Cyclic Codes and Self-Dual Codes over $F_2 + uF_2$

A. Bonnecaze, P. Udaya*

May 4, 1998

Abstract

We introduce linear cyclic codes over the ring $F_2 + uF_2 = \{0, 1, u, \overline{u} = u + 1\}$, where $u^2 = 0$. This ring shares many properties of $\mathbf{Z}_4$ and F_4 and admits a linear "Gray map". Cyclic codes are described as modules over $(F_2 + uF_2)^n$ which may not be free. Self-dual codes of odd length exists as in the case of $\mathbf{Z}_4$-codes. We exhibit some extremal codes of this very interesting family.

Index Terms: Codes over rings, Cyclic codes, Self-dual codes, Gray map.

1 Introduction

Among the four rings of four elements, the Galois field F_4 and more recently the ring of integers modulo four $\mathbf{Z}_4$ are the most used in coding theory. $\mathbf{Z}_4$-codes are renowned for producing good nonlinear codes by the Gray map, namely Kerdock, Preparata or Goethals codes. On the other hand, the ring F_4 admits a linear Gray map which does not give good binary codes. The ring $R = F_2 + uF_2$ shares some good properties of both $\mathbf{Z}_4$ and F_4. This alphabet is given by all binary polynomials in indeterminate u of degree less than 2, and is closed under usual binary polynomial addition and multiplication modulo u^2. The set of elements of R is $\{0, 1, u, \overline{u} = u + 1\}$. It is easy to verify that R is a local ring with a maximal ideal given by $\{0, u\}$. The multiplication and addition table for the ring is given by Table 1. The multiplication table coincides with that of $\mathbf{Z}_4$, when u and $\overline{u}$ are replaced by respectively 2 and 3. In this sense, R is analogous to $\mathbf{Z}_4$ and here u plays the role of 2. However, the addition table is different. The addition table is similar to that of the Galois field $F_4 = \{0, 1, \beta, \beta^2 = \beta + 1\}$, when $\overline{u}$ and u are replaced respectively by β and β^2. Note that from the definition, the characteristic of the ring is 2. Thus, in the structure of alphabets, R lies in between $\mathbf{Z}_4$ and F_4. This ring can also be viewed as a vector space of dimension 2 over F_2. Moreover, the sets $\{0, 1\}$, $\{0, u\}$ and $\{0, \overline{u}\}$ form three subspaces in R and the subspace $\{0, 1\}$ $(= F_2)$ is a subring. Note that the ring R is isomorphic to the quotient ring $\mathbf{Z}[X]/(2, (X + 1)^2)$, which was first used by Bachoc [1] in connection with constructions of modular lattices.

*The authors are with the Department of Mathematics, City Campus, Royal Melbourne Institute of Technology, GPO Box 2476V, Melbourne VIC - 3001, Australia. P. Udaya acknowledges the support of the ARC Grant #A49701206.

$*$	0	1	$\overline{u}$	u
0	0	0	0	0
1	0	1	$\overline{u}$	u
$\overline{u}$	0	$\overline{u}$	1	u
u	0	u	u	0

$+$	0	1	$\overline{u}$	u
0	0	1	$\overline{u}$	u
1	1	0	u	$\overline{u}$
$\overline{u}$	$\overline{u}$	u	0	1
u	u	$\overline{u}$	1	0

Table 1: Multiplication and addition tables for the ring $F_2 + \overline{u}F_2$.

In this paper, we describe the structure of cyclic codes and cyclic self-dual codes over R. Since F_2 is a subring of R, the minimum distance of a lifted cyclic code over R is not increased. However, the dimension is higher and the binary Gray image is **linear**. Unlike the $\mathbf{Z}_4$ case, here, free codes are not interesting and the best codes are obtained when the minimum distance of the residue code is about the double of the minimum distance of the torsion code. The image by the linear Gray map of cyclic codes over R leads to a new representation of some class of $< \mathsf{u}, \mathsf{u}+\mathsf{v} >$ constructed codes. This is remarkable since certain good $< \mathsf{u}, \mathsf{u}+\mathsf{v} >$ constructed binary codes have a simple representation as cyclic R codes (See also [17]). Note that cyclic $\mathbf{Z}_4$ codes reveal the structure of certain good binary non linear codes. Indeed $\mathbf{Z}_4$ cyclic codes could also be viewed as a generalization of $< \mathsf{u}, \mathsf{u}+\mathsf{v} >$ construction codes (see [10]).

The paper is organized as follows. Section 2 is devoted to the study of cyclic codes over R. All good codes of lengths 7 and 15 are given. Self-dual codes of odd length are introduced in section 3. They represent a very interesting family since they produce modular lattices [1]. Codes of lengths 15 and 31 are particularly interesting. Some of their binary images are self-dual binary codes of parameters $[30, 15, 6]$ and $[62, 31, 10]$.

2 Cyclic Codes over $F_2 + uF_2$

We first establish some terminology. The set of R^n of n-tuples from R is an R-module. By a *linear code C over R* (or a R-code), we mean an additive submodule of R^n. Duality for codes is understood with respect to the form $xy = \sum_i x_i y_i$. C is said to be self-dual if $C = C^{\perp}$. Two codes are equivalent if one can be obtained from the other by permuting the coordinates and if necessary exchanging 1 and $\overline{u}$ in certain coordinates. The Lee weight w_L of $x = (x_1, \cdots, x_n)$ is defined as $n_1(x) + 2n_2(x)$. A non-zero linear code C over R, has a generator matrix which after a suitable permutation of the coordinates can be written in the form

$$\mathbf{G} = \begin{bmatrix} I_{k_1} & A & B \\ 0 & uI_{k_2} & uD \end{bmatrix}$$

where A and B are matrices over R and D is an F_2 matrix. The code C then contains all codewords $[v_0, v_1]G$, where v_0 is a vector of length k_1 over R and v_1 is a vector of length k_2 over F_2. Thus, C contains a total of $4^{k_1}2^{k_2}$ codewords. The parameters of C are given by $[n, 4^{k_1}2^{k_2}, d_{Lee}]$, where d_{Lee} represents the minimum Lee distance of C. Following [6], we associate to the code C two binary codes. The residue code C_1 define as $C_1 = \{x \in F_2^n \mid \exists y \in$

$F_2^n \mid x + uy \in C\}$ and the torsion code C_2 defined as $C_2 = \{x \in F_2^n \mid ux \in C\}$.
A cyclic code of length n over R is a linear code with the property that if $(c_0, c_1, \cdots, c_{n\perp 1}) \in C$ then $(c_1, c_2, \cdots, c_0) \in C$. We assume that n is odd and represent codewords by polynomials. Then cyclic codes are ideals in the ring

$$\mathcal{R}_n = R[x]/(x^n - 1).$$

2.1 Galois extension ring of R

The method of constructing Galois rings over R is similar to the construction of Galois rings over $\mathbf{Z}_4$. The general case of such rings over $R = F_2[u]/(w(u)^k), k > 1$, where $w(u)$ is an irreducible polynomial of degree $m \geq 1$ over F_2 has been studied in [18]. The ring $F_2 + uF_2$ is a special case of these rings when $w(u) = u$ and $k = 2$. Let $R[x]$ be the ring of polynomials over R. We have a natural homomorphic mapping, from R to its residue field F_2. For any $a \in R$, let $\hat{a}$ denote the polynomial reduction modulo u. Now, define a polynomial reduction mapping $\mu : R[x] \to F_2[x]$ in the obvious way:

$$f(x) = \sum_{i=0}^{r} a_i x^i \xrightarrow{\mu} \sum_{i=0}^{r} \hat{a}_i x^i.$$

A monic polynomial f over $R[x]$ is said to be a basic irreducible polynomial if its projection $\mu(f)$ is irreducible over $F_2[x]$. The Galois ring of R denoted as $GR(R, r)$ is defined as $R[x]/(f(x))$, where $f(x)$ is a basic monic irreducible polynomial of degree r over R. Hence the ring $GR(R, r)$ is a module over R. The basic monic irreducible polynomial of degree r over R can be lifted from a monic irreducible polynomial over F_2. The trick is to consider a monic irreducible polynomial over F_2 which is a subring of R. For any polynomial $f(x) \in F_2[x]$, let $\underline{f}(x)$ denote the same polynomial viewed as an element of $R[x]$. Since F_2 is a subring of R, we will not make distinction between f and $\underline{f}$ if the context is clear. Any irreducible polynomial over the subring is obviously irreducible over the ring. Thus any monic irreducible polynomial $f(x)$ over F_2 is a basic monic irreducible over R.
Note that this is not the situation in the $\mathbf{Z}_4$ case where the polynomial lift from the ground field $\mathbf{Z}_2$ is non trivial [8]. Like Galois fields, $GR(R, r)$ is unique for a given r [11]. The group of units of $GR(R, r)$ denoted by $GR^\star(R, r)$ is given by a direct product of two groups:

$$GR^\star(R, r) = G_C \times G_A,$$

where G_C is a cyclic group of order $2^r - 1$ and G_A is an Abelian group of order 2^r [18, 5].

Lemma 1 *The set $\{G_C, 0\}$ is isomorphic to the residue field F_{2^r} and is also a subspace of $GR(R, r)$. Thus, the set is a subring over $GR(R, r)$.*

Proof: Since G_C is cyclic, the set $\{G_C, 0\}$ satisfies the multiplicative axiom of a field. For every, $\alpha_1, \alpha_2 \in G_C, (\alpha_1 + \alpha_2)^{2^m} = (\alpha_1 + \alpha_2)$, since the characteristic of R is 2. This implies that $(\alpha_1 + \alpha_2)^{2^m \perp 1} = 1$ and $(\alpha_1 + \alpha_2) \in \{G_C, 0\}$. Thus, $\{G_C, 0\}$ is closed under addition which proves the lemma. □

Using Lemma 1, the elements of G_A are given by the set $\{(1 + u\alpha), \alpha \in F_{2^r}\}$. The zero divisors of the ring R are given by the elements of the maximal ideal generated by u, namely $\{(u\alpha), \alpha \in F_{2^r}\}$. Thus we have,

Lemma 2 *The only ideals of* $GR(R,r)$ *are* $(0),(1)$ *and* (u).
Thus any element of $GR(R,r)$ can be uniquely represented as

$$\alpha = \alpha_1 + u\alpha_2, \alpha_1, \alpha_2 \in F_{2^r}. \tag{1}$$

This is analogous to the p-adic representation considered in [3].
The Galois automorphism group of $GR(R,r)$ is cyclic of order r and is generated by the Frobenius map σ defined by

$$\sigma(\alpha) = (\alpha_1)^2 + u(\alpha_2)^2, \alpha \in GR(R,r),$$

where α is as in (1).

2.2 Cyclic codes, Generators and Idempotent Polynomials

In order to define cyclic codes of length n over R, we need to know a factorization of the polynomial $x^n - 1$ over R and study the ideals in the polynomial algebra generated by $x^n - 1$. We first demonstrate that such a factorization exists by using addition properties of the ring. Since there exists a primitive element in $GR(R,r)$, the polynomial $(x^n - 1)$, where $n = 2^r - 1$, factors linearly over $GR(R,r)$. We have

$$(x^n - 1) = (x - \alpha)(x - \alpha^2)\cdots(x - \alpha^n),$$

where α is a primitive element of $\{G_C, 0\} = F_{2^r}$. Define the minimal polynomial of $\alpha, \alpha \in F_{2^r}$ in $GR(R,r)$ as

$$m(\alpha) = (x - \alpha)(x - \sigma(\alpha))\cdots(x - \sigma^{t\perp 1}(\alpha)),$$

where $\alpha \in F_{2^r}$ of order $2^t - 1, t$ divides r. It is easy to see that if $(x - \alpha)$ divides $(x^n - 1)$, then $(x - \sigma(\alpha)) = (x - \alpha^2)$ also divides $(x^n - 1)$. Similarly the minimal polynomial of any non-zero element α also divides $(x^n - 1)$ and $m(\alpha)$ is a polynomial over R. Moreover, since α belongs to F_{2^r} of $GR(R,r)$, $m(\alpha)$ is a polynomial over F_2 in R. Thus, considering minimal polynomials of elements of G_C belonging to distinct Frobenius classes gives the factorization of $(x^n - 1)$ over R:

$$(x^n - 1) = m(\alpha_1)m(\alpha_2)\cdots m(\alpha_t),$$

where $\alpha_1, \alpha_2, \cdots, \alpha_t$ are generators of distinct Frobenius classes. The Factorization of $(x^n - 1)$ can also be obtained as follows. We know that F_2 is a subring of R and that over the binary field, $x^n - 1$ factors uniquely as a product of pairwise irreducible polynomials. If any polynomial factors over a subring, it also factors over the ring. Thus, the factorization $x^n - 1 = f_1 f_2 \cdots f_r$ carries over R. Note that this is not the situation in the $\mathbf{Z}_4$ case where the factorization has to be achieved by a non trivial lift [8].
We have the following lemma.

Lemma 3 *If* $x^n - 1 = f_1 f_2 \cdots f_r$, *where* f_i *are basic irreducible and pairwise coprime, then this factorization is unique. The factorization is obtained from factorization of the binary polynomial* $x^n - 1$.

Proof: The factorization is demonstrated above. The ring R is a local ring with unique

maximal ideal. By Hensel's Lemma [11], regular polynomials (polynomials which are not zero divisors) over R have a unique factorization. From [11] any zero divisor $f(x)$ in R can be uniquely written as $uf'(x)$, where $f'(x)$ is a regular polynomial. In particular (x^n-1) is regular and hence the lemma is proved. □

We define f as a primary polynomial if (f), the ideal generated by f, is a primary ideal [11]. The maximal ideal contains all zero divisors. In Lemma 2, we have given the structure of the prime ideal in $R[x]/(f(x))$ ([13]). Now we give the structure of all ideals in $\mathcal{R}_n$ along the lines of results of [13] for $\mathbf{Z}_4$-cyclic codes.

Theorem 1 *Let n be odd. Let $x^n-1 = f_1 f_2 \cdots f_r$, where the f_i $(1 \leq i \leq r)$ are basic irreducible and pairwise polynomials. Let $\hat{f}_i$ denote the product of all f_j except f_i. Then any ideal in the ring is a sum of $(\hat{f}_i)$ and $(u\hat{f}_j)$.*

Proof: The proof is similar to the proof given in [13, Theorem 1] for ideals in $\mathbf{Z}_4[x]/(x^n-1)$ as in this case also, ideals in $\mathcal{R}_n$ can be written as

$$I \cong I_1 \oplus I_2 \oplus \cdots I_t,$$

where $I_i, i = 1, \cdots$, is an ideal of the Galois Ring $R[x]/(f_i)$. The only ideals in $R[x]/(f_i)$ are $(0), (1)$ or (u). The ideals (1) and (u) in $I_i = R[x]/(f_i)$ correspond respectively to the ideals (f_i) and $(\hat{f}_i)$ in $\mathcal{R}_n$. In any case the ideal I is a sum of (f_i) and $(\hat{f}_j)$ since $(f_1 f_2 \cdots f_t) = (f_1)(f_2)\cdots(f_t)$. □

As a consequence of the above theorem, the number of cyclic codes over R of length n is 3^t, where t is the number of basic irreducible polynomial factors in x^n-1 over R. The following two theorems characterize cyclic codes and their duals over R by giving generator polynomial description. We omit the proofs as they are identical to the corresponding theorems in [13] for $\mathbf{Z}_4$ cyclic codes.

Theorem 2 *Suppose C is a cyclic code of odd length n over R, then there are unique, monic polynomials f, g, h such that $C = (fh, ufg)$, where $fgh = x^n - 1$ and $|C| = 4^{deg(g)} 2^{deg(h)}$.*
when $h = 1, C = (f)$ and $|C| = 4^{n \perp deg(f)}$,
when $g = 1, C = (uf)$ and $|C| = 2^{n \perp deg(f)}$.

Theorem 3 *Suppose $C = (fh, ufg)$ is a cyclic code of odd length n over R, where f, g, h are monic polynomials such that $fgh = x^n - 1$, and $|C| = 4^{deg(g)} 2^{deg(h)}$. Then, the dual of C is $C^\perp = (g^\star h^\star, ug^\star f^\star)$ and $|C^\perp| = 4^{deg(f)} 2^{deg(h)}$*
If $h = 1$, $C = (f)$ and $|C^\perp| = (g^\star)$. If $g = 1$, $C = (uf)$ and $|C^\perp| = (h^\star, uf^\star)$. where $f^\star, g^\star$ and $h^\star$ are respectively reciprocal polynomials of f, h and g.
Hence, with any cyclic code over R, the residue and torsion codes are given by

1. The residue code $C_1 = \mu(fh)$ of dimension $deg(g)$
2. The torsion code $C_2 = \mu(f)$ of dimension $deg(g) + deg(h)$.

Note that the code C over R is completely determined from the residue and torsion codes, as the residue field obtained using the homomorphic mapping μ is a subring in R. A code is free if and only if the dimension of the residue code is equal to the dimension of the torsion

code.

We define an *idempotent* in $R[x]$ as a polynomial $e(x)$ such that

$$e(x)^2 = e(x) \bmod (x^n - 1).$$

Let $C = (f)$ be a free code (respectively $C = (uf)$) over R, then C has an idempotent generator $e(x)$ which is given by the idempotent generator of the binary residue (respectively torsion) code. This is a straightforward consequence of factorization of $(x^n - 1)$ in R. Note that, if the code is free, the idempotent of its dual is given by $1 - e(x^{\perp 1})$. But, this is not true for a code which has only a torsion part. In general if $C = (fh, ufg)$, the idempotent polynomial of C is given by $e_1(x) + ue_2(x)$, where $\mu(e_1(x))$ and $\mu(e_2(x))$ are the idempotent polynomials of the residue and torsion codes.

2.3 Binary codes obtained from Cyclic codes over $F_2 + uF_2$

For any element of R expressed as $x + uy$, we let

$$\phi(x + uy) = (y, x + y),$$

where $x, y \in F_2$.

Lemma 4 *If a code C is linear or self-dual so is $\phi(C)$. The minimum Lee weight of C is equal to the minimum Hamming weight of $\phi(C)$.*

In the next lemma, we relate minimum Lee weight of a code C to its component binary codes.

Lemma 5 *The minimum Lee weight of C is upper bounded by $min(d_1, 2d_2)$, where d_1 and d_2 are respectively minimum distances of the residue and torsion code. When the code is free, its minimum distance is exactly the minimum distance of its residue code.*

Proof: Since the codes C_1 (residue) and uC_2 (code obtained by multiplying u with C_2) completely include in C, the result is obvious. □

In the above lemma we get a rough idea of the minimum distance of the R-codes. In general it is difficult to find the exact minimum distance and weight distribution. But, for the simplex code (free code generated by $(x^n - 1)/f$, where f is a primitive irreducible polynomial of degree r), the weight distribution can be computed using the vector space structure of $GR(R, r)$ [18]. The weight distribution depends on the ranks of the matrices $M_\alpha = [1, \alpha]$ formed by adjoining the element 1 with every α belonging to F_{2^r} [18]. It is easy to verify that there are $2^r - 2$ such matrices whose rank is 2. The rest will have rank 1. The weight distribution is given in Table 2. The Simplex code is the analog version of the $\mathbf{Z}_4$ Kerdock code. The codewords of the Simplex code share many properties of m-sequences over F_2 but are not field m-sequences. They form an interesting class of optimal sequences with respect to Hamming correlation [18].

The main implication of Lemma 5, is that the minimum distance of a free code is equal to that of its residue code. This is the reason why free codes are not interesting over R in the sense that the parameters of their binary image are not good.

n_0	n_1	$n_{\overline{u}}$	n_u	Number of codewords
2^r-1				1
$2^{r\perp 1}-1$	$2^{r\perp 1}$			(2^r-1)
$2^{r\perp 1}-1$		$2^{r\perp 1}$		(2^r-1)
$2^{r\perp 1}-1$			$2^{r\perp 1}$	(2^r-1)
$2^{r\perp 2}-1$	$2^{r\perp 2}$	$2^{r\perp 2}$	$2^{r\perp 2}$	$(2^r-2)(2^r-1)$

Table 2: Weight Distribution of Simplex Codes over R

2.4 Examples

2.4.1 Length 7

Table 3 presents all the 3^3-2 non trivial cyclic codes of length 7. The factorization of x^7+1 is $f_1f_2f_3$ where $f_1 := x+1,\ f_2 := x^3+x+1,\ f_3 := x^3+x^2+1$. Optimal codes are indicated by the symbol * (by an optimal code, we mean a binary code having the maximal minimum distance for the given length and the dimension).

Remark The binary Gray image of the free codes considered in our paper can be equivalently expressed as repeated root cyclic codes in the sense of [4]. However, this is not true when the code is not free. For example, the codes corresponding to the second and fourth row are not equivalent to the code of parameters $[14,3,8]$ of Table 1 in [4]. Similarly, the binary image of the code corresponding to the 13^{th} row is self-dual and not equivalent to the self-dual cyclic code given in [16] (itself equivalent to D_{14} [12]).

2.4.2 Length 15

Table 4 presents all good cyclic codes of length 15. The factorization of $x^{15}+1$ is equal to $f_1f_2f_3f_4f_5$, where $f_1 := x+1,\ f_2 := x^2+x+1,\ f_3 := x^4+x+1,\ f_4 = x^4+x^3+1,\ f_5 = x^4+x^3+x^2+x+1$.

3 Self-dual codes over F_2+uF_2

The extended quadratic residue $\mathbf{Z}_4$-codes represent one of the most important classes of self-dual $\mathbf{Z}_4$-codes. In lengths 8, 24, 32, or 48 these codes are extremal type II codes [2], and are involved in the construction of even unimodular lattices, including the Leech lattice. But we must note that over this ring, the good constructions differ from that of $\mathbf{Z}_4$ case where free codes are the most interesting. Over R, we are not going to consider quadratic residue codes. We will prefer to consider codes whose rates k_1 and k_2 are approximately the same. Recently, it has been shown in [14] that non trivial cyclic self-dual $\mathbf{Z}_4$-codes of odd length n exist. This property also holds over R. In this section, we study such cyclic codes and their extensions. Most of their structural properties match those of self-dual $\mathbf{Z}_4$-codes. The condition for a cyclic code of odd length n to be self-dual is given by the following theorem.

Generator	Order	Properties	d_{Lee}	Binary Image
(uf_2f_3)	2		14	$[14,1,14]^\star$
(uf_1f_3)	2^3		8	$[14,3,8]^\star$
(uf_3)	2^4		6	$[14,4,6]$
(uf_1f_2)	2^3		8	$[14,3,8]^\star$
(uf_2)	2^4		6	$[14,4,6]$
(uf_1)	2^6		4	$[14,6,4]$
(u)	2^7		2	$[14,7,2]$
(f_2f_3)	4		7	$[14,2,7]$
$(f_2f_3,\, uf_1f_3)$	4.2^3		6	$[14,5,6]^\star$
$(f_2f_3,\, uf_1f_2)$	4.2^3		6	$[14,5,6]^\star$
$(f_2f_3,\, uf_1)$	4.2^6		2	$[14,8,2]$
(f_1f_3)	4^3	simplex over R	4	$[14,6,4]$
$(f_1f_3,\, uf_2f_3)$	$4^3.2$	self-dual	4	$[14,7,4]^\star$
$(f_1f_3,\, uf_1f_2)$	$4^3.2^3$		4	$[14,9,4]^\star$
$(f_1f_3,\, uf_2)$	$4^3.2^4$		2	$[14,10,2]$
(f_3)	4^4	extended self-dual	3	$[14,8,3]$
$(f_3,\, uf_1f_2)$	$4^4.2^3$		2	$[14,11,2]^\star$
(f_1f_2)	4^3	simplex over R	4	$[14,6,4]$
$(f_1f_2,\, uf_2f_3)$	$4^3.2$	self-dual	4	$[14,7,4]^\star$
$(f_1f_2,\, uf_1f_3)$	$4^3.2^3$		4	$[14,9,4]^\star$
$(f_1f_2,\, uf_3)$	$4^3.2^4$		2	$[14,10,2]$
(f_2)	4^4	extended self-dual	3	$[14,8,3]$
$(f_2,\, uf_1f_3)$	$4^4.2^3$		2	$[14,11,2]^\star$
(f_1)	4^6		2	$[14,12,2]^\star$
$(f_1,\, uf_2f_3)$	$4^6.2$		2	$[14,13,2]^\star$

Table 3: Examples of cyclic codes of length 7. The symbol "$\star$" means that the code is optimal.

Generator	Order	d_{Lee}	Properties	Binary Image
$(f_1f_4, uf_1f_2f_3f_5)$	$4^{10}2^4$	4		$[30, 24, 4]^\star$
$(f_1f_3, uf_1f_2f_4f_5)$	$4^{10}2^4$	4		$[30, 24, 4]^\star$
$(f_4f_5, uf_1f_2f_3f_4)$	4^72^4	5		$[30, 18, 5]$
$(f_3f_5, uf_1f_2f_3f_4)$	4^72^4	5		$[30, 18, 5]$
$(f_1f_4f_5, uf_2f_3f_4)$	4^62^5	6		$[30, 17, 6]$
$(f_1f_2f_3f_5, uf_3f_4)$	4^42^7	6	self-dual	$[30, 15, 6]$
$(f_1f_3f_5, uf_2f_3f_4)$	4^62^5	6		$[30, 17, 6]$
$(f_1f_3f_4, uf_2f_4f_5)$	4^62^5	6		$[30, 17, 6]$
$(f_1f_3f_4, uf_2f_3f_5)$	4^62^5	6		$[30, 17, 6]$
$(f_1f_2f_4f_5, uf_3f_4)$	4^42^7	6	self-dual	$[30, 15, 6]$
$(f_2f_3f_5, uf_1f_2f_4f_5)$	4^52^4	7		$[30, 14, 7]$
$(f_2f_4f_5, uf_1f_2f_3f_5)$	4^52^4	7		$[30, 14, 7]$
$(f_1f_2f_3f_5, uf_1f_3f_4)$	4^42^6	8		$[30, 14, 8]$
$(f_1f_2f_4f_5, uf_1f_3f_4)$	4^42^6	8		$[30, 14, 8]$
$(f_1f_3f_4f_5, uf_2f_4f_5)$	4^22^5	10		$[30, 9, 10]$
$(f_1f_3f_4f_5, uf_2f_3f_5)$	4^22^5	10		$[30, 9, 10]$
$(uf_1f_3f_5)$	2^6	12		$[30, 6, 12]$
$(uf_1f_3f_4)$	2^6	12		$[30, 6, 12]$
$(uf_1f_4f_5)$	2^6	12		$[30, 6, 12]$
$(uf_2f_3f_5)$	2^5	14		$[30, 5, 14]$
$(f_2f_3f_4f_5, uf_1f_2f_4f_5)$	4.2^4	14		$[30, 6, 14]^\star$
$(f_2f_3f_4f_5, uf_1f_2f_3f_5)$	4.2^4	14		$[30, 6, 14]^\star$
$(uf_2f_4f_5)$	2^5	14		$[30, 5, 14]$
$(f_2f_3f_4f_5)$	4	15		$[30, 2, 15]$
$(uf_1f_2f_4f_5)$	2^4	16		$[30, 4, 16]^\star$
$(uf_1f_2f_3f_5)$	2^4	16		$[30, 4, 16]$
$(uf_1f_3f_4f_5)$	2^4	20		$[30, 4, 20]^\star$

Table 4: Examples of cyclic codes of length 15. The symbol "$\star$" means that the code is optimal.

Theorem 4 *Let C be a cyclic code over R, $C = (fh, ufg)$ where $fgh = x^n - 1$, n odd. Then C is self-dual if and only if $f = g^\star$ and $h = h^\star$.*

Proof: Note that the factorization of $x^n - 1$ is the binary factorization. Hence [14, Theorem 2] holds with $\epsilon = 1$, where $\epsilon = f/g^\star = h/h^\star$. □

The condition of existence of a self-dual code of odd length n has been studied deeply in [14]. The following theorem is due to [14] which applies to codes over R.

Theorem 5 *Non trivial cyclic self-dual codes of length n exist if and only if $-1 \not\equiv 2^i \pmod{n}$ for any i.*

As a consequence of the above theorem, non trivial self-dual cyclic codes do not exist for lengths 17 and 19. Similarly to $\mathbf{Z}_4$ case, the conditions in the above theorem can be further refined by using a number theoretical result of Peter Moree [14, Appendix].

3.1 Examples

If C is self-dual of odd length n, it is always possible to construct an other self-dual code of length $n+1$. Let $C = (fh, ufg)$, then from Theorem 3, $x+1$ has to divide the polynomial h. Consider an R-cyclic code given by $\hat{C} = (f\hat{h}, uf\hat{g})$, where $\hat{g} = (x+1)g$ and $\hat{h} = h/(x+1)$. Then, the code formed by extending $\hat{C}$ is a self-dual code of length $n+1$. This construction is equivalent to the method using shadow codes in [6].

3.1.1 Length 21

For length 21, there exist three self-dual codes with different swe's. Among them, just one has good parameters. The factorization of $x^{21} + 1$ is equal to $f_1 f_2 f_3 f_4 f_5 f_6$, where

$$\begin{aligned} f_1 &:= x + 1, \\ f_2 &:= x^2 + x + 1, \\ f_3 &:= x^3 + x + 1, \\ f_4 &:= x^3 + x^2 + 1, \\ f_5 &:= x^6 + x^4 + x^2 + x + 1, \\ f_6 &:= x^6 + x^5 + x^4 + x^2 + 1. \end{aligned}$$

The most interesting code is $C21_1 := (fh,\ ufg)$ where $f := f_5,\ g := f_6,\ h := f_1 f_2 f_3 f_4$. It is a self-dual code of parameters $[21, 4^6 2^9, 6]$. Its swe is given in appendix.
Its binary Gray image has parameters $[42, 21, 6]$. It is possible to extend this code as explained at the beginning of this section. We obtain an extremal binary self-dual code of

parameters $[44, 22, 8]$ and weight distribution

Weights	Number of codewords
$8, 36$	196
$10, 34$	672
$12, 32$	11529
$14, 30$	49728
$16, 28$	209982
$18, 26$	483168
$20, 24$	826868
22	1030016

Note that this weight enumerator correspond in [7] to W_1 with $\beta = 38$.
The two other codes are less interesting since their minimum distance is only 4. Their binary Gray images are self-dual codes of parameters $[42, 21, 4]$. Their constructions are given in the following table.

Name	f	g	h	Order
$C21_2$	f_3	f_4	$f_1 f_2 f_5 f_6$	$4^3 2^{15}$
$C21_3$	$f_3 f_5$	$f_4 f_6$	$f_1 f_2$	$4^9 2^3$

3.1.2 Length 23

For length 23, there exists just one non trivial self-dual code: $C23$. The factorization of $x^{23} + 1$ is equal to $f_1 f_2 f_3$, where

$$\begin{aligned} f_1 &:= x + 1, \\ f_2 &:= x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1, \\ f_3 &:= x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1. \end{aligned}$$

$C23 := (fh,\ ufg)$ where $f := f_2,\ g := f_3,\ h := f_1$. It is a self-dual code of parameters $[23, 4^{11}2, 8]$. Its binary image is a self-dual $[46, 23, 8]$ code. The code $C23$ can also be extended to obtain a $[24, 12, 8]$ cyclic self-dual with binary Gray image of parameters $[48, 24, 8]$.

3.1.3 Length 31

In length 31, there exist five inequivalent cyclic self-dual codes according to the criterion given in [9]. Among them, just two have good parameters. The factorization of $x^{31} + 1$ is equal to $(x + 1) f_1 f_{1c} f_2 f_{2c} f_3 f_{3c}$, where

$$\begin{aligned} f_1 &:= 1 + x^2 + x^5, \\ f_{1c} &:= 1 + x^3 + x^5, \\ f_2 &:= 1 + x + x^2 + x^3 + x^5, \\ f_{2c} &:= 1 + x^4 + x^3 + x^2 + x^5, \\ f_3 &:= 1 + x + x^2 + x^4 + x^5, \\ f_{3c} &:= 1 + x^4 + x^3 + x + x^5. \end{aligned}$$

The most interesting code is $C31_1 := (fh,\ ufg)$ where $f := f_1 f_2,\ g := f_{1c} f_{2c},\ h := (1+x) f_3 f_{3c}$. It is a self-dual code of parameters $[31, 4^{10}2^{11}, 10]$. Its swe is given in Appendix. Note that the minimum distances of its residue and torsion code are respectively 10 and 5. Its Gray image is a self-dual binary (type I) code of parameters $[62, 31, 10]$ with weight distribution

Weights	Number of codewords
$10, 52$	186
$12, 50$	2046
$14, 48$	26195
$16, 46$	253673
$18, 44$	1726390
$20, 42$	8579746
$22, 40$	31945624
$24, 38$	90300520
$26, 36$	195388164
$28, 34$	325634540
$30, 32$	419884739

As explained in section 3.1, it is possible to construct a self-dual code of length 32 from $C31_1$. We obtain a $[32, 4^{11}2^{10}, 12]$ code with swe given in appendix.
Its Gray image is an extremal binary self-dual type II code with parameters $[64, 32, 12]$ and weight distribution

Weights	Number of codewords
$12, 52$	2976
$16, 48$	454956
$20, 44$	18275616
$24, 40$	233419584
$28, 36$	1041971008
32	1706719014

The second interesting code, $C31_2$, has the same parameters as $C31_1$. We have $C31_2 := (fh,\ ufg)$ where $f := f_1 f_{1c},\ g := f_2 f_{2c},\ h := (1+x) f_3 f_{3c}$. Similarly, this code gives self-dual codes of lengths 32 over R and 62 and 64 over F_2 with same weight enumerators.
The three other self-dual codes correspond to the case where the difference between the rates k_1 and k_2 is large. Hence, they have bad parameters in the sense that their minimum distance is less than or equal to 8. Their constructions are given in the following table.

Name	f	g	h	Order
$C31_3$	f_1	f_{1c}	$(1+x) f_2 f_{2c} f_3 f_{3c}$	$4^5 2^{21}$
$C31_4$	$f_1 f_2 f_3$	$f_{1c} f_{2c} f_{3c}$	$1+x$	$4^{15} 2^1$
$C31_5$	$f_1 f_{2c} f_3$	$f_{1c} f_2 f_{3c}$	$1+x$	$4^{15} 2^1$

Note that it is possible to obtain self-dual R-codes of lengths 35 and 39, but they are not extremal in view of Lemma 5.

4 Conclusion

We studied cyclic codes over F_2+uF_2 and constructed some interesting self-dual cyclic codes over this ring. The generalization to $F_p + uF_p + \cdots + u^kF_p$ may be of interest in coding theory. These rings have already been used in the construction of optimal frequency hopping sequences [18].
We think codes over $F_2 + uF_2$ could be of importance because of two reasons:

1 They can lead to optimal linear binary codes. We have given such good codes in lengths 42, 44, 62 and 64. Furthermore, a type II $[24, 12, 12]$ R-code has also been obtained in [6].

2 These codes are interesting from a decoding point of view. The binary Gray image of a code over $F_2 + uF_2$ can be decoded in the ring [17]. This means that the decoding problem for a code of length $2n$ changes to one of length n. Since the characteristic of the ring is two, we obtain considerable advantage in decoding complexity.

The next length to consider is 63. In this length, we may get a binary code whose performance could be compared to the $[127, 78, 15]$ BCH code used in the industry to convert data rates from 9.6 Kbps to 16 Kbps.

The advantage of this ring compared to $\mathbf{Z}_4$ is mainly due to the fact that our codes can be easily decoded and implemented. Even though the minimum distance of the Gray images of these codes are not as good as some exceptional $\mathbf{Z}_4$ cyclic codes, they can correct naturally some extra burst errors along with random errors [17].

Appendix

The swe of the self-dual code $C21_1 := (fh,\ ufg)$ of parameters $[21, 4^6 2^9, 6]$, where $f := f_5,\ g := f_6,\ h := f_1f_2f_3f_4$.

$$
\begin{aligned}
&x^{21} + 28x^{18}z^3 + 84x^{17}z^4 + 273x^{16}z^5 + 924x^{15}z^6 + \\
&1956x^{14}z^7 + 84x^{13}y^8 + 2982x^{13}z^8 + 1092x^{12}y^8z + 4340x^{12}z^9 + \\
&6552x^{11}y^8z^2 + 5796x^{11}z^{10} + 24024x^{10}y^8z^3 + 5796x^{10}z^{11} + 2688x^9y^{12} + \\
&60060x^9y^8z^4 + 4340x^9z^{12} + 24192x^8y^{12}z + 108108x^8y^8z^5 + \\
&2982x^8z^{13} + 96768x^7y^{12}z^2 + 144144x^7y^8z^6 + 1956x^7z^{14} + \\
&225792x^6y^{12}z^3 + 144144x^6y^8z^7 + 924x^6z^{15} + 338688x^5y^{12}z^4 + \\
&108108x^5y^8z^8 + 273x^5z^{16} + 338688x^4y^{12}z^5 + 60060x^4y^8z^9 + \\
&84x^4z^{17} + 225792x^3y^{12}z^6 + 24024x^3y^8z^{10} + 28x^3z^{18} + \\
&96768x^2y^{12}z^7 + 6552x^2y^8z^{11} + 24192xy^{12}z^8 + 1092xy^8z^{12} + \\
&2688y^{12}z^9 + 84y^8z^{13} + z^{21}.
\end{aligned}
$$

The swe of $C31_1$ is

$$x^{31} + 142600\,x^{12}z^{19} + 2635\,x^7z^{24} + 806\,x^6z^{25} + 186\,x^5z^{26} + 190464\,y^{20}z^{11} + 33728\,y^{16}z^{15} +$$
$$31426560\,x^8y^{20}z^3 + 1201560\,x^{16}y^{12}z^3 + 31426560\,x^3y^{20}z^8 + 62853120\,x^7y^{20}z^4 +$$
$$4806240\,x^{15}y^{12}z^4 + 186\,x^{26}z^5 + 7905\,x^{23}z^8 + 2635\,x^{24}z^7 +$$
$$85560\,x^{11}z^{20} + 195300\,x^{13}z^{18} + 33728\,x^{15}y^{16} + 23560\,x^{18}y^{12}z + 190464\,x^{11}y^{20} + 41602\,x^{10}z^{21} +$$
$$18910\,x^{22}z^9 + 301971\,x^{15}z^{16} + 212040\,x^2y^{12}z^{17} + 251100\,x^{14}z^{17} + 85560\,x^{20}z^{11} +$$
$$251100\,x^{17}z^{14} + 1240\,x^{19}y^{12} + 41602\,x^{21}z^{10} + 212040\,x^{17}y^{12}z^2 + 195300\,x^{18}z^{13} + 33643680\,x^6y^{12}z^{13} +$$
$$301971\,x^{16}z^{15} + 142600\,x^{19}z^{12} + 18910\,x^9z^{22} + 3541440\,x^{13}y^{16}z^2 + 7905\,x^8z^{23} +$$
$$1240\,y^{12}z^{19} + z^{31} + 806\,x^{25}z^6 + 62481120\,x^{12}y^{12}z^7 + 46038720\,x^{11}y^{16}z^4 +$$
$$93721680\,x^{11}y^{12}z^8 + 2095104\,x^{10}y^{20}z + 101285184\,x^{10}y^{16}z^5 + 114548720\,x^{10}y^{12}z^9 +$$
$$10475520\,x^9y^{20}z^2 + 168808640\,x^9y^{16}z^6 + 114548720\,x^9y^{12}z^{10} + 217039680\,x^8y^{16}z^7 +$$
$$93721680\,x^8y^{12}z^{11} + 217039680\,x^7y^{16}z^8 + 62481120\,x^7y^{12}z^{12} + 87994368\,x^6y^{20}z^5 +$$
$$168808640\,x^6y^{16}z^9 + 87994368\,x^5y^{20}z^6 + 101285184\,x^5y^{16}z^{10} + 14418720\,x^5y^{12}z^{14} +$$
$$505920\,xy^{16}z^{14} + 505920\,x^{14}y^{16}z + 14418720\,x^{14}y^{12}z^5 + 33643680\,x^{13}y^{12}z^6 + 15346240\,x^{12}y^{16}z^3 +$$
$$62853120\,x^4y^{20}z^7 + 46038720\,x^4y^{16}z^{11} + 4806240\,x^4y^{12}z^{15} + 15346240\,x^3y^{16}z^{12} +$$
$$1201560\,x^3y^{12}z^{16} + 10475520\,x^2y^{20}z^9 + 3541440\,x^2y^{16}z^{13} + 2095104\,xy^{20}z^{10} + 23560\,xy^{12}z^{18}.$$

The swe of the self-dual code of parameters $[32, 4^{11}2^{10}, 12]$ obtained by extending $C31_1$ as explained in section 3.1.

$$249924480\,x^8y^{12}z^{12} + 868158720\,x^8y^{16}z^8 + 251412480\,x^8y^{20}z^4 + 366555904\,x^{10}y^{12}z^{10} +$$
$$540187648\,x^{10}y^{16}z^6 + 33521664\,x^{10}y^{20}z^2 + 249924480\,x^{12}y^{12}z^8 + 122769920\,x^{12}y^{16}z^4 +$$
$$76899840\,x^{14}y^{12}z^6 + 8094720\,x^{14}y^{16}z^2 + 9612480\,x^{16}y^{12}z^4 + 376960\,x^{18}y^{12}z^2 +$$
$$469303296\,x^6y^{20}z^6 + 540187648\,x^6y^{16}z^{10} + 76899840\,x^6y^{12}z^{14} + 251412480\,x^4y^{20}z^8 +$$
$$122769920\,x^4y^{16}z^{12} + 9612480\,x^4y^{12}z^{16} + 33521664\,x^2y^{20}z^{10} + 8094720\,x^2y^{16}z^{14} +$$
$$376960\,x^2y^{12}z^{18} + x^{32} + 2097152\,y^{32} + z^{32} + 992\,x^{26}z^6 + 10540\,x^{24}z^8 + 60512\,x^{22}z^{10} +$$
$$1984\,x^{20}y^{12} + 228160\,x^{20}z^{12} + 446400\,x^{18}z^{14} + 67456\,x^{16}y^{16} + 603942\,x^{16}z^{16} + 446400\,x^{14}z^{18} +$$
$$507904\,x^{12}y^{20} + 228160\,x^{12}z^{20} + 60512\,x^{10}z^{22} + 10540\,x^8z^{24} + 992\,x^6z^{26} + 507904\,y^{20}z^{12} +$$
$$67456\,y^{16}z^{16} + 1984\,y^{12}z^{20}.$$

Acknowledgement

We wish to thank Serdar Boztas, Masaaki Harada, Vera Pless and Patrick Solé for their comments on the manuscript. We also thank the referees for their useful comments which improved the presentation of the paper.

References

[1] C. Bachoc. Application of Coding Theory to the Construction of Modular Lattices. *J.C.T. series A*, 1997.

[2] A. Bonnecaze, P. Solé, C. Bachoc, and B. Mourrain. Type II codes over Z_4. *IEEE Trans. Inform Theory*, 43:969–976, 1997.

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

[4] G. Castagnoli, J.L. Massey, P.A. Scholler, and N. von Seeman. On Repeated-Root Cyclic Codes. *IEEE Trans. Inform. Theory*, 37:337–342, 1991.

[5] H.L. Clasen. *Studies of the Multiplications in* $GF(q)[x]/(a(x))$. PhD thesis, Delft University of Technology, Netherlands, 1978.

[6] S.T. Dougherty, P. Gaborit, M. Harada, and P. Solé. Type II and Type IV Codes over F2+uF2. *preprint*, 1997.

[7] S.T. Dougherty, A. Gulliver, M. Harada. Extremal Binary Self-Dual Codes. *IEEE Trans. Inform. Theory*, 43:2036–2047, 1997.

[8] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, and P. Solé. The Z_4-Linearity of Kerdock, Preparata, Goethals and Related Codes. *IEEE Trans. Inform. Theory*, 40:301–319, 1994.

[9] W.C. Huffman, V. Job and V. Pless, Multipliers and Generalized Multipliers of Cyclic Objects and Cyclic Codes. *J. Combin. Theory 62, No. 2, 183-215, March 1993.*

[10] C.L. Liu, B. G. Ong and G. R. Ruth. A Construction Scheme for Linear and Non-Linear Codes. *Discrete Mathematics*, 4:171–184, 1973.

[11] B.R. McDonald. *Finite Rings with Identity*. Marcel Dekker, Pure and Applied Mathematics, 1974.

[12] V. Pless. A Classification of Self-Orthogonal Codes over $GF(2)$. *Discrete Math.*, 3:209–246, 1972.

[13] V. Pless and Z. Qian. Cyclic Codes and Quadratic Residue Codes over Z_4. *IEEE Trans. Inform. Theory*, 42:1594–1600, 1996.

[14] V. Pless, P. Solé, and Z. Qian. Cyclic Self-Dual Z_4-Codes. *Finite Fields and their applications*, 3:48–69, 1997.

[15] E.M. Rains and N.J.A. Sloane. Self-Dual Codes. *preprint written for the Handbook of Coding Teory*, 1997.

[16] N.J.A. Sloane and J.G. Thompson. Cyclic Self-Dual Codes. *IEEE Trans. Inform. Theory*, 29:364–366, 1983.

[17] P. Udaya and .A. Bonnecaze, Decoding Cyclic Codes over $F_2 + uF_2$. *Submitted*, 1998.

[18] P. Udaya and M.U. Siddiqi. Optimal Large Linear Complexity Frequency Hopping Patterns Derived from Polynomial Residue Class Rings. *Submitted*, 1995.