Advances in Mathematics of Communications
Volume 11, No. 2, 2017, 353–357

doi:10.3934/amc.2017028

ON COMPLEMENTARY DUAL ADDITIVE CYCLIC CODES

Cem Güneri

Faculty of Engineering and Natural Sciences
Sabancı University, 34956, İstanbul, Turkey

Ferruh Özbudak

Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, 06531, Ankara, Turkey

Funda Özdemir

Faculty of Engineering and Natural Sciences
Sabancı University, 34956, İstanbul, Turkey

(Communicated by Ivelisse Rubio)

Abstract. A code is said to be complementary dual if it meets its dual trivially. We give a sufficient condition for a special class of additive cyclic codes to be complementary dual.

1. Introduction

Additive cylic codes (AC codes) are a nonlinear generalization of linear cyclic codes and introduced by Bierbrauer in [1]. The alphabet of these codes is not a finite field but a vector space E over the ground field $\mathbb{F}_q$. Properties of AC codes and their relations to quantum codes are studied in [1, 2]. Bierbrauer also obtained a BCH type lower bound on the minimum distance of AC codes. Another lower bound on the minimum distance of AC codes were recently obtained by the authors using the number of rational points of certain algebraic curves over finite fields ([7]). This bound is the only general bound on such codes aside from Bierbrauer's BCH bound.

Linear complementary dual (LCD) codes are linear codes that meet their dual trivially. These codes were introduced by Massey in [9]. They were rediscovered recently in the context of counter measures to passive and active side channel analysis on embedded crypto-systems ([4]). Characterization of cyclic LCD codes ([11]), their asymptotic goodness ([10]) and quasi-cylic LCD codes ([8, 5]) have been studied so far. The purpose of this research is to study complementary dual subclass of AC codes.

2. Preliminaries

Let q be a prime power, $F = \mathbb{F}_{q^r}$ and $E = \mathbb{F}_q^m$, 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

2010 *Mathematics Subject Classification:* Primary: 58F15, 58F17; Secondary: 53C35.
Key words and phrases: Additive cyclic code, complementary dual code.

order n and α be a generator of W. Fix $A = \{i_1, ..., i_s\} \subset \mathbb{Z}/n\mathbb{Z}$. 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

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

Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\} \subset F$ be a linearly independent set over $\mathbb{F}_q$. Define an F-linear code of length mn

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

Consider the $\mathbb{F}_q$-linear mapping

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

where Tr denotes the trace map from F to $\mathbb{F}_q$. Note that ϕ_Γ is surjective since Γ is linearly independent. Extend ϕ_Γ naturally as follows:

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

Definition 2.1. An additive cyclic code of length n over E is defined as

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

The set A is called the defining set of the code.

The code $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is an additive subgroup of E^n. It is not difficult to see that $\phi_\Gamma\big(\mathcal{B}(A)\big) \subset E^n$ is closed under cyclic shift. If we view the code in $\mathbb{F}_q^{mn}$ as

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

then it is an $\mathbb{F}_q$-linear code of length mn over $\mathbb{F}_q$, which is equal to $\mathrm{Tr}\big((\mathcal{B}(A), \Gamma)\big)$. Moreover, as a length mn code over $\mathbb{F}_q$, it is closed under shift by m coordinates. Hence over $\mathbb{F}_q$, $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is a quasi-cyclic code of length mn and index m. Classical cyclic codes correspond to the special case $m = 1$. In this case $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is the cyclic code of length n over $\mathbb{F}_q$ whose dual's defining zeros are $\{\alpha^{i_1}, \ldots, \alpha^{i_s}\}$.

Define

$$\begin{aligned}V_F(Z) : \;=\; & \{\big(p_1(\alpha^0), \ldots, p_m(\alpha^0); \;\ldots \\ & \ldots \;; p_1(\alpha^{n-1}), \ldots, p_m(\alpha^{n-1})\big) : p_i(x) \in \mathcal{P}(Z)\}\end{aligned}$$

for a a q-cyclotomic coset Z mod n. To simplify notation, we will denote the codeword in $V_F(Z)$ determined by $p_i(x) \in \mathcal{P}(Z)$ as $(p_1(x), \ldots, p_m(x))$.

Let $\overline{(\mathcal{B}(A), \Gamma)}$ be the Galois closure of $(\mathcal{B}(A), \Gamma)$, i.e. the smallest Galois closed code containing $(\mathcal{B}(A), \Gamma)$. Assume that $\overline{(\mathcal{B}(A), \Gamma)}^{\perp} = \overline{(\mathcal{B}(B), \Gamma')}$ for some $B \subset \mathbb{Z}/n\mathbb{Z}$ and $\Gamma' \subset F^m$. Then $\phi_\Gamma\big(\mathcal{B}(A)\big)^{\perp} = \phi_{\Gamma'}\big(\mathcal{B}(B)\big)$ ([7, Lemma 11]). Here the dual is with respect to the Euclidean dot product on E^n: $(u_1, ..., u_n) \cdot (v_1, ..., v_n) =$

$\sum_{i=1}^{n} u_i \cdot v_i$, for $u_i, v_i \in E = \mathbb{F}_q^m$, where $u_i \cdot v_i$ is the Euclidean product. We can decompose $\overline{(\mathcal{B}(A), \Gamma)}^{\perp}$ as

$$\overline{(\mathcal{B}(A), \Gamma)}^{\perp} = \bigoplus_{Z} \left[\overline{(\mathcal{B}(A \cap Z), \Gamma)}^{\perp} \cap V_F(-Z)\right],$$

where Z runs through all q-cyclotomic cosets mod n ([7, Corollary 15]). If every summand here can be written in the form $\overline{(\mathcal{B}(B_Z), \Gamma')}$, then it follows that $B = \bigcup_Z B_Z$.

In the case $m = 2$, the following result gives the set B explicitly, hence the dual code.

Theorem 2.2 ([7, Theorem 4])**.** *Let $m = 2$, $\Gamma = (1, \gamma)$ and $b = [\mathbb{F}_q(\gamma) : \mathbb{F}_q] > 1$. Let $Z = \{i, iq, ..., iq^{s-1}\}$ be a q-cyclotomic coset mod n of length s. For $\Gamma' = (-\gamma, 1)$, we have the following:*

i. If $A \cap Z = \emptyset$, then $B_Z = -Z$.

ii. If $A \cap Z = \{iq^{u_1}, iq^{u_2}, ..., iq^{u_t}\}$ for some $0 \le u_1 < u_2 < \cdots < u_t \le s-1$ and b does not divide s, then $B_Z = \emptyset$.

iii. If $A \cap Z = \{iq^{u_1}, iq^{u_2}, ..., iq^{u_t}\}$ for some $0 \le u_1 < u_2 < \cdots < u_t \le s-1$ and b divides s, set $\hat{A}_Z = \{iq^{u_a + \ell b} \text{ mod } n : 0 \le \ell \le r-1\}$ for some $a \in \{1, \ldots, t\}$. Then

- *$B_Z = \emptyset$ if $A \cap Z \not\subseteq \hat{A}_Z$.*
- *$B_Z = -\hat{A}_Z$ if $A \cap Z \subseteq \hat{A}_Z$.*

3. Additive cyclic codes with complementary duals

Let $n = q^r - 1$ and $m = 2$ in this section. For $\Gamma = (1, \gamma)$, the dual of $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is $\phi_{\Gamma'}(\mathcal{B}(B))$, where $\Gamma' = (-\gamma, 1)$ and the set B is determined explicitly in Theorem 2.2. Elements of $\phi_\Gamma\big(\mathcal{B}(A)\big)$ and its dual $\phi_{\Gamma'}(\mathcal{B}(B))$ are of the form $c_f = \big(\mathrm{Tr}(f(x)), \mathrm{Tr}(\gamma f(x))\big)$ for $f(x) \in \mathcal{P}(A)$ and $c_g = \big(\mathrm{Tr}(-\gamma g(x)), \mathrm{Tr}(g(x))\big)$ for $g(x) \in \mathcal{P}(B)$, respectively. Then $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is not complementary dual if and only if there exist $f(x) \in \mathcal{P}(A)$ and $g(x) \in \mathcal{P}(B)$ such that $c_f \neq \vec{0} \neq c_g$ and $c_f = c_g$. We will use the following result.

Lemma 3.1 ([6, Proposition 2.3])**.** *Let $\lambda_j \in \mathbb{F}_{q^r}$ and i_j be positive integers, for $j = 1, 2, \ldots, s$. Assume that the q-cyclotomic cosets containing i_j's are distinct. Then $\mathrm{Tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in $\mathbb{F}_{q^r}$ if and only if $\mathrm{Tr}(\lambda_j x^{i_j}) = 0$ for all x in $\mathbb{F}_{q^r}$ and for all $j = 1, 2, \ldots, s$.*

A slight modification of Lemma 3.1 is needed for our purposes.

Lemma 3.2. *Let $\lambda_0, \lambda_j \in F$ and i_j be positive integers, for $j = 1, 2, \ldots, s$. Assume that the q-cyclotomic cosets mod n containing i_j's are distinct. Then $\mathrm{Tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in F^* if and only if $\mathrm{Tr}(\lambda_0) = 0$ and $\mathrm{Tr}(\lambda_j x^{i_j}) = 0$ for all x in F^* and for all $j = 1, 2, \ldots, s$.*

Proof. Assume $\mathrm{Tr}(\lambda_0 + \lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = 0$ for all x in F^*. By linearity of the trace map, $\mathrm{Tr}(\lambda_1 x^{i_1} + \lambda_2 x^{i_2} + \cdots + \lambda_s x^{i_s}) = -\mathrm{Tr}(\lambda_0) =: c$ for all x in F^*. Then

$$(q^r - 1)c \quad = \quad \sum_{x \in F^*} \mathrm{Tr}(\lambda_1 x^{i_1} + \cdots + \lambda_s x^{i_s})$$

$$\begin{aligned} &= \mathrm{Tr}\big(\sum_{x\in F^*}(\lambda_1 x^{i_1}+\cdots+\lambda_s x^{i_s})\big)\\ &= \mathrm{Tr}\big(\lambda_1\sum_{x\in F^*}x^{i_1}+\cdots+\lambda_s\sum_{x\in F^*}x^{i_s}\big)\\ &= 0\end{aligned}$$

where the last equality follows from the fact that if i is not a multiple of q^r-1, then $\sum_{x\in F^*}x^i=0$. Therefore $c=0$, i.e. $\mathrm{Tr}(\lambda_0)=0$ and $\mathrm{Tr}(\lambda_1x^{i_1}+\lambda_2x^{i_2}+\cdots+\lambda_sx^{i_s})=0$ for all x in F^*. By Lemma 3.1 , $\mathrm{Tr}(\lambda_0)=0$ and $\mathrm{Tr}(\lambda_jx^{i_j})=0$ for all x in F^* and for all $j=1,2,\ldots,s$.

The converse is immediate from linearity of the trace map. □

For $A\subseteq\mathbb{Z}/n\mathbb{Z}$, denote by $\overline{A}$ the union of all q-cyclotomic cosets mod n intersecting A nontrivially.

Proposition 3.3. *Let A and B be defining sets for the additive cyclic code and its dual as before. If $\overline{A}\cap B=\emptyset$, then $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is complementary dual.*

Proof. Let $f(x)\in\mathcal{P}(A)$ and $g(x)\in\mathcal{P}(B)$, and suppose $c_f=c_g$. Then $\mathrm{Tr}(f(x)+\gamma g(x))=0$ and $\mathrm{Tr}(\gamma f(x)-g(x))=0$ for all $x\in F^*$. By the assumption $\overline{A}\cap B=\emptyset$, exponents of f and g cannot lie in the same cyclotomic coset. Some exponents that appear in f (or in g) may be from the same cyclotomic coset. This is no harm for concluding $\mathrm{Tr}(f(x))=0=\mathrm{Tr}(\gamma g(x))$ and $\mathrm{Tr}(\gamma f(x))=0=\mathrm{Tr}(g(x))$ for all x in F^* (by Lemma 3.2), since $\mathrm{Tr}(ax^j+bx^{jq})=\mathrm{Tr}((a+b^{1/q})x^j)$. Therefore, $c_f=\vec{0}=c_g$, i.e. anything in the intersection $\phi_\Gamma\big(\mathcal{B}(A)\big)\cap\phi_{\Gamma'}\big(\mathcal{B}(B)\big)$ has to be $\vec{0}$. □

Theorem 3.4. *Let $b=[\mathbb{F}_q(\gamma):\mathbb{F}_q]>1$. Then $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is complementary dual if the following conditions are satisfied by every q-cyclotomic coset Z mod n:*

i. $A\cap Z=\emptyset$ if and only if $A\cap(-Z)=\emptyset$.

ii. If $A\cap Z\neq\emptyset$, then $A\cap Z$ is not contained in the q^b-cyclotomic coset mod n of some element in $A\cap Z$.

Proof. If a cyclotomic coset Z does not intersect A, then we also have $\overline{A}\cap Z=\emptyset$. Therefore, such a cyclotomic coset cannot contribute to $\overline{A}\cap B$.

Now assume that a cyclotomic coset Z intersects A. By assumption i, we have $A\cap(-Z)\neq\emptyset$ too. If b does not divide $|Z|=|-Z|$, then by Theorem 2.2 part ii, we have $B_{-Z}=B\cap Z=\emptyset$ and such Z cannot contribute to $\overline{A}\cap B$. So assume that b divides $|Z|=|-Z|$. Note that $\hat{A}_{-Z}$ is nothing but the q^b-cyclotomic coset mod n of some element in $A\cap(-Z)$. Hence assumption ii implies that $A\cap(-Z)\not\subseteq\hat{A}_{-Z}$ and therefore (by Theorem 2.2), we have $B_{-Z}=B\cap Z=\emptyset$. Therefore such a coset Z cannot contribute to $\overline{A}\cap B$ even if b divides $|Z|$. The result follows from Proposition 3.3. □

Corollary 3.5. *Let $b=[\mathbb{F}_q(\gamma):\mathbb{F}_q]=r$. Then $\phi_\Gamma\big(\mathcal{B}(A)\big)$ is complementary dual if the following conditions are satisfied by every q-cyclotomic coset Z mod n:*

i. $A\cap Z=\emptyset$ if and only if $A\cap(-Z)=\emptyset$.

ii. If $A\cap Z\neq\emptyset$, then there exists at least two elements from Z in A.

Proof. Since $b=r$, q^b-cyclotomic coset mod n of any element in $A\cap Z$ consists of a single element. Hence by ii, $A\cap Z$ satisfies condition ii in Theorem 3.4 and the result follows. □

In the following table, by using our results we present examples of AC complementary dual codes over $E = \mathbb{F}_2^2$. In this table, M and d stand for the size and minimum distance of the code, respectively. The computational algebra system Magma [3] is used for computations.

r	b	A	M	d
4	4, 2	$\{1, 2, 7, 11\}$	4^8	4
4	4	$\{1, 4, 7, 11\}$	4^8	4
4	4, 2	$\{3, 6, 5, 10\}$	4^6	6
5	5	$\{1, 2, 15, 23\}$	4^{10}	10
6	6, 3	$\{1, 4, 31, 47\}$	4^{12}	24
6	6, 3, 2	$\{1, 2, 31, 47\}$	4^{12}	24
6	6, 3, 2	$\{1, 2, 31, 47, 21, 42\}$	4^{14}	22
7	7	$\{1, 2, 63, 126\}$	4^{14}	54
8	8, 4, 2	$\{4, 8, 127, 191\}$	4^{16}	112
8	8, 2	$\{1, 16, 127, 191\}$	4^{16}	112

Acknowledgments

The first author is supported by TÜBİTAK project 114F432. The third author is supported by TÜBİTAK BİDEB 2211 National PhD Scholarship Programme.

References

[1] J. Bierbrauer, The theory of cyclic codes and a generalization to additive codes, *Des. Codes Crypt.*, **25** (2002), 189–206.

[2] J. Bierbrauer and Y. Edel, Quantum twisted codes, *J. Combin. Des.*, **8** (2000), 174–188.

[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I. The user language, *J. Symb. Comput.*, **24** (1997), 235–265.

[4] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, in *Proc. 4th ICMCTA Meeting*, Palmela, Portugal, 2014.

[5] M. Esmaeili and S. Yari, On complementary-dual quasi-cyclic codes, *Finite Fields Appl.*, **15** (2009), 375–386.

[6] C. Güneri, Artin-Schreier curves and weights of two-dimensional cyclic codes, *Finite Fields Appl.*, **10** (2004), 481–505.

[7] C. Güneri, F. Özbudak and F. Özdemir, Hasse-Weil bound for additive cyclic codes, *Des. Codes Crypt.*, **82** (2017), 249–263.

[8] C. Güneri, B. Özkaya and P. Solé, Quasi-cyclic complementary dual codes, *Finite Fields Appl.*, **42** (2016), 67–80.

[9] J. L. Massey, Linear codes with complementary duals, *Discrete Math.*, **106-107** (1992), 337–342.

[10] N. Sendrier, Linear codes with complementary duals meet the Gilbert-Varshamov bound, *Discrete Math.*, **285** (2004), 345–347.

[11] X. Yang and J. L. Massey, The condition for a cyclic code to have a complementary dual, *Discrete Math.*, **126** (1994), 391–393.

Received February 2016; revised March 2016.

E-mail address: guneri@sabanciuniv.edu
E-mail address: ozbudak@metu.edu.tr
E-mail address: fundaeksi@sabanciuniv.edu