Negacyclic Codes of Even Length over Z_4

Taher Abualrub and Marwan Abukhaled

Department of Mathematics and Statistics
American University of Sharjah
Sharjah-UAE

Abstract

In this paper we study negacyclic codes of length $n = 2^e$ for some integer e. We found the set of generators for this type of codes as ideals in the ring $D_4 = Z_4[x] \ / \ \langle x^n + 1 \rangle$. It will be shown that any negacyclic code has the form $\langle \alpha(x+1)^m \rangle$, $\alpha = 1, 2$, and $m = 0, 1, ..., n-1$. It will also be shown that the element 2 is in every nonzero code of the form $\langle (x+1)^m \rangle$. As such, it is concluded that negacyclic codes of length $n = 2^e$ for some integer e have a very low minimum distance. Dual codes of length $n = 2^e$ over Z_4 will also be studied.

1 Introduction

The study of linear and cyclic codes over Z_4 has provided useful results in coding theory [1-4, 6-8]. It was shown in [6] that important families of binary nonlinear codes are in fact images under the Gray map of linear codes over Z_4. For example, the Gray map [6] was used to show that Kerdock and Preparata codes can be constructed as binary images via the Gray map of linear codes over Z_4.

Wolfmann in [10] studied negacyclic codes of odd length over Z_4. He showed that this is an important class of codes and must be given some attention from the coding community. He defined a (linear) negacyclic code over Z_4 to be an ideal in the ring $D_4 = Z_4[x] \ / \ \langle x^n + 1 \rangle$. In this correspondence, we note that negacyclic codes mean linear negacyclic codes. In [10], Wolfmann also showed that over Z_4, the structure of negacyclic codes is similar to that of cyclic codes. Furthermore, he showed that if C is a negacyclic code of odd length n then its polynomial representation I is a principle ideal generated by a constant polynomial or a polynomial of the kind $g(x) = a(x)[b(x) + 2]$ where $x^n + 1 = a(x)b(x)c(x)$ in $Z_4[x]$ and where $a(x)$, $b(x)$, and $c(x)$ are pairwise coprime polynomials. He also studied the Gray image of negacyclic codes and showed that the Gray image of a linear negacyclic code over Z_4 is a binary-distance-invariant (not necessary linear cyclic code. One of the many problems that Wolfmann posted for future studies in [10] was the study of negacyclic codes of even length.

In this paper, we study negacyclic codes of even length over Z_4. In particular, the length $n = 2^e$ for some integer e.

Cyclic codes of length n over a field of characteristic p where p divides n are called repeatd-root cyclic codes. Castagnoli et al [5] and Van Lint [9] studied this kind of codes and showed that these codes are asymptotically bad even though they can be optimal in few cases. In a study of cyclic codes of length $n = 2^e$ ([1], and [2]) it was shown that the class of cyclic codes

of length $n = 2^e$ is indeed a big one. It was also shown that the ring $R_4 = Z_4[x] / \langle x^n - 1 \rangle$ is not a principle ideal ring and hence the ideals (cyclic codes) are not principle ideals. In [1], the subject of dual codes of length $n = 2^e$ was studied as well. The structure of cyclic dual codes was given including a list of all cyclic *self dual* codes of length 8.

In this paper, it will be shown that the structure of the ring D_4 is different from that of R_4. It will also be shown that the class of negacyclic codes of length $n = 2^e$ is not a big class of codes as in the case of cyclic codes. The fact that the ring D_4 is a principle ideal ring and hence ideals (negacyclic codes) are principle ideals will be established. Furthermore, it will be shown that this class of codes is not a good class for since all codes have very low minimum distance. The objectives of this study will be reached in the following sequel: section 2 covers a study of the ring D_4 and the structure of negacyclic codes in it whereas section 3 covers a study of the structure of dual negacyclic codes.

We assume throughout this paper that $n = 2^e$.

2 Negacyclic Codes

By $Z_4 = \{0, 1, 2, 3\}$, it is meant the ring of integers modulo 4.

Construct the ring

$$D_4 = Z_4[x] / \langle x^n + 1 \rangle = \left\{ f(x) : \ f(x) = a_0 + a_1 x + ... a_{n-1} x^{n-1} \right\}$$

where $a_i \in Z_4 \ \forall \ i = 0, 1, ..., n-1$, and $x^n = -1$.

In [1], it was shown that $(x^n + 1)$ is an irreducible polynomial over Z_4. It is worth mentioning that if Z_4 is a field, then the ring D_4 will only have the two trivial ideals; the zero ideal and the D_4 itself.

since any element c in Z_4 can be written as $c = a + 2b$ where $a, \ b$ are elements in Z_2 then any element in D_4 can be expressed in the form

$$f(x) = \sum_{i=0}^{n-1} a_i (x+1)^i + 2 \sum_{i=0}^{n-1} b_i (x+1)^i \quad \text{where } a_i, \ b_i = 0, 1, \text{ for all } i = 0, 1, ..., n-1.$$

As in the case of cyclic codes, it is convenient to represent code words of length n by polynomials modulo $x^n + 1$. We identify $v = (v_0, ..., v_{n-1})$ with the polynomial $v(x) = v_0 + v_1 x + ... + v_{n-1} x^{n-1}$ in the ring D_4.

Definition 1 *By a negacyclic code over Z_4, it is meant an ideal in the ring D_4.*

The proof of the following lemma can be found in [1].

Lemma 1 *Let $m = 2^k$ where $k > 0$. Then $x^m + 1 = (x+1)^m + 2x^{m/2}$ in $Z_4[x]$.*

A particular instant of the this lemma is that, in the ring D_4 we have, $0 = x^n + 1 = (x+1)^n + 2x^{n/2}$. This implies that $(x+1)^n = 2x^{n/2} \Rightarrow (x+1)^{2n} = 0$. This proves the following lemma:

Lemma 2 *$(x+1)$ is a nilpotent element in D_4 whose nilindex is equal to $e = 2n$.*

Notice that if a and b are nilpotent elements in a ring R then using the Binomial Theorem on the ring D_4 it can easily be shown that $(a \pm b)$ is also a nilpotent element.

Lemma 3 *Let* $f(x) = \sum_{i=0}^{n-1} a_i(x+1)^i + 2\sum_{i=0}^{n-1} b_i(x+1)^i$ *be an element in* D_4 *where* $a_i,\ b_i = 0, 1$. *Then* $f(x)$ *is a unit in* D_4 *iff* $a_o = \pm 1$.

Proof. $\Rightarrow$) Suppose $f(x)$ is a unit. If $a_0 = 0$, then $f(x) = (x+1)^j h(x)$ where $j \geq 1$. But then

$$f(x)^{2n} = \left[(x+1)^j h(x)\right]^{2n} = 0.$$

Therefore, $f(x)$ is not a unit.

$\Leftarrow$) Suppose $f(x) = \pm 1 + \sum_{i=1}^{n-1} a_i(x+1)^i + 2\sum_{i=0}^{n-1} b_i(x+1)^i$. Since $(x+1)$ is nilpotent then

$$\sum_{i=1}^{n-1} a_i(x+1)^i + 2\sum_{i=0}^{n-1} b_i(x+1)^i$$

is also a nilpotent element with

$$\left[\sum_{i=1}^{n-1} a_i(x+1)^i + 2\sum_{i=0}^{n-1} b_i(x+1)^i\right]^{2n} = 0.$$

Hence $f(x) = \pm 1 + a$ where $a^{2n} = 0$. Then,

$$(a-1)(-1(a^{2n-1} + a^{2n-2} + a^{2n-2} + ... + 1)) = -(a^{2n} - 1) = 1,$$

and

$$(a+1)(-1(a^{2n-1} - a^{2n-2} + a^{2n-2} - a^{2n-3} + ... - 1) = -(a^{2n} - 1) = 1.$$

Hence $f(x)$ is a unit. ■

Lemma 4 D_4 *is a local ring with maximal ideal* $M = \langle x+1\rangle = \langle x-1\rangle$.

Proof. In D_4, it was established that

$$0 = x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} - ... + 1) + 2.$$

It follows that $2 \in \langle x+1\rangle = \langle x-1\rangle$. Since any element in D_4 has the form

$$f(x) = \sum_{i=0}^{n-1} a_i(x+1)^i + 2\sum_{i=0}^{n-1} b_i(x+1)^i \text{ where } a_i = 0, 1,\ b_i = 0, 1 \text{ for all } i = 0, 1, ..., n-1,$$

then the only elements that are not in M are the ones for which $a_0 = \pm 1$. But these are unit elements by the above lemma. Therefore D_4 is a local ring with maximal ideal $M = \langle x+1\rangle = \langle x-1\rangle$. ■

Since $(x+1)^n = 2x^{n/2}$ and $x^{n/2}$ is a unit in D_4 then $2 = \langle (x+1)^n\rangle$.

Lemma 5 *If* R *is a finite local ring with maximal ideal* $M = \langle a\rangle$. *Then any ideal* I *in* R *is given by* $I = \langle a^n\rangle$.

Proof. Let $i \in I \subseteq M = \langle a \rangle$. Then $i = ar_1$ for some $r_1 \in R$. If r_1 is a unit then $I = M$, otherwise $r_1 \in M$ since R is a local ring. Hence $r_1 = ar_2$ for some $r_2 \in R$ which implies that $i = a^2 r_2$. Continuing in this process leads to $i = a^n$ for some integer n. Therefore $I = \langle a^n \rangle$ for some integer n. ■

The main result can now be stated:

Theorem 1 *D_4 is a principal ideal ring with nonzero ideals (negacyclic codes) given by $C = \langle \alpha(x+1)^m \rangle$ where $\alpha = 1,\ 2$, and $m = 0, 1, 2, ..., n-1$.*

Proof. Follows directly from lemmas 4 and 5 in addition to the fact that $\langle 2 \rangle = \langle (x+1)^n \rangle$. ■

Since $\langle 2 \rangle = \langle (x+1)^n \rangle$, then 2 is an element in any nonzero negacyclic code of the form $\langle (x+1)^m \rangle$. This shows that the minimum Hamming and Lee wights of any negacyclic code of length $n = 2^e$ and of the form $\langle (x+1)^m \rangle$ is equal to 1 and 2 respectively. Also, this shows that the minimum Euclidean weight for this type of codes is at most 4. For this reason, this class of codes may be classified as a bad one in terms of the minimum distance.

3 Dual Codes

Definition 2 *Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ be any two vectors over Z_4. Define an inner product over Z_4 by $u \cdot v = u_1 v_1 + \ldots + u_n v_n$. the vectors u and v are said to be orthogonal if $u \cdot v = 0$.*

Definition 3 *Let C be a negacyclic code of length n. The dual of C is denoted by $C^{\perp}$ and is defined by $C^{\perp} = \{u :\ u.v = 0\ \forall v \in C\}$.*

The following theorem is the same as in [8] except that a field is replaced by a ring. We state it without proof.

Theorem 2 *Let $f(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1}$ and $b(x) = b_0 + b_1 x + ... + b_{n-1} x^{n-1}$. Then $a(x)b(x) = 0$ iff the vector $(a_0, a_1, ..., a_{n-1})$ is orthogonal to the vector $(b_{n-1}, b_{n-2}, ..., b_0)$ and to all its cyclic shifts.*

Definition 4 *If $f(x) = a_0 + a_1 x + ... + a_r x^r$, then the reciprocal of $f(x)$ is the polynomial $f^*(x) = a_r + a_{r-1} x + ... + a_0 x^r$. Symbolically $f^*(x)$ can be represented by $f^*(x) = x^r f(\frac{1}{x})$.*

If I is an ideal in D_4, then $I^* = \{f^*(x) :\ f(x) \in I\}$ is also an ideal.

Definition 5 *Let I be an ideal in D_4. The annihilator of I (denoted by $A(I)$), which is an ideal in D_4 is given by*

$$A(I) = \{g(x) :\ f(x)g(x) = 0 \text{ for all } f(x) \in I\}$$

It is clear that if C is a negacylcic code whose associated ideal I, then the associated ideal for $C^{\perp}$ is $A^*(I)$.

The following lemma and its proof can be found in [1].

Lemma 6 *If $f(x) = (x+1)^r$, then $f(x) = f^*(x)$.*

Theorem 3 *Let C be a negacylcic code of length n over Z_4.*

1. If $C = \langle (x+1)^i \rangle$, then $C^\perp = \langle 2(x+1)^{n-i} \rangle$.
2. If $C = \langle 2(x+1)^i \rangle$, then $C^\perp = \langle (x+1)^{n-i} \rangle$.

Proof. Suppose $C = \langle (x+1)^i \rangle$. $2(x+1)^{n-i}(x+1)^i = 2(x+1)^n = 0$. Hence $\langle 2(x+1)^{n-i} \rangle \subseteq A(C)$. Suppose that $A(C) = \langle \alpha(x+1)^j \rangle$ for some $j = 0, 1, ..., n-1$. Since $\alpha(x+1)^j.(x+1)^i = 0$, then α must equal 2. The smallest power j satisfies $2(x+1)^j.(x+1)^i = 0$ is $j = n-i$. Therefore, $\langle 2(x+1)^{n-i} \rangle = A(C)$. From lemma 6, $A(C) = A^*(C) = C^\perp$ and consequently $C^\perp = \langle 2(x+1)^{n-i} \rangle$.This establishes (1). The proof of two is similar. ■

4 Conclusion

The negacyclic codes studied here are taken over Z_4 and have a length of $n = 2^e$. Contrary to the case of cyclic codes of the same length, it was shown that the ring D_4 is a principal ideal ring. We constructed a set of generators for this type of codes and their duals. It was also shown that the element 2 is in every negacyclic code of the form $\langle (x+1)^m \rangle$ which implies that this class of negacyclic codes has a very low minimum distance. In particular, these codes are asymptotically bad. It will be very interesting to see what kind of applications might arise from this type of codes. Open problems include the study of negacyclic codes of other lengths. In particular the study of negacyclic codes of length $n = 2e$ where e is an odd integer.

References

[1] T. Abualrub and R. Oehmke, "On the Generators of Z_4 Cyclic Codes," Submitted IEEE Tran. Inform. Theory.

[2] T. Abualrub and R. Oehmke, "Cyclic Codes of length 2^e over Z_m," Proc. International Workshop on Coding and Cryptography, WCC 2001, Paris France, 2001, 15-21.

[3] T. Blackford, "Cyclic Codes over Z_4 of Odly Even Length," Proc. International Workshop on Coding and Cryptography, WCC 2001, Paris France, 2001, 83-92.

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

[5] G. Castagnoli, J. L. Massey, P. A. Schoeller, and N. Von Seeman, "On Repeated Root Cyclic Codes," IEEE. Tran. Inform Theory, vol. 37, no. 2, pp. 337-342, 1991.

[6] A. R. Hammons, P. V. Kumar and A. R. Calderbank, N. J. A. Sloane, and P. Sole, "The Z_4-Linearity of Kerdock, Preparata, Goethals, and Related Codes," IEEE Trans. Inform. Theory, vol. 40, 301-319, Mar. 1994.

[7] P. Kanwar and S. R. Lopez-Permouth, "Cyclic Codes over the Integers Modulo p," Finite Fields and their Applications, vol. 3, number 4 (1997), pp. 334-352.

[8] V. Pless and Z. Qian, "Cyclic Codes and Quadratic Residue Codes over Z_4," IEEE, Trans. Inform. Theory, vol. 42, pp1594-1600, 1996.

[9] J. H. Van Lint, "Repeated-Root Cyclic Codes," IEEE Trans. on Inform. Theory, vol. 37, no. 2, pp. 343-345, 1991.

[10] J. Wolfmann, "Negacyclic and Cyclic Codes over Z_4," IEEE Trans. on Inform. Theory, vol. 45, n0. 7, pp 2527-2532, November 1999.