AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **38** (2007), Pages 195–205

Reversible cyclic codes over Z_4

Taher Abualrub

Department of Mathematics and Statistics
American University of Sharjah
Sharjah
UAE
abualrub@aus.edu

Irfan Siap

Education Faculty
Adıyaman University,
Adıyaman
Turkey
isiap@gantep.edu.tr

Abstract

In this paper we study reversible cyclic codes of an arbitrary 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. A classification of reversible cyclic codes with respect to their generators will follow. We also study the minimum Hamming distance of cyclic codes over Z_4. Examples of reversible cyclic codes of lengths 5–10 with their minimum Hamming distance will be studied as well.

1 Introduction

Let $Z_4 = \{0, 1, 2, 3\}$ represent the ring of integers modulo four. 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 a linear code which is invariant under 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 $R_n = Z_4[x]/\left(x^n - 1\right)$. Under this identification, cyclic codes can be viewed as ideals in R_n. A code C is called reversible if it is invariant under a reversal of its entries 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 a codeword $u = (u_0, u_1, \cdots, u_{n-1})$, $w(u)$ is the number of nonzero entries in u. The Hamming distance of a linear code C is given by

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

For each polynomial $p(x) = p_0 + p_1 x + \cdots + p_r x^r$ with $p_r \neq 0$, we define the reciprocal of $p(x)$ to be the polynomial $p^*(x) = x^r p(1/x) = p_r + p_{r-1}x^{r-1} + \cdots + p_0 x^r$. Note that $(p^*(x))^* = p(x)$, $\deg p^*(x) \leq \deg p(x)$ 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 in [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 an arbitrary length n. Such codes have applications in the subject of DNA computing. In DNA computing researchers are interested in designing a new set of sequences (codewords) for each experiment depending on various design constraints. One particular common constraint for preventing errors is to minimize the similarity between sequences (codewords) under some distance measure, such as the Hamming distance. Reversible cyclic codes will satisfy the following two 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 minimize the similarity between codewords and the reverse of codewords.

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. In section 4, we study the minimum Hamming distance of cyclic codes over Z_4. This section will provide some results that make computing the minimum Hamming distance of these codes easily by hand. Section 5 includes a list of reversible cyclic codes of lengths $5 - 10$ with their minimum Hamming distance. Section 6 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 an arbitrary length n. Most of the previous work

on cyclic codes in R_n was restricted to the case where n is odd [5,7,9]. Little work was done on cyclic codes in R_n for even length [1-4]. [3] has studied cyclic codes of length $n = 2^e$. It was shown that the ring R_n is not a principal ideal ring. In [4], the case where $n = 2e$ and $\gcd(e, n) = 1$ are studied and the fact that R_n is not a principal ideal ring is also shown. Our approach in studying these codes will be more 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 $\varphi(x) = x \mod 2$.

As in Theorem 14 in [6], φ is a ring homomorphism with the kernel:

$$\ker\varphi = \{2r(x) : r(x) \text{ is a binary polynomial in } C\}.$$

Now, we define $J = \{r(x) : 2r(x) \in \ker\varphi\}$. It is clear 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 $a(x) \mid (x^n - 1) \mod 2$. 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 we can write C as $C = (g(x) + 2p(x),\ 2a(x))$ where $p(x)$ is a binary polynomial and $g(x) | (x^n - 1) \bmod 4$, $a(x) | (x^n - 1) \bmod 2$.

Note that under this construction the polynomial $a(x)$ might be considered a divisor of $(x^n - 1) \bmod 4$ or a divisor of $(x^n - 1) \bmod 2$.

We will abbreviate a for $a(x)$ when the context is clear.

Lemma 1 *In the setting above,* $\deg a(x) > \deg p(x)$, *and* $a(x) \mid g(x) \bmod 2$.

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 $C = (g(x) + 2p(x))$. ■

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

Proof. Consider

$$\varphi\left(\frac{x^n - 1}{g}[g + 2p]\right) = \varphi\left(2p\frac{x^n - 1}{g}\right) = 0.$$

So, $\left(2p\dfrac{x^n - 1}{g}\right) \in \ker\varphi = (2a)$ and hence, $a \mid \left(p\dfrac{x^n - 1}{g}\right) \bmod 2$. ■

Lemma 3 *If* $\gcd(a(x), g(x)) = 1$, *then* $C = (g(x),\ 2)$.

Proof. Suppose $\gcd(a(x), g(x)) = 1$. Then, $t(x)a(x) + s(x)g(x) = 1 + 2l$ implies $2t(x)a(x) + 2s(x)g(x) = 2 \in C$. Therefore $C = (g(x),\ 2)$. ■

Lemma 4 *Suppose* n *is odd. Then* $C = (g(x), 2a(x)) = (g(x) + 2a(x))$.

Proof. Suppose $a(x)|g(x) \bmod 2$ and $a(x)|p(x)\left(\frac{x^n-1}{g(x)}\right) \bmod 2$. Then $g(x) = a(x)m_1(x)$ and $p(x)\left(\frac{x^n-1}{g(x)}\right) = a(x)m_2(x)$. 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, $\left(\frac{x^n-1}{g(x)}\right)h(x) = 2\left(\frac{x^n-1}{g(x)}\right)a(x) \in (g(x) + 2a(x))$. Since n is odd then $\gcd\left(\frac{x^n-1}{g(x)},\ g(x)\right) = 1$, and hence, there exist some binary polynomials $f_1(x),\ f_2(x)$ such that

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

Therefore, $g(x) \in (g + 2a)$ and

$$C = (g(x), 2a(x)) = (g(x) + 2a(x)).$$

■

Lemma 5 *If* $C = (g(x) + 2p(x),\ 2a(x)) = (h(x) + 2q(x),\ 2b(x))$, *then* $\deg g = \deg h$, $g(x) = h(x) \bmod a(x)$ *and* $p(x) = q(x)$.

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 $C = (g(x) + 2p(x),\ 2a(x)) = (h(x) + 2q(x),\ 2a(x))$. Since $a|g$ and $a|h$ then $g = h \bmod a$. Also $h(x) \bmod 2 \in \varphi(C) = (g(x))$. Hence $h = g(x)\alpha(x) \bmod 2$ and $\deg h(x) \geq \deg g(x)$. By the same means

$$g(x) \bmod 2 = h(x)\beta(x) = g(x)\alpha(x)\beta(x) \bmod 2$$

and $\deg g(x) \geq \deg h(x)$. Since g and h are monic divisors of $(x^n - 1) \bmod 2$ we get that $g(x) = h(x)$. Since $h(x) + 2q(x) \in C$, then $h(x) + 2q(x) = [g(x) + 2p(x)] + 2a(x)m(x)$. This implies

$$\begin{aligned} 2\left[q(x) - p(x)\right] &= (g(x) - h(x)) + 2a(x)m(x) \\ &= a(x)l(x). \end{aligned}$$

Since $\deg p(x)$ and $\deg q(x)$ are less than $\deg a(x)$ we get that $2\,[q(x) - p(x)]$ and hence $q(x) = p(x)$. ■

We can summarize the above by the following theorem.

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

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 polynomials with $a(x)\ |g(x)\ |(x^n - 1) \mod 4$.

2. *Assume n is even; then either*

   (a) *C is a free module of generator*

$$C = (g(x) + 2p(x))\,,$$

   where $g(x)|\,(x^n - 1) \bmod 2$ and $(g(x) + 2p(x))\,|(x^n - 1) \bmod 4$, or,

   (b) *$C = (g(x) + 2p(x),\ 2a(x))$ where $g(x)$, $a(x)$, and $p(x)$ are polynomials with $g(x)|(x^n - 1) \mod 2$, $a(x)|g(x) \bmod 2$, $a(x)|p(x)\left(\dfrac{x^n - 1}{g(x)}\right) \mod 2$, and $\deg a(x) > \deg p(x)$.*

3 Reversible Cyclic Codes

Definition 1 *A cyclic code of length n over Z_4 will be called reversible if $u \in C$ implies $u^r \in C$.*

Lemma 6 *Let $f(x), g(x)$ be any two polynomials in Z_4, with $\deg f(x) \geq \deg g(x)$. Then, (see [3] 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 2 *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 a reversible cyclic code if and only if f_0 and f_1 are both self-reciprocal.*

Proof. If C is a reversible cyclic code, then the binary cyclic codes $(f_0(x)) \bmod 2$ and $(f_1(x)) \bmod 2$ are reversible and hence f_0, and $f_1 \bmod 2$ are both self-reciprocal. Since n is odd, $(x^n - 1) \bmod 4$ factors uniquely as a product of distinct irreducible

polynomials. If $f_0^* \neq f_0 \bmod 4$ then $(x^n - 1)$ will have multiple factors $\bmod 2$; a contradiction. Therefore f_0, and f_1 are both self-reciprocal.

Conversely, suppose f_0, and f_1 are both self-reciprocal. Let $c(x)$ be an element in C. Then $c(x) = f_0 l_1 + 2 f_1 l_2$ for some polynomials l_1, l_2 where $\deg(l_1) \leq n - \deg(f_0) - 1$, and $\deg(l_2) \leq \deg(f_0) - \deg(f_1) - 1$. We may assume $\deg(c(x)) = n - 1$.

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

So $c^*(x) \in (f_1(x),\ 2f_1(x))$ and hence C is reversible. ■

Lemma 7 *Let $C = (\alpha a(x))$ $\alpha = 1$ or 2 be a cyclic code of even length n. Then C is reversible if and only if $a(x)$ is self-reciprocal.*

Proof. The proof is similar to the case of finite fields as in [8]. ■

4 Minimum Hamming Distance

In this section we give some facts that will help to find the minimum Hamming distance of linear quaternary codes.

Lemma 8 *Let C be a linear code over Z_4 of length n. Let $C_2 = \{c \in Z_2^n \mid 2c \in C\}$. Then, C_2 is a binary code of length n and*

$$d(C) = d(C_2).$$

Proof. It is clear that C_2 is a binary code of length n. Further, if c is a binary word, then $w(c) = w(2c)$. Let $w(c) = d(C)$. If $2c \neq 0$, then $c \pmod 2$ is a nonzero codeword in C_2 and $w(c) \geq w(c \pmod 2)$. Hence $d(C) \geq d(C_2)$. Otherwise, $c = 2c'$ for some $c' \in Z_2^n$, with $c' \in C_2$ and $w(c) = w(c') \geq d(C_2)$. Hence, $d(C) \geq d(C_2)$. Conversely, let $c' \in C_2$ such that $w(c') = d(C_2)$. Since c' is a binary word we have $w(c') = w(2c')$ and $2c' \in C$. Also, $d(C) \leq w(2c') = w(c') = d(C_2)$. Thus $d(C) = d(C_2)$. ■

Lemma 9 *Let $C = (g(x) + 2p(x),\ 2a(x))$ where $a(x) | g(x)$. Then,*

$$C_2 = (a(x)).$$

Proof. Since $2a(x) \in C$ then $(a(x)) \subset C_2$. Conversely, assume that $c \in C_2$ such that $2c \in C$. Then $2c \in \ker \varphi$ and hence $c \in J = (a(x))$. So $C_2 \subset (a(x))$. ■

Example 1 *Consider the cyclic code* $C = ((x^5 + x^4 + x + 1) + 2, 2(x^2 + 1))$ *of length* $n = 8$. *By Lemma 9 we have* $C_2 = (x^2 + 1)$. *So* $d(C_2) = 2$. *By Lemma 8, we know that* $d(C) = d(C_2)$; *hence* $d(C) = 2$.

Definition 2 [1] *Let* $s = b_{e-1}2^{e-1} + b_{e-2}2^{e-2} + \cdots + b_1 2^1 + b_0 2^0$ *be the 2-adic expansion of* s. *Let* $b_{e-1} = b_{e-2} = \cdots = b_{e-q} = 1$ *where* $e - q > 0$ *and* $b_{e-q-1} = 0$.

1. *If* $b_{e-i} = 0$ *for all* $i \in \{q+2, q+3, \ldots, e-1, e\}$, *then* s *is said to have a 2-adic length* q *zero expansion.*
2. *If* $b_{e-i} \neq 0$ *for some* $i \in \{q+2, q+3, \ldots, e-1, e\}$, *then* s *is said to have a 2-adic length* q *nonzero expansion.*

If $e = q$ *then,* s *is said to have 2-adic length* e *expansion or 2-adic full expansion.*

Example 2 $5 = 2^2 + 2^0$ *and hence* $q = 1$, *and 5 has a 2-adic length 1 nonzero expansion.* $6 = 2^2 + 2^1$ *has a 2-adic length 2 zero expansion.* $7 = 2^2 + 2^1 + 2^0$ *and hence* $q = 3$, *and 7 has a 2-adic full expansion.*

Lemma 10 [1] *Let* C *be a binary cyclic of length* 2^e *where* e *is a positive integer. Assume that* $C = (a(x))$ *where* $a(x) = (x^{2^{e-1}} - 1)h(x)$ *for some* $h(x)$. *If* $h(x)$ *generates a cyclic code of length* 2^{e-1} *and minimum distance* d, *then* $d(C) = 2d$.

Theorem 3 *Let* C *be a cyclic code over* Z_4 *of length* 2^e *where* e *is a positive integer. Then* $C = (g(x) + 2p(x), 2a(x))$ *where* $g(x) = (x-1)^t$ *and* $a(x) = (x-1)^s$ *for some* $t > s > 0$.

Further, if $s \leq 2^{e-1}$, *then* $d(C) = 2$. *Otherwise,* s *has 2-adic length* $q \geq 1$ *expansion.*

1. *If* s *has a 2-adic length* q *zero expansion or full expansion* $(e = q)$, *then* $d(C) = 2^q$.
2. *If* s *has a 2-adic length* q *nonzero expansion, then* $d(C) = 2^{q+1}$.

Proof. A similar proof given for codes over $Z_2 + uZ_2$ in [1] can be adapted easily. ■

Example 3 *Consider the cyclic codes* (αf^i) $i = 1, 2 \ldots, 7$ *in Table 3. Here, again* $n = 8 = 2^3$ *and the minimum distances of these cyclic codes with the generators* αf^i *where* $f = x + 1$ *can be computed by Theorem 3. If* $1 \leq i \leq 4 = 2^2$, *then* $d(C) = 2$. *If* $i = 5$, *then* i *has a 2-adic length 1 nonzero expansion; hence* $d(C) = 4$. *If* $i = 6$, *then* i *has a 2-adic length 2 zero expansion, hence* $d(C) = 4$. *Finally, if* $i = 7$, *then* i *has a 2-adic length 3 zero expansion, and hence* $d(C) = 8$.

Example 4 *A List of Reversible Cyclic Codes*

We will list all reversible cyclic codes of odd lengths 5, 7, 9 *and all free module reversible cyclic codes of length* 6, 8, *and* 10 *with their minimum Hamming distance d. This can be done by using Theorems 2, 3, and Lemma 7.*

- Length $n = 5$.

$$\left(x^5 + 1\right) = (x - 1)\left(x^4 + x^3 + x^2 + x + 1\right) \text{ over } Z_2.$$

Since the length $n = 5$ is odd and all the factors above are self-reciprocal polynomials then by Theorem 2, all 9 cyclic codes of this length are reversible.

- Length $n = 6$. To get all factorization of $(x^6 - 1) \bmod 4$ we will factor $(x^6 - 1) \bmod 2$ and then get all factors $(f + 2p)$ where $f|(x^6 - 1) \bmod 2$ and $(f + 2p)|(x^6 - 1) \bmod 4$.

$$\left(x^6 + 1\right) = (x + 1)^2\left(x^2 + x + 1\right) \text{ over } Z_2.$$

From Lemma 7, the only nonzero free module, or single generator reversible cyclic codes of length 6 are given below in Table 1:

Non-Zero Generator Polynomial(s):	$d(C)$
$1,\ 2$	1
$(x-1),\ (x+1)$	2
$(x^2+x+1),\ (x^2-x+1)$	2
$2(x+1),\ 2(x^2+x+1)$	2
(x^2+1+2)	2
$(x-1),\ (x+1)(x^2+x+1)$	2
$(x+1)(x^2-x+1)$	2
$(x^2+x+1)(x^2-x+1)$	3
$2(x-1)(x+1),\ 2(x-1)(x^2+x+1)$	2
$2(x^2+x+1)(x^2-x+1)$	3
$(x-1)(x+1)(x^2+x+1),\ (x-1)(x+1)(x^2-x+1)$	4
$(x+1)(x^2+x+1)(x^2-x+1)$	6
$(x-1)(x^2+x+1)(x^2-x+1)$	6
$2(x-1)(x+1)(x^2+x+1)$	4
$2(x-1)(x^2+x+1)(x^2-x+1)$	6

Table 1: Reversible free module or single generator cyclic codes of length 6 over Z_4.

- Length $n = 7$. The only self-reciprocal factors of $(x^7 - 1)$ are

$$x - 1 \text{ and } (x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

From Theorem 2 the only nonzero reversible cyclic codes of length 7 are given below in Table 2:

Non-Zero Generator Polynomial(s) of C	$d(C)$
1 or 2	1
$(x-1)$	2
$(2(x+1))$	2
$(x-1,2)$	1
$(x^6+x^5+x^4+x^3+x^2+x+1)$	7
$(2(x^6+x^5+x^4+x^3+x^2+x+1))$	7
$(x^6+x^5+x^4+x^3+x^2+x+1,2)$	1

Table 2: Reversible cyclic codes of length 7 over Z_4.

- Length $n=8$. Note that the factorization of $(x^8-1) \bmod 4$ is not unique. To get all factorization we will factor $(x^8-1) \bmod 2$ and then get all factors $f+2p$ where $f|(x^8-1) \bmod 2$ and $(f+2p)|(x^8-1) \bmod 4$.

$$x^8-1=(x+1)^8=f^8 \text{ over } Z_2$$

From Lemma 7, the only nonzero free module or single generator reversible cyclic codes of length 8 are given below in Table 3:

Non-zero Generator polynomial (s) of C	$d(C)$
1, or 2	1
(αf^i) where $\alpha=1,\ 2$ and $1 \le i \le 4$	2
(αf^i) where $\alpha=1,\ 2$ and $5 \le i \le 6$	4
(αf^7) where $\alpha=1,\ 2$	8
$(f+2)$	2
$(f^2+2)\,,(f^2+2x)$	2
(f^2+2+2x)	2
$(f^3+2x+2x^2)$	2
(f^3+2+2x^2)	2
(f^3+2+2x)	2
(f^4+2x^2)	2
(f^4+2)	2
$(f^4+2x+2x^3)$	2
$(f^4+2x^3+2x^2+2x)$	2
(f^4+2x^3+2x+2)	2
$(f^4+2x^3+2x^2+2x+2)$	
(f^4+2+2x^2)	2
$(f^5+2+2x+2x^2+2x^3)$	4
$(f^6+2x+2x^5)$	4

Table 3: Reversible free module or single generator cyclic codes over Z_4 of length 8.

- Length $n = 9$. We know that

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

Since the length n is odd and all the factors above are self-reciprocal then all factors of $(x^9 - 1) \bmod 4$ are self reciprocal polynomials. By Theorem 2, all the 27 cyclic codes of this length are reversible.

- Length $n = 10$.

$$\left(x^{10} + 1\right) = (x-1)(x+1)\left(x^4 + x^3 + x^2 + x + 1\right)\left(x^4 - x^3 + x^2 - x + 1\right) \bmod 4.$$

From Lemma 7 the only nonzero free module or single generator reversible cyclic codes of length 10 are given below in Table 4:

Non-Zero Generator Polynomial(s) of C	$d(C)$
1, or 2	1
$(x-1),\ (x+1),$	2
$(2(x+1))$	2
(x^2-1)	2
$(2(x^2-1))$	2
$(x^4+x^3+x^2+x+1)$	2
$(x^4-x^3-x^2-x+1)$	2
$(x^4+x^3-x^2+x+1)$	2
$(x^4-x^3+x^2-x+1)$	2
$2(x^4+x^3+x^2+x+1)$	2
(x^5+1)	2
$(x^5+2x^3+2x^2+1)$	2
(x^5+2x^4+2x+1)	2
$(x^5-1),\ (2(x^5-1))$	2
(x^5+2x^4+2x+1)	2
$(x^5+2x^4+2x^3+2x^2+2x+1)$	2
$(x^5+2x^3+2x^2-1)$	2
(x^5+2x^4+2x-1)	2
$(x^5+2x^4+2x^3+2x^2+2x-1)$	2
(x^6-x^5+x-1)	4
$(x^6-x^5+2x^4+2x^2+x-1)$	4
(x^6+x^5-x-1)	4
$(x^6+x^5+2x^4+2x^2-x-1)$	4
$2(x^6+x^5+x+1)$	4
$(x^8+x^6+x^4+x^2+1),\ (2(x^8+x^6+x^4+x^2+1))$	4
$(x^9+x^8+...+1),\ (2(x^9+x^8+...+1))$	10
$(x^9-x^8+x^7-x^6+x^5-x^4+x^3-x^2+x-1)$	10

Table 4: Reversible free module or single generator cyclic codes over Z_4 of length 10.

5 Conclusion

In this paper we studied reversible cyclic codes of length n over Z_4. We found a unique set of generators for these codes as ideals in the ring $R_n = Z_4[x]/(x^n - 1)$. We also studied the minimum Hamming distance of these codes over Z_4. A list of reversible cyclic codes of lengths $5 - 10$ is included. 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}.

We would like to thank the referee(s) for their valuable remarks.

References

[1] T. Abualrub, and I. Siap, On The Construction of Cyclic Codes over the Ring $Z_2 + uZ_2$, *Proc.* 9^{th} *WSEAS Internat. Conf. Appl. Math.* Istanbul, Turkey, (2006), 430–435.

[2] T. Abualrub and I. Siap, Reversible quaternary cyclic codes, *Proc.* 9^{th} *WSEAS Internat. Conf. Appl. Math.* Istanbul, Turkey, (2006), 441–446.

[3] T. Abualrub and R. Oehmke, On the generators of Z_4 cyclic codes, *IEEE Trans. Info. Theory* 49 no. 9 (2003), 2126–2133.

[4] T. Blackford, Cyclic codes over Z_4 of oddly even length, *Proc. Internat. Workshop Coding Crypto.* WCC (2001), Paris, 83–92.

[5] A.R. Calderbank and N.J.A. Sloane, Modular and p-adic cyclic codes, *Des. Codes Cryptogr.* 6 (1995), 21–35.

[6] A.R. Calderbank, E.M. Rains, P.W. Shor and N.J.A. Sloane, Quantum error corrections via codes over $GF(4)$, *IEEE Trans. Info. Theory* 44 No. 4 (1998), 1369–1387.

[7] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solè, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Info. Theory* 40 (1994), 301–319.

[8] J.L. Massey, Reversible Codes, *Information and Control* 7 (1964), 369–380.

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

(Received 28 Apr 2006; revised 8 Oct 2006)