Monomials and binomials over finite fields 
as \( \mathcal{R} \)-orthomorphisms

By WUN-SENG CHOU (Taipei) and HARALD NIEDERREITER (Singapore)

Abstract. We give criteria for both monomials and binomials of the form 
\( ax^{(q+1)/2} + bx \) to be \( \mathcal{R} \)-orthomorphisms of the finite field \( \mathbb{F}_q \) of odd order \( q \). We also 
prove existence theorems for \( \mathcal{R} \)-orthomorphisms of this form.

1. Introduction

Throughout this paper, \( q \) is a prime power and \( \mathbb{F}_q \) is the finite field 
of order \( q \). The polynomial \( f(x) \in \mathbb{F}_q[x] \) is called a permutation polynomial of \( \mathbb{F}_q \) if the function \( \sigma : \mathbb{F}_q \rightarrow \mathbb{F}_q \), defined by \( \sigma : a \mapsto f(a) \), is 
a permutation of \( \mathbb{F}_q \). Permutation polynomials of finite fields have been 
studied extensively (see [4, Chapter 7]). One important and useful class of 
permutation polynomials is the class of so-called orthomorphisms. Recall 
that \( f(x) \) is an orthomorphism of \( \mathbb{F}_q \) if both \( f(x) \) and \( f(x) - x \) are permuta-
tion polynomials of \( \mathbb{F}_q \). Orthomorphisms have interesting applications, 
for instance to the construction of orthogonal Latin squares (see [9, Chap-
ter 22]) and cryptology (see [8]). Orthomorphisms of \( \mathbb{F}_q \) are also closely 
connected with complete mapping polynomials of \( \mathbb{F}_q \), since \( f(x) \in \mathbb{F}_q[x] \) 
is an orthomorphism of \( \mathbb{F}_q \) if and only if \( -f(x) \) is a complete mapping 
polynomial of \( \mathbb{F}_q \). Complete mapping polynomials of \( \mathbb{F}_q \) were first studied 
by Niederreiter and Robinson [6], [7].

In this paper we consider a special class of orthomorphisms. Let 
\( \mathcal{R} \) be a nonempty set of positive integers. Then \( f(x) \) is called an \( \mathcal{R} \)-
orthomorphism of \( \mathbb{F}_q \) if each polynomial \( f^{(r)}(x) \) is an orthomorphism of \( \mathbb{F}_q \),
where \( r \in \mathcal{R} \) and \( f^{(r)}(x) \) is the \( r \)th iterated composition of \( f(x) \) with itself. The definition of \( \mathcal{R} \)-orthomorphisms is given explicitly by Cohen, Niederreiter, Shparlinski, and Zieve [1]. They also present examples of both linearized and sublinearized polynomials that are \( \mathcal{R} \)-orthomorphisms. In fact, some special types of \( \mathcal{R} \)-orthomorphisms have been used in combinatorial design theory (see [2]).

In Section 2 we study monomials as \( \mathcal{R} \)-orthomorphisms. Especially, we consider the monomial \( f(x) = ax^{(q+1)/2} \) as a concrete example, where \( q \) is odd. We show that for any positive integer \( k \) and any sufficiently large \( q \equiv 1 \mod 4 \) there exists an \( \mathcal{R}_k \)-orthomorphism of \( F_q \) of this form, where \( \mathcal{R}_k = \{1, 2, \ldots, k\} \). We study the special kind of binomials \( f(x) = ax^{(q+1)/2} + bx \) in Section 3. We show in this section that if \( \mathcal{R} \) is finite and \( q \) is sufficiently large, then there is at least one ordered pair \( (a, b) \in F_q^* \times F_q^* \) such that the polynomial \( f(x) = ax^{(q+1)/2} + bx \) is an \( \mathcal{R} \)-orthomorphism of \( F_q \). Here the lower bound on \( q \) is smaller than that in a comparable result in [1, Theorem 3].

2. Monomials as \( \mathcal{R} \)-orthomorphisms

In this section, \( f(x) \) is a monomial \( f(x) = ax^n \in F_q[x] \) with \( a \neq 0 \). Then, for any positive integer \( i \), we have \( f^{(i)}(x) = a^{n^i - 1 + \cdots + n + 1}x^n \). So, \( f^{(i)}(x) \) is a permutation polynomial of \( F_q \) if and only if \( \gcd(n^i, q - 1) = 1 \) (and thus, \( \gcd(n, q - 1) = 1 \)). The following is a criterion for \( f(x) \) to be an \( \mathcal{R} \)-orthomorphism. By the above remarks, the proof is obvious.

**Lemma 2.1.** The monomial \( f(x) = ax^n \in F_q[x], a \neq 0, \) is an \( \mathcal{R} \)-orthomorphism of \( F_q \) if and only if \( \gcd(n, q - 1) = 1 \) and for each \( m \in \mathcal{R} \), the equation

\[
\frac{x^{nm} - y^{nm}}{x - y} = a^{-(n^m - 1 + \cdots + n + 1)}
\]

has no solution in \( F_q \times F_q \setminus \{ (\alpha, \alpha) : \alpha \in F_q \} \).

From this lemma, it is trivial that for \( n = 1 \), \( f(x) = ax \in F_q[x] \) is an \( \mathcal{R} \)-orthomorphism of \( F_q \) if and only if \( a \neq 0, 1 \) and \( \mathcal{R} \) contains no multiple of the (multiplicative) order \( \text{ord}(a) \) of \( a \). So, if \( \mathcal{R} = \mathcal{R}_k = \{1, 2, \ldots, k\} \), then \( f(x) = ax, a \neq 0, \) is an \( \mathcal{R}_k \)-orthomorphism of \( F_q \) if and only if \( 1 \leq k < \text{ord}(a) \). For \( n > 1 \), let \( e_m = \gcd(n^{m-1} + \cdots + n + 1, q - 1) \) and \( d_m = \gcd(n - 1, \frac{q - 1}{e_m}) \).
Lemma 2.2. Let \( f(x) = ax^n \in F_q[x] \) with \( a \neq 0 \) and \( n > 1 \) and let \( m \) be a positive integer. Then \( f^{(m)}(x) - x \) has a root in \( F_q^* \) if and only if \( \text{ord}(a) \) divides \( (q - 1)/d_m \).

Proof. The polynomial \( f^{(m)}(x) - x \) has a root in \( F_q^* \) if and only if
\[
q^{n^{m-1} + n^{m-2} + \cdots + n + 1} n^{m-1} - 1 = 1
\]
has a root in \( F_q^* \). If \( g \) is a primitive element of \( F_q \) and \( a = g^s \) for some \( s > 0 \), then the last statement is equivalent to the existence of a positive integer \( t \) satisfying
\[
1 = g^{s(n^{m-1} + \cdots + n + 1) + t(n^{m-1})} = g^{(n^{m-1} + \cdots + n + 1)(s + t(n-1))},
\]
Thus, \( f^{(m)}(x) - x \) having a root in \( F_q^* \) is equivalent to \( s + y(n - 1) \equiv 0 \mod (q - 1)/e_m \) having a solution \( t \), which is equivalent to \( d_m | s \), and thus \( \text{ord}(a) \) dividing \( (q - 1)/d_m \). \( \square \)

The above lemma gives a necessary condition for a monomial to be an \( \mathcal{R} \)-orthomorphism.

Corollary 2.3. If \( f(x) = ax^n \in F_q[x] \), with \( n > 1 \) and \( a \neq 0 \), is an \( \mathcal{R} \)-orthomorphism of \( F_q \), then for all \( m \in \mathcal{R} \), \( \text{ord}(a) \) does not divide \( (q - 1)/d_m \).

We omit the proof because it is obvious. In the following, we consider the special kind of monomial \( f(x) = ax^{(q+1)/2} \in F_q[x] \), \( a \neq 0 \), \( q \) odd. Moreover, we take \( \mathcal{R} = \mathcal{R}_k \) with a positive integer \( k \). We first establish the following result on the iterates \( f^{(r)}(x) \).

Lemma 2.4. Let \( f(x) = ax^{(q+1)/2} \in F_q[x] \) with \( a \in F_q^* \) and \( q \) odd. Then, as functions on \( F_q \), the iterates of \( f \) are given by
\[
\begin{align*}
f^{(4s+1)}(x) &= a^{4s+1}x^{(q+1)/2}, \\
f^{(4s+2)}(x) &= a^{(q-1)/2 + 4s + 2}x, \\
f^{(4s+3)}(x) &= a^{(q-1)/2 + 4s + 3}x^{(q+1)/2}, \\
f^{(4(s+1))}(x) &= a^{d(s+1)}x,
\end{align*}
\]
for any nonnegative integer \( s \).

Proof. This is shown by straightforward induction, using the fact that \( x^q = x \) as a function on \( F_q \). \( \square \)
Notice that $f(x)$ is a permutation polynomial of $F_q$ if and only if $q \equiv 1$ \pmod{4}, because we need $\gcd((q + 1)/2, q - 1) = 1$. From now on in this section, we assume that $q \equiv 1$ \pmod{4}.

It follows from Lemma 2.4 that for an even positive integer $m$, $f^{(m)}(x) - x$ is a permutation polynomial of $F_q$ if and only if $\text{ord}(a)$ does not divide $m$ if $m \equiv 0 \pmod{4}$, or $m + 2^{-1}$ if $m \equiv 2 \pmod{4}$. Notice that if $c_m = \gcd(m, q - 1)$, then $\gcd(q - 1, \frac{m - 1}{2} + m) = c_m$ if $q \equiv 1 \pmod{8}$, and $\gcd(q - 1, \frac{m - 1}{2} + m) = 2c_m$ if $q \equiv 5 \pmod{8}$.

For the consideration of $f^{(m)}(x) - x$ for odd positive integers $m$, we recall the following result from [4, Theorem 7.11]. We denote by $\eta$ the quadratic character of $F_q$, with the convention $\eta(0) = 0$.

**Lemma 2.5.** For odd $q$, the polynomial $x^{(q+1)/2} + bx \in F_q[x]$ is a permutation polynomial of $F_q$ if and only if $\eta(b^2 - 1) = 1$.

Thus, for an odd positive integer $m$, it follows from Lemmas 2.4 and 2.5 that $f^{(m)}(x) - x$ is a permutation polynomial of $F_q$ if and only if $\eta(a^{2m} - 1) = 1$.

**Theorem 2.6.** Let $q$ be a prime power with $q \equiv 1 \pmod{4}$, let $k$ be a positive integer, and let $R_k = \{1, 2, \ldots, k\}$. Suppose that

$$q \geq 2^{(k-3)/2}(k + 1)^2q^{1/2} + 2^{(k-7)/2}(5k^2 + 12) + 1.$$ 

Then there exists an $a \in F_q^*$ such that $f(x) = ax^{(q+1)/2} \in F_q[x]$ is an $R_k$-orthomorphism of $F_q$.

**Proof.** For an odd positive integer $m$, define $g_m(x) = x^{2m} - 1$. For a positive integer $m$ with $m \equiv 0 \pmod{4}$, define $h_{0,m}(x) = x^{e_m} - 1$; and for $m \equiv 2 \pmod{4}$, define $h_{2,m}(x)$ to be either $h_{2,m}(x) = x^{e_m} - 1$ if $q \equiv 1$ \pmod{8}, or $h_{2,m}(x) = x^{2m} - 1$ if $q \equiv 5 \pmod{8}$. Now let $A_0$ be the set of roots in $F_q$ of all polynomials of the form $g_m(x)$ for odd integers $m$ with $1 \leq m \leq k$. It is easy to see that

$$|A_0| \leq 2 + \sum_{m=1 \text{ odd}}^{k} (2m - 2) \leq \frac{k^2 + 3}{2}.$$ 

Also, let $A_e$ be the set of roots in $F_q$ of all polynomials $h_{0,m}(x)$ and $h_{2,m}(x)$ for even integers $m$ with $1 \leq m \leq k$. Then it is not difficult to see that

$$|A_e \setminus A_o| \leq \sum_{m=1 \text{ mod 0}}^{k} (m - 2) \leq \frac{k^2}{8}.$$
Let $N$ be the number of elements $a \in F_q^*$ such that $f(x) = ax^{(q+1)/2}$ is an $R_k$-orthomorphism. Then

$$N = \frac{1}{2^{\left\lfloor \frac{k+1}{2} \right\rfloor}} \sum_{a \in F_q^* \setminus (A_o \cup A_e)} \prod_{m=1}^{k} (1 + \eta(a^{2m} - 1))$$

$$= \frac{1}{2^{\left\lfloor \frac{k+1}{2} \right\rfloor}} \left( \sum_{a \in F_q^*} \prod_{m=1, m \text{ odd}}^{k} (1 + \eta(a^{2m} - 1)) - \sum_{a \in A_o \cup A_e} \prod_{m=1, m \text{ odd}}^{k} (1 + \eta(a^{2m} - 1)) \right),$$

and so

$$N \geq \frac{N_1}{2^{\left\lfloor (k+1)/2 \right\rfloor}} - \frac{1}{2} |A_o \cup A_e| \geq \frac{N_1}{2^{\left\lfloor (k+1)/2 \right\rfloor}} - \frac{5k^2 + 12}{16},$$

with

$$N_1 := \sum_{a \in F_q^*} \prod_{m=1, m \text{ odd}}^{k} (1 + \eta(a^{2m} - 1)).$$

We can write

$$N_1 = q - 1 + \sum_{r=1}^{\left\lfloor (k+1)/2 \right\rfloor} \sum_{1 \leq m_1 < \ldots < m_r \leq k} \sum_{a \in F_q^* \atop m_j \text{ odd}} \eta \left( \prod_{j=1}^{r} (a^{2m_j} - 1) \right).$$

Consider the innermost sum on the right-hand side of (2.1). If the polynomial $\prod_{j=1}^{r} (x^{2m_j} - 1)$ is a square in $F_q[x]$, then the corresponding sum is clearly nonnegative. Otherwise by the Weil bound [4, Theorem 5.41],

$$\left| \sum_{a \in F_q^*} \eta \left( \prod_{j=1}^{r} (a^{2m_j} - 1) \right) \right| < 2q^{1/2} \sum_{j=1}^{r} m_j.$$

Therefore

$$N_1 > q - 1 - 2q^{1/2} \sum_{r=1}^{\left\lfloor (k+1)/2 \right\rfloor} \sum_{1 \leq m_1 < \ldots < m_r \leq k} \sum_{m_j \text{ odd}}^{r} m_j.$$
\[ q - 1 - 2^{\left(\frac{k+1}{2}\right)}q^{1/2}\sum_{m=1}^{k} m \]
\[ \geq q - 1 - 2^{\left(\frac{k+1}{2}\right)}\frac{(k+1)^2}{4}. \]

Altogether,
\[ N > \frac{q - 1}{2^{\left(\frac{k+1}{2}\right)}} - \frac{(k+1)^2}{4}q^{1/2} - \frac{5k^2 + 12}{16}, \]
and the desired result follows. \(\square\)

3. \(\mathcal{R}\)-orthomorphisms of the form \(ax^{(q+1)/2} + bx\)

In this section, we consider \(q\) odd and polynomials of the form \(f(x) = ax^{(q+1)/2} + bx \in F_q[x]\) with \(ab \neq 0\). It follows from Lemma 2.5 that \(f(x)\) is a permutation polynomial of \(F_q\) if and only if \(\eta(b^2 - a^2) = 1\). Note that \(f\) is a linear function when restricted to the squares in \(F_q\) and another linear function when restricted to the nonsquares in \(F_q\). This observation and induction yield the following formulas for the iterates of \(f\) as functions on \(F_q\). If \(\eta(b + a) = \eta(b - a) = 1\), then for each positive integer \(n\) we have
\[ f^{(n)}(x) = \frac{(b + a)^n - (b - a)^n}{2}x^{(q+1)/2} + \frac{(b + a)^n + (b - a)^n}{2}, \]
If \(\eta(b + a) = \eta(b - a) = -1\), then for each positive integer \(n\) we have
\[ f^{(n)}(x) = \frac{(b^2 - a^2)^{(n-1)/2}ax^{(q+1)/2} + (b^2 - a^2)^{(n-1)/2}bx}{2} \]
whenever \(n\) is odd and
\[ f^{(n)}(x) = \frac{(b^2 - a^2)^{n/2}}{2}x \]
whenever \(n\) is even. From these formulas, the following criterion is trivial.

**Lemma 3.1.** Let \(\mathcal{R}\) be a nonempty set of positive integers. Then the polynomial \(f(x) = ax^{(q+1)/2} + bx \in F_q[x]\) with \(ab \neq 0\) is an \(\mathcal{R}\)-orthomorphism of \(F_q\) if and only if one of the following two conditions holds:
1. \(\eta(b + a) = \eta(b - a) = 1\) and \(\eta(((b + a)^m - 1)((b - a)^m - 1)) = 1\) for all \(m \in \mathcal{R}\);
(ii) \( \eta(b + a) = \eta(b - a) = -1 \) and for all \( m \in \mathbb{R} \), \( (b^2 - a^2)^{m/2} \neq 1 \) if \( m \) is even and \( \eta((b^2 - a^2)^{(m-1)/2}(b+a) - (b^2 - a^2)^{(m-1)/2}(b-a) - 1)) = 1 \) if \( m \) is odd.

Using this lemma, we have the following counting formula which is closely related to a result of MENDELSOHN and WOLK [5] (see also EVANS [3]) for the special case where \( q \) is a prime.

**Corollary 3.2.** If \( q \equiv 3 \mod 4 \), then there are exactly \( \frac{(q-3)(q-5)}{4} \) orthomorphisms of \( F_q \) of the form \( f(x) = ax^{(q+1)/2} + bx \in F_q[x] \) with \( ab \neq 0 \). If \( q \equiv 1 \mod 4 \), then there are exactly \( \frac{(q-5)^2}{4} \) orthomorphisms of \( F_q \) of the form \( f(x) = ax^{(q+1)/2} + bx \in F_q[x] \) with \( ab \neq 0 \).

**Proof.** From Lemma 3.1, for \( a, b \in F_q^* \), the polynomial \( f(x) = ax^{(q+1)/2} + bx \) is an orthomorphism of \( F_q \) if and only if \( \eta((b-a)(b+a)) = 1 \) and \( \eta((b-a-1)(b+a-1)) = 1 \). Let \( N \) be the number of orthomorphisms counted in the corollary. After the substitution \( u = b - a \) and \( v = b + a \), we see that \( N \) is the number of ordered pairs \( (u, v) \in G_q \times G_q \) with \( u \neq \pm v, \eta(uv) = 1, \eta((u-1)(v-1)) = 1 \). We can restrict \( u \) and \( v \) to \( G_q := F_q \setminus \{0, 1\} \). Then we can write

\[
N = N_1 - N_2,
\]

where \( N_1 \) is the number of ordered pairs \( (u, v) \in G_q \times G_q \) with \( \eta(uv) = 1, \eta((u-1)(v-1)) = 1 \), and \( N_2 \) is the number of ordered pairs \( (u, v) \in G_q \times G_q \) with \( u = \pm v, \eta(uv) = 1, \eta((u-1)(v-1)) = 1 \). We have

\[
N_1 = \frac{1}{4} \sum_{u,v \in G_q} [1 + \eta(uv)][1 + \eta((u-1)(v-1))]
\]

\[
= \frac{(q-2)^2}{4} + \frac{1}{4} \sum_{u,v \in G_q} \eta(uv) + \frac{1}{4} \sum_{u,v \in G_q} \eta((u-1)(v-1))
\]

\[
+ \frac{1}{4} \sum_{u,v \in G_q} \eta(uv)\eta((u-1)(v-1))
\]

\[
= \frac{(q-2)^2}{4} + \frac{1}{4} \left( \sum_{u \in G_q} \eta(u) \right)^2 + \frac{1}{4} \left( \sum_{u \in G_q} \eta(u-1) \right)^2
\]

\[
+ \frac{1}{4} \left( \sum_{u \in G_q} \eta(u(u-1)) \right)^2
\]
\[
\frac{(q - 2)^2}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = \frac{q^2 - 4q + 7}{4},
\]

where we used [4, Theorem 5.48] to evaluate the last character sum.

Now we consider \( N_2 \). All ordered pairs \((u, v) \in G_q \times G_q \) with \( u = v \) are counted for \( N_2 \) and this gives \( q - 2 \) ordered pairs. If \( u = -v \), then the conditions become \( \eta(-v^2) = 1, \eta(1 - v^2) = 1 \). This is only possible if \( q \equiv 1 \mod 4 \), since only then \( \eta(-1) = 1 \). In this case, it remains to count the number \( N_3 \) of \( v \in G_q \) with \( \eta(1 - v^2) = 1 \). We have

\[
N_3 = \frac{1}{2} \sum_{v \in G_q} (1 + \eta(1 - v^2)) - \frac{1}{2} = \frac{q - 3}{2} + \frac{1}{2} \sum_{v \in G_q} \eta(1 - v^2)
\]

\[
= \frac{q - 3}{2} + \frac{1}{2} \sum_{v \in F_q} \eta(1 - v^2) - \frac{1}{2} = \frac{q - 5}{2},
\]

where we again used [4, Theorem 5.48]. Thus, if \( q \equiv 1 \mod 4 \), then

\[
N_2 = q - 2 + \frac{q - 5}{2} = \frac{3q - 9}{2},
\]

whereas \( N_2 = q - 2 \) if \( q \equiv 3 \mod 4 \). Recalling (3.1), we get the claimed result. \( \square \)

The following theorem shows the existence of \( \mathcal{R} \)-orthomorphisms of \( F_q \) of the form \( f(x) = ax^{(q+1)/2} + bx \in F_q[x] \) for sufficiently large \( q \). The condition on \( q \) in this result is less restrictive than that in the comparable result in [1, Theorem 3].

**Theorem 3.3.** Let \( \mathcal{R} \) be a finite nonempty set of positive integers and \( q \) an odd prime power with

\[
q \geq 2^{R+2} \left( 2 + \sum_{m \in \mathcal{R}} m \right),
\]

where \( R \) is the cardinality of \( \mathcal{R} \). Then there exists at least one ordered pair \((a, b) \in F_q^* \times F_q^* \) such that the polynomial \( f(x) = ax^{(q+1)/2} + bx \) is an \( \mathcal{R} \)-orthomorphism of \( F_q \).

**Proof.** Let \( N \) be the number of ordered pairs \((a, b) \in F_q^* \times F_q^* \) such that the polynomial \( f(x) = ax^{(q+1)/2} + bx \) is an \( \mathcal{R} \)-orthomorphism
of $F_q$. Let $N_1$ be the number of ordered pairs $(a, b) \in F_q \times F_q$ such that
\[ \eta(b + a) = \eta(b - a) = 1 \]
and
\[ \eta(((b + a)^m - 1)((b - a)^m - 1)) = 1 \quad \text{for all } m \in \mathcal{R}. \]

By using only condition (i) in Lemma 3.1, we see that

\[ N_1 \leq N + \# \{(a, b) \in F_q \times F_q : ab = 0, \ \eta(b + a) = \eta(b - a) = 1\}, \]

and so

\[ (3.2) \quad N \geq N_1 - q + 1. \]

Let $C := \{(a, b) \in F_q \times F_q : b = \pm a\}$ and $D$ be the set of $(a, b) \in F_q \times F_q$ with

\[ ((b + a)^m - 1)((b - a)^m - 1) = 0 \quad \text{for some } m \in \mathcal{R}. \]

Then

\[
N_1 = \frac{1}{2^{R+2}} \sum_{(a, b) \in F_q \times F_q} [1 + \eta(b + a)][1 + \eta(b - a)] \\
\cdot \prod_{m \in \mathcal{R}} [1 + \eta(((b + a)^m - 1)((b - a)^m - 1))] \geq \frac{S}{2^{R+2}} - \frac{1}{2}|C \cup D|
\]

with

\[ S := \sum_{a, b \in F_q} [1 + \eta(b + a)][1 + \eta(b - a)] \prod_{m \in \mathcal{R}} [1 + \eta(((b + a)^m - 1)((b - a)^m - 1))]. \]

By carrying out the substitution $u = b + a$ and $v = b - a$ in the sum $S$, we
obtain
\[ S = \sum_{u,v \in F_q} (1 + \eta(u))(1 + \eta(v)) \prod_{m \in \mathcal{R}} (1 + \eta((u^m - 1)(v^m - 1))) \]

\[ = \sum_{u,v \in F_q} (1 + \eta(u))(1 + \eta(v)) \]

\[ + \sum_{r=1}^{R} \sum_{m_1 < m_2 < \ldots < m_r} \sum_{u,v \in F_q} (1 + \eta(u))(1 + \eta(v)) \prod_{j=1}^{r} \eta((u^{m_j} - 1)(v^{m_j} - 1)) \]

\[ = \left( \sum_{u \in F_q} (1 + \eta(u)) \right)^2 \]

\[ + \sum_{r=1}^{R} \sum_{m_1 < m_2 < \ldots < m_r} \left( \sum_{u \in F_q} (1 + \eta(u)) \prod_{j=1}^{r} \eta(u^{m_j} - 1) \right)^2 \geq q^2. \]

In view of (3.2), this yields
\[ N \geq \frac{q^2}{2R+2} - \frac{1}{2} |C| - \frac{1}{2} |D| - q + 1. \]

It is clear that \(|C| = 2q - 1\). Furthermore, \(|D|\) is the number of \((u, v) \in F_q \times F_q\) with \((u^m - 1)(v^m - 1) = 0\) for some \(m \in \mathcal{R}\). Therefore
\[ |D| \leq 2q \sum_{m \in \mathcal{R}} m. \]

Altogether, we get
\[ N \geq \left( \frac{q^2}{2R+2} - 2 - \sum_{m \in \mathcal{R}} m \right)q + \frac{3}{2}, \]

and the desired result follows.

Acknowledgements. This paper was partially supported by the National Science Council in Taiwan, ROC, under the grant number 88-2115-M-001-002. The second author is grateful to the Academia Sinica in Taipei for supporting his visit during which this work was initiated. The authors thank an anonymous referee for several useful suggestions on the presentation of the material.
Monomials and binomials over finite fields as $R$-orthomorphisms

References


