HIGHER DEGREE ERDŐS-GINZBURG-ZIV CONSTANTS

Yair Caro
Department of Mathematics, University of Haifa-Oranim, Israel
yacaro@kvgeva.org.il

John R. Schmitt
Department of Mathematics, Middlebury College, Middlebury, Vermont, USA
jschmitt@middlebury.edu

Received: , Revised: , Accepted: , Published:

Abstract

We generalize the notion of Erdős-Ginzburg-Ziv constants – along the same lines we generalized in earlier work the notion of Davenport constants – to a "higher degree" and obtain various lower and upper bounds. These bounds are sometimes exact as is the case for certain finite commutative rings of prime power cardinality. We also consider to what extent a theorem due independently to W.D. Gao and the first author that relates these two parameters extends to this higher degree setting. Two simple examples that capture the essence of these higher degree Erdős-Ginzburg-Ziv constants are the following. 1) Let $\nu_p(m)$ denote the p-adic valuation of the integer m. Suppose we have integers $t|\binom{m}{2}$ and $n = t + 2^{\nu_2(m)}$; then every sequence S over $\mathbb{Z}_2$ of length $|S| \geq n$ contains a subsequence S' of length t for which $\sum_{a_{i_1},\ldots,a_{i_m} \in S'} a_{i_1} \cdots a_{i_m} \equiv 0 \pmod 2$, and this is sharp. 2) Suppose $k = 3^\alpha$ for some integer $\alpha \geq 2$. Then every sequence S over $\mathbb{Z}_3$ of length $|S| \geq k + 6$ contains a subsequence S' of length k for which $\sum_{a_h,a_i,a_j \in S'} a_h a_i a_j \equiv 0 \pmod 3$. These examples illustrate that if a sequence of elements from a finite commutative ring is long enough, there exists a subsequence of prescribed length for which a certain symmetric expression (symmetric polynomial) has to vanish on it. The Erdős-Ginzburg-Ziv Theorem is just the case where a sequence of length $2n-1$ over $\mathbb{Z}_n$ contains a subsequence $S' = (a_1, \ldots, a_n)$ of length n that vanishes when substituted in the linear symmetric polynomial $x_1 + \cdots + x_n$.

1. Introduction

Throughout this paper, let p denote a prime number and $q = p^\alpha$ a prime power.

Let G be a finite abelian group with $exp(G)$ its exponent. Then for $g_i \in G$,

$$S = (g_1, \ldots, g_\ell) = \prod_{g \in G} g^{v_g(S)}$$

is called a *sequence over* G, where order is disregarded, repetition is allowed and the exponent $v_g(S)$ indicates the number of repetitions of the element g in S. Its *length*, denoted $|S|$, is the number of elements counted with multiplicity, i.e. $|S| = \sum_{g\in G} v_g(S)$. A sequence of G is said to be *zero-sum* if the sum of its elements is zero in G. A sequence S of G is said to be *zero-sum free* if every non-trivial subsequence of S has sum different to zero.

For a group G, the *Davenport constant of* G, which we denote by $\mathsf{D}(G)$, is the smallest positive integer z such that every sequence S over G of length $|S| \geq z$ contains a non-empty zero-sum subsequence, that is, S is not zero-sum free. For a group G, the *Erdős-Ginzburg-Ziv constant of* G is the smallest positive integer z such that every sequence of length $|S| \geq z$ contains a zero-sum subsequence of length $|G|$.

These two constants have been well-studied; see, for instance, the survey paper of W.D. Gao and A. Geroldinger [17]. We recall some of the earlier statements as follows.

Recall that by the Fundamental Theorem of Finite Abelian Groups, for any finite non-trivial abelian group G there exist integers $n_1, \ldots, n_r$ with $1 < n_1 | \ldots | n_r$ so that G can be written uniquely as

$$G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r},$$

where the integer r is called the *rank* of G and denoted $r(G)$. We use $\mathsf{d}^*(G)$ to denote the value $\sum_{i=1}^{r}(n_i - 1)$.

The value of $\mathsf{D}(G)$ was determined independently by J.E. Olson [22] and D. Kruyswijk [13] when G is a p-group, and by J.E. Olson [23] when G has rank at most 2.

Theorem 1 (J.E. Olson [22], [23], and D. Kruyswijk [13])**.** *If G is a p-group or $r(G) \leq 2$, then $\mathsf{D}(G) = 1 + \mathsf{d}^*(G)$.*

P. Erdős, A. Ginzburg, A. Ziv [15] showed that for the cyclic group $\mathbb{Z}_k$ the smallest positive integer z such that every sequence of length $|S| \geq z$ contains a zero-sum subsequence of length $|\mathbb{Z}_k| = k$ is $2k - 1$.

One particular exciting result that connects these two constants is due independently to W.D. Gao [16] and Y. Caro [8],[9].

Theorem 2 (Caro and Gao's $n + \mathsf{D} - 1$ Theorem [16], [8], [9])**.** *Let G be a finite abelian group of order n. The Erdős-Ginzburg-Ziv constant of G equals $n+\mathsf{D}(G)-1$.*

One of the aims of this paper is to explore to what extent this theorem may be generalized. To do so, we first generalize the definition of these two constants, the former of which was previously done in work of the authors [10] and given again here.

Let $(G,+,\cdot)$ be a finite commutative ring. For any positive integer m and any sequence $S=(g_1,\ldots,g_\ell)$ over G, we set

$$e_m(S) := \sum_{1\le i_1<\cdots<i_m\le \ell} \prod_{j=1}^{m} g_{i_j},$$

noting that operations are done coordinate-wise.

The introduction of this m-th degree symmetric polynomial expression given above allows for a generalization of both the Davenport constant and the Erdős-Ginzburg-Ziv constant since both of these constants concern themselves with the vanishing of subsequences (with perhaps additional properties) on linear symmetric polynomial expressions. We also mention that the question of the vanishing of a subsequence over certain symmetric polynomials has already appeared in [1], [5], and [6].

We denote by $\mathsf{D}(G,m)$ the smallest positive integer z such that every sequence S over G of length $|S|\ge z$ contains a subsequence S' of length $|S'|\ge m$ for which $e_m(S')$ equals the zero-element in G. Notice that when $m=1$ we recover the classical Davenport constant discussed above. That is, $\mathsf{D}(G,1)=\mathsf{D}(G)$ and in this case we prefer to use the notation $\mathsf{D}(G)$. As a result and as $e_m(S)$ is a sum of products of degree m, we may consider $\mathsf{D}(G,m)$ as the *m^{th}-degree Davenport constant*. For results on $\mathsf{D}(G,m)$, we refer the reader to earlier work done by the authors [10].

For a finite commutative ring G, we denote by $\mathsf{EGZ}(t,G,m)$ the smallest positive integer z such that every sequence S over G of length $|S|\ge z$ contains a subsequence S' of length t for which $e_m(S')$ evaluates to the zero-element in G. If no such z exists, we define $\mathsf{EGZ}(t,G,m)=\infty$.

Of particular interest are cyclic groups $\mathbb{Z}_k$. For integers k and m, we define $S(k,m) := \{t : t\ge m \text{ and } k \mid \binom{t}{m}\}$. For $k\ge 2, m\ge 1$ and $t\in S(k,m)$, we denote by $\mathsf{EGZ}(t,\mathbb{Z}_k,m)$ (or more simply $\mathsf{EGZ}(t,k,m)$) the smallest positive integer z such that every sequence S over $\mathbb{Z}_k$ of length $|S|\ge z$ contains a subsequence S' of length t for which $e_m(S')=0$. The value of this function in the case $m=1$ was given by P. Erdős, A. Ginzburg, A. Ziv [15] and is therefore called the *Erdős-Ginzburg-Ziv constant*; they gave $\mathsf{EGZ}(k,k,1)=2k-1$. As a result and as $e_m(S)$ is a sum of products of degree m, we may consider $\mathsf{EGZ}(t,G,m)$ as the *m^{th}-degree Erdős-Ginzburg-Ziv constant of G*.

Example 1.1. We give an example to show the usefulness of the condition $t\in S(k,m)$. Let $m=2, t=8$ and $\mathbb{Z}_{10}$, i.e. $k=10$. Let $S=(1^n)$ of length $n\ge t$. For any length 8 subsequence S' of S, we have $e_2(S')=\binom{8}{2}=28$, which is not divisible by 10.

Our results are as follows. We begin in Section 2 by providing a general lower bound on $\mathsf{EGZ}(t,G,m)$ for finite abelian groups G in terms of t,m and the m^{th}-

degree Davenport constant. In Subsection 2.1 we focus on the case of when G is a finite cyclic group, providing both lower and upper bounds for various instances of the parameters. In Subsection 2.1.1, we give a precise determination of the function in the case that the group is $\mathbb{Z}_2$, showing that a generalization of Caro and Gao's $n + \mathsf{D} - 1$ Theorem holds. Such a generalization also holds in the case of $\mathbb{Z}_{p^s}$ when t and m are powers of the same prime as shown in Theorem 12 and more generally for $p-$groups as shown as a consequence of Theorem 13. We frequently use polynomial methods or rely on results established using such methods. We conclude our discussion in Section 3 with a conjecture and two problems.

2. Results

First, we note an easy lower bound on $\mathsf{D}(\mathbb{Z}_n, m)$. Consider the sequence (1^t). If $t = m$, then the only subsequence of length at least m is the given sequence itself and $e_m((1^t)) = 1 \not\equiv 0 \pmod{n}$. Further, suppose that for each ℓ with $t > \ell \geq m$ we have $\binom{\ell}{m} \not\equiv 0 \pmod{n}$. Then there does not exist a subsequence of (1^t) of length at least m which evaluates to zero modulo n. Thus, we define $L(n, m)$ to be the smallest integer $\ell \geq m + 1$ such that $\binom{\ell}{m} \equiv 0 \pmod{n}$. We have

$$\mathsf{D}(\mathbb{Z}_n, m) \geq L(n, m). \tag{1}$$

Clearly, if $t \in S(k, m)$, then $t \geq max\{m + 1, L(k, m)\}$. Also, note that for k odd and $k \geq 3$ we have $L(k, 2) = k$.

As a first step towards exploring a Caro and Gao-type connection between the m^{th}-degree Davenport constant and the m^{th}-degree Erdős-Ginzburg-Ziv constant, we provide a general lower bound on the latter.

Theorem 3. *Let G be a finite abelian group (considered as a finite commutative ring). Then $\mathsf{EGZ}(t, G, m) \geq t + \mathsf{D}(G, m) - m$.*

Proof. If $\mathsf{EGZ}(t, G, m) = \infty$, we are done. So, we may consider the cases where this parameter is finite.

Begin by noting that, by definition, we have $\mathsf{D}(G, m) \geq m + 1$. Let S^* be a sequence over G of length $\mathsf{D}(G, m) - 1$ containing no subsequence S^{**} for which $e_m(S^{**}) = 0$. That is, S^* is an extremal sequence for the m^{th} degree Davenport constant. Notice that S^* does not contain the zero-element since otherwise any subsequence S^{**} of length m containing this zero-element would have $e_m(S^{**}) = 0$. Let $S = (0^{t-m}, S^*)$, which has length $t + \mathsf{D}(G, m) - m - 1 \geq t$. We will show that S contains no subsequence S' of length t for which $e_m(S') = 0$. Any such sequence must have $t - j$ $0'$s and j elements of S^*, where $m \leq j \leq \mathsf{D}(G, m) - 1$. We then have that $e_m(S') = e_m(S^{**})$ for some S^{**} a subsequence of S^*. However, by construction, $e_m(S^{**}) \neq 0$, and so $e_m(S') \neq 0$. □

So, compare Theorem 3 to Theorem 2. We will show that in particular cases equality holds in Theorem 3 but does not hold in general. Note that Inequality (1) and Theorem 3 immediately yield the following.

Corollary 1. *For $t \in S(k,m)$, we have $\mathsf{EGZ}(t,k,m) \geq t + L(k,m) - m$.*

2.1. Results for cyclic groups

Proposition 1. *For $t \in S(k,m)$, we have $\mathsf{EGZ}(t,k,m) \leq (k-1)(t-1)+t-m+1 = k(t-1)-m+2$.*

Proof. Let S be a sequence over $\mathbb{Z}_k$ of length $(k-1)(t-1)+t-m+1$. If some non-zero element g appears t times, then there exists a subsequence $S' = (g^t)$ and we have $e_m(S') = g^m\binom{t}{m} \equiv 0 \pmod{k}$. This implies that there are at most $(k-1)(t-1)$ non-zero elements in S and at least $t-m+1$ elements which are 0. We may form the length-t subsequence $S'' = (0^{t-m+1}, g_1, g_2, \ldots, g_{m-1})$. It is easy to see that $e_m(S'') = 0$. □

Going further, while Proposition 1 gives that $\mathsf{EGZ}(3,3,2) \leq 6$, it is not hard to see that equality, in fact, holds by considering the length-5 sequence $S = (0, 1^2, 2^2)$ over $\mathbb{Z}_3$ and checking that for every subsequence S' of S with $|S'| = 3$, one has $e_2(S') \not\equiv 0 \pmod{3}$.

Now consider the following result given in [10].

Proposition 2 ([10])**.** *For a prime p and integers s and u, we have $L(p^s, p^u) = p^{s+u}$.*

Example 2.1. By Proposition 2, we have $L(5,5) = 25$. Together with Theorem 1, we have $\mathsf{EGZ}(25,5,5) \geq 45$. Theorem 12 given below will show this bound is sharp.

Theorem 4. *Let k be odd and let r be an integer such that $r|k|r^2$. Then $\mathsf{D}(\mathbb{Z}_k, 2) \leq k+r$.*

Proof. Let $S = (g_1, \ldots, g_{k+r})$ be a sequence over $\mathbb{Z}_k$ of length $k+r$. Consider the following sequence over $\mathbb{Z}_r \oplus \mathbb{Z}_k$: $([g_1, g_1^2], \ldots [g_{k+r}, g_{k+r}^2])$. As $r|k$ the group $\mathbb{Z}_r \oplus \mathbb{Z}_k$ is a rank-2 abelian group and so we may apply the Olson's Theorem (i.e. Theorem 1) which says that $\mathsf{D}(\mathbb{Z}_r \oplus \mathbb{Z}_k) = k+r-1$. That is, we have that there is a non-empty subset $J \subset [k+r]$ such that $\sum_{j\in J} g_j \equiv 0 \pmod{r}$ and $\sum_{j\in J} g_j^2 \equiv 0 \pmod{k}$. We show that there exists such a J such that $|J| \geq 2$. If not, then $|J| = 1$ and so $g_1 = 0$. Remove this element from the sequence S to obtain $S \setminus g_1$. Apply Olson's Theorem to this sequence and obtain a J' with the same properties as J. If $|J'| = 1$ also, then $|J \cup J'| \geq 2$. So we now may assume that we have a J such that $|J| \geq 2$. Observe that $(\sum_{j\in J} g_j)^2 = \sum_{j\in J} g_j^2 + 2\sum_{i,j\in J, i\neq j} g_i g_j$. Since $\sum_{j\in J} g_j \equiv 0 \pmod{r}$, it follows that $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{r^2}$. As $k|r^2$, we have $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{k}$. We now have that $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{k}$ *and* $\sum_{j\in J} g_j^2 \equiv 0 \pmod{k}$,

implying that $2\sum_{i,j\in J,i\neq j} g_ig_j \equiv 0 \pmod{k}$. However, as k is odd it follows that $\sum_{i,j\in J,i\neq j} g_ig_j \equiv 0 \pmod{k}$. Let S' be the subsequence of S as chosen by J; then $e_2(S') \equiv 0 \pmod{k}$.

□

Theorem 5. *Suppose that k is odd.*

1. *Let $\ell \geq 1$, and let r be an integer such that $r|k|r^2$. Then $\mathsf{EGZ}(\ell k, k, 2) \leq (\ell+1)k + 2r - 3$. In particular, if $k = r^2$, then $\mathsf{EGZ}(k, k, 2) \leq 2r^2 + 2r - 3$.*
2. *$\mathsf{EGZ}(k, k, 2) \geq k + \mathsf{D}(\mathbb{Z}_k, 2) - 2$.*
3. *In the case that $k = p$ is an odd prime: for $p \equiv 1 \pmod{4}$ we have $\mathsf{EGZ}(p, p, 2) \geq 2p - 1$ and for $p \equiv 3 \pmod{4}$ we have $\mathsf{EGZ}(p, p, 2) \geq 2p$.*

Before giving the proof of Theorem 5, we need to recall a celebrated result that we use in the proof. In 2007 C. Reiher [24] used the Chevalley-Warning Theorem and combinatorial arguments to establish a well-known conjecture of A. Kemnitz; Reiher proved that the minimum number of points one needs to take from $\mathbb{Z}_n \oplus \mathbb{Z}_n$ so that there always exists n of them summing to $(0, 0)$ is $4n-3$. This was generalized in [18] as follows.

Theorem 6 (C. Reiher [24]; A. Geroldinger, F. Halter-Koch [18])**.** *Let $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $1 \leq n_1|n_2$. Then $\mathsf{EGZ}(n_2, \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}, 1) = 2n_1 + 2n_2 - 3$.*

For further remarks and results on $\mathsf{EGZ}(k, \mathbb{Z}_k^d, 1)$, we point the reader to the works of N. Alon and M. Dubiner [2, 3] and Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham [12]. We now proceed to the proof of Theorem 5.

Proof. 1. Let $S = (g_1, \ldots, g_{(\ell+1)k+2r-3})$ be a sequence over $\mathbb{Z}_k$. Recall a basic algebraic fact: $2\sum_{1\leq i\neq j\leq d} g_ig_j = (g_1 + \cdots + g_d)^2 - (g_1^2 + \cdots + g_d^2)$. Consider the following sequence over $\mathbb{Z}_r \oplus \mathbb{Z}_k$:

$$([g_1, g_1^2], \ldots [g_{(\ell+1)k+2r-3}, g_{(\ell+1)k+2r-3}^2]).$$

As $r|k$ the group $\mathbb{Z}_r \oplus \mathbb{Z}_k$ is a rank-2 abelian group with exponent k. For this group, by Theorem 6 as $r|k$ we have $\mathsf{EGZ}(k, \mathbb{Z}_r \oplus \mathbb{Z}_k, 1) = 2k + 2r - 3$. That is, we have that there exists ℓ disjoint non-empty subsets $J_1, \ldots, J_\ell \subset [(\ell+1)k+2r-3]$ with $|J_m| = k$ for $1 \leq m \leq \ell$ such that $\sum_{j\in J_m} g_j \equiv 0 \pmod{r}$ and $\sum_{j\in J_m} g_j^2 \equiv 0 \pmod{k}$. Let $J := \cup_{m=1}^{\ell} J_m$. It follows that $\sum_{j\in J} g_j \equiv 0 \pmod{r}$ and $\sum_{j\in J} g_j^2 \equiv 0 \pmod{k}$. Since $\sum_{j\in J} g_j \equiv 0 \pmod{r}$, it follows that $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{r^2}$. As $k|r^2$, we have $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{k}$. We now have that $(\sum_{j\in J} g_j)^2 \equiv 0 \pmod{k}$ *and* $\sum_{j\in J} g_j^2 \equiv 0 \pmod{k}$, implying that $2\sum_{i,j\in J,i\neq j} g_ig_j \equiv 0 \pmod{k}$. However, as k is odd it follows that $\sum_{i,j\in J,i\neq j} g_ig_j \equiv 0 \pmod{k}$. Let S' be the subsequence of S as chosen by J, then $e_2(S') \equiv 0 \pmod{k}$.

2. By Theorem 3, if $t \in S(k,m)$, then $\mathsf{EGZ}(t,k,m) \geq \mathsf{D}(\mathbb{Z}_k,m)+t-m$. For $k \geq 3$, we have $k \in S(k,2)$ if and only if k is odd. Thus, $\mathsf{EGZ}(k,k,2) \geq \mathsf{D}(\mathbb{Z}_k,2)+k-2$.

3. By a result in [10] (see Section 5 of [10]), we have $\mathsf{D}(\mathbb{Z}_p,2) \geq p+1$ for any prime and a stronger bound holds in the case that $p \equiv 3 \pmod 4$ of $\mathsf{D}(\mathbb{Z}_p,2) \geq p+2$. By this result and Part 2, the result follows.

□

Remark 1. Note that the condition of p being an odd prime given in Theorem 5.3 is necessary as $S=(1^t)$ shows that $\mathsf{EGZ}(2,2,2)=\infty$.

Theorem 7. *The following hold.*

1. *Let k,m be positive integers such that $\gcd(k,m!)=1$. Then $\mathsf{EGZ}(k,k,m) \leq \mathsf{EGZ}(k,\mathbb{Z}_k^{\lceil \frac{m+1}{2} \rceil},1)$. More strongly, if $\gcd(k,3)=1$, then $\mathsf{EGZ}(k,k,3) \leq 4k-3$.*

2. *Let k be a positive integer such that $\gcd(k,3)=1$ (i.e. $k \equiv 1,2 \pmod 3$). Then $\mathsf{EGZ}(k,k,3) \geq k+\mathsf{D}(\mathbb{Z}_k,3)-3$.*

3. *Let q be a prime power. Then $\mathsf{EGZ}(q,q,3) \geq 2q-3$.*

Before giving the proof of this theorem, we need to remind the reader of some classical results.

For $m \geq 0$, the *elementary symmetric polynomial of degree m* is the sum of all distinct products of m distinct variables. Thus, $e_0(x_1,\ldots,x_n)=1, e_1(x_1,\ldots,x_n)=x_1+\cdots+x_n, e_2(x_1,\ldots,x_n)=\sum_{1\leq i<j\leq n} x_ix_j$ and, so on, until, $e_n(x_1,\ldots,x_n)=x_1x_2\ldots x_n$. The *$m$-th power sum polynomial* is $p_m(x_1,\ldots,x_n)=\sum_{i=1}^n x_i^m$.

We now state a historical set of relations between the elementary symmetric polynomials and the power sum polynomials. These 17th-century relations are independently due to Albert Girard and Isaac Newton and known as the Girard-Newton formulae (or sometimes Newton's identities); for more about these identities, see [4].

Theorem 8 (Girard-Newton formulae)**.** *For all $n \geq 1$ and $1 \leq m \leq n$, we have*

$$me_m(x_1,\ldots,x_n)=\sum_{i=1}^{m}(-1)^{i-1}e_{m-i}(x_1,\ldots,x_n)p_i(x_1,\ldots,x_n). \tag{2}$$

We may rewrite Equation (2) in a manner that is independent of the number of variables, that is, we may rewrite Equation (2) in the ring of symmetric functions as

$$me_m=\sum_{i=1}^{m}(-1)^{i-1}e_{m-i}p_i. \tag{3}$$

One may use the Girard-Newton formulae to recursively express elementary symmetric polynomials in terms of power sums as follows:

$$e_m = (-1)^m \sum \prod_{i=1}^{m} \frac{(-p_i)^{j_i}}{j_i! i^{j_i}}, \tag{4}$$

where the sum extends over all solutions to $j_1 + 2j_2 + \cdots + mj_m = m$ such that $j_1, \ldots, j_m \geq 0$. For example, we have $e_1 = p_1,\ e_2 = \frac{1}{2}p_1^2 - \frac{1}{2}p_2,\ e_3 = \frac{1}{6}p_1^3 - \frac{1}{2}p_1p_2 + \frac{1}{3}p_3,\ e_4 = \frac{1}{24}p_1^4 - \frac{1}{4}p_1^2p_2 + \frac{1}{8}p_2^2 + \frac{1}{3}p_1p_3 - \frac{1}{4}p_4$. If we multiply both sides of Equation (4) by $m!$, then we obtain integer coefficients on the right side.

Notice that for Equation (4), each term in the sum of the right side is a product that contains at most m distinct power sum polynomials. For a fixed m we call a set T of power sum polynomials a *dominating set for* e_m if each term in the sum contains at least one member of T. Let $t(m)$ denote the size of the smallest dominating set. For $m = 1$, the only dominating set is $\{p_1\}$, and so $t(1) = 1$. For $m = 2$, the only dominating set is $\{p_1, p_2\}$, and so $t(2) = 2$. For $m = 3$, any dominating set must contain both p_1 and p_3 and $\{p_1, p_3\}$ is a dominating set, and so $t(3) = 2$. More generally, the following was determined previously.

Lemma 1 ([10])**.** *We have $t(m) = \frac{m+2}{2}$ when m is even, and $t(m) = \frac{m+1}{2}$ when m is odd.*

We are now able to give the proof of Theorem 7

Proof. 1. Let $C = \mathsf{EGZ}(k, \mathbb{Z}_k^{t(m)}, 1)$ and let $S = (g_1, \ldots, g_C)$ be a sequence over $\mathbb{Z}_k$. Let $D(m) := \{d_1, d_2, \ldots, d_{t(m)}\}$ be the exponents of a dominating set of size $t(m)$. Consider the following sequence over $\mathbb{Z}_k^{t(m)}$:

$$([g_1^{d_1}, g_1^{d_2}, \ldots, g_1^{d_{t(m)}}], \ldots, [g_C^{d_1}, g_C^{d_2}, \ldots, g_C^{d_{t(m)}}]).$$

By the definition of $\mathsf{EGZ}(k, \mathbb{Z}_k^d, 1)$, we have that there is a subset $J \subset [C]$ such that $\sum_{j\in J}[g_j^{d_1}, g_j^{d_2}, \ldots, g_j^{d_{t(m)}}] = (0, \ldots, 0)$. Thus, $\sum_{j\in J} g_j^{d_1} \equiv 0 \pmod{k}$, $\sum_{j\in J} g_j^{d_2} \equiv 0 \pmod{k}$, and all the way to $\sum_{j\in J} g_j^{d_{t(m)}} \equiv 0 \pmod{k}$. Let S' be the sequence selected by J. We use the fact that the Girard-Newton formulae allow us to express $m!e_m$ as a sum whose terms consist of power sum polynomials. In this sum at least one factor in each term is equal to 0 (mod k) since through $D(m)$ we have created a dominating set. Thus, the sum is 0 (mod k). It follows that $e_m(S') \equiv 0 \pmod{k}$.

The stronger statement given in Theorem 7.1 follows by an application of Theorem 6, where the weaker *gcd* condition follows from the fact that by Equation (3) we have the expression $3e_3 = e_2p_1 - e_1p_2 + p_3$ and as $e_1 = p_1$ we may write $3e_3 = e_2p_1 - p_1p_2 + p_3$. The set $\{p_1, p_3\}$ is a dominating set for this expression.

2. By Theorem 3 if $t \in S(k,m)$, then $\mathsf{EGZ}(t,k,m) \geq \mathsf{D}(\mathbb{Z}_k,m)+t-m$. For $k \geq 4, k \in S(k,3)$ if and only if $k \not\equiv 0 \pmod 3$. Thus, $\mathsf{EGZ}(k,k,3) \geq k + \mathsf{D}(\mathbb{Z}_k,3)-3$.

3. The sequence $S = (1^{q-1})$ shows that $\mathsf{D}(\mathbb{Z}_q,3) \geq q$. Thus, $\mathsf{EGZ}(q,q,3) \geq q+\mathsf{D}(\mathbb{Z}_q,3)-3 = 2q-3$.

□

Problem 1. *Determine a lower bound for* $\mathsf{EGZ}(k,k,m)$ *for* $k \in S(k,m)$ *and an upper bound for* $\mathsf{EGZ}(k,k,m)$ *for all* k,m.

2.1.1. Exact determination for $\mathbb{Z}_2$

In order to prove a generalization of the Caro-Gao Theorem for the cyclic group of order 2, we need some preparatory lemmas. To prove these lemmas, we provide some necessary background.

Let p be a prime number and $n > 1$ an integer. The *p-adic valuation of n*, denoted $\nu_p(n)$, is the exponent of p in the canonical decomposition in prime numbers of n (and if p does not divide n, then $\nu_p(n) = 0$). The base-p expansion of n is written as such, $n = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0$.

Theorem 9 (E. Kummer, 1852 [21])**.** *The p-adic valuation of the binomial coefficient $\binom{n}{m}$ is equal to the number of 'carry-overs' when performing the addition in base p of $n-m$ and m.*

Recall Inequality (1): $\mathsf{D}(\mathbb{Z}_n,m) \geq L(n,m)$ and the discussion that precedes it. In particular, we have $\mathsf{D}(\mathbb{Z}_2,m) \geq L(2,m)$. Notice that any sequence S containing the element 0 has a subsequence S for which $e_m(S') = 0$. Any sequence S not containing 0 and of length $L(2,m)$, we have $e_m(S) \equiv 0 \pmod 2$.

Lemma 2. $\mathsf{D}(\mathbb{Z}_2,m) = m + 2^{\nu_2(m)}$.

Proof. Let m be a positive integer with 2−adic valuation $\nu_2(m)$.

Notice that any sequence S containing the element 0 has a subsequence S for which $e_m(S') = 0$. We will show that any sequence S not containing 0 and of length $m+2^{\nu_2(m)}$), that is $S = (1^{m+2^{\nu_2(m)}})$ we have $e_m(S) = \binom{m+2^{\nu_2(m)}}{m} \equiv 0 \pmod 2$ and sequences of shorter length do not have this property.

We begin by showing that for $m+1 \leq j < m+2^{\nu_2(m)}$ we have $\binom{j}{m} \not\equiv 0 \pmod 2$.

We will use Kummer's Theorem to compute 2-adic valuation of this binomial coefficient $\binom{j}{m}$: it is equal to the number of 'carry-overs' when performing the addition in base 2 of $j-m$ and m. Begin by noticing that base-2 expansion of m has 0's to the right of position $\nu_2(m)$ (and a 1 in position $\nu_2(m)$). That is, the base-2 expansion of m ends with $0\cdot 2^{\nu_2(m)-1}+\cdots+0\cdot 2^0$. As $m+1 \leq j < m+2^{\nu_2(m)}$, we have $1 \leq j-m < 2^{\nu_2(m)}$. Thus, the base-2 expansion does not have a 1 to the

left of position $\nu_2(m)$. Thus, when we add m and $j-m$ in base-2, there are no 'carry-overs'. By Kummer's Theorem, the 2-adic valuation of $\binom{j}{m}$ is 0. That is, 2 does not divide $\binom{j}{m}$ for $m+1 \leq j < m+2^{\nu_2(m)}$.

Now consider $j = m + 2^{\nu_2(m)}$. In this case, $j - m = 2^{\nu_2(m)}$. Thus, the base-2 expansion of $j-m$ is $1 \cdot 2^{\nu_2(m)}$. As m has a 1 in position $\nu_2(m)$, when we add m and $j-m$ in base-2 there is at least one 'carry-over'. Thus, some positive power of 2 divides $\binom{m+2^{\nu_2(m)}}{m}$. □

Lemma 3. *Suppose that $i \geq m + 2^{\nu_2(m)}$. Then for some j in the interval $[i - 2^{\nu_2(m)}, \ldots, i]$, we have $\binom{j}{m} \equiv 0 \pmod 2$.*

Proof. As the interval has length $2^{\nu_2(m)} + 1$, there exists some integer j with a 0 in position $\nu_2(m)$ of its base-2 expansion and $j - m \geq 2^{\nu_2(m)}$. As m has a 1 in position $\nu_2(m)$, $j-m$ has 1 in position $\nu_2(m)$ of the base-2 expansion. Thus, when we add m and $j-m$ in base-2 there is at least one 'carry-over'. Thus, by Kummer's Theorem, some positive power of 2 divides $\binom{j}{m}$. □

The next theorem shows that a generalized Caro-Gao Theorem holds in a particular case.

Theorem 10. *For $t \in S(2,m)$, we have $\mathsf{EGZ}(t,2,m) = t + 2^{\nu_2(m)} = t + \mathsf{D}(\mathbb{Z}_2, m) - m$.*

Proof. By Lemma 2, we only need show $\mathsf{EGZ}(t,2,m) = t + 2^{\nu_2(m)}$.

By Theorem 3, we have $\mathsf{EGZ}(t,2,m) \geq t + 2^{\nu_2(m)}$.

We now prove the upper bound. Let $S = (0^{t+2^{\nu_2(m)}-i}, 1^i)$ be a sequence of length $t + 2^{\nu_2(m)}$, where $0 \leq i \leq t + 2^{\nu_2(m)}$. We consider several cases, in each case showing that there exists a subsequence S' of length t such that $e_m(S') \equiv 0 \pmod 2$.

1. $i \geq t \geq m+1$.
   There exists the subsequence $S' = (1^t)$. As $t \in S(2,m)$, we have $e_m(S') = \binom{t}{2} \equiv 0 \pmod 2$.

2. $i \leq m-1$.
   Then the number of 0's that S contains is at least $t + 2^{\nu_2(m)} - i \geq t + 1 - i > t - i$. Let $S' = (0^{t-i}, 1^i)$. As each summand in $e_m(S')$ equals 0, we have $e_m(S') \equiv 0 \pmod 2$.

3. $m \leq i \leq m + 2^{\nu_2(m)} - 1$.
   Then the number of 0's that S contains is at least $t + 2^{\nu_2(m)} - i \geq t - m + 1$. Let $S' = (0^{t-m+1}, 1^{m-1})$. As each summand in $e_m(S')$ equals 0, we have $e_m(S') \equiv 0 \pmod 2$.

4. $m + 2^{\nu_2(m)} \leq i \leq t-1$.
   Then the number of 0′s that S contains is at least $t + 2^{\nu_2(m)} - i \geq 2^{\nu_2(m)} + 1$. By Lemma 3, there exists a $j \in [i - 2^{\nu_2(m)}, \ldots, i]$ such that $\binom{i-j}{m} \equiv 0 \pmod 2$. Let $S' = (0^{t-(i-j)}, 1^{(i-j)})$. Each summand in $e_m(S')$ is either 0 or 1, and the number of the latter is $\binom{i-j}{m}$. Thus, $e_m(S') = \binom{i-j}{m} \equiv 0 \pmod 2$.

□

2.2. Prime power parameters yield a Caro-Gao-type theorem

In this subsection, we investigate the $\mathsf{EGZ}(t,k,m)$ when the parameters are restricted to being powers of the same prime. Central to establishing our results here and later is the use of a tool from the polynomial method tool-kit, as follows.

Theorem 11 (U. Schauz [25], D. Brink [7])**.** *Let $P_1(t_1,\ldots,t_n),\ldots,P_r(t_1,\ldots,t_n)$ be polynomials in the ring $\mathbb{Z}[t_1,\ldots,t_n]$, let p be a prime, let $v_1,\ldots,v_r \in \mathbb{Z}^+$, let $A_1,\ldots,A_n$ be nonempty subsets of $\mathbb{Z}$ such that for each i, the elements of A_i are pairwise incongruent modulo p, and put $A = \prod_{i=1}^n A_i$. Let*

$$Z_A = \{x \in A \mid P_j(x) \equiv 0 \pmod{p^{v_j}}\ \forall 1 \leq j \leq r\},\ \mathbf{z}_A = \#Z_A.$$

a) If $\sum_{j=1}^r (p^{v_j}-1)\deg(P_j) < \sum_{i=1}^n (\#A_i - 1)$, then $\mathbf{z}_A \neq 1$.
b) (Boolean Case) If $A = \{0,1\}^n$ and $\sum_{j=1}^r (p^{v_j}-1)\deg(P_j) < n$, then $\mathbf{z}_A \neq 1$.

When we apply Theorem 11, most notably the Boolean Case, we will use a system of polynomials to encode the combinatorial problem in the zero set of this system. When applied, the Boolean Case will guarantee the existence of a non-zero boolean vector in the zero set. If the j^{th} entry of this vector is 1, then this will correspond to selecting the j^{th} entry of a given sequence S whereas 0 corresponds to not selecting this entry. In the proofs that make use of this theorem, we will write it so that the first polynomial (or set of polynomials) that we give will ensure that we pick out a subsequence that sums to the zero-element and the second polynomial that we give will ensure that the subsequence that we pick out is of the desired length. We note that Theorem 11 has been generalized (see [11]), though the statement given here is sufficient for our purposes.

To warm the reader to the employment of this method, we begin with an example.

Example 2.2. We compute $\mathsf{EGZ}(16,8,2)$. First, note that $16 \in S(8,2)$. Let $g_1,\ldots,g_{30}$ be integers.

Let $P = \sum_{1\leq i<\cdots<j\leq 30} g_i g_j x_i x_j$ and $Q = \sum_{1\leq i\leq 30} x_i$. We seek a particular type of member of the set of shared zeros of $P \equiv 0 \pmod{2^3}, Q \equiv 0 \pmod{2^4}$. We use the Boolean Case of Theorem 11. First note that the zero-vector is a shared zero of this polynomial system. Note that the hypothesis of Theorem 11 is satisfied, that

is, we have $(2^3-1)deg(P)+(2^4-1)deg(Q) = 7*2+15*1 = 29 < 30$. Thus, there exists a shared zero other than the zero-vector. This boolean vector of length 30 must have precisely 16 1′s in it as guaranteed by $Q \equiv 0 \pmod{2^4}$. These 1′s select a subsequence S' of the above list of integers of length 16 such that $e_2(S') \equiv 0 \pmod 8$. Thus, $\mathsf{EGZ}(16,8,2) \leq 30$.

We now show that $\mathsf{EGZ}(16,8,2) > 29$. Consider the sequence $S = (0^{14}, 1^{15})$. We show there is no subsequence S' of length 16 such that $e_2(S') \equiv 0 \pmod 8$. Let x count the number of 1′s in any subsequence S'. Then $e_2(S') \equiv \binom{x}{2} \pmod 8$. However, as we have $2 \leq x \leq 15$, $\binom{x}{2} \not\equiv 0 \pmod 8$.

Thus, $\mathsf{EGZ}(16,8,2) = 30$.

Notice that Part 3 of the following theorem is a Caro-Gao-type statement.

Theorem 12. *1. Let r and s be positive integers with $r \geq s$, p a prime, $m \geq 1$ and $p^r > mp^s - m$. We have $\mathsf{EGZ}(p^r, p^s, m) \leq p^r + mp^s - m$.*

2. Let $t \in S(p^s, p^u)$. Then $\mathsf{EGZ}(t, p^s, p^u) \geq t + p^{s+u} - p^u$. Furthermore, if $t = p^r$ where $r > u$, then $\mathsf{EGZ}(p^r, p^s, p^u) \geq p^r + p^{s+u} - p^u$.

3. Let r, s, u be positive integers with $r \geq s + u$. Then $\mathsf{EGZ}(p^r, p^s, p^u) = p^r + p^{s+u} - p^u$.

Proof. 1. Let $S = (g_1, \ldots, g_{p^r+mp^s-m})$ be a sequence over $\mathbb{Z}_{p^s}$. Let

$$P = \sum_{1 \leq i_1 < \cdots < i_m \leq p^r+mp^s-m} g_{i_1} \cdots g_{i_m} x_{i_1} \cdots x_{i_m},$$

$$Q = \sum_{1 \leq i \leq p^r+mp^s-m} x_i.$$

We seek a particular type of member of the set of shared zeros of $P \equiv 0 \pmod{p^s}, Q \equiv 0 \pmod{p^r}$. We use the Boolean Case of Theorem 11.

First note that the zero-vector is a shared zero of this polynomial system. Note that the hypothesis of Theorem 11 is satisfied, that is, we have

$$(p^s\text{–}1)deg(P) + (p^r\text{–}1)deg(Q) = p^r + mp^s - (m+1) < p^r + mp^s - m.$$

Thus, there exists a shared zero other than the zero-vector. This boolean vector of length p^r+mp^s-m must have precisely p^r 1′s in it as $Q \equiv 0 \pmod{p^r}$ and by hypothesis $p^r + mp^s - m < 2p^r$. These 1′s select a subsequence S' of the sequence S such that $e_m(S') \equiv 0 \pmod{p^s}$. Thus, $\mathsf{EGZ}(p^r, p^s, m) \leq p^r + mp^s - m$.

2. By Theorem 3, if $t \in S(k,m)$, then $\mathsf{EGZ}(t,k,m) \geq t + \mathsf{D}(\mathbb{Z}_k, m) - m$. By a result in [10] (see Theorem 2.7 of that paper), we know that $\mathsf{D}(\mathbb{Z}_{p^s}, p^u) = p^{s+u}$. Hence $\mathsf{EGZ}(t, p^s, p^u) \geq t + p^{s+u} - p^u$. In the case that $t = p^r$ and as $t \geq m+1$, we then know that $r > u$. As a result, $\mathsf{EGZ}(p^r, p^s, p^u) \geq p^r + p^{s+u} - p^u$.

3. With $m = p^u$ and $r \geq s + u$, we have $p^r \geq p^{s+u} > p^u(p^s - 1)$. By Part 1, we have $\mathsf{EGZ}(p^r, p^s, p^u) \leq p^r + p^u p^s - p^u$. By Part 2, we infer that equality holds. □

2.2.1. Results for p-groups

Theorem 13. *Let p be a prime. Let $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ be a $p-$group of rank r. Let $h = \sum_{i=1}^{r} \alpha_i$.*

1. *Suppose that $p^h > \sum_{j=1}^{r} m(p^{\alpha_j} - 1)$. Then $\mathsf{EGZ}(p^h, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, m) \leq p^h + m\sum_{j=1}^{r}(p^{\alpha_j} - 1)$.*
2. *$\mathsf{EGZ}(t, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) \geq t + p^s \sum_{j=1}^{r}(p^{\alpha_j} - 1)$.*
3. *Suppose that $p^h > \sum_{j=1}^{r} p^s(p^{\alpha_j} - 1)$. Then $\mathsf{EGZ}(p^h, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) = p^h + p^s \sum_{j=1}^{r}(p^{\alpha_j} - 1)$.*

Proof. 1. Let $\omega = p^h + \sum_{j=1}^{r} m(p^{\alpha_j} - 1)$. Let $S = (g_1, \ldots, g_\omega)$ be a sequence over $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$, where $g_i = (a_i^{(1)}, \ldots, a_i^{(r)})$. For each $1 \leq j \leq r$,

$$P_j = \sum_{1 \leq i_1 < \cdots < i_m \leq \omega} a_{i_1}^{(j)} \cdots a_{i_m}^{(j)} x_{i_1} \cdots x_{i_m},$$

$$Q = \sum_{1 \leq i \leq \omega} x_i.$$

We seek a particular type of member of the set of shared zeros of $P_j \equiv 0 \pmod{p^{\alpha_j}}, Q \equiv 0 \pmod{p^h}$ for $1 \leq j \leq r$. We use the Boolean Case of Theorem 11. First note that the zero-vector is a shared zero of this polynomial system. Note that the hypothesis of Theorem 11 is satisfied, that is, we have $\sum_{j=1}^{r}(p^{\alpha_j}-1)deg(P_j) + (p^{\sum_{j=1}^{r}\alpha_j} - 1)deg(Q) = \sum_{j=1}^{r}(p^{\alpha_j}-1)m + (p^h - 1) < \omega$. Thus, there exists a shared zero other than the zero-vector. This Boolean vector of length ω must have precisely p^h 1′s in it as $Q \equiv 0 \pmod{p^h}$ and by hypothesis $p^h > \sum_{j=1}^{r} m(p^{\alpha_j} - 1)$. These 1′s select a subsequence S' of length p^h such that $e_m(S')$ evaluates to the zero-element in the ring. Thus, $\mathsf{EGZ}(p^h, \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_r}}, m) \leq \omega$.

2. By Theorem 3, we have $\mathsf{EGZ}(t, G, m) \geq t + \mathsf{D}(G, m) - m$. By a result in [10] (see Theorem 3.7 of [10]), we know that $\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) = p^s\left(\sum_{i=1}^{r}(p^{\alpha_i} - 1) + 1\right) = p^s\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}})$. Hence,

$$\begin{aligned}\mathsf{EGZ}(t, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) &\geq t + p^s\left(\sum_{i=1}^{r}(p^{\alpha_i}-1)+1\right) - p^s \\ &= t + p^s\sum_{i=1}^{r}(p^{\alpha_i}-1).\end{aligned}$$

3. Part 1 with $m = p^s$ and Part 2 together imply the result.

□

An immediate consequence is another Caro-Gao-type statement.

Corollary 2. *Let p be a prime. Let $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ be a $p-$group of rank r. Let $h = \sum_{i=1}^{r}\alpha_i$. Suppose that $p^h > \sum_{j=1}^{r} p^s(p^{\alpha_j}-1)$. Then*

$$\mathsf{EGZ}(p^h, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) = p^h + \mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) - p^s.$$

Proof. It was shown in [10] that $\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) = p^s(\sum_{j=1}^{r}(p^{\alpha_j}-1)+1)$. Thus, by Theorem 13.3, the result follows immediately. □

Theorem 14. *Let p be a prime such that $p > m$. Let $G = \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ be a $p-$group of rank r. Let $h = \sum_{i=1}^{r}\alpha_i$ and suppose that $p^h > (\lfloor\frac{m}{2}\rfloor+1)(\sum_{i=1}^{r}p^{\alpha_i}-1)$. Then $\mathsf{EGZ}(p^h, \mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, m) \leq p^h + (\lfloor\frac{m}{2}\rfloor+1)(\sum_{i=1}^{r}p^{\alpha_i}-1)$.*

Proof. Let $\omega = p^h + (\lfloor\frac{m}{2}\rfloor+1)(\sum_{i=1}^{r}p^{\alpha_i}-1)$. Let $S = (g_1, \ldots, g_\omega)$ be a sequence over $\mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_r}}$, where $g_i = (a_i^{(1)}, \ldots, a_i^{(r)})$.

For each coordinate $j = 1, \ldots, r$, we define a set of $\lfloor\frac{m}{2}\rfloor + 1$ linear polynomials as follows. Let $u \in \{1, \ldots, \lfloor\frac{m}{2}\rfloor, m\}$. Then define

$$P_{j,u} = \sum_{i=1}^{\omega}(a_i^{(j)})^u x_i.$$

Define another linear polynomial

$$Q = \sum_{i=1}^{\omega} x_i.$$

We seek a particular type of member of the set of shared zeros of $P_{j,u} \equiv 0 \pmod{p^{\alpha_j}}$ for $j \in \{1, \ldots, \lfloor\frac{m}{2}\rfloor, m\}$ and $Q \equiv 0 \pmod{p^h}$. We use the Boolean Case of Theorem 11.

First note that the zero-vector is a shared zero of this polynomial system. Note that the hypothesis of Theorem 11 is satisfied, that is, we have

$$\begin{aligned}\omega &> (p^h-1)deg(Q)+\sum_{j=1}^{r}\sum_{u\in\{1,\ldots,\lfloor\frac{m}{2}\rfloor,m\}}(p^{\alpha_j}-1)deg(P_{j,u})\\ &= p^h-1+(\lfloor\frac{m}{2}\rfloor+1)(\sum_{i=1}^{r}p^{\alpha_j}-1).\end{aligned}$$

Thus, there exists a shared zero other than the zero-vector. This boolean vector of length ω must have precisely p^h $1'$s in it as $Q\equiv 0 \pmod{p^h}$ and by the hypothesis $2p^h>\omega$.

We now must show that these $1'$s select a length-p^h subsequence S' such that $e_m(S')$ equals the zero-element in $\mathbb{Z}_{p^{\alpha_1}}\oplus\cdots\oplus\mathbb{Z}_{p^{\alpha_r}}$.

We point out that $\{p_1,\ldots,p_{\lfloor\frac{m}{2}\rfloor},p_m\}$ is a minimum dominating set for the elementary symmetric polynomial e_m (see Section 4 of [10]). By the Newton-Girard formulae, $m!e_m$ may be written as a sum of products, where each product has an integer coefficient and each product contains at least one of the elements from the above dominating set. Now as each of these polynomials in the dominating set evaluate to 0 on S', so does $m!e_m$. The hypothesis that $p>m$ implies that $\gcd(p,m!)=1$. This now implies that $e_m(S')$ equals the zero-element. □

3. Problems and conjectures

Problem 1. *Determine a lower bound for* $\mathsf{EGZ}(k,k,m)$ *for* $k\in S(k,m)$ *and an upper bound for* $\mathsf{EGZ}(k,k,m)$ *for all* k,m.

Motivated by Theorem 10 and computations provided to us by Benjamin Girard [19], we give the following.

Conjecture 1. $\mathsf{EGZ}(t,q,q)=t+q^2-q=t+\mathsf{D}(\mathbb{Z}_q,q)-q$.

It is certainly the case that something more nuanced is true in the case that k and m are not both equal to a prime power q. This is evidenced by the following computations provided to us by Benjamin Girard [19]:

$$\mathsf{EGZ}(9,9,2)=17>9+\mathsf{D}(\mathbb{Z}_9,2)-2=9+9-2=16,$$

and

$$\mathsf{EGZ}(10,6,6)=19>10+\mathsf{D}(\mathbb{Z}_6,6)-6=10+13-6=17.$$

Problem 2. *Determine an upper bound for the m^{th}-degree Erdős-Ginzburg-Ziv constant for general abelian groups.*

Acknowledgments. We give thanks to BIRS-CMO 2019 and Casa Matemática Oaxaca, Mexico for supporting and hosting the event Zero-Sum Ramsey Theory: Graphs, Sequences and More 19w5132. We are grateful for helpful comments from Qinghai Zhao.

References

[1] T. Ahmed, A. Bialostocki, T. Pham and L.A. Vinh, Power sum polynomials as relaxed EGZ polynomials, *Integers* **19** (2019), #A49, 10pp.

[2] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, in *Combinatorics, Paul Erdős is Eighty, Vol. 1*, 33-50, *Bolyai Soc. Math. Stud.*, János Bolyai Math. Soc., Budapest, 1993.

[3] N. Alon and M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), no. 3, 301–309.

[4] S. Bera and S.K. Mukherjee, Generalized power sum and Newton-Girard identities, *Graphs Combin.* **36** (2020), no. 6, 1957–1964.

[5] A. Bialostocki and T.D. Luong, An analogue of the Erdős-Ginzburg-Ziv theorem for quadratic symmetric polynomials, *Integers* **9** (2009), #A36, 459–465.

[6] A. Bialostocki and T.D. Luong, Cubic symmetric polynomials yielding variations of the Erdős-Ginzburg-Ziv theorem, *Acta Math. Hungar.* **142** (2014), no. 1, 152–166.

[7] D. Brink, Chevalley's theorem with restricted variables, *Combinatorica* **31** (2011), 127–130.

[8] Y. Caro, Zero-sum sequences in abelian non-cyclic groups, *Israel J. Math.* **92** (1995), no. 1-3, 221–233.

[9] Y. Caro, Remarks on a zero-sum theorem, *J. Combin. Theory Ser. A* **76** (1996), no. 2, 315–322.

[10] Y. Caro, B. Girard, and J.R. Schmitt, Higher degree Davenport constants over finite commutative rings, *Integers* **21** (2021), #A120.

[11] P.L. Clark, A. Forrow, and J.R. Schmitt, Warning's second theorem with restricted variables, *Combinatorica* **37** (2017), no. 3, 397–417.

[12] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, and L. Rackham, Zero-sum problems in finite abelian groups and affine caps, *Q. J. Math.* **58** (2007), no. 2, 159–186.

[13] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite abelian groups I, *Reports ZW-1967-009*, Mathematical Centre, Amsterdam, 1967.

[14] P. van Emde Boas, A combinatorial problem on finite abelian groups II, *Reports ZW-1969-007*, Mathematical Centre, Amsterdam, 1969.

[15] P. Erdős, A. Ginzburg, and A. Ziv, Theorem in the additive number theory, Bull. Res. Council Israel Sect. F **10F** (1961), no. 1, 41–43.

[16] W.D. Gao, A combinatorial problem on finite abelian groups, *J. Number Theory* **58** (1996), no. 1, 100–103.

[17] W.D. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, *Expo. Math.* **24** (2006), no. 4, 337–369.

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

[19] B. Girard, personal communication.

[20] H. Harborth, Ein Extremalproblem für Gitterpunkte, *J. Reine Angew. Math.* **262(263)** (1973), 356–360.

[21] E.E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. Reine Agnew. Math.* **44** (1852), 93–146.

[22] J.E. Olson, A combinatorial problem on finite Abelian groups I, *J. Number Theory* **1** (1969), 8–10.

[23] J.E. Olson, A combinatorial problem on finite Abelian groups. II, *J. Number Theory* **1** (1969), 195–199.

[24] C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, *Ramanujan J.* **13** (2007), no. 1-3, 333-337.

[25] U. Schauz, Algebraically solvable problems: describing polynomials as equivalent to explicit solutions, *Electron. J. Combin.* **15** (2008), no. 1, Research Paper 10, 35pp.