WEIGHT ESTIMATES FOR CYCLIC CODES VIA WEIL-SERRE BOUND FOR ADDITIVE EQUATIONS

Cem Güneri
Faculty of Engineering and Natural Sciences
Sabancı University
Tuzla, 34956, İstanbul, Turkey
e-mail: guneri@sabanciuniv.edu

Ferruh Özbudak
Department of Mathematics
Middle East Technical University
İnönü Bulvarı, 06531, Ankara, Turkey
e-mail: ozbudak@metu.edu.tr

Abstract. Wolfmann gave a general weight estimate for a large class of cyclic codes using the Weil-Serre bound. His estimate can be applied to any cyclic code over a prime finite field $\mathbb{F}_p$ but there are codes over extension fields to which Wolfmann's bound does not apply. We extend Wolfmann's result to all cyclic codes over any finite field. Interestingly, the problem of estimating weights of cyclic codes reduces to computation of degrees of left greatest common divisors in the ring of additive polynomials with coefficients from a finite field.

Keywords: Cyclic code, trace representation, additive polynomial, left greatest common divisor, Weil-Serre bound.

1. Introduction to Wolfmann's Result

Weights in cyclic codes can be determined by the number of solutions of certain equations over finite fields. Let $\mathbb{F}_q$ be the finite field with $q = p^e$ elements ($e \geq 1$) and $\mathbb{F}_{q^m}$ be its extension of degree $m \geq 2$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and C be a q-ary cyclic code of length $n = q^m - 1$ such that $\{t_1, t_2, \ldots, t_s\} \subseteq \{1, \ldots, n-1\}$ is a *basic zero set* for the dual cyclic code $C^\perp$. In other words, the generator polynomial of $C^\perp$ is $\prod_{j=1}^{s} f_j(x)$, where $f_j(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of α^{t_j} for $j = 1, \ldots, s$. If Tr denotes the trace map from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, then one has the following representation for C ([6, Proposition 2.1]):

$$C = \left\{ \left(\mathrm{Tr}(f(\alpha^0)), \ldots, \mathrm{Tr}(f(\alpha^{n-1})) \right) : f(x) = \sum_{j=1}^{s} \lambda_j x^{t_j} \in \mathbb{F}_{q^m}[x] \right\} \tag{1.1}$$

Then by Hilbert's Theorem 90 ([3, Theorem 2.25]), we have that the weight of the codeword $c_{\boldsymbol{\lambda}} \in C$, determined by $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_s) \in \mathbb{F}_{q^m}^s$ as above, is

$$w(c_{\boldsymbol{\lambda}}) = q^m - \frac{N_{\boldsymbol{\lambda}}}{q}, \tag{1.2}$$

where $N_{\boldsymbol{\lambda}}$ is the number of solutions of the following equation in $\mathbb{F}_{q^m} \times \mathbb{F}_{q^m}$:

$$y^q - y = \lambda_1 x^{t_1} + \cdots + \lambda_s x^{t_s} \tag{1.3}$$

If we assume that each exponent t_j in (1.3) is relatively prime to p, then the equation defines an irreducible Artin-Schreier type curve for any choice of coefficients $\lambda_1, \ldots, \lambda_s$, as long as not all

$\lambda_j = 0$. Genus of such a curve is given by

$$g = \frac{(q-1)(t-1)}{2},$$

where $t := \max\{t_j : \lambda_j \neq 0\}$ (see [5, Proposition III.7.10] for these facts). One can estimate the number of $\mathbb{F}_{q^m}$-rational points of such a curve by the Weil-Serre estimate ([5, Theorem V.3.1]).

Using these observations, Wolfmann wrote a general algebraic geometric bound on the weights of a q-ary cyclic code of length $q^m - 1$ under the assumption that the dual code's basic zeros $\{t_1, t_2, \ldots, t_s\}$ are all relatively prime to the characteristic p (see [6]). Note that an element t_j in a basic zero set for a cylic code can be replaced by any other element in its q-cyclotomic coset $\{t_j, qt_j, q^2t_j, \ldots\}$ mod $(q^m - 1)$. When $q = p$ is a prime, the smallest member of the cyclotomic coset is necessarily relatively prime to p. Hence, Wolfmann's bound applies to any cyclic code of length $p^m - 1$ over a prime finite field $\mathbb{F}_p$.

2. Dealing with Reducible Additive Equations and an Extension of Wolfmann's Bound to All Cyclic Codes

The following examples show that equations of the form (1.3), which are related to cyclic codes, need not define irreducible curves when q is not prime.

Example 2.1. Let $q = 4$ and $n = 4^3 - 1 = 63$. Consider the 4-ary cyclic code C of length n whose dual's basic zero set is $\{1, 2\}$. In other words, if α is a primite element of $\mathbb{F}_{64}$, then the generator polynomial of the dual code $C^\perp$ is $f_1(x)f_2(x)$, where $f_i(x)$ denotes the minimal polynomial of α^i over $\mathbb{F}_4$.

Observe that the 4-cyclotomic coset mod 63 containing 2 is $\{2, 8, 32\}$ and none of the elements in the coset is relatively prime to the characteristic 2.

Here is the related family of curves we have to study to estimate weights of codewords in C:

$$\mathcal{F} = \left\{y^4 - y = \lambda_1 x + \lambda_2 x^2 : \ \lambda_1, \lambda_2 \in \mathbb{F}_{64}\right\}$$

If only one of the coefficients λ_1 or λ_2 is nonzero, the resulting curve is rational with 64 (affine) rational points over $\mathbb{F}_{64}$. However, for the equation $y^4 - y = x + x^2$, we have

$$\begin{aligned} y^4 + y + x^2 + x &= y^4 + y^2 + x^2 + y^2 + y + x \\ &= \left(y^2 + y + x\right)^2 + \left(y^2 + y + x\right) \\ &= \left(y^2 + y + x\right)\left(y^2 + y + x + 1\right) \end{aligned}$$

Hence the curve defined by $y^4 + y = x^2 + x$ has 2 irreducible components both of which are rational curves. Therefore, there are 128 (affine) rational points over $\mathbb{F}_{64}$.

Example 2.2. Let us present another explicit decomposition of a reducible curve of the form (1.3) when $q = 16$:

$$\begin{aligned} y^{16}+y+x^8+x^2 &= (y^8+y^4+y^2+y+x^4+x^2)^2 \\ &\quad +(y^8+y^4+y^2+y+x^4+x^2) \\ &= (y^8+y^4+y^2+y+x^4+x^2) \\ &\quad (y^8+y^4+y^2+y+x^4+x^2+\underbrace{1}_{\nu^2+\nu}) \\ &= (y^4+y+x^2)(y^4+y+x^2+1) \\ &\quad (y^4+y+x^2+\nu)(y^4+y+x^2+\nu+1) \end{aligned}$$

Here, ν is defined in such a way that $\mathbb{F}_4=\mathbb{F}_2(\nu)$ with $\nu^2+\nu+1=0$. Each of the four factors in the last step above defines a rational curve over the field of definition, which is some extension of $\mathbb{F}_{16}$.

Motivated by such examples, we studied factorizations of "reducible equations" of the form (1.3) in [1, 2]. Naturally, explicit factorization as in the above examples is rather complicated and can only be done in specific situations. In particular, we could write weight bounds for all cyclic codes over prime fields $\mathbb{F}_p$ and their square extensions $\mathbb{F}_{p^2}$ by carrying out explicit factorizations of related reducible equations (cf. [1, Theorem 3.2, Theorem 3.3]). Our code bound was an extension of Wolfmann's bound. A more effective result that applies to all cyclic codes over all finite fields required a less computational and non-explicit approach. In order to describe this result, let us introduce some terminology.

A polynomial of the form

$$A(T)=a_nT^{p^n}+a_{n-1}T^{p^{n-1}}+\cdots+a_1T^p+a_0T$$

with coefficients in a field K of characteristic p is called an *additive polynomial*. We further assume that K is a perfect field. Our main objects of study are equations of the form

$$A(T)=z \tag{2.1}$$

for $z\in K(x)$. We will refer to (2.1) as an *additive equation*. Note that (1.3) is an example of an additive equation. By abuse of language we will call (2.1) an *irreducible additive equation* if the polynomial $A(T)-z$ is irreducible over $K(x)$. Otherwise, (2.1) will be called a *reducible additive equation*.

Let $A(T)$ and $B(T)$ be two additive polynomials in $K[T]$ defined by

$$\begin{aligned} A(T) &= a_nT^{p^n}+a_{n-1}T^{p^{n-1}}+\cdots+a_1T^p+a_0T, \\ B(T) &= b_mT^{p^m}+b_{m-1}T^{p^{m-1}}+\cdots+b_1T^p+b_0T, \end{aligned}$$

where $a_nb_m\neq 0$. Note that the ordinary product of A and B is not an additive polynomial but their composition

$$A(T)\circ B(T):=A(B(T)) \tag{2.2}$$

produces an additive polynomial. Under summation and composition, the set of additive polynomials forms a subring of $K[T]$. We will denote this ring by $\mathcal{R}$ throughout.

We say that A is *left divisible* by B if there exists another additive polynomial $C(T) \in \mathcal{R}$ such that $A = B \circ C$. If A is not left divisible by B then, assuming that $\deg A \geq \deg B$, one can carry out a left division of A by B as

$$A(T) = B(T) \circ \left(\left(\frac{a_n}{b_m} \right)^{1/p^m} T^{p^{n-m}} + \cdots \right) + R(T),$$

where $R(T) \in \mathcal{R}$ is of degree less than $\deg B$, unless $R = 0$. Hence, over a perfect field K, the ring $\mathcal{R}$ has a left Euclidean algorithm and any two additive polynomials $A, B \in \mathcal{R}$ have a monic *left greatest common divisor* $\mathrm{lgcd}(A, B)$ in $\mathcal{R}$.

Assume that A is monic, separable and splits completely in K with the zero set W. Hence, $W \subseteq K$ and $|W| = p^n$. It is well-known that the set W is an $\mathbb{F}_p$-linear subspace of K. There is another $\mathbb{F}_p$-subspace of K associated with A. Namely, let $\overline{W}$ be the set of elements $u \in K$ such that

$$A(T) = \left(T^p - \frac{1}{u^{p-1}} T \right) \circ Q(T) \tag{2.3}$$

for some $Q(T) \in \mathcal{R}$. The space $\overline{W}$ is called the *adjoint space* of A. Its dimension is equal to that of W (i.e. $\dim_{\mathbb{F}_p}(\overline{W}) = n$). We refer to [4, Theorems 14, 15 and 16] for the proofs of these facts.

The following is our main theorem in [2], which determines when an additive equation is reducible and if so, describes its factorization to irreducible components.

Theorem 2.3. *Let $A(T), B_1(T), \ldots, B_t(T) \in \mathcal{R}$ be nonzero additive polynomials and assume that A is monic, separable and splits in K. Let $r_1, \ldots, r_t$ be distinct positive integers with $\gcd(p, r_i) = 1$, for all $1 \leq i \leq t$. Set*

$$L(T) := \mathrm{lgcd}(A(T), B_1(T), B_2(T), \ldots, B_t(T)).$$

Let $\hat{A}(T), \hat{B}_1(T), \ldots, \hat{B}_t(T) \in \mathcal{R}$ be additive polynomials such that

$$\begin{aligned} A(T) &= L(T) \circ \hat{A}(T) \quad \text{and} \\ B_i(T) &= L(T) \circ \hat{B}_i(T) \quad \text{for } 1 \leq i \leq t. \end{aligned}$$

Let W be the set of roots of $L(T)$. Then,

i)

$$A(T) - \sum_{i=1}^{t} B_i(x^{r_i}) \text{ is irreducible over } K(x) \text{ if and only if } L(T) = T.$$

ii) The following polynomial identity holds in the ring $K(x)[T]$:

$$A(T) - \sum_{i=1}^{t} B_i(x^{r_i}) = \prod_{w \in W} \left(\hat{A}(T) - \sum_{i=1}^{t} \hat{B}_i(x^{r_i}) - w \right)$$

iii) for each $w \in W$, the polynomial

$$\hat{A}(T) - \sum_{i=1}^{t} \hat{B}_i(x^{r_i}) - w \in K(x)[T]$$

is irreducible.

If K is a finite field, Theorem 2.3 yields a Weil-Serre type bound for a large class of (reducible or irreducible) additive equations.

Corollary 2.4. *Let $K = \mathbb{F}_q$ be a finite field of characteristic p in Theorem 2.3 and let N denote the number of solutions $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ of*

$$A(y) = \sum_{i=1}^{t} B_i(x^{r_i}). \tag{2.4}$$

If $\deg A = p^n$ and $\deg L = p^\mu$, then

$$|N - qp^\mu| \leq \frac{(p^n - p^\mu)(R-1)}{2} \lfloor 2\sqrt{q} \rfloor, \tag{2.5}$$

where $R = \max\{r_1, \ldots, r_t\}$.

When these results are applied to (reducible or irreducible) additive equations with $A(T) = T^q - T$ (cf (1.3)), we obtain the necessary estimates for determining weight bounds for arbitrary cyclic codes. Our method requires the degrees of certain left greatest common divisor polynomials. It can be shown by examples that our bounds perform very well against the BCH bound and they yield the exact minimum distance in some cases.

References

[1] C. Güneri and F. Özbudak, "Cyclic codes and reducible additive equations", *IEEE Trans. Inform. Theory*, vol. 53, no. 2, 848-853, 2007.

[2] C. Güneri and F. Özbudak, "Weil-Serre type bounds for cyclic codes", *IEEE Trans. Inform. Theory*, vol. 54, no. 12, 5381-5395, 2008.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, 1997.

[4] O. Ore, "On a special class of polynomials", *Trans. Amer. Math. Soc.*, vol. 35, no. 3, 559-584, 1933.

[5] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[6] J. Wolfmann, "New bounds on cyclic codes from algebraic curves", in: Lecture Notes in Computer Science, vol. 388, pp. 47-62, New York: Springer-Verlag, 1989.