Proceedings of the 9th WSEAS International Conference on Applied Mathematics, Istanbul, Turkey, May 27-29, 2006 (pp441-446)

Reversible Quaternary Cyclic Codes

Taher Abualrub
Department of Mathematics, American University of Sharjah, Sharjah-UAE
Irfan Siap
Adıyaman Education Faculty, Gaziantep University, Adıyaman, Turkey.

Abstract

In this paper we study reversible cyclic codes of any length n over the ring Z_4. First we find a set of generators for cyclic codes over Z_4 with no restrictions on the length n. We then classify reversible cyclic codes with respect to their generators. Examples of reversible cyclic codes of lengths 8 and 9 with their minimum Hamming distance will be studied as well.

Key-Words: The ring Z_4, Linear Codes, Cyclic Codes, Quaternary Codes, Reversible Cyclic Codes

1 Introduction

Consider the ring $Z_4 = \{0, 1, 2, 3\}$. A linear code C of length n over Z_4 is defined to be an additive submodule of the Z_4-module Z_4^n. A cyclic code of length n over Z_4 is defined to be a submodule of Z_4^n that is invariant with respect to the shift operator that maps the element $(c_0, \ldots, c_{n-1})$ of Z_4^n to the element $(c_{n-1}, c_0, \ldots, c_{n-2})$. For each element $(c_0, \ldots, c_{n-1})$ of Z_4^n we associate a polynomial $c_0 + c_1x + \ldots c_{n-1}x^{n-1}$ in the ring $R_n = Z_4[x]/(x^n - 1)$. In this case cyclic codes are defined to be ideals in R_n. A code C is called reversible if it is invariant under a reversal of the digits in all its codewords. i.e., a cyclic code C is called reversible if for each codeword $u = (u_0, u_1, \cdots, u_{n-1}) \in C$ then the reverse of u, $u^r = (u_{n-1}, u_{n-2}, \cdots, u_0)$ is also in C. The Hamming distance between codewords u and v, denoted by $H(u, v)$, is simply the number of coordinates in which these two codewords differ. The Hamming weight of any codeword $u = (u_0, u_1, \cdots, u_{n-1})$, $w(u)$ is the number of nonzero entries in u. The Hamming distance of any linear code C is given by

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

For each polynomial $p(x) = p_0 + p_1x + \cdots + p_rx^r$ with $p_r \neq 0$, we define the reciprocal of $p(x)$ to be the polynomial $p^*(x) = x^r p(1/x) = p_r + p_{r-1}x^{r-1} + \cdots + p_0x^r$. Note that deg $p^*(x) \leq$ deg $p(x)$ and if $p_0 \neq 0$, then $p(x)$ and $p^*(x)$ always have the same degree. $p(x)$ is called self-reciprocal if and only if $p(x) = p^*(x)$.

Reversible cyclic codes over finite fields were studied first by [8]. it was shown that $C = (f(x))$ is reversible if and only if $f(x)$ is a self reciprocal polynomial.

In this paper we study reversible cyclic codes over Z_4 of any length n. Such codes have applications in the subject of DNA computing. In particular this class of codes is important because it satisfies the following constraints.

- The Hamming constraint: For any two different codewords $u,\ v \in C$, $H(u,\ v) \geq d$.
- The reverse-constraint: For any two codewords $u, v \in C$, $H(u, v^r) \geq d$.

These two constraints will make non-desirable hybridization between a codeword and another codeword less likely to happen.

Also, this class of codes have some applications in constructing certain data storage and retrieval systems. We note that we put no restrictions on the length n.

The rest of the paper is organized as follows. In section 2, we study cyclic codes of length n over Z_4 and we find a unique set of generators for them. In section 3, we study reversible cyclic codes over Z_4 and we put a set of constraints on their generator polynomials. Section 4 includes a list of all reversible cyclic codes of lengths 8 and 9. Section 5 Concludes the paper

2 Generators for Cyclic Codes

A cyclic code C in $R_n = Z_4[x]/(x^n - 1)$ is an ideal in R_n. Our goal in this section is to find a set of generators for C for any length n. Most previous work on cyclic codes in R_n was restricted to the case where n is odd [3, 6, 9]. Little work was done on cyclic codes in R_n for even length [1,2, 10]. [1] has studied cyclic codes of length $n = 2^e$. It was shown that the ring R_n is not a principal ideal ring. [2] has studied the case where $n = 2e$ and $\gcd(e, n) = 1$ and has also shown that R_n is not a principal ideal ring. Our approach in studying these codes will be general and doesn't depend on the length n.

Let C be a cyclic code in R_n. Define $\varphi : C \to Z_2[x]/(x^n - 1)$ by $\varphi(x) = x \mod 2$.

φ is a ring homomorphism with $\ker\varphi = \{2r(x) : r(x)$ is a binary polynomial in C.$\}$. Let $J = \{r(x) : 2r(x) \in \ker\varphi\}$. It is easy to check that J is an ideal in $Z_2[x]/(x^n - 1)$ and hence a cyclic code in $Z_2[x]/(x^n - 1)$. So $J = (a(x))$ where $a(x) \mid (x^n - 1)$. This implies that $\ker\varphi = (2a(x))$ with $a(x) | (x^n - 1) \mod 2$. The image of φ is also an ideal and hence a binary cyclic code that has a generator $g(x)$ with $g(x) \mid (x^n - 1) \mod 2$. This implies that $C = (g(x) + 2p(x),\ 2a(x))$ where $p(x)$ is a binary polynomial.

Note that with this construction $g(x)$, and $a(x)$ are binary polynomials divisors of $(x^n - 1) \mod 2$ rather than $\mod 4$.

Claim 1 *We may assume* $\deg a(x) > \deg p(x)$, *and* $a(x) \mid g(x) \mod 2$.

Proof. Since

$$\begin{aligned} C &= (g(x) + 2p(x),\ 2a(x)) \\ &= \left(g(x) + 2\left[p(x) + x^i a(x)\right],\ 2a(x)\right), \end{aligned}$$

then we may assume $\deg a(x) > \deg(p(x)$. Since

$$2g(x) \in \ker\varphi = (2a(x)),$$

then $a(x) \mid g(x)$. If $g(x) = a(x)$, then $C = (g(x) + 2p(x))$. ∎

Claim 2 $a(x)|p(x)\left(\dfrac{x^n - 1}{g(x)}\right) \mod 2.$

Proof.

$$\begin{aligned} \varphi\left(\frac{x^n - 1}{g}[g + 2p]\right) &= \varphi\left(2p\frac{x^n - 1}{g}\right) = 0 \\ \text{So, } \left(2p\frac{x^n - 1}{g}\right) &\in \ker\varphi = (2a) \text{ and hence,} \\ & a\left|\left(p\frac{x^n - 1}{g}\right)\right. \mod 2. \end{aligned}$$

∎

Claim 3 *If* $C = (g(x) + 2p(x),\ 2a(x)) = (h(x) + 2q(x),\ 2b(x))$ *then* $g(x) = h(x),\ a(x) = b(x)$ *and* $p(x) = q(x) \bmod a(x))$.

Proof. From the construction of C we have $J = \{r(x) : 2r(x) \in \ker\varphi\} = (a(x)) = (b(x))$. Hence $a(x) = b(x)$.

Suppose $C = (g(x) + 2p(x),\ 2a(x)) = (h(x) + 2q(x),\ 2b(x))$. Note that $h(x) \in \varphi(C) = (g(x))$. Hence $h = g(x)\alpha(x)$ and $\deg h(x) \geq \deg g(x)$. By the same means $g(x) = h(x)\beta(x) = g(x)\alpha(x)\beta(x)$ and $\deg g(x) \geq \deg h(x)$. Since g, and h are factors of $(x^n - 1) \bmod 2$ and $(x^n - 1)$ factors uniquely over Z_2 into a product of irreducible polynomials then $\alpha(x) = \beta(x) = 1$ and $g(x) = h(x)$. Since $g(x) + 2q(x) \in C$, then $g(x) + 2q(x) = [g(x) + 2p(x)] + 2a(x)m(x)$. This implies

$$2[g(x) - p(x)] = 2a(x)m(x)$$

Therefore $p(x) = q(x) \bmod a(x))$. ∎

Claim 4 *If* $\gcd(a(x), g(x)) = 1$, *then* $C = (g(x),\ 2)$.

Proof. Suppose $\gcd(a(x), g(x)) = 1$, then $t(x)a(x) + s(x)g(x) = 1 \Rightarrow 2t(x)a(x) + 2s(x)g(x) = 2 \in C$. Therefore $C = (g(x),\ 2)$. ∎

Claim 5 *Suppose n is odd, then* $C = (g(x), 2a(x)) = (g(x) + 2a(x))$

Proof. Suppose $a(x)|g(x)$ and $a(x)|p(x)\left(\dfrac{x^n - 1}{g(x)}\right)$. Then $g(x) = a(x)m_1(x)$ and $p(x)\left(\dfrac{x^n - 1}{g(x)}\right) = a(x)m_2(x)$ Since n is odd then $(x^n - 1)$ factors uniquely as a product of distinct irreducible polynomials. This implies that $a(x)$ must be a factor of $p(x)$. But $p(x)$ has degree less than $a(x)$. Hence $p(x) = 0$ and $C = (g(x), 2a(x))$. Let $h(x) = g(x) + 2a(x)$. $2h(x) = 2g(x) \in (g(x) + 2a(x))$. Also, $\left(\dfrac{x^n - 1}{g(x)}\right)h(x) = 2\left(\dfrac{x^n - 1}{g(x)}\right)a(x) \in (g(x) + 2a(x))$. Since n is odd then $\gcd\left(\dfrac{x^n - 1}{g(x)},\ g(x)\right) = 1$, and hence there exist some binary polynomials $f_1(x),\ f_2(x)$ such that

$$\begin{aligned} 1 &= \left(\frac{x^n - 1}{g(x)}\right) f_1(x) + g(x)f_2(x) \\ 2a(x) &= 2\left(\frac{x^n - 1}{g(x)}\right) a(x)f_1 + 2g(x)a(x)f_2 \\ &\in (g + 2a). \text{ Hence } g(x) \in (g + 2a) \text{ and} \\ C &= (g(x), 2a(x)) = (g(x) + 2a(x)) \end{aligned}$$

■

We can summarize the above by the following theorem.

Theorem 6 *Let C be a cyclic code in $R_n = Z_4[x]/(x^n-1)$. Then*

1. *If n is odd then R_n is a principal ideal ring and $C = (g(x), 2a(x)) = (g(x) + 2a(x))$ where $g(x)$, $a(x)$ are binary polynomials with $a(x) \mid g(x) \mid (x^n - 1) \bmod 2$.*
2. *If n is not odd then*
   - *(a) If $g(x) = a(x)$, then $C = (g(x) + 2p(x))$ where $g(x)$, $p(x)$ are binary polynomials with $g(x)|(x^n - 1) \bmod 2$, and $g(x)|p(x)\left(\frac{x^n-1}{g(x)}\right)$.*
   - *(b) $C = (g(x) + 2p(x),\ 2a(x))$ where $g(x)$, $a(x)$, and $p(x)$ are binary polynomials with $a(x)|g(x)|(x^n - 1) \bmod 2$, $a(x)|p(x)\left(\frac{x^n-1}{g(x)}\right)$ and $\deg g(x) > \deg a(x) > \deg p(x)$.*

3 Reversible Cyclic Codes

Definition 7 *A cyclic code of length n over Z_4 will be called reversible if $\forall u \in C$, then $u^r \in C$.*

Lemma 8 *Let $f(x), g(x)$ be any two polynomials in Z_4, with $\deg f(x) \geq \deg g(x)$. Then (see [1] for the proof)*

1. *$[f(x)g(x)]^* = f(x)^*g(x)^*$, and*
2. *$[f(x)+g(x)]^* = f(x)^* + x^{\deg f - \deg g}g^*(x)$.*

Theorem 9 *Let $C = (f_0 + 2f_1) = (f_0,\ 2f_1)$ be a linear cyclic code of odd length n over Z_4. Then C is reversible cyclic code if and only if f_0, and f_1 are self-reciprocal.*

Proof. Let $c(x)$ be an element in C. Then $c(x) = f_0l_1 + 2f_1l_2$ for some polynomials l_1, l_2 where $\deg(l_1(x) \leq n - \deg(f_0) - 1$, and $\deg(l_2(x)) \leq \deg(f_0) - \deg(f_1) - 1$. We may assume $\deg(c(x)) = n-1$. C is reversible if and only if $c^*(x) \in C$ if and only if

$$\begin{aligned} x^{n-1}c(1/x) &= x^{n-1}\left[l_1(1/x)f_0(1/x) + 2l_2(1/x)f_1(1/x)\right] \\ &= \left[x^{n-\deg(f_0)-1}l_1(1/x)f_0^*(x)\right] \\ &\quad + \left[2x^{n-\deg(f_1)-1}l_2(1/x)f_1(x)^*\right] \\ &= l_1^*(x)f_0^*(x) + 2l_2^*(x)f_1^*(x). \end{aligned}$$

Hence, $C = (f_0, 2f_1) \subseteq (f_1(x)^*,\ 2f_1(x)^*)$. Similarly we get that $(f_0(x)^*,\ 2f_1(x)^*) \subset (f_0,\ 2f_1)$, and hence $(f_0(x)^*,\ 2f_1(x)^*) = (f_0,\ 2f_1) = C$. Therefore, C is reversible if and only if f_0, and f_1 are self-reciprocal. ■

Theorem 10 *Let $C = (g(x) + 2p(x))$ or $C = (2a(x))$ be a cyclic code where n is even. Then C can not be reversible unless $p(x) = 0$.*

Proof. Suppose $C = (g(x) + 2p(x))$ is reversible. Then $C \bmod(2)$ is a binary cyclic reversible code and hence $g(x)$ is self-reciprocal. This implies

$$\begin{aligned} (g(x) + 2p(x))^* &= g(x)^* + 2x^ip^*(x) \\ &= g(x) + 2x^ip^*(x) \\ &= [g(x) + 2p(x)]\, m(x) \in C \end{aligned}$$

This implies that $m(x) = 1$, $i = 0$, $\deg p(x) = \deg g(x)$, and $p(x) = p^*(x)$. But $\deg p(x) < \deg\ g(x)$. Therefore, C can not be reversible. ■

Theorem 11 *Suppose $C = (g(x) + 2p(x),\ 2a(x))$ with $a(x)|g(x)|(x^n-1)$, $a|p\left(\frac{x^n-1}{g(x)}\right)$ and $\deg g(x) > \deg a(x) > \deg p(x)$. C is a reversible cyclic code if and only if*

1. *$g(x)$, $a(x)$ are self-reciprocal*
2. *$a(x) \mid \left(x^ip^*(x) + p(x)\right)$*

Proof. $\Rightarrow$) Suppose C is reversible cyclic code. The binary codes $(g(x))$, $(a(x))$ must be reversible cyclic codes and hence $g(x)$, and $a(x)$ are self-reciprocal. Since C is reversible then

$$\begin{aligned} (g(x) + 2p(x))^* &= g^*(x) + 2x^ip^*(x) \\ &= g(x) + 2x^ip^*(x) \\ &= (g(x) + 2p(x))\, m_1(x) + 2a(x)m_2(x) \end{aligned}$$

This implies that $m_1(x) = 1$ and $2x^ip^*(x) + 2p(x) = 2a(x)m_2(x)$. Hence $\left(x^ip^* + p\right) \in a(x) \Rightarrow a \mid \left(x^ip^* + p\right) \bmod\ 2$.

$\Leftarrow$) For C to be reversible it is suffices to show $(g(x) + 2p(x))^*$, and $a^*(x)$ are in C. Since $a(x)$ is self-reciprocal then $a^*(x) = a(x) \in C$. Also,

$$\begin{aligned} (g(x) + 2p(x))^* &= g^*(x) + 2x^ip^*(x) = g(x) + 2x^ip^*(x) \\ &= (g(x) + 2p(x)) + 2p(x) + 2x^ip^*(x) \\ \in C. &\quad \left(\begin{array}{c} \text{Since } 2p(x) + 2x^ip^*(x) \\ \in (2a(x)) \end{array}\right) \end{aligned}$$

Hence, C is reversible. ■

Proceedings of the 9th WSEAS International Conference on Applied Mathematics, Istanbul, Turkey, May 27-29, 2006 (pp441-446)

4 Examples

- Length $n = 8$. $(x^8 + 1) = (x + 1)^8$ over Z_2. Let $f = (x + 1)$. The tables below give the generator polynomial for all reversible cyclic codes of length 8.

	Non-zero Generator polynomial (s) of C	$d(C)$
1	1, or 2	1
2	(αf^i) where $\alpha = 1,\ 2$ and $1 \leq i \leq 4$	2
3	(αf^i) where $\alpha = 1,\ 2$ and $5 \leq i \leq 6$	4
4	(αf^7) where $\alpha = 1,\ 2$	8
5	$(x + 1, 2)$	1
6	$(x^2 + 1, 2)$, $(x^2 + 1, 2(x + 1))$	$1, 2$
7	$((x^2 + 1) + 2, 2(x + 1))$	2
8	$((x^3 + x^2 + x + 1), 2)$	1
9	$((x^3 + x^2 + x + 1), 2(x + 1))$	2
10	$((x^3 + x^2 + x + 1) + 2, 2(x + 1))$	2
11	$((x^3 + x^2 + x + 1), 2(x^2 + 1))$	2
12	$((x^3 + x^2 + x + 1) + 2(x + 1), 2(x^2 + 1))$	2
13	$((x^4 + 1), 2)$, $((x^4 + 1), 2(x + 1))$	$1, 2$
14	$((x^4 + 1) + 2, 2(x + 1))$, $\left((x^4 + 1), 2(x + 1)^2\right)$	$2, 2$
15	$\left((x^4 + 1) + 2, 2(x + 1)^2\right)$	2
16	$\left((x^4 + 1) + 2x, 2(x + 1)^2\right)$	2
17	$\left((x^4 + 1) + 2(x + 1), 2(x + 1)^2\right)$	2
18	$((x^5 + x^4 + x + 1), 2)$	1
19	$((x^5 + x^4 + x + 1), 2(x + 1))$	2
20	$((x^5 + x^4 + x + 1) + 2, 2(x + 1))$	2
21	$((x^5 + x^4 + x + 1), 2(x^2 + 1))$	2
22	$((x^5 + x^4 + x + 1) + 2, 2(x^2 + 1))$	2
23	$((x^5 + x^4 + x + 1), 2(x^3 + x^2 + x + 1))$	2
24	$((x^5 + x^4 + x + 1) + 2(x + 1), 2(x^3 + x^2 + x + 1))$	2
25	$((x^5 + x^4 + x + 1) + 2(x^2 + 1), 2(x^3 + x^2 + x + 1))$	2
26	$((x^5 + x^4 + x + 1) + 2(x^2 + x), 2(x^3 + x^2 + x + 1))$	2
27	$((x^5 + x^4 + x + 1), 2(x^4 + 1))$	2
28	$((x^5 + x^4 + x + 1) + (x + 1), 2(x^4 + 1))$	2
29	$((x^5 + x^4 + x + 1) + (x^3 + x^2), 2(x^4 + 1))$	2

Table 1: Reversible Cyclic Codes of Length 8.

	Generator polynomial (s) of C	$d(C)$
30	$\left(\left(x^5+x^4+x+1\right)+(x^3+x^2+x+1), 2(x^4+1)\right)$	2
31	$\left(\left(x^6+x^4+x^2+1\right), 2(x+1)\right)$, $\left(\left(x^6+x^4+x^2+1\right), 2(x+1)\right)$	2, 2
32	$\left(\left(x^6+x^4+x^2+1\right)+2, 2(x+1)\right)$	2
33	$\left(\left(x^6+x^4+x^2+1\right), 2(x^2+1)\right)$	2
34	$\left(\left(x^6+x^4+x^2+1\right)+2, 2(x^2+1)\right)$	2
35	$\left(\left(x^6+x^4+x^2+1\right)+2x, 2(x^2+1)\right)$	2
36	$\left(\left(x^6+x^4+x^2+1\right)+2(x+1), 2(x^2+1)\right)$	2
37	$\left(\left(x^6+x^4+x^2+1\right), 2(x^3+x^2+x+1)\right)$	2
38	$\left(\left(x^6+x^4+x^2+1\right)+2(x^2+1), 2(x^3+x^2+x+1)\right)$	2
39	$\left(\left(x^6+x^4+x^2+1\right), 2(x^4+1)\right)$	2
40	$\left(\left(x^6+x^4+x^2+1\right)+2(x^2+1), 2(x^4+1)\right)$	2
41	$\left(\left(x^6+x^4+x^2+1\right)+2(x^3+x), 2(x^4+1)\right)$	2
42	$\left(\left(x^6+x^4+x^2+1\right)+2(x^3+x^2+x+1), 2(x^4+1)\right)$	2
43	$\left(\left(x^6+x^4+x^2+1\right), 2(x^5+x^4+x+1)\right)$	4
44	$\left(\left(x^6+x^4+x^2+1\right)+2(x^4+1), 2(x^5+x^4+x+1)\right)$	4
45	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2\right)$	1
46	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x+1)\right)$	2
47	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2, 2(x+1)\right)$	2
48	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x^2+1)\right)$	2
49	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2(x+1), 2(x^2+1)\right)$	2
50	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x^3+x^2+x+1)\right)$	2
51	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2(x^2+1),\right.$ $\left.2(x^3+x^2+x+1)\right)$	2
52	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x^4+1)\right)$	2
53	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2(x^3+x^2+x+1),\right.$ $\left.2(x^4+1)\right)$	2
54	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x^5+x^4+x+1)\right)$	4
55	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2(x^4+1),\right.$ $\left.2(x^5+x^4+x+1)\right)$	4
56	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right), 2(x^6+x^4+x^2+1)\right)$	4
57	$\left(\left(x^7+x^6+x^5+x^4+x^3+x^2+x+1\right)+2(x^5+x^4+x+1),\right.$ $\left.2(x^6+x^4+x^2+1)\right)$	4

Table 2: More Reversible Cyclic Codes of Length 8.

- Length $n = 9$. We know that

  $(x^9+1) = \left(x^6 + x^3 + 1\right)\left(x^2 + x + 1\right)(x+1)$ over Z_2.

  Since the length n is odd and all the factors above are self-reciprocal polynomials then by Theorem 9, all the 27 cyclic codes of this length are reversible.

5 Conclusion Remarks

In this paper we studied reversible cyclic codes of length n over Z_4. We found a unique set of generators for theses codes as ideals in the ring $R_n = Z_4[x]/\left(x^n - 1\right)$. A list of all reversible cyclic codes of lengths 8 and 9 is included in section 4. Open problems include the study of reversible negacyclic codes over Z_4. Also it will be interesting to study these codes over Z_{2^e}.

References

[1] T. Abualrub and R. Oehmke, "On the generators of Z_4 cyclic codes," *IEEE Trans. Info. Theory*, vol. 49, no. 9, pp. 2126-2133, Sept. 2003.

[2] T. Blackford, "Cyclic Codes over Z_4 of Oddly Even Length," *Proc. International Workshop on Coding and Cryptography, WCC 2001*, Paris France, 83–92, 2001.

[3] A. R. Calderbank and N. J. A. Sloane, "Modular and p-adic Cyclic Codes," *Des. Codes Cryptogr.*, vol. 6, pp. 21–35, 1995.

[4] A. Robert Calderbank, Eric M. Rains, P. W. Shor, and Neil J. A. Sloane, "Quantum Error Corrections Via Codes over $GF(4)$," *IEEE Trans. Inform. Theory*, Vol. 4, No. 4, pp. 1369-1387, July 1998.

[5] Guy Catagoli, James L.Massey, Philipp A. Schoeller and Niklaus von Seemann, "On Repeated-Root Cyclic Codes," *IEEE Trans. Inform. Theory*, Vol. 37, No. 2, pp. 337-342, March 1991.

[6] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. Sloane, and P. Solė, "The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes," *IEEE Trans. Info. Theory*, vol. 40, pp. 301-319, Mar. 1994.

[7] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, Ninth Impression, North-Holland, Amsterdam, 1977.

[8] J. L. Massey, "Reversible Codes," *Information and Control*, vol. 7, pp. 369-380, 1964

[9] V. Pless and Z. Qian, "Cyclic Codes and Quadratic Residue Codes over Z_4," *IEEE Trans. Inform. Theory*, vol. 42, no. 5, 1594–1600, 1996.

[10] J.H. Van Lint, "Repeated-Root Cyclic Codes," *IEEE Trans. Inform. Theory* Theory, Vol. 37, No. 2, pp. 343-345, March 1991.