An upper bound on the covering radius of a class of cyclic codes

Evgeniya Velikova
velikova@fmi.uni-sofia.bg
Asen Bojilov
bojilov@fmi.uni-sofia.bg
Faculty of Mathematics and Informatics, Sofia University,
5 James Baucher blvd, Sofia, BULGARIA

Abstract. In this paper we consider a class of cyclic $[p^m - 1, p^m - 2m - 1]$-codes over $\mathbb{Z}_p$, where $p \neq 2$ is a prime number, and we show that these codes have covering radius at most 3.

1 On the number of solutions of some equations

Let $F$ be the Galois field $\text{GF}(q)$ where $q = p^m$ and $p = \text{char} F$ is prime. We assume that $p \neq 2$ and that $\beta$ is a generator of the multiplicative group $F^*$ of the field $F$. Let us define the following sets

$$Q = \langle \beta^2 \rangle \cup \{0\} = \{a \in F \mid \exists b \in F: a = b^2\}$$

of the perfect squares in $F$ and

$$N = \beta\langle \beta^2 \rangle = F \setminus Q = \{a \in F \mid \exists b \in F: a = \beta b^2\}$$

of nonsquares in $F$.

We shall prove the next lemma following [5].

Lemma 1.1 Let $M$ be the set of the solutions $(x, y)$ of the equation $Ax^2 + By^2 = C$ in the finite field $F$ with $q$ elements and let $D = AB \neq 0$. Then the following fact holds

$$|M| = \begin{cases} 
q - \left(\frac{-D}{q}\right), & \text{if } C \neq 0, \\
q + \left(\frac{-D}{q}\right)(q - 1), & \text{if } C = 0,
\end{cases}$$

1This work was partially supported by the SF of Sofia University under Contract 171/05.2008.
Proof. Let us denote
\[ M_{x_0} = \{ y \in F \mid Ax_0^2 + By^2 = C \} = \{ y \in F \mid y^2 = -D \left( x_0^2 - \frac{C}{A} \right) \in Q \} \]

Therefore,
\[ |M_{x_0}| = \begin{cases} 0, & \text{if } -D \left( x_0^2 - \frac{C}{A} \right) \in N, \\ 1, & \text{if } \left( x_0^2 - \frac{C}{A} \right) = 0, \\ 2, & \text{if } D \left( x_0^2 - \frac{C}{A} \right) \neq 0 \text{ and } \left( x_0^2 - \frac{C}{A} \right) \in Q \end{cases} \]

and
\[ |M_{x_0}| = \left( \frac{-D(x_0^2 - \frac{C}{A})}{q} \right) + 1 = \left( \frac{-D}{q} \right) \left( \frac{x_0^2 - \frac{C}{A}}{q} \right) + 1, \]

where
\[ \left( \frac{a}{q} \right) = \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{if } a \in Q, a \neq 0, \\ -1, & \text{if } a \in N \end{cases} \]

is the generalized symbol of Legendre in the finite field \( F \) with \( q \) elements.

Therefore,
\[ |M| = \sum_{x \in F} |M_x| = \sum_{x \in F} \left( \left( \frac{-D}{q} \right) \left( \frac{x^2 - \frac{C}{A}}{q} \right) + 1 \right) = q + \left( \frac{-D}{q} \right) \sum_{x \in F} \left( \frac{x^2 - \frac{C}{A}}{q} \right). \]

First, let us consider the case \( A = 1 \) and \( B = -1 \). It is clear that
\[ |M| = \begin{cases} q - 1, & \text{if } C \neq 0, \\ 2q - 1, & \text{if } C = 0. \end{cases} \]

In this case \( D = -1 \)
\[ \sum_{x \in F} \left( \frac{x^2 - \frac{C}{A}}{q} \right) = \begin{cases} -1, & \text{if } C \neq 0, \\ q - 1, & \text{if } C = 0. \end{cases} \]

Now in the general case we have that
\[ |M| = q + \left( \frac{-D}{q} \right) \sum_{x \in F} \left( \frac{x^2 - \frac{C}{A}}{q} \right) = \begin{cases} q + \left( \frac{-D}{q} \right) \left( -1 \right) = q + \left( \frac{-D}{q} \right), & \text{if } C \neq 0, \\ q + \left( \frac{-D}{q} \right) (q - 1), & \text{if } C = 0. \end{cases} \]

\[ \square \]
Lemma 1.2 Let \( f(x) = Ax^2 + Bx + C \in F[x] \), \( A \neq 0 \), \( B \neq 0 \), and let
\[
M = \{ x^2 \mid x \in F, \ f(x^2) = f(\gamma x^2) \text{ for some } \gamma \in N \}.
\]
Then \(|M| = \frac{q+1}{2}\).

Proof. Let \( x \) be a solution of the equation \( f(x^2) = f(\gamma x^2) \) for some \( \gamma \in N \). Obviously \( x = 0 \) is a solution of that equation. For the next considerations we shall assume that \( x \neq 0 \). Then
\[
Ax^4 + Bx^2 + C = A\gamma^2 x^4 + B\gamma x^2 + C
\]
\[
Ax^2 + B = A\gamma^2 x^2 + B\gamma
\]
\[
A(1 - \gamma^2)x^2 = B(\gamma - 1)
\]
and
\[-A(1 + \gamma)x^2 = B,
\]
since \( \gamma \neq 1 \ (1 \in Q) \).

Note that \( \gamma \in N \) iff there exists \( u \in F, \ b \neq 0 \) such that \( \gamma = \beta u^2 \).
We are looking for \( \gamma \) in such form and \( u \neq 0 \).
It is clear that \( \gamma \neq -1 \ (B \neq 0) \). Then
\[
x^2 = -\frac{B}{A} \cdot \frac{1}{1 + \gamma}.
\]

If \( AB \in N \) then \( 1 + \gamma \in N \) and we must find \( v \in F \) such that \( 1 + \beta u^2 = \beta v^2 \).
From Lemma 1.1 we know that there exist \( q - 1 \) pairs \((u, v)\) which are the solutions of the last equation. Note that \( u = 0 \) is not a solution and therefore we have \( \frac{q-1}{2} \) different elements \( \gamma \) such that \( 1 + \gamma \in N \) and \(|M| = \frac{q-1}{2} + 1 = \frac{q+1}{2} \).

Analogously, the case \( AB \in Q \) give us again that \(|M| = \frac{q+1}{2} \). Indeed, \( 1 + \gamma \in Q \) and we must find \( v \in F \) such that \( 1 + \beta u^2 = v^2 \). By Lemma 1.1 it follows that there exist \( q + 1 \) pairs \((u, v)\) which are the solutions of the last equation. Note that \( u = 0 \) is a solution and therefore we have \( \frac{q-1}{2} \) (\( \gamma \neq 0 \)) different elements \( \gamma \) such that \( 1 + \gamma \in N \) and \(|M| = \frac{q-1}{2} + 1 = \frac{q+1}{2} \). \( \square \)
2 On covering radius of some cyclic codes

Let us denote by \( f_a(x) \in \mathbb{Z}_p[x] \) the minimal polynomial of \( a \in F \), \(|F| = q = p^m\). Clearly, \( f_a \) is an irreducible polynomial and \( \deg f_\beta = \deg f_{\beta^{-1}} = m \).

We consider the cyclic code \( C \) of length \( q - 1 \) over the field \( F \) generated by \( g(x) = f_\beta(x)f_{\beta^{-1}}(x) \). Hence, \( C \) is a \([q - 1, q - 1 - 2m]\)-code.

Following the techniques of [1], [3] and [4], we obtain the next theorem.

**Theorem 2.1** The \([p^m - 1, p^m - 1 - 2m]\)-code \( C \) defined above has covering radius at most 3 for \( p \neq 2 \) and \( q > 36 \).

**Proof.**

Let \( H = \begin{pmatrix} 1 & \beta & \beta^2 & \cdots & \beta^{q-1} \\ 1 & \gamma & \gamma^2 & \cdots & \gamma^{q-1} \end{pmatrix} \)

be a parity check matrix of the code \( C \).

Let \( s = (a, b) \in F^2 \), \((a, b) \neq (0, 0)\). We shall prove that there exists a vector \( e \in F^{q-1} \) with syndrome \( s \). For that purpose we must prove that the system

\[
\begin{align*}
& a_1x_1 + a_2x_2 + \cdots + a_lx_l = a \\
& a_1x_1 + a_2x_2 + \cdots + a_lx_l = b
\end{align*}
\]

has a solution with \( a_1, a_2, \ldots, a_l \in \mathbb{Z}_p \) and \( x_1, x_2, \ldots, x_l \in F \) for some natural number \( l \leq 3 \).

For \( l = 1 \) it is clear that the system (1) has a solution iff \( ab \) is a nonzero perfect square in \( \mathbb{Z}_p \).

Let us consider the following system

\[
\begin{align*}
& x_1 + x_2 + x_3 = a \\
& \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = b
\end{align*}
\]

where \((a, b) \neq (0, 0)\) and \( ab \neq 1 \).

Set \( y_i = \frac{1}{x_i} \). Then we obtain an analogous system as (2) in which \( a \) and \( b \) are changed. Hence, we may assume that \( b \neq 0 \).

Let us consider the function \( D_1(y) = 4by^2 + (-a^2b^2 + 6ab + 3)y + 4a \).

In the case \(-a^2b^2 + 6ab + 3 \neq 0\) by Lemma 1.2 it follows that there are \( c \in F \) and \( \gamma \in N \) such that \( D_1(c^2) = D_1(\gamma c^2) \) and \( c^2 \) takes \( \frac{q+1}{2} \) different values. We choose \( y = c^2 \) or \( y = \gamma c^2 \) in such a way that \( D = -yD_1(y) \) is a perfect square.
If $q > 35$, it is clear that there exists $y$ such that $y \neq 0$, $y \neq -\frac{1}{b}$, $y \neq -a$ and the system (2) has a solution

$$x_1 = \frac{a + y}{1 + y^b}, \quad x_2 = \frac{(ab - 1)y + \sqrt{D}}{2b(1 + y^b)}, \quad x_3 = \frac{(ab - 1)y - \sqrt{D}}{2b(1 + y^b)}.$$  

In the case $-a^2b^2 + 6ab + 3 = 0$ we consider the system

$$\begin{cases} x_1 + x_2 + x_3 = \frac{a}{2} \\ \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} = \frac{b}{2}. \end{cases}$$

It is clear that $-\frac{a^2b^2}{16} + \frac{3ab}{2} + 3 \neq 0$ and this system has a solution $x_1, x_2, x_3$ which is a solution of the system (1) with $a_1 = a_2 = a_3 = 2$.

Therefore, the covering radius of code $C$ is at most 3. \hfill \Box

References


