On LCD codes over $Z_4$

Ridhima Thakral$^1$, Sucheta Dutt$^{2*}$ and Ranjeet Sehmi$^3$

$^{1,2,3}$ Department of Applied Sciences, Punjab Engineering College (Deemed to be University), Chandigarh, India
E-mail: suchetappec@yahoo.co.in

Abstract. Linear complementary dual (LCD) codes are being utilized to protect cryptographic implementations from side-channel and fault attacks. In this work, LCD codes over the ring $Z_4$ are examined. It is observed that an LCD cyclic code over $Z_4$ of odd length is always reversible. However, the converse of this result does not hold. A suitable example to validate this statement is presented. Further, a necessary and sufficient condition for a reversible cyclic code of odd length to be an LCD code is obtained. Finally, it is found that among cyclic codes of length $2^k$, no non-trivial LCD code exists.

1. Introduction
Cryptographic algorithms in sensitive devices are prone to side-channel and fault attacks. These attacks try to extract the information being processed when a cryptographic algorithm runs over a device. To overcome this problem, LCD codes were proposed by Massey in 1992 [8] and it was observed that LCD codes are an optimal solution for the two-user binary additive channel. The fact that LCD codes can be utilized as an offset to side-channel attacks was shown by Carlet and Guilley [1] and various structures of LCD codes over a Galois field, GF($q$), were presented. Since then it has become a topic of keen interest amongst researchers which has led to various constructions and characterizations of LCD codes over a field. It was proved by Yang and Massey [3] that a cyclic code of length $m$ over a field of characteristic $p$, where $(m, p) = 1$, is an LCD code if and only if it is reversible.

The analysis of LCD codes over a ring is a recent phenomenon in comparison to its study over a field. It was established by Gannon and Kulosman [2] that over the ring $Z_4$, a cyclic code of odd length is an LCD code if and only if it is generated by a self reciprocal monic polynomial which divides $x^m - 1$ in $Z_4[x]$. It was shown by Kaur [6] that a cyclic code over a ring is reversible if and only if the set of reciprocal polynomials of its generators also generates the code. It was observed by the same author that a cyclic code of length 4 over $Z_4$ is reversible.

Throughout this paper, LCD cyclic codes are studied over the ring $Z_4$. It is noticed that an LCD cyclic code of odd length is always reversible. But the converse of this result is not true. A suitable example is provided to validate this statement. A necessary and sufficient condition for a reversible cyclic code of odd length to be an LCD code is obtained. Moreover, it is observed that no cyclic code of length 4 is an LCD code. Further, it is proved that for a non-trivial cyclic code of length $2^k$, the intersection of the code with its dual is non-trivial. This establishes that among cyclic codes of length $2^k$, there does not exist any non-trivial LCD code.
2. Preliminaries

To begin with, we introduce some notations and definitions required to proceed further.

A code of length \( m \) over a ring \( R \) is linear if it forms a sub-module of \( R^m \) over \( R \). A linear code \( C \) of length \( m \) is cyclic if for every \( (s_0, s_1, \ldots, s_{m-1}) \) in \( C \), \( (s_{m-1}, s_0, \ldots, s_{m-2}) \) also belongs to \( C \). The dual of a linear code \( C \) over \( R \) is the set \( C^\perp = \{ s \in R^m : s \cdot t = 0 \text{ for every } t \in C \} \).

A linear code whose intersection with its dual is trivial is said to be an LCD code. A code \( C \) is said to be reversible if its dual is trivial. A code is said to be reversible if it is invariant under reversing the order of the coordinates of each of its codewords.

Vectors of \( R^m \) can be expressed as polynomials in \( R_m = R[x]/\langle x^m - 1 \rangle \) by the mapping \( \phi : R_m \rightarrow R_m \) defined by \( \phi(s_0, s_1, \ldots, s_{m-1}) = s_0 + s_1x + \ldots + s_{m-1}x^{m-1} \). Under the mapping \( \phi \), a cyclic code \( C \subseteq R^m \) is associated with an ideal \( I \) of \( R_m \). In rest of the paper, we shall refer to a cyclic code over a ring \( R \) and its associated ideal in \( R_m \) interchangeably.

The reciprocal polynomial of a polynomial \( v(x) \) of degree \( k \) is given by \( v^*(x) = x^k v(\frac{1}{x}) \). If \( v^*(x) \) is equal to \( v(x) \), then \( v(x) \) is designated as a self reciprocal polynomial. For an ideal \( I \) in \( R_m \), the set \( I^* = \{ v^*(x) : v(x) \in I \} \) is also an ideal in \( R_m \). For any two polynomials \( s(x) = s_0 + s_1x + \ldots + s_{m-1}x^{m-1} \) and \( t(x) = t_0 + t_1x + \ldots + t_{m-1}x^{m-1} \) in \( R_m \), \( s(x)t(x) = 0 \) if and only if \( f_0, f_1, \ldots, f_{m-1} \) is orthogonal to the vector associated with the reciprocal polynomial of \( t(x) \) under \( \phi \), i.e. \( (t_{m-1}, \ldots, t_0) \) and all its cyclic shifts. The ideal \( Ann(I) = \{ s(x) : s(x)t(x) = 0 \text{ for every } t(x) \in I \} \) is called as the annihilator of an ideal \( I \).

3. LCD codes over \( Z_4 \)

The structure of a cyclic code of odd length over \( Z_4 \) has been given by Abualrub and Siap [7]. They have also given a necessary and sufficient condition for a cyclic code of odd length to be reversible. We reproduce their results as Lemma 3.1 and Lemma 3.2 below for ready reference. Further, we reproduce below the results of Gannon and Kulomsan [2] and Kaur [6] as Lemma 3.3 and Lemma 3.4 respectively.

**Lemma 3.1** [7, Lemma 4]: If \( C = < f_1, f_2 > \) is a cyclic code over \( Z_4 \) of odd length \( m \). Then \( C = < f_1 + f_2 > \), where \( f_1 \) and \( f_2 \) are binary monic polynomials with \( f_2(x)|f_1(x)|(x^m - 1) \mod 4 \).

**Lemma 3.2** [7, Theorem 2]: Let \( C = < f_1, f_2 > = < f_1 + f_2 > \) be a cyclic code over \( Z_4 \) of odd length. Then \( C \) is reversible if and only if \( f_1 \) and \( f_2 \) are both self reciprocal monic polynomials.

**Lemma 3.3** [2, Theorem 2.1]: A cyclic code over \( Z_4 \) of odd length \( m \) is an LCD code if and only if it is generated by a self reciprocal monic polynomial which divides \( x^m - 1 \) in \( Z_4[x] \).

**Lemma 3.4** [6]: A cyclic code over a ring \( R \) with generators \( f_j(x), 1 \leq j \leq k \) is reversible if and only if the set of reciprocal polynomials \( \{ f_j^*(x) : 1 \leq j \leq k \} \) also generates the code.

The following theorem is an immediate implication of Lemma 3.3 and Lemma 3.4.

**Theorem 3.1**: An LCD cyclic code of odd length over \( Z_4 \) is reversible.

The converse of Theorem 3.1 is not true as is clear from the example given below.

**Example 3.1**: Consider the cyclic code \( C = < f_1, f_2 > = < x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, 2 > \) of length 7 over \( Z_4 \). It can be easily seen that \( f_1(x) \) and \( f_2(x) \) are both self reciprocal monomials. It follows from Lemma 3.2 that \( C \) is reversible. By Lemma 3.1, \( C \) can also be written as \( < x^6 + x^5 + x^4 + x^3 + x^2 + x + 3 > = < h(x) > \), say, then \( h^*(x) = 3x^6 + x^5 + x^4 + x^3 + x^2 + x + 1. \)
Clearly $h(x) \neq h^*(x)$. It follows from Lemma 3.3 that $C$ is not an LCD code.

Theorem 3.2 given below provides a necessary and sufficient condition for a reversible cyclic code of odd length over $Z_4$ to be an LCD code.

**Theorem 3.2**: A reversible cyclic code of odd length $m$ over $Z_4$ is an LCD code if and only if it is generated by a binary monic polynomial which divides $x^m - 1$ in $Z_4[x]$.

**Proof**: Consider a cyclic code $C$ of odd length $m$ over $Z_4$. By Lemma 3.1, $C = \langle f_1, 2f_2 \rangle = \langle f_1 + 2f_2 \rangle$, where $f_1$ and $f_2$ are two binary monic polynomials in $Z_4[x]$ with $f_2(x)|f_1(x)|(x^m - 1)$. Suppose $C$ is reversible. Then by Lemma 3.2, $f_1$ and $f_2$ are both self reciprocal polynomials, i.e. $f_1 = f_1^*$ and $f_2 = f_2^*$. It is known that $(f_1 + f_2)^* = f_1^* + x^{deg f_1 - deg f_2} f_2^*$ for any two polynomials $f_1$ and $f_2$ over a commutative ring $R$. Suppose $C$ is an LCD code. Lemma 3.3 implies that $f_1 + 2f_2$ is a self reciprocal polynomial. Therefore, we have

$$f_1 + 2f_2 = (f_1 + 2f_2)^* = f_1^* + x^{deg f_1 - deg f_2} f_2^*.$$

It follows that $deg f_1 = deg f_2$. Since $f_2(x)|f_1(x)$, we must have $f_1(x)$ equal to $f_2(x)$. Thus, $C = \langle f_1(x), 2f_1(x) \rangle = \langle f_1(x) \rangle$.

Conversely, suppose $C = \langle f(x) \rangle$, where $f(x)$ is a binary monic polynomial which divides $x^m - 1$ in $Z_4[x]$. It follows from Lemma 3.2 that the polynomial $f(x)$ is self reciprocal which together with Lemma 3.3 further gives that $C$ is an LCD code.

The following examples 3.2 and 3.3 illustrate Theorem 3.2.

**Example 3.2**: Consider the cyclic code $C = \langle f(x) \rangle = \langle x^4 + x^3 + x^2 + x + 1 \rangle$ of length 5 over $Z_4$. It can be easily seen that $f(x)$ is a self reciprocal polynomial. Therefore, by Lemma 3.2, $C$ is reversible. Also, $C$ is an LCD code by Lemma 3.3. The generator $f(x)$ of $C$ is clearly a binary monic polynomial which divides $x^5 - 1$ in $Z_4[x]$. This is an example showing that the condition in Theorem 3.2 is sufficient.

**Example 3.3**: Consider the cyclic code $D = \langle f_1, 2f_2 \rangle = \langle x^4 + x^3 + x^2 + x + 1, 2 \rangle$ of length 5 over $Z_4$. It is easy to see that $f_1(x)$ and $f_2(x)$ are both self reciprocal polynomials. It follows from Lemma 3.2 that $D$ is reversible. By Lemma 3.1, $D$ can also be written as $\langle x^4 + x^3 + x^2 + x + 3 \rangle = \langle f(x) \rangle$, say. Since $f(x) \neq f^*(x)$, $f(x)$ is not a self reciprocal polynomial. Therefore, by Lemma 3.3, $D$ is not an LCD code. Also the generator $f(x)$ of $D$ is clearly a monic, non-binary polynomial which does not divide $x^5 - 1$ in $Z_4[x]$. This is an example showing that the condition in Theorem 3.2 is necessary.

We recall below the structure of a cyclic code of length $2^k$ over $Z_4$ in terms of its distinguished set of generators given by Abualrub and Oehmke as follows.

**Lemma 3.5** [5]: Let $C$ be a cyclic code of length $m = 2^k$ over $Z_4$. Then $C$ has one of the following forms:

(i) $C = \langle (x + 1)^a \rangle$;
(ii) $C = \langle (x + 1)^a + 2(x + 1)^b h(x) \rangle$;
(iii) $C = \langle 2(x + 1)^i \rangle$;
(iv) $C = \langle (x + 1)^a + 2(x + 1)^b h(x), 2(x + 1)^i \rangle$,

where $a < m$, $h(x)$ is a unit in $R_2$ of degree atmost $i - b - 1$ and $i$ is the smallest integer such that $2(x + 1)^i$ belongs to $C$. 

3
Further, the following lemmas 3.6-3.9 give the structure of the dual of a cyclic code of length $2^k$ over $Z_4$.

**Lemma 3.6** [5, Theorem 23]: Let $C = \langle (x + 1)^a \rangle$ be a cyclic code of length $m = 2^k$ over $Z_4$, where $a < m$. Then $C^\perp$ is as given below:

(i) If $a > m/2$, then $C^\perp = \langle (x + 1)^{m/2} + 2(x + 1)^{m-a} \rangle$;

(ii) If $a = m/2$, then $C^\perp = \langle (x + 1)^{m/2} + 2 \rangle$;

(iii) If $a < m/2$, then $C^\perp = \langle (x + 1)^{m-a} + 2(x + 1)^{m/2-a} \rangle$.

**Lemma 3.7** [5, Theorem 24]: Let $C = \langle (x + 1)^a + 2(x + 1)^b h(x) \rangle$ be a cyclic code of length $m = 2^k$ over $Z_4$, where $a < m$ and $h(x)$ is a unit in $R_2$ of degree at most $i - b - 1$. Then $C^\perp$ is as given below:

(i) If $a > b + m/2$, then $C^\perp = \langle l^*(x), 2(x + 1)^{m-a} \rangle$, where $l(x) = (x + 1)^{a-b} + 2(x + 1)^{a-b-m/2} + 2h(x)$ and $l^*(x) = (x + 1)^{a-b} + 2(x + 1)^{a-b-m/2} + 2x^{a-b}h(\frac{1}{2})$;

(ii) If $a = b + m/2$, then $C^\perp = \langle l^*(x), 2(x + 1)^{m-a} \rangle$, where $l(x) = (x + 1)^{m/2} + 2h(x) + 2$ and $l^*(x) = (x + 1)^{m/2} + 2x^{m/2}h(\frac{1}{2})$;

(iii) If $m/2 < a < b + m/2$, then $C^\perp = \langle l^*(x), 2(x + 1)^{m-a} \rangle$, where $l(x) = (x + 1)^{m/2} + 2(x + 1)^{m/2+b-a}h(x) + 2$ and $l^*(x) = (x + 1)^{m/2} + 2x^{m/2}h(\frac{1}{2})$;

(iv) If $a \leq m/2$, then $C^\perp = \langle l^*(x) \rangle$, where $l(x) = (x+1)^{m-a} + 2(x+1)^{m/2-2a}h(x)$ and $l^*(x) = (x + 1)^{m-a} + 2(x + 1)^{m/2-2a} + 2x^{a-b}h(x) + 2x^{a-b}h(\frac{1}{2})$.

**Lemma 3.8** [5, Theorem 25]: Let $C = \langle 2(x + 1)^i \rangle$, where $i$ is the smallest integer such that $2(x + 1)^i \in C$, be a cyclic code over $Z_4$ of length $m = 2^k$. Then $C^\perp = \langle (x + 1)^{m-i} \rangle$.

**Lemma 3.9** [5, Theorem 26]: Let $C = \langle v(x), 2(x + 1)^i \rangle$, where $v(x) = (x + 1)^a + 2(x + 1)^b h(x)$, be a cyclic code over $Z_4$ of length $m = 2^k$. Then $C^\perp = \text{Ann}(\langle v(x) \rangle)^\perp \cap \text{Ann}(\langle 2(x + 1)^i \rangle)^\perp$.

Following table lists all non-trivial cyclic codes of length 4 over $Z_4$ along with their dual codes which are computed using lemmas 3.5-3.9. A non-zero element has been identified in the third column of the table which belongs to the code as well as its dual. Therefore, it is concluded that none of the non-trivial cyclic codes of length 4 over $Z_4$ is an LCD code.

| $C$                     | $C^\perp$                          | Non-zero element in $C \cap C^\perp$ |
|-------------------------|------------------------------------|--------------------------------------|
| $< 2 >$                 | $< 2 >$                            | $2$                                  |
| $< x + 3 >$             | $< x^3 + x^2 + x + 1 >$            | $2(x + 1)^3$                         |
| $< x + 1 >$             | $< x^3 + 3x^2 + x + 3 >$           | $2(x + 1)^3$                         |
| $< x^2 + 3 >$           | $< x^2 + 1 >$                      | $2(x + 1)^2$                         |
| $< x^2 + 2x + 3 >$      | $< x^2 + 2x + 1 >$                 | $2(x + 1)^2$                         |
| $< 2(x^3 + x^2 + x + 1) >$ | $< (x + 1), 2 >$                 | $2(x + 1)^3$                         |
| $< 2(x^3 + 1) >$        | $< (x^3 + 1), 2 >$                 | $2(x^2 + 1)$                         |
| $< 2(x + 1) >$          | $< (x^3 + x^2 + x + 1), 2 >$      | $2(x + 1)^3$                         |
| $< x^2 + 3, (x + 1) >$  | $< x^3 + x^2 + x + 1, 2(x^2 + 1) >$ | $2(x + 1)^3$                         |
| $< x^2 + 1, 2(x + 1) >$ | $< x^3 + x^2 + 3x + 3, 2(x^2 + 1) >$ | $2(x^2 + 1)$                         |
| $< x^3 + x^2 + x + 1, 2(x + 1) >$ | $< x^3 + x^2 + x + 3, 2(x + 1) >$ | $2(x + 1)$                           |
We now prove the main result of the paper.

**Theorem 3.3:** Let $C$ be a non-trivial cyclic code of length $m = 2^k$ over $Z_4$. Then $C$ is not an LCD code.

**Proof:** Let $C$ be a non-trivial cyclic code of length $m = 2^k$ over $Z_4$. Then by Lemma 3.5, $C$ has one of the following forms:

(i) $C = < (x + 1)^a >$;
(ii) $C = < (x + 1)^a + 2(x+1)b h(x) >$;
(iii) $C = < 2(x+1)^i >$;
(iv) $C = < (x + 1)^a + 2(x+1)b h(x), 2(x+1)^i >$,

where $a < m$, $h(x)$ is a unit in $R_2$ of degree at most $i - b - 1$ and $i$ is the smallest integer such that $2(x+1)^i$ belongs to $C$.

Case 1: $C = < (x + 1)^a >$, $a < m$.

(i) If $a \geq m/2$, then by Lemma 3.6, $C^\perp = < (x+1)^{m/2} + 2(x+1)^{m-a} >$. Clearly, $2(x+1)^a \in C$ and $2(x+1)^{m-a} \in C^\perp$. As $2a-m \geq 0$ and $C^\perp$ is an ideal, $2(x+1)^a = 2(x+1)^{m-a}(x+1)^{2a-m} \in C^\perp$ and we have $C \cap C^\perp \neq \{0\}$.

(ii) If $a < m/2$, then by Lemma 3.6, $C^\perp = < (x+1)^{m-a} + 2(x+1)^{m/2-a} >$. Since $m - 2a > 0$ and $(x+1)^a \in C$, $2(x+1)^a(x+1)^{m-2a} = 2(x+1)^{m-a} \in C$. Also $2(x+1)^{m-a} \in C^\perp$, therefore $C \cap C^\perp \neq \{0\}$.

Case 2: $C = < (x + 1)^a + 2(x+1)b h(x) >$, where $a < m$ and $h(x)$ is a unit in $R_2$ of degree at most $i - b - 1$.

(i) If $a > m/2$, then by Lemma 3.7, $C^\perp = < \psi(x), 2(x+1)^{m-a} >$, where

$$\psi(x) = \begin{cases} (x+1)^{m/2} + 2x^{a-b}(x+1)^{m/2+b-a} h(\frac{1}{x}) + 2, & \text{if } m/2 < a < b + m/2. \\ (x+1)^{a-b} + 2(x+1)^{a-b-m/2} + 2x^{a-b} h(\frac{1}{x}), & \text{if } a \geq b + m/2. \end{cases}$$

It is convenient to see that $2(x+1)^a \in C \cap C^\perp$.

(ii) If $a \leq m/2$, then by Lemma 3.7, $C^\perp = < (x+1)^{m-a} + 2(x+1)^{m/2-a} + 2x^{a-b}(x+1)^{m+b-2a} h(\frac{1}{x}) >$. Using the same argument as in Case 1(ii), we find that $2(x+1)^{m-a} \in C \cap C^\perp$.

Case 3: $C = < 2(x+1)^i >$, where $i$ is the smallest integer such that $2(x+1)^i \in C$.

By Lemma 3.8, $C^\perp = < (x+1)^{m-i}, 2 >$. In this case, $2(x+1)^i \in C^\perp$ and hence $C \cap C^\perp \neq \{0\}$.

Case 4: $C = < v(x), 2(x+1)^i >$, where $v(x) = (x+1)^a + 2(x+1)^b h(x)$.

By Lemma 3.9, $C^\perp = Ann(< v(x) >)^* \cap Ann(< 2(x+1)^i >)^*$. In this case, the result follows directly from the previous cases.

Combining cases 1 to 4 above, we obtain that for any non-trivial cyclic code of length $2^k$ over $Z_4$, the intersection of $C$ and $C^\perp$ always contains a non-zero element. It follows that $C$ is not an LCD code. \[\square\]
4. Conclusion
In this paper it is shown that an LCD cyclic code over $\mathbb{Z}_4$ of odd length is reversible but the converse of this result does not hold. A counter example has been given to support this statement. Further, it is proved that a reversible cyclic code of odd length $m$ is an LCD code if and only if it is generated by a binary monic polynomial which divides $x^m - 1$ in $\mathbb{Z}_4[x]$. Next, it is demonstrated that none of the non-trivial cyclic codes of length 4 over $\mathbb{Z}_4$ is an LCD code. Finally, it is proved that no non-trivial cyclic code of length $2^k$ over $\mathbb{Z}_4$ is an LCD code.

References
[1] Carlet C and Guilley S 2016 Complementary dual codes for counter measures to side channel attacks AIMS’ Journals 10 131-150
[2] Kulosman H and Gannon S 2019 The condition for a cyclic code over $\mathbb{Z}_4$ of odd length to have a complementary dual Preprint 1905.12309v1[math.RA]
[3] Yang X and Massey J L 1994 The condition for a cyclic code to have a complementary dual Discrete Mathematics 126 391-393
[4] Abualrub T and Oehmke R 2003 Cyclic codes of length $2^e$ over $\mathbb{Z}_4$ Discrete Applied Mathematics 128 3-9
[5] Abualrub T and Oehmke R 2003 On the generators of $\mathbb{Z}_4$ cyclic codes of length $2^e$ IEEE Trans. of Inf. Theory 49 2126-2123
[6] Kaur J 2017 Cyclic codes over galois rings Ph.D Thesis PEC University of Technology
[7] Abualrub T and Siap I 2007 Reversible cyclic codes over $\mathbb{Z}_4$ Australasian Journal of Combinatorics 38 195-205
[8] Massey J L 1992 Linear codes with complementary duals Discrete Mathematics 106-107 337-342