Available online at www.sciencedirect.com
SCIENCE DIRECT
ELSEVIER
Journal of Combinatorial Theory, Series A 107 (2004) 69–86
Journal of Combinatorial Theory Series A
http://www.elsevier.com/locate/jcta

A variant of Kemnitz Conjecture

W.D. Gao[a] and R. Thangadurai[b,*]

[a] *Department of Computer Science and Technology, University of Petroleum, Shuiku Road, Changping, Beijing 102200, China*
[b] *School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, India*

Received 18 July 2003

Abstract

For any integer $n \geqslant 3$, by $g(\mathbb{Z}_n \oplus \mathbb{Z}_n)$ we denote the smallest positive integer t such that every subset of cardinality t of the group $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contains a subset of cardinality n whose sum is zero. Kemnitz (Extremalprobleme für Gitterpunkte, Ph.D. Thesis, Technische Universität Braunschweig, 1982) proved that $g(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p - 1$ for $p = 3, 5, 7$. In this paper, as our main result, we prove that $g(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p - 1$ for all primes $p \geqslant 67$.

MSC: primary 11B75; secondary 20K99

Keywords: Zero-sum; Subset-sum; Finite abelian groups

1. Introduction

Let G be a finite abelian group (additively written). From the structure theorem of finite abelian groups, we know that $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_d}$ with $1 < n_1 | n_2 | \cdots | n_d$, where $n_d = \exp(G) := n$ is the exponent of G and d is the rank of G. When $n_1 = n_2 = \cdots = n_d = n$, we write $\mathbb{Z}_n^d$ instead of $\underbrace{\mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \cdots \oplus \mathbb{Z}_n}_{d \text{ times}}$.

*Corresponding author. Fax: +91-532-266-7576.
E-mail address: thanga@mri.ernet.in (R. Thangadurai).

0097-3165/$ - see front matter
doi:10.1016/j.jcta.2004.03.009

Definition 1. By $g(G)$ we denote the smallest positive integer t such that every subset S of G of cardinality $|S| \geqslant t$ contains a subset S' of cardinality $|S'| = \exp(G)$ whose sum is the identity element of G.

This constant $g(G)$ was first introduced by Harborth [18] for the group $G = \mathbb{Z}_n^d$. Kemnitz [20] proved that

$$(n-1)2^{d-1} + 1 \leqslant g(\mathbb{Z}_n^d) \leqslant (n-1)n^{d-1} + 1 \quad \text{for all } n \geqslant 3$$

and $g(\mathbb{Z}_n^d) \geqslant n2^{d-1} + 1$ for even integers n. Therefore, it follows that $g(\mathbb{Z}_n) = n$ for all odd integer n. Kemnitz [20] studied this constant when $d = 2$ and computed for small values of $p = 3, 5, 7$ and indeed, he proved that for these primes $g(\mathbb{Z}_p^2) = 2p - 1$.

Also, it is known that $g(\mathbb{Z}_3^3) = 10$ and $g(\mathbb{Z}_3^4) = 21$ (see [4–5,12,18–20]). Further, it is known in [9] that $g(\mathbb{Z}_3^5) = 45$ and also in [3], it is known that $112 \leqslant g(\mathbb{Z}_3^6) \leqslant 114$. More generally, it known from the work of Meshulam [21] that $g(\mathbb{Z}_3^d) \leqslant (1 + o(1)) \frac{3^d}{d}$. We shall conjecture the following.

Conjecture 1. *For all integers $n \geqslant 3$, we have*

$$g(\mathbb{Z}_n^2) = \begin{cases} 2n - 1 & \text{if } n \text{ is odd}, \\ 2n + 1 & \text{if } n \text{ is even}. \end{cases}$$

From the following examples, one can see that Conjecture 1 is sharp.

For n is odd, let $A = \{(0,0), (0,1), \ldots, (0, n-2), (1,1), (1,2), \ldots, (1, n-1)\}$ be a subset of $\mathbb{Z}_n^2$. Then $|A| = 2n - 2$ and A contains no zero-sum subset of cardinality n. Hence, $g(\mathbb{Z}_n^2) \geqslant |A| + 1 = 2n - 1$; for n is even, let $A = \{(0,0), (0,1), \ldots, (0, n-1), (1,0), (1,2), \ldots, (1, n-1)\}$. Then $|A| = 2n$ and A contains no zero-sum subset of cardinality n. Hence, $g(\mathbb{Z}_n^2) \geqslant |A| + 1 = 2n + 1$.

In this article, we shall prove the following theorem.

Theorem 1. *Conjecture* 1 *is true for all primes $p \geqslant 67$. That is, for every prime $p \geqslant 67$, we have $g(\mathbb{Z}_p^2) = 2p - 1$.*

In the last section, we shall prove that Conjecture 1 is true for $n = 4$ and we shall provide an equivalent criterion as well.

Before we discuss further, we shall introduce notations once for all. A sequence in G is a multi-set in G and throughout we use multiplicative notation. Let $S = \prod_{i=1}^{\ell} g_i$ be a sequence in G. For every $g \in G$, let $v_g(S)$ (a non-negative integer) denote the multiplicity of g in S. We call $|S| = \ell$ the length of S. The length is the cardinality of S as a multi-set whence

$$|S| = \sum_{g \in G} v_g(S).$$

Let $\sigma(S) = \sum_{i=1}^{\ell} g_i$. We say T is a subsequence of S if T is a subset of the multi-set S. We denote any subsequence T of S by $T \mid S$. Also, if T is a subsequence of S, then the deleted sequence ST^{-1}, we mean the sequence after removing the elements of T from S. We say that the sequence $S = \prod_{i=1}^{\ell} g_i$ in G is

- a *zero-sum sequence*, if $\sigma(S) = 0$ in G,
- a *square-free sequence*, if $v_g(S) = 0$ or 1. In other words, S is a subset of G,
- a *zero-sum free sequence*, if none of its subsequence is a zero-sum sequence,
- a *minimal zero-sum sequence*, if it is a zero-sum sequence and its proper subsequences are all zero-sum free sequences.

For every $1 \leqslant k \leqslant \ell$, define

$$\sum_k (S) = \{g_{i_1} + g_{i_2} + \cdots + g_{i_k} \mid 1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant \ell\}$$

and define

$$\sum (S) = \{g_{i_1} + g_{i_2} + \cdots + g_{i_l} \mid 1 \leqslant i_1 < i_2 < \cdots < i_l \leqslant \ell, 1 \leqslant l \leqslant \ell\}.$$

Clearly, $\sum (S) = \bigcup_{k=1}^{\ell} \sum_k (S)$.

If $S = \prod_{i=1}^{2p-1} (a_i, b_i)$ is a sequence in $\mathbb{Z}_p^2$, then $T = \prod_{i=1}^{2p-1} a_i$ is the sequence in $\mathbb{Z}_p$ where the elements a_i are simply the first co-ordinates of S. (We call T as the first co-ordinate sequence.) One can write T in the following form:

$$T = x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r} y_1^2 y_2^2 \cdots y_u^2 z_1 z_2 \cdots z_v,$$

where $x_1, \ldots, x_r, y_1, \ldots, y_u, z_1, \ldots, z_v$ are pairwise distinct elements in $\mathbb{Z}_p$, r, u, $v \geqslant 0$, $m_1, m_2, \ldots, m_r \geqslant 3$ are integers and $m_1 + m_2 + \cdots + m_r + 2u + v = 2p - 1$. Throughout this article, we shall freely use these constants r, u, v without mentioning.

We shall define the invariant $h(.)$ for the given sequence S as follows:

$$h = h(S) := \max\{v_g(S) : g \in G\}$$

the maximum of the multiplicities of elements occurring in the sequence S.

We shall define a function $s(G)$ which is analogues to $g(G)$ as follows.

Definition 2. By $s(G)$, we denote the smallest positive integer t such that every sequence S in G of length $|S| \geqslant t$ contains a zero-sum subsequence S' of length $|S'| = \exp(G)$.

This constant was studied by many authors. In 1961, Erdős, et al. [10] proved that $s(\mathbb{Z}_n) = 2n - 1$. In 1983, the following conjecture was made by Kemnitz [19,20].

Conjecture 2 (Kemnitz [20]). *For all* $n \geqslant 2$, $s(\mathbb{Z}_n \oplus \mathbb{Z}_n) = 4n - 3$.

Conjecture 2 is sharp in the following way; Let $S = (0,0)^{n-1}\ (0,1)^{n-1}\ (1,0)^{n-1}$ $(1,1)^{n-1}$ be a sequence in $\mathbb{Z}_n^2$. Then $|S| = 4n-4$ and S contains no zero-sum subsequence of length n. Hence, $s(\mathbb{Z}_n^2) \geqslant |S| + 1 = 4n-3$.

Kemnitz proved this conjecture for primes $p = 3, 5, 7$ by proving $g(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p-1$ for these primes. But for a general prime p, if one knows the value of $g(\mathbb{Z}_p \oplus \mathbb{Z}_p)$ for all primes, then it is not yet known that $s(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2g(\mathbb{Z}_p \oplus \mathbb{Z}_p) - 1$. The best known result related to Conjecture 2 (in one direction) is (due to Gao [14]) $s(\mathbb{Z}_n \oplus \mathbb{Z}_n) \leqslant 4n-2$ for every $n = p^k$ for any prime power. It should be mentioned that Ronayi [24] first proved the same result when $k = 1$. In another direction, the best result known (due to Gao [15] (more general) and Thangadurai [26] (for this particular case)) is as follows. If S is a sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ of length $4n-3$ and $h(S) \geqslant n/2$, then there exists a zero-sum subsequence of S of length n.

Now we shall state a corollary to Theorem 1 related to $s(\mathbb{Z}_p^2)$ as follows.

Corollary 1. *Let $p \geqslant 67$ be any prime number. Let S be any sequence in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ of length $4p-3$. If $h(S) \leqslant 2$, then there exists a zero-sum subsequence of length p.*

2. Preliminaries

In this section, we shall work-out some preliminaries for our main result.

Theorem 2.1 (Dias De Silva [8], Alon et al. [1–2]). *If A is a non-empty subset of $\mathbb{Z}_p$ and if $1 \leqslant k \leqslant |A|$, then*

$$\left|\sum_k (A)\right| \geqslant \min\{p, k(|A|-k)+1\}.$$

Theorem 2.2 (Gao [13]). *Let $n \geqslant 5$ and let W be a zero-sum free sequence in $\mathbb{Z}_n$.*

(1) *If $|W| = n-1$, then $W = a^{n-1}$ for some $a \in \mathbb{Z}_n$ with $(a,n) = 1$.*
(2) *If $|W| = n-2$, then $W = a^{n-2}$ or $W = a^{n-3}(2a)$ for some $a \in \mathbb{Z}_n$ with $(a,n) = 1$.*

Theorem 2.3 (Dias De Silva [8]). *Let $p > 3$ be a prime. Set $k = \lfloor \sqrt{4p-7} \rfloor + 1$ and set $\ell = [k/2]$. Let S be a square-free sequence in $\mathbb{Z}_p$ of length k. Then $\sum_\ell (S) = \mathbb{Z}_p$.*

Theorem 2.4 (Cauchy–Davenport Inequality [6–7]). *If $A_1, A_2, \ldots, A_\ell$ are non-empty subsets of $\mathbb{Z}_p$, then*

$$|A_1 + A_2 + \cdots + A_\ell| \geqslant \min\left\{p, \sum_{i=1}^{\ell} |A_i| - \ell + 1\right\}.$$

The following technical lemma is very crucial for our main result and also it generalizes a Lemma 4.7 in [25].

Lemma 2.5. *Let* $S = \prod_{i=1}^{2p-1}(a_i, b_i)$ *be a square-free sequence of length* $2p-1$ *in* $\mathbb{Z}_p^2$. *Write*

$$S = \prod_{i=1}^{\ell} \prod_{j=1}^{n_i} (x_i, b_j^{(i)}),$$

where $n_1, n_2, \ldots, n_\ell \geqslant 1$, $\ell \geqslant 1$, $x_1, x_2, \ldots, x_\ell$ *are pairwise distinct elements of* $\mathbb{Z}_p$, *and* $n_1 + n_2 + \cdots + n_\ell = 2p - 1$. *Let* $W = \prod_{i=1}^{\ell} x_i^{l_i}$ *be a zero-sum subsequence of the first co-ordinate sequence* T *such that* $|W| = p$, *where* $0 \leqslant l_i \leqslant n_i$ *and* $l_1 + l_2 + \cdots + l_\ell = p$. *Suppose that* $1 + \sum_{i=1}^{\ell} l_i(n_i - l_i) \geqslant p$. *Then* S *contains a zero-sum subsequence of length* p.

Proof. Since S is a square-free sequence in $\mathbb{Z}_p^2$, for every $i \in \{1, 2, \ldots, \ell\}$, we have $b_1^{(i)}, b_2^{(i)}, \ldots, b_{n_i}^{(i)}$ are pairwise distinct in $\mathbb{Z}_p$. Set $B_i = \{b_1^{(i)}, b_2^{(i)}, \ldots, b_{n_i}^{(i)}\}$ for every $i = 1, 2, \ldots, \ell$. Then it suffices to prove that

$$0 \in \sum_{l_1} (B_1) + \sum_{l_2} (B_2) + \cdots + \sum_{l_\ell} (B_\ell).$$

By Theorem 2.1, we see that for each i, we have

$$\left| \sum_{l_i} (B_i) \right| \geqslant l_i(n_i - l_i) + 1. \tag{1}$$

Therefore, by Theorem 2.4, we have

$$\left| \sum_{l_1} (B_1) + \cdots + \sum_{l_\ell} (B_\ell) \right| \geqslant \min \left\{ p, \left| \sum_{l_1} (B_1) \right| + \cdots + \left| \sum_{l_\ell} (B_\ell) \right| - \ell + 1 \right\}.$$

Therefore, by Eq. (1), LHS of the above inequality is at least

$$\begin{aligned} &\geqslant \min\{p, (l_1(n_1 - l_1) + 1) + \cdots + (l_\ell(n_\ell - l_\ell) + 1) - \ell + 1\} \\ &= \min\{p, l_1(n_1 - l_1) + \cdots + l_\ell(n_\ell - l_\ell) + 1\} \\ &= p. \end{aligned}$$

Therefore, we have

$$\sum_{l_1} (B_1) + \sum_{l_2} (B_2) + \cdots + \sum_{l_\ell} (B_\ell) = \mathbb{Z}_p$$
$$\Rightarrow 0 \in \sum_{l_1} (B_1) + \sum_{l_2} (B_2) + \cdots + \sum_{l_\ell} (B_\ell).$$

Thus the lemma follows. $\square$

Lemma 2.6. *Let p be any prime number, and let T be a sequence in $\mathbb{Z}_p \backslash \{0\}$ of length p. Set $h = h(T)$. Then $\sum_{\leqslant h}(T) = \mathbb{Z}_p$, where $\sum_{\leqslant h}(T) = \bigcup_{r=1}^{h} \sum_r(T)$.*

Proof. Note that one can distribute the elements of T into h nonempty subsets $A_1, A_2, \ldots, A_h$. By Cauchy–Davenport inequality (Theorem 2.4), we have

$$\left|\sum_{\leqslant h}(T)\right| \geqslant \min\{p, |A_1 \cup \{0\}| + \cdots + |A_h \cup \{0\}| - h + 1\} = p.$$

Therefore, $\sum_{\leqslant h}(T) = \mathbb{Z}_p$. $\square$

Theorem 2.7. *Let p be any prime number and $2 \leqslant k \leqslant p - 1$. Let S be a sequence in $\mathbb{Z}_p$ of length $2p - k$. Suppose that $0 \notin \sum_p(S)$. Then $h(S) \geqslant p - k + 1$.*

Proof. Without loss of generality, we may assume that $S = 0^h T$ with $|T| = 2p - k - h$. Assume to the contrary that $h \leqslant p - k$. Therefore, $|T| \geqslant p$ and T is a sequence in $\mathbb{Z}_p \backslash \{0\}$. By Lemma 2.6, $\sum_{\leqslant h}(T) = \mathbb{Z}_p$. Especially, $\sigma(T) \in \sum_{\leqslant h}(T)$. That is, there is a subsequence Q of T such that $\sigma(Q) = \sigma(T)$ and $1 \leqslant |Q| \leqslant h$. Set $T_1 = TQ^{-1}$. Then $\sigma(T_1) = 0$ and $p - h \leqslant |T| - h \leqslant |T_1| \leqslant |T| - 1$. If $|T_1| \leqslant p$, then $T_1 0^{p-|T_1|}$ is a zero-sum subsequence of S of length p which is a contradiction. Therefore, $|T_1| \geqslant p$. Apply Lemma 2.6 to T_1, one can find a subsequence Q_1 of T_1 such that $\sigma(Q_1) = 0$ and $1 \leqslant |Q_1| \leqslant h$, set $T_2 = T_1 Q_1^{-1}$. Then $\sigma(T_2) = 0$ and $p - h \leqslant |T_1| - h \leqslant |T_2| \leqslant |T_1| - 1$. Continuing the same procedure we finally get a zero-sum subsequence of S of length p which is again a contradiction. Thus the theorem is proved. $\square$

3. Proof of Theorem 1

Throughout this section, let p be an odd prime, $S = \prod_{i=1}^{2p-1}(a_i, b_i)$ a sequence in $\mathbb{Z}_p^2$,

$$T = x_1^{m_1} \cdots x_r^{m_r} y_1^2 \cdots y_u^2 z_1 \cdots z_v$$

be the first co-ordinate sequence with $r, u, v \in \mathbb{N}_0$, $m_1, \ldots, m_r \in \mathbb{N}_{\geqslant 3}$, $x_1, \ldots, x_r$, $y_1, \ldots, y_u$, $z_1, \ldots, z_v \in \mathbb{Z}_p$ pairwise distinct, and let $h = h(T)$. In a series of propositions, we shall prove, under various additional assumptions, that S has a zero-sum subsequence of length p. Putting everything together we shall obtain a proof of Theorem 1.

Proposition 3.1. *If $h \in \{2, p\}$, then S has a zero-sum subsequence of length p.*

Proof. Let $h(T) = p$. Without loss of generality we can assume that $a_1 = a_2 = \cdots = a_p = 0$. Since S is square-free sequence in $\mathbb{Z}_p^2$, the sequence $b_1, b_2, \ldots, b_p$ runs through every residue classes of modulo p. Hence, $b_1 + b_2 + \cdots + b_p = 0$ in $\mathbb{Z}_p$. Thus $\prod_{i=1}^{p}(0, b_i)$ is a zero-sum subsequence of length p in S.

Let $h(T) = 2$. Then every residue classes modulo p can be appearing at most 2 times. Since $|S| = 2p - 1$ and we have p distinct residue classes modulo p, we see, by Pigeon hole principle, that $p - 1$ distinct residue classes modulo p has to appear exactly 2 times and only one residue class (we can assume it to be 0) has to appear exactly once. Thus we are in the following situation:

$$S = (0, z) \prod_{i=1}^{p-1}(i, x_i) \prod_{i=1}^{p-1}(i, y_i),$$

where $x_i \not\equiv y_i \pmod p$ for all $i = 1, 2, \ldots, p - 1$. We have $W = 0 \prod_{i=1}^{p-1} i$ is a zero-sum subsequence of T of length p. Since

$$1(1-1) + \underbrace{1(2-1) + 1(2-1) + \cdots + 1(2-1)}_{p-1 \text{ times}} + 1 = p,$$

by Lemma 2.5, S has a zero-sum subsequence of length p. $\square$

Proposition 3.2. *If* $\left(\prod_{i=1}^{r} x_i^2 \prod_{i=1}^{u} y_i\right)^{-1} \cdot T$ *has a zero-sum subsequence of length p and* $r + u + v \leqslant \frac{p+3}{2}$, *then S has a zero-sum subsequence of length p.*

Proof. By Proposition 3.1, we can assume that $3 \leqslant h \leqslant p - 1$. By assumption, we have $R = c_1^{\ell_1} c_2^{\ell_2} \cdots c_t^{\ell_t} c_{t+1} \cdots c_s$ is the zero-sum subsequence of length p of $\left(\prod_{i=1}^{r} x_i^2 \prod_{i=1}^{u} y_i\right)^{-1} \cdot T$ where $c_1, c_2, \ldots, c_s$ are pairwise distinct elements of $\mathbb{Z}_p$, $t \geqslant 1$ and $2 \leqslant \ell_i \leqslant m_{j_i} - 2$ for all $i = 1, 2, \ldots, t$. Note that $p = |R| = \ell_1 + \ell_2 + \cdots + \ell_t + s - t$. Without loss of generality, we may assume that $m_{j_i} = m_i$ (by renaming the indices, if necessary). We have to prove that S has a zero-sum subsequence of length p. If we can prove $1 + \sum_{i=1}^{t} \ell_i(m_i - \ell_i) \geqslant p$, then by Lemma 2.5, it follows that S does have a zero-sum subsequence of length p. Now, consider

$$\begin{aligned} 1 + \sum_{i=1}^{t} \ell_i(m_i - \ell_i) \geqslant 1 + \sum_{i=1}^{t} 2(m_i - 2) &= 1 + 2(m_1 + m_2 + \cdots + m_t) - 4t \\ &\geqslant 1 + 2(\ell_1 + 2 + \cdots + \ell_t + 2) - 4t \geqslant 1 + 2(\ell_1 + \cdots + \ell_t) \\ &= 1 + 2(p - s + t) = 1 + 2p - 2(s - t) \geqslant 1 + 2p - 2(p + 1)/2 \\ &= p. \qquad \square \end{aligned}$$

Proposition 3.3. *If, for some* $x \in \mathbb{Z}_p$,

$$T = 0^{p-1} \cdot 1^{p-1} \cdot x \quad \text{or} \quad T = 0^{p-1} \cdot 1^{p-2} \cdot 2 \cdot (p-1),$$

then S has a zero-sum subsequence of length p.

Proof. Suppose $T = 0^{p-1}1^{p-1}x$. Then $W = 0^{x-1}1^{p-x}x$ is a zero-sum subsequence of T of length p, whenever $x \neq 0, 1$. Note that $(x-1)(p-x) + (p-x)x + 1 = (p-x)(2x-1) + 1 \geqslant p$. Hence, by Lemma 2.5, there exists a zero-sum subsequence of length p.

If $x = 0$ or 1, it follows from Proposition 3.1 that S contains a zero-sum subsequence of length p.

Suppose $T = 0^{p-1}1^{p-2}(2)(p-1)$. Then set $W = 0^{p-2}1(p-1)$ which is obviously a zero-sum subsequence of length p and we have $p-2+p-3+1 \geqslant p$. Thus by Lemma 2.5, we have a zero-sum subsequence of S of length p. □

Proposition 3.4. *If $p \geqslant 11$ and $h \geqslant \frac{p+5}{2}$, then S has a zero-sum subsequence of length p.*

Proof. Without loss of generality, we may assume that $a_{2p-h} = a_{2p+1-h} = \cdots = a_{2p-1} = a$. Therefore, the first co-ordinate sequence $T = a^h \prod_{i=1}^{2p-1-h} a_i$.

Claim 1. There is a subset $I \subset \{1, 2, \ldots, 2p-1-h\}$ such that $(p - |I|)a + \sum_{i \in I} a_i = 0$ in $\mathbb{Z}_p$ and such that $p - h + 2 \leqslant |I| \leqslant p - 2$.

To prove the Claim 1, we may assume that $a = 0$. Then it suffices to prove that there is a subset $I \subset \{1, 2, \ldots, 2p-1-h\}$ such that $\sum_{i \in I} a_i = 0$ and such that $p - h + 2 \leqslant |I| \leqslant p - 2$.

By Proposition 3.1, we may assume that $h \leqslant p-1$. Let I be the maximal subset of $\{1, 2, \ldots, 2p-1-h\}$ such that $\sum_{i \in I} a_i = 0$ and $|I| \leqslant p$. By Lemma 2.6, one can get $p - h \leqslant |I| \leqslant p$. Set $J = \{1, 2, \ldots, 2p-1-h\} \backslash I$. If I satisfies $p - h + 2 \leqslant |I| \leqslant p - 2$, then nothing to prove. Now, we distinguish cases.

Case 1: $|I| = p$. Since $h \leqslant p-1$, we see that $\prod_{i \in I} a_i$ cannot be a minimal zero-sum sequence. Therefore, there is a subset $A \subset I$ such that $\sum_{i \in A} a_i = 0$ and $1 \leqslant |A| \leqslant p-1$. But, $a_i \neq 0$ for $i = 1, 2, \ldots, 2p-1-h$. Therefore, $2 \leqslant |A| \leqslant p-2$. Now letting I be the maximal one of A and $I \backslash A$, and we see that Claim 1 is satisfied.

Case 2: $|I| = p-h$, $p-h+1$ or $p-1$. We distinguish sub-cases.

Sub-case 1: $h = p-1$. Since $a_i \neq 0$ for $i = 1, 2, \ldots, p$, $|I| = 2$ or $|I| = p-1$. If $|I| = 2$, then $|J| = p-2$ and $\prod_{j \in J} a_j$ is zero-sum free sequence in $\mathbb{Z}_p$. By Theorem 2.2, we see that $\prod_{j \in J} a_j = a^{p-2}$ or $\prod_{j \in J} a_j = a^{p-3}(2a)$ for some $a \neq 0$. Without loss of generality, we may assume that $a = 1$. Now, $T = 0^{p-1}1^{p-2}(x)(-x)$ or $T = 0^{p-1}1^{p-3}(2)(x)(-x)$ for some $x \in \mathbb{Z}_p \backslash \{0\}$. If $T = 0^{p-1}1^{p-3}(2)(x)(-x)$, and if $2 \leqslant x \leqslant p-3$, then we have $1^x(-x)$ is a zero-sum subsequence of T of length $1+x$. But, $3 \leqslant 1 + x \leqslant p-2$. This satisfies the Claim 1. So, we may assume that $x = 1, p-2$ or $p-1$. If $x = p-2 = -2$, then $T = 0^{p-1}1^{p-3}(2)(2)(-2)$ and hence, $1^{p-4}(2)(2)$ is a zero-sum subsequence of length $p-2$. Now it remains to check the case when $x = 1, p-1$. Now we have $T = 0^{p-1}1^{p-2}(2)(-1)$. Also, if $T = 0^{p-1}1^{p-2}(x)(-x)$, one can reduce it to the case $T = 0^{p-1}1^{p-1}(-1)$. But by Proposition 3.3, it follows that S does have a zero-sum subsequence of length p. So, we do not need to consider these cases at all.

If $|I| = p-1$, we derive that $\prod_{i\in I} a_i$ is a minimal zero-sum sequence. By Theorem 2.2, we infer that $\prod_{i\in I} a_i = a^{p-2}(2a)$. Without loss of generality, we may assume that $a=1$. Now, $T = 0^{p-1}1^{p-2}(2)(x)$. Similarly to above, it reduces to $T = 0^{p-1}1^{p-2}(2)(-1)$ or $T = 0^{p-1}1^{p-1}(2)$, then by Proposition 3.3, S does have a zero-sum subsequence of length p.

Sub-case 2: $h = p-2$. We may assume that $|I| = 2, 3$ or $p-1$. Assume to the contrary that Claim 1 is not true.

If $|I| = 2$, then $|J| = p-1$ and $\prod_{j\in J} a_j$ is zero-sum free sequence in $\mathbb{Z}_p$. By Theorem 2.2, we have $\prod_{j\in J} a_j = a^{p-1}$ which is a contradiction to the assumption that $h = p-2$.

If $|I| = 3$, then $|J| = p-2$ and $\prod_{j\in J} a_j$ is zero-sum free sequence in $\mathbb{Z}_p$. By Theorem 2.2, we have $\prod_{j\in J} a_j = a^{p-3}(2a)$ or $\prod_{j\in J} a_j = a^{p-2}$ for some $a \neq 0 \in \mathbb{Z}_p$. We may assume that $a=1$. Now, $T = 0^{p-2}1^{p-3}(2)(x)(y)(-x-y)$ or $T = 0^{p-2}1^{p-2}(x)(y)(-x-y)$. If $T = 0^{p-2}1^{p-3}(2)(x)(y)(-x-y)$, one can easily derive that $x, y, -x-y \in \{1, p-2, p-1\}$. Since $x+y+(-x-y) = 0$, we infer that $\{x, y, -x-y\} = \{1, 1, -2\}$, $\{-1, -1, 2\}$, $\{-1, -2, 3\}$ or $\{-2, -2, 4\}$. Since $h = p-2$, we have $\{x, y, -x-y\} = \{-1, -1, 2\}$, $\{-1, -2, 3\}$ or $\{-2, -2, 4\}$. But, $1+1+(-1)+(-1) = 0$, $-1+(-2)+1+1+1 = 0$ and $-2+(-2)+1+1+1+1 = 0$, which is a contradiction on the assumption that Claim 1 is not true.

If $T = 0^{p-2}1^{p-2}(x)(y)(-x-y)$, since Claim 1 is not true and $h = p-2$, one can derive that $x, y, -x-y \in \{2, p-2, p-1\}$. Note that $x+y+(-x-y) = 0$, we have $\{x, y, -x-y\} = \{2, 2, -4\}$, $\{-2, -2, 4\}$, $\{-1, -1, 2\}$ or $\{-1, -2, 3\}$ and similarly to above, one can derive a contradiction.

If $|I| = p-1$, then $\prod_{i\in I} a_i$ is a minimal zero-sum sequence. By Theorem 2.2, we see that $\prod_{i\in I} a_i = a^{p-2}(2a)$ for some $a \neq 0$ in $\mathbb{Z}_p$. We may assume that $a=1$. Now, $T = 0^{p-2}1^{p-2}(2)(x)(y)$. Since Claim 1 is not true, $x, y \in \{1, p-2, p-1\}$. Since $h = p-2, x, y \in \{p-2, p-1\}$. Then $\{x, y\} = \{-1, -1\}$, $\{-2, -2\}$ or $\{-1, -2\}$. But $-1+(-1)+1+1 = 0$, $-2+(-2)+1+1+1+1 = 0$, $-1+(-2)+1+1+1 = 0$, a contradiction to the assumption that Claim 1 is not true.

Sub-case 3: $\frac{p+5}{2} \leqslant h \leqslant p-3$. If $|I| = p-h$, then $|J| = p-1$ and $\prod_{j\in J} a_j$ is zero-sum free sequence in $\mathbb{Z}_p$. By Theorem 2.2, we have $\prod_{j\in J} a_j = a^{p-1}$ which is a contradiction on the assumption that $h \leqslant p-3$. If $|I| = p-1$, then $\prod_{j\in J} a_j$ is a minimal zero-sum sequence in $\mathbb{Z}_p$ and by Theorem 2.2, we see, $\prod_{j\in J} a_j = a^{p-2}(2a)$ which is again a contradiction on $h \leqslant p-3$. If $|I| = p-h+1$, then $|J| = p-2$ and $\prod_{j\in J} a_j$ is zero-sum free sequence in $\mathbb{Z}_p$. By Theorem 2.2, we have $\prod_{j\in J} a_j = a^{p-2}$ or $\prod_{j\in J} a_j = a^{p-3}(2a)$ for some $a \neq 0$ in $\mathbb{Z}_p$. But $h \leqslant p-3$, we have $\prod_{j\in J} a_j = a^{p-3}(2a)$ and $h = p-3$. We may assume that $a=1$. Now, $T = 0^{p-3}1^{p-3}(2)(x)(y)(z)(w)$. Assume to the contrary that Claim 1 is not true, then $x, y, z, w \in \{1, p-3, p-2, p-1\}$. Note that $h = p-3$, we have $x, y, z, w \in \{p-3, p-2, p-1\}$. It easy to check that there is a zero-sum subsequence of T of length between 5 and 8. (Here, we need to assume $p \geqslant 11$.). Thus Claim 1 is established.

Now, we can rewrite S as follows;

$$S=\prod_{i=1}^{2p-1-h}(a_i,b_i)\prod_{i=1}^{h}(a,c_i)$$

with $c_1,c_2,\dots,c_h$ are pairwise distinct elements in $\mathbb{Z}_p$. By Claim 1, we have an index set $I\subset\{1,2,\dots,2p-1-h\}$ such that $p-h+2\leqslant|I|\leqslant p-2$ and $\sum_{i\in I}a_i+(p-|I|)a\equiv 0\ (\mathrm{mod}\,p)$. Let $b=\sum_{i\in I}b_i$. Let $C=\{c_1,c_2,\dots,c_h\}\subset\mathbb{Z}_p$ and $\ell=p-|I|$. Since I satisfies $p-h+2\leqslant|I|\leqslant p-2$, it is clear that ℓ satisfying $2\leqslant\ell\leqslant h-2$. By Theorem 2.1, we see that

$$\left|\sum_{\ell}(C)\right|\geqslant\min\{p,\ell(h-\ell+1)\}\geqslant\min\{p,2(h-2+1)\}\geqslant p.$$

Now the theorem follows from Lemma 2.5. □

Proposition 3.5. *If $p\geqslant 5$, $r+u+v\leqslant\frac{p-1}{4}$ and $h\leqslant\frac{p+3}{2}$, then S has a zero-sum subsequence of length p.*

Proof. Let

$$W=x_1^{m_1-2}x_2^{m_2-2}\cdots x_r^{m_r-2}y_1y_2\cdots y_uz_1z_2\cdots z_v$$

be a subsequence of T. Then the length of W is

$$|W|=|T|-2r-u=2p-1-2r-u\geqslant 2p-1-\frac{p-1}{2}=2p-1-\frac{p-1}{2}$$

and

$$h(W)=h(T)-2\leqslant\frac{p-1}{2}.$$

If W does not have a zero-sum subsequence of length p, then by Theorem 2.7, $h(W)\geqslant p-(p-1)/2=(p+1)/2$ which is a contradiction. Therefore, W contains a zero-sum subsequence Q of length p. Hence, by Lemma 2.5 the result follows. □

Proposition 3.6. *If $p\geqslant 67$ and $h\geqslant\lfloor\sqrt{4p-7}\rfloor+2$, then S has a zero-sum subsequence of length p.*

Proof. Let $k=\lfloor\sqrt{4p-7}\rfloor+1$. By Proposition 3.4, we may assume that $k+1\leqslant h\leqslant\frac{p+3}{2}$. We distinguish two cases.

Case 1: *T contains at least k distinct elements*. Without loss of generality, we may assume that $a_1,a_2,\dots,a_k$ are distinct. Set $\ell=[k/2]$ and $A=\{a_1,a_2,\dots,a_k\}\subset\mathbb{Z}_p$. By Theorem 2.3, we have

$$\sum_{\ell}(A)=\mathbb{Z}_p. \tag{2}$$

Since $h(T) \geqslant k+1$, the deleted sequence TA^{-1} contains some element a (say) with $v_a(TA^{-1}) \geqslant h-1 \geqslant k$. Without loss of generality, we may assume that $a_{k+1} = \cdots = a_{k+h-1} = a$. Then the corresponding second co-ordinates $b_{k+1}, b_{k+2}, \ldots, b_{k+h-1}$ are pairwise distinct in $\mathbb{Z}_p$. Set $B = \{b_{k+1}, b_{k+2}, \ldots, b_{k+h-1}\} \subset \mathbb{Z}_p$. Then again by Theorem 2.3, we see that

$$\sum_{\ell}(B) = \mathbb{Z}_p. \tag{3}$$

Note that $2p-1-h-k > p-2\ell > 0$, one can choose a subset $J \subset \{k+h, k+h+1, \ldots, 2p-1\}$ such that $|J| = p-2\ell$ and $a_j \neq a$ holds for every $j \in J$. Set $\alpha = \ell a + \sum_{j\in J} a_j$. By Eq. (2), there is a subset $I \subset \{1, 2, \ldots, k\}$ such that $\alpha + \sum_{i\in I} a_i = 0$ and $|I| = \ell$. Set $\beta = \sum_{i\in I} b_i + \sum_{j\in J} b_j$. Now by Eq. (3), there is a subset $L \subset \{k+1, k+2, \ldots, k+h-1\}$ such that $\beta + \sum_{l\in L} b_l = 0$ and $|L| = \ell$. Therefore,

$$\prod_{i\in I}(a_i, b_i)\prod_{l\in L}(a, b_l)\prod_{j\in J}(a_j, b_j)$$

is a zero-sum subsequence of S of length p.

Case 2: T *contains at most* $k-1$ *distinct elements*. Since by assumption, $p \geqslant 67$, we see that $k-1 \leqslant \frac{p-1}{4}$. Also, by assumption, we have $h \leqslant (p+3)/2$. Therefore, the result follows from Proposition 3.5. □

Proposition 3.7. *If* $p \geqslant 47$, $r+u+v \geqslant \frac{p-1}{4}$ *and* $h \leqslant \lfloor\sqrt{4p-7}\rfloor + 1$, *then* S *has a zero-sum subsequence of length* p.

Proof. First we note that it is enough to assume that $r+u+v \geqslant p/3$. For, suppose $\frac{p-3}{4} \leqslant r+u+v < \frac{p}{3}$. As $h(T) \leqslant k \leqslant p/3$, in a similar way to the proof of Proposition 3.5 one can derive that S contains a zero-sum subsequence of length p. So, we may assume that $r+u+v \geqslant p/3$. Set $t = [\frac{p}{3}]$. Write

$$T = x_1^{m_1}x_2^{m_2}\cdots x_r^{m_r}y_1^2y_2^2\cdots y_u^2 z_1z_2\cdots z_v,$$

where $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v$ are pairwise distinct elements in $\mathbb{Z}_p$, and $m_1, m_2, \ldots, m_r \geqslant 3$, $r, u, v \geqslant 0$ are integers satisfying $m_1 + m_2 + \cdots + m_r + 2u + v = 2p-1$. Set

$$A = \begin{cases} y_1y_2\cdots y_t & \text{if} \quad t \leqslant u, \\ x_{r-(t-u)+1}x_{r-(t-u)+2}\cdots x_r y_1y_2\cdots y_u & \text{if} \quad u < t \leqslant u+r, \\ x_1x_2\cdots x_r y_1y_2\cdots y_u z_{v-(t-u-r)+1}\cdots z_v & \text{if} \quad t > u+r \end{cases}$$

and

$$U = \begin{cases} \prod_{i=1}^{r} x_i^{m_i-1} \prod_{i=1}^{u} y_i \prod_{i=1}^{v} z_i & \text{if} \quad t \leqslant u, \\ \prod_{i=1}^{r-(t-u)} x_i^{m_i-1} \prod_{i=r-(t-u)+1}^{r} x_i^{m_i-2} \prod_{i=1}^{u} y_i \prod_{i=1}^{v} z_i & \text{if} \quad u < t \leqslant u+r, \\ \prod_{i=1}^{r} x_i^{m_i-2} \prod_{i=1}^{u} y_i \prod_{i=1}^{v-(t-u-r)} z_i & \text{if} \quad t > u+r. \end{cases}$$

By the making of U, it is clear that

$$|U| = \begin{cases} 2p-1-r-u & \text{if } t \leqslant u, \\ 2p-1-r-t & \text{if } u < t \leqslant u+r, \\ 2p-1-r-t & \text{if } t > u+r. \end{cases}$$

Therefore, $|U| \geqslant p-1$. Also, by Theorem 2.1, we have

$$\left|\sum_4 (A)\right| \geqslant \min\{p, 4(t-4)+1\} = p \Rightarrow \sum_4 (A) = \mathbb{Z}_p. \tag{4}$$

We distinguish cases.

Case 1: $r+u+v \leqslant p-4$. Then one can find a subsequence Q of U such that $x_1x_2\cdots x_r y_1 y_2 \cdots y_u | Q | U$ and such that $|Q| = p-4$. By Eq. (4), we see that there is subsequence R of A such that $|R| = 4$ and RQ is a zero-sum subsequence of length p. Set $W = RQ$. Now $W = RQ = x_1^{l_1} x_2^{l_2} \cdots x_r^{l_r} y_1^{f_1} y_2^{f_2} \cdots y_u^{f_u} Z$ with $Z \mid z_1 z_2 \cdots z_v$, where $1 \leqslant l_i \leqslant m_i - 1$ for all $i = 1, 2, \ldots, r$, $1 \leqslant f_1, f_2, \ldots, f_u \leqslant 2$ and $f_i = 2$ holds for at most $4(=|R|)$ of $i \in \{1, 2, \ldots, u\}$. If $m_1 + m_2 + \cdots + m_r - r + u + 1 - 4 \geqslant p$, then by Lemma 2.5, we know that S contains a zero-sum subsequence of length p. Therefore, we may assume that, $m_1 + m_2 + \cdots + m_r + u - r + 1 - 4 \leqslant p - 1$. But $m_1 + m_2 + \cdots + m_r = 2p - 1 - 2u - v$. Therefore, $2p - 1 - u - v - r + 1 - 4 \leqslant p - 1$. Hence, $u + v + r \geqslant p - 3$, which is a contradiction to the assumption that $r + u + v \leqslant p - 4$.

Case 2: $u + v + r = p - 3$. Set $t = \left[\frac{p+12}{3}\right]$. Write

$$T = x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r} y_1^2 y_2^2 \cdots y_u^2 z_1 z_2 \cdots z_v,$$

where $x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v$ are pairwise distinct, $m_1, m_2, \ldots, m_r \geqslant 3$ and $r, u, v \geqslant 0$ are integers satisfying $m_1 + m_2 + \cdots + m_r + 2u + v = 2p - 1$. Set

$$A = \begin{cases} y_1 y_2 \cdots y_t & \text{if } t \leqslant u, \\ x_{r-(t-u)+1} x_{r-(t-u)+2} \cdots x_r y_1 y_2 \cdots y_u & \text{if } u < t \leqslant u+r, \\ x_1 x_2 \cdots x_r y_1 y_2 \cdots y_u z_{v-(t-u-r)+1} \cdots z_v & \text{if } t > u+r \end{cases}$$

and

$$U = \begin{cases} x_1^{m_1-1}x_2^{m_2-1}\cdots x_r^{m_r-1}y_1y_2\cdots y_u z_1 z_2\cdots z_v & \text{if } t\leqslant u, \\ \prod_{i=1}^{r-(t-u)} x_i^{m_i-1} \prod_{i=r-(t-u)+1}^{r} x_i^{m_i-2} \prod_{i=1}^{u} y_i \prod_{i=1}^{v} z_i & \text{if } u<t\leqslant u+r, \\ x_1^{m_1-2}x_2^{m_2-2}\cdots x_r^{m_r-2}y_1y_2\cdots y_u z_1 z_2\cdots z_{v-(t-u-r)} & \text{if } t>u+r. \end{cases}$$

By the making of U we get

$$|U| = \begin{cases} 2p-1-r-u & \text{if } t\leqslant u, \\ 2p-1-r-t & \text{if } u<t\leqslant u+r, \\ 2p-1-r-t & \text{if } t>u+r. \end{cases}$$

Note that $3r+2u+v\leqslant 2p-1$ and $u+v+r\geqslant p-4$, we derive that $r=\frac{1}{2}((3r+2u+v)-(u+v+r))-u/2\leqslant\frac{p+3}{2}-u/2$. Therefore, we always have $|U|\geqslant p-1$. By Theorem 2.1, we have

$$\left|\sum_3(A)\right|\geqslant\min\{p,3(t-3)+1\}=p\Rightarrow\sum_3(A)=\mathbb{Z}_p. \tag{5}$$

Since $u+v+r=p-3$, one can find a subsequence Q of U such that

$$x_1x_2\cdots x_r y_1y_2\cdots y_u|Q|U$$

and $|Q|=p-3$. By Eq. (5), there is subsequence R of A such that $|R|=3$ and RQ is a zero-sum subsequence of length p. Set $W=RQ$. Now $W=RQ=x_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}y_1^{f_1}y_2^{f_2}\cdots y_u^{f_u}Z$ with $Z\,|\,z_1z_2\cdots z_v$, where $1\leqslant l_i\leqslant m_i-1$ for all $i=1,2,\dots,r$, $1\leqslant f_1,f_2,\dots,f_u\leqslant 2$ and $f_i=2$ holds for at most $3(=|R|)$ of $i\in\{1,2,\dots,u\}$. If $m_1+m_2+\cdots+m_r-r+u+1-3\geqslant p$, by Lemma 2.5, we see that S contains a zero-sum subsequence of length p. Therefore, we may assume that, $m_1+m_2+\cdots+m_r-r+u+1-3\leqslant p-1$. But $m_1+m_2+\cdots+m_r=2p-1-2u-v$. Therefore, $2p-1-u-v-r+1-3\leqslant p-1$. Hence, $u+v+r\geqslant p-2$ which is a contradiction to the assumption.

Case 3: $u+v+r=p$. Write $T=0^{m_0}1^{m_1}\cdots(p-1)^{m_{p-1}}$, where $m_i\geqslant 1$ and $m_0+\cdots+m_{p-1}=2p-1$. Since, $0+1+\cdots+(p-1)=0$ and $m_0+m_1+\cdots+m_{p-1}-p+1=p$, by Lemma 2.5, S contains a zero-sum subsequence of length p.

Case 4: $u+v+r=p-2$. Set $t=\frac{p+3}{2}$. Define A and U in a similar way to Case 2. Then $|A|=t$. By Theorem 2.1, we have

$$\left|\sum_2(A)\right|\geqslant\min\{p,2(t-2)+1\}=p\Rightarrow\sum_2(A)=\mathbb{Z}_p. \tag{6}$$

By the making of U, we get

$$|U| = \begin{cases} 2p-1-r-u & \text{if } t\leqslant u, \\ 2p-1-r-t & \text{if } u<t\leqslant u+r, \\ 2p-1-r-t & \text{if } t>u+r. \end{cases}$$

If $r \leqslant \frac{p-1}{2}$, then $|U| \geqslant p-2$. Then one can find a subsequence Q of U such that $x_1x_2\cdots x_ry_1y_2\cdots y_u|Q|U$ and $|Q| = p-2$. By Eq. (6), there is subsequence R of A such that $|R| = 2$ and RQ is a zero-sum subsequence of length p. Now $RQ = x_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}y_1^{f_1}y_2^{f_2}\cdots y_u^{f_u}Z$ with $Z \mid z_1z_2\cdots z_v$, where $1 \leqslant l_i \leqslant m_i - 1$ for all $i = 1, 2, \ldots, r$, $1 \leqslant f_1, f_2, \ldots, f_u \leqslant 2$ and $f_i = 2$ holds for at most $2(=|R|)$ of $i \in \{1, \ldots, u\}$. If $m_1 + m_2 + \cdots + m_r - r + u + 1 - 2 \geqslant p$, by Lemma 2.5, S contains a zero-sum subsequence of length p. Therefore, we may assume that, $m_1 + m_2 + \cdots + m_r - r + u + 1 - 2 \leqslant p - 1$. But $m_1 + m_2 + \cdots + m_r = 2p - 1 - 2u - v$. Therefore, $2p - 1 - u - v - r + 1 - 2 \leqslant p - 1$. Hence, $u + v + r \geqslant p - 1$, which is a contradiction to the assumption.

Now we assume that $r \geqslant \frac{p+1}{2}$. Since $3r + 2u + v \leqslant 2p - 1$ and $u + v + r = p - 2$, $r - v = (3r + 2u + v) - 2(r + u + v) \leqslant 2p - 1 - 2(p-2) = 3$. Therefore, $v \geqslant r - 3 \geqslant \frac{p+1}{2} - 3 = \frac{p-5}{2}$. So,

$$v \geqslant \frac{p-5}{2} \tag{7}$$

Set $A_0 = \{z_1, z_2, \ldots, z_v\}$. By Theorem 2.1,

$$\sum_3 (A_0) = \mathbb{Z}_p. \tag{8}$$

Note that $r + u < p - 3 < p + 1 = (m_1 - 1) + (m_2 - 1) + \cdots + (m_r - 1) + u$, one can find a subsequence Q of $x_1^{m_1-1}x_2^{m_2-1}\cdots x_r^{m_r-1}y_1y_2\cdots y_u$ such that

$$x_1x_2\cdots x_ry_1y_2\cdots y_u|Q|x_1^{m_1-1}x_2^{m_2-1}\cdots x_r^{m_r-1}y_1y_2\cdots y_u$$

and

$$|Q| = p - 3.$$

By Eq. (8), there is subsequence R of A such that $|R| = 3$ and RQ is a zero-sum subsequence. Now, $RQ = x_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}y_1y_2\cdots y_uZ$ with $Z \mid z_1z_2\cdots z_v$, where $1 \leqslant l_i \leqslant m_i - 1$ for all $i = 1, 2, \ldots, r$. Since $m_1 + m_2 + \cdots + m_r - r + u + 1 = 2p - 1 - 2u - v - r + u + 1 = 2p - (u + v + r) = 2p - (p-2) > p$, by Lemma 2.5, S contains a zero-sum subsequence of length p. This completes the proof of Case 4.

Case 5: $u + v + r = p - 1$. In this case we have $r \geqslant 1$, and we can assume that

$$\{x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v\} = \mathbb{Z}_p \backslash \{a\},$$

for some $a \in \mathbb{Z}_p$. Without loss of generality, we may assume that $a = 0$. Therefore,

$$\{x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v\} = \mathbb{Z}_p \backslash \{0\}. \tag{9}$$

We distinguish sub-cases.

Sub-case 1: $r \geqslant 5$. Since $3r + 2u + v \leqslant 2p - 1$ *and* $u + v + r = p - 1$, $r - v = (3r + 2u + v) - 2(r + u + v) \leqslant 2p - 1 - 2(p-1) = 1$. Therefore, $v \geqslant r - 1 \geqslant 4$. Set

$$A = \{y_1, y_2, \ldots, y_u, z_1, z_2, \ldots, z_v\} \quad \text{and} \quad B = \{x_1, x_2, \ldots, x_r\}.$$

Then by Cauchy—Davenport's inequality (Theorem 2.4) and Theorem 2.1, we see that

$$\begin{aligned}\left|\sum_{u+v-1}(A)+\sum_{2}(B)\right| &\geqslant \min\{p,(u+v)+2r-3-1\}\\ &=\min\{p,p-1+r-4\}=p.\end{aligned}$$

Therefore, there are subsequences $A_0 \mid A$ and $B_0 \mid B$ such that $|A_0|=u+v-1, |B_0|=2$ and $\sigma(x_1x_2\cdots x_rB_0A_0)=0$. (here σ means the sum). Set $Q=x_1x_2\cdots x_rB_0A_0$. Then $|Q|=r+2+u+v-1=p$, and

$$Q=x_1^{l_1}x_2^{l_2}\cdots x_r^{l_r}y_1^{f_1}y_2^{f_2}\cdots y_u^{f_u}Z,$$

where $Z|z_1z_2\cdots z_v$, $1\leqslant l_i\leqslant 2\leqslant m_i-1$ and $l_i=2$ holds for exactly 2 of i, $0\leqslant f_1, f_2, \ldots, f_u\leqslant 1$ and at most one of $f_i=0$. Since $m_1+m_2+\cdots+m_r-r+u+1-1=2p-1-v-u-r=p$, by Lemma 2.5, S contains a zero-sum subsequence of length p.

Sub-case 2: $r\leqslant 4$ *and* $\max\{m_i\}\geqslant 6$. Without loss of generality, we may assume that $m_1\geqslant 6$.

Let $A=\{y_1,y_2,\ldots,y_u,z_1,z_2,\ldots,z_v\}$. By Theorem 2.1, we have $\sum_{u+v-2}(A)=\mathbb{Z}_p$. Set $Q=x_1^4x_2x_3\cdots x_r$. Then there is a subsequence R of $y_1y_2\cdots y_uz_1z_2\cdots z_v$ such that $|R|=u+v-2$ and $\sigma(QR)=0$. Set $W=QR$. Then $W=x_1^4x_2x_3\cdots x_rR$. Note that $4(m_1-4)+(m_2-1)+\cdots+(m_r-1)+u-2+1\geqslant 2m_1-2+m_2-1+\cdots+m_r-1+u-1=m_1+(m_1+m_2+\cdots+m_r)+u-r-2=m_1+(2p-1-2u-v)+u-r-2=m_1+p-2>p$. Now the theorem follows from Lemma 2.5.

Sub-case 3: $r\leqslant 4$ and $\max\{m_i\}\leqslant 5$. Since $\mathbb{Z}_p\oplus\mathbb{Z}_p$ is the union of its $p+1$ subgroups each of order p, there exists a subgroup H of $\mathbb{Z}_p\oplus\mathbb{Z}_p$ such that $|H|=p$ and

$$(a_i,b_i)-(a_j,b_j)\in H$$

holds for at least $\frac{(2p-1)(2p-2)}{2(p+1)}>2p-5$ pairs. Therefore, by choosing suitable automorphism to act on S, we may assume that

$$H=\{(0,g)\mid g\in\mathbb{Z}_p\}$$

and

$$a_i=a_j$$

holds for at least $2p-4$ pair of $1\leqslant i<j\leqslant 2p-1$. But by assumption, we see that $r\leqslant 4$ and $\max\{m_i\}\leqslant 5$ implies that the number of the pairs of $1\leqslant i<j\leqslant 2p-1$ which satisfying

$$a_i=a_j$$

is at most

$$\frac{m_1(m_1-1)}{2}+\frac{m_2(m_2-1)}{2}+\cdots+\frac{m_r(m_r-1)}{2}+u\leqslant 10r+u\leqslant 40+u<2p-4,$$

as $u<p-1$. This contradiction shows that we can act on S with suitable automorphism and reduce it to the above cases. Thus the proof of the theorem is complete. $\square$

Proof of Theorem 1. Let S be a square-free sequence in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ of length $2p-1$. Let T be the first co-ordinate sequence of S. Set $k = [\sqrt{4p-7}] + 1$. If $h(T) \geqslant k+1$, then the theorem follows from Proposition 3.6. If $h(T) \leqslant k$ and $u+v+r \leqslant \frac{p-1}{4}$, then it follows from Proposition 3.5. So, let $h(T) \leqslant k$ and $u+v+r > \frac{p-1}{4}$ and the theorem follows from Proposition 3.7. $\square$

Proof of Corollary 1. Let S be a sequence in $\mathbb{Z}_p \oplus \mathbb{Z}_p$ of length $4p-3$. By our assumption, $h(S) \leqslant 2$. Hence, by Pigeon hole principle, we see that S has a square-free subsequence R of length at least $2p-1$. Hence, by Theorem 1, R does has a zero-sum subsequence of length p and so does S. $\square$

4. Concluding remarks

In this section, we shall prove an equivalent criterion for Conjecture 1 when n is even and using that we verify Conjecture 1 for $n=4$.

Theorem 4.1. *Let $n \geqslant 4$ be any even integer. Then the following two conditions are equivalent*:

(1) $g(\mathbb{Z}_n \oplus \mathbb{Z}_n) = 2n+1$.
(2) *Every square-free zero-sum sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ of length $2n+1$ has a zero-sum subsequence of length n.*

Proof. Clearly, (1) implies (2). Assuming (2) we want to prove (1). Let $S = \prod_{i=1}^{2n+1} a_i$ be any square-free sequence in $\mathbb{Z}_n^2$ of length $2n+1$. Set $a = \sum_{i=1}^{2n+1} a_i$, and consider the shifted sequence $R = \prod_{i=1}^{2n+1}(a_i - a)$. Clearly, R is a square-free sequence of length $2n+1$. Moreover, we see that

$$\sigma(R) = \sum_{i=1}^{2n+1}(a_i - a) = \sum_{i=1}^{2n+1} a_i - (2n+1)a = \sum_{i=1}^{2n+1} a_i - a = 0.$$

Therefore, by the assumption (2), R contains a zero-sum subsequence $\prod_{j=1}^{n}(a_{i_j} - a)$ of length n. Hence, $\prod_{j=1}^{n} a_{i_j}$ is a zero-sum subsequence of S of length n. This completes the proof. $\square$

Theorem 4.2. $g(\mathbb{Z}_4 \oplus \mathbb{Z}_4) = 9$.

Proof. We know that $g(\mathbb{Z}_4 \oplus \mathbb{Z}_4) \geqslant 9$. So, it is enough to prove the upper bound. Let S be a square-free sequence in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ of length 9. By Theorem 4.1, it is enough to assume that S is a zero-sum sequence.

First we assume that 0, the zero element of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ does not appearing in S. Then either there exists an element x together with $-x$ appearing in S or the three distinct elements of order 2 appearing in S.

In the first case, we get a zero-sum subsequence $T = Sx^{-1}(-x)^{-1}$ of length 7. But T cannot be minimal zero-sum sequence as its length is $2n-1 = D(\mathbb{Z}_4 \oplus \mathbb{Z}_4) = 7$ (here $D(\mathbb{Z}_n \oplus \mathbb{Z}_n)$ is the Davenport's constant for the group $\mathbb{Z}_n \oplus \mathbb{Z}_n$ which is defined as the smallest positive integer t such that any sequence in $\mathbb{Z}_n \oplus \mathbb{Z}_n$ of length at least t has a zero-sum subsequence) because any minimal zero-sum sequence of length 7 in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ contains an element which is appearing at least 3 times. (see for instance, Proposition 4.2 in [17]). Hence, T has a zero-sum subsequence of length <7. Since every element of T is non-zero, T has a zero-sum subsequence R of length at least 2. By taking R or TR^{-1}, we can as well assume that the length of R is 2 or 3 or 4. If $|R| = 3$, then $|TR^{-1}| = 4$ and we are done. Otherwise, i.e, if $|R| = 2$, then we have $Rx(-x)$ is a zero-sum subsequence of length 4 of S.

In the second case, that is, if all the three $(2,0), (0,2), (2,2)$ elements of order 2 are appearing in S, then $T = S(0,2)^{-1}(2,0)^{-1}(2,2)^{-1}$ and does not contain a zero-sum subsequence of length 2. This means for some $x \in \mathbb{Z}_4 \oplus \mathbb{Z}_4$ and $v_x(T) = 1$ implies $v_{-x}(T) = 0$. That is, all the other elements of order 4 is appearing in T without their respective inverses. So, $(3,2)$ or $(1,2)$ appears in S. Without loss of generality we may assume that $(3,2)$ appears in S (otherwise, we consider $-S$ instead of S). Then we can assume that $(3,0)$ does not appear because otherwise $(2,0), (0,2), (3,2), (3,0)$ forms a zero-sum subsequence of length 4. Hence, $(1,0)$ has to appear in T as its inverse $(3,0)$ does not appear in T. But, $(3,2) + (1,0) = (0,2)$ which would imply $(2,2), (2,0), (3,2), (1,0)$ is a zero-sum subsequence of length 4.

So, it remains to consider the case that 0 appears in S. Set $T = S0^{-1}$, then T is a zero-sum subsequence of length 8. Since $D(\mathbb{Z}_4 \oplus \mathbb{Z}_4) = 7$, (well-known Davenport Constant for the group $(\mathbb{Z}_4 \oplus \mathbb{Z}_4)$) T contains a proper zero-sum subsequence R. Then, TR^{-1} is also a zero-sum subsequence. Let W be the smaller (in length) one of R and TR^{-1}. Then, $|W| = 2, 3, 4$. We may assume that $|W| = 2$. Suppose $W = x(-x)$. Let $y \in TW^{-1}$. Set $T_1 = Tx^{-1}y^{-1}$. Clearly, T_1 is not zero-sum. Again by using Proposition 4.2 in [17], we obtain that $T_1(-\sigma(T_1))$ contains a proper zero-sum subsequence. Hence, T_1 contains a proper zero-sum subsequence W_1. Then, $|W_1| = 2, 3, 4, 5$. We may assume that $|W_1| = 2, 5$. If $|W_1| = 5$, then $TW_1^{-1}(0)$ is a zero-sum subsequence of S of length 4 and we are done. If $|W_1| = 2$ then WW_1 is a zero-sum subsequence of length 4. Thus the theorem follows. $\square$

Remark. In the similar spirit as Theorem 4.1, when n is odd, we can give an equivalent condition for Conjecture 1 as follows. *Every zero-sum sequence S of length $2n$ which has a square-free subsequence of length $2n-1$ has a zero-sum subsequence of length n.* We omit the proof of this fact.

Acknowledgments

W.D. Gao supported by NSFC with Grant No. 19971058 and 10271080. We thank the referee/s for his/her useful suggestions to improve the presentation of the paper.

References

[1] N. Alon, M.B. Nathanson, I.Z. Ruzsa, Adding distinct congruence classes modulo a prime, *Amer.* Math. Monthly 102 (3) (1995) 250–255.
[2] N. Alon, M.B. Nathanson, I.Z. Ruzsa, Polynomial methods and restricted sums of congruence classes, J. Number Theory 56 (2) (1996) 404–417.
[3] J. Bierbrauer, Y. Edel, Bounds on affine caps, J. Combin. Des. 10 (2) (2002) 111–115.
[4] J.L. Brenner, Problem 6298, Amer. Math. Monthly 89 (1982) 279–280.
[5] T.C. Brown, J.P. Buhler, A density version of a geometric Ramsey theorem, J. Combin. Theory Ser. A 32 (1) (1982) 20–34.
[6] A.L. Cauchy, Recherches sur les nombers, J. Ecole Polytech. cashier 16 9 (1813) 99–123.
[7] H. Davenport, On the addition of residue classes, J. London Math. Soc. 10 (1935) 30–32.
[8] J.A. Dias De Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. London Math. Soc. 26 (2) (1994) 140–146.
[9] Y. Edel, S. Ferret, I. Landjev, L. Storme, The classification of the largest caps in AG$(5, 3)$, J. Combin. Theory Ser. A 99 (1) (2002) 95–110.
[10] P. Erdős, A. Ginzburg, A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel 10F (1961) 41–43.
[12] P. Frankl, R.L. Graham, V. Rödl, On subsets of abelian groups with no three term arithmetic progression, J. Combin. Theory Ser. A 45 (1) (1987) 157–161.
[13] W.D. Gao, An addition theorem for finite cyclic groups, Discrete Math. 163 (1–3) (1997) 257–265.
[14] W.D. Gao, A note on a zero—sum problem, J. Combin. Theory Ser. A 95 (2) (2001) 387–389.
[15] W.D. Gao, On zero—sum subsequences of restricted size—II, Discrete Math. 271 (1–3) (2003) 51–59.
[17] W.D. Gao, A. Geroldinger, On zero—sum sequences in $\mathbb{Z}_n \oplus \mathbb{Z}_n$, Integers 3 (A8) (2003) 45 (electronic).
[18] H. Harborth, Ein Extremalproblem Für Gitterpunkte, J. Reine Angew. Math. 262/263 (1973) 356–360.
[19] A. Kemnitz, Extremalprobleme für Gitterpunkte, Ph.D. Thesis, Technische Universität Braunschweig, 1982.
[20] A. Kemnitz, On a lattice point problem, Ars Combinatorica 16b (1983) 151–160.
[21] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progression, J. Combin. Theory Ser. A 71 (1) (1995) 168–172.
[24] L. Rónyai, On a conjecture of Kemnitz, Combinatorica 20 (4) (2000) 569–573.
[25] B. Sury, R. Thangadurai, Gao's conjecture on zero—sum sequences, Proceedings of Indian Academic Sciences (Math. Sci.), Vol. 112, No. 3, 2002, pp. 399–414.
[26] R. Thangadurai, On a conjecture of Kemnitz, C. R. Math. Acad. Sci. Soc. R. Can. 23 (2) (2001) 39–45.