ON BINARY CYCLIC CODES WITH MINIMUM DISTANCE $d = 3$

P. Charpin, A. Tietäväinen, and V. Zinoviev

We consider binary cyclic codes of length $2^m - 1$ generated by a product of two or several minimal polynomials. Sufficient conditions for the minimum distance of such a code to be equal to three are found.

1. Introduction

Denote the finite field of order $q$, $q = 2^m$, $m \geq 4$, by $\mathbb{F}_q$. Let $\gamma$ be a primitive element of $\mathbb{F}_{2^m}$ and $m_i(x)$ be the minimal polynomial of $\gamma^i$ over $\mathbb{F}_2$. We assume that $0 \leq i < j \leq 2^m - 2$ and that $i$ and $j$, $0 \leq i < j \leq 2^m - 2$, are not in the same cyclotomic coset modulo $n = 2^m - 1$. Denote the binary cyclic code of length $n$ with generator $m_i(x)m_j(x)$ by $C_{i,j}(m)$ or, briefly, by $C_{i,j}$. The minimum distance of $C_{i,j}$ is denoted by $d_{i,j} = d_{i,j}(m)$.

It is well known [1] that the case $(i,j) = (1,3)$ corresponds to the 2-error-correcting BCH codes. The following pairs $(i,j)$ also define codes with minimum distance five (of course, there are many equivalent pairs): $(1,2^t + 1)$ if $\gcd(t,m) = 1$ (see [1, Sec 15.4]); $(1,2^{2t} - 2^t + 1)$ for odd $m$ if $\gcd(t,m) = 1$ (see [2, 3]) and for even $m$ if $\gcd(t,m)$ is odd (see [2]) and if $\gcd(t,m) = 1$ (see [4]). On the other hand, it was proved in [5] that for fixed $t$ ($t \equiv 3 \pmod{4}$, $t \geq 4$) there is no infinite family of codes $C_{1,t}(m)$ with minimum distance 5. It is natural to try to characterize all pairs $(i,j)$ that give codes with a certain minimum distance $d$, where $d = 2, 3, 4, or 5$. If $d = 2$, this can easily be done (see Lemma 1). However, in all other cases the task is certainly much more difficult. In this paper we consider the case $d = 3$.

We consider also (binary cyclic) codes $C_{i_1, \ldots, i_t}$, whose generating polynomial is the product of one or several minimal functions $m_{i_1}(x), \ldots, m_{i_t}(x)$. We find sufficient conditions (Theorems 1 and 2) for the cyclic code $C_{i_1, \ldots, i_t}$ to have minimum distance $d = 3$. We also find lower bounds on the number of codewords of weight three (Theorems 3 and 4). The codes $C_{i_1, \ldots, i_t}$ are investigated in a more detailed way. In the case $t = 2^n(n^2 - 1)$ we give necessary and sufficient conditions that $d_{i_1, \ldots, i_t}$ equals three (Theorem 5). The results of this paper were in part announced in [6].

As usual, we identify the vector $c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_2^n$ and the polynomial

$$c(x) = \sum_{t=0}^{n-1} c_t x^t \in \mathbb{F}_2[x]/(x^n + 1).$$

A vector $c$ is an element of $C_{i,j}$ if and only if

$$c(\gamma^i) = c(\gamma^j) = 0.$$  \hspace{1cm} (1)

Thus, $d_{i,j} \leq 3$ if there is a trinomial $c(x) = 1 + x^a + x^b$, $1 \leq a < b < n$, such that Eqs (1) are valid.

We begin with a simple example (mentioned in [7] for the case $(i,j) = (1,7)$). Let $m$ be even. Then 3 divides $2^m - 1$. Denote $(2^m - 1)/3$ by $u$. Then $\gamma^u$ (denote it by $\beta = \gamma^u$) is a primitive element of $\mathbb{F}_4$ and,
therefore, the minimal polynomial of $\beta$ is $1 + x + z^2$. If we choose $c(x) = 1 + z^u + z^{2u}$, we see that Eqs. (1) are valid for all $i$ and $j$ which are not divisible by 3. Thus, we have proved the following result.

**Proposition 1.** Let $m, m > 2$, be even and $i, j, 1 \leq i < j \leq 2^m - 2$, be arbitrary integers. If $\gcd(i, 3) = \gcd(j, 3) = 1$, then the code $C_{i,j}$ of length $2^m - 1$ has distance $d_{i,j} \leq 3$.

In the sequel, we generalize this observation for the case where $m$ has an arbitrary divisor $g \geq 2$. This approach gives a way of characterizing some infinite classes of codes with minimum distance $d \geq 3$.

## 2. General results

First, we characterize the codes $C_{i,j}$ with minimum distance $d_{i,j} = 2$.

**Lemma 1.** Let $i, j, 0 \leq i < j \leq 2^m - 2$, be arbitrary integers that do not belong to the same cyclotomic coset modulo $2^m - 1$. Then the binary cyclic code $C_{i,j}$ of length $n = 2^m - 1$ with generating polynomial $g(x) = m_i(x)m_j(x)$ has distance $d_{i,j} = 2$ if and only if $\gcd(n, i, j) > 1$.

**Proof.** Since $\gamma$ is a primitive $n$th root of unity, $d_{i,j} = 2$ if and only if there exist $k$ and $\ell$, $0 \leq \ell < k < n$, such that

$$\gamma^{ki} = \gamma^{\ell i}, \quad \gamma^{kj} = \gamma^{\ell j}$$

or, equivalently,

$$(k - \ell)i \equiv (k - \ell)j \equiv 0 \pmod{n}$$

Both congruences are valid if and only if $n/\gcd(n, i, j)$ divides $k - \ell$. Therefore, such $k$ and $\ell$ exist if and only if $\gcd(n, i, j) > 1$.

**Definition.** Denote by $K_g(r)$ the cyclotomic coset of $r$ modulo $2^g - 1$, i.e.,

$$K_g(r) = \{ r2^k \pmod{2^g - 1} : k = 0, 1, \ldots, g - 1 \}$$

For any integer $i, 0 \leq i \leq 2^m - 2$, we say that $i$ belongs to $K_g(r)$ if an integer $j, j = 0, 1, \ldots, g - 1$, exists such that $r2^j \equiv r \pmod{2^g - 1}$.

**Theorem 1.** Let $i, j, 0 < i < j < 2^m - 1$, be arbitrary integers that do not belong to the same cyclotomic coset modulo $2^m - 1$. Let $g$ be an arbitrary divisor of $m$. If there exists an integer $r$, $0 < r < 2^g - 1$, where $\gcd(r, 2^g - 1) = 1$, such that both $i$ and $j$ are in $K_g(r)$, then the binary cyclic code $C_{i,j}$ of length $2^m - 1$ generated by the polynomial $g(x) = m_i(x)m_j(x)$ has minimum distance $d_{i,j} \leq 3$. If, moreover, $\gcd(n, i, j) = 1$, then $d_{i,j} = 3$.

**Proof.** If $\gamma$ is a primitive $n$th element of $\mathbb{F}_q, q = 2^m$, then $[8]$ the element $\beta = \gamma^u$, where $u = (2^m - 1)/(2^g - 1)$, is a primitive element of $\mathbb{F}_{2^g}$. Let $k$ be an integer in the interval $[1, 2^g - 2]$ such that

$$1 + \beta + \beta^k = 0.$$

Define

$$c(x) = 1 + x^{u(1/r)} + x^{u(k/r)}, \quad (2)$$

where the quotients $1/r$ and $k/r$ are calculated in the ring $\mathbb{F}_2[x]$ of integers modulo $2^g - 1$ and, therefore, lie in the interval $[1, 2^g - 2]$. We claim that $c(x)$ is a codeword of $C_{i,j}$. To check this, it suffices to show that both $\gamma^i$ and $\gamma^j$ are roots of the polynomial $c(x)$. Indeed, since $i \in K_g(r)$, nonnegative integers $k$ and $\ell$ exist such that

$$i = \ell(2^g - 1) + 2^k r.$$

Thus,

$$c(\gamma^i) = 1 + \gamma^{u(1/r)} + \gamma^{u(k/r)} = 1 + \beta^{(1/r)} + \beta^{(k/r)}$$

$$= 1 + \beta^{2^k r(1/r)} + \beta^{2^k r(k/r)} = 1 + \beta^{2^k} + \beta^{2^{2k}} = (1 + \beta + \beta^k)^{2^k} = 0.$$

288
Similarly we can show that \( c(\gamma^k) = 0 \). Thus, we have proved that \( c(x) \) of type (2) belongs to \( C_{1,i,j} \) and, therefore, the minimum distance of this code is \( d \leq 3 \). If now \( \gcd(n, i, j) = 1 \), then by Lemma 1 the code \( C \) has distance \( d > 2 \), whence it follows that \( d = 3 \). \( \Delta \)

Note that Proposition 1 is a particular case \((g = 2)\) of the first statement of Theorem 1.

As follows from the proofs, the statements given above (i.e., Lemma 1 and Theorem 1) can be generalized to the case where the code \( C \) is generated by a polynomial \( g(x) \) which is a product of several minimal functions. In particular, the following generalization of Theorem 1 is valid.

**Theorem 2.** Let \( i_1, \ldots, i_n, 0 < i_1 < \cdots < i_n < 2^m - 1 \), be arbitrary integers that belong to distinct cyclotomic cosets modulo \( 2^m - 1 \). Let \( g \) be an arbitrary divisor of \( m \). If there exists an integer \( r, 0 < r < 2^g - 1 \), where \( \gcd(r, 2^g - 1) = 1 \), such that all integers \( i_1, \ldots, i_n \), are in \( K_3(r) \), then the binary cyclic code \( C_{i_1, \ldots, i_n} \) of length \( 2^m - 1 \) generated by the polynomial \( g(x) = m_{i_1}(x) \cdots m_{i_n}(x) \) has minimum distance \( d_{i_1, \ldots, i_n} \leq 3 \). If, moreover, \( \gcd(n, i_1, \ldots, i_n) = 1 \), then \( d_{i_1, \ldots, i_n} = 3 \).

We emphasize that Theorems 1 and 2 give only sufficient conditions that the binary cyclic code \( C = C_{i_1, \ldots, i_n} \) has minimum distance \( d_{i_1, \ldots, i_n} = 3 \). For such a code \( C \), we now try to estimate the number of codewords of weight three (denote it by \( B_3 \)). We need some notations. Let \( I(r) \) be the set of all integers \( i \) in \([1, n - 1]\) such that \( i \in K_3(r) \) (see Definition). Clearly, \( I(r) \) is a join of cosets modulo \( n \). Denote by \( J(r) \) a set of representatives of these cosets and denote by \( C_{J(r)} \) the binary cyclic code of length \( n \) generated by the polynomial

\[
g_{J(r)}(x) = \prod_{i \in I(r)} m_i(x).
\]

**Theorem 3.** Let \( i_1, \ldots, i_n, 0 < i_1 < \cdots < i_n < 2^m - 1 \), be arbitrary integers, \( g \) be an arbitrary divisor of \( m \), and an integer \( r, 0 < r < 2^g - 1 \), where \( \gcd(r, 2^g - 1) = 1 \), be such that \( \{i_1, \ldots, i_n\} \subseteq J(r) \). Then \( B_3 \) for the binary cyclic code \( C_{i_1, \ldots, i_n} \) of length \( 2^m - 1 \) satisfies the inequality

\[
B_3 \geq B = (2^m - 1)(2^g - 2)/6.
\]

For the code \( C_{J(r)} \), i.e., if \( \{i_1, \ldots, i_n\} = J(r) \), the inequality in (3) turns into the equality.

**Proof.** Let \( u = (2^m - 1)(2^g - 1) \). Then the order of the element \( \beta = \gamma^u \) is \( 2^g - 1 \) and, therefore, \( \beta \) is a primitive element of the field \( \mathbb{F}_{2^m} \), of order \( 2^g \), the latter being a subfield of \( \mathbb{F}_{2^n} \).

For each integer \( a, 1 \leq a \leq 2^g - 2 \), there is exactly one integer \( b \) in the interval \([1, 2^g - 2]\) such that

\[
1 + \beta^a + \beta^b = 0,
\]

and, of course, \( b \neq a \). Thus, there are exactly \((2^g - 2)/2\) pairs \((a, b), 1 \leq a < b \leq 2^g - 2\), such that the trinomial

\[
c(x) = 1 + x^{au/r} + x^{bu/r}
\]

(where the quotients \( a/r \) and \( b/r \) are calculated in the ring \( \mathbb{Z}_{2^m - 1} \)) is a codeword of any such code \( C = C_{i_1, \ldots, i_n} \). Hence, we have found \((2^g - 2)/2\) weight-3 codewords of type (5) that belong to \( C \). From any such codeword we obtain, by shifting, \( n = 2^m - 1 \) codewords of the type

\[
x^t c(x) = x^t + x^{at+u(r)} + x^{bt+u(r)}, \quad t = 0, 1, \ldots, 2^m - 2
\]

Thus, we have obtained the set of \((2^m - 1)(2^g - 2)/2\) codewords of weight 3. But it is easily seen from the construction that each word is obtained exactly three times. Thus, the number \( B_3 \) of codewords of weight three in \( C_{i_1, \ldots, i_n} \) satisfies the inequality (3).

Assume now that \( C = C_{J(r)} \). Consider an arbitrary weight-3 word of this code with locators \( \{\gamma^a, \gamma^b\} \). Then, by the definition,

\[
1 + \gamma^{au(2^g - 1)+r} + \gamma^{bu(2^g - 1)+r} = 0
\]

for any \( \ell \in [0, u - 1] \), \( u = (2^m - 1)/(2^g - 1) \). Therefore, by adding to any such equation (which corresponds to the case \( \ell = 0 \)), we obtain

\[
\gamma^{a\ell} \left( \gamma^{au(2^g - 1)} + 1 \right) + \gamma^{b\ell} \left( \gamma^{bu(2^g - 1)} + 1 \right) = 0
\]

289
for any \( \ell \). Thus, the polynomial

\[
Q(x) = \gamma^x(x^u + 1) + \gamma^x(x^v + 1)
\]

has as its roots all \( u \) elements of the type \( \lambda_\ell = (\gamma^x)^{2^u - 1} = \beta^\ell \), where \( \ell \in [0, u - 1] \). Since each such element \( \lambda_\ell \) is a non-root of unity, the polynomial \( x^u + 1 \) (which has as its roots all those \( u \) elements \( \lambda_\ell \)) should divide \( Q(x) \). So the remainder \( R(x) \) of \( Q(x) \) modulo \( x^u + 1 \) must be the zero polynomial. We have

\[
R(x) = \gamma^a(x^a + 1) + \gamma^b(x^b + 1),
\]

where \( a' < u, b' < u, a' \equiv a \) (modu), and \( b' \equiv b \) (modu). The equation \( R(x) = 0 \) is satisfied if and only if one of the following conditions holds:

(i) \( \gamma^x = \gamma^x \) and \( a' = b' \);

(ii) \( x^a = 1 \) and \( x^b = 1 \).

Condition (i) is impossible, because \( \gamma^x + \gamma^x \) equals 1. So, (ii) holds, proving that \( a' = b' = 0 \). Therefore, \( u \) divides \( a \) and \( b \). Hence, any weight-3 codeword of the code \( C_{k(x)} \) (up to a shift \( t \)) is of the form (6)

Therefore, the number \( B_3 \) (of weight-3 codewords in \( C_{k(x)} \)) satisfies \( B_i \), i.e., corresponds to the equality in (3).

It is difficult to determine the number of codewords of weight three for an arbitrary code \( C_{i_1, \ldots, i_s} \). We give here a statement which is a generalization of Theorem 3.

Theorem 4. Let \( i_1, \ldots, i_s, 1 \leq i_1 < \ldots < i_s \leq 2^m - 2 \), be arbitrary integers. Let \( \{g_1, \ldots, g_s\} \) be distinct divisors of \( m \) such that \( \gcd(g_i, g_j) = 1 \) for any \( 1 \leq h < \ell \leq k \). If there exist \( k \) integers \( r_h \), where \( 1 \leq r_h \leq 2^{2^{k_h}} - 2 \), \( \gcd(r_h, 2^{2^k} - 1) = 1 \), such that

\[
\{i_1, \ldots, i_s\} \subseteq K_{g_h}(r_h)
\]

for any \( h (h = 1, \ldots, k) \), then the number \( B_3 \) of codewords of weight three in \( C_{i_1, \ldots, i_s} \) satisfies the inequality

\[
B_3 \geq \frac{2^m - 1}{6} \sum_{h=1}^k (2^{2^{k_h}} - 2).
\]

Proof. Recalling the arguments that we used in the proof of Theorem 3, we see that for any \( h, h \in \{1, \ldots, k\} \), in \( C = C_{i_1, \ldots, i_s} \), there are exactly \( (2^m - 1)(2^{2^k} - 2)/6 \) weight-3 codewords of the form

\[
c_h(x) = x^1 + x^{u_3}(a_1/r_h^u) + x^{u_3}(a_2/r_h^u),
\]

where \( u \in \{0, 1, \ldots, 2^m - 2\} \), \( u_h = (2^m - 1)/(2^{2^k} - 1) \), the integers \( a_1 \) and \( a_2 \), \( 1 \leq a_1 < a_2 \leq 2^{2^k} - 2 \), are defined by the equation

\[
1 + \beta_h^{a_1} + \beta_h^{a_2} = 0
\]

(here \( \beta_h = \gamma_h^{a_1} \) is a primitive element of the field \( \mathbb{F}_{2^{2^k}} \), and the quotients \( a_1/r_h \) and \( a_2/r_h \) are calculated in the ring of integers modulo \( 2^{2^k} - 1 \). Therefore, to prove Theorem 4, it suffices to show that \( c_h(x) \) does not coincide with a codeword of another type, say, of type \( c_2(x) \) (which corresponds, for instance, to a divisor \( g_2 \in \{g_1, \ldots, g_s\} \) of \( m \)),

\[
c_2(x) = x^u + x^{u_3}(a_1/r_h^u) + x^{u_3}(a_2/r_h^u), \quad h \neq \ell.
\]

Assume the contrary, i.e., \( c_h(x) = c_2(x) \). Then the quotients of the locators of \( c_h(x) \) and \( c_2(x) \) are, respectively, \( \gamma^{a_1} \) and \( \gamma^{a_2} \). Since \( \gcd(u_h, u_3) = (2^m - 1)/\gcd(2^{2^k} - 1, 2^{2^k} - 1) = 2^m - 1 \), they are equal to 1, which provides a contradiction.

Example 1. Let \( m = 6 \). Then the divisors of \( m \) are the numbers 2 and 3. Since 1, 11, and 23 belong to both the coset \( K_2 \) and the coset \( K_3 \), all the (binary cyclic) codes \( C_{1,11}, C_{1,23}, C_{1,1}, C_{1,12}, C_{1,23} \) and \( C_{1,11} \) have minimum distance \( d = 3 \) by Theorem 2. Then, by Theorem 4, we have \( B_3 \geq 84 \). In this case, this bound is attained for all codes mentioned above.
3. The codes $C_{1,t}$

In this section, we consider cyclic codes $C_{1,t}$ of length $n = 2^m - 1$ with roots $\gamma$ and $\gamma^t$, where an integer $t$ is not a power of 2. Note that if $n$ is a prime, then any code $C_{i,j}$ is equivalent to some code $C_{1,t}$. The code $C_{1,t}$ has a codeword of weight three if and only if there are two distinct nonzero elements $\alpha_1$ and $\alpha_2$ of $\mathbb{F}_{2^n}$ which satisfy

$$\alpha_1^t + \alpha_2^t + (\alpha_1 + \alpha_2)^t = 0.$$

Since $C_{1,t}$ is cyclic, we can take $\alpha_1 = 1$. Thus, we have the following result.

**Proposition 2.** The code $C_{1,t}$ has minimum distance $d_{1,t} = 3$ if and only if the polynomial

$$U_t(z) = 1 + z^t + (1 + z)^t$$

has at least one root in $\mathbb{F}_{2^n} \setminus \{0, 1\}$.

**Proof.** By Theorem 1, we know that if $t = (2^g - 1)\ell + 2^k$ for some $k < g$, where $g$ divides $m$, then $C_{1,t}$ has minimum distance $d_{1,t} = 3$. Here we want to generalize this result and also to obtain sufficient conditions that $d_{1,t} > 3$. Moreover, we want to present some cases where the bound on $B_2$ given in Theorem 4 is attained.

**Example 2.** For some $t$, the minimum distance is at least 4 when $m$ is odd. Take, for example, $t = 13$. Then the polynomial

$$U_{13}(x) = x(1 + x)(x^2 + x + 1)^5$$

has roots in $\mathbb{F}_{2^n} \setminus \{0, 1\}$ if and only if $m$ is even. Thus, according to Proposition 2, $d_{1,13} \geq 4$ if and only if $m$ is odd.

**Example 3.** The next case, $t = 21$, is a little more complicated. We have

$$U_{21}(x) = x(1 + x)(x^2 + x^3 + 1)(x^6 + x^4 + x^3 + x + 1)(x^6 + x^5 + x^3 + x^2 + 1).$$

Hence, the minimum distance of $C_{1,21}$ is at least 4 if and only if 6 does not divide $m$. Note that this last case is not covered by Theorem 1.

Now, we have two observations. First, $U_t(x)$ is a product of minimal polynomials over $\mathbb{F}_2$. This is because

$$U_t(\beta^2) = 1 + \beta^t + (1 + \beta^t)^t = (1 + \beta^t + (1 + \beta)^t)^2 = (U_t(\beta))^2,$$

and, therefore, whenever $\beta$ is a root of $U_t(x)$, the element $\beta^2$ is a root, too. Second, we have the following statement.

**Proposition 3.** Let $m$ be a prime and $t$ be an integer such that $1 < t < m + 3$. Then the code $C_{1,t}$ of length $2^m - 1$ has minimum distance $d \geq 4$.

**Proof.** The polynomial $U_t(x)$ has degree $t - 1$. Moreover, the elements 0 and 1 are roots of $U_t(x)$. Therefore, $U_t(x)$ may be represented in the form $U_t(x) = (x^2 + x)V_t(x)$, where the degree of $V_t(x)$ is $t - 3$. If an element $\beta \in \mathbb{F}_{2^n}$ exists such that $V_t(\beta) = 0$, then the minimal polynomial of $\beta$ divides $V_t(x)$ and should have degree $m$. This contradicts the last assumption of the proposition.

Furthermore, we have the following fact.

**Proposition 4.** Let $g$ and $t \geq 3$ be arbitrary integers such that $2^g < t$ and assume that the equivalence

$$t \equiv 2^k \pmod{2^g - 1}$$

holds for some integer $k$, $k \geq 1$. Then the polynomial $x^{2^k} + x$ divides $U_t(x)$, i.e., all elements of the field $\mathbb{F}_{2^g}$ are roots of $U_t(x)$.

**Proof.** Let $\beta$ be a nonzero element of $\mathbb{F}_{2^g}$, i.e., $\beta^{2^g-1} = 1$. Then we have

$$U_t(\beta) = 1 + \beta^t + (1 + \beta)^t = 1 + \beta^{2^k} + (1 + \beta)^{2^k} = 0.$$

$\triangle$
Proposition 5. Let $u, v, 1 \leq v < u$, be arbitrary integers and let $t = 2^u \pm (2^v - 1)$. Then

\[
U_t(z) = \begin{cases} 
(z^{2^u} + z) (z^{2^v} + z) / (z^2 + z) & \text{if } t = 2^u + 2^v - 1, \\
(z^{2^u} + z) \left( \frac{z^{2^{u+v}} + z}{z^2 + z} \right)^2 & \text{if } t = 2^u - 2^v + 1.
\end{cases}
\tag{7}
\]

\textbf{Proof.} First consider the case $t = 2^u + 2^v - 1$. The condition $t \equiv 2^u \pmod{2^u - 1}$ and Proposition 4 imply that

\[(z^{2^u} + z) \mid U_t(z).\]

Similarly, from the condition $t \equiv 2^v \pmod{2^v - 1}$ we obtain that

\[(z^{2^v} + z) \mid U_t(z).\]

Define

\[L(z) = \frac{(z^{2^u} + z)(z^{2^v} + z)}{z(z + 1)}.\]

It is clear that the degree of $L(z)$ is equal to $t - 1$, i.e., it is exactly the degree of $U_t(z)$. This means that if $\gcd(u, v) = 1$, then we have proved that $L(z) = U_t(z)$. Assume now that $\gcd(u, v) > 1$ and consider the derivative of $U_t(z)$:

\[U_t'(z) = z^{t-1} + (1 + z)^{t-1}.\]

Let $\beta \in (F_{2^u} \cap F_{2^v}) \setminus \{0, 1\}$, i.e., the conditions $\beta^{2^u-1} = 1$ and $\beta^{2^v-1} = 1$ hold simultaneously. Then, if $\beta$ is neither 0 nor 1,

\[U_t'(\beta) = \beta^{2^u-1+2^v-1} + (1 + \beta)^{2^u-1+2^v-1} = 1 + 1 = 0.\]

Set

\[W(z) = \frac{\gcd(z^{2^u} + z, z^{2^v} + z)}{z(z + 1)}.\]

Then we have proved that $(W(z))^2 \mid L(z)$. Therefore, in each case $L(z) = U_t(z)$.

Let now $t = 2^u - 2^v + 1$. Similarly to the previous case, the condition $t \equiv 2^u \pmod{2^u - 1}$ and Proposition 4 imply that $z^{2^v} + z$ divides $U_t(z)$. Since $t = 2^u(2^{u-v} - 1) + 1$, we have $t \equiv 1 \pmod{2^u - 1}$, and therefore $z^{2^{u-v}} + z$ also divides $U_t(z)$. Now let us show that $U_t(z)$ is actually divisible by the polynomial

\[\left( \frac{z^{2^{u-v}} + z}{z^2 + z} \right)^2.\tag{8}\]

This last condition is equivalent to the fact that for any element $\beta \in F_{2^{u-v}} \setminus \{0, 1\}$ the polynomial $(z + \beta)^{2^v}$ divides $U_t(z)$. Now represent $U_t(z)$ in the following form:

\[U_t(z) = 1 + z^t + (1 + z)^t = 1 + z^{2^u(2^{u-v} - 1)}z^t + \frac{(1 + z)^t}{(z + 1)^2^{v-1}(1 + z)}(1 + z).
\]

Now, replacing $z^{2^v}$ in the expression above by the element $\beta^{2^v}$, we can find the remainder, say, $R_t(z)$, of the division of $U_t(z)$ by $(z^{2^v} + \beta^{2^v})$. Since $\beta^{2^{u-v} - 1} = 1$, we have

\[R_t(z) = 1 + \beta^{2^v}z^{2^{u-v} - 1}z + (1 + \beta^{2^v})^{2^{v-1} - 1}(1 + z) = 1 + z + (1 + z) = 0.
\]

Thus, $U_t(z)$ is divisible by the polynomial (7). On the other hand, it is easy to see that the polynomials $z^t$ and $(1 + z)^2$ do not divide $U_t(z)$. Now the second equality of (7) follows by comparing the degrees of both polynomials.

Using Proposition 5, we can now formulate the necessary and sufficient conditions for the code $C_{1, t}$, where $t = 2^u \pm (2^v - 1)$, to have minimum distance $d = 3$. Also, these two classes of codes are interesting in the sense that the lower bound on $B_3$ in Theorem 4 is exact.
Theorem 5. Let \( u, v, 1 \leq u < v \), be arbitrary integers and let \( t = 2^u \pm (2^v - 1) \). Denote
\[
\delta_t = \begin{cases} 
\gcd(m,u) & \text{if } t = 2^u + 2^v - 1, \\
\gcd(m,u-v) & \text{if } t = 2^u - 2^v + 1, 
\end{cases}
\]
and \( \delta_t = \gcd(m,v) \). Then the code \( C_{1,t} \) has minimum distance \( d_{1,t} \geq 4 \) if and only if \( \delta_1 = \delta_2 = 1 \), and \( d_{1,t} = 3 \) otherwise. For the number \( B_3 \) of this code we have the following expression:
\[
B_3 = \frac{2^m - 1}{6} \left( 2^{d_1} + 2^{d_2} - 2^{d_3} - 2 \right),
\]
where \( \delta_3 = \gcd(\delta_1, \delta_2) \).

Proof. First, consider the case \( t = 2^u + 2^v - 1 \). If \( \delta_1 = \delta_2 = 1 \), then the polynomial
\[
U_t(x) = (x^{2^u} + x)(x^{2^v} + x)/(x^2 + x)
\]
has no roots in the field \( \mathbb{F}_{2^m} \) distinct from 0 and 1, and therefore \( d_{1,t} \geq 4 \). Otherwise, \( C_{1,t} \) contains codewords of weight three. Since we know all the roots of \( U_t(x) \), we can write down the exact expression for the number \( B_3 \) in \( C_{1,t} \). If \( \delta_1 > 1 \) but \( \delta_2 = 1 \) (and, therefore, \( \delta_3 = 1 \)), then the polynomial \( U_t(x) \) has \( 2^{d_1} - 2 \) roots (which are elements of \( \mathbb{F}_{2^{d_1}} \)) distinct from 0 and 1. Recalling the arguments that we have used for the proof of Theorem 3, we obtain in this case the following expression:
\[
B_3 = \frac{2^m - 1}{6} \left( 2^{d_1} - 2 \right),
\]
which coincides with (10) for the case \( \delta_2 = \delta_3 = 1 \). Let now \( \delta_1 > 1 \) and \( \delta_2 > 1 \), but \( \delta_3 = 1 \). Then the polynomial \( U_t(x) \) has \( 2^{d_1} - 2 \) roots (elements of \( \mathbb{F}_{2^{d_1}} \)) distinct from 0 and 1 and \( 2^{d_2} - 2 \) roots (elements of \( \mathbb{F}_{2^{d_2}} \)) distinct from 0 and 1. Since the intersection of these fields is only the subfield \( \mathbb{F}_2 = \{0,1\} \), in this case the polynomial \( U_t(x) \) has \( (2^{d_1} - 2) + (2^{d_2} - 2) \) different roots distinct from 0 and 1. This gives that the number of codewords of weight three is
\[
B_3 = \frac{2^m - 1}{6} \left( ((2^{d_1} - 2) + (2^{d_2} - 2) \right),
\]
which exactly agrees with the lower bound of Theorem 4. Thus, for this case that bound is exact. Let now all \( \delta_i > 1 \), \( i = 1, 2, 3 \). This means that the intersection of \( \mathbb{F}_{2^{d_1}} \) and \( \mathbb{F}_{2^{d_2}} \) is a subfield \( \mathbb{F}_{2^{d_3}} \). Therefore, in this case the polynomial \( U_t(x) \) has
\[
(2^{d_1} - 2) + (2^{d_2} - 2) - (2^{d_3} - 2)
\]
different roots, which gives the corresponding expression for \( B_3 \). The case \( t = 2^u - 2^v + 1 \) is quite similar. The fact that \( U_t(x) \) is divisible by the polynomial (10), i.e., that \( U_t(x) \) has multiple roots, does not influence the number of weight-3 codewords corresponding to the divisor \( \delta_1 \) of \( m \). The derivation of the expression for \( B_3 \) is similar to the previous case \( \Delta \).

4. The case \( g = 3 \)

In this section, we treat the case \( g = 3 \), i.e., the case where codes are of length \( n = 2^m - 1 \), and 3 divides \( m \). Let \( C = C_{1,t_2} \), to be a binary cyclic code generated by the polynomial \( g(x) = m_1(x) \) \( m_1(x) \), where the integers \( t_i, 0 < i_j < n \), are in distinct cyclotomic cosets modulo \( n \). All such integers \( t_i \) (representatives of the cyclotomic cosets modulo \( n \)) belong to one of three cyclotomic cosets modulo \( t_i \), namely, \( K_3(0), K_3(1) \), and \( K_3(2) \). As above, denote by \( J(r) \) the set of all such integers \( t_i \) that belonging to \( K_3(r) \), where \( r = 0, 1, 3 \).

Proposition 6. Let 3 divide \( m \). Let integers \( t_1, \ldots, t_3 \) (representatives of distinct cyclotomic cosets modulo \( n = 2^m - 1 \)), where \( \gcd(n, t_1, \ldots, t_3) = 1 \), be such that \( \{t_1, \ldots, t_3\} \subseteq K_3(r), r \in \{1, 3\} \). Then
(a) the cyclic code \( C = C_{1,1,4} \) has minimum distance \( d = 3 \);
(b) the number \( B_3 \) for \( C \) satisfies the inequality \( B_3 \geq 2^m - 1 \);
(c) these codewords are the trinomials \( c_h(x) = 1 + x^{(h/r)} + x^{u(3/r)} \) and all their cyclic shifts, where \( h \in \{1, 2\}, u = (2^m - 1)/7 \), and the quotients \( h/r \) and \( 3/r \) are calculated in the ring \( \mathbb{Z}_7 \).

**Proof.** By Theorem 2, the code \( C \) has minimum distance three. Let \( \gamma \) be a primitive element of the field \( \mathbb{F}_{2^m} \). Then \( \beta = \gamma^u \), where \( u = (2^m - 1)/7 \), is a primitive element of the field \( \mathbb{F}_8 \), the latter being a subfield of \( \mathbb{F}_{2^m} \). Since
\[
x^2 + 1 = (x^3 + x + 1) (x^3 + x^2 + 1) (x + 1),
\]
the minimal polynomial of \( \beta \) over \( \mathbb{F}_2 \) is \( m_1(x) = 1 + x^h + x^3 \), where \( h \) is either 1 or 2. Assume, for instance, that it is \( m_1(x) \), i.e., \( 1 + \beta + \beta^3 = 0 \), and let
\[
f(x) = 1 + x^{(1/r)} + x^{(3/r)},
\]
where the division is made in the ring \( \mathbb{Z}_7 \). Then the polynomial \( c(x) = f(x^u) \) is a codeword of the code \( C = C_{1,1,4} \), for any \( i_1, \ldots, i_4 \), from the set \( J(r) \). In particular, \( c(x) \) is a codeword of the code \( C_{J(r)} \) (see the proof of Theorem 3). If \( r = 1 \), then \( c(x) = 1 + x^u + x^{3u} \). The condition \( i \in J(1) \) means that \( i = 7i_1 + i_2 \), where \( i_2 \in K_3(1) \) (i.e., \( i_2 = 2^i \)). Therefore, for such \( i \) we have
\[
c(y) = 1 + \gamma^{i_2u} + \gamma^{3i_2u}
= 1 + \beta^{i_2} + \beta^{3i_2}
= (1 + \beta + \beta^3)^{i_2} = 0.
\]

If \( r = 3 \), then \( c(x) = 1 + x^{(1/3)} + x^{2u} \). Since \( \beta^{1/3} = \beta^3 \), we have \( c(x) = 1 + x^u + x^{5u} \). With the help of cyclic shifts by \( 2u \) positions, we obtain
\[
c'(x) = x^{2u} c(x) = 1 + x^{2u} + x^{3u}.
\]
Similarly, the condition \( i \in J(3) \) means that \( i = 7i_1 + i_2 \), where \( i_2 \in K_3(3) \) (i.e., \( i_2 = 2^2 \)). Therefore, we have
\[
c'(y) = 1 + \gamma^{2i_2u} + \gamma^{3i_2u}
= 1 + \beta^{2i_2} + \beta^{3i_2}
= (1 + \beta^6 + \beta^9)^{i_2}
= (1 + \beta + \beta^3)^{2i_2} = 0.
\]

Thus, we have proved that the polynomial \( 1 + x^u + x^{3u} \) and all its cyclic shifts are codewords of a code \( C_{i_1, \ldots, i_4} \), where \( \{i_1, \ldots, i_4\} \) is any (nonempty) subset of \( J(1) \), while the polynomial \( 1 + x^{2u} + x^{3u} \) and all its cyclic shifts are codewords of a code \( C_{i_1, \ldots, i_2} \), where \( \{i_1, \ldots, i_2\} \) is any (nonempty) subset of \( J(3) \). So for any such code \( C \) we have \( B_3 \geq 2^m - 1 \). For the code \( C_{J(r)} \), where \( r \in \{1, 3\} \), this number is exactly the maximal possible number (see Theorem 3). \( \triangle \)

For the code \( C_{3,5} \), the divisibility of \( m \) by 3 is a necessary and sufficient condition for \( d_{3,5} = 3 \). For the proof we apply the method used in [9].

**Proposition 1.** The code \( C_{3,5} \) of length \( 2^m - 1 \) has distance \( d_{3,5} = 3 \) if and only if 3 divides \( m \). In this case, its minimum-weight codewords are exactly all \( B_3 = 2^m - 1 \) codewords of weight three of the code \( C_{J(3)} \). If 3 does not divide \( m \), the code \( C_{3,5} \) has minimum distance \( d_{3,5} \geq 4 \).

**Proof.** Note that \( C_{3,5} \) cannot have minimum distance two because \( \text{gcd}(3, 5) = 1 \). Therefore, we assume that there is a codeword \( c(x) \) of weight three in \( C_{3,5} \) given by its locators \( \{X_1, X_2, X_3\} \). Define the locator polynomial of \( c(x) \) as
\[
s(x) = \prod_{i=1}^3 (1 - X_i z) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3,
\]
where

\[
\sigma_1 = X_1 + X_2 + X_3 + X_1 X_2 + X_1 X_3 + X_2 X_3
\]
\[
\sigma_2 = X_1 X_2 + X_1 X_3 + X_2 X_3 - X_1 - X_2 - X_3
\]
\[
\sigma_3 = -1.
\]
<table>
<thead>
<tr>
<th>n</th>
<th>m</th>
<th>g</th>
<th>B₃</th>
<th>r</th>
<th>J(r), Representatives of Cosets</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>1</td>
<td>1, 5, 7</td>
</tr>
<tr>
<td>63</td>
<td>6</td>
<td>2</td>
<td>21</td>
<td>1</td>
<td>1, 5, 7, 11, 13, 23, 31</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>63</td>
<td>1</td>
<td>9</td>
<td>1, 9, 11, 15, 23</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>5, 13, 27, 31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>255</td>
<td>8</td>
<td>2</td>
<td>85</td>
<td>1</td>
<td>1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 43, 47, 53, 55, 59, 61, 85, 91, 95, 119, 127</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>595</td>
<td>1</td>
<td>17, 19, 23, 31, 47, 53, 61, 91</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>11, 13, 29, 37, 43, 59, 119, 127</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>511</td>
<td>9</td>
<td>3</td>
<td>511</td>
<td>1</td>
<td>1, 9, 11, 15, 23, 25, 29, 37, 39, 43, 51, 53, 57, 79, 85, 93, 95, 107, 109, 123, 127, 183, 191, 219, 239</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>5, 13, 17, 19, 27, 31, 41, 45, 47, 55, 59, 61, 73, 75, 83, 87, 103, 111, 117, 125, 255, 171, 187, 223</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5115</td>
<td>1</td>
<td>33, 35, 39, 47, 63, 95, 101, 109, 125, 219, 157, 159, 171, 187, 343, 221</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>17, 37, 43, 55, 79, 99, 105, 117, 127, 167, 179, 189, 375, 347, 223, 251</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>9, 41, 49, 51, 71, 103, 111, 165, 173, 175, 191, 351, 235, 237, 253, 439</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>259</td>
<td>15, 23, 27, 29, 61, 77, 85, 89, 91, 123, 147, 151, 511, 213, 215, 247, 495</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

and its power sum symmetric functions

\[ S_k = X_1^k + X_2^k + X_3^k, \quad k \in \{0, 1, \ldots, n-1\}. \]

It is known that the elements \( \sigma_1 \) and functions \( S_k \) are related by the Newton identities. This means that they satisfy the relations

\[
\begin{align*}
S_1 + \sigma_1 &= 0, \\
S_3 + S_2 \sigma_1 + S_1 \sigma_2 + \sigma_3 &= 0, \\
S_5 + S_4 \sigma_1 + S_3 \sigma_2 + S_2 \sigma_3 &= 0.
\end{align*}
\]

Taking cyclic shifts of the codeword \( c(z) \), we can assume \( S_1 = 1 \). Furthermore, by the definition of \( C_{3,5} \), we have \( S_3 = S_5 = 0 \). Thus, by (11) we obtain

\[ \sigma_1 = S_1 = 1, \quad \sigma_2 = 0, \quad \sigma_3 = 1 \]
(recall that $S_3 = S_3^2$) Then $\sigma_\epsilon(z) = 1 + z + z^3$ is the unique locator polynomial up to a cyclic shift for a codeword of weight three. But this polynomial splits in the field of order $2^m$ if and only if $3$ divides $m$. Therefore, $C_{3,4}$ has minimum distance $d_{3,5} = 3$ if and only if $3$ divides $m$. Otherwise, $d_{3,5} \geq 4$. The number $B_3$ for this code equals $n$ (i.e., the number of different cyclic shifts of the polynomial $\sigma_\epsilon(z) = 1 + z + z^3$).

5. A table of codes with $d \leq 3$

To illustrate the results of the previous sections, we give a table of binary cyclic codes of length $n = 2^{2r} - 1$ with minimum distance $d \leq 3$ (Table 1). For any divisor $g$ of $m$ and for any coset representative $g$ modulo $2^r - 1$, where $r$ and $2^r - 1$ are coprime, a complete list $J(r)$ of representatives of cosets modulo $n$ is given. Any cyclic code $C_f$ generated by the polynomial

$$m_j = \prod_{i \in I} m_i(x),$$

where $I$ is any nonempty subset of $J(r)$, has minimum distance $d \leq 3$. If it satisfies the conditions of Lemma 1, then $d = 2$. The number $B_3 \geq r$, where $B$ is defined by (3) and is given in the table, can be evaluated according to Theorems 3, 4, and 5.

The authors are indebted to N. Sendrier [10] for checking some numerical results with his own programs.

REFERENCES