On the duals of binary BCH codes

José Felipe Voloch

Abstract: We give bounds for the minimal distance of duals of binary BCH codes in a range where the Carlitz-Uchiyama bound is trivial. This is done by estimating the number of points on certain curves over finite fields.

Keywords: BCH codes, Carlitz-Uchiyama bound, minimal distance

Introduction

The minimal distance of the dual of a binary BCH code of designed distance δ can be estimated by the Carlitz-Uchiyama bound ([MS], Ch. 9, thm 18) when δ is not too large. The question of whether the Carlitz-Uchiyama bound can be improved was raised in [MS] and studied in a number of papers such as [W], where it is shown that the bound is sometimes sharp and in [AL], where several improvements are obtained. The Carlitz-Uchiyama bound is a consequence of Weil's Riemann Hypothesis for curves over finite fields. This note will give some other improvements on the Carlitz-Uchiyama bound using the method of [SV], which gives a method for improving on Weil's bound in some cases. Unfortunately, the bound we seek is not a direct consequence of the results of [SV] and a more careful analysis of the relevant curves is needed. (See the remark below). We will discuss the dimensions of the codes for which our bounds improve previous results and present some numerical examples.

The results

Let m be a positive integer, $q = 2^m, n = q - 1$ and $\delta < n$ another positive integer. Let α be a fixed primitive n-th root of unity in $\mathbf{F}_q$. The (narrow-sense, primitive) BCH code of designed distance δ is the cyclic code of length n generated by the least common multiple of the minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ over $\mathbf{F}_2$. Its dual is thus also a cyclic code of length n which we denote by C_δ. If δ is even, the code thus obtained is the

same as the one obtained by replacing δ by $\delta+1$, so we can and will restrict to the case $\delta = 2t+1$ is odd. With these assumptions, the weight w of any non-zero codeword of C_δ satisfies the Carlitz-Uchiyama bound $|w - 2^{m-1}| \leq (t-1)2^{m/2}$. This bound is non-trivial only for $t - 1 < 2^{m/2-1}$ and is in fact sharp for some values of t in this range ([W]). We will provide a non-trivial bound on the weight for an extended range of values of t.

Theorem. *The minimal weight w of of the dual of a binary BCH code of length $2^m - 1$ and designed distance $\delta = 2t+1$, with $2^{m/2-1} < t < 2^{\lceil m/2 \rceil}$, satisfies $w \geq \lfloor q/(t+1+\epsilon) \rfloor - 1$, where $\epsilon = 0$ for t odd and $\epsilon = 1$ for t even.*

Proof: As is well-known (see e.g. [S, VIII.2.12]), given a codeword of C_δ, there exists $f(x) \in \mathbf{F}_q[x]$ of odd degree $d \leq 2t-1$ such that the coordinates of the codeword are given by $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(\alpha^i)), i = 1, \ldots, n$ and therefore, the weight of the codeword is $q - 1 - N$, where N is the number of solutions $x \in \mathbf{F}_q^*$ of $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(x)) = 0$, which by the additive form of Hilbert's theorem 90, is half the number of affine points over $\mathbf{F}_q$ with $x \neq 0$ on the curve X given by $y^2 - y = f(x)$.

Following [SV], we consider the function W on X which is the determinant of the matrix whose first row is $1, x^q, x^{2q}, \ldots, x^{rq}, y^q$ and the other rows are the first $r+1$ Hasse derivatives of $1, x, x^2, \ldots, x^r, y$, where r is either $(d+1)/2$ or $(d+3)/2$ and is chosen to be odd. By [SV] corollary 2.6, W vanishes on the affine $\mathbf{F}_q$-rational points of X with multiplicity at least $r+1$. We now study the behaviour of W at infinity.

Now, it is straightforward to show that $W = \sum_{j=0}^{m-1} f^{2^j} + \sum_{i=1}^{r} D^{(i)}(y)(x^q - x)^i$, where $D^{(i)}$ is the i-th Hasse derivative. Now, in a completion of $\mathbf{F}_q(x)$ at a place where f has a zero, we have $y = \sum_{j=0}^{\infty} f^{2^j}$, so $D^{(i)}(y) = \sum_{2^j | i} (D^{(i/2^j)}(f))^{2^j}$ and this latter expression gives $D^{(i)}(y)$ as a polynomial in x, which is therefore valid globally. It also follows that W itself is a polynomial. By the above expression we get that $\deg D^{(i)}(y)$ is at most $2^{\nu(i)}d - i$, where $\nu(i)$ is the largest exponent such that $2^{\nu(i)}$ divides i. It follows that $\deg D^{(i)}(y)(x^q - x)^i \leq iq + 2^{\nu(i)}d - i$. By our choice, r is odd and an elementary argument shows that the maximum over $i = 1, \ldots, r$ of the last expression is $rq + d - r$, achieved when

$i = r$ because of our restriction on the range of t. Also the degree of $\sum_{j=0}^{m-1} f^{2^j}$ is at most $dq/2$, which is smaller than $rq+d-r$ under our assumptions. Therefore $\deg W \leq rq+d-r$.

If W is identically zero then, for $x \in \mathbf{F}_q$, $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(f(x)) = \sum_{j=0}^{m-1} f(x)^{2^j} = W(x) = 0$, so the codeword corresponding to f is the zero codeword, which is irrelevant for the calculation of the minimal weight. We can thus assume that W is not identically zero. It follows that $N \leq (\deg W)/(r+1)$. Recalling our choice of r, the theorem follows from a simple calculation.

Remarks:

(i) One can use the results of [SV] directly to get an upper bound for $\deg W$ which, in the notation there, is $(\deg S - v_P(S))/2$, for P the point at infinity on X. But this bound will be far worse than the one obtained above. On the other hand, the issue of showing that W is not identically zero, which is usually crucial in applying the results of [SV], does not pose a problem here.

(ii) We still get a bound without the restrictions on t, but the bound is trivial for $t \geq 2^{\lceil m/2 \rceil}$ and is worse than than the Carlitz-Uchiyama bound for $t < \sqrt{q}/2$. Note that the Carlitz-Uchiyama bound is trivial for $t \geq \sqrt{q}/2$ while ours is not. In the range given in the statement of the Theorem, our bound compares with those obtained in [AL] and gives an improvement on their bound for roughly the top two-thirds of the interval. The numerical results obtained in [AL] seem to indicate that our bounds as well as their bounds might be far from being best possible.

The dimension of the codes for which the theorem applies can be readily computed by the same method of [MS] Ch. 9 Corollary 8, which shows that the dimension of C_δ is mt if $2t-1 < 2^{\lceil m/2 \rceil}+1$. In the range $2^{\lceil m/2 \rceil}+1 \leq 2t-1 < 2^{\lceil m/2 \rceil+1}$, we have that,for m even, $\dim C_\delta = m(t-1/2)$ and, for $m = 2k+1$ odd, $\dim C_\delta = mt, m(t-1)$ or $m(t-2)$ according to whether $2t-1 < 2^{k+1}+1, 2^{k+1}+1 \leq 2t-1 < 2^{k+1}+2^k+1$ or $2t-1 \geq 2^{k+1}+2^k+1$.

As for some numerical examples, if we take $q = 32, t = 6$, we get minimal weight at least three, which attained, since the code has generator polynomial x^5+x^3+1. Another example is $q = 16, t = 3$, in this case the Weil bound is attained by $y^2+y = x^5$ but this

corresponds to the zero codeword, so that is irrelevant. The bound is again three, which is again attained. It has been noted in the literature that, when $q = 2^m$ with m even and $t = 2^{m/2-1} + 1$, the Carlitz-Uchiyama bound is attained. Indeed, as in the case $q = 16$, the curve $y^2 + y = x^{q/2-1}$ attains the Weil bound, but again it leads to the zero codeword, so that is irrelevant. Our bound provides a non-trivial estimate of the least non-zero weight.

Acknowledgements: The author would like to thank the NSA for financial support.

References.

[AL] D. Augot and F. Levy-dit-Vehel, Bounds on the minimum distance of the duals of BCH codes, IEEE Trans. Inform. Theory 42 (1996), 1257–1260.

[MS] J. MacWilliams and N. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

[S] H. Stichtenoth, *Algebraic function fields and codes.* Berlin: Springer, 1993.

[SV] K-O. Stöhr and J.F. Voloch, Weierstrass Points and Curves over Finite Fields, Proc. London Math. Soc.(3) **52** (1986) 1–19.

[W] J. Wolfmann, The number of points of certain algebraic curves over finite fields, Comm. Algebra **17** (1989) 2055–2060.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: voloch@math.utexas.edu