QUADRATIC SYMMETRIC POLYNOMIALS
AND AN ANALOGUE OF THE DAVENPORT CONSTANT

H. GODINHO¹, A. LEMOS²,∗,†, V. G. L. NEUMANN³,‡ and F. A. A. OLIVEIRA⁴

¹Departamento de Matemática, Universidade de Brasília, Brasília-DF, Brazil
e-mail: hemar@mat.unb.br

²Departamento de Matemática, Universidade Federal de Viçosa, Viçosa-MG, Brazil
e-mail: abiliolemos@ufv.com.br

³Departamento de Matemática, Universidade Federal de Uberlândia, Uberlândia-MG, Brazil
e-mail: victor.neumann@ufu.br

⁴Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Sul-Campus Farroupilha,
Farroupilha-RS, Brazil
e-mail: filipe.oliveira@farroupilha.ifrs.edu.br

(Received August 5, 2022; revised January 25, 2023; accepted February 21, 2023)

Abstract. We define the constant \( D(\varphi_F, p) \), an analogue for the Davenport constant, for sequences on the finite field \( \mathbb{F}_p \), defined via quadratic symmetric polynomials. Next, we state a series of results presenting either the exact value of \( D(\varphi_F, p) \), or lower and upper bounds for this constant.

1. Introduction

Let \( p \) be a prime, and denote by \( \mathbb{F}_p \) the field of \( p \) elements, and \( \mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\} \). A sequence \( S = a_1 a_2 \cdots a_m \) of length \( |S| = m \) over \( \mathbb{F}_p \) will also be written as

\[
S = [u_1]^{n_1} [u_2]^{n_2} \cdots [u_t]^{n_t} := \underbrace{u_1 u_1 \cdots u_1}_{n_1 \text{ times}} \underbrace{u_2 u_2 \cdots u_2}_{n_2 \text{ times}} \cdots \underbrace{u_t u_t \cdots u_t}_{n_t \text{ times}},
\]

∗Corresponding author.
†The second author was partially supported by FAPEMIG grant APQ-02546-21 and
FAPEMIG grant RED-00133-21.
‡The third author was partially supported by FAPEMIG grant APQ-00470-22 and FAPEMIG
grant RED-00133-21.

Key words and phrases: Davenport constant, sequence, symmetric polynomial.
Mathematics Subject Classification: 11P70, 11B30.

0236-5294/$20.00 © 2023 Akadémiai Kiadó, Budapest, Hungary
where \( u_1, \ldots, u_t \) are distinct elements of \( \mathbb{F}_p \) and \( m = n_1 + n_2 + \cdots + n_t \). A subsequence \( T \) of \( S \) is a sequence of the form
\[
T = [u_1]^{s_1} [u_2]^{s_2} \cdots [u_t]^{s_t}, \quad \text{with } 0 \leq s_j \leq n_j, \ j = 1, \ldots, t,
\]
where \( s_j = 0 \) denotes that the element \( u_j \) does not appear in \( T \).

Let \( s_{n,k} \) be the symmetric polynomial
\[
s_{n,k} := s_{n,k}(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k,
\]
in \( n \) variables and degree \( k \). For any polynomial \( F(y_1, \ldots, y_r) \in \mathbb{F}_p[y_1, \ldots, y_r] \) define the symmetric polynomial in \( n \) variables
\[
\varphi_{F,n} = F(s_{n,1}, s_{n,2}, \ldots, s_{n,r}) \in \mathbb{F}_p[x_1, x_2, \ldots, x_n].
\]

**Definition 1.1.** Let \( F \) be a polynomial in \( \mathbb{F}_p[y_1, \ldots, y_r] \) and \( S \) be a sequence of length \( |S| = n \) over \( \mathbb{F}_p \) denoted by \( S = a_1 a_2 \cdots a_n \). We define
\[
\varphi_F(S) := \varphi_F|_S(S) = F(s_{n,1}, s_{n,2}, \ldots, s_{n,r})(a_1, a_2, \ldots, a_n).
\]
Observe that the order of appearance of an element in the sequence is not relevant for the evaluation of \( \varphi_F(S) \).

**Example 1.2.** Let \( F(y_1, y_2) = ay_1^2 + by_1 y_2 + cy_2^4 \), and \( S = a_1 a_2 a_3 a_4 \). Then
\[
\varphi_{F,4} = a(s_{4,1})^2 + b(s_{4,1}) \cdot (s_{4,2}) + c(s_{4,2})^4,
\]
and
\[
\varphi_F(S) = a(a_1 + a_2 + a_3 + a_4)^2 + b(a_1 + a_2 + a_3 + a_4)(a_1^2 + a_2^2 + a_3^2 + a_4^2)
\]
\[
+ c(a_1^4 + a_2^4 + a_3^4 + a_4^4).
\]

**Definition 1.3.** Let \( F \) be a polynomial in \( \mathbb{F}_p[y_1, \ldots, y_r] \) and \( S \) be a sequence of length \( m \) over \( \mathbb{F}_p \) denoted by \( S = a_1 a_2 \cdots a_m \).

(i) The sequence \( S \) will be called a \( \varphi_F \)-zero sequence if \( \varphi_F(S) = 0 \).

(ii) The sequence \( S \) will be called a \( \varphi_F \)-zero free sequence if for any subsequence \( T = b_1 \cdots b_r \) of \( S \) we have \( \varphi_F(T) \neq 0 \).

**Definition 1.4.** The Davenport \( \varphi_F \)-constant \( D(\varphi_F, p) \) is defined as the smallest value \( \ell \) such that any sequence over \( \mathbb{F}_p \) of length at least \( \ell \) has a \( \varphi_F \)-zero subsequence.

**Definition 1.5.** Let \( F \) be a polynomial in \( \mathbb{F}_p[y_1, \ldots, y_r] \) and \( S \) be a sequence of length \( m \) over \( \mathbb{F}_p \) denoted by \( S = a_1 a_2 \cdots a_m \). The sequence \( S \) will be called an extremal \( \varphi_F \)-zero free sequence if for any nonempty subsequence \( T = b_1 \cdots b_r \) of \( S \) we have \( \varphi_F(T) \neq 0 \) and \( m = D(\varphi_F, p) - 1 \).
The study of zero-sum sequences over finite abelian groups is a very active and beautiful area of research in Additive Number Theory, and the concept of $\varphi_F$-zero sequence is an extension of these classical ideas, just by taking into the definitions above the polynomial $F(y_1) = y_1$, for in this case $\varphi_{F,n} = s_{n,1} = x_1 + \cdots + x_n$ and $D(\varphi_F, p) = D(\mathbb{Z}_p)$, the classical Davenport constant over $\mathbb{Z}_p$, the additive subgroup of $\mathbb{F}_p$. In this context, a $\varphi_F$-zero sequence is called a zero-sum sequence, a $\varphi_F$-zero free sequence is called a zero-sum free sequence and an extremal $\varphi_F$-zero free sequence is called an extremal zero-sum free sequence. For our purposes here in this paper, we need the following consequence of the results given in Olson [4].

**Theorem 1.6.** Let $p$ be a prime. Then

1. $D(\mathbb{Z}_p) = p$ and any extremal zero-sum free sequence in $\mathbb{Z}_p$ is of the form $[u]^{p-1}$, for $u \in \mathbb{Z}_p \setminus \{0\}$.
2. $D(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p - 1$.

We refer the interested reader to [2] and [3] for more information on zero-sum sequences over finite abelian groups.

Our work was very much inspired by Bialostocki and Luong [1], who presented a generalization of the Erdős–Ginzburg–Ziv constant (EGZ-constant), via quadratic symmetric polynomials. Our goal is to present three theorems describing bounds for $D(\varphi_F, p)$ for the specific classes of quadratic polynomials, and also make whenever possible, a complete list of all extremal $\varphi_F$-zero free sequences. For this purpose we define $M(\varphi_F, p)$ as the set of all extremal $\varphi_F$-zero free sequences in $\mathbb{F}_p$. In almost all cases covered by Theorem 2.1, we were able to give a complete answer for the questions presented. The results given in Theorems 3.1, 4.4 and 4.5, although simpler to state, were more challenging and revealed an interesting relation between $D(\varphi_F, p)$ and the distribution of quadratic residues modulo $p$. This research is in its initial stage, but already revealed some interesting questions waiting to be answered. We close this paper with some comments and questions, indicating possible directions for the development of the theory.

2. The polynomial $\varphi_{F,m} = a s_{m,1}^2 + b s_{m,2} + c s_{m,1}$ – the general case

Let $F(y_1, y_2) = a y_1^2 + b y_2 + c y_1$, in this case

$$(2.1) \quad \varphi_{F,m} = F(s_{m,1}, s_{m,2}) = a s_{m,1}^2 + b s_{m,2} + c s_{m,1}.$$ 

We are interested in symmetric quadratic polynomials, so we will always assume that either $a$ or $b$ are not zero in (2.1). Next we present our first result.
THEOREM 2.1. Let \( p \) be an odd prime. Then the following statements are true:

(i) If \( a = 0 \) and \( b \neq 0 \), then \( D(\varphi_F, p) = p \) and
\[
M(\varphi_F, p) = \{[u]^\alpha[-u - cb^{-1}]^{p-1-\alpha} \mid u \in \mathbb{F}_p \setminus \{0, -cb^{-1}\} \text{ and } 0 \leq \alpha \leq p-1\}.
\]

(ii) If \( a \neq 0 \) and \( b = c = 0 \), then \( D(\varphi_F, p) = p \) and
\[
M(\varphi_F, p) = \{[u]^{p-1} \mid u \in \mathbb{F}_p^*\}.
\]

(iii) If \( a \neq 0 \), \( b = 0 \) and \( c \neq 0 \), then
\[
D(\varphi_F, p) = p - 1 \quad \text{and} \quad M(\varphi_F, p) = \{[ca^{-1}]^{p-2}\}.
\]

(iv) If \( ab \neq 0 \) then \( D(\varphi_F, p) \leq 2p - 1 \).

The proof of this Theorem will be presented in the form of a series of three lemmas.

LEMMA 2.2. Let \( p \) be an odd prime. Then the following statements are true:

(i) If \( a = 0 \) and \( b \neq 0 \), then \( D(\varphi_F, p) = p \) and
\[
M(\varphi_F, p) = \{[u]^\alpha[-u - cb^{-1}]^{p-1-\alpha} \mid u \in \mathbb{F}_p \setminus \{0, -cb^{-1}\} \text{ and } 0 \leq \alpha \leq p-1\}.
\]

(ii) If \( a \neq 0 \) and \( b = c = 0 \), then \( D(\varphi_F, p) = p \) and
\[
M(\varphi_F, p) = \{[u]^{p-1} \mid u \in \mathbb{F}_p^*\}.
\]

Proof. Initially suppose \( a = 0 \) and \( b \neq 0 \), then it follows from (2.1) that for all \( k \in \mathbb{N} \),
\[
(2.2) \quad \varphi_F,k = \sum_{i=1}^{k} (bx_i^2 + cx_i) = \sum_{i=1}^{r} f(x_i), \quad \text{with } f(u) = bu^2 + cu.
\]

Given a sequence \( T = u_1 u_2 \cdots u_k \) over \( \mathbb{F}_p \), consider the sequence \( S = f(u_1)f(u_2) \cdots f(u_k) \) in \( \mathbb{Z}_p \). From (2.2) and Theorem 1.6 it follows that \( D(\varphi_F, p) \leq D(\mathbb{Z}_p) = p \), and if \( S \) is an extremal zero-sum free sequence in \( \mathbb{Z}_p \), then \( S = [f(u)]^{p-1} \). Since
\[
f(u_i) = f(u_j) \iff u_i = u_j \text{ or } u_j = -u_i - cb^{-1},
\]
we have that \( M(\varphi_F, p) = \{[u]^\alpha[-u - cb^{-1}]^{p-1-\alpha} \mid u \in \mathbb{F}_p \setminus \{0, -cb^{-1}\} \} \).

If \( a \neq 0 \) and \( b = c = 0 \), then it follows that (2.1) has the form
\[
\varphi_F,k = a s_{k,1}^2.
\]
From Theorem 1.6 it is easy to conclude that $D(\varphi_F, p) = D(\mathbb{Z}_p) = p$ and

$$M(\varphi_F, p) = \{[u]^{p-1} : u \in \mathbb{F}_p \setminus \{0\}\}. \quad \square$$

**Lemma 2.3.** Let $p$ be an odd prime. If $a \neq 0$, $b = 0$ and $c \neq 0$, then

$$D(\varphi_F, p) = p - 1 \quad \text{and} \quad M(\varphi_F, p) = \{[ca^{-1}]^{p-2}\}.$$

**Proof.** Now let us assume $ac \neq 0$ and $b = 0$, and we will have

$$\varphi_{F,k} = as_{k,1}^2 + cs_{k,1} = a(x_1 + \cdots + x_k)^2 + c(x_1 + \cdots + x_k).$$

Hence for any zero-sum sequence $S$ in $\mathbb{Z}_p$, we have $\varphi_F(S) = 0$, therefore it follows from Theorem 1.6 that $D(\varphi_F, p) \leq D(\mathbb{Z}_p) = p$. Let us suppose that we can find a $\varphi_F$-zero free sequence $S_0 = u_1u_2 \cdots u_{p-1}$ of length $p - 1$. In particular, $S_0$ must also be a zero-sum free sequence in $\mathbb{Z}_p$ (see (2.3)), then it follows from Theorem 1.6 that $S_0 = [u]^{p-1}$, for some $u \in \mathbb{Z}_p \setminus \{0\}$. Let $T_j = [u]^j$ be a subsequence of $S_0$. Considering $T_j$ also a sequence over $\mathbb{F}_p$ we would have

$$\varphi_F(T_j) = a(aju)^2 + c(ja) = jau + c,$$

and it is always possible to find a $j$ such that $\varphi_F(T_j) = 0$, contradicting the hypothesis that $S_0$ is a $\varphi_F$-zero free sequence. Therefore $D(\varphi_F, p) \leq p - 1$.

Now consider the sequence $S = [ca^{-1}]^{p-2}$ and observe that, for any $1 \leq j \leq p - 2$ we have

$$\varphi_F([ca^{-1}]^j) = jca^{-1}(j + 1) \neq 0,$$

thus $S$ is a $\varphi_F$-zero free sequence, proving that $D(\varphi_F, p) = p - 1$.

Suppose $S = w_1w_2 \cdots w_{p-2}$ is also a $\varphi_F$-zero free sequence over $\mathbb{F}_p$. Then for any subsequence $T = v_1 \cdots v_t$ of $S$ we have (see (2.3))

$$v_1 + \cdots + v_t \equiv 0 \pmod{p} \quad \text{and} \quad v_1 + \cdots + v_t \equiv -c \cdot a^{-1} \pmod{p}.$$

In particular the sequence, with $v_0 = ca^{-1}$,

$$w_1w_2 \cdots w_{p-2}v_0$$

is a zero-sum free sequence in $\mathbb{Z}_p$. Again it follows from Theorem 1.6 that

$$w_1 = w_2 = \cdots = w_{p-2} = ca^{-1},$$

completing the proof. \quad \square

**Lemma 2.4.** If $ab \neq 0$ then $D(\varphi_F, p) \leq 2p - 1$. 

*Acta Mathematica Hungarica* 169, 2023
Proof. Let \( S = u_1 u_2 \cdots u_m \) be any sequence over \( \mathbb{F}_p \) of length \( m \geq 2p - 1 \), and consider the sequence
\[
U = [u_1, u_1^2] [u_2, u_2^2] \cdots [u_m, u_m^2] \quad \text{over} \quad \mathbb{Z}_p \oplus \mathbb{Z}_p.
\]
According to Theorem 1.6, since \( m \geq 2p - 1 \), we can find a subsequence \( V \) of \( U \) of length \( k \leq 2p - 1 \), say
\[
V = [v_1, v_1^2] [v_2, v_2^2] \cdots [v_k, v_k^2],
\]
such that modulo \( p \) we have
\[
v_1 + v_2 + \cdots + v_k \equiv 0 \quad \text{and} \quad v_1^2 + v_2^2 + \cdots + v_k^2 \equiv 0
\]
hence
\[
\varphi_F(V) = a(v_1 + v_2 + \cdots + v_k)^2 + b(v_1^2 + v_2^2 + \cdots + v_k^2) + c(v_1 + v_2 + \cdots + v_k) = 0
\]
over \( \mathbb{F}_p \), and this proves that \( D(\varphi_F, p) \leq 2p - 1 \). \( \square \)

3. The polynomial \( \varphi_{F,m} = as_{m,1}^2 + bs_{m,2} \), with \( ab \neq 0 \)

In this section we are interested in the symmetric polynomial \( \varphi_{F,m} = as_{m,1}^2 + bs_{m,2} \), with \( ab \neq 0 \). With no loss in generality, we start by rewriting the polynomial \( \varphi_{F,p} \) as
\[
\varphi_{F,k} = s_{k,1}^2 + \lambda s_{k,2}, \quad \text{with} \ \lambda \neq 0.
\]
This is the main result of this section.

Theorem 3.1. Let \( p \) be an odd prime, then
\[
D(\varphi_F, p) = 1, \quad \text{if} \ \lambda = p - 1,
\]
\[
2p - 1 \geq D(\varphi_F, p) \geq p - \lambda + 1, \quad \text{otherwise}.
\]
In particular, for \( p \geq 5 \) we have
(a) if \( \lambda = p - 2 \) then \( 3 \leq D(\varphi_F, p) \leq \frac{k-1}{k}(p-1) + 1; \)
(b) if \( \lambda = p - 3 \) then \( 4 \leq D(\varphi_F, p) \leq \frac{2k-2}{k}(p-1) + 1, \) where \( k \) is the smallest positive integer greater than 2 such that \( k \mid p - 1 \).

We are going to divide the proof into two lemmas, taking into account the possible values of \( \lambda \) (see (3.1)).

Lemma 3.2. Let \( p \) be an odd prime, then
\[
D(\varphi_F, p) = 1, \quad \text{if} \ \lambda = p - 1, \quad 2p - 1 \geq D(\varphi_F, p) \geq p - \lambda + 1, \quad \text{otherwise}.
\]
Proof. The upper bound follows from Theorem 2.1(iv). Next, observe that if \( S = [u]^k \) then it follows from (3.1) that

\[
\varphi_F(S) = (uk)^2 + \lambda ku^2 = u^2 k(k + \lambda).
\]

If \( \lambda = p - 1 \) then \( \varphi_F([u]) = u^2 - u^2 = 0 \) (see (3.2)), hence any sequence has a \( \varphi_F \)-zero subsequence, thus \( D(\varphi_F, p) = 1 \). For \( \lambda \neq p - 1 \), (see (3.2)), we can have \( \varphi_F([u]^k) \neq 0 \), as long as \( k \leq (p - \lambda) - 1 \). Now, consider the sequence \( S = [u]^{p-\lambda-1}[tu] \) for some \( u, t \in \mathbb{F}_p^* \) with \( t \neq 1 \). From the considerations above, we have \( \varphi_F(T) \neq 0 \) for the subsequence \( T = [u]^k \), with \( 1 \leq k \leq p - \lambda - 1 \). Let us consider now the subsequence \( T = [u]^k[tu] \). In this case

\[
\varphi_F(T) = (ku + tu)^2 + \lambda (ku^2 + t^2 u^2) = u^2 (k^2 + (2t + \lambda)k + (\lambda + 1)t^2).
\]

Observe that if \( \Delta(t) = (2t + \lambda)^2 - 4(\lambda + 1)t^2 \) is not a square in \( \mathbb{F}_p \), then \( \varphi_F(T) \neq 0 \) for any \( k \in \mathbb{F}_p^* \), and observe also that \( \lambda \neq 0 \) and \( \lambda + 1 \neq 0 \), since \( 1 \leq \lambda \leq p - 2 \). If \( -(\lambda + 1) \) is not a square, then \( -(\lambda + 1) \neq 1 \) and so \( -2^{-1}\lambda \neq 1 \). Thus, it suffices to choose \( t = -2^{-1}\lambda \neq 1 \), since \( \Delta(-2^{-1}\lambda) = -(\lambda + 1)\lambda^2 \). So let us consider that there exists \( r \in \mathbb{F}_p^* \) such that \( r^2 = -(\lambda + 1) \). Since there exist non-quadratic residues, there must exist \( s \in \mathbb{F}_p^* \) such that \( s^2 + 1 \) is not a square. Since \( -(s)^2 + 1 \) is also not a square, we can choose this \( s \) in such way that \( rs \neq 1 \). Rewrite \( \Delta(t) \) as

\[
\Delta(t) = (2t + \lambda)^2 + (2rt)^2 = (2rt)^2((2t + \lambda)(2rt)^{-1})^2 + 1).
\]

Observe that \( \lambda(2rs - 2)^{-1} \neq 1 \), since if \( \lambda(2rs - 2)^{-1} = 1 \) then \( \lambda = 2rs - 2 \). But from \( r^2 = -(\lambda + 1) \), we get \( (r + s)^2 = s^2 + 1 \). This is not possible, since \( s^2 + 1 \) is not a square. So, we may choose \( t = \lambda(2rs - 2)^{-1} \neq 1 \) and we have

\[
(2t + \lambda)(2rt)^{-1} = s \quad \text{and} \quad \Delta(t) = (2rt)^2(s^2 + 1).
\]

Since \( \Delta(t) \) is not a square, this implies that \( S = [u]^{p-\lambda-1}[tu] \) is a \( \varphi_F \)-zero free sequence and \( D(\varphi_F, p) \geq p - \lambda + 1 \). \[ \square \]

Lemma 3.3. Let \( p \) be an odd prime such that \( p \geq 5 \), then

\[
D(\varphi_F, p) \leq \begin{cases} 
\frac{k-1}{k}(p-1) + 1 & \text{if } \lambda = p - 2, \\
\frac{2k-2}{k}(p-1) + 1 & \text{if } \lambda = p - 3,
\end{cases}
\]

where \( k \) is the smallest positive integer greater than 2 such that \( k \mid p - 1 \).
Proof. Let \( \alpha \in \mathbb{F}_p^\ast \) be a generator of \( \mathbb{F}_p^\ast \) and let \( \beta = \alpha^{\frac{p-1}{k}} \). Since \( k > 2 \), we have \( \beta^2 \neq 1 \) and for all \( a \in \mathbb{F}_p^\ast \)

\[
\sum_{j=0}^{k-1} a \beta^j = a \frac{\beta^k - 1}{\beta - 1} = 0 \quad \text{and} \quad \sum_{j=0}^{k-1} (a \beta^j)^2 = a^2 \frac{\beta^{2k} - 1}{\beta^2 - 1} = 0.
\]

Hence, a \( \varphi_F \)-zero free sequence \( S = [v_1]^d_1 [v_2]^d_2 \cdots [v_m]^d_m \) can not have a subsequence of the form \( V = [a] [a \beta] \cdots [a \beta^{k-1}] \), since \( \varphi_F(V) = 0 \) (see (3.3)). From the considerations following (3.2), if \( \lambda = p - 2 \), we must have \( d_1 = \cdots = d_m = 1 \), so the \( \varphi_F \)-zero free sequence \( S \) contains at most \( k - 1 \) elements of each lateral class of the group generated by \( \beta \). Since there are \( \frac{p-1}{k} \) lateral classes we must have

\[
D(\varphi_F, p) \leq (k - 1) \frac{p - 1}{k} + 1.
\]

By a similar reasoning, if \( \lambda = p - 3 \) then we must have, for any \( j \in \{1, 2, \ldots, m\} \), \( d_j \leq 2 \), hence

\[
D(\varphi_F, p) \leq 2(k - 1) \frac{p - 1}{k} + 1,
\]

completing the proof. \( \square \)

A computer search using Sagemath [5], gives us Table 1 containing the exact value for \( D(\varphi_F, p) \), for \( F = x_1^2 + \lambda x_2 \), \( 3 \leq p \leq 11 \) and \( 1 \leq \lambda \leq p - 2 \), and also presenting examples of extremal \( \varphi_F \)-zero free sequences and the cardinality of the set \( M(\varphi_F, p) \). Observe that, when \( \lambda = p - 2 \), the upper bound given in Lemma 3.3 is attained when \( p = 5 \) and \( p = 7 \), but as \( p \) grows (bigger than 17, for example), a computer search reveals that the exact value of \( D(\varphi_F, p) \) tends to be smaller than \( p/2 \).

4. The polynomial \( \varphi_F,m = as_m^2 + bs_m,2 + cs_m,1 \), with \( abc \neq 0 \)

With no loss in generality we will rewrite the symmetric polynomial \( \varphi_F,m \) as

\[
\varphi_F,m = s_m^2 + \lambda s_m,2 + \mu s_m,1, \quad \text{with} \quad \lambda \mu \neq 0 \pmod{p},
\]

and for any \( S = [u_1]^{t_1} \cdots [u_r]^{t_r} \) we have

\[
\varphi_F(S) \equiv \left( \sum_{i=1}^{r} t_i u_i \right)^2 + \sum_{i=1}^{r} t_i u_i (\lambda u_i + \mu) \pmod{p}.
\]
Let us define
\[
\omega_o = -\mu \cdot \lambda^{-1}.
\]

**Lemma 4.1.** The sequence \([\omega_o]^{p-1}\) is the only \(\varphi_F\)-zero free sequence among all the sequences of the form \([u]^{p-1}\).

**Proof.** We have
\[
\varphi_F([\omega_o]^t) \equiv (t\mu \lambda^{-1})^2 + \lambda t(\mu \lambda^{-1})^2 - t\mu(\mu \lambda^{-1}) \equiv (t\mu \lambda^{-1})^2 \neq 0 \pmod{p},
\]
for any \(t \in \{1, 2, 3, \ldots, p-1\}\). Hence \(S = [\omega_o]^{p-1}\) is a \(\varphi_F\)-zero free sequence, and also observe that for any other value \(u \neq \omega_o\) there is a \(t_o \in \{1, 2, \ldots, p-1\}\)

| \(F\) | \(D(\varphi_F, p)\) | Some elements of \(M(\varphi_F, p)\) | \(|M(\varphi_F, p)|\) |
|-----|------------------|-------------------------------|------------------|
| \(x_1^2 + x_2\) | \(D(\varphi_F, 3) = 3\) | \([1][2]\) | 1 |
| \(x_1^2 + x_2\) | \(D(\varphi_F, 5) = 7\) | \([1][3][4]^3, [2]^3[3]^3\) | 2 |
| \(x_1^2 + 2x_2\) | \(D(\varphi_F, 5) = 6\) | \([1][2][2][4], [1]^2[2][3]^2\) | 4 |
| \(x_1^2 + 3x_2\) | \(D(\varphi_F, 5) = 4\) | \([1][2][3], [1][2][4]\) | 4 |
| \(x_1^2 + x_2\) | \(D(\varphi_F, 7) = 7\) | \([1][3][6]^3\) | 15 |
| \(x_1^2 + 2x_2\) | \(D(\varphi_F, 7) = 8\) | \([1][4][5]^3, [2]^4[3]^3\) | 6 |
| \(x_1^2 + 3x_2\) | \(D(\varphi_F, 7) = 8\) | \([1][3][5][5], [2][4][3][6]^2\) | 12 |
| \(x_1^2 + 4x_2\) | \(D(\varphi_F, 7) = 5\) | \([1][2][2]^3, [3]^2[4]^2\) | 9 |
| \(x_1^2 + 5x_2\) | \(D(\varphi_F, 7) = 5\) | \([1][2][3][5], [2][3][4][6]\) | 9 |
| \(x_1^2 + x_2\) | \(D(\varphi_F, 11) = 13\) | \([1][9][3]^3, [2][9][6]^2[7]\) | 40 |
| \(x_1^2 + 2x_2\) | \(D(\varphi_F, 11) = 12\) | \([1][8][4]^3, [2][8][5]^2[8]\) | 50 |
| \(x_1^2 + 3x_2\) | \(D(\varphi_F, 11) = 12\) | \([1][6][7][8][3]^3, [2][2][5][6]^2[7]^3\) | 10 |
| \(x_1^2 + 4x_2\) | \(D(\varphi_F, 11) = 11\) | \([1][6][6]^5, [3][5][8][5]^5\) | 15 |
| \(x_1^2 + 5x_2\) | \(D(\varphi_F, 11) = 11\) | \([1][5][2]^5, [3][5][7][5]^5\) | 10 |
| \(x_1^2 + 6x_2\) | \(D(\varphi_F, 11) = 11\) | \([1][4][3][10]^3, [4][4][5][3][7][3]^3\) | 10 |
| \(x_1^2 + 7x_2\) | \(D(\varphi_F, 11) = 9\) | \([1][3][5][3][7]^2, [4][3][6][2][9]^3\) | 10 |
| \(x_1^2 + 8x_2\) | \(D(\varphi_F, 11) = 8\) | \([1][2][2][3][5][6], [3][6][2][7][2][8]^2\) | 60 |
| \(x_1^2 + 9x_2\) | \(D(\varphi_F, 11) = 6\) | \([1][2][3][4][7], [4][5][6][7][9]\) | 60 |

Table 1: Exact values of \(D(\varphi_F, p)\) for \(F = x_1^2 + \lambda x_2\)
such that
\[(t_o + \lambda)u + \mu \equiv 0 \pmod{p},\]
in particular
\[
\varphi_F([u]^{t_o}) = t_o u (t_o u + \lambda u + \mu) \equiv 0 \pmod{p},
\]
completing the proof.  \(\square\)

**Lemma 4.2.** Let \(p = 3\) and consider (4.1), then
\begin{enumerate}
\item \(D(\varphi_F, 3) = 3\) if \(\lambda = 1\);
\item \(D(\varphi_F, 3) = 4\) if \(\lambda = 2\).
\end{enumerate}

**Proof.** Let \(u \in \{1, 2\}\). Since
\[
\varphi_F([u]^k) = ku(ku + \lambda u + \mu) \equiv 0 \pmod{3},
\]
any \(\varphi_F\)-zero free sequence in \(\mathbb{F}_3\) has the form \([1]^r [2]^s\) with \(0 \leq r, s \leq 2\) and \((r, s) \neq (0, 0)\). For \(\lambda = 1\) we have
\[
\varphi_F([\mu]) = 0, \quad \text{and} \quad \varphi_F([2\mu]^2) = 1,
\]
so an extremal \(\varphi_F\)-zero free sequence is \([2\mu]^2\).

For \(\lambda = 2\) we have
\[
\varphi_F([\mu]) = \varphi_F([\mu]^2) = \mu^2 = 1, \quad \varphi_F([2\mu]) = 2\mu^2 = 2, \\
\varphi_F([\mu]^2 [2\mu]) = 2\mu^2 = 2, \quad \varphi_F([2\mu]^2) = 0.
\]
Thus, an extremal \(\varphi_F\)-zero free sequence is \([\mu]^2 [2\mu]\).  \(\square\)

**Lemma 4.3.** Let \(p\) be a prime number such that \(p \geq 5\). Then, there exists an \(u \in \mathbb{F}_p^\ast\), such that \(-u(\lambda u + \mu)\) is not a quadratic residue modulo \(p\).

**Proof.** First observe that we can always find \(z_0 \in \mathbb{F}_p^\ast\) and \(z_1 \in \{1, 2, 3, 4\}\) such that
\[
\left(\frac{z_0}{p}\right) = -\left(\frac{z_0 + 1}{p}\right) \quad \text{and} \quad \left(\frac{z_1}{p}\right) = \left(\frac{z_1 + 1}{p}\right).
\]
Considering \(j = \lambda \mu^{-1} u\), we have
\[
\left(\frac{-u(\lambda u + \mu)}{p}\right) = \left(\frac{-\lambda}{p}\right) \cdot \left(\frac{\mu^2}{p}\right) \cdot \left(\frac{j}{p}\right) \cdot \left(\frac{j + 1}{p}\right),
\]
since
\[-u(\lambda u + \mu) = -\lambda^{-1} \mu^2 (\lambda \mu^{-1} u). (\lambda \mu^{-1} u + 1) = -\lambda^{-1} \mu^2 (j.(j + 1)).\]
Hence, according to $-\lambda$ being or not a quadratic residue modulo $p$, we can choose $j \in \{z_0, z_1\}$, in such a way that $-u(\lambda u + \mu)$ is not a quadratic residue modulo $p$. \qed

**Theorem 4.4.** Let $p \geq 5$ be a prime number and $s$ a positive integer. If for all $i \in \{1, \ldots, s\}$, we have $\left(\frac{j}{p}\right) = 1$, then $2p - 1 \geq D(\varphi_F, p) \geq p + s$.

**Proof.** The upper bound follows from Theorem 2.1(iv). Consider the sequence $S = [\omega_0]^{p-1}[u]^s$, with $u$ given in Lemma 4.3 and $\omega_0$ defined in (4.3). Since $\omega_0(\lambda \omega_0 + \mu) = 0$, we have $u \neq \omega_0$. Let $T = [\omega_0]^t[u]^i$ be any subsequence of $S$. Hence (see (4.2))

$$\varphi_F(T) = (t\omega_o + iu)^2 + i(u(\lambda u + \mu)).$$

According to the hypothesis and Lemma 4.3 we have

$$\left(\frac{-i(u(\lambda u + \mu))}{p}\right) = \left(\frac{i}{p}\right) \left(\frac{-u(\lambda u + \mu)}{p}\right) = -1.$$ 

Hence $S$ is a $\varphi_F$-zero free sequence, thus $D(\varphi_F, p) \geq (p - 1) + s + 1$ as desired. \qed

At this point, since $\omega_o$ has the property described in Lemma 4.1, one would expect to always find a $\varphi_F$-zero free sequence of the form $[\omega_o]^{p-1}[u_1]^{k_1} \cdots [u_t]^{k_t}$ in the set $M(\varphi_F, p)$. But thus far we do not have an answer for this supposition, although if this is the case one would obtain a better upper bound for the constant $D(\varphi_F, p)$.

**Theorem 4.5.** If among the extremal $\varphi_F$-zero free sequences in the set $M(\varphi_F, p)$ we can find a sequence of the type $S = [\omega_0]^{p-1}[u_1]^{k_1} \cdots [u_t]^{k_t}$, with $\omega_0$ as defined in (4.3), then

$$D(\varphi_F, p) \leq (p - 1) + \frac{p - 1}{2}.$$ 

**Proof.** After reordering the indexes, we can assume that $k_1 \geq \cdots \geq k_t$. Let $T = [\omega_o]^t[u_1]^{k_1} \cdots [u_t]^{k_t}$ be any subsequence of $S$. Since we are assuming that $S$ is a $\varphi_F$-zero free sequence, we must have $\varphi_F(T) \equiv 0 \pmod{p}$.

Let $\mathcal{N} = \{ (\ell_1, \ldots, \ell_t) : 0 \leq \ell_r \leq k_r, r = 1, \ldots, t \}$, then we can write

$$(4.5) \quad \varphi_F(T) = A(j, I)^2 - B(I),$$

with $I = (i_1, \ldots, i_t) \in \mathcal{N}$ and

$$(4.6) \quad B(I) = -\sum_{r=1}^{t} i_r u_r(\lambda u_r + \mu) \quad \text{and} \quad A(j, I) = j\omega_o + \sum_{r=1}^{t} i_r u_r.$$ 

*Acta Mathematica Hungarica* 169, 2023
Let $\mathcal{N}^* = \mathcal{N} \setminus \{(0, \ldots, 0)\}$. Note that for any $I \in \mathcal{N}^*$, we must have

\begin{equation}
\left( \frac{B(I)}{p} \right) = -1,
\end{equation}

otherwise $B(I) \equiv 0 \pmod{p}$ or $\left( \frac{B(I)}{p} \right) = 1$, which means that we could find $j \in \{0, 1, 2, \ldots, p - 1\}$ such that $A(j, I)^2 \equiv B(I) \pmod{p}$. In that case we would have found two $\varphi_F$-zero subsequences

$$T_0 = [\omega_o]^{j_0} [u_1]^{i_1} \cdots [u_t]^{i_t} \quad \text{and} \quad T_1 = [\omega_o]^{j_1} [u_1]^{i_1} \cdots [u_t]^{i_t}$$

of $S$ that is a $\varphi_F$-zero free sequence, a contradiction.

Now define the following disjoint subsets of $\mathcal{N}^*$:

\begin{align*}
\mathcal{I}_1 &= \{ (1, 0, \ldots, 0), (1, 1, 0, \ldots, 0), \ldots, (1, 1, \ldots, 1) \} \\
\mathcal{I}_2 &= \{ (2, 1, \ldots, 1), (2, 2, 1, \ldots, 1), \ldots, (2, 2, \ldots, 2) \} \\
\mathcal{I}_3 &= \{ (3, 2, \ldots, 2), (3, 3, 2, \ldots, 2), \ldots, (3, 3, \ldots, 3) \} \\
&\vdots \\
\mathcal{I}_{k_t} &= \{ (k_t, k_t - 1, \ldots, k_t - 1), \ldots, (k_t, k_t, \ldots, k_t) \} \\
\mathcal{I}_{k_t+1} &= \{ (k_t + 1, k_t, \ldots, k_t), \ldots, (k_t + 1, k_t + 1, \ldots, k_t) \} \\
&\vdots \\
\mathcal{I}_{k_t-1} &= \{ (k_t-1, k_t-1 - 1, \ldots, k_t-1 - 1, k_t), \ldots, (k_t-1, k_t-1, \ldots, k_t-1, k_t) \} \\
\mathcal{I}_{k_t} &= \{ (k_t-1 + 1, k_t-1, \ldots, k_t-1, k_t), \ldots, (k_t-1 + 1, k_t-1 + 1, \ldots, k_t-1 + 1, k_t-1, k_t) \} \\
&\vdots \\
\mathcal{I}_{k_3} &= \{ (k_2, k_2 - 1, k_3, \ldots, k_t), (k_2, k_2, k_3, \ldots, k_t) \} \\
\mathcal{I}_{k_2+1} &= \{ (k_2 + 1, k_2, k_3, \ldots, k_t) \} \\
&\vdots \\
\mathcal{I}_{k_1} &= \{ (k_1, k_2, k_3, \ldots, k_t) \}
\end{align*}

Let $\mathcal{J} = \mathcal{I}_1 \cup \mathcal{I}_2 \cup \cdots \cup \mathcal{I}_{k_t}$ and observe that $\mathcal{J} \subset \mathcal{N}^*$. Also note that the cardinality of this set $\mathcal{J}$ is equal to

$$|\mathcal{J}| = tk_t + (t - 1)(k_{t-1} - k_t) + (t - 2)(k_{t-2} - k_{t-1}) + \cdots + (t - j)(k_{t-j} - k_{t-j+1}) + \cdots + 2(k_2 - k_3) + k_1 - k_2 = k_1 + k_2 + \cdots + k_t.$$
Let $I_0 = (i_1, \ldots, i_t), I_1 = (i^*_1, \ldots, i^*_t) \in J$. By the formation of $J$, we may always assume $i_s \leq i^*_s$, for all $s \in \{1, \ldots, t\}$, and for at least one $r \in \{1, \ldots, t\}$ we have $i_r < i^*_r$. Thus,

$$I^* = (i^*_1 - i_1, \ldots, i^*_r - i_r, \ldots, i^*_t - i_t) \in N^*$$

and therefore, according to (4.7), we must have

$$B(I^*) = B(I_1) - B(I_0) \not\equiv 0 \pmod{p},$$

since $B(I)$ is a linear form in the indexes $i$ (see (4.6)). Therefore the values of $B(I)$ are all distinct for any $I \in J$, and also $\left(\frac{B(I)}{p}\right) = -1$, for all $I \in J$, (see (4.7)). The conclusion is that

$$|J| = k_1 + k_2 + \cdots + k_t \leq \frac{p-1}{2}.$$ 

Therefore, the length of the sequence $S$ is at most

$$|S| = p - 1 + k_1 + k_2 + \cdots + k_t \leq p - 1 + \frac{p-1}{2}. \quad \square$$

### 5. The special case of $\varphi_{F,m} = s_{m,1}^2 + s_{m,2} + s_{m,1}$

We want to present some results and comments about this special case, as a way of shedding more light on the bounds given in Theorems 4.4 and 4.5. Let us start with the corollary below, which is a straightforward consequence of the Quadratic Reciprocity Law and Theorem 4.4.

**Corollary 5.1.** Let $p$ be an odd prime. Then

(i) $D(\varphi_F, p) \geq p + 2$ if $p \equiv \pm 1 \pmod{24}$;

(ii) $D(\varphi_F, p) \geq p + 4$ if $p \equiv \pm 1 \pmod{60}$;

(iii) $D(\varphi_F, p) \geq p + 6$ if $p \equiv \pm 1$ or $\pm 49 \pmod{120}$.

Using these ideas it is easy to obtain Table 2 containing lower bounds for the Davenport $\varphi_F$-constant $D(\varphi_F, p)$.

On the other hand, a computer search using Sagemath [5], gives us the Table 3 containing the exact value for $D(\varphi_F, p)$, for $p \leq 31$, and also presenting extremal $\varphi_F$-zero free sequences, and the cardinality of the set $M(\varphi_F, p)$.

Observe that in the examples of extremal $\varphi_F$-zero free sequences given in Table 3, we can always find a sequence with the term $[-1]^{p-1}$. This strengthens our initial supposition that it is always possible to find extremal $\varphi_F$-zero free sequences containing the term $[\omega_v]^{p-1}$ (see (4.3)), for any prime $p$. But even for this special case we were not able to prove it. On the other hand, the tables above show us, that the exact value of $D(\varphi_F, p)$ seems to be closer to
Table 2: Bounds for $D(\varphi_F, p)$

| $D(\varphi_F, p)$ | Some elements of $M(\varphi_F, p)$ | $|M(\varphi_F, p)|$ |
|-------------------|-----------------------------------|----------------|
| $D(\varphi_F, 3) = 3$ | $[-1]^2$ | 1 |
| $D(\varphi_F, 5) = 6$ | $[1][-1]^4, [3][-1]^4$ | 2 |
| $D(\varphi_F, 7) = 9$ | $[1]^2[-1]^6, [1][5][-1]^6, [5]^2[-1]^6$ | 3 |
| $D(\varphi_F, 11) = 12$ | $[1]^8[2]^3, [3][-1]^{10}$ | 8 |
| $D(\varphi_F, 13) = 15$ | $[1]^{10}[7]^4, [1][2][-1]^{12}$ | 6 |
| $D(\varphi_F, 17) = 19$ | $[2]^2[-1]^{16}, [2][7][-1]^{16}$ | 16 |
| $D(\varphi_F, 23) = 27$ | $[1]^4[-1]^{22}, [1]^3[-2][-1]^{22}$ | 25 |
| $D(\varphi_F, 29) = 31$ | $[1]^{26}[12][13]^3, [6]^{12}[10]^{18}, [1][3][-1]^{28}$ | 54 |
| $D(\varphi_F, 31) = 34$ | $[1][11]^2[-1]^{30}, [7][8][22][-1]^{30}$ | 54 |

Table 3: Exact values of $D(\varphi_F, p)$

the lower bound given in Theorem 4.4. In conclusion, there are many points here to be clarified, and we believe that these are questions worthy to be pursued.

Acknowledgement. The authors would like to express their gratitude to the referees for their helpful suggestions which improved the presentation of this paper.
References

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

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

[3] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC (2006).

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

[5] The Sage Developers, SageMath, the Sage Mathematics Software System (Version 9.2), www.sagemath.org (2020).

Springer Nature or its licensor (e.g., a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.