A Case When Three Weights in a Cyclic Code is Impossible

Gary McGuire

Department of Mathematics
NUI Maynooth
Co. Kildare
Ireland

Abstract

We show that the dual code of the cyclic code C with two zeros α, α^t cannot have three weights in the case that m is even, $t \equiv 0 \pmod 3$, and $d(C) > 3$. The proof involves the partial calculation of a coset weight distribution.

1 Introduction

Let $n = 2^m - 1$ and let $F = \mathbb{F}_{2^m}$. Let α be a primitive root of F. Let C denote the cyclic code of length n with two zeros α and α^t, where $t \geq 3$ is odd. The minimum distance $d = d(C)$ of C satisfies $3 \leq d \leq 5$. We do not assume that t is relatively prime to n, but we do assume that $\dim C^\perp = 2m$.

These cyclic codes and their weight distributions arise in a surprising variety of different places. They are closely related to the crosscorrelation functions of m-sequences (maximal length linear feedback shift register sequences) related by a decimation t, see [1] for example. They arise in the study of the nonlinearity of power functions from F to F (see [1]), which are used in S-boxes in Feistel ciphers in cryptography. The weights give rise to exponential sums of the type that number theorists have studied, and results such as the Weil-Carlitz-Uchiyama bound have consequences for the weights. And in coding theory itself, they are in one sense the "simplest" cyclic codes for which the minimum distance is not completely known.

Of particular interest are the cases when $C^\perp$ has exactly three nonzero weights. There are many conjectures and results on the instances that $C^\perp$ is a three-weight code. These results are closely related to questions about three-valued crosscorrelation functions. The paper of Canteaut-Charpin-Dobbertin [1] has a study of the weight divisibility of these three-weight codes. These cases often correspond to power functions of maximal nonlinearity. It is therefore of great interest to classify the values of m and t for which $C^\perp$ is a three-weight code. Such a classification is probably difficult. We present a partial result in that direction here.

It is shown in [2] that when m is even and $t \not\equiv 0 \pmod 3$, the minimum distance of C must be equal to 3. In this case it is possible for $C^\perp$ to have three weights, as happens for example when $m = 6$ and $t = 5$ or 13. In this paper we consider the case when m is even and $t \equiv 0 \pmod 3$. We will prove that $C^\perp$ cannot have three weights when $d > 3$. We remark that there are many examples of C with m even, $t \equiv 0 \pmod 3$ and $d > 3$; one occurs when $m = 10$, $t = 9$. There are also many examples of C with m even, $t \equiv 0 \pmod 3$ and $d = 3$.

However, we do not know of an example with m even, $t \equiv 0 \pmod 3$, $d = 3$, and $C^\perp$ having three weights, so it is possible that our result can be extended to the case $d = 3$.

We index vectors of length n by F^* (the nonzero elements of F). The support of a vector is the subset of F^* where the vector has nonzero entries.

2 The Result

Suppose then that $C^\perp$ has the three weights $w_1 = 2^{m-1} - a$, $w_2 = 2^{m-1}$, and $w_3 = 2^{m-1} + b$ (the weights must have this form). Let A_i be the number of codewords of weight i in $C^\perp$, and let B_i be the number of codewords of weight i in C. Since C is a subcode of the Hamming code we have $B_1 = B_2 = 0$.

The MacWilliams identities give

$$A_{w_1} = \frac{2^{m-1}(2^m - 1)(2^{m-1} + b)}{a(a+b)} \tag{1}$$

$$A_{w_2} = \frac{(2^m - 1)(2^{m-1}(a-b) - 2^{2m-2} + ab + 2^m ab)}{ab} \tag{2}$$

$$A_{w_3} = \frac{2^{m-1}(2^m - 1)(2^{m-1} - a)}{b(a+b)} \tag{3}$$

$$B_3 = \left(\frac{2^m - 1}{3}\right)\left(a - b - 1 + \frac{ab}{2^{m-1}}\right). \tag{4}$$

Let $h_t(x) = x^t + (x+1)^t + 1$. Let $N(m,t)$ denote the number of distinct roots of $h_t(x)$ in F. The following result is not hard (see [4]).

Theorem 1 *[4]*

$$N(m,t) = \frac{6B_3}{2^m - 1} + 2.$$

Theorem 1 and equation 4 yield

Corollary 2

$$N(m,t) = 2(a-b) + \frac{ab}{2^{m-2}}.$$

Consider next the annihilator polynomial of $C^\perp$

$$F(x) = 2^{2m}\left(1 - \frac{x}{w_1}\right)\left(1 - \frac{x}{w_2}\right)\left(1 - \frac{x}{w_3}\right) \tag{5}$$

whose roots are the weights. We express $F(x)$ in its Krawtchouk expansion

$$F(x) = \alpha_0 P_0(x) + \alpha_1 P_1(x) + \alpha_2 P_2(x) + \alpha_3 P_3(x) \tag{6}$$

where $P_k(x) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{n-x}{k-j}$ is the k-th binary Krawtchouk polynomial.

Lemma 3 *If $B_3 = 0$ then*

$$\alpha_2 = \frac{1}{2^{m-1} - 1}\left(\frac{ab}{2^{m-2}} + 1\right) \quad \textit{and} \quad \alpha_3 = \frac{3}{2^{m-1} - 1}.$$

Proof: As shown in [4], equating coefficients gives

$$\alpha_3 = \frac{3 \cdot 2^{m-1}}{w_1 w_3} \tag{7}$$

and

$$\frac{\alpha_2}{\alpha_3} = \frac{2}{3}(w_1 + w_3 + 2^{m-1}) - n. \tag{8}$$

Substituting (7) into (8) and using equation (4) together with $B_3 = 0$ gives the result. □

The following result follows from Theorem 3.2 in Delsarte [3]:

Lemma 4 *Let $B_i(x)$ be the number of vectors of weight i in $C + x$, where $x \in \mathbb{F}_2^m$. Then $\sum_{i=0}^{3} \alpha_i B_i(x) = 1$ for all $x \in \mathbb{F}_2^m$.*

Let $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\} \subseteq F$.

Theorem 5 *If m is even and $t \equiv 0 \pmod 3$, then the number of weight 4 codewords in C whose support contains $\{1, \omega\}$ is $d - 3$, where $d = gcd(t, 2^m - 1)$.*

Proof: Since the parity check matrix for C is

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^t & \alpha^{2t} & \dots & \alpha^{(n-1)t} \end{pmatrix}, \tag{9}$$

the weight 4 codewords containing $\{1, \omega\}$ correspond to solutions $y \in F \setminus \{0, 1, \omega, \omega^2\}$ of

$$1 + \omega^t + y^t + (1 + \omega + y)^t = 0.$$

Since $3|t$ this becomes $y^t + (\omega^2 + y)^t = 0$, or

$$\left(1 + \frac{\omega^2}{y}\right)^t = 1. \tag{10}$$

Let $d = gcd(t, 2^m - 1)$. Let $r_1 = 1, r_2, \dots, r_d \in F$ be the roots of $x^d - 1$, i.e., the t-th roots of unity in F. Choosing $y = \omega^2/(1 + r_i)$ for $i = 2, 3, \dots, d$ gives $d - 1$ solutions to (10), and these are all the solutions to (10) in F.

However, the solutions $y = 1$ and $y = \omega$ do not correspond to weight 4 codewords. Thus there are $d - 3$ weight 4 codewords whose support contains $\{1, \omega\}$. □

Theorem 6 *If m is even and $t \equiv 0 \pmod 3$ and $d(C) > 3$, then it is not possible for $C^\perp$ to have three weights.*

Proof: Suppose $C^\perp$ has three weights and continue the notation as above. Let x be the vector of weight 2 with support $\{1, \omega\}$, and consider the coset $C + x$. For this coset we have $B_0(x) = 0$, and $B_1(x) = 0$ because $d > 3$. Also $B_2(x) = d - 2$ by Theorem 5.

Then Lemmas 3 and 4 give

$$\frac{1}{2^{m-1} - 1}\left(\frac{ab}{2^{m-2}} + 1\right)(d - 2) + \frac{3}{2^{m-1} - 1} B_3(x) = 1$$

or

$$\left(\frac{ab}{2^{m-2}}+1\right)(d-2)+3B_3(x)=2^{m-1}-1. \tag{11}$$

Note that $\frac{ab}{2^{m-2}}$ is an integer by equation (4). Since m is even and $3|t$, d is divisible by 3 and $2^{m-1}\equiv 2 \pmod 3$. Taking equation (11) modulo 3 gives

$$\frac{ab}{2^{m-2}}+1\equiv 1 \pmod 3$$

from which we conclude $ab\equiv 0 \pmod 3$.

Returning to equation (2) we find

$$\frac{A_{w_2}}{2^m-1}=\frac{2^{m-1}(a-b)-2^{2m-2}}{ab}+1+2^m,$$

and since 2^m-1 divides A_{w_2} we obtain

$$\frac{2^{m-1}[a-b-2^{m-1}]}{ab}\in\mathbb{Z}.$$

Since 3 divides ab we must have $a-b-2^{m-1}\equiv 0 \pmod 3$ which implies $a-b\equiv 2 \pmod 3$. Now Corollary 2 implies $N(m,t)\equiv 1 \pmod 3$.

On the other hand, 2^m-1 divides B_3 because $3|t$ (see [4]), so Theorem 1 implies $N(m,t)\equiv 2 \pmod 3$. This contradiction completes the proof. □

References

[1] A. Canteaut, P. Charpin, H. Dobbertin, Weight divisibility of cyclic codes, highly nonlinear functions on F_{2^m}, and crosscorrelation of maximum-length sequences, *SIAM J. Disc. Math.*, 13 (2000) 105–138.

[2] P. Charpin, A. Tietäväinen, and V. Zinoviev. On binary cyclic codes with minimum distance $d=3$. *Problems Inform. Transmission*, 33(4):287–296, 1997.

[3] P. Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Information and Control*, **23** (1973) 407–438.

[4] G. McGuire, On certain 3-weight cyclic codes having symmetric weights and a conjecture of Helleseth, *Proceedings of SETA'01.*