On the complementary dual code over $\mathbb{F}_2 + u\mathbb{F}_2$

B. Pashaei Rad
Department of Mathematics
Science and Research Branch
Islamic Azad University (IAU), Tehran
Iran
b.pashaeerad@gmail.com

H.R. Maimani*
Mathematics Section
Department of Basic Sciences
Shahid Rajaee Teacher Training University
P.O. Box 16785-163, Tehran
Iran
maimani@ipm.ir

A. Tehranian
Department of Mathematics
Science and Research Branch
Islamic Azad University (IAU)
Tehran
Iran
tehranian@srbiau.ac.ir

Abstract. A linear complementary dual code (an LCD code) is a linear code, whose satisfies in $C \cap C^{\perp} = \{0\}$. A binary LCD code play an important role in armoring implementation against side-channel attacks and fault injection attacks. All non-binary LCD codes with characteristic 2 can be transformed into binary LCD codes by expansion. In this paper, we consider the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$, which is a ring with characteristic 2 and obtain some properties of LCD codes over this ring. Also we characterize all LCD free cycle codes over R.

Keywords: cyclic code, LCD code, dual code.

1. Introduction

Throughout this paper $\mathbb{F}_2$ is the field of order 2 and $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$. The ring R is a ring of characteristic two and has four elements $\{0, 1, u, \overline{u} = u+1\}$ such that $u^2 = 0$. This ring is a local ring with a maximal ideal $\{0, u\}$, that shares some good properties of $\mathbb{Z}_4$. A *linear code* C of length n is defined to be an additive submodule of the R-module R^n. Codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$

∗. Corresponding author

where studied by Bachoc [1], Bonnecaze and Udaya [2], and Dougherty et al. [3].

The *Hamming weight* of a codeword $u = (u_1, u_2, \cdots, u_n)$, $w(u)$ is the number of nonzero entries in u. The *Hamming distance* of a linear code C is given by

$$d(C) = \min\{w(u) : u \in C, u \neq 0\}.$$

Suppose that C is a linear code of length n over $R = \mathbb{F}_2 + u\mathbb{F}_2$. we defined the *dual code* of C as

$$C^{\perp} = \{x' \in R^n; x'.x = 0, \forall x \in C\}.$$

With respect to inner product over R by $x.y = x_0y_0 + \cdots + x_{n-1}y_{n-1}$. A linear code with a *complementary-dual* (LCD code) was defined by Massy [5], is a linear code C satisfying $C \cap C^{\perp} = \{0\}$. In general for any linear code C over finite rings there is $(C^{\perp})^{\perp} \neq C$, but over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2$, we have $(C^{\perp})^{\perp} = C$ [4].

Suppose that $f(x)$ is a monic polynomial of degree m with $f(0) = c \neq 0$, then we called $f^*(x) = c^{-1}x^m f(x^{-1})$ the monic *reciprocal* polynomial of $f(x)$. A monic polynomial $f(x)$ is called *reciprocal polynomial*, if $f(x) = f^*(x)$.

Let C be a linear code of length n over the ring R. A $k \times n$ matrix, G, over the ring R is called a *generator matrix* for C if the rows of G generate C and there is no proper subset of the rows of G generates C

Theorem 1.1 ([9])**.** *Suppose that $R = \mathbb{F}_2 + u\mathbb{F}_2$. Any nonzero R-linear code C is permutation-equivalent to a R-linear code with a generator matrix of the form*

$$\begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix} \tag{1}$$

where I_{k_1},I_{k_2} denote the $k_1 \times k_1$ and $k_2 \times k_2$ are identity matrices, respectively A and D are F_2-matrices and B is a R-matrix. Then C is an abelian group of type $4^{k_1}2^{k_2}$, and C is a free R-module if and only if $k_2 = 0$.

The following theorem we stat a good results for finding the LCD code based on generating matrix.

Theorem 1.2 ([6])**.** *Let C be a free linear code over R with generator matrix G. Then C is an LCD code if and only if $k \times k$ matrix GG^T is invertible, where k is the number of rows of G.*

A linear code C over R is called *cyclic*, if it is invertible under a cyclic shift, i.e. , if $(x_0, x_1, \ldots, x_{n-1}, x_{n-2})$ is in C, then $(x_{n-1}, x_0, x_1, \ldots, x_{n-2}) \in C$. It is not difficult to see that every cyclic codes of length n over R are equivalent to an ideal of the ring $R_n = \frac{R[x]}{<x^n-1>}$.

Theorem 1.3 ([9])**.** *Let n be an odd positive integer, then every ideal of $R = \mathbb{F}_2 + u\mathbb{F}_2$ is principal.*

based on the Theorem 1.3, the factorization of $x^n - 1$ is important. This factorization over R_n is not unique , but if n is an odd positive integer we have the following theorem.

Theorem 1.4 ([2]). *Let n be an odd positive integer.*

If $x^n - 1 = f_1(x)f_2(x)\dots f_r(x)$, where f_i are basic irreducible and pairwise co-prime, then this factorization is unique. The factorization is obtained from factorization of the polynomial $x^n - 1$ over $\mathbb{F}_2$.

Theorem 1.5 ([2, 4]). *Suppose that C is a cyclic code of odd length n over R, then there are unique, monic polynomials $f(x), g(x), h(x)$ such that $C = (f(x)h(x), uf(x)g(x))$, where $x^n - 1 = f(x)g(x)h(x)$ and $|C| = 4^{deg(g(x))}2^{deg(h(x))}$.*

Corollary 1.1 ([4]). *Suppose $C = (f(x)h(x), uf(x)g(x))$ is a cyclic code of odd length n over R, where $f(x), g(x), h(x)$ are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$, then*

1. *If h(x)=1, then $C = (f(x)), |C| = 4^{n-deg(f(x))}$,*
2. *If g(x)=1, then $C = (uf(x)), |C| = 2^{n-deg(f(x))}$.*

Theorem 1.6 ([4]). *Suppose that $C = (f(x)h(x), uf(x)g(x))$ is a cyclic code of odd length n over R, where $f(x), g(x), h(x)$ are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$, and $|C| = 4^{deg(g(x))}2^{deg(h(x))}$. Then the dual of C is $C^\perp = (g^*(x)h^*(x), ug^*(x)f^*(x))$ and $|C^\perp| = 4^{deg(f(x))}2^{deg(h(x))}$, where $f^*(x), g^*(x)$ and $h^*(x)$ are reciprocal polynomials of $f(x), h(x)$ and $g(x)$, respectively.*

Corollary 1.2 ([4]). *Suppose that $C = (f(x)h(x), uf(x)g(x))$ is a cyclic code of odd length n over R, where $f(x), g(x), h(x)$ are monic polynomials such that $x^n - 1 = f(x)g(x)h(x)$ and $C^\perp = (g^*(x)h^*(x), ug^*(x)f^*(x))$, then*

1. *If $h(x) = 1$, then $C = (f(x))$ and $C^\perp = (g^*(x))$,*
2. *If $g(x) = 1$, then $C = (uf(x))$ and $C^\perp = (h^*(x), uf^*(x))$.*

In the rest of the paper we study the LCD free codes over $R = \mathbb{F}_2 + u\mathbb{F}_2$ with $u^2 = 0$.

2. Main results

In this section we study free linear code over R.

Theorem 2.1. *Suppose that C is a free linear code over $R = \mathbb{F}_2 + u\mathbb{F}_2$ with generator matrix*

$$G = \begin{bmatrix} I_{k_1} & A & B_1 + uB_2 & A & B_1 + uB_2. \end{bmatrix} \tag{2}$$

Hence C is an LCD code.

Proof. We have $GG^T = I_{k_1}$. Hence C is an LCD code by Theorem 1.2. □

Theorem 2.2. *Suppose that C is a free linear code over $R = \mathbb{F}_2 + u\mathbb{F}_2$ with generator matrix $G = \begin{bmatrix} I_{k_1} & \alpha A & uB_1 \end{bmatrix}$. If $\frac{1}{\alpha^2}$ is not an eigenvalue of matrix A, then C is an LCD code.*

Proof. If C is not an LCD code, then $GG^T = I_{k_1} + \alpha^2 AA^T$ is not invertible. Hence there exists a vector v, such that $(I_{k_1} + \alpha^2 AA^T)v = 0$ and therefore $\alpha^2 AA^T v = -I_{k_1} v = v$. So $(\frac{1}{\alpha^2} I_{k_1} + AA^T)v = 0$ and we conclude that $\frac{1}{\alpha^2}$ is an eigenvalue. □

Lemma 2.1. *Let $C = (f(x))$ be a cyclic free code, where $f(x) \mid x^n - 1$. Suppose that $g(x) = \frac{x^n - 1}{f(x)}$. Cyclic code C is an LCD code if and only if $g.c.d(f(x), g^*(x)) = 1$.*

Proof. Let $k(x) = l.c.m(f(x), g^*(x))$. It is not difficult to see that $C \cap C^\perp = (k(x))$. Hence $C \cap C^\perp = 0$ if and only if $deg(k(x)) = n$. Since $deg(f(x)) = k$ and $deg(g^*(x)) = deg(g(x)) = n - k$, then $deg(k(x)) = n$ if and only if $gcd(f(x), g^*(x)) = 1$. □

The following theorem state that which polynomials are good as a generator for cyclic code.

Theorem 2.3. *Let $C = (f(x))$ be a free cyclic code over $R = \mathbb{F}_2 + u\mathbb{F}$ of length n with generator polynomial $f(x)$. Then C is an LCD code if and only if $f(x)$ is a self reciprocal polynomial.*

Proof. Suppose that $C = (f(x))$ is an LCD code and $x^n - 1 = f(x)g(x)$. Then $gcd(f(x), g^*(x)) = 1$ by Lemma 2.1. We have $f^*(x).g^*(x) = x^n - 1 = f(x)g(x)$ and therefore $f(x) \mid f^*(x).g^*(x)$. Hence $f(x) \mid f^*(x)$. So there exists a polynomial $l(x) \in F_2[x]$ such that $f^*(x) = l(x).f(x)$. We know that $degf^*(x) = degf(x)$, and so $l(x)$ is a constant and this fact implies that $f^*(x) = f(x)$.

For converse, if $f^*(x) \neq f(x)$, then $g.c.d(f(x), g^*(x)) \neq 1$. Hence C is not LCD code by Lemma 2.1. □

Based on the above results, there is a good relation between the factorization of $x^n - 1$ and free cyclic code over the ring R. This construction used for cyclic LCD codes over fields [7]. Here we stat this construction.

Let n be an odd positive integer. The *cyclotomic coset* of 2 (or 2-cyclotomic coset) module n containing i is defined by

$$C_i = \{i2^j (\mathrm{mod}\, n) \in \mathbb{Z}_n : j = 0, 1, 2, \cdots\}.$$

It is not difficult to see that cyclotomic cosets is a partition of $\mathbb{Z}_n$. A subset $\{t_1, t_2, \cdots, t_k\}$ is called a *complete set of representatives* of cyclotomic cosets of 2 module n if $C_{t_i} \cap C_{t_j} = \emptyset$ for any $1 \leq i < j \leq k$ and $\bigcup_{l=1}^{k} C_l = \mathbb{Z}_n$.

If α is a primitive element of field $\mathbb{F}_{2^n}$, then $\prod_{j \in C_i}(x - \alpha^j)$ is the minimal polynomial of α^j over $\mathbb{F}_2$. Now we have the following theorem.

Theorem 2.4. *Let n be an odd integer. Suppose that m is an positive integer such that $n \mid 2^m - 1$. Let α be a primitive element of $\mathbb{F}_{2^m}$ and let $M^{(j)}(x)$ be the minimal polynomial of α^j with respect to $\mathbb{F}_q$ and $\{t_1, t_2, \cdots, t_k\}$ is a complete set of representatives of cyclotomic cosets of 2 module n. Then*

$$x^n - 1 = \prod_{i=1}^{k} M^{(\frac{(2^n-1)t_i}{n})}(x).$$

A 2-cyclotomic coset, C_i, is called symmetric if $-i \in C_i$ and is called anti-symmetric, otherwise. Suppose that $\{t_1, t_2, \cdots, t_k\}$ is a complete set of representatives of cyclotomic cosets of 2 module n. Also suppose that for $1 \leq i \leq s$, 2-cyclotomic cosets C_i's are symmetric and for for $s+1 \leq i \leq s+l$, 2-cyclotomic cosets C_i's are anti-symmetric, where $s + 2l = k$. Hence we can decompose the polynomial $x^n - 1$ as follows

$$x^n - 1 = \prod_{i=1}^{s} M^{(\frac{(2^n-1)t_i}{n})}(x) \prod_{i=s+1}^{s+l} M^{(\frac{(2^n-1)t_i}{n})}(x) M^{(-\frac{(2^n-1)t_i}{n})}(x).$$

The following theorem give a good characterization of LCD code over $\mathbb{F}_2 + u\mathbb{F}_2$.

Theorem 2.5. *Let n be an odd prime and C be a cyclic free code over $\mathbb{F}_2 + u\mathbb{F}_2$ with generator $g(x)$. Hence C ia an LCD code if and only if*

$$g(x) = \prod_{i=1}^{s} (M^{(\frac{(2^n-1)t_i}{n})}(x))^{a_i} \prod_{i=s+1}^{s+l} (M^{(\frac{(2^n-1)t_i}{n})}(x) M^{(-\frac{(2^n-1)t_i}{n})}(x))^{b_i}.$$

where $a_i, b_i \in \{0, 1\}$

Proof. By Theorem 2.3, the cyclic free code C with generator $f(x)$ is an LCD code if and only if α is a root of $f(x)$ implies that α^{-1} is a root of $f(x)$. □

Theorem 2.6. *If $7|n$, then there exists an $[n, n-6, d]$ LCD cyclic code over the ring R with $d \leq 7$.*

Proof. Let $a = \frac{n}{7}$. We have $C_a = \{\frac{n}{7}, \frac{2n}{7}, \frac{4n}{7}\}$. Hence C_a is an anti-symmetric coset. Now consider the cyclic code, C, with the generator matrix $g(x)$, where

$$g(x) = M_a M_{-a}.$$

Since $deg(g(x)) = 6$ and weight of $g(x))$ is at most 7, the result is obtained. □

References

[1] C. Bachoc, *Application of coding theory to the construction of modular lattices*, J. Combin. Theory Ser. A, 78 (1997), 92-119.

[2] A. Bonnecaze and U. Parampalli, *Cyclic codes and self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45 (1999), 1250-1255.

[3] S.T. Dougherty, Gaborit, P. Harada and M. Sole *Type II codes over* $\mathbb{F}_2+u\mathbb{F}_2$, IEEE Trans. Inform. Theory, 45 (1999), 32-45.

[4] S.T. Dougherty, J.L. Kim, H. Kulosman and H. Liu, *Self-dual codes over commutative frobenius ring*, Finite Fields Appl., 16 (2010), 14-26.

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

[6] X. Liu, H. Liu, *LCD codes over finite chain ring*, Finite Fields Appl., 34 (2015), 1-19.

[7] Y. Rao, R. Li, L. Lv, G. Chen and F. Zuo, *On binary LCD cyclic codes*, Procedia Computer Science, 107 (2017), 778-783.

[8] J.H. Van Lint, *Introduction to coding theory*, Springer, NewYork, 1982.

[9] Z. Xian Wan, *Quaternary codes*, Word Scientific Publishing Co. Pte. Ltd (series on applied mathematics; v.8), 1997.

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

Accepted: 23.03.2019