HAL open science

Hasse-Weil Bound for Additive Cyclic Codes

Cem Güneri, Ferruh Özbudak, Fundä Ozdemir

To cite this version:

Cem Güneri, Ferruh Özbudak, Fundä Ozdemir. Hasse-Weil Bound for Additive Cyclic Codes. WCC2015 - 9th International Workshop on Coding and Cryptography 2015, Anne Canteaut, Gaëtan Leurent, Maria Naya-Plasencia, Apr 2015, Paris, France. hal-01275733

HAL Id: hal-01275733

https://inria.hal.science/hal-01275733v1

Submitted on 18 Feb 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Hasse-Weil Bound for Additive Cyclic Codes

Cem Güneri[1] Ferruh Özbudak[2] Funda Özdemir[1]

[1] Faculty of Engineering and Natural Sciences, Sabancı University, 34956 İstanbul, Turkey
guneri@sabanciuniv.edu , fundaeksi@sabanciuniv.edu
[2] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, 06531, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. We obtain a bound on the minimum distance of additive cyclic codes via number of rational points on certain algebraic curves over finite fields. This is an extension of the analogous bound in the case of classical cyclic codes. Our result seems to be the only general bound on such codes aside from Bierbrauer's BCH bound.

Keywords: additive cyclic code, algebraic curve over a finite field, Hasse-Weil bound

1 Introduction

Algebraic curves over finite fields and the Hasse-Weil bound on their number of rational points was used by Wolfmann to obtain a bound on the minimum distance of cyclic codes ([5]). This bound did not apply to certain cyclic codes which are defined over extension fields rather than prime finite fields. Wolfmann's bound was extended to all cyclic codes over all finite fields by the first two authors in [3]. Main tools in relating the weights in cyclic codes and the number of rational points on certain algebraic curves are the trace representation of the codes and Hilbert's Theorem 90.

Bierbrauer introduced a generalization of cyclic codes and named them additive cyclic codes in [1]. He also proved a BCH bound for the minimum distance of additive cyclic codes. Our goal is to find a Hasse-Weil type bound on these codes and hence extend the analogous result from cyclic codes. We first need to introduce additive cyclic codes.

Let q be a prime power, $F = \mathbb{F}_{q^r}$ and $E = \mathbb{F}_q^m$ throughout, where $m \leq r$ are positive integers. Let $n \mid (q^r - 1)$ be a positive integer, W be the multiplicative subgroup of F^* of order n and α be a generator of W. Fix $A = \{i_1, ..., i_s\} \subset \mathbb{Z}/n\mathbb{Z}$, where $i_j \geq 1$ for all j. Let

$$\mathcal{P}(A) := \{a_1 x^{i_1} + ... + a_s x^{i_s} : a_1, \ldots, a_s \in F\},$$

which is an F-linear space of polynomials and set

$$\mathcal{B}(A) := \{(f(\alpha^0), \ldots, f(\alpha^{n-1})) : f(x) \in \mathcal{P}(A)\}.$$

Consider a surjective $\mathbb{F}_q$-linear mapping

$$\begin{aligned}\phi : F &\longrightarrow E\\ x &\longmapsto (\mathrm{Tr}(\gamma_1 x), \ldots, \mathrm{Tr}(\gamma_m x))\end{aligned}$$

for some subset $\{\gamma_1, \ldots, \gamma_m\} \subset E$, where Tr denotes the trace map from F to $\mathbb{F}_q$. Note that $\{\gamma_1, \ldots, \gamma_m\}$ is linearly independent over $\mathbb{F}_q$ since ϕ is onto. Extend ϕ naturally as follows:

$$\begin{aligned}\phi : F^n &\longrightarrow E^n\\ (x_1, \ldots, x_n) &\longmapsto (\phi(x_1), \ldots, \phi(x_n)).\end{aligned}$$

Definition 1 With the notation so far, we define the **additive cyclic code** $\mathcal{C}(A)$ of length n over E as

$$\mathcal{C}(A) := \phi(\mathcal{B}(A)) = \{\phi\big(f(\alpha^0), \ldots, f(\alpha^{n-1})\big) : f(x) \in \mathcal{P}(A)\}.$$

Remark 2 The code $\mathcal{C}(A)$ is not linear over its alphabet E but over $\mathbb{F}_q$. If we view $\mathcal{C}(A)$ in $\mathbb{F}_q^{mn}$ as

$$\begin{aligned}\mathcal{C}(A) = \big\{\big(&\mathrm{Tr}(\gamma_1 f(\alpha^0)), \ldots, \mathrm{Tr}(\gamma_m f(\alpha^0)); \cdots\\ &\cdots ; \mathrm{Tr}(\gamma_1 f(\alpha^{n-1})), ..., \mathrm{Tr}(\gamma_m f(\alpha^{n-1}))\big) : f(x) \in \mathcal{P}(A)\big\},\end{aligned}$$

then it is an $\mathbb{F}_q$-linear code of length mn over $\mathbb{F}_q$.

Remark 3 It is not difficult to see that $\mathcal{C}(A) \subset E^n$ is closed under cyclic shift. This justifies (together with Remark 2) the name additive cyclic. This means that when $\mathcal{C}(A)$ is viewed in $\mathbb{F}_q^{mn}$, it is closed under shift by m units. Hence over $\mathbb{F}_q$, $\mathcal{C}(A)$ is a quasi-cyclic code of length mn and index m.

Remark 4 Classical cyclic codes correspond to the special case $m = 1$. In this case $\mathcal{C}(A)$ is the cyclic code of length n over $\mathbb{F}_q$ whose dual's defining zeros are $\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$ (see [3] and [5]).

2 A Bound on the Minimum Distance

Let $n = q^r - 1$ in the rest of this manuscript. Since $i_j > 0$ for all j, we have $f(0) = 0$ for any $f(x) \in \mathcal{P}(A)$. Hence the weight of the codeword $c_f = (\phi(f(\alpha^0)), ..., \phi(f(\alpha^{n-1}))) \in \mathcal{C}(A)$ is

$$\begin{aligned}wt(c_f) &= n - |\{x \in F : \phi(f(x)) = 0\}| + 1\\ &= q^r - |\{x \in F : \mathrm{Tr}(\gamma_i f(x)) = 0 \text{ for all } 1 \le i \le m\}|. \qquad (1)\end{aligned}$$

Let us define the following $\mathbb{F}_q$-linear subspace in F.

$$V := \{x \in F : \mathrm{Tr}(\gamma_1 x) = \cdots = \mathrm{Tr}(\gamma_m x) = 0\}. \qquad (2)$$

Since $\{\gamma_1, ..., \gamma_m\}$ is linearly independent over $\mathbb{F}_q$, V is an $\mathbb{F}_q$-subspace of codimension m in F (cf. [2, Proposition 2.1]). We will use the following result.

Lemma 5 ([2], Corollary 2.5) *For every $\mathbb{F}_q$-linear subspace U in F of codimension m, there exists a uniquely determined monic q-additive polynomial $A(T) \in F[T]$ of degree q^m, which splits in F and satisfies*

$$U = \mathrm{Im}(A) = \{A(y) : y \in F\}.$$

The following is now easy to observe.

Proposition 6 *Let U be an $\mathbb{F}_q$-subspace of codimension m in F and let $A(T) \in F[T]$ be the monic q-additive polynomial attached to U as in Lemma 5. Define*

$$B(T) = \prod_{u \in U} (T - u) \in F[T],$$

which is another q-additive polynomial. Then

$$U = \mathrm{Im}(A) = \mathrm{Ker}(B) \quad \textit{and} \quad B(A(T)) = T^{q^r} - T.$$

Remark 7 Let $U = \{x \in F : \mathrm{Tr}(x) = 0\}$ be a codimension 1 $\mathbb{F}_q$-subspace of F. Then it is easily seen that $B(T) = \mathrm{Tr}(T)$ and $A(T) = T^q - T$ so that $\mathrm{Im}(A) = U = \mathrm{Ker}(B)$. This, in fact, is the well-known Hilbert's Theorem 90, i.e.

$$\mathrm{Tr}(x) = 0 \text{ if and only if } y^q - y = x \text{ for some } y \in F.$$

So, Proposition 6 can be viewed as a generalization of Hilbert's Theorem 90.

By (1) and (2), computing the weight of the codeword $c_f \in \mathcal{C}(A)$ requires determination of the number of $x \in F$ such that $f(x) \in V$. Let $A(T)$ and $B(T)$ be the q-additive polynomials of degree q^m and q^{r-m}, respectively, that are attached to V as in Proposition 6. By the same Proposition, we have

$$f(x) \in V \text{ for } x \in F \quad \text{if and only if} \quad A(y) = f(x) \text{ for some } y \in F.$$

Moreover, if $A(y) = f(x)$ then $A(y + y_0) = A(y) = f(x)$ for all $y_0 \in \mathrm{Ker}(A)$. Note that there are $\deg A = q^m$ such y_0's and all lie in F since A splits in F (cf. Lemma 5). Hence,

$$wt(c_f) = q^r - \frac{|\mathcal{X}_f^{af}(F)|}{q^m}, \tag{3}$$

where $|\mathcal{X}_f^{af}(F)|$ denotes the number of affine F-rational points on the curve $\mathcal{X}_f$ defined by

$$A(Y) = f(X). \tag{4}$$

These observations lead to the following, which is an extension of the algebraic geometric bound on the distance of classical cyclic codes to additive cyclic codes.

Theorem 1 *Consider the additive cyclic code $\mathcal{C}(A)$ of length $n = q^r - 1$ over E, where $A = \{i_1, ..., i_s\} \subset \mathbb{Z}/n\mathbb{Z}$. Assume that $\gcd(i_j, q) = 1$ for all j and let $i = \max\{i_j : 1 \le j \le s\}$. Then,*

$$d(\mathcal{C}(A)) \ge q^r - q^{r-m} - \frac{(q^m - 1)(i - 1)\lfloor 2\sqrt{q^r} \rfloor}{2q^m}.$$

Proof. Since the weights of all codewords are related to F-rational affine points on the family $\mathcal{F} = \{A(Y) = f(X) : f(X) \in \mathcal{P}(A)\}$, writing an upper bound on the number of affine F-rational points that applies to all members of $\mathcal{F}$ will yield a lower bound on the minimum distance of $\mathcal{C}(A)$. The assumption on i_j's guarantee that any curve in $\mathcal{F}$ (except for the one with $f(X) = 0$) is irreducible. Moreover, any such curve has one F-rational point at infinity. The number $(q^m - 1)(i-1)/2$ is an upper bound on the genera of the curves in $\mathcal{F}$ (see [3]). Therefore, Serre's improvement on the Hasse-Weil bound ([4, Theorem 5.3.1]) yields

$$|\mathcal{X}^{af}(F)| \leq q^r + \frac{(q^m-1)(i-1)}{2}\lfloor 2\sqrt{q^r}\rfloor,$$

for any $\mathcal{X} \in \mathcal{F}$. The result follows by (3). □

Remark 8 As stated in Remark 4, Wolfmann's bound for classical cyclic codes corresponds to $m = 1$ in the above result. In that case, curves (4) related to codewords are Artin-Schreier type curves, i.e. $A(T) = T^q - T$ in (4) (cf. Remark 7).

3 Extending the Bound

Note that the assumption $\gcd(i_j, q) = 1$ (for all j) in Theorem 1 is made to guarantee that the equation

$$A(Y) = \lambda_1 X^{i_1} + \cdots + \lambda_s X^{i_s} \tag{5}$$

defines an irreducible curve over F whose genus and hence the Hasse-Weil bound on the number of its F-rational points are known. A Hasse-Weil bound on reducible curves was obtained in [3] to extend Wolfmann's minimum distance bound on cyclic codes to more general class of cyclic codes. The same result is also helpful for extending Theorem 1. We need some background first.

Let p be the characteristic of F. A polynomial of the form

$$a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T \quad (a_i \in F)$$

is called an additive polynomial in $F[T]$. What we called a q-additive polynomial in the previous sections refer to additive polynomials whose exponents are powers of q. Note that the composition of two additive polynomials is again an additive polynomial. In fact, the set of all additive polynomials in $F[T]$ forms a ring $\mathcal{R}$ under polynomial addition and composition.

The ring $\mathcal{R}$ is noncommutative. We say that $A \in \mathcal{R}$ is left divisible by

$$B(T) = b_v T^{p^v} + b_{v-1} T^{p^{v-1}} + \cdots + b_1 T^p + b_0 T \in \mathcal{R}$$

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

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

where $R(T) \in \mathcal{R}$ is of degree less than $\deg B$, unless $R = 0$. Hence, over the perfect field F, 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 $\mathcal{R}$. In fact, if we denote the right ideal generated by A, B in $\mathcal{R}$ as

$$< A, B >_R := \{A(T) \circ P_1(T) + B(T) \circ P_2(T) : \quad P_1, P_2 \in \mathcal{R}\},$$

then $\mathrm{lgcd}(A, B) \in \mathcal{R}$ is the monic generator of this principal ideal.

Now suppose $i_j = r_j p^{a_j}$ where $p \nmid r_j$ (for all $1 \leq j \leq s$). Note that although i_j's are pairwise distinct, this need not be the case for r_j's. Let us assume that the distinct p-free parts among i_j's are ordered as $r_1, \ldots, r_t$ ($t \leq s$). Write the equation (5) as

$$A(Y) = B_1(X^{r_1}) + \cdots + B_t(X^{r_t}), \tag{6}$$

where $B_j(T) \in \mathcal{R}$ is an additive polynomial over F for all $1 \leq j \leq t$.

Lemma 9 ([3], Corollary 2.9, Corollary 2.11) *With the notation above, consider the curve X defined over $F = \mathbb{F}_{q^r}$ by (6). Let*

$$L(T) = \mathrm{lgcd}\big(A(T), B_1(T), \ldots, B_t(T)\big) \in \mathcal{R}.$$

i. Equation (6) defines an irreducible curve over F if and only if $L(T) = T$.
ii. Let $\deg A = p^a$, $\deg L = p^\mu$. Then

$$|\mathcal{X}^{af}(F)| \leq q^r p^\mu + \frac{(p^a - p^\mu)(R-1)}{2} \lfloor 2\sqrt{q^r} \rfloor, \tag{7}$$

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

Remark 10 In case i_j's are all relatively prime to q as in Theorem 1, we have $t = s$, $i_j = r_j$ and $B_j(T) = \lambda_j T$ for all j (cf. (5)). In particular $L(T) = T$ so that $\mu = 0$ and inequality (7) reduces to Hasse-Weil inequality.

Results in Lemma 9 leads to a bound on the minimum distance of any cyclic code, extending Wolfmann's bound (see [3]). These results also apply to additive cyclic codes. Among all the curves (reducible or irreducible) in the family $\mathcal{F} = \{A(Y) = \lambda_1 X^{i_1} + \cdots + \lambda_s X^{i_s} : \lambda_j \in F\}$, one has to determine the maximal possible Hasse-Weil bound and proceeds as in the proof of Theorem 1. This involves determining degrees of left greatest common divisors for the additive cyclic code in hand. For the purpose of determining such possible degrees, the notion of LGCD trees were introduced in [3]. The same method can be applied for additive cyclic codes too.

References

1. Bierbrauer, J., "The theory of cyclic codes and a generalization to additive codes", *Des. Codes Cryptogr.*, vol. 25, 189-206, 2002.
2. Garcia, A., Özbudak, F., "Some maximal function fields and additive polynomials", *Comm. Algebra*, vol. 35, 1553-1566, 2007.

3. Güneri, C., Özbudak, F., "Weil-Serre type bounds for cyclic codes", *IEEE Trans. Inform. Theory*, vol. 54, 5381-5395, 2008.
4. Stichtenoth, H., Algebraic Function Fields and Codes, *Springer GTM*, vol. 254, 2009.
5. Wolfmann, J., "New bounds on cyclic codes from algebraic curves", *Coding theory and applications (Toulon, 1988), Lecture Notes in Comput. Sci.*, vol. 388, 47-62, 1989.