Higher degree Davenport constants over finite commutative rings

Yair Caro, Benjamin Girard, John R. Schmitt

HIGHER DEGREE DAVENPORT CONSTANTS OVER FINITE COMMUTATIVE RINGS

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

Benjamin Girard
Sorbonne Université and Université de Paris, CNRS, Institut de Mathématiques de Jussieu - Paris Rive Gauche, Paris, France
benjamin.girard@imj-prg.fr

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

Abstract

We generalize the notion of Davenport constants to a 'higher degree' and obtain various lower and upper bounds, which are sometimes exact as is the case for certain finite commutative rings of prime power cardinality. Two simple examples that capture the essence of these higher degree Davenport constants are the following. 1) Suppose $n = 2^k$, then every sequence of integers S of length $2n$ contains a subsequence S' of length at least two such that $\sum_{a_i,a_j \in S'} a_i a_j \equiv 0 \pmod{n}$ and the bound is sharp. 2) Suppose $n \equiv 1 \pmod 2$, then every sequence of integers S of length $2n-1$ contains a subsequence S' of length at least two such that $\sum_{a_i,a_j \in S'} a_i a_j \equiv 0 \pmod{n}$. These examples illustrate that if a sequence of elements from a finite commutative ring is long enough, certain symmetric expressions have to vanish on the elements of a subsequence.

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. A finite sequence $S = (g_1, \ldots, g_\ell)$ of elements of G is called a *sequence over* G, where order is disregarded and repetition is allowed. Its *length*, denoted $|S|$, is the number of elements therein, counted with multiplicity. 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 t such that every sequence S over G of length $|S| \geq t$ contains a non-empty zero-sum subsequence. That is, we seek the smallest t for which there is a non-trivial solution of

$$\varepsilon_1 g_1 + \cdots + \varepsilon_t g_t = 0,$$

where each ε_i is 0 or 1.

Study of this number intensified in the 1960s with K. Rogers [16] in 1963, and later with H. Davenport in 1966 as explained by J.E. Olson in [14] and has continued unabated since; see, for example, a useful survey by W. Gao and A. Geroldinger [8].

The cyclic group with n elements will be denoted $\mathbb{Z}_n$. Further, it is well-known that by the Fundamental Theorem of Finite Abelian Groups that for any finite non-trivial abelian group G there exist integers $n_1, \ldots, n_r$ where $1 < n_1 \mid \ldots \mid n_r$ so that G can be written uniquely as

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

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 [14] and D. Kruyswijk [6] when G is a p-group, and by J.E. Olson [15] when G has rank at most 2.

Theorem 1.1. [J.E. Olson [14], [15], and D. Kruyswijk [6]] If G is a p-group or $r(G) \leq 2$, then $\mathsf{D}(G) = 1 + \mathsf{d}^*(G)$.

The value of $\mathsf{D}(G)$ is unknown in general. For a survey of results, see the work of A. Geroldinger [9] and the work of A. Geroldinger and F. Halter-Koch [10]. Recently, B. Girard [11] has shown that for all integers $r \geq 1$, $\mathsf{D}(\mathbb{Z}_n^r) \sim rn$ as $n \to \infty$.

We now introduce our object of study. Let $(A, +, \cdot)$ be a finite commutative ring. For any positive integer m and any sequence $S = (a_1, \ldots, a_\ell)$ over A, we set

$$e_m(S) := \sum_{1 \leq i_1 < \cdots < i_m \leq \ell} \prod_{j=1}^{m} a_{i_j}.$$

We say that S is an *m-zero sequence* whenever $e_m(S) = 0$, and that it is an *m-zero free sequence* whenever, for every subsequence S' of S such that $|S'| \geq m$, one has $e_m(S') \neq 0$. We denote by $\mathsf{D}(A, m)$ the smallest positive integer t such that every sequence S over A of length $|S| \geq t$ contains a subsequence S' of length $|S'| \geq m$ for which $e_m(S') = 0$.

Notice that when $m = 1$ we recover the classical Davenport constant discussed above. As a result, we may consider $\mathsf{D}(A, m)$ as the *m^{th}-degree Davenport constant.*

In this paper we examine this higher degree Davenport constant. This line of investigation that we follow is suggested by the work of A. Bialostocki and T.D. Luong [4], [5], and T. Ahmed, A. Bialostocki, T. Pham and Le Anh Vinh [1].

We proceed as follows. In Section 2 we examine the higher degree Davenport constant in the case that $A = \mathbb{Z}_n$. Of particular use is a result of R. Baker and W. Schmidt [2] (and see also [3]). We obtain a precise result in the case that n is a prime power and m is power of the same prime. In Section 3 we give an upper bound for the higher degree Davenport constant in the case that A is of the form $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ and a lower bound for any A of the form $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_b}$ from which we deduce a sharp value of the higher Davenport constant for rings of the form $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ when m is also a power of p. In Section 4 we show how to use the classical Girard-Newton formulae, which allow one to express the elementary symmetric polynomial of degree k by a combination of power sum polynomials, to obtain upper bounds. In Section 5 we present some open problems.

2. Bounds for cyclic groups

First, we note an easy lower bound on $\mathsf{D}(\mathbb{Z}_n, m)$. Consider the sequence $\mathbf{1} := (1, \ldots, 1)$ of length t. If $t = m$, then the only subsequence of length at least m is the given sequence itself and $e_m(\mathbf{1}) = 1 \not\equiv 0 \pmod{n}$. Further, suppose that for each ℓ with $t > \ell \geq m$ we have $\binom{\ell}{m} \not\equiv 0 \pmod{n}$. Then there exists no subsequence of $\mathbf{1}$ of length at least m which evaluates to zero modulo n. Thus, we define $L(n, m)$ to be the smallest integer $t \geq m + 1$ such that $\binom{t}{m} \equiv 0 \pmod{n}$. We have

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

Throughout the remainder of this section, let $n = p^r = q$.

An s-tuple $(\varepsilon_1, \ldots, \varepsilon_s)$ with each $\varepsilon_i = 0$ or 1 will be called *idempotent*. Whenever $\varepsilon_1 + \cdots + \varepsilon_s$ is even (respectively, odd), an idempotent s-tuple will be called *even* (respectively, *odd*). Further, for a fixed m, an idempotent s-tuple will be called m − *artificial* (or just *artificial* when m is clear) whenever $\varepsilon_1 + \cdots + \varepsilon_s \leq m - 1$, i.e. the number of ε_i that take on the value 1 is strictly less than m.

We will apply the following theorem of R.C. Baker and W.M. Schmidt [2, 3].

Theorem 2.1. [R.C. Baker, W.M. Schmidt [2, 3]] Suppose that $\mathcal{F}_1, \ldots, \mathcal{F}_\ell$ are polynomials in $\mathbf{x} = (x_1, \ldots, x_s)$ with coefficients in respective p-groups $G_1, \ldots, G_\ell$, and of respective degrees $d_1, \ldots, d_\ell$. Write A or B, respectively, for the number of even or the number of odd idempotent solutions of

$$\mathcal{F}_1(\varepsilon) = 0, \ldots, \mathcal{F}_\ell(\varepsilon) = 0.$$

If

$$s > d_1(\mathsf{D}(G_1) - 1) + \cdots + d_s(\mathsf{D}(G_\ell) - 1),$$

then

$$A \equiv B \pmod{p}.$$

To facilitate an application of Theorem 2.1 to our specific setting, we define for integers $q = p^r$ and m the function $U(q, m)$ to be the smallest integer $t \geq m(q-1)+1$ such that

$$\sum_{0 \leq 2j \leq m-1} \binom{t}{2j} \not\equiv \sum_{1 \leq 2j+1 \leq m-1} \binom{t}{2j+1} \pmod{p}.$$

Furthermore, for integers n and m we denote the set of all m-artificial idempotent n-tuples with $\varepsilon_1 + \cdots + \varepsilon_n$ equal to an even (odd) integer by $E(n, m, even)$ ($E(n, m, odd)$). Clearly, we have

$$|E(n, m, even)| = \sum_{0 \leq 2j \leq m-1} \binom{t}{2j} \quad \text{and} \quad |E(n, m, odd)| = \sum_{1 \leq 2j+1 \leq m-1} \binom{t}{2j+1}.$$

Theorem 2.2. Let r be a non-negative integer, p a prime, $q = p^r$ and $m \geq 1$. We have

$$L(q, m) \leq \mathsf{D}(\mathbb{Z}_q, m) \leq U(q, m).$$

Proof. The lower bound was established above. We establish the upper bound.

For a sequence $S = (a_1, \ldots, a_\ell)$ as opposed to seeking subsequences S' of length at least m such that $e_m(S') \equiv 0 \pmod{q}$, we may seek idempotent solutions that are not m-artificial to the following polynomial equation,

$$\sum_{1 \leq i_1 < \cdots < i_m \leq \ell} \prod_{j=1}^{m} a_{i_j} x_{i_j} \equiv 0 \pmod{q}.$$

To prove the upper bound, consider this degree-m polynomial equation when the number of variables is $U(q, m) \geq m(q-1)+1$, i.e. $\ell \geq m(q-1)+1$.

Clearly, all m-artificial idempotent $U(q, m)$-tuples are solutions to this equation since each monomial of the polynomial is a product of m variables (and so at least one variable in each monomial evaluates as 0 and so each monomial evaluates as 0). From these solutions, we know that the number of even idempotent solutions A is at least $E(U(q, m), m, even)$ and the number of odd idempotent solutions B is at least $E(U(q, m), m, odd)$. By the definition of $U(q, m)$, we have that $|E(U(q, m), m, even)| \not\equiv |E(U(q, m), m, odd)| \pmod{p}$. Thus, by Theorem 2.1, there exists an idempotent solution that is not m-artificial. $\square$

2.1. Properties of $U(q,m)$ and $L(q,m)$

The lower bound $L(q,m)$ and upper bound $U(q,m)$ provided in Theorem 2.2 motivate us to a numerical understanding of these functions in order to make them effective.

We begin with an investigation of $U(q,m)$.

Using Pascal's Identity and induction, one may show that

$$\sum_{0\leq 2j\leq m-1}\binom{t}{2j}-\sum_{1\leq 2j+1\leq m-1}\binom{t}{2j+1}=(-1)^{m-1}\binom{t-1}{m-1}.$$

Thus, an alternate definition of $U(q,m)$ is the smallest integer $t\geq m(q-1)+1$ such that $\binom{t-1}{m-1}\not\equiv 0 \pmod p$. The former definition naturally arises in the proof of Theorem 2.2 while the latter we use below.

We recall some classical results in number theory from the 19th-century.

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, $n=a_kp^k+a_{k-1}p^{k-1}+\cdots+a_1p+a_0$. Let $s_p(n)=a_k+a_{k-1}+\cdots+a_1+a_0$.

Theorem 2.3 (A.-M. Legendre, 1808 [13])**.** Let p be a prime and let n be a positive integer. Then

$$\nu_p(n!)=\frac{n-s_p(n)}{p-1}.$$

Legendre's Theorem was used to establish the following.

Theorem 2.4 (E. Kummer, 1852 [12])**.** 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.

When one uses Legendre's Theorem to prove Kummer's Theorem, an intermediate step gives

$$\begin{aligned}\nu_p(\binom{n}{m}) &= \nu_p(n!)-\nu_p(m!)-\nu_p((n-m)!) &(2)\\ &= \frac{s_p(m)+s_p(n-m)-s_p(n)}{p-1}. &(3)\end{aligned}$$

We repeatedly use this identity in the proofs given below.

Proposition 2.5. For an integer $m\geq 1$, a prime p and q a power of p, we have the following.

1. $m(q-1)+1 \leq U(q,m) \leq mq$.
2. For $p \geq 2m-1, U(q,m) = m(q-1)+1$.
3. For $m \leq p \leq 2m-2, U(q,m) = mq+m-p$.
4. For $p \geq m$, the roots of $\binom{t-1}{m-1} \in \mathbb{Z}_p[t]$ are $1, 2, \ldots, m-1$.

Proof. 1. The lower bound is by the definition. Now assume that $U(q,m) > m(q-1)+1$. Consider the largest integer $T \geq m(q-1)+1$ such that $\binom{t-1}{m-1} \equiv 0 \pmod{q}$ for all integers $m(q-1)+1 \leq t \leq T$. The integer T is well-defined by assumption, and we have $U(q,m) = T+1$. For the sake of contradiction, we assume that $T \geq mq$. By definition, we have $\binom{T-1}{m-1} \equiv \ldots \equiv \binom{m(q-1)}{m-1} \equiv 0 \pmod{p}$. By Pascal's Rule, we obtain $\binom{T-2}{m-2} \equiv \ldots \equiv \binom{m(q-1)}{m-2} \equiv 0 \pmod{p}$. We may iterate the application of Pascal's Rule $m-1$ times to obtain $0 \equiv \binom{m(q-1)}{m-1} \equiv \binom{m(q-1)}{m-2} \equiv \ldots \equiv \binom{m(q-1)}{1} \equiv \binom{m(q-1)}{0} \equiv 1 \pmod{p}$, a contradiction.

2. By the definition of $U(q,m)$, we must show that $\binom{m(q-1)+1-1}{m-1} \not\equiv 0 \pmod{p}$. We use Equation 3 to show $\nu_p(\binom{m(q-1)}{m-1}) = 0$.

   Note that the base-p expansion of $mq-m$ is $(m-1)p^\alpha + (p-1)p^{\alpha-1} + \cdots + (p-1)p + (p-m)$. The base-$p$ expansion of $m-1$ is $(m-1)$ since $p \geq 2m-1$. Subtracting, we find the base-p expansion of $m(q-1)-(m-1)$ is $(m-1)p^\alpha + (p-1)p^{\alpha-1} + \cdots + (p-1)p + (p-2m+1)$. By Equation 3

$$\begin{aligned}
\nu_p\left(\binom{m(q-1)}{m-1}\right) &= \frac{s_p(m-1) + s_p(m(q-1)-(m-1)) - s_p(m(q-1))}{p-1} \\
&= \frac{(m-1) + [(m-1) + (p-1)(\alpha-1) + (p-2m+1)]}{p-1} \\
&\quad - \frac{[(m-1) + (p-1)(\alpha-1) + (p-m)]}{p-1} \\
&= 0.
\end{aligned}$$

3. We begin by noting that the difference between the claimed value and the smallest $U(q,m)$ allowed by the definition is $2m-p-1$. Thus, by the definition of $U(q,m)$, we must show that $\binom{mq-p+m-1}{m-1} \not\equiv 0 \pmod{p}$ and that $\binom{mq-p+m-1-j}{m-1} \equiv 0 \pmod{p}$ for $1 \leq j \leq 2m-p-1$.

   We use Equation 3 to first show $\nu_p(\binom{mq-p+m-1}{m-1}) = 0$. Note that the base-$p$ expansion of $mq-p+m-1$ is $(m-1)p^\alpha + (p-1)p^{\alpha-1} + \cdots + (p-1)p + (m-1)$. The base-$p$ expansion of $m-1$ is $(m-1)$ since $m \leq p$. Subtracting, the base-p expansion of $mq-p+m-1-(m-1) = mq-p$ is $(m-1)p^\alpha + (p-1)p^{\alpha-1} + \cdots + (p-1)p + 0$. By Equation 3

$$\begin{aligned}
&\nu_p(\binom{mq-p+m-1}{m-1}) \\
&= \frac{s_p(m-1)+s_p(mq-p)-s_p(mq-p+m-1)}{p-1} \\
&= \frac{(m-1)+[(m-1)+(p-1)(\alpha-1)]-[2(m-1)+(p-1)(\alpha-1)]}{p-1} \\
&= 0.
\end{aligned}$$

We now use Equation 3 to show $\nu_p(\binom{mq-p+m-1-j}{m-1}) \neq 0$ for $1 \leq j \leq 2m-p-1$. First note that since $m \leq p$, we have $j \leq m-1$. Note that the base-p expansion of $mq-p+m-1-j$ is $(m-1)p^\alpha+(p-1)p^{\alpha-1}+\cdots+(p-1)p+(m-1)-j$. The base-$p$ expansion of $m-1$ is $(m-1)$ since $m \leq p$. Subtracting, the base-p expansion of $mq-p+m-1-j-(m-1) = mq-p-j$ is $(m-1)p^\alpha+(p-1)p^{\alpha-1}+\cdots+(p-2)p+(p-j)$. By Equation 3

$$\begin{aligned}
&\nu_p(\binom{mq-p+m-1-j}{m-1}) \\
&= \frac{s_p(m-1)+s_p(mq-p-j)-s_p(mq-p+m-1-j)}{p-1} \\
&= \frac{(m-1)+[(m-1)+(p-1)(\alpha-1)-1+(p-j)]}{p-1} \\
&\qquad - \frac{[2(m-1)+(p-1)(\alpha-1)-j]}{p-1} \\
&= 1.
\end{aligned}$$

4. Consider $\binom{t-1}{m-1}$ as a polynomial in $\mathbb{Z}_p[t]$. Since

$$\binom{t-1}{m-1} = \frac{(t-1)(t-2)\ldots(t-(m-1))}{(m-1)!},$$

this polynomial clearly is of degree $m-1$ with roots $1, 2 \ldots, m-1$.

□

We now give the value of $L(q,m)$ in the case that q and m are powers of the same prime p.

Proposition 2.6. For a prime p and integers r and s, we have $L(p^r, p^s) = p^{r+s}$.

Proof. By definition, we must show that the smallest integer $t \geq p^s+1$ for which $\binom{t}{p^s} \equiv 0 \pmod{p^r}$ is $t = p^{r+s}$. We must show that $\nu_p(\binom{t}{p^s}) < r$ for $p^s+1 \leq t < p^{r+s}$ and that $\nu_p(\binom{p^{r+s}}{p^s}) = r$.

We first show that $\nu_p(\binom{p^{r+s}}{p^s}) = r$. Note that the base-$p$ expansion of p^{r+s} is $1p^{r+s}+0p^{r+s-1}+\cdots+0p+0$ and the base-p expansion of p^s is $1p^s+0p^{s-1}+\cdots+0p+0$. Subtracting, the base-$p$ expansion of $p^{r+s}-p^s$ is $(p-1)p^{r+s-1}+\cdots+(p-1)p^s+0p^{s-1}+\cdots+0p+0$. By Equation 3,

$$\begin{aligned}\nu_p(\binom{p^{r+s}}{p^s}) &= \frac{s_p(p^s)+s_p(p^{r+s}-p^s)-s_p(p^{r+s})}{p-1}\\ &= \frac{1+r(p-1)-1}{p-1}\\ &= r.\end{aligned}$$

We now show that $\nu_p(\binom{t}{p^s}) < r$ for $p^s+1 \le t < p^{r+s}$. The base-p expansion of t is $t_{r+s-1}p^{r+s-1}+\cdots+t_1p+t_0$ and for p^s is $1p^s+0p^{s-1}+\cdots+0p+0$. Subtracting, the base-$p$ expansion of $t-p^s$ is $t'_{r+s-1}p^{r+s-1}+\cdots+t'_{s+1}p^{s+1}+t'_sp^s+t_{s-1}p^{s-1}+\cdots+t_1p+t_0$. By Equation 3

$$\begin{aligned}\nu_p(\binom{t}{p^s}) &= \frac{s_p(p^s)+s_p(t-p^s)-s_p(t)}{p-1}\\ &= \frac{1+(t'_{r+s-1}+\cdots+t'_s+t_{s-1}+\cdots+t_1+t_0)-(t_{r+s-1}+\cdots+t_0)}{p-1}.\end{aligned}$$

After cancelling like terms, we obtain

$$\nu_p(\binom{t}{p^s}) = \frac{1+(t'_{r+s-1}-t_{r+s-1})+\cdots+(t'_s-t_s)}{p-1}.$$

By the rules of subtraction and as $t \ge p^s+1$, there exists an index i with $s \le i \le r+s-1$ for which $t'_i - t_i = -1$. Thus,

$$\nu_p(\binom{t}{p^s}) \le \frac{1-1+(r-1)(p-1)}{p-1} = r-1.$$

□

Theorem 2.7. For integers r and s, and a prime p, for $q = p^r$ we have $\mathsf{D}(\mathbb{Z}_q, p^s) = p^{r+s}$.

Proof. We apply Theorem 2.2. From Part 1 of Proposition 2.5, we have $\mathsf{D}(\mathbb{Z}_q, p^s) \le U(q, p^s) \le qp^s = p^{r+s}$. From Proposition 2.6, we have $\mathsf{D}(\mathbb{Z}_q, p^s) \ge L(q, p^s) = p^{r+s}$. Thus, equality holds. □

3. More general lower and upper bounds

We now provide a generalization of Theorem 2.2 to products of the form $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$. We proceed in a similar way as in the set-up and proof of Theorem 2.2.

Define $U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m)$ to be the smallest integer $t \geq m\sum_{i=1}^{r}(p^{\alpha_i} - 1) + 1$ such that

$$\sum_{0 \leq 2j \leq m-1} \binom{t}{2j} \not\equiv \sum_{1 \leq 2j+1 \leq m-1} \binom{t}{2j+1} \pmod{p}.$$

As before, an alternate definition of $U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m)$ is the smallest integer $t \geq m\sum_{i=1}^{r}(p^{\alpha_i} - 1) + 1$ such that $\binom{t-1}{m-1} \not\equiv 0 \pmod{p}$.

Theorem 3.1. $\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, m) \leq U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m)$.

Proof. Let $S = (a_1, \ldots, a_\ell)$ be a sequence over $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$. For each $1 \leq i \leq \ell$, we write $a_i = [a_{i,1}, \ldots, a_{i,r}]$ where $a_{i,k} \in \mathbb{Z}_{p^{\alpha_k}}$ for all $1 \leq k \leq r$. As opposed to seeking subsequences S' of length at least m such that $e_m(S') = 0$, we may seek idempotent solutions that are not m-artificial to the following *system* of r polynomial equations,

$$\sum_{1 \leq i_1 < \cdots < i_m \leq \ell} \prod_{j=1}^{m} a_{i_j,k} x_{i_j} \equiv 0 \pmod{p^{\alpha_k}} \quad \forall k \text{ where } 1 \leq k \leq r.$$

To prove the upper bound, consider this system of polynomial equations, each of which is of degree m, when the number of variables is $U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m) \geq m\sum_{i=1}^{r}(p^{\alpha_i} - 1) + 1$.

Clearly, all m-artificial idempotent $U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m)$-tuples are solutions to this system of equations since each monomial of each polynomial is a product of m variables (and so at least one variable in each monomial evaluates as 0 and so each monomial evaluates as 0). From these solutions, we know that the number of even idempotent solutions A is at least $E(U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m), m, even)$ and the number of odd idempotent solutions B is at least $E(U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m), m, odd)$. By the definition of $U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m)$, we have that

$$|E(U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m), m, even)| \not\equiv |E(U((p^{\alpha_1}, \ldots, p^{\alpha_r}), m), m, odd)| \pmod{p}.$$

Thus, by Theorem 2.1, there exists an idempotent solution that is not m-artificial. □

Corollary 3.2.

$$\begin{aligned} \mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, m) &\leq m(\sum_{i=1}^{r}(p^{\alpha_i} - 1) + 1) \\ &= m\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}). \end{aligned}$$

Proof. The same argument as in the proof of Proposition 2.5.1 implies that

$$U((p^{\alpha_1},\ldots,p^{\alpha_r}),m) \quad \leq \quad (m\sum_{i=1}^{r}(p^{\alpha_i}-1)+1)+m-1 = m(\sum_{i=1}^{r}(p^{\alpha_i}-1)+1).$$

The result then follows from Theorems 1.1 and 3.1. □

Lemma 3.3. For every integer z such that $\binom{z}{m} \equiv 0 \pmod{n}$, we have $z < m$ or $z \geq L(n,m)$.

Proof. This follows immediately from the definition of $L(n,m)$. □

Theorem 3.4. Let A be the ring $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_b}$. We have

$$\mathsf{D}(A,m) \geq \sum_{j=1}^{b} L(n_j,m) - (b-1)m.$$

Proof. We show that the following sequence S is m-zero free over $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_b}$.

Let S be a sequence over $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_b}$ with elements $g_1 = [1,1,\ldots,1]$ repeated $L(n_1,m)-1$ times, $g_2 = [0,1,\ldots,1]$ repeated $L(n_2,m)-m$ times, $\ldots, g_b = [0,\ldots,0,1]$ repeated $L(n_b,m)-m$ times. (Notice that the number of times that g_1 is repeated is different in format from that of the other g_is.) The sequence S has length $|S| = (L(n_1,m)-m)+\ldots+(L(n_b,m)-m)+m-1$.

For the sake of contradiction, let S' be an m-zero subsequence of length at least m. For $i = 1,\ldots,b$, let $s_i \geq 0$ be the number of times g_i appears in S'. Since S' is a subsequence, we have $s_1 \leq L(n_1,m)-1, s_2 \leq L(n_2,m)-m, \ldots, s_b \leq L(n_b,m)-m$. Since S' is an m-zero sequence of length at least m, we have $|S'| = s_1+\ldots+s_b \geq m$. We also have

$$\begin{aligned}
\binom{s_1}{m} &\equiv 0 \pmod{n_1}\\
\binom{s_1+s_2}{m} &\equiv 0 \pmod{n_2}\\
&\cdots\\
&\cdots\\
\binom{s_1+s_2+\ldots+s_b}{m} &\equiv 0 \pmod{n_b}.
\end{aligned}$$

We now prove by induction on $i \in [0,b-1]$ that S' has the following property: $P(i) : s_1+\ldots+s_{b-i} \geq m$.

We first establish the base case. When $i = 0$, we have that since S' is an m-zero sequence of length at least m, $|S'| = s_1+\ldots+s_b \geq m$. Now we establish the induction step and so we assume that $P(i)$ holds for some $i \in [0,b-2]$. That is, assume that

$s_1 + \ldots + s_{b-i} \geq m$ for some $i \in [0, b-2]$. Since $\binom{s_1+\ldots+s_{b-i}}{m} \equiv 0 \pmod{n_{b-i}}$, Lemma 3.3 implies that $s_1 + \ldots + s_{b-i} \geq L(n_{b-i}, m)$. If $s_1 + \ldots + s_{b-(i+1)} < m$, then

$$\begin{aligned} L(n_{b-i}, m) &\leq s_1 + \ldots + s_{b-i} \\ &= (s_1 + \ldots + s_{b-(i+1)}) + s_{b-i} \\ &\leq m - 1 + (L(n_{b-i}, m) - m) \\ &= L(n_{b-i}, m) - 1, \end{aligned}$$

a contradiction. Therefore, $s_1 + \ldots + s_{b-(i+1)} \geq m$.

In particular, we have established that $s_1 \geq m$. Since $\binom{s_1}{m} \equiv 0 \pmod{n_1}$, Lemma 3.3 yields $s_1 \geq L(n_1, m)$, contradicting the fact that the number s_1 of copies of g_1 contained in S' is at most $L(n_1, m) - 1$. □

Remark 3.5. When $m = 1$, Theorem 3.4 recovers the well-known lower bound for the Davenport constant. That is, $\mathsf{D}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \geq \sum_{i=1}^{r}(n_i - 1) + 1$, which Theorem 1.1 shows to be sharp for p-groups and groups of rank at most 2. Theorem 3.4 shows that it is sharp whenever A is a product of the form $\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}$ and m is a power of p.

Remark 3.6. We wish to emphasize that Theorem 3.4 is for *any* direct product of cyclic groups. That is, say, for example, we consider $\mathbb{Z}_6$, which is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_3$. The theorem applies to both representations and we may *choose* the one for which the theorem provides the best bound.

Theorem 3.7. For a prime p and $s \geq 0$, we have

$$\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) = p^s \left(\sum_{i=1}^{r} (p^{\alpha_i} - 1) + 1 \right) = p^s \mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}).$$

Proof. By Corollary 3.2, we have

$$\mathsf{D}(\mathbb{Z}_{p^{\alpha_1}} \oplus \cdots \oplus \mathbb{Z}_{p^{\alpha_r}}, p^s) \leq p^s \left(\sum_{i=1}^{r} (p^{\alpha_i} - 1) + 1 \right).$$

On the other hand, Theorem 3.4 gives

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

The last equality follows directly from Theorem 1.1. □

4. Improved bounds for $\mathsf{D}(\mathbb{Z}_n, m)$ using the Girard-Newton formulae

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).

The symmetric functions that will be of interest to us consist of the following. For $k \geq 0$, the *elementary symmetric polynomial of degree* k is the sum of all distinct products of k distinct variables. Thus, $e_0(x_1, \ldots, x_n) = 1, e_1(x_1, \ldots, x_n) = x_1 + \cdots + x_n, e_2(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$ and, so on, until, $e_n(x_1, \ldots, x_n) = x_1 x_2 \ldots x_n$. The *$k$-th power sum polynomial* is $p_k(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^k$.

Theorem 4.1 (Girard-Newton formulae)**.** For all $n \geq 1$ and $1 \leq k \leq n$, we have

$$k e_k(x_1, \ldots, x_n) = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i}(x_1, \ldots, x_n) p_i(x_1, \ldots, x_n). \tag{4}$$

We may rewrite Equations 4 in a manner that is independent of the number of variables, that is, we may rewrite Equations 4 in the ring of symmetric functions as

$$k e_k = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i} p_i. \tag{5}$$

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

$$e_k = (-1)^k \sum \prod_{i=1}^{k} \frac{(-p_i)^{j_i}}{j_i! i^{j_i}}, \tag{6}$$

where the sum extends over all solutions to $j_1 + 2j_2 + \cdots + kj_k = k$ such that $j_1, \ldots, j_k \geq 0$. For example, we have $e_1 = p_1,\ e_2 = \frac{1}{2}p_1^2 - \frac{1}{2}p_2,\ e_3 = \frac{1}{6}p_1^3 - \frac{1}{2}p_1 p_2 + \frac{1}{3}p_3,\ e_4 = \frac{1}{24}p_1^4 - \frac{1}{4}p_1^2 p_2 + \frac{1}{8}p_2^2 + \frac{1}{3}p_1 p_3 - \frac{1}{4}p_4$. Upon multiplying both sides of Equation 6 by $k!$, we obtain on the right side *integer* coefficients.

Notice that for Equation 6, each term in the sum of the right side is a product that contains at most k distinct power sum polynomials. For a fixed k we call a set T of power sum polynomials a *dominating set for* e_k if each term in the sum contains at least one member of T. Let $t(k)$ denote the size of the smallest dominating set. For $k = 1$, the only dominating set is $\{p_1\}$, and so $t(1) = 1$. For $k = 2$, the only dominating set is $\{p_1, p_2\}$, and so $t(2) = 2$. For $k = 3$, any dominating set must contain both p_1 and p_3 and $\{p_1, p_3\}$ is a dominating set, and so $t(3) = 2$.

Lemma 4.2. We have $t(k) = \frac{k+2}{2}$ when k is even, $t(k) = \frac{k+1}{2}$ when k is odd.

Proof. We may determine the size of the smallest dominating set by examining the solutions to the equation $j_1 + 2j_2 + \cdots + kj_k = k$ such that $j_1, \ldots, j_k \geq 0$. There are solutions of the form (where we only specify the non-zero terms): $j_i = j_{k-i} = 1$ for $1 \leq i \leq k/2 - 1$; $j_{k/2} = 2$; and, $j_k = 1$. Thus selecting one element from each of the following sets $\{p_1, p_{k-1}\}, \ldots, \{p_{k/2-1}, p_{k/2+1}\}, \{p_{k/2}\}, \{p_k\}$ is necessary to form a dominating set. Thus, $t(k) \geq k/2 + 1$. Also, whenever $k/2 + 1 \leq i \leq k$ there is no solution with $j_i \geq 2$ and for any solution there is at most one index i, where $k/2 + 1 \leq i \leq k$, so that $j_i = 1$. This implies that for any solution where for $k/2 + 1 \leq i \leq k - 1$ we have $j_i = 1$, we also have $j_{i'} \geq 1$ for $1 \leq i' \leq k/2 - 1$. Thus, $\{p_1, \ldots, p_{k/2}, p_k\}$ is a dominating set of size $k/2 + 1$. When k is odd a similar argument allows us to claim that $\{p_1, \ldots, p_{(k-1)/2}, p_k\}$ is a minimum-sized dominating set.

□

Theorem 4.3. Let $n = 2^{\nu_2(n)}m$ with $m \geq 3$, and $b := \lfloor \frac{\nu_2(n)-1}{2} \rfloor$. We have

1. $\mathsf{D}(\mathbb{Z}_n, 2) \leq 2n - 1$ when $\nu_2(n) = 0$ (i.e. when n is odd), and
2. $\mathsf{D}(\mathbb{Z}_n, 2) \leq (2 + \frac{1}{2^b})n - 1$ when $\nu_2(n) \geq 1$ (i.e. when n is even).

Proof.

1. Let n be an odd integer, $n \geq 3$. Let S be a sequence $(a_1, \ldots, a_{2n-1})$ in $\mathbb{Z}_n$. We may assume that all the elements in S are non-zero. Consider the following elements of $\mathbb{Z}_n \oplus \mathbb{Z}_n$: $[a_1, a_1^2], \ldots, [a_{2n-1}, a_{2n-1}^2]$. Recall Theorem 1.1, which gives here $\mathsf{D}(\mathbb{Z}_n \oplus \mathbb{Z}_n) = 2n - 1$. That is, there exists a non-empty subset $J \subseteq \{1, \ldots, 2n-1\}$ such that $\sum_{j\in J}[a_j, a_j^2] = (0, 0)$, and necessarily $|J| \geq 2$. As a result, we have that $\sum_{j\in J} a_j \times \sum_{j\in J} a_j \equiv 0 \pmod{n}$ and that $\sum_{j\in J} a_j \times \sum_{j\in J} a_j = \sum_{j\in J} a_j^2 + 2\sum_{i\neq j,\ i,j\in J} a_i a_j = 2\sum_{i\neq j,\ i,j\in J} a_i a_j$. Thus, $2\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{n}$, and as n is odd we have $\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{n}$. Thus, $\mathsf{D}(\mathbb{Z}_n, 2) \leq 2n - 1$.

2. Let $n = 2^{\nu_2(n)}m$ be an integer such that $\nu_2(n) \geq 1, m \geq 3$, and, for convenience, let $b := \lfloor \frac{\nu_2(n)-1}{2} \rfloor \geq 0$. Let S be a sequence $(a_1, \ldots, a_{(2+\frac{1}{2^b})n-1})$ in $\mathbb{Z}_n$. We may assume that all the elements in S are non-zero.

   Case: $\nu_2(n)$ is odd

   In this case, we have $\nu_2(n) = 2b + 1$. Consider the following elements of $\mathbb{Z}_{m2^{\nu_2(n)-b}} \oplus \mathbb{Z}_{m2^{\nu_2(n)+1}} = \mathbb{Z}_{m2^{b+1}} \oplus \mathbb{Z}_{2n} = \mathbb{Z}_{\frac{n}{2^b}} \oplus \mathbb{Z}_{2n}$:

   $$[a_1, a_1^2], \ldots, [a_{(2+\frac{1}{2^b})n-1}, a_{(2+\frac{1}{2^b})n-1}^2].$$

   Recall Theorem 1.1, which gives here $\mathsf{D}(\mathbb{Z}_{\frac{n}{2^b}} \oplus \mathbb{Z}_{2n}) = (2 + \frac{1}{2^b})n - 1$. That is, there exists a non-empty subset $J \subseteq \{1, \ldots, (2 + \frac{1}{2^b})n - 1\}$ such that $\sum_{j\in J}[a_j, a_j^2] = (0, 0)$, and necessarily $|J| \geq 2$. That is, we have $\sum_{j\in J} a_j \equiv 0 \pmod{2^{b+1}m}$ and $\sum_{j\in J} a_j^2 \equiv 0 \pmod{2n}$. As a result, we have that

$\sum_{j\in J} a_j \times \sum_{j\in J} a_j \equiv 0 \pmod{2^{b+1}m} \times 0 \pmod{2^{b+1}m} \equiv 0 \pmod{2^{2b+2}m^2} \equiv 0 \pmod{2n}$ and that $\sum_{j\in J} a_j \times \sum_{j\in J} a_j = \sum_{j\in J} a_j^2 + 2\sum_{i\neq j,\ i,j\in J} a_i a_j = 2\sum_{i\neq j,\ i,j\in J} a_i a_j$. Thus, $2\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{2n}$, and so we have $\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{n}$. Thus, $\mathsf{D}(\mathbb{Z}_n, 2) \leq (2+\frac{1}{2^b})n - 1$.

Case: $\nu_2(n)$ is even

In this case, we have $\nu_2(n) = 2b+2$. Consider the following elements of $\mathbb{Z}_{m2^{\nu_2(n)-b}} \oplus \mathbb{Z}_{m2^{\nu_2(n)+1}} = \mathbb{Z}_{m2^{b+2}} \oplus \mathbb{Z}_{2n} = \mathbb{Z}_{\frac{n}{2^b}} \oplus \mathbb{Z}_{2n}$:

$$[a_1, a_1^2], \ldots, [a_{(2+\frac{1}{2^b})n-1}, a^2_{(2+\frac{1}{2^b})n-1}].$$

Recall Theorem 1.1, which gives here $\mathsf{D}(\mathbb{Z}_{\frac{n}{2^b}} \oplus \mathbb{Z}_{2n}) = (2+\frac{1}{2^b})n - 1$. That is, there exists a non-empty subset $J \subseteq \{1, \ldots, (2+\frac{1}{2^b})n-1\}$ such that $\sum_{j\in J}[a_j, a_j^2] = (0,0)$, and necessarily $|J| \geq 2$. That is, we have $\sum_{j\in J} a_j \equiv 0 \pmod{2^{b+2}m}$ and $\sum_{j\in J} a_j^2 \equiv 0 \pmod{2n}$. As a result, we have that $\sum_{j\in J} a_j \times \sum_{j\in J} a_j \equiv 0 \pmod{2^{b+2}m} \times 0 \pmod{2^{b+2}m} \equiv 0 \pmod{2^{2b+4}m^2} \equiv 0 \pmod{4n} \equiv 0 \pmod{2n}$ and that

$$\sum_{j\in J} a_j \times \sum_{j\in J} a_j = \sum_{j\in J} a_j^2 + 2\sum_{i\neq j,\ i,j\in J} a_i a_j = 2\sum_{i\neq j,\ i,j\in J} a_i a_j.$$

Thus, $2\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{2n}$, and so we have $\sum_{i\neq j,\ i,j\in J} a_i a_j \equiv 0 \pmod{n}$. Thus, $\mathsf{D}(\mathbb{Z}_n, 2) \leq (2+\frac{1}{2^b})n - 1$.

□

Remark 4.4. Notice that Theorem 4.3 provides an upper bound on $\mathsf{D}(\mathbb{Z}_n, 2)$ for any $n \geq 3$, whereas Theorem 2.2 and Proposition 2.5 only provide upper bounds in the case that n is a prime power.

Theorem 4.5. Let $n \geq 2$ and $\gcd(n, m!) = 1$. We have $\mathsf{D}(\mathbb{Z}_n, m) \leq \mathsf{D}(\mathbb{Z}_n^{t(m)}) + m - 1$.

Proof. Let $n \geq 2$ be an integer such that $\gcd(n, m!) = 1$, and let $M = \mathsf{D}(\mathbb{Z}_n^{t(m)}) + m - 1$. Let S be a sequence $(a_1, \ldots, a_M)$ over $\mathbb{Z}_n$.

Case: m is even. Recall that for m even, we have that $\{p_1, \ldots, p_{m/2}, p_m\}$ is a minimum size dominating set for e_m. Consider the following M elements of $\mathbb{Z}_n^{t(m)}$:

$$[a_1^1, a_1^2, \ldots, a_1^{m/2}, a_1^m], [a_2^1, a_2^2, \ldots, a_2^{m/2}, a_2^m], \ldots, [a_M^1, a_M^2, \ldots, a_M^{m/2}, a_M^m].$$

Obviously, $M = \mathsf{D}(\mathbb{Z}_n^{t(m)}) + m - 1 \geq \mathsf{D}(\mathbb{Z}_n^{t(m)})$. That is, there exists a non-empty subset $J \subseteq \{1, \ldots, M\}$ such that

$$\sum_{j\in J} [a_j, \ldots, a_j^{m/2}, a_j^m] = \overbrace{[0, \ldots, 0]}^{t(m)}.$$

Now, choose J such that $|J|$ is largest. From Equation 6, we have that $m!e_m$ may be written as a sum of terms where each term is a product that contains at least one element from the above dominating set and each term has an integer coefficient. As a result, we may conclude that e_m evaluates to zero modulo n over J. If $|J| \geq m$, we are done. So, assume $|J| \leq m-1$, and consider the complement of J, $J^c = \{1, \ldots, M\} \setminus J$. By the assumptions, $|J^c| \geq \mathsf{D}(\mathbb{Z}_n^{t(m)})$. Therefore, there exists a non-empty subset $J' \subseteq J^c$ such that

$$\sum_{j \in J'} [a_j, \ldots, a_j^{m/2}, a_j^m] = \overbrace{[0, \ldots, 0]}^{t(m)}.$$

As a result, we may consider $J \cup J'$ which has size strictly larger than J and the same property as J, contradicting the choice made above.

Case: m is odd. We proceed in a similar manner to the previous case, save that we have that $\{p_1, \ldots, p_{(m-1)/2}, p_m\}$ is a minimum dominating set for e_m. □

5. Concluding remarks and open problems

The most natural candidate for further research is the case of $\mathsf{D}(\mathbb{Z}_n, 2)$, which in our opinion preserves the same combinatorial and number-theoretic flavor of the $m = 1$ case.

It is already known from Theorem 2.7 that $\mathsf{D}(\mathbb{Z}_{2^r}, 2) = 2^{r+1}$. Further upper bounds are obtained in Theorem 4.3.

We have computed $\mathsf{D}(\mathbb{Z}_n, 2)$ for $2 \leq n \leq 16$ and $n = 18$. The results are presented in the list of following pairs $(n, \mathsf{D}(\mathbb{Z}_n, 2))$: $(2,4), (3,5), (4,8), (5,6), (6,7), (7,10), (8,16), (9,9), (10,9), (11,13), (12,12), (13,14), (14,13), (15,12), (16,32)$ and $(18,13)$.

We arrange this list as such:

1. $(2,4), (4,8), (8,16), (16,32)$: this is the case that n is a power of 2 and is already known from Theorem 2.7 that $\mathsf{D}(\mathbb{Z}_{2^r}, 2) = 2^{r+1}$;

2. $(9,9), (12,12)$: in this case we have $\mathsf{D}(\mathbb{Z}_n, 2) = n$.

   Problem 5.1. For which n does $\mathsf{D}(\mathbb{Z}_n, 2) = n$ hold?

3. $(10,9), (14,13), (15,12), (18,13)$: in this case we have $\mathsf{D}(\mathbb{Z}_n, 2) < n$.

   Problem 5.2. For which n does $\mathsf{D}(\mathbb{Z}_n, 2) < n$ hold?

4. $(3,5), (5,6), (7,10), (11,13), (13,14)$: this is the case when n is a prime.

   We claim that $\mathsf{D}(\mathbb{Z}_p, 2) \geq p+1$. For $p = 2$, this is established by Theorem 2.7. For $p \geq 3$ consider the following sequence of length p: $S = (1, \ldots, 1, \frac{p+1}{2})$.

Any 2-zero subsequence must contain at least two elements. For a subsequence S' we have $e_2(S') = \frac{j(j-1)}{2} + j\frac{p+1}{2} \equiv \frac{j}{2}(j+p) \not\equiv 0 \pmod{p}$ where j counts the number of 1's in S' for $1 \leq j \leq p-1$. Thus, no 2-zero subsequence exists.

Problem 5.3. For a prime p with $p \equiv 1 \pmod 4$, does $\mathsf{D}(\mathbb{Z}_p, 2) = p+1$ hold?

We claim that $\mathsf{D}(\mathbb{Z}_p, 2) \geq p+2$ for $p \equiv 3 \pmod 4$. For $p \geq 3$, consider the following sequence of length $p+1$: $S = (1, \ldots, 1, \frac{p+1}{2}, \frac{p+1}{2})$. From the above, the only case that we need to consider is when S' contains two copies of $\frac{p+1}{2}$. For any such subsequence S' we have

$$e_2(S') \quad = \quad \frac{j(j-1)}{2} + 2j\frac{p+1}{2} + \frac{(p+1)^2}{4} = \frac{j^2 + (j+1)^2 + p(4j+p+2)}{4},$$

where j counts the number of 1's in S' and $1 \leq j \leq p-1$. Note that

$$j^2 + (j+1)^2 + p(4j+p+2) \equiv j^2 + (j+1)^2 \pmod p.$$

However, a prime is expressible as the sum of two squares if and only if congruent to 1 (mod 4), a fact first observed by A. Girard in 1625 (and later by P. de Fermat).

Problem 5.4. Given a prime p, let $q = p^r$ and $m = p^s$ be two powers of p. Is it true that every m-zero free sequence S of length $\mathsf{D}(\mathbb{Z}_q, m) - 1 = mq - 1$ over $\mathbb{Z}_q$ has the form $S = (a, \ldots, a)$, where a generates the additive group of $\mathbb{Z}_q$?

Problem 5.5. Determine an upper bound for $\mathsf{D}(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_b}, m)$.

Problem 5.6. In light of Theorem 4.5: determine an upper bound for $\mathsf{D}(\mathbb{Z}_n, m)$ when $\gcd(n, m!) > 1$.

Acknowledgment. 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.

References

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

[2] R.C. Baker and W.M. Schmidt, Diophantine problems in variables restricted to the values 0 and 1, *J. Number Theory* **12** (1980), 460–486.

[3] R.C. Baker and W.M. Schmidt, Addendum: "Diophantine problems in variables restricted to the values 0 and 1", *J. Number Theory* **13** (1981), 270.

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

[5] 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.

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

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

[8] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: a survey, *Expo. Math.* **24** (4) (2006), 337–369.

[9] A. Geroldinger, Additive group theory and non-unique factorizations, Combinatorial number theory and additive group theory, 1–86, *Adv. Courses Math. CRM Barcelona,* Birkhäuser Verlag, Basel, 2009.

[10] A. Geroldinger and F. Halter-Koch, Non-unique factorizations. Algebraic, combinatorial and analytic theory, *Pure and Applied Mathematics* 278. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[11] B. Girard, An asymptotically tight bound for the Davenport constant, *J. Éc. polytech. Math.* **5** (2018), 605–611.

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

[13] A.-M. Legendre, *Essai sur la théorie des nombres, Second Edition,* Paris, Chez Courcier, Imprimeur-Libraire pour les Mathématiques, quai des Augustins, **57**, pp. 8–10, 1808.

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

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

[16] K. Rogers, A combinatorial problem in Abelian groups, *Proc. Cambridge Philos. Soc.* **59** (1963), 559–562.