Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 154 (2019) 663–668

Procedia Computer Science

www.elsevier.com/locate/procedia

8th International Congress of Information and Communication Technology, ICICT 2019

LCD MDS Codes From Cyclic Codes

Qiang Fu[a**], Rui Hu Li[a], Luo Bin Guo[a]

[a]*Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, China*

Abstract

Linear codes with complementary-duals (LCD) have many applications in cryptography, communication systems and data storage. A q-ary linear code C is called LCD if $C \cap C^{\perp} = \{0\}$ holds. Using method of coset theory, we deduce a characterization of LCD cyclic code by its defining set. Then two families of q-ary MDS cyclic LCD codes with lengthes $n|(q+1)$ and $n|(q-1)$ are determined and many new classes of LCD MDS codes are gained.

Keywords: LCD code, MDS code, cyclotomic coset, cyclic code;

1. Introduction

Refs [5-6] first present cyclic LCD codes and [4] constructed LCD MDS codes through Reed-Solomon (RS) codes and presented several methods of constructing LCD codes. Since then, researchers paid much attention to this topic and present many results, such as, LCD cyclic codes in [7-8], a condition that negacyclic codes are LCD codes in [9], LCD MDS codes through GRS codes in [11].

Inspired by [4,9-11], we study the methods of constructing LCD MDS codes from q-ary cyclic codes in this paper. This paper has five parts. In Section 2 we will provide some required basic knowledge on cyclic codes and LCD codes. We derive some classes of LCD codes with length $n|(q+1)$ and new LCD codes from these MDS codes in Section 3. In Section 4, we discuss LCD codes with $n|(q-1)$. The last Section gives the conclusion.

* *Corresponding author:+(86) 17792026335
Email: fuqiangkgd@163.com

1877-0509
10.1016/j.procs.2019.06.104

2. Cyclic LCD Codes

We will recall preliminaries and notations on cyclic and LCD codes.

Notations**:** (1) For basics of cyclic codes and notations, see [1-3],the theory of q-cyclotomic coset, see [12].

(2) Since [11] has shown there are $[n,k]_q$ MDS LCD codes for all $n \geq 2$ and $k \in \{0,1,n-1,n\}$, we only give proof for $[n,k]_q$ MDS LCD codes with $2 \leq k \leq n-2$.

(3) For $n \geq 3$, we use Z_n to denote the ring of integer ring Z module n.

Definition 2.1 Suppose $\gcd(n,q)=1$, ξ is a primitive root of unity in some extension field that covers F_q. If C is cyclic with generator polynomial $g(x)$, $Z=\{\xi^i \mid g(\xi^i)=0\}$ is called the zero set of C and $T=\{i \mid \xi^i \in Z\}$ is called the defining set of C, respectively.

From [2-3], we know the defining set T of a q-ary cyclic code C of length n is the union of some q-cyclotomic cosets of modulo n, i.e. $T=\cup_i C_i$. If $T=C_b \cup C_{b+1} \cup \cdots$ -2 , the code with defining set T is a BCH code of designed distance δ, such a code has distance $d \geq \delta$.

When $b=1$, C is narrow-sense and otherwise non-narrow-sense. If $n=q^m-1$, C is called primitive and otherwise imprimitive. It is obvious that F_q^n and $\{\mathbf{0}\}$ are cyclic codes with defining set $T=\varnothing$ and $T=Z_n$. Both F_q^n and $\{\mathbf{0}\}$ are trivial LCD codes.

Proposition 2.2 [6] Let C be a linear code of length n. G and H are generator matrix and parity-check matrix of C. Then the following are equivalent:

1. C is LCD.
2. HH^T is invertible.
3. GG^T is invertible.
4. $\mathrm{C}+\mathrm{C}^{\perp}=F_q^n$.

Proposition 2.3 [7] Let C be a cyclic codewith generator polynomial $g(x)$. Then the following statements are equivalent.

1. C is LCD.
2. $g(x)$ is self-reciprocal.
3. β^{-1} is a root of $g(x)$ for every root β of $g(x)$ over splitting field of $g(x)$.

Proposition 2.4 Let $\gcd(n,q)=1$, C_i be cyclic codes with defining sets T_i for i=1,2. Then $\mathrm{C}_1 \cap \mathrm{C}_2$, $\mathrm{C}_1+\mathrm{C}_2$ have defining set $T_1 \cup T_2$, $T_1 \cap T_2$. $\mathrm{C}_1 \subseteq \mathrm{C}_2$ if and only if $T_2 \subseteq T_1$.

Lemma 2.5 Suppose C is a q-ary cyclic code of length n with T, $T^{-1}=\{-i \mid i \in T\}$. Then C is LCD if and only if $T=T^{-1}$.

Proof. According to Theorem 4.4.11 in [3], the defining set of $\mathrm{C}^{\perp}$ is $T^{\perp}=Z_n \setminus T^{-1}$. If $T=T^{-1}$, then $Z_n=T^{\perp} \cup T$ and $\mathrm{C} \cap \mathrm{C}^{\perp}$ is trivial, then the sufficiency holds. If C is LCD, then $\mathrm{C}+\mathrm{C}^{\perp}=F_q^n$ which can imply $T \cap T^{\perp}=T \cap (Z_n \setminus T^{-1})=\varnothing$. Hence $T=T^{-1}$ and the necessity follows.

Based on the theory of coset, we can present Lemma 2.5 in the following form.

Lemma **2.6** T is a defining set and deduces C, then C is LCD if and only if each $C_t \subseteq T$ is symmetric or C_t is asymmetric and $C_{-t} \subseteq T$.

3. Cyclic LCD MDS Codes with Length $n|(q+1)$

We will investigate LCD cyclic MDS codes with code length $n|(q+1)$ and determine new LCD MDS codes in these cyclic codes. We will show for suitable k with $1 \leq k \leq n-1$, there exists an $[n,k,n-k+1]_q$ LCD cyclic MDS code. Our discussions are presented in two subsections according to the different lengths of cyclic LCD codes.

3.1 Cyclic LCD codes with even n

Lemma 3.1. *For odd q and even n,* $n|(q+1)$, k *is odd and* $1 \le k \le n-1$, *then* C *is LCD and has* $[n,k,n-k+1]_q$.

Proof. *Let* $s = n/2$. *It is easy to check that* $C_0 = \{0\}$, $C_s = \{s\}$ *and* $C_i = \{i, n-i\}$ *are symmetric, here* $1 \le i \le s-1$.

Let $T_a = \cup_{i=0}^{a} C_{s-i}$ for $0 \le a \le s-1$. Then $|T_a| = 2a+1$. With a defining set T_a, the cyclic code C is LCD and has $[n, n-2a-1, 2a+2]_q$, hence C is LCD and *n-2a-1* is odd. $C^{\perp}$ is an $[n, 2a+1, n-2a]_q$ LCD MDS code with odd dimension. Hence we complete the proof.

According to Lemma 3.1, we have

Corollary 3.2. Let $q \ge 5$ be odd, even *n* and $n|(q+1)$. Then there is an $[n,k,n-k+1]_q$ new LCD MDS code for odd *k* with $3 \le k \le n-3$ if one of these conditions holds in the following:

(1) $n = q+1$;

(2) For square *q* and $q > n \ge max\{6, q^{1/2}+2\}$;

(3) For non-square *q* and $q < 4^{2n}(2n)^2$.

3.2 Cyclic LCD codes with odd n

In [10], for odd length *n* and $n|(q+1)/2$, a class of even dimensional LCD MDS codes were constructed from negacyclic codes. Now, we will discuss LCD cyclic MDS codes with odd length and construct new LCD MDS codes.

Lemma 3.3. If *n* is odd, $n|(q+1)$, $1 \le k \le n-1$, then C is LCD and has $[n,k,n-k+1]_q$.

Proof. It is easy to check that $C_0 = \{0\}, C_i = \{i, n-i\}$ are symmetric, for $1 \le i \le (n-1)/2$.

Let $s = (n-1)/2$ and denote $T_a = \cup_{i=0}^{a} C_{s-i}$ for $0 \le a \le s-1$. Then $|T_a| = 2a+2$. The cyclic code C with defining set T_a is an LCD code and has $[n, n-2a-2, 2a+3]_q$, hence C is LCD with odd dimension. $C^{\perp}$ is an $[n, 2a+2, n-2a-1]_q$ LCD cyclic MDS code with even dimension. Hence the lemma follows.

It is obvious that Lemma 3.3 constructs much more LCD MDS codes than that in [10]. If *q* is even and *n* is odd, then known $[n,k,n-k+1]_q$ LCD MDS codes with $n|(q+1)$, for $1 \le k \le n-1$, derived through GRS codes in [10] can also be constructed from special cyclic codes.

Corollary 3.4. Let *q* and *n* be odd. If $n|(q+1)$ and $n \ge q^{1/2}+2$, then there exists an $[n, n-k, k+1]_q$ new cyclic LCD MDS codes for odd *k* with $3 \le k \le n-2$.

4. LCD MDS Codes Derived from Cyclic Codes with Length $n|(q-1)$

In this part of our paper, we study construction of new LCD MDS codes that can be derived from cyclic codes with code length $n|(q-1)$. Firstly, we give some facts on elements of finite fields and *q*-cyclotomic coset of module *n*.

Fact (1) If *n* is even, then C_0 and C_s are symmetric, $C_i = \{i\}$ is asymmetric for $1 \le i \le s-1$, and $(C_i, C_{n-i}) = (C_i, C_{-i})$ is asymmetric cosets pair for $1 \le i \le s-1$.

(2) Let $T_i = \cup_{j=0}^{i}(C_{-j} \cup C_j)$ for $0 \le i \le s-1$, $T_{i-} = T_i \setminus C_{-i}, T_{i+} = T_i \cup C_i$. It is not difficult to check that $T_0 \subset T_1 \subset \cdots$ for $1 \le i \le s-1$, $T_{i-1} \subset T_{i-} \subset T_i$ and $T_{i-1} \subset T_{i+} \subset T_i$. Denote $Q_i = Z_n \setminus T_i, Q_{i-} = Z_n \setminus T_{i-}$, $Q_{i+} = Z_n \setminus T_{i+}$, then $Q_{i-} = Q_i \cup C_{-i}$ and $Q_{i+} = Q_i \cup C_i$, $Q_{i-1} \supseteq Q_{i-} \supseteq Q_i$ and $Q_{i-1} \supseteq Q_{i+} \supseteq Q_i$, $Q_{i-} \cup Q_{i+} = Q_{i-1}$, $Q_{i-} \cap Q_{i+} = Q_i$ for $1 \le i \le s-1$.

Lemma 4.1 *Let* $q \ge 4$, $n|(q-1)$ *and* $n \ge 3$. *If* $k = 2i+1$ *is odd and* $1 \le k \le n-1$, *then* C_i *is cyclic,* C_i *has a generator matrix* G_i such *that* $G_i G_i^T = diag\{1, N, \cdots$, *where*

$$N=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}.$$

Proof. *(1) Let* $T_i, T_{i-}, T_{i+}, Q_i, Q_{i-}, Q_{i+}$ *be defined as above. Denote the codes with defining sets* Q_i, Q_{i-}, Q_{i+} *as* C_i, C_{i-} *and* C_{i+}. *Then the following facts hold:*

$$|T_i|=2i+1,\ |T_{i-}|=|T_{i-}|=2i;\ \mathrm{C}_{i-1}=\mathrm{C}_{i-}\cap\mathrm{C}_{i+},\ \mathrm{C}_i=\mathrm{C}_{i-}+\mathrm{C}_{i+};\ \mathrm{C}_{i-}=[n,2i,n-2i+1]_q,$$
$$\mathrm{C}_{i+}=[n,2i,n-2i+1]_q,\ \mathrm{C}_i=[n,2i+1,n-2i]_q.$$

From $T_i=T_i^{-1}$ and $T_i^{\perp}=Z_n\square T_i^{-1}=Q_i$, one can derive C_i is an LCD MDS code for $0\le i\le s-1$. Since $(C_i,C_{n-i})=(C_i,C_{-i})$ is asymmetric cosets pair for $1\le i\le s-1$, we can derive $Q_{i-}^{\perp}=T_i\square C_i$, $Q_{i+}^{\perp}=T_i\square C_{-i}$. Thus, we have $Q_{i-}\cup Q_{i-}^{\perp}=Z_n\equiv C_i$, $Q_{i+}\cup Q_{i+}^{\perp}=Z_n\ \ C_{-i}$. Hence $\mathrm{C}_{i-}\cap\mathrm{C}_{i-}^{\perp}$ and $\mathrm{C}_{i+}\cap\mathrm{C}_{i+}^{\perp}$ are both codes with dimension one.

Let α_0 be a nonzero vector of C_0, from C_0 is an LCD code, we can choose α_0 such that $(\alpha_0,\alpha_0)=1$. Let α_{-1} be vector of $\mathrm{C}_{1-}\cap\mathrm{C}_{1-}^{\perp}$, α_1 be a nonzero vector of $\mathrm{C}_{1+}\cap\mathrm{C}_{1+}^{\perp}$. From $Q_0\supset Q_{1-}$ and $Q_0\supset Q_{1+}$, one can deduce $\mathrm{C}_0\subset\mathrm{C}_{1-}$ and $\mathrm{C}_0\subset\mathrm{C}_{1+}$, hence $(\alpha_0,\alpha_{-1})=0$ and $(\alpha_0,\alpha_1)=0$. It is not difficult to check $G_1=(\alpha_0^T,\alpha_{-1}^T,\alpha_1^T)^T$ is a generator matrix of C_1. From C_1 is an LCD code, one can deduce

$$G_1G_1^T=\begin{pmatrix}1 & 0 & 0\\ 0 & 0 & \alpha_{-1}\alpha_1^T\\ 0 & \alpha_1\alpha_{-1}^T & 0\end{pmatrix}$$

is invertible, hence one can choose α_1 such that $(\alpha_{-1},\alpha_1)=\alpha_{-1}\alpha_1^T=1$.

We can choose α_{-i} and α_i for $1\le i\le s-1$, such that α_{-i} is a nonzero vector of $\mathrm{C}_{i-}\cap\mathrm{C}_{i-}^{\perp}$, α_i is a nonzero vector of $\mathrm{C}_{i+}\cap\mathrm{C}_{i+}^{\perp}$, and $(\alpha_{-i},\alpha_i)=1$.

Using inductive method, we can show $\alpha_0,\alpha_{-1},\alpha_1,\cdots$ form a base of C_i, and the matrix

$$G_i=(\alpha_0^T,\alpha_{-1}^T,\alpha_1^T,\cdots)^T$$

satisfies $G_iG_i^T=diag\{1,N,\cdots\}$. Thus the lemma follows.

Corollary 4.2 Let $q\ge 4$, $n|(q-1)$ and $n\ge 3$.

(1) For even *n*, *k* is odd and $1\le k\le n-1$, then C is LCD and has $[n,k,n-k+1]_q$.

(2)For odd *n* and $1\le k\le n-1$, then C is LCD and has $[n,k,n-k+1]_q$.

Proof. (1) holds from Lemma 4.1.

(2) From Lemma 4.1, we know C is LCD and has $[n,k,n-k+1]_q$, $\mathrm{C}^{\perp}$ is an $[n,k,n-k+1]_q$ LCD cyclic MDS code with even dimension. Thus (2) follows.

Theorem 4.3 *Let* $q\ge 4$, $n|(q-1)$ *and* $n\ge 3$.

(1) If $N=n+1$, then there exists an $[N,k,N-k+1]_q$ LCD MDS code whenever $2\le k\le n-1$.

(2) Let $N=n+2$. If *n* is odd, then there exists an $[N,k,N-k+1]_q$ LCD MDS code whenever $2\le k\le n$. If *n* is even, there exists an $[N,k,N-k+1]_q$ LCD MDS code whenever *k*=2, or $3\le k\le n-1$ and *k* odd, or *k*=*n*.

Proof. Let C_i, C_{i-} and C_{i+} as be given in Lemma 4.1, and the generator matrices of these three codes are be G_i, G_{i-} and G_{i+}. According to Lemma 4.1, we know

$$G_i = \begin{pmatrix} \alpha_0 \\ \alpha_{-1} \\ \alpha_1 \\ \cdots \\ \alpha_{-i} \\ \alpha_i \end{pmatrix} \quad \begin{pmatrix} G_{i-1} \\ \\ \\ \\ \omega_i' \end{pmatrix} = \begin{pmatrix} G_{i-} \\ \alpha_i \end{pmatrix}.$$

From the proof of Lemma 4.1, one can deduce $wt(\alpha_0) = n, wt(\alpha_{-i}) = wt(\alpha_i) \geq n-2i+1$ for $1 \leq i \leq s-1$.

(1) For $1 \leq i \leq s-1$, let $\bar{G}_{i-}$ and $\bar{G}_i$ generate C_{i-} and C_i, where

$$\bar{G}_{i-} = \begin{pmatrix} G_{i-1} & 0 \\ \alpha_{-i} & 1 \end{pmatrix}, \bar{G}_i = \begin{pmatrix} G_{i-1} & 0 \\ \alpha_{-i} & 0 \\ \alpha_i & 1 \end{pmatrix}.$$

Then, we have

$$\bar{G}_{i-}\bar{G}_{i-}^T = \begin{pmatrix} G_{i-1}G_{i-1}^T & 0 \\ 0 & 1 \end{pmatrix}, \bar{G}_i\bar{G}_i^T = \begin{pmatrix} G_{i-1}G_{i-1}^T & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

Since C_{i-1} is LCD, we can deduce C_{i-} and C_i are all LCD codes. From

$$\mathrm{C}_{i-1} = [n, 2i-1, n-2i+2]_q,\ \mathrm{C}_{i-} = [n, 2i, n-2i+1]_q, \mathrm{C}_i = [n, 2i+1, n-2i]_q,$$

then

$$\bar{\mathrm{C}}_{i-} = [n+1, 2i, n-2i+2]_q \text{ and } \bar{\mathrm{C}}_i = [n+1, 2i+1, n-2i+1]_q.$$

These two codes are LCD. Hence, (1) holds.

(2) Now we will show (2) holds in two steps.

(2.1) Let $x \neq 0$ and $x^2 \neq 1$. *Construct*

$$G_i = \begin{pmatrix} G_{i-1} & 0 & 0 \\ \alpha_{-i} & 1 & 0 \\ \alpha_i & 0 & x \end{pmatrix},$$

for $1 \leq i \leq s-1$. It is *not* difficult to check G_i generates a code $\mathrm{C}_i = [n+2, 2i+1, n-2i+2]_q$ and this code is LCD and MDS. For odd *n*, then $\mathrm{C}_i^{\perp}$ is an LCD $[n+2, n-2i+1, 2i+2]_q$ code with even dimension.

(2.2) Denote the codes derived from defining sets $P_0 = Z_n \setminus C_0, P_1 = Z_n \setminus C_1$ as $\mathrm{D}_0, \mathrm{D}_1$, then D_0 is an $[n,1,n]$ LCD code and D_1 is a self-orthogonal $[n,1,n]$ BCH code. From $P_1^{\perp} \subset P_0$, one can deduce $\mathrm{D}_0 \subset \mathrm{D}_1^{\perp}$.

Let β_i be a nonzero vector of D_i for i=0,1 such that $(\beta_0, \beta_0) = \beta_0\beta_0^T = 1$. Then $< \beta_0, \beta_1 >$ generates an $[n,2,n-1]$ cyclic code with defining set $P = Z_n \setminus (C_0 \cup C_1)$. Let y be an non zero element in F_q such that $y^2 \neq -1$. Construct

$$\bar{G}' = \begin{pmatrix} \beta_0 & 0 \\ \beta_1 & 1 \end{pmatrix}, \bar{G}'' = \begin{pmatrix} \beta_0 & 0 & y \\ \beta_1 & 1 & 0 \end{pmatrix},$$

Then $\bar{G}'\bar{G}'^T$ and $\bar{G}''\bar{G}''^T$ are all invertible matrices, and LCD codes can be deduced by these matrices $\bar{G}'$ and $\bar{G}''$.

It is easy to check that $\bar{G}'$ generates an $[n+1,2,n]_q$ LCD MDS code and $\bar{G}''$ generates an $[n+2,2,n+1]_q$ LCD MDS code. Thus there is an $[n+1,n-1,3]_q$ and an $[n+2,n,3]_q$ LCD MDS code.

5. Conclusion

We first proposed the necessary condition that a cyclic code is LCD, at the same time it is a sufficient condition in this paper using terminology of cosets. We then studied LCD cyclic MDS codes with length n|(q+1) and n|(q-1). For the case n|(q+1), we discuss the construction of MDS cyclic codes for even n and odd n. For the case n|(q-1), we construct some new LCD MDS codes.

6. Acknowledgement

This work was financial supported by National NSFC under Grant Nos.11471011 and 11801564 and by Department of Basic Sciences Research Foundation with No. 2019201.

7. References

1. Peterson W W and Weldon E J. Error-correcting codes 2nd ed. The M. I. T. Press, Cambridge: Mass.-London, 1972.
2. Macwilliams F J and Sloane N J A. The Theory of Error-Correcting Codes. Amsterdam, the Netherlands: North-Holland, 1977.
3. Huffman W C and Pless V. Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge:2003
4. Carlet C and Guilley S. Complementary dual codes for counter-measures to side-channel attacks. Advance in Mathematics of Communication 2016;10:131-150.
5. Massey J L. Reversible codes. Information and Control 1964; 7: 369-380.
6. Massey J L. Linear codes with complementary duals. Discrete Math. 1992;106/107: 337-342.
7. Ding C, Li C and Li S. LCD cyclic codes over finite fields. IEEE Trans. Inform. Theory 2017;63:4344-4356.
8. Li C, Ding C and Li S. Parameters of two classes of LCD BCH codes. IEEE Trans. Inform. Theory 2015; 61:5322-5330.
9. Zhu S, Pang B, Sun Z. The reversible negacyclic codes over finite fields. arXiv:1610.08206v1.
10. Sari M and Koroglu M E. On MDS negacyclic LCD Codes. arXiv:1611.06371v1.
11. Jin L. Construction of MDS codes with complementary duals. IEEE Trans. Inform. Theory 2017;63:2843-2847.
12. Sloane N J A and Thompson J G. Cyclic self-dual codes. IEEE Trans. Inform. Theory 1983; 29: 364-366.
13. Yang X, Massey J L. The condition for a cyclic code to have a complementary dual. Discrete Math. 1994; 126:391-393.
14. Roth R. Introduction to Coding theory. Cambridge University Press, 2006.
15. Grassl M. Bounds on the minimum distance of linear codes. http://www.codetables.de. Accessed 29 Dec., 2018.