-1.$$

By applying Lemma 4 repeatedly to the sequence $\phi(S) = (\phi(g_1), \cdots, \phi(g_s))$ of elements in G/H, we can find t disjoint subsequences $S_1, \cdots, S_t$ of S such that

$$\prod(\phi(S_j)) = 1 \text{ and } |S_j| = f$$

for every $j \in \{1, \cdots, t\}$. Thus,

$$\prod(S_j) \in H$$

for every $j \in \{1, \cdots, t\}$.

Since $s(H) \leq c|H|-1$, we have $s(H) \leq \lfloor c|H|-1 \rfloor = t$. Hence, we can find $|H|$ distinct indices $\ell_1, \cdots, \ell_{|H|}$ such that the product

$$\prod_{j=1}^{|H|} \prod(S_{\ell_j}) = 1.$$

Therefore, T contains a 1-product subsequence of length n, namely, the concatenation $S_{\ell_1}S_{\ell_2}\cdots S_{\ell_{|H|}}$. □

Recall that A group is said to be supersolvable if it has a normal cyclic series (i.e., a series of normal subgroups whose factors are cyclic).

The following lemma follows from [10, Corollary 10.5.2].

Lemma 6. *Let G be a finite supersolvable group and p the smallest prime divisor of $|G|$. Then there exists a normal subgroup H of index p.*

Lemma 7. [2] *Let S be a sequence of elements in a cyclic group C_n of order n such that $|S| \geq \frac{n+1}{2}$. If S contains no nonempty 1-product subsequence, then there is an element such that it occurs at least $2|S| - n + 1$ times in S.*

If an element a occurs t times in a sequence S, we call t the multiplicity of a in S. The sum of multiplicities of a and b in S is referred as to the combined multiplicity of a and b in S.

Lemma 8. *Let k be an integer satisfying $n/2 < k < n$, and let S be a sequence of $n+k-1$ elements in C_n. If S contains no 1-product subsequence of length n, then there exist two distinct elements a and b in S such that the combined multiplicity of a and b in S is at least $2k$. Furthermore, if $k \geq 2n/3$, then ab^{-1} generates C_n.*

Proof. The first part of the lemma was proved in [16]. It remains to prove that ab^{-1} generates C_n when $k \geq 2n/3$.

Assume to the contrary that $k \geq 2n/3$, but ab^{-1} does not generate C_n. Let l be the order of ab^{-1}. Then $l|n$ and $l \leq \frac{n}{2}$. We will show that the subsequence

$$T = (\underbrace{a, \cdots, a}_{k}, \underbrace{b, \cdots, b}_{k})$$

contains a 1-product subsequence of length n, and so does S, which yields a contradiction.

Multiplying every term of T by b^{-1}, we get a new sequence

$$T' = (\underbrace{ab^{-1}, \cdots, ab^{-1}}_{k}, \underbrace{1, \cdots, 1}_{k}).$$

It suffices to prove that T' contains a 1-product subsequence of length n. If $l = \frac{n}{2} < k$, then

$$(\underbrace{ab^{-1}, \cdots, ab^{-1}}_{l}, \underbrace{1, \cdots, 1}_{l})$$

is a 1-product subsequence of T' of length n. Next assume that $l < \frac{n}{2}$, so $l \leq \frac{n}{3}$. It is not hard to check that $n - l\lfloor \frac{k}{l} \rfloor \leq k$, and therefore, the following sequence

$$(\underbrace{ab^{-1}, \cdots, ab^{-1}}_{l\lfloor \frac{k}{l} \rfloor}, \underbrace{1, \cdots, 1}_{n-l\lfloor \frac{k}{l} \rfloor})$$

is a 1-product subsequence of T' of length n. This completes the proof. □

We use the following generators and relations for the dihedral group D_{2m} of order $2m$ and the dicyclic group Q_{4m} of order $4m$ respectively.

$$D_{2m} = \langle a, b | a^2 = b^m = 1, ba = ab^{-1} \rangle,$$

and

$$Q_{4m} = \langle x, y | x^2 = y^m, y^{2m} = 1, yx = xy^{-1} \rangle.$$

Lemma 9. *The following statements hold.*

(a) *If $G = D_{2m}$ is the dihedral group of order $2m$, then $s(G) = 3m = \frac{3}{2}|G|$.*
(b) *If $G = Q_{4m}$ is the dicyclic group of order $4m$, then $s(G) = 6m = \frac{3}{2}|G|$.*
(c) *If G is a non-abelian group of order pq with p, q primes, then $s(G) = pq + p + q - 2 \leq \frac{3}{2}|G|$.*
(d) *If G is a non-cyclic abelian group of order n, then $s(G) \leq 3n/2$.*
(e) *If G is a finite non-cyclic p-group for some prime p, then $s(G) \leq \frac{7}{4}|G| - 1$.*

Proof. Proofs for parts (a), (b), (c) and (d) can be found in [1, 5, 9]. We will prove only the last statement here.

Let G be a finite non-cyclic p-group of order p^r. We will prove the result by induction on r. Since G is non-cyclic, we have $r \geq 2$. If $r = 2$, then G is abelian, so $s(G) \leq \frac{3}{2}|G| \leq \frac{7}{4}|G| - 1$. Suppose that $s(G) \leq \frac{7}{4}|G| - 1$ holds for $r = \ell \, (\geq 2)$. We want to show that $s(G) \leq \frac{7}{4}|G| - 1$ holds for $r = \ell + 1$. If $p \geq 3$ and $\ell + 1 \geq 3$ or $p = 2$ and $\ell + 1 \geq 4$, then since G is a non-cyclic group of order $p^{\ell+1}$, it follows easily from [17, page 59, (4.4)] (or [15, page 141, 5.3.4]) that G contains a non-cyclic maximal normal subgroup H of order p^ℓ. By the induction assumption, $s(H) \leq \frac{7}{4}|H| - 1$. It follows from Lemma 5 that $s(G) \leq \frac{7}{4}|G| - 1$. It remains to check the case where $\ell + 1 = 3$ and $p = 2$. By (d), we may assume that G is not abelian. Thus, G is either a dihedral group or a dicyclic group. It follows from (a) or (b) that $s(G) = \frac{3}{2}|G| < \frac{7}{4}|G| - 1$. $\square$

3. Main Result

We will prove our main result by using the minimal counterexample method. Throughout this section, we always assume that G is a minimal counterexample (i.e., G is a non-cyclic solvable group of minimal order n such that $s(G) > \frac{7}{4}n - 1$), p is the smallest prime divisor of n, and let $m = \frac{n}{p}$. We will divide our proof into a series of Lemmas.

Lemma 10. *Let G be the minimal counterexample group of order n. Then every proper normal subgroup of G must be cyclic. Furthermore, G has a cyclic normal subgroup H of order m and index p. If $p = 2$, then $4|m$ and $m \geq 12$. If $p \geq 3$, then $m \geq p(p+2)$.*

Proof. The first statement follows from Lemma 5. Since G is solvable, G has a proper normal subgroup G_0 of prime index and G_0 is cyclic by Lemma 5. Since every subgroup of G_0 is a normal subgroup of G, we conclude that G is supersolvable. By Lemma 6, there exists a normal subgroup H of index p the smallest prime divisor of n, and as mentioned earlier H is cyclic.

As before, let $m = |H| = n/p$. By Lemma 9, we know that m is a composite number and m is not a power of p. If $p \geq 3$, then $m \geq p(p+2)$.

Next, let $p = 2$. If 4 does not divide m, then we claim that G is either a dihedral group if $2 \not| m$, or a dicyclic group if $2|m$. So $s(G) \leq \frac{7}{4}n - 1$ by Lemma 9, which yields a contradiction.

Let $H = \langle a \rangle \lhd G$ and $G = \langle H, b \rangle$, where b is a 2- element in G. We first show that $\langle b \rangle$ is a Sylow 2-subgroup of G. For otherwise, the order $o(b)$ of b must be 2, and any Sylow 2-subgroup of G

must be isomorphic to the 4-group. Thus, the Sylow 2-subgroup H_2 of H is a central subgroup of G, and therefore, $\langle H_2^{'}, b\rangle$ is a proper non-cyclic normal subgroup, contradicting the first statement of the lemma. Here $H_2^{'}$ denotes the complement of H_2 in H. Now, we have $G = \langle H_2^{'}, b\rangle = \langle x, b\rangle$, where $x = a^2$ and $x^b = x^s$. Since b^2 is a central element, we have $s^2 \equiv 1 \pmod{o(x)}$. If $o(x)$ is a prime power, than $s \equiv 1 \pmod{o(x)}$ or $\equiv -1 \pmod{o(x)}$. The former implies that G is abelian, which is impossible. The latter implies that G is a dihedral group or a dicyclic group. Next, assume that $o(x) = p_1^{l_1} \cdots p_k^{l_k}$ is not a prime power, where all $p_j > p$ are all primes for $1 \leq j \leq k$. Let H_{p_j} be the Sylow p_j-subgroup of H and $K_j = \langle H_{p_j}, b\rangle$. If K_j is abelian for some j, then H_{p_j} must be a central subgroup of G, so $\langle H_{p_j}^{'}, b\rangle$ is a proper non-cyclic normal subgroup of G, which yields a contradiction. Thus, as proved earlier, all K_j are either dihedral groups or dicyclic groups. Therefore, G is either a dihedral group or a dicyclic group, proving the claim. Hence,

$$m \geq \begin{cases} p(p+2), & \text{if } p > 2 \\ 12, \text{ and } 4|m & \text{if } p = 2 \end{cases} \tag{1}$$

□

The following notations will be used throughout this section. Let H be the same cyclic normal subgroup of G, of order m as used in the above lemma, $s = \lfloor \frac{7}{4}n - 1\rfloor$ and $t = \lfloor \frac{7}{4}m - 1\rfloor$. Let S be a sequence of s elements in G that contains no 1-product subsequence of length n.

Let ϕ be the natural homomorphism from G onto G/H. Just as in the proof of Lemma 5, applying Lemma 4 repeatedly on the sequence $\phi(S)$ results in a set A consisting of t disjoint subsequences $S_1, \cdots, S_t$ of S such that

(I) each sequence S_j in A is of length p and
(II) $\prod(S_j) \in H$ for each $j \in \{1, \cdots, t\}$.

The above method of finding disjoint subsequences of length p with products in H will also be used in proofs of the next few lemmas.

Let Ω denote the collection of all such $A's$ (i.e., each member of Ω consists of t disjoint subsequences of S and satisfies Conditions (I) and (II) above). Let $A = \{S_j\}_{j=1}^t$ be any member of Ω and $h_j = \prod(S_j) \in H$ for every $j \in \{1, \cdots, t\}$. For every element $h \in H$, we denote by $A(h)$ the multiplicity of h occurring in $h_1, \cdots, h_t$.

Lemma 11. *Let $k = t - m + 1$. Then for each $A \in \Omega$, there exists a unique pair of $x, y \in H$ such that*

$$A(x) + A(y) \geq 2k.$$

Furthermore, xy^{-1} generates H.

Proof. Since the sequence S contains no 1-product subsequence of length n, we infer that the sequence $(h_1, \cdots, h_t)$ in H contains no 1-product subsequence of length m. Note that $t = m+k-1$ and $k = t - m + 1 = \lfloor \frac{7}{4}m\rfloor - m \geq 2m/3$. It follows from Lemma 8 that there exist two distinct elements x, y such that their combined multiplicity in $(h_1, \cdots, h_t)$ is at least $2k$, so

$$A(x) + A(y) \geq 2k.$$

Moreover, xy^{-1} generates H.

Next, we show the uniqueness of such a pair. Assume that there is another pair of two distinct elements u and v in H such that $\{u, v\} \neq \{x, y\}$ and

$$A(u) + A(v) \geq 2k.$$

Without loss of generality, we may assume that $u \notin \{x, y\}$. Since $(h_1, \cdots, h_t)$ contains no 1-product subsequence of length m, $A(v) \leq m - 1$. Therefore, $A(u) \geq 2k - m + 1$ and thus

$$A(u) + A(x) + A(y) \geq 4k - m + 1 = (m + k - 1) + (3k - 2m + 2) > m - k + 1 = t,$$

which yields a contradiction. This proves the lemma. □

Choose $A \in \Omega$ such that the sum $A(x) + A(y)$ attains the minimal possible value, where (x, y) is the unique pair obtained in Lemma 11 corresponding to the given A. Let

$$B = \left\{ S_{i_j} \in A \mid \prod(S_{i_j}) \in \{x, y\} \right\}.$$

Clearly, $f = |B| = A(x) + A(y)$. Let $\prod_{j=1}^{f} S_{i_j}$ denote the concatenation of disjoint subsequences $S_{i_1}, \cdots, S_{i_f}$ of S. We may rearrange this subsequence to form a main subsequence T of S of length $|T| = p|B| = p(A(x) + A(y)) = pf$. In what follows, we will describe the structure of T, and then use it to show that T, and therefore, S, contains a 1-product subsequence of length n. This contradiction will lead to the desired result.

Lemma 12. *If the product of some subsequence of T of length p is in H, then the product of terms of the subsequence in any order is in $\{x, y\}$.*

Proof. Assume to the contrary that there is a subsequence U of T, of length p, such that the product $\prod(U) \in H$, but the product of terms of U in some order does not belong to the set $\{x, y\}$. Note that since $\prod(U) \in H$ and G/H is abelian, the product of terms of U in any order is in H. Without loss generality, we may assume that $\prod(U) \in H \setminus \{x, y\}$. Let

$$C = \left\{ S_{i_j} \in B \mid I_{S_{i_j}} \cap I_U \neq \emptyset \right\}.$$

Thus, $|C| \leq p$. By concatenating the subsequences in C, we get a sequence of length $p|C|$. Deleting U from the resulting sequence, we obtain a sequence W of length $p(|C| - 1)$. Since G/H is abelian, in G/H the image of the product of W in any order under the natural mapping is 1. Thus the product of W in any order is in H. As mentioned earlier, by using Lemma 4 repeatedly on W we can choose $|C| - 2$ disjoint subsequences from W of each length p and each product in H. Deleting these subsequences from W, we get a remaining subsequence of length p with its product in H (because both the product of W and the multiplication of products of first $|C| - 2$ subsequences are in H). In this way, can divide W into $|C| - 1$ disjoint subsequences $W_1, \cdots, W_{|C|-1|}$ with each of length p and each product in H. Now, let A' be a member of Ω as follows:

$$A' = (A \setminus C) \cup \{U, W_1, \cdots, W_{|C|-1}\}.$$

By Lemma 11, there exists a unique pair of elements $x', y' \in H$ such that

$$A'(x') + A'(y') \geq 2k.$$

Let $D = \{U, W_1, \cdots, W_{|C|-1}\}$, and as before, let $D(x)$ (resp. $D(y)$) denote the multiplicity of x (resp. y) occurring in the sequence $(h_0, h_1, \cdots, h_{|C|-1})$, where

$$h_0 = \prod(U), h_1 = \prod(W_1), \cdots, h_{|C|-1} = \prod(W_{|C|-1}).$$

Since $h_0 = \prod(U) \in H \setminus \{x, y\}$, we have $D(x) + D(y) \leq |C| - 1$. Since $A'(x) + A'(y) = A(x) + A(y) - |C| + D(x) + D(y) < A(x) + A(y)$, it follows from the minimality of A that

$$\{x', y'\} \neq \{x, y\}.$$

Without loss of generality, we may assume that $x' \notin \{x, y\}$. Thus

$$A(x') \geq A'(x') - |C| \geq 2k - A'(y') - p \geq 2k - m + 1 - p.$$

It follows that

$$t = m + k - 1 \geq A(x') + A(x) + A(y) \geq 4k - m + 1 - p.$$

Therefore,

$$m + k - 1 \geq 4k - m + 1 - p.$$

This gives that $3k - 2m + 2 \leq p$. Substituting k by $\lfloor \frac{7m}{4} \rfloor - m$ in the last inequality, we obtain that

$$3\lfloor \frac{7m}{4} \rfloor - 5m + 2 \leq p.$$

Hence,

$$3(\frac{7m-3}{4}) - 5m + 2 \leq p.$$

This implies that $m \leq 4p + 1$, which yields a contradiction to (1). □

Lemma 13. *Let $G/H = \{H, bH, \cdots, b^{p-1}H\}$ be the collection of all distinct left cosets of H, and T_i be the main subsequence of T consisting of all terms of T that are in b^iH for each $i \in \{0, 1, \cdots, p-1\}$. If $|T_i| \geq p + 2$ for some $i \in \{0, 1, \cdots, p-1\}$, then T_i can be rearranged in the following way.*

$$\underbrace{\alpha, \cdots, \alpha}_{u}, \underbrace{\beta, \cdots, \beta}_{v},$$

where $\alpha \neq \beta, u \geq v \geq 0$ and $u + v = |T_i|$. Moreover, $v \leq 1$ if $p > 2$.

We remark that the order of terms in T does not affect whether or not T has a 1-product subsequence of length n. Without loss of generality, we may always assume that $T = T_0T_1 \cdots T_{p-1}$.

Proof. If $|T_i| \geq p + 2$, we show that for any three terms in T_i, two of them must be equal. Thus, T_i contains at most two distinct group elements of G, so the first part of the lemma follows.

Choose three arbitrary terms $\gamma_1, \gamma_2, \gamma_3$ from T_i, and then choose $p - 1$ terms $\theta_1, \cdots, \theta_{p-1}$ from the remaining $|T_i| - 3$ terms of T_i. Since all terms of T_i are in the same coset b^iH and $[G : H] = p$, products $\gamma_\ell\theta_1 \cdots \theta_{p-1} \in H$ for all $\ell \in \{1, 2, 3\}$. By Lemma 12, we conclude that at least two of the above products are equal, and thus at least two of γ_1, γ_2, and γ_3 are equal. This completes the proof for the first part.

Next, assume that $p > 2$ and $v \geq 2$. Choose four terms $\alpha, \alpha, \beta, \beta$ from T_i, and then choose any $p - 2$ terms $\delta_1, \cdots, \delta_{p-2}$ from the remaining $|T_i| - 4$ terms of T_i. As before, we conclude that the following products

$$\alpha^2\delta_1 \cdots \delta_{p-2}, \ \alpha\beta\delta_1 \cdots \delta_{p-2}, \ \text{ and } \beta^2\delta_1 \cdots \delta_{p-2}$$

are all in H, and it follows from Lemma 12 again that at least two of $\alpha^2, \alpha\beta$, and β^2 are equal. Since $(|G|, 2) = 1$, this implies that $\alpha = \beta$, which yields a contradiction. □

Lemma 14. *let α and β be two distinct elements of G such that they both appear at least p times in T. If $\alpha \notin H$ and $\beta \notin H$, then $\alpha^p = \beta^p$. If $\alpha \notin H$ and $\beta \in H$, then $\alpha^p \neq \beta^p$. Moreover, $|T_0| \geq p + 2$ and $|T_j| \geq p + 2$ for some $j \in \{1, \cdots, p-1\}$.*

Proof. Applying Lemma 12 on the subsequence $(\alpha, \cdots, \alpha)$ of T, of length p, we conclude that $\alpha^p \in \{x, y\}$. Similarly, we have $\beta^p \in \{x, y\}$. If $\alpha^p \neq \beta^p$, then $\{\alpha^p, \beta^p\} = \{x, y\}$, so by Lemma 11, $\alpha^p(\beta^p)^{-1}$ generates H. Note that α^p commutes with α, and α^p commutes with $\alpha^p(\beta^p)^{-1}$ (since both α^p and β^p are in H). Since α and $\alpha^p(\beta^p)^{-1}$ generate G, we conclude that α^p is a central element. Similarly, we can prove that β^p is also a central element. Therefore, $\alpha^p(\beta^p)^{-1}$ is a central element of G, and thus $G = \langle \alpha, \alpha^p(\beta^p)^{-1} \rangle$ is abelian, which yields a contradiction. So we must have $\alpha^p = \beta^p$.

Next, we prove the second part of the lemma. Assume to the contrary that $\alpha \notin H$ and $\beta \in H$, but $\alpha^p = \beta^p$. We will show that T has a 1-product subsequence of length n, which yields a contradiction. To do so, we distinguish two cases according to if $p = 2$ or not.

Case 1. If $p = 2$, we have $\alpha \in T_1$, $\beta \in T_0$, and $\alpha^2 = \beta^2$. Let w, z be any two elements of G such that they both occur at least twice in T. We first show that $w^2 = z^2$.

If w, z are in the same T_i, as we mentioned earlier in the proof of Lemma 13, at least two of w^2, wz and z^2 are equal, so we must have $w^2 = z^2$.

If w, z are not in the same T_i, without loss generality, we may assume that $w \in T_1$ and $z \in T_0$, Since $w, \alpha \in T_1$ and they both occur at least twice in T, by what we just proved, $w^2 = \alpha^2$. Similarly, we have $z^2 = \beta^2$. Therefore, $w^2 = \alpha^2 = \beta^2 = z^2$.

Since $|T| \geq 4k \geq 7$, there exists an $i \in \{0, 1\}$ such that $|T_i| \geq 4$. If $|T_i| \geq 4$, then by Lemma 13, we can rearrange T_i to the following form

$$\underbrace{\alpha_i, \cdots, \alpha_i}_{u_i}, \underbrace{\beta_i, \cdots, \beta_i}_{v_i},$$

where $\alpha_i \neq \beta_i$, $u_i \geq v_i \geq 0$ and $u_i + v_i = |T_i|$. As we proved earlier, $\alpha_i^2 = \alpha^2$. Moreover, if $v_i \geq 2$, we have $\alpha_i^2 = \beta_i^2 = \alpha^2$.

Note that for each i with $|T_i| \geq 4$, we have

$$2\lfloor \frac{u_i}{2} \rfloor + 2\lfloor \frac{v_i}{2} \rfloor \geq |T_i| - 2.$$

Thus

$$\begin{aligned} \sum_{|T_i| \geq 4} 2(\lfloor \tfrac{u_i}{2} \rfloor + \lfloor \tfrac{v_i}{2} \rfloor) &\geq |T_0| + |T_1| - 3 - 2 \\ &\geq 4k - 5 = 4\lfloor \tfrac{3m}{4} \rfloor - 5 \\ &\geq 3m - 3 - 5 = 2m + m - 8 \\ &> 2m \ \text{(since } m \geq 12). \end{aligned}$$

Hence, for each i such that $|T_i| \geq 4$, there exist $s_i \in \{0, 1, \cdots, \lfloor \frac{u_i}{2} \rfloor\}$ and $t_i \in \{0, 1, \cdots, \lfloor \frac{v_i}{2} \rfloor\}$ such that

$$\sum_{|T_i| \geq 4} 2(s_i + t_i) = 2m.$$

Therefore,

$$\prod_{|T_i| \geq 4} (\alpha_i^2)^{s_i} (\beta_i^2)^{t_i} = (\alpha^2)^m = 1$$

(note that if $v_i \leq 1$, then $t_i = 0$, so such a term $(\beta_i^2)^{t_i}$ can be ignored from the above product). We just showed that T has a 1-product subsequence of length $2m = n$, which yields a contradiction.

Case 2. If $p > 2$, we have $\alpha \notin T_0$, $\beta \in T_0$ and $\alpha^p = \beta^p$. Let w, z be any two elements of G such that they both occur at least p times in T. We remark that w, z cannot occur in the same T_i. Using a similar method to Case 1, we can easily show that $w^p = z^p = \alpha^p$.

If $|T_i| \geq p+2$ for some $i \in \{0, 1, \cdots, p-1\}$, then by Lemma 13, we can rearrange T_i to the following form

$$\underbrace{\alpha_i, \cdots, \alpha_i}_{u_i}, \underbrace{\beta_i, \cdots, \beta_i}_{v_i},$$

where $\alpha_i \neq \beta_i$, $0 \leq v_i \leq 1$ and $u_i + v_i = |T_i|$.

Clearly, $p\lfloor \frac{u_i}{p} \rfloor \geq |T_i| - p$ when $|T_i| \geq p+2$. Since $|T| \geq 2kp > p(p+1)$, $|T_i| \geq p+2$ holds for at least one $i \in \{0, 1, \cdots, p-1\}$. Thus,

$$\begin{aligned} \textstyle\sum_{|T_i| \geq p+2} p\lfloor \frac{u_i}{p} \rfloor &\geq \textstyle\sum_{i=0}^{p-1} |T_i| - p - (p-1)(p+1) \\ &= |T| - p(p+1) + 1 \geq 2kp - p(p+1) + 1 \\ &= 2p(\lfloor \tfrac{3m}{4} \rfloor) - p(p+1) + 1 \geq 2p(\tfrac{3m-3}{4}) - p(p+1) + 1 \\ &= pm + \tfrac{m-3}{2}p - p(p+1) + 1 > pm \ \ (\text{since } m \geq p(p+2)). \end{aligned}$$

Similar to Case 1, for each i with $|T_i| \geq p+2$ we can find $s_i \in \{0, 1, \cdots, \lfloor \frac{u_i}{p} \rfloor\}$ such that

$$\sum_{|T_i| \geq p+2} ps_i = mp.$$

Thus,

$$\prod_{|T_i| \geq p+2} (\alpha_i^p)^{s_i} = (\alpha^p)^m = 1.$$

Again, T has a 1-product subsequence of length $pm = n$, which yields a contradiction. This completes the proof of the second part.

As we proved above, for each i with $|T_i| \geq p+2$, there exist s_i and t_i ($t_i = 0$ when $p > 2$) such that

$$\sum_{|T_i| \geq p+2} (ps_i + pt_i) = mp \ \ (*).$$

If $s_i > 0$ (resp. $t_i > 0$) for some $i > 0$, then we have $\alpha_i^p = \alpha^p$ (resp. $\beta_i^p = \alpha^p$). If $|T_0| \leq p+1$, then

$$\prod_{|T_i| \geq p+2} (\alpha_i^p)^{s_i} (\beta_i^p)^{t_i} = \prod_{|T_i| \geq p+2, i > 0} (\alpha_i^p)^{s_i} (\beta_i^p)^{t_i} = (\alpha^p)^m = 1$$

Thus, T has a 1-product subsequence of length $pm = n$, which yields a contradiction. So, we must have $|T_0| \geq p+2$.

Next, assume that $|T_j| \leq p+1$ for all $j \in \{1, \cdots, p-1\}$. $(*)$ now reduces to $p(s_0 + t_0) = mp = n$. If $t_0 = 0$, then $\alpha_0^{ps_0} = 1$, which yields a contradiction. So, we must have $p = 2$ and $t_0 > 0$. As we proved earlier in Case 1, $\alpha_0^2 = \beta_0^2$, so $(\alpha_0^2)^{s_0}(\beta_0^2)^{t_0} = (\alpha_0^2)^{s_0+t_0} = 1$, which yields a contradiction again. Therefore, $|T_j| \geq p+2$ for some $j \in \{1, \cdots, p-1\}$. □

In the following lemma, we will describe the structure of T in detail.

Lemma 15. *(I) If $p = 2$, then $T = T_0T_1$, and T_0, T_1 can be rearranged as follows:*

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}), T_1 = (\underbrace{\alpha_1, \cdots, \alpha_1}_{u_1}, \underbrace{\alpha_1', \cdots, \alpha_1'}_{v_1}),$$

where $u_i \geq v_i, 0 \leq v_i \leq 1, u_i \geq 2(2k-m)$ for every $i \in \{0, 1\}$, and $\sum_{i=0}^{1}(u_i + v_i) = |T|$.

(II) If $p = 3$, then $T = T_0T_1T_2$. By replacing b with b^2 if necessary, we may assume that $|T_1| \geq |T_2|$. T_0, T_1, T_2 can be rearranged as follows:

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}), T_1 = (\underbrace{\alpha_1, \cdots, \alpha_1}_{u_1}, \underbrace{\alpha_1', \cdots, \alpha_1'}_{v_1}), T_2 = (\underbrace{\alpha_2, \cdots, \alpha_2}_{u_2}),$$

where $u_i \geq v_i, u_i \geq 3(2k-m)-1, 0 \leq v_i \leq 1$ for every $i \in \{0,1\}$, $\sum_{i=0}^{1}(u_i+v_i)+u_2 = |T|$ and $v_0+v_1+u_2 \leq 2$.

(III) If $p \geq 5$, then there is some $j \in \{1, \cdots, p-1\}$ such that $T = T_0T_j$, or $T = T_0T_jT_{p-j}$ with $|T_{p-j}| = 1$, where $T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}), T_j = (\underbrace{\alpha_j, \cdots, \alpha_j}_{u_j}, \underbrace{\alpha_j', \cdots, \alpha_j'}_{v_j})$ with $0 \leq v_0, v_j \leq 1$ and $u_0, u_j \geq p(2k-m)$. Furthermore, if $|T_{p-j}| = 1$ then $v_0 = v_j = 0$.

Proof. By Lemma 14, we have $|T_0| \geq p+2$ and $|T_j| \geq p+2$ holds for some $j \in \{1, \cdots, p-1\}$. It follows from Lemma 13 that there exist $\alpha_0 \in T_0$ and $\alpha_j \in T_j$ such that α_0 and α_j occur at least p times in T_0 and T_j respectively. By Lemma 14, $\alpha_0^p \neq \alpha_j^p$, and thus, it follows from Lemma 12 that $\{\alpha_0^p, \alpha_j^p\} = \{x, y\}$ and $H = \langle \alpha_j^p \alpha_0^{-p} \rangle$.

We first show the following:

$$\alpha_0\beta \neq \beta\alpha_0 \quad \text{for all} \quad \beta \in G \setminus H. \tag{2}$$

Assume to the contrary that α_0 commutes with some element $g \in G \setminus H$. Since g and H generate G, we conclude that α_0 is a central element in G. In particular, α_0 commutes with α_j. Since α_j and $\alpha_j^p\alpha_0^{-p}$ generate G and they commute each other, we conclude that G is abelian, which yields a contradiction. This proves our claim.

(I) Since $p = 2$, we have that $T = T_0T_1$. By Lemma 13, T_0, T_1 can be rearranged as follows:

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}), \ T_1 = (\underbrace{\alpha_1, \cdots, \alpha_1}_{u_1}, \underbrace{\alpha_1', \cdots, \alpha_1'}_{v_1}),$$

where $u_0 \geq v_0, u_1 \geq v_1,$ and $u_0 + v_0 + u_1 + v_1 = |T|$.

We first prove that $0 \leq v_0 \leq 1$ and $0 \leq v_1 \leq 1$. If $v_1 \geq 2$, then by Lemma 12 and Lemma 14

$$\alpha_1\alpha_1' = \alpha_1'\alpha_1 = \alpha_0^2 = x, \ \text{ and } \alpha_1^2 = (\alpha_1')^2 = y, \text{ where } x, y \in H \text{ and } H = \langle xy^{-1} \rangle.$$

Therefore,

$$\alpha_1^2(\alpha_1')^2 = (\alpha_1\alpha_1')^2 = (\alpha_0^2)^2.$$

Hence, $(\alpha_0^2\alpha_1^{-2})^2 = 1$. Since $xy^{-1} = \alpha_0^2\alpha_1^{-2}$ generates H, we have $m = |H| \leq 2$, a contradiction. This proves that $v_1 \leq 1$. Similarly, we can prove that $v_0 \leq 1$.

It remains to show that $u_0,\, u_1 \geq 2(2k-m)$. If $v_0 = 0$ or $v_1 = 0$, then $u_0 + u_1 \geq 4k-1$. If $u_0 \geq 2m$, then $\alpha_0^{2m} = 1$, so T has a 1-product subsequence of length $n = 2m$, which yields a contradiction. Therefore, $u_0 \leq 2m-1$, and hence, $u_1 \geq 4k-1-(2m-1) = 2(2k-m)$. Similarly, we can prove $u_0 \geq 2(2k-m)$.

Now, assume that $v_0 = v_1 = 1$. Then, $u_0 + u_1 \geq 4k-2$. If $u_0 \geq 2m-2$, then $\alpha_0^{2m-2}(\alpha_1\alpha_1') = \alpha_0^{2m-2}\alpha_0^2 = 1$, so again we derive a contradiction. Hence, $u_0 \leq 2m-3$. Now, $u_1 \geq 4k-2-(2m-3) > 2(2k-m)$. Similarly, we can prove $u_0 \geq 4k-2-(2m-3) > 2(2k-m)$.

(II) $p = 3$. By Lemma 13, we have that

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}),\ T_1 = (\underbrace{\alpha_1, \cdots, \alpha_1}_{u_1}, \underbrace{\alpha_1', \cdots, \alpha_1'}_{v_1}),\ T_2 = (\underbrace{\alpha_2, \cdots, \alpha_2}_{u_2}, \underbrace{\alpha_2', \cdots, \alpha_2'}_{v_2}),$$

where $u_i \geq v_i$ and $0 \leq v_i \leq 1$ for every $i \in \{0, 1, 2\}$.

We first show that $v_2 = 0$. Assume to the contrary that $v_2 = 1$. Note that any product of three elements from distinct cosets of H belongs to H. By Lemma 12, we may suppose $\alpha_1\alpha_2\alpha_0 = x$. By (2) and Lemma 12, we have that

$$\alpha_1\alpha_0\alpha_2 = y,\ \alpha_1\alpha_0\alpha_2' = x,\ \alpha_1\alpha_2'\alpha_0 = y.$$

Since $\alpha_1\alpha_0\alpha_2 = y = \alpha_1\alpha_2'\alpha_0$, we obtain that

$$\alpha_0\alpha_2\alpha_0^{-1} = \alpha_2'.$$

Since $\alpha_1\alpha_2\alpha_0 = x = \alpha_1\alpha_0\alpha_2'$, we obtain that

$$\alpha_0^{-1}\alpha_2\alpha_0 = \alpha_2'.$$

Equating the above two equations and simplifying the result, we have

$$\alpha_0^2\alpha_2 = \alpha_2\alpha_0^2. \tag{3}$$

Since the order α_0 is odd, it follows from (3) that $\alpha_0\alpha_2 = \alpha_2\alpha_0$, which yields a contradiction to (2). Thus $v_2 = 0$.

Next we show that $v_0 + v_1 + u_2 \leq 2$. Using the same argument as above, we can easily prove that if $u_2 \geq 1$, then $v_0 = v_1 = 0$.

We now show that $u_2 \leq 2$. Assume to the contrary that $u_2 \geq 3$. We first assert that $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$. If $\alpha_1\alpha_2 = \alpha_2\alpha_1$, then

$$(\alpha_1\alpha_2)^3 = (\alpha_2\alpha_1)^3 = \alpha_1^3\alpha_2^3 = \alpha_1^6 \text{ (by Lemma 14, } \alpha_1^3 = \alpha_2^3). \tag{4}$$

By Lemma 14, $\alpha_1^3 \neq \alpha_0^3$, and then by Lemma 12, $\alpha_1\alpha_2\alpha_0 \in \{\alpha_0^3, \alpha_1^3\}$. If $\alpha_1\alpha_2\alpha_0 = \alpha_0^3$, then $(\alpha_1\alpha_2)^3 = (\alpha_0^2)^3$. This, together with (4), shows that $\alpha_1^6 = \alpha_0^6$. Hence, $(\alpha_1^3\alpha_0^{-3})^2 = 1$. Since $\alpha_1^3\alpha_0^{-3}$ generates H, we have $m = |H| \leq 2$, which yields a contradiction. Next, assume that $\alpha_1\alpha_2\alpha_0 = \alpha_1^3$. Note that α_0 commutes with $\alpha_1\alpha_2$ since both of them are in H. We obtain

$$(\alpha_1\alpha_2)^3\alpha_0^3 = (\alpha_1\alpha_2\alpha_0)^3 = (\alpha_1^3)^3.$$

This, together with (4), implies that $\alpha_0^3 = \alpha_1^3$, which yields a contradiction again. This proves the assertion that $\alpha_1\alpha_2 \neq \alpha_2\alpha_1$.

It follows from Lemma 12 that

$$\{\alpha_1\alpha_2\alpha_0, \alpha_2\alpha_1\alpha_0\} = \{\alpha_0^3, \alpha_1^3\} = \{x, y\}.$$

We may suppose $\alpha_0\alpha_1\alpha_2 = \alpha_0^3$ (the other case where $\alpha_2\alpha_1\alpha_0 = \alpha_0^3$ can be dealt with similarly). Then

$$(\alpha_1\alpha_2)^3 = \alpha_0^6. \tag{5}$$

By (2) and $\alpha_0\alpha_1\alpha_2 = \alpha_0^3$, we infer that $\alpha_1\alpha_0\alpha_2 = \alpha_1^3 = \alpha_2^3$. Therefore,

$$\alpha_1\alpha_0 = \alpha_2^2$$

and

$$\alpha_0\alpha_2 = \alpha_1^2. \tag{6}$$

Hence,

$$(\alpha_1\alpha_0)^3 = \alpha_1^6. \tag{7}$$

If $u_0 \geq 3m-6$, then by (5), we have that $\alpha_0^{3m-6}(\alpha_1\alpha_2)^3 = \alpha_0^{3m} = 1$, so T has a 1-product subsequence of length $n = 3m$, which yields a contradiction. Thus, $u_0 \leq 3m-7$. Note that we have already proved that $v_0 = v_1 = v_2 = 0$ (since $u_2 \geq 1$). Therefore,

$$u_1 + u_2 \geq |T| - (3m-7) \geq 6k - (3m-7) \geq \frac{3m+5}{2}.$$

Now, we can choose $\ell_1 \in \{0, 1, \cdots, \lfloor \frac{u_1}{3} \rfloor\}$ and $\ell_2 \in \{0, 1, \cdots, \lfloor \frac{u_2}{3} \rfloor\}$ so that

$$6\ell_1 + 6\ell_2 = 3m-3.$$

Since $(u_1 - 3\ell_1) + (u_2 - 3\ell_2) \geq \frac{3m+5}{2} - \frac{3m-3}{2} = 4$, we infer that either $u_1 - 3\ell_1 = u_2 - 3\ell_2 = 2$, or $u_1 - 3\ell_1 \geq 3$, or $u_2 - 3\ell_2 \geq 3$. If $u_0 \geq \frac{3m-1}{2}$, then by (6) and (7), at least one of the following equalities holds

$$(\alpha_1\alpha_0)^{3\ell_1}(\alpha_0\alpha_2)^{3\ell_2}(\alpha_0\alpha_2)\alpha_1 = \alpha_1^{3m} = 1,\ (\alpha_1\alpha_0)^{3\ell_1}(\alpha_0\alpha_2)^{3\ell_2}\alpha_1^3 = 1 \text{ and } (\alpha_1\alpha_0)^{3\ell_1}(\alpha_0\alpha_2)^{3\ell_2}\alpha_2^3 = 1.$$

This implies that T contains a 1-product subsequence of length $n = 3m$, which yields a contradiction. So, we must have that $u_0 \leq \frac{3m-1}{2} - 1$. Thus $u_1 + u_2 \geq 6k - u_0 \geq 3m-3$. If $u_1 + u_2 \geq 3m+4$, then $3[\frac{u_1}{3}] + 3[\frac{u_2}{3}] \geq 3m$. Therefore, there exist $f_1 \in \{0, 1, \cdots, \lfloor \frac{u_1}{3} \rfloor\}$ and $f_2 \in \{0, 1, \cdots, \lfloor \frac{u_2}{3} \rfloor\}$ such that $3f_1 + 3f_2 = 3m$. So

$$\alpha_1^{3f_1}\alpha_2^{3f_2} = \alpha_1^{3m} = 1,$$

and then, as before, we derive a contradiction. Therefore, we must have $u_1 + u_2 \leq 3m+3$. It follows that $u_0 \geq 6k - (u_1 + u_2) \geq \frac{3m-15}{2}$. We now have

$$\frac{3m-15}{2} \leq u_0 \leq \frac{3m-3}{2}.$$

and

$$3m-3 \leq u_1 + u_2 \leq 3m+3.$$

Since $|T_1| = u_1 \geq |T_2| = u_2$, we have $u_1 \geq \frac{3m-3}{2} = \frac{3m-15}{2} + 6$. By (7), we have

$$(\alpha_1\alpha_0)^{\frac{3m-15}{2}}\alpha_1^{12}\alpha_2^3 = (\alpha_1\alpha_0)^{\frac{3m-15}{2}}\alpha_1^9\alpha_2^6 = (\alpha_1\alpha_0)^{\frac{3m-15}{2}}\alpha_1^6\alpha_2^9 = \alpha_1^{3m} = 1.$$

As before, we derive a contradiction. So $u_2 \leq 2$, and hence, $v_0 + v_1 + u_2 \leq 2$.

It remains to prove that $u_0, u_1 \geq 3(2k-m)$. To do so, we will use an argument similar to that used in (I) and present only an outline of the proof here. If $u_2 = 0$ and one of v_0 and v_1 is 0, then $u_0 + u_1 \geq 6k-1$. As before, we can prove that $u_0, u_1 \leq 3m-1$, and then $u_0, u_1 \geq 6k-1-(3m-1) = 3(2k-m)$. If $u_2 = 0$ and $v_0 = v_1 = 1$, then $u_0 + u_1 \geq 6k-2$. By Lemma 12, $\{\alpha_1\alpha_1'\alpha_0, \alpha_1\alpha_1'\alpha_0'\} = \{\alpha_0^3, \alpha_1^3\}$. If $u_1 \geq 3m-2$, then either $(\alpha_1\alpha_1'\alpha_0)\alpha_1^{3m-3} = 1$ or $(\alpha_1\alpha_1'\alpha_0')\alpha_1^{3m-3} = 1$ is equal to the product of a subsequence of T of length $n = 3m$, which yields a contradiction. So we must have $u_1 \leq 3m-3$, and thus $u_0 \geq 6k-2-(3m-3) \geq 3(2k-m)$. Similarly, we can prove that $u_0 \leq 3m-3$ and thus $u_1 \geq 3(2k-m)$ as desired.

Next, assume that $u_2 \in \{1, 2\}$. As mentioned earlier, $v_0 = v_1 = 0$. If $u_2 = 1$, then $u_0 + u_1 \geq 6k-1$; if $u_2 = 2$, then $u_0 + u_1 \geq 6k-2$. Using the same argument as above, we can easily show that $u_0, u_1 \geq 3(2k-m)$ as desired.

(III) $p \geq 5$. By Lemma 14 and Lemma 13, we know that $|T_j| \geq p+2$ for some $j \geq 1$ and

$$T_j = (\underbrace{\alpha_j, \cdots, \alpha_j}_{u_j}, \underbrace{\alpha_j', \cdots, \alpha_j'}_{v_j})$$

where $0 \le v_j \le 1$, and

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0})$$

where $0 \le v_0 \le 1$.

We first prove that $|T_i| = 0$ holds for all $i \in \{1, \cdots, p-1\} \setminus \{j, p-j\}$. Assume to the contrary that $|T_i| \ge 1$ holds for some $i \in \{1, \cdots, p-1\} \setminus \{j, p-j\}$. Take any $\alpha_i \in T_i$, and take $(p-1)'s$ α_j from T_j. By letting $n = p$ and $C_p = G/H$ in Lemma 7, we get the following subsequence of T,

$$\alpha_i, \underbrace{\alpha_j, \cdots, \alpha_j}_{p-1},$$

which contains a nonempty subsequence such that its product is in H. Since $i \notin \{j, p-j\}$, such a subsequence is of the form

$$\alpha_i, \underbrace{\alpha_j, \cdots, \alpha_j}_{r},$$

where $2 \le r \le p-2$. Hence,

$$\alpha_0^{p-r-2} \alpha_j^r \alpha_i \alpha_0 \in H.$$

By Lemma 12, $\alpha_0^{p-r-2}\alpha_j^r\alpha_i\alpha_0$, $\alpha_0^{p-r-2}\alpha_j^r\alpha_0\alpha_i$ and $\alpha_0^{p-r-2}\alpha_j^{r-1}\alpha_0\alpha_j\alpha_i$ are all in $\{x, y\}$. By (2), we can show that the middle term is different from the first and the third, so we must have

$$\alpha_0^{p-r-2}\alpha_j^r\alpha_i\alpha_0 = \alpha_0^{p-r-2}\alpha_j^{r-1}\alpha_0\alpha_j\alpha_i.$$

Thus $\alpha_j\alpha_i\alpha_0 = \alpha_0\alpha_j\alpha_i$. This is a contradiction to (2) (since $\alpha_j\alpha_i \notin H$). This proves that $|T_i| = 0$ for all $i \in \{1, \cdots, p-1\} \setminus \{j, p-j\}$.

Next, we prove that $|T_{p-j}| \le 1$. Assume to the contrary that $|T_{p-j}| \ge 2$. Take any two terms $\alpha_{p-j}, \alpha_{p-j}'$ from T_{p-j}. Then $\alpha_0^{p-5}\alpha_{p-j}\alpha_{p-j}'\alpha_j^2\alpha_0 \in H$. Using a similar argument to the above, we can show that $\alpha_j^2\alpha_0 = \alpha_0\alpha_j^2$, which yields a contradiction to (2). In a similar way to (II), we can prove that if $|T_{p-j}| \ge 1$, then $v_0 = v_j = 0$, and show that $u_0, u_j \ge p(2k - m)$ as well. $\square$

Lemma 16. *Let $|H| = m = p^r p_1^{r_1} \cdots p_w^{r_w}$, where $p, p_1, \cdots, p_w$ are pairwise distinct primes, $w \ge 1$, $r \ge 0$ and $r_i \ge 1$ for every $i \in \{1, \cdots, w\}$. Then the following statements hold.*

(I) *Every Sylow p-subgroup of G is cyclic.*
(II) *If $g \in G$ and $o(g)|p^r$ then g is central. Moreover, if $o(g)|m$, then $g \in H$.*
(III) *If g is an element in $G \setminus H$, then $o(g)|\frac{n}{p_1 \cdots p_w}$.*

Proof. (I) If r=0, clearly, the result is true. Assume that $r \ge 1$. By Lemma 15, there are $\alpha \in G \setminus H$ and $\gamma \in H$ such that both α and γ occur at least p times in T. By Lemma 14, $\alpha^p \ne \gamma^p$, and by Lemma 12 and Lemma 11, $\alpha^p\gamma^{-p}$ generates H. Therefore, p^r divides the order of $\alpha^p\gamma^{-p}$. Hence, p^r divides either the order of α^p or the order of γ^{-p}. Since $\gamma \in H$, the order of γ^{-p} divides $\frac{m}{p} = p^{r-1}p_1^{r_1} \cdots p_w^{r_w}$, so the latter is impossible. Thus, p^r divides the order of α^p. Therefore, p^{r+1} divides the order of α. So, there exists an element b of order p^{r+1}, and thus it generates a Sylow p-subgroup $\langle b \rangle$. Hence, every Sylow p-subgroup of G is cyclic.

(II) Let $g \in G$ with $o(g)|p^r$. Since g is conjugate to an element $g_0 \in \langle b \rangle$ and $o(g_0) = o(g)$ divides p^r, we have $g_0 \in \langle b^p \rangle \subseteq H$, so it is central. Hence, g is central. Next, assume that the order of g divides m. Then we may write $g = g_1 g_2$ such that $(o(g_1), p) = 1$ and $o(g_2)$ divides p^r. As proved above, $g_2 \in H$, and clearly, $g_1 \in H$, so $g \in H$.

(III) Let $g \in G \setminus H$ and $o(g) = \frac{pm}{l}$, where l is a positive divisor of n. If $(p, l) \neq 1$, then $o(g)$ divides m. By part (II), g must be in H, which yields a contradiction. Thus, we have $(p, l) = 1$, and then $l = p_1^{s_1} \cdots p_w^{s_w}$. If $s_i = 0$ for some $i \in \{1, \cdots, w\}$, then $p_i^{r_i} | o(g)$. Let M_i be the Sylow p_i-subgroup of G and let $\eta = g^{m_0}$ where $m_0 = \frac{o(g)}{p_i^{r_i}}$. Then η has order $p_i^{r_i}$, so η generates M_i and $g\eta = \eta g$. Since $G = \langle H, g\rangle$, η is central and so is M_i. Since G is not abelian, $G \neq \langle M_i, b\rangle$. As proved earlier in Lemma 10, $\langle M_i', b\rangle$ is a proper non-cyclic normal subgroup of G, which yields a contradiction to Lemma 10. Therefore, $l = p_1^{s_1} \cdots p_w^{s_w}$ and $s_i \geq 1$ for all $i \in \{1, \cdots, w\}$. □

We are now in position to complete the proof of our main result.

Proof of Theorem 2. Let $n = p^{r+1} p_1^{r_1} \cdots p_w^{r_w}$ as in Lemma 16 and $l = p_1 \cdots p_w$. By Lemma 16, for every element $g \in G \setminus H$ we have

$$g^{\frac{n}{l}} = 1. \tag{8}$$

We distinguish two cases according to if $p = 2$ or not.

Case 1. If $p = 2$, then $l \geq 3$. We will show that T contains a 1-product subsequence of length n, which yields a contradiction.

We know from Lemma 15 that $T = T_0T_1$, and T_0, T_1 can be rearranged as follows:

$$T_0 = (\underbrace{\alpha_0, \cdots, \alpha_0}_{u_0}, \underbrace{\alpha_0', \cdots, \alpha_0'}_{v_0}), \ \ T_1 = (\underbrace{\alpha_1, \cdots, \alpha_1}_{u_1}, \underbrace{\alpha_1', \cdots, \alpha_1'}_{v_1}),$$

where $u_i \geq v_i, 0 \leq v_i \leq 1, u_i \geq 2(2k - m)$ for every $i \in \{0, 1\}$, and $\sum_{i=0}^{1}(u_i + v_i) = |T|$.

It follows from Lemma 10 and Lemma 15 that $4|m$, and $u_0, u_1 \geq 2(2k - m) \geq 2(2\lfloor \frac{3m}{4} \rfloor - m) = m$.

We first show that $u_1 < \frac{4m}{3}$. If $u_1 \geq \frac{4m}{3}$, then

$$u_1 \geq \frac{4m}{3} \geq \frac{l-1}{2}\frac{2m}{l} + \frac{2m}{l} \ \ (\text{ since } l \geq 3).$$

and

$$u_0 \geq m > \frac{l-1}{2}\frac{2m}{l}.$$

Since $(\alpha_1\alpha_0)^{\frac{2m}{l}} = (\alpha_1)^{\frac{2m}{l}} = 1$ by (8), we have $(\alpha_1\alpha_0)^{\frac{l-1}{2}\frac{2m}{l}} \alpha_1^{\frac{2m}{l}} = 1$, so we conclude that T has a 1-product of subsequence of length $n = 2m$, which yields a contradiction. So, we must have that $u_1 < \frac{4m}{3}$. Thus, $u_0 \geq 4k - 2 - (\frac{4m}{3} - \frac{1}{3}) \geq \frac{5m-5}{3} > \frac{4m}{3}$.

If $l \neq 5$, since $l \geq 3$ and l is odd, we can easily check that

$$[\frac{l}{3}]\frac{2m}{l} + 2(m - 3[\frac{l}{3}]\frac{m}{l}) = 2m - 4[\frac{l}{3}]\frac{m}{l} \leq m \leq u_1 \text{ and } 2[\frac{l}{3}]\frac{2m}{l} \leq \frac{4m}{3} \leq u_0.$$

Since $(\alpha_1\alpha_0^2)^{\frac{2m}{l}} = (\alpha_1)^{2\frac{m}{l}} = 1$ by (8), we have

$$(\alpha_1\alpha_0^2)^{[\frac{l}{3}]\frac{2m}{l}}(\alpha_1^2)^{m-3[\frac{l}{3}]\frac{m}{l}} = 1.$$

As before, we can obtain a 1-product subsequence of T of length n, deriving a contradiction.

Next, assume that $l = 5$. Clearly, $2\frac{2m}{5} + \frac{2m}{5} \leq \frac{4m}{3} \leq u_0$ and $\frac{2m}{5} + \frac{2m}{5} < m \leq u_1$. Using (8), we have

$$(\alpha_1\alpha_0^2)^{\frac{2m}{5}}(\alpha_1\alpha_0)^{\frac{2m}{5}} = 1.$$

As before, we can obtain a 1-product subsequence of T, deriving a contradiction.

Case 2. If $p \geq 3$, then by Lemma 15 we have

$$u_0, u_j \geq p(2k - m) \geq \frac{m-3}{2}p.$$

We first show that $u_j < \frac{2pm}{3}$ and $u_0 \geq \frac{5pm}{6} - \frac{3p}{2} - \frac{19}{6}$. Assume to the contrary that $u_j \geq \frac{2pm}{3}$. If $\frac{m}{l} \geq 3$, then

$$u_0 \geq \frac{m-3}{2}p \geq \frac{l-1}{2}\frac{pm}{l}.$$

Note that

$$u_j \geq \frac{2pm}{3} \geq \frac{l-1}{2}\frac{pm}{l} + \frac{pm}{l} \quad (\text{ since } l \geq 5).$$

Since

$$(\alpha_j\alpha_0)^{\frac{l-1}{2}\frac{pm}{l}}\alpha_j^{\frac{pm}{l}} = 1,$$

as before, we can derive a contradiction.

If $\frac{m}{l} < 3$, since both m and l are odd, we have $\frac{m}{l} = 1$. Therefore, $(\alpha_j\alpha_0)^p = \alpha_j^p = 1$ by (8). Let $\ell_0 = [\frac{m}{3} + 1]p \leq u_0$, and let $\ell_j = pm - 2\ell_0$. Then $\ell_0 + \ell_j = pm - \ell_0 < \frac{2pm}{3} \leq u_j$. Since

$$(\alpha_j\alpha_0)^{\ell_0}\alpha_j^{\ell_j} = 1,$$

we derive a contradiction again. Thus, we always have that

$$u_j < \frac{2pm}{3}.$$

Therefore,

$$u_0 \geq 2kp - 2 - u_j \geq \frac{5pm}{6} - \frac{3p}{2} - \frac{19}{6}.$$

If $l \geq 7$, similar to Case 1, we have

$$(\alpha_j\alpha_0^2)^{[\frac{l}{3}]\frac{pm}{l}}\alpha_j^{pm-3[\frac{l}{3}]\frac{pm}{l}} = 1.$$

As before, we can derive a contradiction.

So, we have $l < 7$. Since l is odd, we have $l \leq 5$. Since $p < l$, we must have $p = 3$ and $l = 5$. Since

$$(\alpha_j\alpha_0^2)^{\frac{pm}{5}}(\alpha_j\alpha_0)^{\frac{pm}{5}} = 1,$$

we derive a contradiction.

In all cases, we are able to derive a contradiction. Therefore, such a minimal counterexample G does not exist. This completes the proof of our main result. □

ACKNOWLEDGEMENTS

We would like to thank the referee for some useful comments which help improve the readability of the paper. 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 acknowledge the kind hospitality from the host institution. The research was supported 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 was also supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada.

References

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

[2] J.D. Bovey, P. Erdős and I. Niven, Conditions for zero-sum modulo n, Canada Math. Bull. 18 (1975) 27-29.

[3] V. Dimitrov, On the strong Davenport constant of nonabelian finite p-groups, Math. Balkanica (N. S.) 18 (2004) 129-140.

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

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

[6] W.D. Gao, An improvement of Erdős-Ginzburg -Ziv theorem, Acta Math. Sinca 39 (1996) 514-523.

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

[8] A. Geroldinger and F. Halter-Koch, Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory, volume 278 of Pure and Applied Mathematics. Chapman and Hall/CRC, 2006.

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

[10] M. Hall, The Theory of Groups, Reprinting of the 1968 edition, Chelsea Publishing Co., New York, 1976.

[11] Y.O. Hamidoune and D. Quiroz , On subsequence weighted products, Combin. Probab. Comput. 14 (2005) 485-489.

[12] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer, 1996.

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

[14] J.E. Olson and E.T. White, Sums from a sequences of group elements, Number theory and algebra, pp. 215-222. Academic Press, New York, 1977.

[15] D. Robinson, A Course in the Theory of Groups, Second edition, Graduate Texts in Mathematics, 80. Springer-Verlag, New York, 1996.

[16] S. Savchev and F. Chen, Long n-zero-free sequences in finite cyclic groups, Discrete Math. 308 (2008) 1-8.

[17] M. Suzuki, Group Theory II, Translated from the Japanese, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 248. Springer-Verlag, New York, 1986.

[18] T. Tao and V.H. Vu, Additive Combinatorics, Cambridge Univ. Press, Cambridge, 2006.

[19] T. Yuster and B. Peterson, A generalization of an addition theorem for sovable groups, Canad. J. Math. 36 (1984) 529-536.

[20] T. Yuster, Bounds for counter-example to an addition theorem in solvable groups, Arch. Math. (Basel) 51 (1988) 223-231.

[21] J.J. Zhuang and W.D. Gao, Erdős-Ginzburg-Ziv theorem for dihedral groups of large prime index, European J. Combin. 26 (2005) 1053-1059.

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China

E-mail address: `wdgao1963@yahoo.com.cn`

Department of Mathematics, Brock University, St. Catharines, Ontario, Canada, L2S 3A1

E-mail address: `yli@brocku.ca`