ON THE ESTIMATION OF MINIMUM DISTANCE OF DUALS OF BCH CODES[1]

Alberto Cáceres
University of Puerto Rico at Humacao, Humacao PR, 00661

Oscar Moreno
University of Puerto Rico at Rio Piedras, Rio Piedras PR, 00931

CONGRESUS NUMERANTIUM
VOLUME 81, December 1991

ABSTRACT. *MacWilliams-Sloane Research Problem (9.5) in* The Theory of Error Correcting Codes, *viewed under the light of new results about exponential sums and weights of codes, is a call to strengthen the Carlitz-Uchiyama Bound. In this paper we give account of a new bound which falls between the MacWilliams-Sloane proposal and the Carlitz-Uchiyama one. We show an example that meets this bound proving it is tight, and as a consequence proves that MacWilliams-Sloane is not true.*

1. INTRODUCTION

The minimum distance of duals of BCH codes is estimated by the use of the Carlitz-Uchiyama bound for exponential sums. In Research problem (9.5), MacWilliams and Sloane [MS], propose the strenghtening of this estimation from

$$2^{m-1} - (t-1)2^{m/2} \leq w \leq 2^{m-1} + (t-1)2^{m/2}$$

to

$$2^{m-1} - (t-1)2^{[m/2]} \leq w \leq 2^{m-1} + (t-1)2^{[m/2]}$$

where $(2t-1)$ is the designed distance of the original BCH code and w is the weight of codewords of its dual. By use of an example we prove that in general this is not possible. This was also found independently by F. Rodier [R], who furthermore obtained an infinite sequence of duals of binary BCH codes that also proves false the proposed strenghtening. On improving the Carlitz-Uchiyama bound, O. Moreno, S. Litsyn and C. Moreno [MLM] have established a new bound for duals of cyclic codes which our example and Rodier's meet. We prove that this new bound is tight and hence determine the actual minimum distance of duals of binary BCH codes.

2. CHARACTERIZATION OF DUALS AND THE NEW BOUND

In order to prove our claim we need to invoke a Delsarte type of result characterizing duals of cyclic codes in terms of traces of polynomials. Computing the weights of codewords will be done by means of exponetial sums. C. Moreno and V. Kumar [MK] have proven the Propositions 1 and 2 and its Corollary.

[1]This work was partially supported by Component IV of EPSCoR of Puerto Rico

Let $F = GF(2^m)$ be the Galois field of 2^m elements and $N = 2^m - 1$ the block length of cyclic codes, α a primitive element of F and T the trace function from F down to $F = GF(2)$, then

Proposition 1. The dual code of the cyclic code C with zeroes $\alpha^{i_1}, \ldots, \alpha^{i_s}$ is given by $C^{\perp} = T(C^{\#})$, where

$$T(C^{\#}) = \{(T(f(\alpha^{i_1}), (T(f(\alpha^{i_2}), \ldots, (T(f(\alpha^N))f \in P(C)\}$$

in which $P(C)$ consists of every polynomial f in $F[x]$ such that the monomial terms in f have degrees lying in $\{i_1, i_2, \ldots, i_s\}$. ∎

Proposition 2. The weights of $C^{\perp}$ are given by $W(C^{\perp}) = \left\{ \frac{2^m - \sum_{x \in F} (-1)^{Tr(f(x))}}{2} : f \in P(C) \right\}$ ∎

Corollary. $\left| \sum_{x \in F} (-1)^{Tr(f(x))} \right| \leq W \quad \forall f \in P(C)$ if and only if $d_{min} \geq \frac{2^m - W}{2}$ ∎

This equivalence shows that the MacWilliams-Sloane proposal on weights of codewords of duals of BCH codes is a call to strenghten the Carlitz-Uchiyama bound. Recently O. Moreno, S. Litsyn and C. Moreno [MLM] have found an improvement of this bound for the binary case according to the following proposition.

Proposition 3. Let $f \in F[X]$ be a polynomial whose terms have degrees lying in $i_1, i_2, \ldots, i_s$, let $j = max w(i_k) : k = 1, \ldots, s$, where $w(i)$ is the number of ones in the binary expression of i, $\lambda = [\frac{m}{j}]$, the ceiling of $\frac{m}{j}$, then

$$\left| \sum_{x \in F} (-1)^{Tr(f(x))} \right| \leq \frac{degf - 1}{2} 2^{\lambda - 1} \cdot [2 \cdot 2^{m/2 - \lambda - 1}].$$

If $degt = 7$, $\lambda - 1$ can be substituted by λ ∎

3. APPLICATION TO BCH CODES

Proposition 3 provides a new bound for duals of cyclic codes. As a direct application consder the $(t = 4)$-error correcting BCH code over $GF(2^9)$. Its zeroes are $\alpha^1, \alpha^3, \alpha^5, \alpha^7$,
$j = max\{w(1), w(2), w(5), w(7)\} = 3$, $[\lambda = \frac{9}{3}] = 3$. By Proposition 2, correpsonding polynomials will have monomial terms in $\{1, 3, 5, 7\}$ and will satisfy

$$\left| \sum_{x \in F} (-1)^{Tr(f(x))} \right| \leq \frac{7 - 1}{2} 2^3 \cdot [2 \cdot 2^{9/2 - 3}] = 120$$

estimating the minimum disstance greater than or equal to 196. MacWilliams-Sloane proposal will give 208. This new bound is actually met by polynomial $f(X) = X^7$ as we prove in the following

Theorem. Let $F = GF(2^9)$. For $f(X) = X^7$, $\left| \sum_{x \in F} (-1)^{Tr(f(x))} \right| = 120$

Proof: Since the basis is equal to -1 we can use the convenient identity

$$\left|\sum_{x\in F}(-1)^{Tr(f(x))}\right| = |F| - 2\sum_{x\in F}(-1)^{Tr(X^7)}.$$

Being $|F| = 512$ we prove that the last sum $\sum_{x\in F}(-1)^{Tr(X^7)} = 196$

If $\alpha \in F$ is a primitive element, $(\alpha^i)^7 = (\alpha^j)^7$ implies $7i \equiv 7j \pmod{511}$, i.e., $7(i-j) = 511k = 7 \times 73k$, hence $i \equiv j \pmod{73}$ which means that after $x = 0$, the first 73 powers of α will repeat seven times. That reduces the sum to

$$\sum_{x\in F} Tr(x^7) = Tr(0) + 7\sum_{i=1}^{73} Tr(\alpha^{7i})$$

Every element α^{7i} is the a 73-root of unity and satisfies the polynomial $X^{73}-1$ which factors as follows:

$$\begin{aligned} X^{73}-1 \;=\; & (1+X)(1+X^8+X^9)(1+X^3+X^6+X^8+X^9)(1+X^5+X^7+X^8+X^9) \\ & (1+X+X^9)(1+X+X^2+X^4+X^9)(1+X^3+X^1+X^6+X^9) \\ & (1+X^2+X^5+X^6+X^9)(1+X^3+X^4+X^7+X^9) \end{aligned}$$

The 73-th root of unity which are also roots of the first four irreducible factors are $1+9+9+9 = 28$ in number. Those are the only irreducible factors with a significative term of degree one less than the factors degree, i.e., non null trace term. Hence they are the only 73-th roots of unity with trace equal to 1. Any other 73-th root of unity must then have trace equal to zero. Since $Tr(0) = 0$ our sum becomes:

$$\sum_{x\in F} Tr(x^7) = 0 + 7 \times 28 = 196$$ ∎

The rest of Rodier's codes also meet the bound of 120.

REFERENCES

[MS] Mac Williams F. J. and Sloane N.J.A., *The Theory of Error Correcting Codes*, North Holland Pub. Co. Third Printing, 1981.

[R] Rodier, Francois, *On the Spectra of the Duals of Binary BCH codes of Designed Distance* $\delta = 9$, Preprint

[MK] Moreno O. and Kumar V. , *Minimum Distance Bounds for Cyclic Codes and Deligne's Theorem,* Submitted to IEEE Transactions od Information Theory.

[MLM] Moreno O., Litsyn S. and Moreno C. *Divisibility Properties of Exponential Sums in One and Several Variables.* 1990 Preprint.