On Binary Cyclic Codes with $d = 3$

Pascale Charpin

INRIA,Codes,Domaine de Voluceau-Rocquencourt
BP 105 - 78153, Le Chesnay, FRANCE

Aimo Tietäväinen

Victor Zinoviev

Institute for Problems of Information Transmission
of the Russian Academy of Sciences
Bol'shoi Karetnyi 19, Moscow 101447, RUSSIA

Turku Centre for Computer Science
TUCS Technical Report No 26
June 1996

ISBN 951-650-782-4
ISSN 1239-1891

Abstract

We characterize several classes of cyclic codes of length $2^m - 1$ which have minimum distance three. We are mainly interested in codes with generator $m_i(x)m_j(x)$, but we also treat the cases when the generator polynomial is a product of several (or many) such $m_i(x)$.

Keywords: cyclic code, trinomials

TUCS Research Group
Coding Theory Group

1 Introduction

Denote the finite field of order q by F_q. Let γ be a primitive element of F_{2^m} and $m_s(x)$ the minimal polynomial of γ^s over F_2. We assume that i and j are not in the same 2-cyclotomic coset modulo $n := 2^m - 1$ and denote the binary cyclic code of length n with generator $m_i(x)m_j(x)$ by $C_{i,j}$. The minimum distance of $C_{i,j}$ is denoted by $d_{i,j}$. Van Lint and Wilson [8], [9] studied the minimum distance of some codes $C_{i,j}$. In [8] they proved that in general $d_{i,j}$ cannot be more than five. Observing that the case $(i,j) = (1,3)$ corresponds to the 2-error-correcting BCH code whose minimum distance is five, they were interested in the existence of other pairs (i,j) defining other codes with minimum distance five. We have here a different point of view. We are interested in the codes $C_{i,j}$ whose minimum distance is (at most) three. We found the sufficient conditions (Theorems 2 and 3) when a cyclic code $C_{i_1,\dots,i_s}$ with generator $m_{i_1}(x)\cdots m_{i_s}(x)$ has the minimal distance 3. We bound the number of codewords of weight 3 and sometimes this bound is exact (Theorems 3 and 4). The results of this paper were partially announced in [4].

As usual, we identify the vector $\underline{a} = (a_0, ..., a_{n-1}) \in F_2^n$ and the polynomial

$$a(x) = \sum_{\ell=0}^{n-1} a_\ell x^\ell \in F_2[x]/(x^n + 1) .$$

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

$$a(\gamma^i) = a(\gamma^j) = 0. \tag{1}$$

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

We begin with a simple example. Let m be even. Then 3 divides $2^m - 1$. Denote $(2^m - 1)/3$ by u. Then γ^u is a primitive element of F_4 and therefore its minimal polynomial is $1 + x + x^2$. If we choose $a(x) = 1 + x^u + x^{2u}$, we see that the equations (1) are valid for all i and j which are not divisible by 3. Thus we have proved the following result.

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

In the sequel we generalize this result in order to characterize other infinite classes of codes with minimum distance (at most) three.

2 General results

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

Lemma 1 *A code $C_{i,j}$ of length $n = 2^m - 1$ has the minimum distance $d_{i,j} = 2$ if and only if $gcd(n, i, j) > 1$.*

Proof: Since γ is a primitive nth root of unity, $d_{i,j} = 2$ if and only if there are k and ℓ, $0 \leq \ell < k < n$, such that

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

or equivalently,

$$(k - \ell)i \equiv (k - \ell)j \equiv 0 \ (mod\ n).$$

Because these congruences are valid if and only if $n/gcd(n, i, j)$ divides $k - \ell$, we see that these k and ℓ exist if and only if $gcd(n, i, j) > 1$. $\square$

Definition 1 *Denote by $K_\ell(r)$ the 2-cyclotomic coset of r modulo $2^\ell - 1$; i.e.,*

$$K_\ell(r) = \{\ r2^k\ (mod\ 2^\ell - 1) :\ k = 0, 1,\ \ldots,\ \ell - 1\ \}.$$

For any integer i, $0 \leq i \leq 2^m - 2$, we say that i belongs to $K_\ell(r)$ if there is an integer $j, j = 0, 1, \ldots, m - 1$, such that $i2^j \equiv r\ (mod\ 2^\ell - 1)$.

Theorem 1 *Assume that g is a factor of m and r is an integer $(0 < r < 2^g - 1)$ such that $gcd(r, 2^g - 1) = 1$. Let C_I be a binary cyclic code of length $2^m - 1$ generated by a polynomial of the form*

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

where I is a set of representatives of some 2-cyclotomic cosets modulo $2^m - 1$ and assume that all the elements of I are in the coset $K_g(r)$ modulo $2^g - 1$. Then the minimum distance of C_I is at most three.

Proof: If $u = (2^m - 1)/(2^g - 1)$ then $\beta := \gamma^u$ is a primitive element of F_{2^g}. Let b be such an integer in the interval $[1, 2^g - 2]$ that

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

Define

$$a(x) = 1 + x^{u(1/r)} + x^{u(b/r)} . \tag{2}$$

where the quotients $1/r$ and b/r are calculated modulo $2^g - 1$ and are in the interval $[1, 2^g - 2]$. If $i \in I$ then there are non-negative integers k and ℓ such that

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

Thus

$$\begin{aligned} a(\gamma^i) &= 1 + \gamma^{ui(1/r)} + \gamma^{ui(b/r)} \\ &= 1 + \beta^{i(1/r)} + \beta^{i(b/r)} \\ &= 1 + \beta^{2^k} + \beta^{b2^k} \\ &= (1 + \beta + \beta^b)^{2^k} = 0 . \end{aligned}$$

So we have proved that $a(x)$ of type (2) is in C_I and therefore the minimum distance of C_I is at most three. $\square$

Choosing $I = \{i, j\}$ and using Lemma 1 we obtain the following corollary of Theorem 1.

Theorem 2 *If g $(< m)$ is a factor of m, an integer r $(0 < r < 2^g - 1)$ is such that $gcd(r, 2^g - 1) = 1$ and the integers i and j $(0 < i, j < 2^m - 1)$ are in $K_g(r)$ then the minimum distance of the code $C_{i,j}$ of length $n = 2^m - 1$ is not more than 3: $d_{i,j} \leq 3$. If, further, $gcd(i, j, 2^m - 1) = 1$ then $d_{i,j} = 3$.*

Note that Proposition 1 is the special case $g = 2$ of the first statement of Theorem 2.

Let I_r be the set of all integers i in the range $[1, n-1]$ such that i is in the coset $K_g(r)$ (see Definition 1). As I_r is a union of cyclotomic cosets modulo n, let us denote by J_r a set of representatives of these cosets. Let C_{I_r} be the binary cyclic code of length n generated by

$$g_r(x) = \prod_{i \in J_r} m_i(x) .$$

Theorem 3 *Notation and hypotheses are the same as in Theorem 1. Let C be a code generated by a product of some $m_i(X)$, $i \in J_r$. Set $B = (2^m - 1)(2^g - 2)/6$. Then the number of codewords of weight three in C is at least B. For the code C_{I_r} this number is exactly B.*

Proof: Let $u = (2^m - 1)/(2^g - 1)$. Then the element $\beta = \gamma^u$ has the order $2^g - 1$ and therefore β is a primitive element of the field F_{2^g} of order 2^g, which is a subfield of F_{2^m}. As we know, in F_{2^g} there are $(2^g - 1)(2^g - 2)/6$ different triples of nonzero elements $\{\alpha_1, \alpha_2, \alpha_3\}$ such that

$$\alpha_1 \ + \ \alpha_2 \ + \ \alpha_3 \ = \ 0 \ .$$

Any such expression might be reduced to the following identity:

$$1 \ + \ \beta^b \ + \ \beta^h \ = \ 0 \ , \tag{3}$$

where b and h are some integers in the range $[1, 2^g - 2]$. Let

$$a(x) \ = \ 1 \ + \ x^b \ + \ x^h \tag{4}$$

be such a triple expressed as a trinomial from $F_2[x]/(x^{2^g - 1} - 1)$. Note that the element β is a root of $a(x)$. Therefore, we find $(2^g - 2)/2$ codewords of weight three which belong to any code C (see (3)). The locators of these codewords are :

$$\{ \ 1, \ \beta^b, \ \beta^h \ \} \ , \quad b \neq h \neq 0, \quad b \in [1, 2^g - 2] \ , \quad h \in [1, 2^g - 2] \ . \tag{5}$$

¿From any such codeword we obtain by shifting the codewords whose locators are

$$\{ \ \gamma^k, \quad \gamma^k \beta^b, \quad \gamma^k \beta^h \ \} \ , \quad k \in [0, 2^m - 2] \ .$$

Now we have a set of $(2^m - 1)(2^g - 2)/2$ codewords of weight three. But it is clear, by construction, that any such codeword is obtained exactly three times. So we have at least B distinct codewords of weight three in any code C.

Now consider the code C_{I_r} and any codeword of weight three of this code with locators $\{1, \ \gamma^a, \ \gamma^b\}$. Then we have by definition:

$$1 \ + \ \gamma^{a(\ell(2^g - 1) + r)} \ + \ \gamma^{b(\ell(2^g - 1) + r)} \ = \ 0 \ ,$$

for any $\ell \in [0, u - 1]$, $u = (2^m - 1)/(2^g - 1)$. So by adding the first equation $(\ell = 0)$ we obtain

$$\gamma^{ar}(\gamma^{a\ell(2^g - 1)} + 1) \ + \ \gamma^{br}(\gamma^{b\ell(2^g - 1)} + 1) \ = \ 0 \ ,$$

for any ℓ. Thus the polynomial

$$Q(x) = \gamma^{ar}(x^a + 1) \ + \ \gamma^{br}(x^b + 1)$$

has the roots $\lambda_\ell = (\gamma^\ell)^{2^g-1} = \beta^\ell$, $\ell \in [0, u-1]$. Since the λ_ℓ are the uth roots of unity, the polynomial $x^u + 1$ divides $Q(x)$. So the remainder $R(x)$ of $Q(x)$ modulo $x^u + 1$ must be the zero polynomial. We have

$$R(X) = \gamma^{ar}(x^{a'} + 1) \ + \ \gamma^{br}(x^{b'} + 1),$$

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

(i) $\gamma^{ar} = \gamma^{br}$ and $a' = b'$;

(ii) $x^{a'} = 1$ and $x^{b'} = 1$.

The condition **(i)** is impossible, because by the hypothesis $\gamma^{ar} + \gamma^{br}$ equals 1. So **(ii)** holds, proving that $a' = b' = 0$. Therefore u divides a and b. Hence any codeword of weight three of C_{I_r} has a set of locators of the form given by (5) (up to shift). There are exactly B codewords of weight three in C_{I_r}. $\square$

It seems difficult to determine the number of codewords of weight three for the arbitrary code $C_{i_1,\ldots,i_k}$. The more general result might be formulated now as the following statement.

Theorem 4 *Let* $P = \{p_1, \ldots, p_s\}$ *be the set of primes dividing* m. *Suppose we have* k *arbitrary integers* $i_1, \ldots, i_k$, $0 \le i_j \le 2^m - 2$, *such that there exist* h *primes* p_ℓ *from the set* P *and* h *integers* $r_\ell, 1 \le r_\ell \le 2^{p_\ell} - 2$, *such that*

$$i_1, i_2, \ldots, i_k \ \in K_{p_\ell}(r_\ell) \ ,$$

and $gcd(r_\ell, 2^{p_\ell} - 1) = 1$ *for all such numbers* r_ℓ *and primes* p_ℓ. *Then the cyclic code* $C_{i_1,\ldots,i_k}$ *generated by* $m_{i_1}(x) \ldots, m_{i_k}(x)$ *has the minimum distance three and for the number* B_3 *of codewords of weight three in* $C_{i_1,\ldots,i_k}$ *the following inequality is valid:*

$$B_3 \ \ge \sum_{\ell \in \{\ell_1, \ldots, \ell_h\}} (2^m - 1)\frac{2^{p_\ell} - 2}{6} \ .$$

Proof: Follows directly from Theorems 1 and 3. $\square$

3 The codes $C_{1,t}$

In this section we consider the cyclic codes $C_{1,t}$ of length $n = 2^m - 1$ with roots α and α^t for some integer t, which is not a power of 2. Note that if

n is prime then any code $C_{i,j}$ is equivalent to a code $C_{1,t}$. The code $C_{1,t}$ has a codeword of weight three if and only if there are two different nonzero elements α_1 and α_2 from F_{2^m} satisfying

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

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

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

$$U_t(x) \ = \ 1 \ + \ x^t \ + \ (1+x)^t$$

has at least one root in $F_{2^m} \setminus \{0,1\}$.

¿From Theorem 1 we know that if $t = (2^g-1)\ell + 2^k$ for some $k < g$ and where g divides m, then $C_{1,t}$ has the minimal distance 3. We want to give here more general results for the codes with minimum distance greater than 3. Moreover we want to give some examples, when the bound for B_3 of Theorem 4 is reached. We start with an example.

Example 1. For some t the minimum distance is at least 4 when m is odd. Take $t = 13$. Then the polynomial

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

has roots (which are not 0, or 1), if and only if m is even. According to Proposition 1 the minimum distance is three when m is even.

Example 2. The next case, $t = 21$, is more complicated. We have

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

It is easy to see that the minimum distance of $C_{1,21}$ is at least 4, unless 6 divides 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 F_2. It is because

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

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

Proposition 3 *Assume that m is a prime. Then if $t < m+3$, the code $C_{1,t}$ of length 2^m-1 has the minimum distance $d \geq 4$.*

Proof: The polynomial $U_t(x)$ has degree $t-1$. Moreover, the elements 0 and 1 are roots of $U_t(x)$. So $U_t(x) = (x^2+x)V_t(x)$ where the degree of $V_t(x)$ is $t-3$. If there is an element $\beta \in F_{2^m}$ such that $V_t(\beta) = 0$, then the minimal polynomial of β divides $V_t(x)$ and should have degree m, that contradicts the condition of the proposition. $\square$

Moreover we have the following property.

Proposition 4 *Let g be a divisor of m and let an integer t, where $2^g < t$, be such that the congruence*

$$t \equiv 2^k \ (mod\ 2^g - 1)$$

is valid for some integer k, $k < g$. Then the polynomial $x^{2^g} + x$ divides $U_t(x)$, i.e. all elements $\beta \in F_{2^g}$ are roots of $U_t(x)$.

Proof: Let $\beta \in F_{2^g}$, i. e. $\beta^{2^g-1} = 1$. Then we have

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

$\square$

By Proposition 4 we can find a class of codes $C_{1,t}$ for which either we can say that the minimum distance is equal to 3 or we can say that the minimum distance is at least 4, depending on m.

Theorem 5 *Suppose that $t = 2^u + 2^v - 1$, where $v < u$. If $gcd(m,u) = gcd(m,v) = 1$, then $C_{1,t}$ has the minimal distance at least four. Otherwise, $C_{1,t}$ has the minimal distance three.*

Proof: The condition

$$t \equiv 2^v \ (mod\ 2^u - 1)$$

and Proposition 4 imply that

$$(x^{2^u} + x) \mid U_t(x).$$

Let $u = \ell v + k$, where $k < v$. Then

$$t = 2^k(2^{v\ell} - 1) + 2^k + 2^v - 1 .$$

So $t \equiv 2^k \ (mod\ 2^v - 1)$ and $(x^{2^v} + x) \mid U_t(x)$. Set

$$L(x) = \frac{(x^{2^u} + x)(x^{2^v} + x)}{x(x+1)}.$$

Clearly the degree of $L(x)$ is $t-1$, which is exactly the degree of $U_t(x)$. If $gcd(u,v)=1$, we have then proved that $L(x)=U_t(x)$. Suppose that $gcd(u,v)>1$ and consider the derivative of $U_t(x)$:

$$U_t'(x) \ = \ x^{t-1} \ + \ (1+x)^{t-1}.$$

Let $\beta \in F_{2^u} \bigcap F_{2^v}$. Then

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

unless $\beta = 0$ or 1. Set

$$W(x) \ = \ \frac{gcd(x^{2^u}+x, \ x^{2^v}+x)}{x(x+1)} \ .$$

Then we have proved that $W(x)^2 \mid L(x)$. So in any case $L(x)=U_t(x)$. If $gcd(u,m)=gcd(v,m)=1$, then $U_t(x)$ has no roots in F_{2^m} and, therefore, the code $C_{1,t}$ has distance at least four. Otherwise $C_{1,t}$ contains codewords of weight 3. $\square$

Remark 1. Since we know exactly the roots of $U_t(x)$, we can determine the number of the codewords of minimum weight 3 for the code $C_{1,t}$. When $gcd(u,v)=1$, the polynomial $U_t(x)$ has 2^u+2^v-4 roots different from 0 and 1. Using the fact that $C_{1,t}$ is a cyclic code and that $U_t(x+1)=U_t(x)$ we obtain for the number B_3 of codewords of weight 3:

$$B_3 \ = \ \frac{(2^m-1)}{6}((2^u-2)+(2^v-2)),$$

which is exactly what we expected from Theorem 4. In this case the lower bound is reached.

4 The case p=3

In this section we treat the case $p=3$ – i.e. the codes are of length $n=2^m-1$, and 3 divides m. Let $C_{i,j}$ be a cyclic code with two zeros, γ^i and γ^j, where the integers i and j are not in the same cyclotomic coset modulo n.

Theorem 6 *Assume that* 3 *divides* m, $u=(2^m-1)/7$ *and* $\beta=\gamma^u$. *Let* r *be* 1 *or* 3 *and let* i *and* j *be integers such that* $0<i,j<2^m-2$, $gcd(i,n)=gcd(j,n)=1$, *and* $i,j\in K_3(r)$. *Then:*
(a) *the cyclic code* $C_{i,j}$ *has minimum distance three;*
(b) $C_{i,j}$ *has at least* 2^m-1 *codewords of weight three;*
(c) *these codewords are the trinomial* $t_h(x)=1+x^{u(h/r)}+x^{u(3/r)}$, *where* $h=1$ *or* 2, *and its shifts (and, where the division is in the ring* Z_7*).*

Proof: By hypothesis $gcd(i,j)$ is prime to n and we have :

$$i = 7i_1 + i_2 \quad \text{and} \quad j = 7j_1 + j_2 \ ,$$

where i_2 and j_2 are both in $K_3(r)$ and r is 1 or 3.

By Lemma 1 and Theorem 1, the code $C_{i,j}$ has minimum distance three. Since

$$x^7 + 1 = \left(x^3 + x + 1\right)\left(x^3 + x^2 + 1\right)(x+1) \ ,$$

the minimal polynomial of β over F_2 is $m_h(x) = 1 + x^h + x^3$, where h is either 1 or 2. Suppose it is $m_1(x)$, i.e. $1 + \beta + \beta^3 = 0$, and let

$$a(x) \ = \ 1 \ + \ x^{(1/r)} \ + \ x^{(3/r)},$$

where the division is in the ring Z_7. Then the polynomial $c(x) \ = \ a(x^u)$ is a codeword of the code C_{I_r}; therefore it is a codeword of $C_{i,j}$ (see proof of Theorem 1).

If $r = 1$ then $c(x) = 1 + x^u + x^{3u}$. We have, for any i such that $i_2 \in K_3(1)$,

$$c(\gamma^i) \ = \ 1 \ + \ \gamma^{iu} \ + \ \gamma^{3iu} \ = 1 \ + \ \beta^{i_2} \ + \ \beta^{3i_2} \ = (1 \ + \ \beta \ + \ \beta^3)^{i_2} = 0$$

and there are exactly $3u$ such γ^i. If $r = 3$, $c(x) = 1 \ + \ x^{u(1/3)} \ + \ x^u$. It is easy to check that $\beta^{1/3} = \beta^5$. So $c(x) = 1 + x^u + x^{5u}$. By shifting, we obtain

$$c'(x) = x^{2u} c(x) = 1 + x^{2u} + x^{3u} \ .$$

For any i such that $i_2 \in K_3(3)$,

$$c(\gamma^i) \ = \ 1 \ + \ \gamma^{2iu} \ + \ \gamma^{3iu} \ = 1 \ + \ \beta^{2i_2} \ + \ \beta^{3i_2} \ = (1 \ + \ \beta^3 \ + \ \beta^2)^{2^\ell + 1} = 0 \ ,$$

since $i_2 = 3.2^\ell$, by definition. There are exactly $3u$ such γ^i.

We have proved that the codeword $1 + x^u + x^{3u}$ and its shifts are codewords of C_{I_1}, while the codeword $1 + x^{2u} + x^{3u}$ and its shifts are codewords of C_{I_3}. So we have $2^m - 1$ codewords of weight three in C_{I_1} (respectively, in C_{I_3}) and this number is exactly the maximal number we can have (see Theorem 3). □

For the code $C_{3,5}$ we can say a little more. For the proof we use the method used in [2].

Proposition 5 *The code $C_{3,5}$ has minimum distance three if and only if 3 divides m. In this case its minimum weight codewords are exactly the elements of the code C_{I_3}, where 3 is a coset representative modulo 7. When 3 does not divide m, the code $C_{3,5}$ has minimum distance at least four.*

Proof: Note that $C_{3,5}$ cannot have minimum distance two because $gcd(3,5) = 1$. So we suppose that there is a codeword x of weight three in $C_{3,5}$ given by its locators $\{X_1,\ X_2,\ X_3\}$ and we use the method introduced in [2]. Define the locator polynomial of x

$$\sigma_{\mathrm{x}}(x) = \prod_{i=1}^{3}(1 - X_i x) = 1 + \sigma_1 x + \sigma_2 x^2 + \sigma_3 x^3 \ ,$$

and its power sum symmetric functions

$$A_k = X_1^k + X_2^k + X_3^k \quad , \quad k \in [0, n] \ .$$

We know that the σ_i and the A_i are linked by the Newton Identities. It means that they satisfy

$$\begin{aligned} A_1 + \sigma_1 &= 0 \\ A_3 + A_2\sigma_1 + A_1\sigma_2 + \sigma_3 &= 0 \\ A_5 + A_4\sigma_1 + A_3\sigma_2 + A_2\sigma_3 &= 0 \end{aligned} \tag{6}$$

By shifting we can take $A_1 = 1$ and by the definition of $C_{3,5}$, we have $A_3 = A_5 = 0$. So by replacing in (6) we obtain

$$\sigma_1 = A_1 = 1 \quad , \quad \sigma_2 = 0 \ \text{ and } \ \sigma_3 = 1$$

(note that $A_{2k} = A_k^2$). Then the locator polynomial is here unique, up to a shift, and it is $\sigma_{\mathrm{x}}(x) = 1 + x + x^3$. But this polynomial splits in the field of order 2^m if and only if 3 divides m. So if 3 does not divide m, the minimum distance is at least four. When 3 divides m by Theorem 6 the code $C_{3,5}$ has $d = 3$ and the number of codewords of weight three is exactly $2^m - 1$ and that is exactly the number of codewords of weight three in C_{I_3}, in the case $p = 3$. □

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 $n = 2^m - 1$ with the minimum distance $d \leq 3$. For any divisor g of m and for any coset representative r modulo $2^g - 1$, where r prime to $2^g - 1$, a list J_r of representatives of cosets modulo n is given. Any cyclic code C_I generated by the generating polynomial

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

n	m	g	B_3	r	J_r, Representatives of Cosets
15	4	2	5	1	1, 5, 7
63	6	2	21	1	1,5, 7, 11, 13, 23, 31
		3	63	1	1, 9, 11, 15, 23
				3	3, 5, 13, 27, 31
255	8	2	85	1	1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 43, 47, 53, 55, 59, 61, 85, 91, 95, 119, 127
		4	595	1	1, 17, 19, 23, 31, 47, 53, 61, 91
				7	7, 11, 13, 29, 37, 43, 59, 119, 127
511	9	3	511	1	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
				3	3, 5, 13, 17, 19, 27, 31, 41, 45, 47, 55, 59, 61, 73, 75, 83, 87, 103, 111, 117, 125, 255, 171, 187, 223
1023	10	2	341	1	1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 71, 73, 77, 79, 83, 85, 89, 91, 95, 101, 103, 107, 109, 115, 119, 121, 125, 127, 149, 151, 511, 341, 155, 157, 167, 173, 175, 179, 181, 187, 191, 343, 347, 367, 205, 215, 221, 223, 235, 239, 245, 247, 251, 253, 379, 383, 439, 479
		5	5115	1	1, 33, 35, 39, 47, 63, 95, 101, 109, 125, 219, 157, 159, 171, 187, 343, 221
				3	3, 17, 37, 43, 55, 79, 99, 105, 117, 127, 167, 179, 189, 375, 347, 223, 251
				5	5, 9, 41, 49, 51, 71, 103, 111, 165, 173, 175, 191, 351, 235, 237, 253, 439
				7	7, 19, 25, 45, 59, 69, 87, 107, 121, 149, 255, 183, 205, 231, 245, 379, 479
				11	11, 13, 21, 53, 57, 73, 75, 83, 115, 119, 181, 363, 367, 207, 239, 383, 447
				15	15, 23, 27, 29, 61, 77, 85, 89, 91, 123, 147, 151, 511, 213, 215, 247, 495

Table 1: Codes of length $n = 2^m - 1$ and minimum distance at most three.

where I is any nonempty subset of J_r, has the minimum distance at most three. It can have minimum distance two, when it satifies the hypothesis of Lemma 1. The number B_3 of the codewords of weight three might be evaluated according to Theorems 3 and 4.

Acknowledgements

The authors are indebted to Nicolas Sendrier for checking some numerical results with his own programs. The third author thanks Paul Camion for the possibility to work in INRIA (project CODES) as an invited professor in 1995.

References

[1] D. Audibert and N. Sendrier, *Distribution des poids des codes cycliques binaires de longueur* 63. INRIA-report Number 2299, July 1994.

[2] D. Augot, P. Charpin and N. Sendrier, *The minimum distance of some binary codes via the Newton's Identities*, EUROCODE'90, LNCS 514, pp. 65-73, Springer-Verlag, 1991.

[3] E.R. Berlekamp, *The weight enumerators for certain subcodes of the second order Reed-Muller codes*, Info. and Control, 17(1970) 485-500.

[4] P. Charpin, A. Tietäväinen and V. Zinoviev, *On Binary Cyclic Codes with Minimum Distance Three*, Proceedings, Fifth Intern. Workshop on Algebraic and Combinatorial Coding Theory, June 1-7, 1996, Sozopol, Bulgaria, pp. 93-97.

[5] T. Kasami, *The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes*, Info. and Control, 18(1971) 369-394.

[6] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Vol. 30, 1984.

[7] F.J. MacWilliams and N.J.A. Sloane, *The theory of Error Correcting Codes*, North-Holland, New York, 1986.

[8] J.H. van Lint and R.M. Wilson, *On the minimum distance of cyclic codes*, IEEE Transactions on Information Theory, vol. 32, pp. 23-40, January 1986.

[9] J.H. van Lint and R.M. Wilson, *Binary cyclic codes generated by* $m_1 m_7$, IEEE Transactions on Information Theory, vol. 32, p. 283, March 1986.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**