ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Discrete Applied Mathematics 128 (2003) 27–46

DISCRETE
APPLIED
MATHEMATICS

www.elsevier.com/locate/dam

Cyclic codes over Z_4 of oddly even length

Thomas Blackford

Department of Mathematics, Rensselaer Polytechnic Institute, 110 Eighth Street,
12180-3590 Troy, NY, USA

Received 23 February 2001; received in revised form 8 August 2001; accepted 8 April 2002

Abstract

This paper classifies all cyclic codes over Z_4 of length $2n, n$ odd. Descriptions are given in terms of discrete Fourier transforms, generator polynomials, parity check matrices, and the concatenated $(a+b|b)$ construction. Some results about the minimum Lee weights of these codes and self-dual codes are also included. © 2003 Elsevier Science B.V. All rights reserved.

Keywords: Cyclic codes; Z_4-linear codes; Galois rings

0. Introduction

Recently the discovery of good nonlinear binary codes that come from Z_4-linear codes via the Gray map (developed in [6]) motivated the study of codes over rings in general. In particular, much has been written about cyclic and extended cyclic codes over rings. Calderbank and Sloane [3], Rajan and Siddiqui [10], and Kanwar and Lopez-Permouth [7] give complete presentations of cyclic codes over integer residue rings Z_m using generator polynomials and discrete Fourier transforms, respectively. Blackford [1] and Wan [14] give a description of cyclic codes over the Galois rings $GR(p^a, m)$. Bonnecaze and Udaya [11] describe cyclic codes over the ring $F_2 + uF_2$, where $u^2 = 0$. Cyclic codes over Z_4 of odd length were thoroughly examined by Pless and Qian [9]. However, in all of these cases, it is assumed that the codelength is relatively prime to the characteristic of the ring. In this paper, we wish to study a class of codes in which the characteristic of the ring's residue field divides the codelength, namely the cyclic codes over Z_4 of length $2n$, when n is odd.

Cyclic codes of length n over a field of characteristic p, where p divides n are called *repeated-root cyclic codes* and have been studied by Castagnoli et al. [5] and

E-mail address: blackj@rpi.edu (T. Blackford).

0166-218X/03/$ - see front matter © 2003 Elsevier Science B.V. All rights reserved.
PII: S0166-218X(02)00434-1

Van Lint [13] among others. They have shown that these codes have a concatenated construction and are asymptotically bad. However, in a few cases they are optimal, and in some cases they are subcodes of Reed–Muller codes with the same minimum weight as their parent code. Cyclic codes over Z_4 also have interesting properties, in part because of their algebraic structure. In particular, not all cyclic codes of this type are principally generated. We classify these codes using a transform approach, and we will show that they can be viewed as coming from constacyclic codes over a local ring via an analogue of the Gray map. We will also give information about their size, duals, minimum Lee distances and generator polynomials. We also give some examples of self-dual codes.

It should be noted that a certain subclass of cyclic codes over Z_4, namely the minimal cyclic codes, was discussed in [2,12] in the context of quadriphase sequence design.

Throughout this paper, n is an odd positive integer.

1. Basic structure

Recall a linear code of length N over a commutative ring R is *constacyclic* if for some unit $a \in R$, the code is invariant under the automorphism

$$(c_0, c_1, \ldots, c_{N-1}) \mapsto (ac_{N-1}, c_0, \ldots, c_{N-2}).$$

In the case $a = 1$, we say that the code is cyclic. Constacyclic codes of length N over R can be identified as ideals in the quotient ring $R[X]/(X^N - a)$ via the isomorphism from R^N to $R[X]/(X^N - a)$ defined by

$$(c_0, c_1, \ldots, c_{N-1}) \mapsto c_0 + c_1X + \cdots + c_{N-1}X^{N-1}.$$

In the case where $R = F_q$, $a = 1$ and $(N, q) = 1$, the ideals are of the form $\langle f \rangle$, where f is a divisor of $X^N - 1$ in $F_q[X]$. In the case $R = Z_4$ and N is odd, every cyclic code is of the form $\langle f, 2g \rangle$, where $g|f|X^N - 1$ in $Z_4[X]$ and f, g are monic polynomials [3]. (It has been shown that these ideals are principal.) These codes are easy to classify since $X^N - 1$ has a unique factorization in $Z_4[X]$. However, $Z_4[X]$ is not a unique factorization ring, and $X^N - 1$ can factor different ways if N is even. For example,

$$\begin{aligned} X^4 - 1 &= (X - 1)(X + 1)(X^2 + 1), \\ &= (X - 1)^2(X^2 + 2X - 1). \end{aligned}$$

Thus classifying cyclic codes of even length using generator polynomials can be difficult. Instead, we begin by using a transform approach, and return to generator polynomials later.

This paper will focus on codes over Z_4 of length $2n$, in which n is an odd integer. (This is called an *oddly even* length.)

We introduce the polynomial residue ring $\mathscr{R}$, defined by

$$\mathscr{R} := \frac{Z_4[u]}{(u^2 - 1)}.$$

There exists a natural isomorphism ψ: $\mathscr{R}^n \to (Z_4)^{2n}$, defined by the rule

$$\psi(a_0 + b_0u, a_1 + b_1u, \ldots, a_{n-1} + b_{n-1}u) = (a_0, a_1, \ldots, a_{n-1}, b_0, b_1, \ldots, b_{n-1}).$$

A cyclic shift of a vector in $(Z_4)^{2n}$ corresponds to a constacyclic shift of its ψ-preimage under the constant u.

$$\begin{aligned}&\psi(u[a_{n-1}+b_{n-1}u], a_0+b_0u, \ldots, a_{n-2}+b_{n-2}u)\\ &\quad=\psi(b_{n-1}+a_{n-1}u, a_0+b_0u, \ldots, a_{n-2}+b_{n-2}u)\\ &\quad=(b_{n-1}, a_0, a_1, \ldots, a_{n-2}, a_{n-1}, b_0, \ldots, b_{n-2})\end{aligned}$$

Thus we get the following theorem.

Theorem 1. *Cyclic codes over Z_4 of length $2n$ correspond to constacyclic codes over $\mathscr{R}$* modulo X^n-u *via the isomorphism defined by the commutative diagram.*

$$\begin{tikzcd}\dfrac{\mathscr{R}[X]}{(X^n-u)} \arrow[r, "\psi"] \arrow[d] & \dfrac{Z_4[X]}{(X^{2n}-1)} \arrow[d] \\ \mathscr{R}^n \arrow[r, "\psi"] & (Z_4)^{2n}\end{tikzcd}$$

where the vertical maps correspond to the bijections between vectors and polynomials.

We shall see shortly that $\mathscr{R}$ is a finite local ring, and so by Hensel's Lemma, X^n-u factors uniquely as $f_1\ldots f_r$ in $\mathscr{R}[X]$, where the f_i's are monic, irreducible and pairwise relatively prime. By the Chinese Remainder Theorem,

$$\frac{\mathscr{R}[X]}{(X^n-u)} \cong \frac{\mathscr{R}[X]}{(f_1)} \oplus \cdots \oplus \frac{\mathscr{R}[X]}{(f_r)}.$$

We would like to study the rings $\mathscr{R}[X]/(f_i)$ in more detail.

1.1. Galois rings

We begin by recalling the Galois rings of characteristic 4 described in [6,8], and several other sources. If $h(X)$ is a monic basic irreducible polynomial in $Z_4[X]$ of degree m that divides $X^{2^m-1}-1$, then

$$GR(4,m)=\frac{Z_4[X]}{(h(X))}.$$

It is a local ring with maximal ideal $\langle 2\rangle$ and residue field $GF(2^m)$. The polynomial h can be chosen so that $\zeta=X+(h(X))$ is a primitive (2^m-1)st root of unity, and the set $\mathscr{T}_m=\{0,1,\zeta,\ldots,\zeta^{2^m-2}\}$, called the Teichmuller set of representatives of $GR(4,m)$, is a complete set of coset representatives of $GR(4,m)$ modulo 2. Each $\lambda\in GR(4,m)$ has a unique 2-adic expansion $a+2b$, where $a,b\in\mathscr{T}_m$. The Frobenius automorphism f of $GR(4,m)$ is defined $\lambda^f=a^2+2b^2$, and it generates the group of automorphisms of $GR(4,m)$ fixing Z_4, which is cyclic of order m. The trace map from $GR(4,m)$ to Z_4 is defined as follows:

$$T_m(\lambda)=\lambda+\lambda^f+\cdots+\lambda^{f^{m-1}}.$$

Next, we define an extension ring, $\mathscr{R}_4(u,m)$, to be

$$\mathscr{R}_4(u,m)=\frac{GR(4,m)[u]}{(u^2-1)}.$$

Note that $\mathscr{R}_4(u,1)=\mathscr{R}$, and that $\mathscr{R}_4(u,m)$ can also be defined to be $GR(4,m)\oplus uGR(4,m)$, with $u^2=1$. Of course any element of this ring must be of the form $\lambda=a_0+a_1u$, where $a_0,a_1\in GR(4,m)$, and $\lambda=0$ if and only if $a_0=a_1=0$. If $\lambda\in\mathscr{R}_4(u,m)$, let $\bar{\lambda}$ denote λ reduced modulo 2.

We now give some results about the ideal structure of this ring.

Lemma 1. *Let $R=\mathscr{R}_4(u,m)$.*

1. *R is a local ring with maximal ideal $\langle 2,u-1\rangle$ and residue field $GF(2^m)$.*
2. *The ideals of R consist of $\langle 0\rangle,\langle 1\rangle,\langle 2\rangle,\langle 2,u-1\rangle,\langle 2u+2\rangle$, and $\langle u-1+2t\rangle$, where $t\in\mathscr{T}_m$.*
3. *Every element $\lambda\in R$ can be uniquely expressed in the form*

$$\lambda=a+2b+(u-1)c+(2u+2)d,$$

where $a,b,c,d\in\mathscr{T}_m$.

Proof. (1) Clearly $R/2R\cong GF(2^m)[u]/(u^2+1)$. It is well known that this is a local ring with maximal ideal $\langle\overline{u+1}\rangle$ and residue field $GF(2^m)$.

(2) Let I be a nonzero proper ideal of R. If $I\subseteq 2R$, then either $I=\langle 2\rangle$ or $\langle 2u+2\rangle$, since in general the ideals of $GF(2^m)[X]/(X^{2^a}-1)$ are precisely of the form $\langle X-1\rangle^k$, for $0\leqslant k\leqslant 2^a$. Suppose $I\nsubseteq 2R$. Then $\bar{I}$, the ideal of I reduced modulo 2 must be $\langle\overline{u+1}\rangle$, Therefore, I must include some element of the form $u-1+2b$, for some $b\in\mathscr{T}_m$ (by the division algorithm for local commutative rings). Thus $\langle u-1+2b\rangle\subseteq I$. If $I\neq\langle u-1+2b\rangle$, then $u-1+2c\in I$ for some $c\in\mathscr{T}_m$, $c\neq b$; then $2(c-b)\in I$, which implies $\langle 2\rangle\subseteq I$, which implies $I=\langle 2,u-1\rangle$. Thus the list of ideals is exhaustive and distinct.

(3) Every element of R can be expressed in the form $\lambda_0+\lambda_1(u-1)$, where $\lambda_0,\lambda_1\in GR(4,m)$. Using the 2-adic expansions of λ_i, we get the desired expansion. □

We can extend the Frobenius automorphism from $GR(4,m)$ to $\mathscr{R}_4(u,m)$ by defining $(\lambda_0+\lambda_1u)^f=\lambda_0^f+\lambda_1^fu$. We can also extend the trace map to define $T_m:\mathscr{R}(u,m)\to\mathscr{R}$ by the rule

$$T_m(\lambda)=\lambda+\lambda^f+\cdots+\lambda^{f^{m-1}}.$$

1.2. A discrete Fourier transform

We now introduce a discrete Fourier transform that will help in classifying cyclic codes over Z_4 of length $2n$ (n odd) and determine their concatenated structure. For the remainder of this paper, assume m to be the order of 2 modulo n, let ζ be a primitive

nth root of unity in the Galois ring $GR(4,m)$. Also, let $cl_2(i)$ be the 2-cyclotomic coset of i modulo n, and let m_i be the size of this coset.

Definition 1. Let $\mathbf{a} \in (Z_4)^{2n}$. The discrete Fourier transform of $\mathbf{a}$ is the vector $[A_0, A_1, \ldots, A_{n-1}] \in \mathscr{R}_4(u,m)^n$, where

$$A_i = a(u\zeta^i) = \sum_{j=0}^{2n-1} a_j u^j \zeta^{ij},$$

for $0 \leqslant i \leqslant n$. Define the Mattson–Solomon (MS) polynomial of $\mathbf{a}$ to be the polynomial

$$\sum_{i=0}^{n-1} A_{n-i} Z^i.$$

It is easy to check that $A_i \in \mathscr{R}_4(u, m_i)$, and that $A_{2i} = A_i^f$ for all i, where subscripts are calculated modulo n.

Define the discrete Fourier transform and Mattson–Solomon polynomial of an element of $Z_4[X]/(X^{2n}-1)$, to be the transform and Mattson–Solomon polynomial of its corresponding vector in $(Z_4)^{2n}$, respectively.

Lemma 2 (Inversion formula). *Suppose* $\mathbf{a} \in (Z_4)^{2n}$, *and* $A(Z)$ *is its MS polynomial. Then*

$$\mathbf{a} = \psi[(1,u,1,u,\ldots,1) * \frac{1}{n}(A(1), A(\zeta), \ldots, A(\zeta^{n-1}))],$$

where $*$ *denotes componentwise multiplication of vectors.*

Proof. Let $0 \leqslant t \leqslant n-1$. Then

$$\begin{aligned} A(\zeta^t) &= \sum_{i=0}^{n-1} A_i \zeta^{-it} \\ &= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{2n-1} a_j u^j \zeta^{ij} \right) \zeta^{-it} \\ &= \sum_{j=0}^{2n-1} a_j u^j \sum_{i=0}^{n-1} \zeta^{i(j-t)} \\ &= n[a_t u^t + a_{t+n} u^{t+n}]. \end{aligned}$$

The last line follows from the well known fact that $\sum_{i=0}^{n-1} \zeta^{ki} = 0$ unless $k \equiv 0 \bmod n$. Hence $u^{-t}(1/n)A(\zeta^t) = a_t + u a_{t+n}$. Noting that $u^{-t} = u$ if t is odd and $u^{-t} = 1$ if t is even, we get the result. □

Lemma 3. *If* $a(X), b(X) \in Z_4[X]/(X^{2n}-1)$, *and* $A(Z), B(Z)$ *are their respective MS polynomials, then*

1. *The MS polynomial of* $a(X)+b(X)$ is $A(Z)+B(Z)$.
2. *The MS polynomial of* $a(X)b(X)$ $(\operatorname{mod} X^{2n}-1)$ is $A(Z)*B(Z)=\sum A_iB_iZ^i$ ($*$ *denotes componentwise multiplication.*)
3. *The MS polynomials of* 0 *and* 1 *are* 0 *and* $\sum_{i=0}^{n-1} Z^i$, *respectively.*
4. *The MS polynomial of* $Xa(X)$ *is* $uA(\zeta^{-1}Z)$.

Proof. (1) and (3) are clear. (2) follows from the fact that $u\zeta^i$ is a root of $X^{2n}-1$. (4) is a specific case of (2) with $b(X)=X$. □

Let $\mathscr{A}$ be the set of all transform vectors $[A_0,\ldots,A_{n-1}]\in\mathscr{R}_4(u,m)^n$ such that $A_{2i}=A_i^f$ for all i. We make $\mathscr{A}$ a ring via componentwise addition and multiplication. Then

$$\mathscr{A}\cong\oplus_{i\in I}\,\mathscr{R}_4(u,m_i),$$

where I is a complete set of 2-cyclotomic coset representatives modulo n. Indeed, this is true by noting that for every $i\in I$, $A_i\in\mathscr{R}(u,m_i)$ and A_{i2^k} is completely determined by A_i.

Theorem 2. *The map* γ: $Z_4[X]/(X^{2n}-1)\to\mathscr{A}$ *is a ring isomorphism*, *where* $\gamma(a(X))=[A_0,\ldots,A_{n-1}]$.

Proof. γ is a ring homomorphism by Lemma 3, and the Inversion Formula shows that γ is one-to-one. To show that γ is surjective, let $A=[A_0,\ldots,A_{n-1}]\in\mathscr{A}$, and $A(Z)=\sum_{i=0}^{n-1}A_iZ^i$. We need only show that the vector

$$\mathbf{a}=\psi[(1,u,1,\ldots,1)*\frac{1}{n}(A(1),A(\zeta),\ldots,A(\zeta^{n-1}))]$$

has components in Z_4, and then if $a(X)$ is the corresponding polynomial of $\mathbf{a}$, $\gamma(a(X))=A$. In fact, it is sufficient to show that $A(\zeta^t)\in\mathscr{R}_4(u,1)$. But this is clear, since

$$A(\zeta^t)=\sum_{i\in I}T_{m_i}(A_i\zeta^{it})\in\mathscr{R}_4(u,1).$$

This completes the proof. □

We now wish to use this fact to describe a cyclic code in terms of its generator polynomials. First, recall that *if n is odd*, the polynomial X^n-1 factors uniquely into monic irreducible polynomials f_i in $Z_4[X]$,

$$X^n-1=f_1f_2\ldots f_r,$$

where r is the number of 2-cyclotomic cosets modulo n. We define $f(X)$ to be the minimal polynomial of ζ^i over Z_4 if f is the unique monic irreducible polynomial divisor of X^n-1 that has ζ^i as a root. It is also the only monic polynomial of least degree having ζ^i as a root.

Lemma 4. *Let f_j be the minimal polynomial of ζ^j in $Z_4[X]$. Then*

1. $f_j(u\zeta^j) \equiv 0 \pmod{\langle u-1\rangle}$,
2. $f_j([u\zeta^j]^2) = 0$,
3. *If $g \in Z_4[X]$ is a monic polynomial such that $g = f_j + 2h$, where $deg(h) < deg(f_j)$, then $g(u\zeta^j) \equiv 0 \pmod{\langle u-1+2t\rangle}$ for some unique $t \in \mathscr{T}_m$.*

Proof. (1) Write $f_j(X) = f_{0,j}(X) + Xf_{1,j}(X)$, where $f_{0,j}, f_{1,j}$ are polynomials in X^2. Note neither $f_{0,j}$ nor $f_{1,j}$ can have ζ^j as a root, since this contradicts the minimality of f_j. Then

$$\begin{aligned} f_j(u\zeta^j) &= f_{0,j}(\zeta^j) + u\zeta^j f_{1,j}(\zeta^j) \\ &= -\zeta^j f_{1,j}(\zeta^j) + u\zeta^j f_{1,j}(\zeta^j) \\ &= (u-1)\zeta^j f_{1,j}(\zeta^j). \end{aligned}$$

This proves (1). (2) is clear since $f_j(\zeta^{2j}) = f_j(\zeta^j)^f = 0$. To prove (3), note $2h(u\zeta^j) \not\equiv 0 \pmod{\langle u-1\rangle}$, since otherwise $h(\zeta^j) \equiv 0 \bmod 2$, again contradicting the minimality of f_j. Thus using this fact and the division algorithm for $GR(4,m)[u]$, we have that for some $A, B, C \in \mathscr{T}_m$, $A \neq 0$, we have

$$\begin{aligned} g(u\zeta^i) &= (A+2B)(u-1) + 2C \\ &= (A+2B)(u-1) + 2CA^{-1}(A+2B) \\ &= (A+2B)[(u-1) + 2CA^{-1}]. \end{aligned}$$

So $g(u\zeta^j) \in \langle u-1+2CA^{-1}\rangle$. In fact, C is uniquely determined by h, so the proof is complete. □

Theorem 3. *Let n be odd and $\mathscr{C}$* be an ideal in $Z_4[X]/(X^{2n}-1)$. *Then $\mathscr{C}$ is of the form*

$$\langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $X^n - 1 = a_1a_2a_3bcd$, a_1, a_2, a_3, b, c and d are monic and pairwise relatively prime in $Z_4[X]$, and $\tilde{b}(X)$ is a monic polynomial such that $\tilde{b} \equiv b$ $(\bmod\, 2Z_4[X])$.

Proof. Let I be the set of distinct 2-cyclotomic coset representatives modulo n. Via the map γ, we know $\mathscr{C}$ is isomorphic to the direct sum

$$\bigoplus_{i\in I} \mathscr{C}_i,$$

where $\mathscr{C}_i$ is an ideal of the ring $\mathscr{R}_4(u, m_i)$, and this ideal consists of all elements $g(u\zeta^i)$, where $g(X) \in \mathscr{C}$. (Hereafter this sum will be called the *decomposition* of $\mathscr{C}$.) Define the polynomials a_1, a_2, a_3, b, c to be products of monic divisors f_i of $X^n - 1$ based on the following rules:

- $f_i \mid a_1$ if $\mathscr{C}_i = \langle 0 \rangle$,
- $f_i \mid a_2$ if $\mathscr{C}_i = \langle 2u+2 \rangle$,
- $f_i \mid a_3$ if $\mathscr{C}_i = \langle 2 \rangle$,
- $f_i \mid c$ if $\mathscr{C}_i = \langle 2, u-1 \rangle$,
- $f_i \mid b$ if $\mathscr{C}_i = \langle u-1+2t \rangle$ for some $t \in \mathscr{T}_m$.

If $g(X)$ is in the ideal

$$\langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

then by using the previous lemma, we see that $g(u\zeta^i) \in \mathscr{C}_i$ for all $i \in I$. (The choice of t depends on the choice of $\tilde{b}$.) □

Corollary 1. *If I is a complete set of 2-cyclotomic coset representatives modulo n (n odd) and m_i is the size of the 2-cyclotomic coset containing i, then the number of cyclic codes over Z_4 of length $2n$ is*

$$\prod_{i \in I} (5 + 2^{m_i}).$$

Proof. The number of ideals in ring $\mathscr{R}_4(u, m_i)$ is $5 + 2^{m_i}$. (The 2^{m_i} ideals are of the form $\langle u-1+2t \rangle$, $t \in \mathscr{T}_{m_i}$.) □

It is interesting to note that the class of cyclic codes of even length is a much larger class than the cyclic codes of odd length. For example, there are only 27 cyclic codes of length 7, but 1183 cyclic codes of length 14. Also, there are 31,525,197,391,593,507 distinct cyclic codes of length 106 over Z_4. This is largely due to the fact that there are 2^{52} possible monic liftings of the polynomial $X^{52} + \cdots + X + 1$ in $Z_4[X]$, which in turn correspond to the 2^{52} choices of $t \in \mathscr{T}_{52}$. However, as we shall see in Section 3, this does not necessarily guarantee codes with good weight properties.

2. The size and dual of cyclic codes

2.1. The size of cyclic codes

Lemma 5. *If $\mathscr{C}$ is a cyclic code of length $2n$ over Z_4, and*

$$\mathscr{C} = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd = X^n - 1$ and $\tilde{b}$ is monic and $\tilde{b} \equiv b \pmod{2Z_4[X]}$, then $\mathscr{C}$ has size $4^{k_1}2^{k_2}$, where

$$k_1 = 2deg(d) + deg(b) + deg(c),$$

$$k_2 = deg(a_2) + 2deg(a_3) + deg(c).$$

Proof. If I is a complete set of 2-cyclotomic coset representatives modulo n, then the size of $\mathscr{C}$ is

$$\prod_{i\in I} |\mathscr{C}_i|,$$

where $\mathscr{C}_i$ is the ideal of $\mathscr{R}_4(u, m_i)$ generated by the set $\{g(u\zeta^i)\colon\ g(X)\in\mathscr{C}\}$. Note

- if $\mathscr{C}_i=\langle 1\rangle$, then $d(\zeta^i)=0$ and $|\mathscr{C}_i|=4^{2m_i}$,
- if $\mathscr{C}_i=\langle 2, u-1\rangle$, then $c(\zeta^i)=0$ and $|\mathscr{C}_i|=4^{m_i}2^{m_i}$,
- if $\mathscr{C}_i=\langle 2\rangle$, then $a_3(\zeta^i)=0$ and $|\mathscr{C}_i|=4^{m_i}$,
- if $\mathscr{C}_i=\langle u-1+2t\rangle$, then $b(\zeta^i)=0$ and $|\mathscr{C}_i|=4^{m_i}$,
- if $\mathscr{C}_i=\langle 2u+2\rangle$, then $a_2(\zeta^i)=0$ and $|\mathscr{C}_i|=2^{m_i}$,
- if $\mathscr{C}_i=\langle 0\rangle$, then $a_1(\zeta^i)=0$ and $|\mathscr{C}_i|=1$.

Calculating the product, we get the exponents k_1 and k_2. □

2.2. The duals of cyclic codes

To calculate the dual of a cyclic code of length $2n$, we make several preliminary observations. First, note that if $\mathscr{U}$ and $\mathscr{V}$ are constacyclic codes in $\mathscr{R}[X]/\langle X^n-u\rangle$, then $\mathscr{U}$ and $\mathscr{V}$ are dual if and only if $\psi(\mathscr{U})$ and $\psi(\mathscr{V})$ are dual in $(Z_4)^{2n}$. Indeed, if $\mathbf{u}\in\mathscr{U}$ and $\mathbf{v}\in\mathscr{V}$, where $\mathbf{u}=(a_0+b_0u,\ldots,a_{n-1}+b_{n-1}u)$ and $\mathbf{v}=(r_0+s_0u,\ldots,r_{n-1}+s_{n-1}u)$, then

$$\langle \mathbf{u},\mathbf{v}\rangle=\sum_{i=0}^{n-1}(a_ir_i+b_is_i)+u\sum_{i=0}^{n-1}(r_ib_i+a_is_i).$$

The first sum is $\langle\psi(\mathbf{u}),\psi(\mathbf{v})\rangle$ and the second sum is $\langle\psi(\mathbf{u}),\sigma(\psi(\mathbf{v}))\rangle$, where σ represents a cyclic shift of n coordinates. Thus we see that if $\psi(\mathscr{U})$ and $\psi(\mathscr{V})$ are cyclic and $\mathscr{U}$ and $\mathscr{V}$ are dual, then $\psi(\mathscr{U})$ and $\psi(\mathscr{V})$ are also dual. Therefore we see it is sufficient to find the dual of the corresponding constacyclic code over $\mathscr{R}$.

Lemma 6. *If* $\mathbf{u},\mathbf{v}\in\mathscr{R}^n$, and $U(Z)=\sum U_iZ^i$ *and* $V(Z)=\sum V_iZ^i$ *are the respective MS polynomials of* $\psi(\mathbf{u})$ *and* $\psi(\mathbf{v})$, *and* $U_iV_{n-i}=0$ *for* $0\leqslant i\leqslant n$, *then* $\langle\mathbf{u},\mathbf{v}>=0$.

Proof. Recall from the Inversion Formula that if $U(Z)$ is the MS polynomial for $\psi(\mathbf{u})$, then for $0\leqslant t\leqslant n-1$,

$$u_t=u^t\frac{1}{n}U(\zeta^t).$$

Thus,

$$\begin{aligned}\sum_{i=0}^{n-1}u_iv_i&=\frac{1}{n^2}\sum_{i=0}^{n-1}U(\zeta^i)V(\zeta^i)\\&=\frac{1}{n^2}\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}U_j\zeta^{-ij}\right)\left(\sum_{k=0}^{n-1}V_k\zeta^{-ik}\right)\end{aligned}$$

$$= \frac{1}{n^2}\sum_{j=0}^{n-1} U_j \sum_{k=0}^{n-1} V_k \sum_{i=0}^{n-1} \zeta^{i(j+k)}$$

$$= \frac{1}{n^2}\sum_{j=0}^{n-1} U_j V_{n-j} n$$

$$= 0. \qquad \square$$

Thus if $\mathscr{C}$ and $\mathscr{D}$ are cyclic codes of length $2n$ over Z_4, and if they have the property that $C_i D_{n-i} = 0$ for MS polynomials $\sum C_i Z^i$ of $\mathscr{C}$ and $\sum D_i Z^i$ of $\mathscr{D}$, then $\mathscr{D} \subseteq \mathscr{C}^\perp$. Note that the coefficient C_i comes from the ideal $\mathscr{C}_{n-i}$ of $\mathscr{R}_4(u, m_i)$.

We also remark that in the ring $\mathscr{R}_4(u,m)$, $\langle 0\rangle$ is the largest annihilator of $\langle 1\rangle$, $\langle 2, u-1\rangle$ is the largest annihilator of $\langle 2u+2\rangle$, $\langle 2\rangle$ is the largest annihilator of itself, and if $t \in \mathscr{T}_m$, then $\langle u-1+2t\rangle$ is the largest annihilator of $\langle u-1+2s\rangle$, where $s \in \mathscr{T}_m$ is the unique element such that $s \equiv t+1 \pmod 2$.

Lemma 7. *Let $\mathscr{C}$ be a cyclic code over Z_4 of length $2n$ (n odd), $\mathscr{C}^\perp$ be its dual, and let*

$$\mathscr{C} = \bigoplus_{i \in I} \mathscr{C}_i, \quad \mathscr{C}^\perp = \bigoplus_{i\in I} \mathscr{D}_i$$

be their respective decompositions. Then $\mathscr{C}^\perp$ is defined by the properties

- $\mathscr{D}_i = \langle 1\rangle$ *if* $\mathscr{C}_{n-i} = \langle 0\rangle$,
- $\mathscr{D}_i = \langle 2, u-1\rangle$ *if* $\mathscr{C}_{n-i} = \langle 2u+2\rangle$,
- $\mathscr{D}_i = \langle 2\rangle$ *if* $\mathscr{C}_{n-i} = \langle 2\rangle$,
- $\mathscr{D}_i = \langle u-1+2t\rangle$ *if* $\mathscr{C}_{n-i} = \langle u-1+2s\rangle$ *and* $s \equiv t+1 \bmod 2$,
- $\mathscr{D}_i = \langle 2u+2\rangle$ *if* $\mathscr{C}_{n-i} = \langle 2, u-1\rangle$,
- $\mathscr{D}_i = \langle 0\rangle$ *if* $\mathscr{C}_{n-i} = \langle 1\rangle$.

Proof. Since $\mathscr{C}_i \mathscr{D}_{n-i} = 0$ for all i, then if $\sum C_i Z^i$ and $\sum D_i Z^i$ are MS polynomials of $\mathscr{C}$ and $\mathscr{D}$, respectively, $C_i D_{n-i} = 0$ for all $0 \leqslant i \leqslant n$. Thus $\mathscr{D} \subseteq \mathscr{C}^\perp$ by the previous lemma. Also, $|\mathscr{C}_i||\mathscr{D}_{n-i}| = 4^{2m_i}$ for all $i \in I$, so that $|\mathscr{C}||\mathscr{D}| = 4^{2n}$. Hence $\mathscr{D} = \mathscr{C}^\perp$. $\square$

Lemma 8. *If $b(X)$ is a monic divisor of $X^n - 1$ in $Z_4[X]$, n odd, $\tilde{b}(X)$ is monic and $\tilde{b}(X) \equiv b(X) \pmod{2Z_4[X]}$, then there is a unique monic polynomial $\tilde{b}_\# \in Z_4[X]$ such that $b(X^2) = \tilde{b}(X)\tilde{b}_\#(X)$.*

Proof. Without loss of generality, assume that b is irreducible, so that it is the minimal polynomial of some element ζ^i. By the Division Algorithm for $Z_4[X]$, there exist $q(X), r(X)$ such that

$$b(X^2) = q(X)\tilde{b}(X) + r(X)$$

with $deg(r) < deg(b)$. Reducing modulo 2, we see that since $\bar{r}$ must be a multiple of $\bar{b}$ and $deg(\bar{r}) < deg(\bar{b})$, $r(X) \in 2Z_4[X]$. This also shows that $\bar{b} \equiv \bar{q} \pmod 2$. This implies that $q(u\zeta^i)\tilde{b}(u\zeta^i) \in \langle 2u+2\rangle$, and hence $r(u\zeta^i) \in \langle 2u+2\rangle$. Since the degree of r is less than that of the minimal polynomial of ζ^i, $r(X) = 0$. So $\tilde{b}_{\#}(X)$ can be defined to be $q(X)$.

To show uniqueness, assume that there are two monic polynomials f, g such that $\tilde{b}f = \tilde{b}g = b(X^2)$. If $\tilde{b}(u\zeta^i) \in \langle u-1+2A\rangle$ for some $A \in \mathscr{T}_m$, then there is a unique $B \in \mathscr{T}_m$ such that $(u-1+2A)(u-1+2B) = 0$, and so $f(u\zeta^i)$ and $g(u\zeta^i)$ must both be in $\langle u-1+2B\rangle$. But since $f-g$ is of degree strictly less than the degree of b, then $f = g$. □

Recall that if $f(X)$ is a polynomial of degree m, the reciprocal polynomial of f is $f^*(X) = X^m f(X^{-1})$, so that the roots of f^* are the reciprocals of the roots of f. Note that if $\tilde{b}$ is a lift of a divisor of X^n-1, then $(\tilde{b}^*)_{\#} = (\tilde{b}_{\#})^*$.

We are now ready to give the dual of a cyclic code $\mathscr{C}$ in terms of its polynomial generators.

Theorem 4. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4, and*

$$\mathscr{C} = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd = X^n-1$, $\tilde{b}$ is monic and $\tilde{b} \equiv b \pmod{2Z_4[X]}$, then

$$\mathscr{C}^{\perp} = \langle d^*(X^2)c^*(X^2)a_3^*(X^2)\tilde{b}_{\#}^*(X)a_2^*(X), 2d^*(X^2)c^*(X)b^*(X)\rangle.$$

Proof. Let $\mathscr{D}$ be the second ideal given above, and let $\mathscr{D}_i = \{g(u\zeta^i)\colon g(X) \in \mathscr{D}\}$, and define $\mathscr{C}_i$ in the same way. If $\mathscr{C}_i = \langle 2u+2\rangle$, then $a_2(\zeta^i) = 0$, which means $a_2^*(\zeta^{-i}) = 0$, which means $g(u\zeta^{-i}) \equiv 0 \bmod \langle 2, u-1\rangle$ for all $g(X) \in \mathscr{D}$, which means $\mathscr{D}_{n-i} = \langle 2, u-1\rangle$. Similarly, if $\mathscr{C}_i = \langle u-1+2t\rangle$, then $\tilde{b}(u\zeta^i) \in \langle u-1+2t\rangle$, $\tilde{b}^*(u\zeta^{-i}) \in \langle u-1+2t\rangle$, and $\tilde{b}_{\#}^*(u\zeta^{-i}) \in \langle u-1+2s\rangle$, where $s \equiv t+1 \pmod 2$, and thus $\mathscr{D}_{n-i} = \langle u-1+2s\rangle$. Using the same argument for the other cases, we see that $\mathscr{C}_i\mathscr{D}_{n-i} = 0$ for all i. According to the previous lemma, $\mathscr{D} = \mathscr{C}^{\perp}$. □

2.3. Parity check matrices

Parity check matrices can be used to describe and decode cyclic codes. For cyclic codes of oddly even length over Z_4, we can determine the parity check matrix by writing a codeword of the form $g(X) = g_0(X) + Xg_1(X)$, where g_0, g_1 are polynomials in X^2, and analyzing the quantity

$$g(u\zeta^i) = g_0(\zeta^i) + u\zeta^i g_1(\zeta^i).$$

For example, if $g(u\zeta^i) = 0$, then $g_0(\zeta^i) = g_1(\zeta^i) = 0$. If $g(u\zeta^i) \in \langle u-1+2t\rangle$ for some $t \in \mathscr{T}_m$, and $s = t+1 \pmod 2$, then since $(u-1+2s)(g_0(\zeta^i) + u\zeta^i g_1(\zeta^i)) = 0$, we see that

$$g_0(\zeta^i) + (-1+2s)\zeta^i g_1(\zeta^i) = 0,$$

$$g_0(\zeta^i) + (1+2t)\zeta^i g_1(\zeta^i) = 0.$$

Continuing in this way, we see that if

$$\mathscr{C} = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle$$

and $\mathbf{c} \in \mathscr{C}$, we can use the following rules for determining the parity check matrix.

- if $a_1(\zeta^s) = 0$, then $\mathbf{c}$ is orthogonal to
$$\begin{bmatrix} 1 & 0 & \zeta^{2s} & 0 & \zeta^{4s} & 0 & \cdots & \zeta^{(2n-2)s} & 0 \\ 0 & \zeta^s & 0 & \zeta^{3s} & 0 & \zeta^{5s} & \cdots & 0 & \zeta^{(2n-1)s} \end{bmatrix},$$
- if $a_2(\zeta^s) = 0$, then $\mathbf{c}$ is orthogonal to
$$\begin{bmatrix} 1 & -\zeta^s & \zeta^{2s} & -\zeta^{3s} & \cdots & \zeta^{(2n-2)s} & -\zeta^{(2n-1)s} \\ 2 & 0 & 2\zeta^{2s} & 0 & \cdots & 2\zeta^{(2n-2)s} & 0 \end{bmatrix},$$
- if $a_3(\zeta^s) = 0$, then $\mathbf{c}$ is orthogonal to
$$\begin{bmatrix} 2 & 0 & 2\zeta^{2s} & 0 & \cdots & 2\zeta^{(2n-2)s} & 0 \\ 0 & 2\zeta^s & 0 & 2\zeta^{3s} & \cdots & 0 & 2\zeta^{(2n-1)s} \end{bmatrix},$$
- if $c(\zeta^s) = 0$, then $\mathbf{c}$ is orthogonal to
$$\begin{bmatrix} 2 & 2\zeta^s & 2\zeta^{2s} & 2\zeta^{3s} & \cdots & 2\zeta^{(2n-1)s} \end{bmatrix},$$
- if $b(\zeta^s) = 0$, then $\mathbf{c}$ is orthogonal to
$$\begin{bmatrix} 1 & \gamma\zeta^s & \zeta^{2s} & \gamma\zeta^{3s} & \cdots & \zeta^{(2n-2)s} & \gamma\zeta^{(2n-1)s} \end{bmatrix},$$

  where $\gamma = 1 + 2t$, for the unique $t \in \mathscr{T}_m$ such that $\tilde{b}(u\zeta^s) \in \langle u - 1 + 2t\rangle$.

2.4. Some examples

Example 1. Suppose the codelength is $N = 6$, so $n = 3$. Let $\mathscr{C} = \langle (X^2 - 1)(X^2 + X - 1)\rangle$, and let ζ be a primitive 3rd root of unity so that $\zeta^2 + \zeta + 1 = 0$. The parity check matrix for this code is

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & \gamma\zeta & \zeta^2 & \gamma\zeta^3 & \zeta^4 & \gamma\zeta^5 \end{bmatrix},$$

where $\gamma = 1 + 2\zeta^2$. This is because $g(u\zeta) \in \langle u - 1 + 2\zeta^2\rangle$ for all $g(X) \in \mathscr{C}$. The dual of $\mathscr{C}$ is $< X^2 - X - 1 >$, and by the ring version of Delsarte's Theorem, we obtain a trace description of $\mathscr{C}^\perp$:

$$\mathscr{C}^\perp = \{(a, b, a, b, \ldots, b) + (T_2(\lambda(\gamma\zeta)^i))_{i=0}^{2n-1} : a, b \in Z_4, \lambda \in GR(4, 2)\}.$$

Example 2. Suppose the codelength is $N = 30$, so $n = 15$.

$$X^{15} - 1 = f_0 f_1 f_3 f_5 f_7 \in Z_4[X],$$

where f_i is the minimal polynomial of ζ^i (via the Hensel lift), and ζ is a primitive 15th root of unity, and $\zeta^4+\zeta+1\equiv 0 \pmod 2$. Let $\mathscr{C}$ be the ideal

$$\langle f_1(X^2)f_5(X^2)\tilde{f}_3(X), 2f_1(X^2)f_3(X)\rangle.$$

The lift of f_3 is defined in such a way that

$$\tilde{f}_3(u\zeta^3)\equiv 0 \pmod{\langle u-1+2\zeta\rangle}.$$

Then the parity check matrix for $\mathscr{C}$ is

$$\begin{bmatrix} 1 & 0 & \zeta^2 & 0 & \zeta^4 & 0 & \cdots & \zeta^{28} & 0 \\ 0 & \zeta & 0 & \zeta^3 & 0 & \zeta^5 & \cdots & 0 & \zeta^{29} \\ 1 & \gamma\zeta^3 & \zeta^6 & \gamma\zeta^9 & \zeta^{12} & \gamma\zeta^{15} & \cdots & \zeta^{(28)3} & \gamma\zeta^{(29)3} \\ 2 & 0 & 2\zeta^{10} & 0 & 2\zeta^{20} & 0 & \cdots & 2\zeta^{(28)5} & 0 \\ 0 & 2\zeta^5 & 0 & 2\zeta^{15} & 0 & 2\zeta^{25} & \cdots & 0 & 2\zeta^{(29)5} \end{bmatrix},$$

where $\gamma=1+2\zeta$.

The dual of $\mathscr{C}$ is $\mathscr{D}$, where $\mathscr{D}$ is defined to be the cyclic code such that for all $\mathbf{d}\in\mathscr{D}$,

$$d(u)=d(u\zeta)=0, \quad d(u\zeta^5)\equiv 0 \pmod 2$$

$$d(u\zeta^3)\equiv 0 \pmod{\langle u-1+2\zeta^4\rangle}.$$

Thus

$$\mathscr{C}^{\perp}=\langle f_0(X^2)f_1(X^2)f_5(X^2)\tilde{f}_{3\,\#}(X), 2f_0(X^2)f_1(X^2)f_3(X)\rangle.$$

Note f_3 is its own reciprocal polynomial.

2.5. Self-dual cyclic codes

It is now straightforward to determine the self-dual cyclic codes of length $2n$ over Z_4, where n is odd.

Lemma 9. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4, and $\mathscr{C}\cong\oplus\mathscr{C}_i$ is its decomposition, then $\mathscr{C}$ is self-dual if and only if $\mathscr{C}_i\mathscr{C}_{n-i}=0$ and $|\mathscr{C}_i||\mathscr{C}_{n-i}|=4^{2m_i}$ for all i.*

Proof. Clear. □

This means that if $\mathscr{C}_i=\langle 1\rangle$, $\mathscr{C}_{n-i}=\langle 0\rangle$. If $\mathscr{C}_i=\langle 2, u-1\rangle$, then $\mathscr{C}_{n-i}=\langle 2u+2\rangle$. If $\mathscr{C}_i=\langle 2\rangle$, then $\mathscr{C}_{n-i}=\langle 2\rangle$. If $\mathscr{C}_i=\langle u-1+2t\rangle$, then $\mathscr{C}_{n-i}=\langle u-1+2s\rangle$, where $s=t+1 \pmod 2$.

Observing the relationship between the ideals $\mathscr{C}_i$ and the generator polynomials given in the proof of Theorem 3, it is easy to deduce the next theorem.

Theorem 5. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4, and*

$$\mathscr{C} = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd = X^n - 1$, $\tilde{b}$ is monic and $\tilde{b} \equiv b \bmod 2Z_4[X]$, then $\mathscr{C}$ is self-dual if and only if $a_1 = d^*$, $a_2 = c^*$, $a_3 = a_3^*$, and $\tilde{b} = \tilde{b}_\#^*$.

Corollary 2. *If $-1 \equiv 2^a \pmod{n}$, for some a, then the only cyclic self-dual code of length $2n$ over Z_4* is $2(Z_4)^{2n}$.

Proof. In this case $\mathscr{C}_i = \mathscr{C}_{n-i}$ for all i, so $\mathscr{C}_i = \langle 2\rangle$ for all i. □

Example. There are 13 self-dual codes of length 14 over Z_4. In the decomposition of each of these codes, $\mathscr{C}_0 = \langle 2\rangle$, $\mathscr{C}_1$ and $\mathscr{C}_3$ are chosen so they annihilate each other. If $X^7 - 1 = f_0f_1f_3$, where $f_0 = X - 1$, $f_1 = X^3 + 2X^2 + X - 1$, $f_3 = X^3 - X^2 + 2X - 1$, then the first five self-dual codes are

$$\langle f_1(X^2)f_0(X^2), 2f_1(X^2)\rangle, \quad \langle f_3(X^2)f_0(X^2), 2f_3(X^2)\rangle,$$

$$\langle f_1(X^2)f_0(X^2)f_3(X), 2f_1(X)\rangle, \quad \langle f_3(X^2)f_0(X^2)f_1(X), 2f_3(X)\rangle,$$

$$\langle 2\rangle$$

and the other eight are of the forms $\langle f_0(X^2)\tilde{f}_1(X)(\tilde{f}_1)_\#^*(X)\rangle$. For example, the code

$$\langle X^8 + X^7 + 2X^6 + 2X^4 + 2X^2 - X + 1, 2(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1)\rangle$$

is self-dual (but has a minimum Lee weight of only 4).

3. Minimum Lee weights of cyclic codes

We now present some results on the minimum Lee weights of cyclic codes of length $2n$ over Z_4. Unfortunately, like their binary counterparts, quaternary cyclic codes of even length turn out to be asymptotically bad, and in many cases their weights are no better than the weight of a cyclic code of odd length. However, the fact that the class of oddly even cyclic codes over Z_4 is quite large should give some hope that some good codes exist for certain lengths.

Recall that in the ring Z_4, the Lee weight of 0,1,2 and 3 is 0,1,2 and 1 respectively. The Lee weight of a vector in Z_4^N is the rational sum of the Lee weights of its components. The smallest nonzero Lee weight among the codewords of $\mathscr{C}$ is called the minimum Lee weight of $\mathscr{C}$. It is significant because the minimum Lee weight of $\mathscr{C}$ is equal to the minimum Hamming distance of the $\phi(\mathscr{C})$, the binary Gray image of $\mathscr{C}$ [6]. A code over Z_4 of length N with M codewords and minimum Lee weight d is an (N, M, d) code.

As with repeated-root cyclic codes, codes of oddly even length over Z_4 have a concatenated structure, in which codewords are composed of codewords from cyclic codes of length n. To avoid confusion, we make the following notation: if f is a polynomial of degree less than n, let $\langle f\rangle_n$ denote the ideal generated by f in $Z_4[X]/(X^n-1)$. If no subscript is given, then $\langle f\rangle$ is the ideal generated by f in $Z_4[X]/(X^{2n}-1)$.

Let $\mathbf{c}\in(Z_4)^{2n}$ have MS polynomial $A(Z)+(u-1)B(Z)$, where $A(Z)$ and $B(Z)$ have coefficients in $GR(4,m)$. By the Inversion Formula, $\mathbf{c}$ is permutation equivalent to a vector of the form $(\mathbf{a}-\mathbf{b}|\mathbf{b})$, where $\mathbf{a}$ and $\mathbf{b}$ are vectors of length n corresponding to polynomials $A(Z)$ and $B(Z)$, respectively.

Now assume that $\mathbf{c}$ is a codeword of the code

$$\langle a_1(X^2)a_2(X^2)a_3(X^2)b(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd=X^n-1$. We can determine which cyclic codes that $\mathbf{a}$ and $\mathbf{b}$ come from by looking at the coefficients of their MS polynomials.

To begin, if ζ^i is a root of a_1, then $A_{-i}=B_{-i}=0$, and $\mathbf{a},\mathbf{b}\in\langle a_1\rangle_n$. If ζ^i is a root of a_2, then $A_{-i}=0$ and $B_{-i}\equiv 0 \pmod 2$, so $\mathbf{a}\in\langle a_2\rangle_n$ and $\mathbf{b}\in\langle a_2,2\rangle_n$. Continuing in this way, we also see that $\mathbf{a}$ must lie in $\langle a_3,2\rangle_n,\langle b\rangle_n$, and $\langle c,2\rangle_n$, whereas $\mathbf{b}$ must lie in $\langle a_3,2\rangle$. Summarizing, we get the following.

Theorem 6. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4, and*

$$\mathscr{C}=\langle a_1(X^2)a_2(X^2)a_3(X^2)b(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd=X^n-1$, then every codeword of $\mathscr{C}$ is of the form $(\mathbf{a}-\mathbf{b}|\mathbf{b})$, where $\mathbf{a}\in\langle a_1a_2a_3bc, 2a_1a_2b\rangle_n$, and $\mathbf{b}\in\langle a_1a_2a_3, 2a_1\rangle_n$.

Corollary 3. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4, and*

$$\mathscr{C}=\langle a_1(X^2)a_2(X^2)a_3(X^2)b(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd=X^n-1$, and d_1 is the minimum Lee weight of $\langle a_1a_2a_3bc, 2a_1a_2b\rangle_n$, and d_2 is the minimum Lee weight of $\langle a_1a_2a_3, 2a_1\rangle_n$, then the minimum Lee weight of $\mathscr{C}$ is equal to $\min\{d_1, 2d_2\}$.

Proof. Both $\mathbf{a}-\mathbf{b}$ and $\mathbf{b}$ are codewords of $\langle a_1a_2a_3, 2a_1\rangle_n$. When $\mathbf{b}=0$ or $\mathbf{a}=\mathbf{b}$, then the Lee weight of $\mathbf{c}$ is at least d_1. □

Thus the weight of a code of this type is never better than the weight of a cyclic code of length n. We do get a slight improvement when the polynomial $b(X)$ is replaced with a lift.

Theorem 7. *Let $\mathscr{C}$ be a cyclic code of length $2n$ (n odd) over Z_4, and*

$$\mathscr{C}=\langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd=X^n-1$ and $\tilde{b}$ is a monic polynomial such that $\tilde{b}\equiv b \pmod{2Z_4[X]}$. Then every codeword of $\mathscr{C}$ is of the form $(\mathbf{a}-\mathbf{b}|\mathbf{b})$, where $\mathbf{a}\in\langle a_1a_2a_3bc, 2a_1a_2\rangle_n$, $\mathbf{b}\in\langle a_1a_2a_3, 2a_1\rangle_n$, and $\mathbf{a}+2\sigma(\mathbf{b})\in\langle b\rangle_n$, where σ is a shift of a fixed number of coordinates.

Proof. If ζ^i is a root of b, then $g(u\zeta^i) \in \langle u-1+2\zeta^j\rangle$, for all $g(X) \in \mathscr{C}$, for some fixed integer j, $0 \leqslant j \leqslant n-1$. This means that if $A(Z)+(u-1)B(Z)$ is an MS polynomial of $\mathscr{C}$,

$$A_{-i} = 2B_{-i}\zeta^j,$$

so that $\mathbf{a} \in \langle b, 2\rangle$. Also, noting that $B(\zeta^{-j}Z)$ is the MS polynomial of $\mathbf{b}$ shifted by j positions, we see that $\mathbf{a}+2\sigma(\mathbf{b}) \in \langle b\rangle_n$, where σ is the shift by $n-j$ coordinates. (Note that a different choice of $\tilde{b}(X)$ will produce a different value of j.) The results for when ζ^i is not a root of b carry through as before. This completes the proof. □

Corollary 4. *If $\mathscr{C}$ is a cyclic code of length $2n$ (n odd) over Z_4 with minimum Lee weight d, and*

$$\mathscr{C} = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1a_2a_3bcd = X^n-1$ and $\tilde{b}$ is monic with $\tilde{b} \equiv b$ $(\operatorname{mod} 2Z_4[X])$, then

$$\min\{d_1, 2d_2\} \leqslant d \leqslant 4d_3,$$

where d_1 is the minimum Lee weight of $\langle a_1a_2a_3bc, 2a_1a_2\rangle_n$, d_2 is the minimum Lee weight of $\langle a_1a_2a_3, 2a_1\rangle_n$, and d_3 is the minimum Hamming weight of the binary code $\langle \overline{a_1}\rangle$ of length n.

Proof. It is clear that $d \geqslant \min\{d_1, 2d_2\}$; the argument is the same as in Corollary 3. If $\mathbf{b}=2\mathbf{v}$, where $\mathbf{v}$ is a minimum weight codeword of $\langle\overline{a_1}\rangle_n$, then $\mathbf{b} \in \langle a_1a_2a_3, 2a_1\rangle$ and then $(\mathbf{b}|\mathbf{b})$ is a codeword of $\mathscr{C}$ of Lee weight $4d_3$. □

The fact that the lower bound is not always sharp comes from the fact minimum Lee weight codewords from the two codes of length n might not satisfy the condition that $\mathbf{a}+2\sigma(\mathbf{b}) \in \langle b\rangle_n$. However, it may be that there is no code whose weight attains the upper bound.

3.1. Minimal cyclic codes

A *minimal* cyclic code of length $2n$ over Z_4 is a cyclic code $\mathscr{M}_s$ such that for some s, $0 \leqslant s \leqslant n-1$,

$$c(u\zeta^r) = 0 \quad \forall c(X) \in \mathscr{M}_s, \quad \forall r \notin cl_2(s).$$

A minimal cyclic code is isomorphic to an ideal of $\mathscr{R}_4(u, m_s)$ via the map

$$\mathscr{R}_4(u, m_s) \to \mathscr{M}_s,$$

$$\lambda \mapsto \psi\left(\frac{1}{n}[1, u, 1, u, \ldots, 1] * (A_\lambda(1), \ldots, A_\lambda(\zeta^{n-1}))\right),$$

where

$$A_\lambda(Z) = \lambda Z^{-s} + \lambda^f Z^{-2s} + \cdots + \lambda^{f^{m_s-1}} Z^{-2^{m_s-1}s}.$$

These codes seem to be among the best cyclic codes to consider, and their minimum Lee weights are easy to compute.

Table 1
Minimal cyclic codes of length $2n$ $(f(X) = (X^n - 1)/f_s(X))$

M_s	Size	$\mathscr{C}_1$	$\mathscr{C}_2$	Min. Lee wt.
$\langle f(X^2)\rangle$	4^{2m_s}	$\langle f\rangle_n$	$\langle f\rangle_n$	$d(\mathscr{D}_s)$
$\langle f(X^2)f_s(X), 2f(X^2)\rangle$	$4^{m_s}2^{m_s}$	$\langle 2f\rangle_n$	$\langle f\rangle_n$	$2d(\mathscr{H}_s)$
$\langle f(X^2)f_s(X)\rangle$	4^{m_s}	0	$\langle f\rangle_n$	$2d(\mathscr{D}_s)$
$\langle 2f(X^2)\rangle$	4^{m_s}	$\langle 2f\rangle_n$	$\langle 2f\rangle_n$	$2d(\mathscr{H}_s)$
$\langle 2f(X^2)f_s(X)\rangle$	2^{m_s}	0	$\langle 2f\rangle_n$	$4d(\mathscr{H}_s)$

Let $f_s(X)$ be the minimal polynomial of ζ^s over Z_4, which is also a monic divisor of $X^n - 1$. In terms of polynomial generators, a minimal cyclic code is of the form

$$\mathscr{M}_s = \langle a_1(X^2)a_2(X^2)a_3(X^2)\tilde{b}(X)c(X), 2a_1(X^2)a_2(X)b(X)\rangle,$$

where $a_1(X) = (X^n - 1)/f_s(X)$, and at most one of the polynomials a_2, a_3, b, c is equal to f_s, the rest are equal to 1 ($\tilde{b}$ is still a monic lift of b).

Let $\mathscr{D}_s = \langle a_1\rangle_n$ and $\mathscr{h}_s = \mathscr{D}_s$ reduced modulo 2. Note that $\mathscr{D}_s$ is a minimal cyclic code over Z_4 of length n and $\mathscr{H}_s$ is a binary minimal cyclic code of length n. Let $d(\mathscr{D}_s)$ be the minimum Lee distance of $\mathscr{D}_s$, and let $d(\mathscr{H}_s)$ be the minimum Hamming distance of $\mathscr{H}_s$. A codeword of $\mathscr{M}_s$ is of the form

$$(\mathbf{a} - \mathbf{b}|\mathbf{b}),$$

where $\mathbf{a} \in \mathscr{C}_1$ and $\mathbf{b} \in \mathscr{C}_2$, and $\mathscr{C}_1$ and $\mathscr{C}_2$ are certain cyclic codes of length n that are equal to either $\mathscr{D}_s$, $2\mathscr{H}_s$, or $\langle 0\rangle$. We summarize the results for codes in which $\mathscr{M}_s \ncong \langle u - 1 + 2t\rangle$, where $t \in \mathscr{T}^*_{m_s}$ in Table 1.

Now we consider minimal codes of the form $\langle f(X^2)\tilde{f}_s(X)\rangle$, where $\tilde{f}_s(X) = f_s(X) + 2g(X)$, where $deg(g) < deg(f_s)$. Such a code is isomorphic to an ideal $\langle u - 1 + 2\zeta^j\rangle$, where j is some integer, $0 \leqslant j \leqslant n - 1$. In this case, a codeword is of the form $(\mathbf{a} + \mathbf{b}|\mathbf{b})$, where $\mathbf{a} \in 2\mathscr{H}_s$, $\mathbf{b} \in \mathscr{D}_s$, and $\mathbf{a} + 2\sigma(\mathbf{b}) \in < f_s\rangle_n$, σ being some cyclic shift of coordinates depending on j. But this means that every nth root of unity is a root of the polynomial corresponding to $\mathbf{a} + 2\sigma(\mathbf{b})$, so this vector must be zero. Thus a typical codeword must be permutation-equivalent to the form

$$(2\sigma(\mathbf{b}) + \mathbf{b}|\mathbf{b}).$$

Both the left and right halves of this vector are codewords of $\mathscr{D}_s$, and if $\mathbf{b} \in 2\mathscr{H}_s$, then $(\mathbf{b}|\mathbf{b})$ is a codeword. From these remarks and Corollary 4, we get the following.

Theorem 8. *If $\mathscr{M}_s = \langle f(X^2)\tilde{f}_s(X)\rangle$, where $f(X)f_s(X) = X^n - 1$ and $\tilde{f}_s(X) = f_s(X) + 2g(X)$, $deg(g) < deg(f_s)$, and d is the minimum Lee distance of $\mathscr{M}_s$, then*

$$2d(\mathscr{D}_s) \leqslant d \leqslant 4d(\mathscr{H}_s),$$

where $d(\mathscr{D}_s)$ is the minimum Lee distance of $\langle f(X)\rangle_n$ and $d(\mathscr{H}_s)$ is the minimum Hamming distance of the binary cyclic code $\langle \overline{f(X)}\rangle_n$.

As an example of a minimal code that is better than the lower bound $2d(\mathscr{D}_s)$, consider the code from Example 1, $\mathscr{C} = \langle (X^2 - 1)(X^2 + X - 1)\rangle$. This code has minimum Lee weight 6, whereas the code $\langle (X^2-1)(X^2+X+1)\rangle$ has minimum Lee weight 4. The Gray image of $\mathscr{C}$ yields a nonlinear binary $(12, 2^4, 6)$ code, which equals the performance of the best-known binary linear code with the same parameters. This example indicates that these are the types of codes that are worth investigating, by using various choices for $\tilde{f}$. This example also shows that codes with different choices of $\tilde{f}$ do not necessarily give equivalent codes.

Finally, it is worth noting that a specific class of minimal cyclic codes has been studied in [12,2] in the context of quadriphase sequence design. There the codes $\langle f(X^2)\tilde{f}(X)\rangle$ are given by the trace description

$$\{(T_{m_s}(\lambda(\gamma\zeta^{-s})^i))_{i=0}^{2n-1}\colon\ \lambda \in GR(4, m_s)\}$$

with $\gamma = 1+2\delta$, $\delta \in \mathscr{T}_m$. (This description can also be obtained from the Inversion formula.) The authors of [12,2] give interesting weight properties of these codes.

3.2. Idempotents

Let $\bar{e}(X)$ be the idempotent generator of the cyclic code $\langle \bar{f}\rangle_n$ in $F_2[X]/(X^n+1)$, where $\bar{f}$ is a divisor of X^n+1 in $F_2[X]$, and let $f(X)$ be the Hensel lift of $\bar{f}$. Now let $e(X) = [\bar{e}(X)]^2$ calculated in $Z_4[X]$ modulo (X^n-1). It has been shown that $e(X)$ is the idempotent generator of $\langle f\rangle_n$ in $Z_4[X]/(X^n-1)$. Since

$$e(X)^2 = e(X) + a(X)(X^n-1)$$

for some $a(X)$, substituting X^2 for X gives

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

Thus $e(X^2)$ is an idempotent in $Z_4[X]/(X^{2n}-1)$, and since the transform vector corresponding to $e(X^2)$ consists of only 0's and 1's, we get that $e(X^2)$ is the idempotent generator of $\langle f(X^2)\rangle$. Hence we have shown that

Theorem 9. *If f is a divisor of X^n-1 in $Z_4[X]$, the code $\langle f(X^2)\rangle$ has a unique idempotent generator, namely $e(X^2)$, where $e(X)$ is the idempotent generator of $\langle f\rangle_n$ in $Z_4[X]/(X^n-1)$. Furthermore, $\langle f(X^2)\rangle$ is the only type of cyclic code of length $2n$ that has an idempotent generator.*

This last statement is true since any other type of code will have nonzero nonunits in its transform vector, and idempotents only have 0's and 1's in their transform vector.

3.3. The asymptotic badness of cyclic codes

As stated in the beginning of this section, despite the fact that the class of cyclic codes over Z_4 of length $2n$ is quite large, it is still asymptotically bad; their Gray images do not perform well against optimal binary codes. This follows from the upper bounds given in Corollaries 3 and 4. In one case, the minimum distance is no better than the minimum Lee weight of the quaternary cyclic code $\langle a_1a_2a_3bc, 2a_1a_2b\rangle$. In the other case, the minimum distance is no better than 4 times the minimum Hamming

Table 2
Some optimal codes of oddly even length

Length	Code	Parameters
6	$\langle (X^2-1)(X^2+X-1)\rangle$	$(6, 4^2, 6)$
10	$\langle (X^2-1)(X^4+X^3-X^2+X+1)\rangle$	$(10, 4^4, 8)$
14	$\langle (X^2-1)(X^6+2X^4+X^2-1)(X^3+X^2+2X+1)\rangle$	$(14, 4^3, 12)$

distance of $\langle \overline{a_1}\rangle$. In this case, a sequence of good quaternary cyclic codes of length n implies the existence of a sequence of good binary cyclic codes (but not vice versa).

Even minimal cyclic codes are asymptotically bad. This is because the lengths and minimum distances are increasing much faster than the rates. For example, take the minimal cyclic code $\mathscr{C}_m = \langle f(X^2)\tilde{f}_1(X)\rangle$, of length $2(2^m-1)$, m odd, where $f_1(X)$ is the minimal polynomial of a primitive element $\zeta \in GR(4,m)$ and $f(X)f_1(X) = X^n - 1$. It is known [6] that the minimum Lee weight of $\langle f(X^2)\rangle$ is $2^m - 2^{(m-1)/2}$. From Corollary 4, if d is the minimum Lee distance of $\mathscr{C}_m$, then

$$2^{m+1} - 2^{(m+1)/2} \leqslant d \leqslant 2^{m+1} - 4.$$

Yet the size of the code is still 4^m. This means the Gray image $\phi(\mathscr{C})$ performs no better than a binary linear $[2^{m+2}-4, 2m, 2^{m+1}-4]$ code. The dimension increases at a polynomial rate, while the lengths and distances increase exponentially.

Nonetheless, there are a few cases when cyclic codes of oddly even length are optimal. Three examples we have found are given in Table 2. It is interesting to note that for the case of length 10, different codes of the form $\langle (X^2-1)\tilde{f}(X)\rangle$, where $\tilde{f}$ is a lift of $X^4+X^3+X^2+X+1$, were found whose minimum Lee weights were 4, 6, and 8.

It would be interesting to see what other optimal codes exist in this class.

4. Conclusion

We have classified all codes of oddly even length over Z_4, and have found that this is a relatively large class of codes (compared to cyclic codes of odd length). It would be interesting to see what applications could come from the size of this class. It remains to be seen if it contains any optimal codes. Open problems include the study of cyclic codes over Z_4 of other even lengths and the study of cyclic codes over Z_{p^a} of lengths divisible by p. In particular, it would be interesting to study oddly even cyclic codes over Z_{2^k} and the generalized Gray map images [4] of these codes.

Acknowledgements

The author would like to thank the referees for their helpful comments.

References

[1] T. Blackford, “Permutation groups of extended cyclic codes over Galois rings, Ph.D. Thesis, The Ohio State University, 1999.

[2] S. Boztas, R. Hammons, P.V. Kumar, 4-phase sequences with near-optimum correlation properties, IEEE Trans. Inform. Theory 38 (1992) 1101–1113.

[3] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic codes, Designs, Codes Cryptography 6 (1995) 21–35.

[4] C. Carlet, Z_{2k}-linear codes, IEEE Trans. Inform. Theory 44 (1998) 1543–1547.

[5] G. Castagnoli, J.L. Massey, P.A. Schoeller, N. von Seemann, On repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 337–342.

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

[7] P. Kanwar, S.R. Lopez-Permouth, Cyclic codes over the integers modulo p^m, Finite Fields Appl. 3 (1997) 334–352.

[8] B. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.

[9] V. Pless, Z. Qian, Cyclic codes and quadratic residue codes over Z_4, IEEE Trans. Inform. Theory 42 (1996) 1594–1600.

[10] B. Sundar Rajan, M. Siddiqi, Transform domain characterization of cyclic codes over Z_m, Appl. Algebra Eng. Comm. Comput. 5 (1994) 261–275.

[11] P. Udaya, A. Bonnecaze, Cyclic codes and self-dual codes over $F_2 + uF_2$, IEEE Trans. Inform. Theory 45 (4) (1999) 1250–1255.

[12] P. Udaya, M.U. Siddiqi, Optimal and suboptimal quadriphase sequences derived from maximal length sequences over Z_4, Appl. Algebra Eng. Comm. Comput. 9 (1998) 161–191.

[13] J.H. van Lint, Repeated-root cyclic codes, IEEE Trans. Inform. Theory 37 (2) (1991) 343–345.

[14] Z. Wan, Cyclic codes over Galois rings, Algebra Colloq. 6 (3) (1999) 291–304.