
Designs, Codes and Cryptography, 17, 81–85 (1999)

On the Minimum Distances of Non-Binary Cyclic Codes

PASCALE CHARPIN
INRIA, Codes Domaine de Voluceau-Rocquencourt BP 105 - 78153, Le Chesnay, France

AIMO TIETÄVÄINEN* tietavai@cs.utu.fi
Department of Mathematics and TUCS University of Turku FIN-20014 Turku, Finland

VICTOR ZINOVIEV
Institute for Problems of Information Transmission of the Russian Academy of Sciences Bol'shoi Karetnyi 19 GSP-4, Moscow 101447, Russia

Dedicated to the memory of E. F. Assmus

Received May 22, 1998; Revised May 22, 1998; Accepted June 29, 1998

Abstract. We deal with the minimum distances of q-ary cyclic codes of length $q^m - 1$ generated by products of two distinct minimal polynomials, give a necessary and sufficient condition for the case that the minimum distance is two, show that the minimum distance is at most three if $q > 3$, and consider also the case $q = 3$.

Keywords: cyclic code, minimum distance, non-binary

1. Introduction

Denote the finite field of order q by F_q. Let m be a positive integer, γ a primitive element of F_{q^m} and $m_s(x)$ the minimal polynomial of γ^s over F_q. We assume that $0 \le i < j \le q^m - 2$ and that i and j are not in the same q-cyclotomic coset modulo $n := q^m - 1$ and denote the q-ary 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 $d_{i,j}$. As usual, we identify the vector $\underline{c} = (c_0, \ldots, c_{n-1}) \in F_q^n$ and the polynomial

$$c(x) = \sum_{l=0}^{n-1} c_l x^l \in F_q[x]/(x^n - 1).$$

Thus $c(x)$ is an element of $C_{i,j}$ if and only if

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

In the binary case $q = 2$ there are many results concerning $d_{i,j}$ (see, e.g., [3], [2] and [1] and the references there). In this case $d_{i,j}$ may be any number in the set $\{2, 3, 4, 5\}$ (and even 7 when $m = 3$). It is known [1] that $d_{i,j} = 2$ if and only if $\gcd(i, j, 2^m - 1) > 1$. In [1] we also found sufficient conditions for the equality $d_{i,j} = 3$ and in the case $(i, j) = (1, t)$ where $t = 2^u \pm (2^v - 1)$ also for the inequality $d_{i,j} \ge 4$.

* The work was supported by the Academy of Finland under Grant 37358.

This paper is a natural continuation of [1]. Here we consider q-ary cyclic codes $C_{i,j}$. In the case $q > 2$ the necessary and sufficient condition for $d_{i,j} = 2$ (Theorem 1) looks a little more complicated than in the binary case. In the case $q > 3$ $d_{i,j}$ is either 2 or 3 (Theorem 3). The case $q = 3$ is exceptional. In this case $d_{i,j}$, if it is not 2, is in some cases 3 and in some other cases 4. We give examples for both these possible values but in this case we have not been able to give any necessary and sufficient condition for $d_{i,j} = 3$.

2. Results and Proofs

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

THEOREM 1 *$d_{i,j} = 2$ if and only if at least one of the following two conditions is satisfied:*

$$\left.\begin{array}{ll} \textit{(i)} & \gcd(i, j, q^m - 1) > 1 \\ \textit{(ii)} & \gcd(j - i, q - 1) > 1 \end{array}\right\} \tag{2}$$

Proof. If there is an element of $C_{i,j}$ of weight two then (since $C_{i,j}$ is cyclic) there is an element of $C_{i,j}$ of the form $c(x) = -\alpha + x^k$ where

$$\alpha = \gamma^{\frac{q^m-1}{q-1}a} \in F_q$$

and

$$0 \le a < q - 1,\ 0 < k < q^m - 1. \tag{3}$$

By (1), $c(x)$ is an element of $C_{i,j}$ if and only if

$$-\alpha + \gamma^{ik} = 0,\ -\alpha + \gamma^{jk} = 0.$$

Thus $d_{i,j} = 2$ if and only if the congruences

$$ik \equiv jk \equiv \frac{q^m - 1}{q - 1}a \pmod{q^m - 1} \tag{4}$$

have a solution (k, a) which satisfies the conditions (3). Hence we have to prove that for the solvability of the congruences (4) in the set defined by (3) it is necessary and sufficient that at least one of the conditions (2) is satisfied.

Sufficiency: (i) If $\gcd(i, j, q^m - 1) =: d > 1$ then $k = (q^m - 1)/d$, $a = 0$ is a solution of (4).

(ii) Let $\gcd(j - i, q - 1) =: \delta > 1$. Since $i \equiv j \pmod{\delta}$, the congruences $ik' \equiv a' \pmod{\delta}$ and $jk' \equiv a' \pmod{\delta}$ have a common solution (k', a') where $0 < k' < \delta$, $0 \le a' < \delta$. Then the congruences (4) have the solution

$$k = \frac{q^m - 1}{\delta} \cdot k',\quad a = \frac{q - 1}{\delta} \cdot a'.$$

Necessity: Assume that the congruences (4) have a solution (k, a) in the set defined by (3) and that $\gcd(i, j, q^m - 1) = 1$. We have to prove that $\gcd(j - i, q - 1) > 1$. Assume the contrary: $\gcd(j - i, q - 1) = 1$. The congruences (4) imply

$$\frac{j(q^m - 1)a}{q - 1} \equiv jik = ijk \equiv \frac{i(q^m - 1)a}{q - 1} \pmod{q^m - 1}$$

and so

$$\frac{(j - i)(q^m - 1)a}{q - 1} \equiv 0 \pmod{q^m - 1};$$

i.e., $(j - i)a \equiv 0 \pmod{q - 1}$. Since $\gcd(j - 1, q - 1) = 1$, we thus have $a = 0$. Therefore, by (4),

$$ik \equiv 0, \quad jk \equiv 0 \pmod{q^m - 1}.$$

This is impossible because, by the condition $\gcd(i, j, q^m - 1) = 1$, these congruences do not have any common solution k in the interval $0 < k < q^m - 1$. ■

The code $C_{1,t}$ has an element of weight three if and only if there are nonzero elements a and b of F_q and integers l and k such that $0 < l < k < q^m - 1$, $a + b\gamma^l - \gamma^k = 0$ and $a + b\gamma^{lt} - \gamma^{kt} = 0$. Thus we have the following result.

PROPOSITION 1 *$d_{1,t} \leq 3$ if and only if there are nonzero elements a and b of F_q such that the polynomial*

$$U_{q,t}(x; a, b) := a + bx^t - (a + bx)^t$$

has at least one zero x in $F_{q^m} \setminus \{0, 1\}$.

Consider now the case $q = 3$. Since the number of elements in a sphere of radius 2 in F_3^n is $2n^2 + 1$ and the number of elements in any ternary code $C_{i,j}$ is at least $3^{n-2m} = 3^n/(n+1)^2$, the spheres of radius 2 with centres at the elements of a ternary code $C_{i,j}$ cannot be disjoint. Therefore in the ternary case $d_{i,j} < 5$. Theorem 1 shows that sometimes $d_{i,j} = 2$. In the following we shall see that also the values 3 and 4 both occur.

PROPOSITION 2 *Assume that $q = 3$, $t = 3^s + 1$ and $v = \frac{3^m - 1}{\gcd(3^m - 1, 3^s - 1)}$. Then*

$$d_{1,t} = \begin{cases} 3 \text{ if } v \text{ is even} \\ 4 \text{ if } v \text{ is odd.} \end{cases}$$

In particular, $d_{1,t} = 4$ for all s if m is odd.

Proof. Since neither of the conditions (2) is satisfied, we have $d_{1,t} \geq 3$. Let us use Proposition 1 to find the conditions under which $d_{1,t} \leq 3$. We shall study the polynomials $U_{3,3^s+1}(x; a, b) =: U(x; a, b)$ for all nonzero elements a and b of F_3. There are four polynomials:

$$U_1(x) := U(x; 1, 1) = 1 + x^{3^s+1} - (1 + x)(1 + x^{3^s}) = -(x + x^{3^s});$$

$$U_2(x) := U(x; 2, 2) = 2 + 2x^{3^s+1} - 2^{3^s+1}(1 + x)(1 + x^{3^s})$$

$$\begin{aligned} &= 1 - x - x^{3^s} + x^{3^s+1} = (1-x)(1-x^{3^s}); \\ U_3(x) := U(x;1,2) &= 1 + 2x^{3^s+1} - (1+2x)(1+2x^{3^s}) \\ &= x + x^{3^s} + x^{3^s+1}; \\ U_4(x) := U(x;2,1) &= 2 + x^{3^s+1} - (2+x)(2+x^{3^s}) \\ &= 1 + x + x^{3^s}. \end{aligned}$$

The only zero of $U_2(x)$ in F_{3^m} is 1. Further, $U_3(x) = x^{3^s+1}U_4(x^{-1})$ and $U_4(x+1) = -U_1(x)$. So it is sufficient to examine the zeros of $U_1(x)$ which are of the form γ^k where γ is a primitive element of F_{3^m}. Thus $d_{1,t} = 3$ if and only if the equation $\gamma^{k(3^s-1)} = 2$ has a solution k. Further, we may write this equation as the congruence

$$k(3^s - 1) \equiv (3^m - 1)/2 \pmod{3^m - 1}.$$

Let $g = \gcd(3^m - 1, 3^s - 1)$ and $3^s - 1 = gu$. Then $3^m - 1 = gv$, and the congruence above gets the form

$$2ku \equiv v \pmod{2v}.$$

Since $\gcd(u, v) = 1$, this congruence is solvable if and only if v is even.

If m is odd then $3^m - 1$ is not divisible by 4. Hence v is odd and therefore $d_{1,t} = 4$. ■

Thus we have the following result.

THEOREM 2 *Let $q = 3$. If neither of the conditions (2) is satisfied then $d_{i,j}$ is either 3 or 4 and both these values occur.*

On the other hand, for $q > 3$ the minimum distance $d_{i,j}$ is always at most 3.

THEOREM 3 *Let $q > 3$. If neither of the conditions (2) is satisfied then $d_{i,j} = 3$.*

Proof. By the assumption $\gcd(i, j, q^m - 1) = \gcd(j - i, q - 1) = 1$. Let r and s be the elements of $\{1, 2, \ldots, q-1\}$ such that $i \equiv r \pmod{q-1}$ and $j \equiv s \pmod{q-1}$. Since $\gcd(j - i, q - 1) = 1$, we have $r \neq s$. Let us take $u = (q^m - 1)/(q - 1)$ and $\beta = \gamma^u$. Define

$$a(x) = (x - \beta^r)(x - \beta^s) = x^2 - (\beta^r + \beta^s)x + \beta^{r+s}$$

and let

$$c(x) = a(x^u).$$

Now we claim that $c(x)$ is an element of $C_{i,j}$. Indeed,

$$c(\gamma^i) = a(\gamma^{ui}) = a(\beta^i) = a(\beta^r) = 0,$$

and similarly we can see that $c(\gamma^j) = 0$. Since the weight of $c(x)$ is equal to the weight of $a(x)$ and so equal to 3, we have $d_{i,j} \leq 3$. On the other hand, by Theorem 1 we have $d_{i,j} \geq 3$. Thus $d_{i,j} = 3$. ■

Conclusion

Now we have a necessary and sufficient condition for the case that the minimum distance $d_{i,j}$ is two. We also know that $d_{i,j}$ is at most three if $q > 3$. In the ternary case $q = 3$ we still have an interesting open problem: Find a simple necessary and sufficient condition for $d_{i,j} = 4$.

References

1. P. Charpin, A. Tietäväinen and V. Zinoviev, On binary cyclic codes with minimum distance three, *Problems of Information Transmission*, Vol. 33 (1997) pp. 3–14.
2. H. Janwa, G. McGuire and R.M. Wilson, Double-error-correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$, *Journal of Algebra*, Vol. 178 (1995) pp. 665–676.
3. J. H. van Lint and R. M. Wilson, On the minimum distance of cyclic codes, *IEEE Transactions on Information Theory*, Vol. 32 (1986) pp. 23–40.
4. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York (1986).