Skew Constacyclic Codes over Galois Rings

D. Boucher[*], P. Solé[†] and F. Ulmer[‡]

January 21, 2008

Abstract

We generalize the construction of linear codes via skew polynomial rings by using Galois rings instead of finite fields as coefficients. The resulting non commutative rings are no longer left and right Euclidean. Codes that are principal ideals in quotient rings of skew polynomial rings by a two sided ideals are studied. As an application, skew constacyclic self-dual codes over $GR(4^2)$ are constructed. Euclidean self-dual codes give self-dual $\mathbb{Z}_4-$codes. Hermitian self-dual codes yield $3-$modular lattices and quasi-cyclic self-dual $\mathbb{Z}_4-$codes.

Keywords: cyclic codes, skew polynomial rings, self-dual codes, $\mathbb{Z}_4-$codes, modular lattices

Introduction

Polynomial rings and their ideals are essential to the construction and understanding of cyclic codes. For the first time in [5] *non commutative* skew polynomial rings have been instead of linearized polynomials used to construct a generalization of cyclic codes. In that approach, it is necessary to use as alphabet a finite field with a non trivial Galois automorphism, like, e.g. $\mathbb{F}_4$. In the present work we extend that approach by considering as alphabets Galois rings of even characteristic like, e.g. $GR(4^2)$. The technical difficulty in passing from field alphabet to ring alphabet is that the skew polynomial rings are not Ore rings; in particular they are no longer left and right Euclidean. However, left and right division by unitary polynomials are still well defined. Therefore codes that are principal ideals generated by unitary polynomials in quotient rings of skew polynomial rings by a two sided ideal are studied. In particular the problem of finding central polynomials, that is generators of principal two sided ideals is addressed.

As an application self-dual codes over $GR(4^2)$ are constructed, and used for three of the four applications of [14].

1)*Self-dual Euclidean codes give self-dual $\mathbb{Z}_4$ codes by projection on a trace orthogonal basis.* Many Type I codes in length 24 are obtained and classified by the root systems of their Construction A lattice. New coding constructions of the Odd Leech lattice, the only unimodular lattice of norm 3 in dimension 24 are given thus supplementing the results of [15]. Some new Type II codes in length 24 are also obtained, that yield the Leech lattice by Construction A, though not being Lee-optimal in the sense of Rains [20]. A Type I code in length 40 is constructed that is not Type IV. In fact its Lee and Euclidean distance are better than what would be possible for a Type IV code of that length [9].

2)*Self-dual Hermitian codes build 3-modular lattices.* In particular a simpler construction of one of the two extremal such lattices in dimension 28 is given.

[*] IRMAR, Université de Rennes I, Campus de Beaulieu, 35 042 Rennes, France

[†] I3S, 2000 route des Lucioles, 06903 Sophia Antipolis, France

[‡] IRMAR, Université de Rennes I, Campus de Beaulieu, 35 042 Rennes, France

3)*Self-dual Hermitian codes yield self-dual quasi-cyclic codes over $\mathbb{Z}_4$ by the cubic construction.* Self-dual Type II codes are obtained in length 24 and classified by their symmetrized weight enumerator and root system.

The material is organized as follows. Section 1 contains generalities on skew polynomial rings over Galois rings. Section 2 defines the codes generated by principal ideals in quotient rings where $X^n - 1$ is replaced by a central polynomial. Section 3 explains how to generate central polynomials by using the notion of bound and gives a few examples. Section 4 considers parity check matrices and duals of the constacyclic codes defined before. Section 5 constructs Euclidean self-dual codes over $GR(4^2)$. Section 6 is devoted to self-dual $\mathbb{Z}_4$ codes and their unimodular lattices. Section 7 studies Hermitian self-dual codes over $GR(4^2)$ and $3-$modular lattices. Section 8 considers the cubic construction of self-dual $\mathbb{Z}_4$ codes from Hermitian self-dual codes over $GR(4^2)$.

1 Skew polynomials over Galois rings and their quotients

We follow the presentation of the finite Galois ring $GR(4^m)$ given in [23]. Denote $\mathbb{Z}_4$ the ring $\mathbb{Z}/4\mathbb{Z}$ and consider the homomorphism

$$\begin{array}{rcl} \varphi\colon \mathbb{Z}_4 & \rightarrow & \mathbb{Z}_2 = \mathbb{F}_2 \\ 0,2 & \mapsto & 0 \\ 1,3 & \mapsto & 1 \end{array}$$

and denote by $\overline{a}$ the image $\varphi(a)$. There is a natural extension

$$\begin{array}{rcl} \tilde{\varphi}\colon \mathbb{Z}_4[X] & \rightarrow & \mathbb{Z}_2[X] = \mathbb{F}_2[X] \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \overline{a_i} X^i \end{array}$$

We again denote by $\overline{f}$ the image $\tilde{\varphi}(f)$.

We define $GR(4^m)$ as the ring $\mathbb{Z}_4[X]/(h)$ where $h \in \mathbb{Z}_4[X]$ is a monic polynomial of degree m such that $\overline{h} \in \mathbb{F}_2[X]$ is a primitive irreducible polynomial with the property that the root $\xi = \tilde{X}$ of $\overline{h}$ in $\mathbb{F}_2[X]/(\overline{h})$ is a generator of the multiplicative group of the field. In the following we will use the fact that each element of $GR(4^m)$ can be uniquely written as $\alpha_0 + \alpha_1\xi + \ldots + \alpha_{m-1}\xi^{m-1}$ with $\alpha_i \in \mathbb{Z}_4$ for $0 \leq i \leq m-1$.
To define an automorphism it is more convenient to use the 2-Adic representation in which the elements of $GR(4^m)$ are uniquely written as $a + 2b \in GR(4^m)$ where a and b belong to $\{0, 1, \xi, \ldots, \xi^{2^m-2}\}$ ([23], Section 6.2). We denote by θ the generalized Frobenius map $a + 2b \mapsto a^2 + 2b^2$, which is a ring automorphism of $GR(4^m)$ of order m. The group of automorphisms of $GR(4^m)$ is cyclic of order m and generated by θ. The subring of those elements that are left fixed by θ are the elements of $\mathbb{Z}_4$ (cf. [23], Theorem 6.11). In the following we denote by $GR(4^m)^*$ the set of invertible elements and we use the fact that this set is left invariant by all automorphisms θ^i.

One defines a ring structure on the set

$$GR(4^m)[X,\theta] \;=\; \{\alpha_n X^n + \ldots + \alpha_1 X + \alpha_0 \mid \alpha_i \in GR(4^m) \text{ and } n \in \mathbb{N}\}$$

of formal polynomials where the coefficients are written on the left of the variable X. The addition in $GR(4^m)[X,\theta]$ is defined to be the usual addition of polynomials and the multiplication is defined by the basic rule $X\alpha = \theta(\alpha)X$ ($\alpha \in GR(4^m)$) and extended to all elements of $GR(4^m)[X,\theta]$ by associativity and distributivity. As usual two polynomials are equal if and only if all their coefficients are equal.

Lemma 1 *The center $Z(GR(4^m)[X,\theta])$ of $GR(4^m)[X,\theta]$ is $\mathbb{Z}_4[X^m]$.*

PROOF. The subring of the elements of $GR(4^m)$ that are fixed by θ is $\mathbb{Z}_4$ (cf. [23], Theorem 6.11). For any integer $i \in \mathbb{N}$, the power $X^{i\,m}$ is also in the center $Z(GR(4^m)[X,\theta])$ of $GR(4^m)[X,\theta]$. This follows form the fact that m is the order of the automorphism θ, showing that for any $a \in GR(4^m)[X,\theta]$ we have $X^{i\,m}a = (\theta^m)^i(a)X^{i\,m} = aX^{i\,m}$. This shows that $f = \beta_0 + \beta_1X^m + \beta_2X^{2m} + \ldots + \beta_sX^{s\,m}$ with $\beta_i \in \mathbb{Z}_4$ is a central element. Conversely, for f in $Z(GR(4^m)[X,\theta])$, considering $Xf - fX$ and $\alpha f - f\alpha$ for $\alpha \in GR(4^m)$ one proves that $f \in \mathbb{Z}_4[X^m]$. ■

Since $GR(4^m)$ contains zero divisors, many properties of skew polynomial rings over fields are no longer true :

EXAMPLE. The following are two distinct factorizations of $X^4 - 1 \in GR(4^2)[X,\theta]$ into irreducible monic polynomials $(X+1)(X+1)(X+2\xi+1)(X+2\xi+3)$ and $(X^2+2\xi+1)(X^2+2\xi+3)$. This shows that the degrees in different factorizations of the same polynomial are not unique up to permutation. ■

The ring $GR(4^m)[X,\theta]$ is no longer left or right Euclidean, but left or right division can be defined for some elements. Consider $f = \sum_{i=0}^{s}\alpha_iX^i$ and $g = \sum_{j=0}^{t}\beta_jX^j$. If $s \geq t$ and the leading coefficients β_t of g is invertible, then:

1. We can define a right division of f by g. We simply note that the degree of

$$f \;-\; \frac{\alpha_s}{\theta^{s-t}(\beta_t)}X^{s-t}g$$

is less than the degree of f. To prove this, it is sufficient to compute the leading coefficients of both polynomials and see that they cancel. In the above we use the fact that θ^{s-t} is also an automorphism and that the image of an invertible element is invertible. Iterating the above by subtracting further left multiples of g from the result until the degree is less than the degree of g, we obtain polynomials $\tilde{q}$ and $\tilde{r}$ such that $\deg(\tilde{r}) < \deg(g)$ (as usual we set the degree of 0 to be $-\infty$) and

$$f \;=\; \tilde{q}\,g \;+\; \tilde{r}$$

If $\tilde{r} = 0$ we say that g is a right divisor of f.

2. Similarly to the right division, we can define a left division of f by g using the fact that the degree of

$$f \;-\; g\left(\theta^{-t}\left(\frac{\alpha_s}{\beta_t}\right)X^{s-t}\right)$$

is less than the degree of f. To prove this, it is again sufficient to compute the leading coefficients of both polynomials and see that they cancel. In the above we use the fact that θ^{-t} is also an automorphism and that the image of β_t is again an invertible element. Iterating the above by subtracting further right multiples of g from the result until the degree is less than the degree of g, we obtain polynomials $\tilde{q}$ and $\tilde{r}$ such that $\deg(\tilde{r}) < \deg(g)$ and

$$f \;=\; g\,\tilde{q} \;+\; \tilde{r}$$

If $\tilde{r} = 0$ we say that g is a left divisor of f.

We will also need the fact that the remainder of a division of f by a monic polynomial $g \in GR(4^2)[X, \theta]$ is unique. Suppose

$$f = \tilde{q}_1\, g + \tilde{r}_1 = \tilde{q}_2\, g + \tilde{r}_2$$

are two right divisions by g, then

$$(\tilde{q}_1 - \tilde{q}_2)\, g = \tilde{r}_2 - \tilde{r}_1.$$

If $\tilde{q}_1 - \tilde{q}_2$ is not zero, then the right polynomial is of degree at least the degree of g, while the right polynomial is of degree at most one less than the degree of g. Therefore $\tilde{q}_1 = \tilde{q}_2$, from which we get $\tilde{r}_2 = \tilde{r}_1$. The proof for left division is similar.

Example. In $GR(4^2)[X, \theta]$ the polynomial $X - \xi$ is a right divisor of $X^2 - 1$. This is obtained via

$$(X^2 - 1) - X(X - \xi) \;=\; X^2 - 1 - X^2 + X\xi \;=\; \xi^2 X - 1$$

(here $X\xi = \theta(\xi)X = \xi^2 X$) and in the next step

$$(\xi^2 X - 1) - \xi^2(X - \xi) \;=\; \xi^2 X - 1 - \xi^2 X + \xi^3 \;=\; 0$$

Therefore the remainder is 0 and the left quotient (of the right division) is $X + \xi^2$. We get

$$X^2 - 1 \;=\; (X + \xi^2)\,(X - \xi)$$

■

Note that not all left or right ideals in $GR(4^m)[X, \theta]$ are principal, but in the following we will focus on those ideals. If $I \subseteq GR(4^m)[X, \theta]$ is a two sided ideal, then, by the correspondence of ideals, the left (resp. right) ideals of $GR(4^m)[X, \theta]/I$ are the left (resp. right) ideals of $GR(4^m)[X, \theta]$ containing I.

2 Codes defined by principal ideals with monic generator

Lemma 2 *A left or right ideal in $GR(4^m)[X, \theta]$ generated by a monic central element $f \in \mathbb{Z}_4[X^m]$ of degree n is a two sided principal ideal. The skew polynomials of degree less than n are canonical representatives of the elements of $GR(4^m)[X, \theta]/(f)$. Any right divisor g of f of degree r generates a left principal ideal $(g)/(f)$ in $GR(4^m)[X, \theta]/(f)$. The set of left multiples of g by skew polynomials of degree $k = n - r$ are canonical representatives in $GR(4^m)[X, \theta]/(f)$ of the elements of $(g)/(f)$. In particular the ideal $(g)/(f)$ has the structure of a submodule of $GR(4^m)^n$ and the coefficient vectors of the elements of $(g)/(f)$ form an $[n, k]$ code.*

Proof. Consider the left ideal $(f) \subseteq GR(4^m)[X, \theta]$. Since f is monic, the degree of any non zero $h = t\, f \in (f)$ is at least the degree of f. Since f is a central element, we also have $h = f\, t$ and a left division of h by f is of the form $h = f\, \tilde{q} + \tilde{r}$. Since $\tilde{r} = h - f\, \tilde{q} = h - \tilde{q}\, f \in (f)$ is of degree less than f we have $\tilde{r} = 0$, showing that $h = f\, \tilde{q}$. The reverse inclusion is obtained in a similar way, showing that the left and right ideals generated by f coincide. Therefore the left or right ideal (f) is a two sided ideal.

In $GR(4^m)[X, \theta]/(f)$ an element h can be identified with its unique remainder by left (or right) division by f. Therefore the skew polynomials of degree less than n, corresponding to the possible remainders, are canonical representatives of the elements of $GR(4^m)[X, \theta]/(f)$.

For a right divisor g of f of degree r, the ideal (f) is contained in the left ideal (g). By the correspondence of left ideals we have that $(g)/(f)$ is a left ideal in $GR(4^m)[X, \theta]/(f)$. With the above choice of skew polynomials of degree less than n as canonical representants of the elements of $GR(4^m)[X,\theta]/(f)$, the elements of $(g)/(f)$ are left multiples of g by skew polynomials of degree $k = n - r$. The claim now follows. ∎

As we will see later, not all ideals in the quotient ring $GR(4^m)[X,\theta]/(f)$ are principal ideals.

Definition 1 *A **θ-principal code** over $GR(4^m)$ is the set of coefficient vectors of the code corresponding to an ideal $(g)/(f)$ where $f \in \mathbb{Z}_4[X^m]$ is a monic central polynomial and g a monic right divisor of f.*
*A **θ-cyclic code** over $GR(4^m)$ is a θ-principal code over $GR(4^m)$ where f is of the form $X^n - 1$.*
*A **θ-constacyclic code** over $GR(4^m)$ is a θ-principal code over $GR(4^m)$ where f is of the form $X^n - c$ for $c \in \mathbb{Z}_4$.*

A θ-constacyclic code $\mathcal{C}$ over $GR(4^m)$ is a left ideal $I \subset GR(4^m)[X,\theta]/(X^n - c)$. In particular let $(a_0, a_1, \ldots, a_{n-1}) \in \mathcal{C}$, then $p = a_0 + a_1 X + \ldots + a_{n-1}X^n \in I$. Now $X\,p$ also belongs to I:

$$\begin{aligned} X\,p &= X\,(a_0 + a_1 X + \ldots + a_{n-1}X^n) \\ &= \theta(a_0)X + \theta(a_1)X^2 + \ldots + \theta(a_{n-2})X^{n-1} + \theta(a_{n-1})X^n \\ &= c\,\theta(a_{n-1}) + \theta(a_0)X + \theta(a_1)X^2 + \ldots + \theta(a_{n-2})X^{n-1}. \end{aligned}$$

Therefore $(c\,\theta(a_{n-1}), \theta(a_0), \theta(a_1), \ldots, \theta(a_{n-2})) \in \mathcal{C}$. For θ-cyclic code we have $c = 1$ and we obtain the classical property of cyclic codes when θ is the identity, which justifies the above terminology.

If $g = X^r + g_{r-1}X^{r-1} + \ldots + g_1 X + g_0 \in GR(4^m)[X,\theta]$ divides a polynomial $f \in \mathbb{Z}_4[X^m]$ of degree n, then the generating matrix of the θ-code of type $[n, n-r]$ generated by g is given by

$$G = \begin{pmatrix} g_0 & \ldots & g_{r-1} & 1 & 0 & \ldots & 0 \\ 0 & \theta(g_0) & \ldots & \theta(g_{r-1}) & 1 & \ldots & 0 \\ 0 & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \ldots & 0 & \theta^{n-r-1}(g_0) & \ldots & \theta^{n-r-1}(g_{r-1}) & 1 \end{pmatrix}$$

Note that instead of monic polynomials we could also consider polynomials with invertible leading coefficient. However the set of codes obtained by the above construction would be the same.

Example. The following two factorizations of $X^4 - 1 \in GR(4^2)[X,\theta]$ into irreducible monic polynomials $(X+1)\,(X+1)\,(X+2\xi+1)\,(X+2\xi+3)$ and $(X^2+2\xi+1)\,(X^2+2\xi+3)$ give four θ-cyclic codes defined by the corresponding right factors. ∎

Example. In $GR(4^2)[X,\theta]$ the ideal (X^2-1) is principal. Since $X - \xi$ is a right divisor of $X^2 - 1$, the ideal $(X^2 - 1)$ is contained in the left ideal $(X - \xi)$. By the correspondence of ideals the left multiple of $X - \xi$ form a left ideal. ∎

3 The length of a θ-principal code

This section is a generalization of [6], Section2. We will show that any monic skew polynomial $g \in GR(4^m)[X,\theta]$ divides a central polynomial $f \in \mathbb{Z}_4[X^m]$ generating a two sided ideal and therefore is the generating polynomial of some θ-principal code. The degree N of the central polynomial $f \in \mathbb{Z}_4[X^m]$ of smallest degree that g divides is the minimum numbers of rows that the previous generating matrix has to contain in order for the resulting code to be a θ-principal code over $GR(4^m)$, i.e. for the corresponding code to have the structure of a principal ideal in the quotient of $GR(4^m)[X,\theta]$ by a principal ideal generated by a unitary central polynomial. Therefore N is a bound for the length a θ-principal code over $GR(4^m)$ generated by g.

Definition 2 *(cf [16]) An element $P \in GR(4^m)[X,\theta]$ is bounded if the left ideal (P) contains a two sided ideal (P^*). In this case P^* is a bound for P.*

We adapt the proof of Theorem 15 in [16]. From [23] Chapter 6 we get that $GR(4^m) = \mathbb{Z}_4[\xi]$, showing that $GR(4^m)$ is a free $\mathbb{Z}_4$ module of dimension m.

Lemma 3 *If $P \in GR(4^m)[X,\theta]$ is of degree n, then there exists a bound P^* for P of degree at most $m^2\, n$.*

Proof. The elements in $GR(4^m)[X,\theta]$ of degree less than n form a $GR(4^m)$ module of dimension n and therefore a free $\mathbb{Z}_4$ module of dimension $m\,n$. Considering the remainders of the division

$$X^{m\,i} \;=\; Q_i\,P \;+\; R_i, \qquad i = 0,1\ldots,m\,n,$$

with $\deg(R_i) < n$, there exists a non trivial linear combination $\sum_{i=0}^{m\,n} \delta_i R_i = 0$ where $\delta \in \mathbb{Z}_4$. This shows that

$$\sum_{i=0}^{m\,n} \delta_i X^{m\,i} \;=\; \left(\sum_{i=0}^{m\,n} \delta_i Q_i\right) P.$$

The above polynomial $\sum_{i=0}^{m\,n} \delta_i X^{m\,i}$ is a bound for P. ∎

This degree bound can be improved in the special case of $GR(4^2)$.

Lemma 4 *If $P \in GR(4^2)[X,\theta]$ is of degree n, then there exists a bound P^* for P of degree at most $2n$.*

Proof. Write $P = \sum_{i=0}^{n} P_i X^i$. Define $\hat{P} = \sum_{i=0}^{n} (-1)^{i+1}\theta^{i+1} P_i X^i$. By checking that the coefficients of the odd powers of X in $Q := P\hat{P}$ vanish, we can apply Lemma 1 to show that Q is a bound for P. ∎

As the bound of a polynomial $g \in GR(4^2)[X,\theta]$ of degree r is at most of degree $2r$, such a polynomial will always generate a θ-principal code of length $\leq 2r$. Since the explicit knowledge of the bound g^* is not needed in the generating matrix of the θ-principal code $(g)/(g^*)$, it is easy to compute all codes of length n for generator polynomials of degree $r = n - k$ at most $n/2$.

We will use the following mapping from $GR(4^2)$ to $\mathbb{Z}_4$:

1. To each line of the generator matrix of the code over $GR(4^m)$, we add a line whose entries are multiplied by ξ.

2. The entry $a + \xi b$ is replaced by the two entries $3a$ and $a + b$.

Example. In $GR(4^2)[X,\theta]$ the polynomial $X^2 + \xi\,X + \xi + 1$ is a right divisor of the central polynomial $X^4 + 1$. We obtain a θ-constacyclic code whose generator matrix is

$$\begin{pmatrix} \xi+1 & \xi & 1 & 0 \\ 0 & 3\xi & 3\xi+3 & 1 \end{pmatrix}$$

the first step of the above transformation gives

$$\begin{pmatrix} \xi+1 & \xi & 1 & 0 \\ 3 & 3\xi+3 & \xi & 0 \\ 0 & 3\xi & 3\xi+3 & 1 \\ 0 & \xi+1 & 1 & \xi \end{pmatrix}$$

and the second step gives

$$\begin{pmatrix} 3 & 2 & 0 & 1 & 3 & 1 & 0 & 0 \\ 1 & 3 & 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 3 & 1 & 2 & 3 & 1 \\ 0 & 0 & 3 & 2 & 3 & 1 & 0 & 1 \end{pmatrix}$$

which is the generator matrix of the code over $\mathbb{Z}_4$. ■

The following are the best codes over $\mathbb{Z}_4$ obtained this way, compared to the best known codes. In order to obtain a binary codes from a code over $\mathbb{Z}_4$ we are using the Gray map (cf. [7]), which is a weight- and distance-preserving map from $\mathbb{Z}_4^n$ (with Lee weight metric) to $\mathbb{Z}_2^{2n}$ (with Hamming weight metric). For each n and k we compute all $[n,k]$ θ-principal codes over $GR(4^2)$ and find the best minimal Lee weight d of these codes over $\mathbb{Z}_4$. In the table, both n and k have been multiplied by 4, $A(n,d)$ is the size of the largest binary code of length n and the Hamming distance d obtained from the table in [10].

$n \setminus k$	4		8		12		16		20		24		28	
	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$	d	$\vert\mathcal{C}\vert$
8	4	2^4												
best :	$A_7^3 = 2^4$													
16	8	2^4	6	2^8										
best :	$A_{15}^7 = 2^5$		$A_{15}^5 = 2^8$											
24	12	2^4	8	2^8	6	2^{12}	4	2^{16}						
best :	$A_{23}^{11} = 2^4 3$		$A_{23}^7 = 2^{12}$		$A_{23}^5 = 2^{14}$		$A_{23}^3 = 2^{15} 9$							
32							8	2^{16}	5	2^{20}	4	2^{24}		
best :							$A_{31}^7 = 2^{17}$		$\frac{A_{33}^5}{2} \geq 2^{22}$		$A_{31}^3 = 2^{26}$			
40									8	2^{20}	6	2^{24}	4	2^{28}
best :									$\frac{A_{41}^9}{2} \geq 2^{20}$		$\frac{A_{63}^5}{2^{24}} \geq 2^{28}$		$A_{39}^3 = 5 \cdot 2^{31}$	
48											10	2^{24}	8	2^{28}
best :											$A_{47}^9 = 2^{21} 17$		$\frac{A_{63}^7}{2^{16}} \geq 2^{31}$	

4 Parity check matrix and Euclidean duals of θ-constacyclic codes

In this section we extend the results of [6] on self-dual skew cyclic codes. A code over $GR(4^m)$ is **Euclidean self-dual** if it is equal to its dual w.r.t. the form

$$x.y = \sum_i x_i y_i$$

We shall prove that the Euclidean dual of a θ-constacyclic code $(g)/(X^n - c) \subset GR(4^m)[X,\theta]/(X^n - c)$ for $c \in \{1,3\}$ and such that $m|n$ is again a θ-constacyclic code $(g^\perp)/(X^n - c) \subset GR(4^m)[X,\theta]/(X^n - c)$.

The following lemma explains why the two factors in the decomposition of the generator of a central monic polynomial in two monic polynomials always commute:

Lemma 5 *Suppose that $f \in \mathbb{Z}_4[X^m]$ is a monic polynomial which decomposes into a product of monic polynomials as $h\,g$ over $GR(4^m)[X,\theta]$, then $h\,g = g\,h$ in $GR(4^m)[X,\theta]$.*

PROOF. Since $h\,g$ is a central element we have $(h\,g)\,h = h\,(h\,g)$. Therefore $h\ (g\,h - h\,g) = 0$. Since the leading coefficient of h is invertible, h is not a zero divisor, showing that $h\,g = g\,h$ in $GR(4^m)[X,\theta]$. ■

Using this commutativity result, we can proceed as in the cyclic case to obtain a parity check polynomial:

Lemma 6 *Suppose that $f \in \mathbb{Z}_4[X^m]$ is a monic polynomial which decomposes into a product of monic polynomials as $h\,g$ over $GR(4^m)[X,\theta]$ and denote by $\mathcal{C}$ the θ-principal code corresponding to the left ideal generated by g in $GR(4^m)[X,\theta]/(h\,g)$. Then $a \in \mathcal{C} \Leftrightarrow a(X)\,h = 0$ in $GR(4^m)[X,\theta]/(h\,g)$.*

PROOF. If $a \in \mathcal{C}$, then $a(X) = u\,g$. By the above commutativity result we get $a(X)\,h = (u\,g)\,h = u\,(h\,g) = 0$ in $GR(4^m)[X,\theta]/(h\,g)$.
Conversely, if $a(X)\,h = 0$ in $GR(4^m)[X,\theta]/(f)$, then $a(X)\,h = u\,f = u\,(h\,g) = (u\,g)\,h$ in $GR(4^m)[X,\theta]$. Like in the above proof we use the fact that h is not a zero divisor to obtain $a(X) = u\,g$, showing that $a \in \mathcal{C}$. ■

The parity check matrix is now obtained from the condition $a \in \mathcal{C} \Leftrightarrow a(X)\,h = 0$ in $GR(4^m)[X,\theta]/(h\,g)$:

Lemma 7 *Suppose that m divides n. Let $c \in \{1,2,3\}$ and $X^n - c \in \mathbb{Z}_4[X^m]$ decomposes as $h\,g$ over $GR(4^m)[X,\theta]$. Let $\mathcal{C}$ be the θ-constacyclic code corresponding to the left ideal generated by g in $GR(4^m)[X,\theta]/(X^n - c)$. If $g = g_0 + g_1X + \ldots + g_rX^r$ and $h = h_0 + h_1X + \ldots + h_{n-r}X^{n-r}$, then the following matrix*

$$\begin{pmatrix} h_{n-r} & \ldots & \theta^{n-r-1}(h_1) & \theta^{n-r}(h_0) & 0 & \ldots & 0 \\ 0 & \theta(h_{n-r}) & \ldots & \ldots & \theta^{n-r+1}(h_0) & \ldots & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ldots & \ddots & 0 \\ 0 & \ldots & 0 & \theta^{r-1}(h_{n-r}) & \ldots & \theta^{n-2}(h_1) & \theta^{n-1}(h_0) \end{pmatrix}$$

is a parity check matrix for $\mathcal{C}$.

PROOF. The Lemma 6 shows that for $a(X) \in \mathcal{C}$ the product $a(X)\,h = 0$ in $GR(4^m)[X,\theta]/(X^n - c)$. Now $deg(a(X)\,h) < 2n-r$ and from this we deduce that the coefficients of $X^{n-r}, X^{n-r+1}, \ldots, X^{n-1}$ in this product must be zero. As, for $l \in \{n-r, \ldots, n-1\}$, the coefficient of X^l in $a(X)h(X)$ is

$$\sum_{j=0}^{n-r} a_{l-j}\theta^{l-j}(h_j)$$

we get the result. ■

Corollary 1 *Suppose that m divides n, $c \in \{1,3\}$ and $X^n - c \in \mathbb{Z}_4[X^m]$ decomposes as $h\,g$ over $GR(4^m)[X,\theta]$. Denote by $g = \sum_{i=0}^{r} g_iX^i$ and $h = \sum_{i=0}^{n-r} h_iX^i$. The dual of the θ-constacyclic code $(g)/(X^n - c)$ is the θ-constacyclic code $(g^{\perp})/(X^n - c)$, where*

$$g^{\perp} \;=\; h_{n-r} + \theta(h_{n-r-1})X + \ldots + \theta^{n-r}(h_0)X^{n-r}.$$

Proof. According to the previous result we need to show that the above matrix H is the matrix of a θ-constacyclic code, which amounts to show that $\theta^{n-r}(h_0)X^{n-r}+\ldots+\theta(h_{n-r-1})X+h_{n-r}$ is also a right divisor of X^n-c. The ring $GR(4^m)[X,\theta]$ can be localized to the right at the multiplicative set S generated by X consisting of all integer powers of X^{n_1} where $n_1>0$. This follows from [22] Theorem 2 (see also [8] p. 162) since S verifies the following two necessary and sufficient conditions

1. Condition 1 (right Ore condition): for all $X^{n_1}\in S$ and $f_1\in GR(4^m)[X,\theta]$, there exists $X^{n_2}\in S$ and $f_2\in GR(4^m)[X,\theta]$ such that $f_1\,X^{n_1}=X^{n_2}\,f_2$. To prove this we note that the multiplication rule $X^{n_1}a=\theta^{n_1}(a)X^{n_1}$ allows to shift powers of X from left to right by changing the coefficients.

2. Condition 2: if for $X^{n_1}\in S$ and $f_1\in GR(4^m)[X,\theta]$ we have $X^{n_1}\,f_1=0$, then there exists $X^{n_2}\in S$ such that $f_1\,X^{n_2}=0$. But since X^{n_1} is never a zero divisor, f_1 must be zero.

This shows that the right localization $GR(4^m)[X,\theta]S^{-1}$ exists. We have $aX^{-1}=X^{-1}\theta(a)$ where X^{-1} is the inverse of X in this ring. We now consider the ring $R\subset GR(4^m)[X,\theta]S^{-1}$ consisting of the elements $\sum_{i=0}^{n}X^{-i}a_i$, where the coefficients are on the right and where the multiplication rule is given by $aX^{-1}=X^{-1}\theta(a)$. The ring R is isomorphic to the skew polynomial ring $GR(4^m)[X^{-1},\theta^{-1}]$. The map

$$\begin{array}{rcl}\varphi\colon GR(4^m)[X,\theta] & \to & R\subset GR(4^m)[X,\theta]S^{-1}\\ \displaystyle\sum_{i=0}^{n}a_iX^i & \mapsto & \displaystyle\sum_{i=0}^{n}X^{-i}a_i\end{array}$$

is an anti-isomorphism of rings. For $P_1=\sum_{i=0}^{s}a_iX^i$ and $P_2=\sum_{i=0}^{t}b_iX^i$ we have $\varphi(P_1+P_2)=\varphi(P_1)+\varphi(P_2)$ and

$$\begin{array}{rcccl}\varphi(P_1P_2) & = & \varphi\left(\displaystyle\sum_{k=0}^{s+t}(\sum_{i+j=k}a_i\theta^i(b_j))X^k\right) & = & \displaystyle\sum_k X^{-k}\left(\sum_{i,j}a_i\theta^i(b_j)\right)\\ & = & \displaystyle\sum_k\sum_{i,j}X^{-j}X^{-i}\,\theta^i(b_j)a_i & = & \displaystyle\sum_k\sum_{i,j}X^{-j}b_jX^{-i}a_i\\ & = & \varphi(P_2)\varphi(P_1) & & \end{array}$$

If $X^n-c=g\,h$, then for $k=n-r$ we have

$$\begin{array}{rcccl}X^k\,\varphi(h)\,\varphi(g)\,X^r & = & X^k\varphi(gh)X^r & = & X^k\,\varphi(X^n-c)\,X^r\\ & = & X^k\,(X^{-n}-c)\,X^r & = & 1-cX^n\\ & = & -c\left(X^n-\frac{1}{c}\right). & & \end{array}$$

If $\frac{1}{c}=c$ (i.e. $c\in\{1,3\}$), then $X^k\,\varphi(h)=h_k+\theta(h_{k-1})X+\ldots+\theta^k(h_0)X^k=g^\perp$ divides X^n-c in $GR(4^m)[X,\theta]$. ■

5 Euclidean Self-dual θ-Constacyclic Codes over $GR(4^2)$

Our goal in this section is to compute all Euclidean self-dual θ-constacyclic codes of length $n\leq 40$ over $GR(4^2)[X,\theta]$ where θ is the generalized Frobenius automorphism $a+2b\mapsto a^2+2b^2$. The approach is a generalization of [6]. We need to find all skew polynomials g such that $X^n-c=h\,g$ with $c\in\{1,3\}$ and such that the θ-constacyclic code $C=(g)/(X^n-c)$ is self-dual.

Corollary 1 allows to express the coefficients of the generating polynomial $g^{\perp}$ of $C^{\perp}$ in terms of the coefficients of h. For C to be self-dual, $g^{\perp}$ and g must differ by a constant multiple. This allows to express the coefficients of h in terms of the coefficients of g. Equating the coefficients of $X^n - c - (h\,g) = 0$ to zero, produces a (commutative) polynomial system of equations over $GR(4^2)$ for the coefficients of all skew polynomials g for which $C = C^{\perp}$. All possible generators g of Euclidean self-dual θ-constacyclic codes of given length can then be determined by computing a Groebner base for this polynomial system in Magma.

We use the 2-Adic representation of the elements of $GR(4^2)$ ([23], Section 6.2). The elements of $GR(4^2)$ are uniquely written as $a + 2\,b \in GR(4^2)$ where a and b belong to $\{0, 1, \overline{\xi}, \overline{\xi}^2\}$ and $\overline{\xi} = \tilde{X}$ is a root of $X^2 + X + 1$ in $\mathbb{F}_2[X]/(X^2 + X + 1)$. More precisely, $\overline{\xi} = \varphi(\xi)$ where $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_2; 0, 2 \mapsto 0; 1, 3 \mapsto 1$ (see section 1).

Let $g = \sum_{i=0}^{r-1} g_i\,X^i + X^r$ with $g_0 \neq 0$, the generator polynomial of a self-dual θ-constacyclic code with length $n = 2r$. Let $h = X^r + \sum_{i=0}^{r-1} h_i X^i$ such that $h\,g = X^n - c$.

Then

$$h = X^r + \sum_{i=1}^{r-1} \left(\theta^{r-i}(g_0^{-1})\,\theta^{r-i}(g_{r-i})X^i\right) + \theta^r(g_0^{-1})$$

So the polynomials g of self-dual codes of length $2r$ are characterized by the relation

$$\left(\sum_{i=0}^{r-1} g_i X^i + X^r\right)\ \left(\theta^r(g_0^2) + \sum_{i=1}^{r} \theta^{r-i}(g_0^2\,g_{r-i})X^i\right) = X^{2r} - c$$

In Magma, we write the coefficients g_i as $a_i + \nu b_i$ where ν is an indeterminate representing ”2”. So we define the polynomial ring $\mathbb{F}_4[a_0, \ldots, a_r, b_0, \ldots, b_r][\nu]$ and consider the relations

$$a_i^4 = a_i, b_i^4 = b_i, \nu^2 = 0 \tag{1}$$

Then

$$g_0^{-1} = a_0^2 - \nu\, a_0 b_0$$

We use the addition rules of 2-Adic numbers ([23], Section 6.2) and compute the coefficients of $h\,g - (X^n - c)$. They are of the form $P(a_i, b_j) + \nu Q(a_i, b_j)$ and must cancel. So each coefficient leads to two polynomial relations

$$P(a_i, b_j) = Q(a_i, b_j) = 0 \tag{2}$$

We compute a Groebner basis for all the algebraic relations (1) and (2). We get the coefficients $g_i = \overline{\xi}^k + \nu\,\overline{\xi}^l$ that we transform in the representation : $g_i = \xi^k + 2\,\xi^l$ where $\xi^2 = 3\xi + 3$.
For each generator polynomial g we construct the corresponding code and make the mapping from $GR(4^2)$ to $\mathbb{Z}_4$ explained in section 3.

We made computations for $n \leq 20$ and $c \in \{1, 3\}$ and get self-dual θ-constacyclic codes only for $n \in \{4, 12, 20\}$ and $c = 3$. The result appears in the next section.

6 Self-dual $\mathbb{Z}_4$-codes

For any missing definition on $\mathbb{Z}_4-$codes (resp. lattices) we refer to [23] (resp. [12]).

A **lattice** of dimension n is a discrete additive subgroup of $\mathbb{R}^n$ of maximal $\mathbb{Z}-$rank. The dual L^* of a lattice L is given by

$$L^* := \{x \in \mathbb{R}^n : \ \forall y \in L \ x.y \in \mathbb{Z}\},$$

where $x.y$ stands for the standard inner product of $x, \ y \in \mathbb{R}^n$ The **norm** μ of a lattice is the quantity

$$\mu := \min\{x.x : \ x \neq 0 \ \& \ x \in L\}.$$

A lattice L is **unimodular** iff $L = L^*$. It is then Type II if

$$\forall x \in L, \ x.x \equiv 0 \pmod 2,$$

and Type I otherwise. A lattice is ℓ modular for some prime ℓ if L^* is similar to $L/\sqrt{\ell}$. It was proved in [21, Th. 1] that the norm of a unimodular $n-$dimensional lattice is at most

$$\mu \leq 2(\lfloor n/24 \rfloor + 1),$$

for $n \neq 23$. A unimodular lattice meeting that bound is called **extremal**. Similarly, it was proved in [21, Th. 2] that the norm of a 3$-$modular $n-$dimensional lattice is at most

$$\mu \leq 2(\lfloor n/12 \rfloor + 1),$$

for n even. A 3$-$modular lattice meeting that bound is called **extremal**. For more details and motivation see [12, 21].

A linear code of length n over $\mathbb{Z}_4$ is a submodule of $\mathbb{Z}_4^n$. The dual $C^\perp$ is understood with respect to the standard inner product. A code is **self-dual** if it is equal to its dual.

The **Euclidean weight** of a vector $x = (x_1, x_2, \ldots, x_n)$ is $w_E(x) := \sum_{i=1}^n \min\{x_i^2, (4-x_i)^2\}$.

The **Lee weight** of a vector $x = (x_1, x_2, \ldots, x_n)$ is $w_L(x) := \sum_{i=1}^n \min\{|x_i|, \ |(4-x_i)|\}$.

The composition of a vector $x \in R^n$ say $n_i(x) \, i = 0, 1, 2$ is the number of entries$= i$ in x. For instance $w_L(x) = n_1(x) + 2n_2(x)$. The **symmetrized weight enumerator (swe)** of a code C is then defined as

$$swe_C(a, b, c) = \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)}.$$

The **Euclidean weight enumerator (ewe)** of a code C is then defined as

$$ewe_C(a, b) = \sum_{x \in C} a^{4n - w_E(x)} b^{w_E(x)}.$$

A self-dual code is **Type II** if all vectors in the code have Euclidean weights which are $0 \pmod 8$ and **Type I** otherwise. The minimum Euclidean (resp. Lee) weight of the code is denoted by d_E (resp.d_L). We shall recall the standard A_4 construction of a lattice from a self-dual code over $\mathbb{Z}_4$.

Define the reduction modulo 4, by $\rho : \mathbb{Z}^n \to \mathbb{Z}_4^n$, by

$$\rho(x_1, \ldots, x_n) = (x_1 \pmod 4, \ldots, x_n \pmod 4).$$

Given a code C over $\mathbb{Z}_4$ we construct a lattice by

$$\Lambda(C) = \frac{1}{2}\{x \in \mathbb{Z}^n \mid \rho(x) \in C\}. \tag{3}$$

It is shown in [4] that if C is a Type I code then $\Lambda(C)$ is a Type I unimodular lattice, and that if C is a Type II code then $\Lambda(C)$ is a Type II unimodular lattice and that the minimum norm of the lattice is $\min\{4, \frac{d_E}{4}\}$. For a notion of Type II codes over $GR(4^2)$ we refer to [2].

In order to use this result to construct self-dual codes over $\mathbb{Z}_4$, recall that the Galois ring $R := GR(4^2)$ of order 16 and characteristic 4 is the unique degree 2 Galois extension of $\mathbb{Z}_4$. We may regard that ring as $\mathbb{Z}_4[\alpha]$ where α satisfies the quadratic $X^2 + X + 1 = 0$. Let $\mathbb{F}_4$ denote the unique finite field of order 4. Similarly, we may regard this field as $\mathbb{F}_2[\omega]$ where ω satisfies the same polynomial but read off in $\mathbb{F}_2$. We shall assume that α is mapped to ω by reduction mod 2. In fact the quotient $R/2R$ is isomorphic to $\mathbb{F}_4$. There is a natural notion of **conjugation** on R induced by the complex conjugation. Let $z = t + \alpha t'$ be a generic $z \in R$ with $t, t' \in \mathbb{Z}_4$. We shall denote by $\overline{z}$ the conjugate of z and define it as $\overline{z} = t - t' - \alpha t'$. Define the trace of $z \in R$ down to $\mathbb{Z}_4$ by $T(z) := z + \overline{z}$. From such codes over $GR(4^2)$ we construct self-dual codes over $\mathbb{Z}_4$ by projecting on the Trace orthogonal basis of [14].

For n in $\{4, 12, 20\}$, we give the codes of length n found via the Groebner basis computation. After projection over $\mathbb{Z}_4$, we classify them in classes of self-dual codes over $\mathbb{Z}_4$ with same symmetric weight enumerator (swe) and Euclidean weight enumerator (ewe). The weight enumerators that are not displayed can be obtained from the companion research report. For each class, we give the minimum Euclidean weight d_E, the minimum Hamming distance d, the minimum Lee weight d_L, a generator polynomial g, and the number of codes of the class. For codes whose Euclidean distance is 8 and which are of type II, we compute the root systems generated by the short vectors of their lattices.

For $n = 4$, we find 8 codes which are classified in two classes of 4 codes (table 1). The second code is a Type I code called $\mathcal{E}_8$ in [13].

d_E	d	d_L	Generator polynomial g	swe & ewe
4	4	4	$X^2 + (3\,\xi + 1)\,X + \xi$	$swe = a^8 + 16\,a^4b^4 + 14\,a^4c^4 + 48\,a^3b^4c +$ $96\,a^2b^4c^2 + 48\,ab^4c^3 + 16\,b^8 + 16\,b^4c^4 + c^8$ $ewe = a^{32} + 16\,a^{28}b^4 + 64\,a^{24}b^8 + 96\,a^{20}b^{12} +$ $62\,a^{16}b^{16} + 16\,a^{12}b^{20} + b^{32}$
8	4	6	$X^2 + (3\,\xi + 3)\,X + 3\,\xi$	$swe = a^8 + 14\,a^4\,c^4 + 112\,a^3\,b^4$ $c + 112\,a\,b^4\,c^3 + 16\,b^8 + c^8$ $ewe = a^{32} + 128\,a^{24}\,b^8 + 126\,a^{16}\,b^{16} + b^{32}$

Table 1: Euclidean Self-dual θ-Constacyclic Codes $(g)/(X^4 + 1)$

For $n = 12$, we get 28 classes of self-dual codes of length 24 over $\mathbb{Z}_4$ with the same symmetric weight enumerator and Euclidean weight enumerator. We classify them according to their Euclidean distance $d_E \in \{4, 8, 12, 16\}$.

There are only 4 codes (with same ewe and swe) with Euclidean distance $d_E = 4$. Their distances are $d = 4$ and $d_L = 4$. One of the generator polynomials of this unique class is

$$g = X^6 + (3\,\xi + 1)\,X^3 + \xi$$

The codes with Euclidean distance $d_E = 8$ are classified according their type. There are 8 classes of Type I codes and 12 classes of Type II codes.

The 156 Type I lattices (a.k.a. odd unimodular lattices) in dimension 24 are uniquely characterized by their roots systems formed by their norm 2 vectors [12, Chap. 17]. These are indicated below (table 2) as among $A_1^{24}, A_2^8, A_3^8, D_4^6$. So 8 distinct *swe*'s only yield 4 distinct lattices. It is an open and challenging problem to recover all 156 Type I lattices by Construction A_4 as it has been done for the 24 Niemeier lattices in [3].

Root system	d	d_L	Generator polynomial g	Number of codes
A_1^{24}	4	6	$X^6 + 2\,\xi X^5 + 2\,X^4 + (3\,\xi + 1)\,X^3 + 2\,\xi X^2 + 2\,X + \xi$	4
A_2^8	8	8	$X^6 + 3\,X^5 + (\xi + 3)\,X^4 + (2\,\xi + 1)\,X^3 +$ $(3\,\xi + 2)\,X^2 + X + 1$	8
	4	8	$X^6 + X^5 + (3\,\xi + 2)\,X^4 + 2\,\xi X^3 +$ $(\xi + 2)\,X^2 + (\xi + 1)\,X + 3\,\xi + 3$	8
A_3^8	8	8	$X^6 + (2\,\xi + 1)\,X^5 + (3\,\xi + 1)\,X^4 + (2\,\xi + 1)\,X^3 +$ $(\xi + 2)\,X^2 + (2\,\xi + 1)\,X + 1$	8
	4	6	$X^6 + (\xi + 3)\,X^5 + (3\,\xi + 3)\,X^4 + \xi X^2 + (\xi + 2)\,X + 1$	8
	4	8	$X^6 + (\xi + 1)\,X^5 + 3\,\xi X^4 + 2\,X^3 + (\xi + 1)\,X^2 + \xi\,X + 1$	8
	4	8	$X^6 + (\xi + 3)\,X^5 + \xi X^4 + (3\,\xi + 3)\,X^2 + (\xi + 2)\,X + 1$	4
D_4^6	4	8	$X^6 + 2\,X^5 + 2\,X^4 + (3\,\xi + 1)\,X^3 + 2\,\xi X^2 + 2\,\xi X + \xi$	4

Table 2: Type I Euclidean Self-dual θ-Constacyclic Codes $(g)/(X^{12} + 1)$ with $d_E = 8$

There are exactly 23 unimodular even lattices of norm 2 in dimension 24. They were classified by Niemeier and later by Venkov [12, chap. 18], and are uniquely characterized by the roots systems spanned by their norm 2 vectors. We compute the systems of roots of the lattices obtained by the type II codes by Construction A and find A_1^{24}, A_3^8, D_4^6, D_6^4, D_{12}^2 and E_8^3 (table 3).

The codes of length 24 over $\mathbb{Z}_4$ and Euclidean distance $d_E = 12$ (table 4) are of Type I and give by Construction A the so-called Odd Leech lattice, the unique unimodular lattice of norm 3 in dimension 24 [12, Chap. 17]. They are distinct from the four codes in [15] as their *swe*'s are different (inspection of the monomial terms in $a^{12}c^{12}$ and $a^{15}b^8c$).

The Type II code of length 24 and Euclidean distance $d_E = 16$ (table 5) give rise to the Leech lattice by Construction A. Since their Lee weight is only 8 (and not 12) they are not one of the thirteen Lee-optimal codes classified by Rains [20].

Lastly, for $n = 20$, we did not compute the swe and ewe of all codes. The one generated by the polynomial

$$g = X^{10} + 2\,X^9 + (2\xi + 1)\,X^8 + (\xi + 3)\,X^6 + (2\xi + 1)\,X^5 + (3\xi + 2)\,X^4 + (2\xi + 3)\,X^2 + 2\,X + 1$$

has mimimum Hamming distance $d = 8$, minimum Euclidean distance $d_E = 16$ and minimum

Root system	d	d_L	Generator polynomial g	Number of codes
A_1^{24}	4	8	$X^6 + X^5 + (\xi + 3)\, X^4 + (\xi + 3)\, X^2 + \xi\, X + 3\, \xi$	8
	8	8	$X^6 + X^5 + (\xi + 3)\, X^4 + 3X^3 + (\xi + 2)\, X^2 + X + 3$	16
A_3^8	4	6	$X^6 + (3\xi + 3)\, X^5 + (\xi + 1)\, X^4 + \xi X^2 + \xi X + 3$	8
	4	8	$X^6 + (3\, \xi + 3)\, X^5 + (3\, \xi + 2)\, X^4 +$ $2\, X^3 + (3\, \xi + 1)\, X^2 + \xi\, X + 3$	4
	4	8	$X^6 + (2\, \xi + 2)\, X^5 + (3\, \xi + 3)\, X^3 + (2\, \xi + 2)\, X + 3\, \xi$	4
D_4^6	4	8	$X^6 + (3\, \xi + 1)\, X^5 + (3\, \xi + 1)\, X^4 +$ $(3\, \xi + 2)\, X^2 + (\xi + 2)\, X + 3$	8
	4	8	$X^6 + (3\, \xi + 1)\, X^5 + \xi X^4 +$ $2\, X^3 + (\xi + 1)\, X^2 + (\xi + 2)\, X + 3$	4
D_6^4	8	8	$X^6 + (2\, \xi + 3)\, X^5 + (3\, \xi + 1)\, X^4 +$ $X^3 + (3\, \xi + 2)\, X^2 + (2\, \xi + 1)\, X + 3$	8
	4	8	$X^6 + (3\, \xi + 1)\, X^5 + (\xi + 2)\, X^4 +$ $(\xi + 3)\, X^2 + (\xi + 2)\, X + 3$	4
D_{12}^2	8	8	$X^6 + X^5 + (\xi + 3)\, X^4 + X^3 + (\xi + 2)\, X^2 + X + 3$	8
	4	6	$X^6 + 2\, \xi X^5 + 2\, X^4 + (3\, \xi + 3)\, X^3 + 2\, \xi X^2 + 2\, X + 3\, \xi$	4
E_8^3	4	6	$X^6 + (3\xi + 3)X^3 + 3\xi$	4

Table 3: Type II Euclidean Self-dual θ-Constacyclic Codes $(g)/(X^{12} + 1)$ with $d_E = 8$

d	d_L	Generator polynomial g	swe	Number of codes
4	8	$X^6 + (\xi + 1)\, X^5 + (\xi + 1)\, X^4 +$ $2\, X^3 + 3\, \xi X^2 + \xi\, X + 1$	$a^{24} + \cdots + 768\, a^{15} b^8 c +$ $\cdots + 2648\, a^{12} c^{12} + \cdots$	16
4	8	$X^6 + (\xi + 1)\, X^5 + (3\, \xi + 2)\, X^4 +$ $(\xi + 3)\, X^2 + \xi X + 1$	$a^{24} + \cdots + 768\, a^{15} b^8 c +$ $\cdots + 2612\, a^{12} c^{12} + \cdots$	4
4	8	$X^6 + (2\, \xi + 2)\, X^5 +$ $(3\, \xi + 1)\, X^3 + (2\, \xi + 2)\, X + \xi$	$a^{24} + \cdots + 576\, a^{15} b^8 c +$ $\cdots + 2828\, a^{12} c^{12} + \cdots$	4
8	10	$X^6 + 3\, X^5 + (\xi + 3)\, X^4 +$ $(2\, \xi + 3)\, X^3 + (3\, \xi + 2)\, X^2 + X + 1$	$a^{24} + \cdots + 768\, a^{15} b^8 c +$ $\cdots + 2576\, a^{12} c^{12} + \cdots$	16

Table 4: Euclidean Self-dual θ-Constacyclic Codes $(g)/(X^{12} + 1)$ with $d_E = 12$

d	d_L	Generator polynomial	Number
		g	of codes
4	8	$X^6+(3\,\xi+3)\,X^5+(\xi+3)\,X^4+2\,X^3+(\xi+2)\,X^2+\xi X+3$	8
4	8	$X^6+(3\,\xi+3)\,X^5+3\,\xi X^4+(3\,\xi+3)\,X^2+\xi X+3$	4
4	8	$X^6+2\,X^5+2\,X^4+(3\,\xi+3)\,X^3+2\,\xi X^2+2\,\xi\,X+3\,\xi$	4

Table 5: Euclidean Self-dual θ-Constacyclic Codes $(g)/(X^{12}+1)$ with $d_E=16$

Lee distance $d_L=14$. It is therefore better for the Lee and Euclidean distance than the best possible Type IV code in length 40 [9].

7 Hermitian Self-dual θ-Constacyclic Codes over $GR(4^2)$

We compute Hermitian self-dual θ-constacyclic codes over $GR(4^2)$, which means self-dual Hermitian codes generated by polynomials divisors of $f=X^n-c$ with $c\in\{1,3\}$. We use the same techniques as for self-dual Euclidean codes with the scalar product

$$x._H\,y=\sum_{i=1}^{n}x_i\,\theta(y_i)$$

Following lemma 21 of [6], we get

Lemma 8 *Suppose that m divides n. Let g and $h=\sum_{i=0}^{k}h_i\,X^i$ be elements of $GR(4^m)[X,\theta]$ such that $h\,g=g\,h=X^n-c$ where $c\in\{1,3\}$. The Hermitian dual of the θ-constacyclic code $(g)/(X^n-c)$ is the θ-constacyclic code $(g^H)/(X^n-c)$ where*

$$g^H=\sum_{i=0}^{k}\theta^{m-1+i}(h_{k-i})\,X^i$$

Proof. Let c be a code word and let $g^{\perp}$ the generator polynomial of the Euclidean dual of the code $(g)/(X^n-c)$; then for i in $\{0,\dots k\}$,

$$<c(X),X^i g^{\perp}(X)>=<c(X),X^i\,g^H(X)>_H$$

where $<a(X),b(X)>_H=a._H\,b$ and $<a(X),b(X)>=a.\,b$. Furthermore $g^H(X)$ is a right divisor of X^n-c. Indeed, $g^H=\phi^{m-1}(g^{\perp})$ where ϕ is the morphism from $GR(4^2)[X,\theta]$ to $GR(4^2)[X,\theta]$ defined by $\phi(\sum a_iX^i)=\sum\theta(a_i)X^i$. As $g^{\perp}$ is a right divisor of X^n-c, $g^H=\phi^{m-1}(g^{\perp})$ is also a right divisor of $\phi^{m-1}(X^n-c)=X^n-c$. ■

In $GR(4^2)[X,\theta]$, the polynomial h of a Hermitian self-dual code $(g)/(X^{2r}-c)$ defined by $hg=X^{2r}-c$ becomes

$$h=X^r+\sum_{i=1}^{r-1}\left(\theta^{r-i+1}(g_0^{-1})\,\theta^{r-i+1}(g_{r-i})X^i\right)+\theta^{r+1}(g_0^{-1})$$

so the generators g of Hermitian self-dual codes of length $2r$ are characterized by the relation

$$\left(\sum_{i=0}^{r-1}g_iX^i+X^r\right)\,\left(X^r+\sum_{i=1}^{r-1}\left(\theta^{r-i+1}(g_0^{-1})\,\theta^{r-i+1}(g_{r-i})X^i\right)+\theta^{r+1}(g_0^{-1})\right)=X^{2r}-c$$

We made the computations for $r \leq 10$ and found Hermitian self-dual codes for each r. When r is even, the polynomial f is $X^{2r}-1$, otherwise f is $X^{2r}+1$.
According to [14], from an Hermitian self-dual code of length n, one can construct a 3-modular $\mathbb{Z}$-lattice of dimension $2n$ whose norm is bounded by $2\lfloor \frac{n}{6} \rfloor + 2$. Following [14], the Gramm matrix M of the lattice is obtained from the generator matrix of the code as

$$M = \frac{1}{2} \begin{pmatrix} U\,{}^tU + V\,{}^tV - \frac{1}{2}U\,{}^tV - \frac{1}{2}V\,{}^tU & -\frac{1}{2}U\,{}^tU - \frac{1}{2}V\,{}^tV - \frac{1}{2}U\,{}^tV + V\,{}^tU \\ -\frac{1}{2}U\,{}^tU - \frac{1}{2}V\,{}^tV + U\,{}^tV - \frac{1}{2}V\,{}^tU & U\,{}^tU + V\,{}^tV - \frac{1}{2}U\,{}^tV - \frac{1}{2}V\,{}^tU \end{pmatrix}$$

where $U = \begin{pmatrix} & G_0 \\ 0 & 4I_N \end{pmatrix}$, $V = \begin{pmatrix} & G_1 \\ 0 & 0 \end{pmatrix}$ and $G_0 + \xi\, G_1$ is the generator matrix of the code.
We compare our results with the table of best lattices, given in [18].
In the first row, we give the length $n = 2r$; in the second row, the generator polynomial of a Hermitian self-dual code C of length n, $(g)/(X^{2r} - c)$ where $c = (-1)^{rmod2}$; in the third column, the norm of the lattice constructed from the code C and in the last column, the best known norm (BKN) for 3-modular $\mathbb{Z}$-lattices of dimension $2n$.

Length $2r$	Generator polynomial g	Norm	BKN
4	$X^2 + 2\,\xi + 1$	2	2
6	$X^3 + 2\,X^2 + 2\,X + 2\,\xi + 1$	4	4
8	$X^4 + 2\,X^3 + 2\,X + 2\,\xi + 1$	4	4
10	$X^5 + 2\,X^3 + 2\,X^2 + 2\,\xi + 1$	4	4
12	$X^6 + 2\,X^4 + 2\,X^2 + 2\,\xi + 1$	4	6
14	$X^7 + (3\,\xi + 1)\,X^6 + (\xi + 2)\,X^5 + (\xi + 1)\,X^4 +$ $(3\,\xi + 2)\,X^3 + (3\,\xi + 3)\,X^2 + \xi\,X + 2\xi + 1$	6	6
16	$X^8 + 2\,X^5 + 2\,X^3 + 2\,\xi + 1$	4	6
18	$X^9 + 2\,X^7 + (3\,\xi + 1)\,X^6 + 2\,X^5 + 2\,X^4 + \xi\,X^3 + 2\,X^2 + 2\,\xi + 1$	6	8
20	$X^{10} + (2\,\xi + 1)\,X^8 + (3\,\xi + 2)\,X^6 + 2\,X^5 + \xi\,X^4 + X^2 + 2\,\xi + 1$	6	8

Table 6: Hermitian Self-dual θ-Constacyclic Codes $(g)/(X^{2r} - c)$ with $c = (-1)^{r \bmod 2}$

We notice that the 36 lattices of norm 6 we obtain in length $n = 14$ are all isometric to one of the two known extremal lattices of dimension 28, Beis 14 in the notation of [18]. This lattice was previously constructed by combining Construction A modulo 2 over the Eisenstein integers with Kneser neighboring [1]. We give here another construction of this lattice, without taking neighbors. Similar trade off between alphabet size and neighboring can be observed in [11].

8 Cubic Construction

Following [14], from self-dual codes over $\mathbb{Z}_4$ of length l and Hermitian self-dual codes of length l over $GR(4, 2)$, one can construct $3l$ self-dual codes overs $\mathbb{Z}_4$.
We construct self-dual codes over $\mathbb{Z}_4$ with length 24 and get codes of Euclidean weight 8, 12 or 16. We focus on the Type II codes of Euclidean weight 8 and get the following systems of roots, which improves the results obtained in the previous section : A_2^{12}, A_3^8, A_6^4, A_8^3, A_{24}, D_4^6, D_6^4, D_8^3, D_{12}^2 and D_{24}.
More precisely, for each of the 7 self-dual codes C_1 of length 8 over $\mathbb{Z}_4$ ([13]) and each of the

16 Hermitian self-dual codes C_2 with length 8 over $GR(4^2)$ previously computed, we construct self-dual codes over $\mathbb{Z}_4$ of length 24. If their minimum Euclidean weight is 8 and if the codes are of type II, we compute their root system. In first column of the table, is given the root system; in the second column, the generator matrix of C_1 $(G_1, G_2, G_3$ or $G_4)$; in the third column, the generator polynomial of C_2; in the last column the number of codes which have the same symmetric weight enumerator and Euclidean weight enumerator that the code constructed from C_1 and C_2. There is only one class of codes for each of the root systems A_2^{12}, A_6^4, A_8^3, A_{24}, D_6^4 and D_{12}^2. There are two classes of codes with root system A_3^8, D_6^4 or D_8^3.

Root system	Self-dual code C_1 over $\mathbb{Z}_4$	Hermitian self-dual code C_2 over $GR(4^2)$	Number of equivalent codes
A_2^{12}	G_1	$X^4+2\,X^3+2\,X+2\,\xi+1$	6
A_3^8	G_2	$X^4+2\,X^2+2\,\xi+1$	2
	G_1	$X^4+2\,\xi+1$	2
A_6^4	G_1	$X^4+2\,X^2+2\,\xi+1$	2
A_8^3	G_3	$X^4+2\,X^3+2\,X+2\,\xi+1$	6
A_{24}	G_3	$X^4+2\,X^2+2\,\xi+1$	2
D_4^6	G_3	$X^4+2\,\xi+1$	6
	G_2	$X^4+2\,X^3+2\,X^2+2\,X+2\,\xi+1$	6
D_6^4	G_2	$X^4+2\,\xi+1$	2
D_8^3	G_4	$X^4+2\,X^3+2\,X+2\,\xi+1$	6
	G_4	$X^4+2\,X^3+2\,X^2+2\,X+2\,\xi+1$	6
D_{12}^2	G_3	$X^4+2\,\xi+1$	2
D_{24}	G_4	$X^4+2\,\xi+1$	2
	G_4	$X^4+2\,X^2+2\,\xi+1$	2

Table 7: Self-dual Codes over $\mathbb{Z}_4$ with length 24 obtained from cubic construction

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ 0 & 1 & 0 & 0 & 3 & 1 & 2 & 3 \\ 0 & 0 & 1 & 0 & 1 & 2 & 3 & 3 \\ 0 & 0 & 0 & 1 & 2 & 3 & 1 & 3 \end{pmatrix},\ G_2 = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 2 & 1 \\ 0 & 2 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 1 & 0 & 1 & 1 & 2 & 3 \\ 0 & 0 & 0 & 1 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \end{pmatrix},$$

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \end{pmatrix} \text{ and } G_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

9 Open Problems

There are several possible generalizations to this approach:

1. In the situations of the previous section we considered the factor rings $GR(4^m)[X,\theta]/(f)$ where f is a monic central polynomials. Any monic right factor of f generates a principal ideal $(g)/(f) \subset GR(4^m)[X,\theta]/(f)$ and therefore corresponds to a linear code. Those codes

have similar properties than the classical cyclic codes, in particular any code word is a multiple of g and there will always be $(4^m)^i$ code words. We may also consider ideals that are generated by non unitary polynomials whose leading coefficients are not invertible and more generally non principal ideals. We provide an example in each case:

Example. The code associated with $(2X^2 + (2w + 2)X + 2w) \subset GR(4^2)[X, \theta]/(X^2 + 1)$ contains 16 code words and has lee distance 8. Its mapping to a code over $\mathbb{Z}_4$ and then to a code over $\mathbb{F}_2$ produces a code of length 16 with 2^4 code words and distance 8 over $\mathbb{F}_2$. This has to be compared with the (exact) value $A(15, 7) = 2^5$. ■

Example. The code associated with $(2X + 2w, X^2 + 2w + 1) \subset GR(4^2)[X, \theta]/(X^2 + 1)$ contains 2^{10} code words and has lee distance 4. Its mapping to a code over $\mathbb{Z}_4$ and then to a code over $\mathbb{F}_2$ produces a code of length 16 with 2^{10} code words and distance 4 over $\mathbb{F}_2$. This has to be compared with the (exact) value $A(15, 3) = 2^{11}$. ■

Clearly we obtain much more code this way. This systematic approach should produce very good codes of large length. The result below an the correspondence of ideals seems to suggest that we only need to consider ideals $(f, 2\, f_1)$ where f and f_1 are monic polynomials which contain the ideal I.

2. We may consider other two sided ideals instead of a central polynomial f. According to [19] Section XX Proposition XX.3 and Exercise XX.11.c the two sided ideals of $GR(4^m)[X, \theta]$ are of the form $I = (f, 2\, f_1)$ where f and f_1 are monic polynomials. Any left ideal in $GR(4^m)[X, \theta]/(I)$ is a linear code over $GR(4^m)$. Therefore a first generalization would be to analyze the left ideals in those factor rings.

References

[1] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Comb. Th A 78-1 (1997) 92–119.

[2] K. Betsumiya, Y. Choie, Jacobi forms over totally real fields and Type II codes over Galois Rings $GR(2^m, f)$, Europ. J. of Comb., 25 (2004) 475–486.

[3] Bonnecaze, Alexis, Gaborit, Philippe, Harada, Masaaki, Kitazume, Masaaki, Solé, Patrick *Niemeier lattices and type II codes over Z_4*. Discrete Math. 205 (1999), no. 1-3, 1–21.

[4] A. Bonnecaze, R. Calderbank, P. Solé,*Quaternary Quadratic Residue Codes and Unimodular Lattices*, IEEE Trans. on Information Theory IT-41 (1995) 366-377.

[5] D. Boucher, W. Geiselmann, F. Ulmer, *Skew Cyclic Codes*, Applied Algebra in Engineering, Communication and Computing, 18, 2007, 379 - 389.

[6] D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, Prépublication IRMAR 08-07, to appear in *Journal of Symbolic Computation*

[7] Wieb Bosma, John Cannon and Catherine Playoust (1997). *The Magma Algebra System I: The User Language.* Journal of Symbolic Computation, **24**, pp. 235–265.

[8] N. Bourbaki, *Algèbre commutative.*, Chapitre II, Paris, Hermann (1961).

[9] S. Bouyukleva, M. Harada, *On Type IV self-dual codes over* $\mathbb{Z}_4$, Discrete Math **247** (2002) 25–50.

[10] Andries E. Brouwer (2005). Server for bounds on the minimum distance of q-ary linear codes, $q = 2, 3, 4, 5, 7, 8, 9$.`http://www.win.tue.nl/~aeb/`

[11] R. Chapman, P. Solé,*Universal Codes and Unimodular Lattices*, J. Théorie des Nombres de Bordeaux (1996) 369-376.

[12] Conway, J. H.; Sloane, N. J. A. *Sphere packings, lattices and groups*, Third edition. Grundlehren der Mathematischen Wissenschaften **290**,(1999), Springer-Verlag, New York.

[13] J.H. Conway, N.J.A. Sloane, *Self-dual codes over the integers modulo* 4, J. of Comb. Th. A, **62**, (1993) 30–45.

[14] P. Gaborit, A. M. Natividad and P. Solé *Eisenstein Lattices, Galois Rings and Quaternary Codes* International Journal of Number Theory Volume 2 (2006), 289–303.

[15] T. Aaron Gulliver, Masaaki Harada, *Certain self-dual codes over* $\mathbb{Z}_4$*, and the odd Leech lattice*, Springer Lect. Not. in Comp. Sc. 1255(1997) 130–137.

[16] Jacobson, N., *The theory of rings.*, Publication of the AMS. (1943).

[17] Litsyn S., Rains E.M. and Sloane N. J. A, *Table of Nonlinear Binary Codes*,`http://www.research.att.com/ njas/codes/And/`

[18] Nebe G. and Sloane N. J. A., *Table of Highest Minimal Norms of Modular Lattices*,`http://www.research.att.com/ njas/lattices/modular.html`

[19] Bernard R. McDonald, *Finite Rings with Identity.*, Marcel Dekker Inc. (1974).

[20] Eric Rains, *Optimal self-dual codes over* $\mathbb{Z}_4$, Discr. Math. 203 (1999) 215–228.

[21] E. Rains, N.J.A. Sloane, The shadow theory of modular and unimodular lattices, J. of Number Theory **73** (1998) 359–389.

[22] Ribenboim, P., *Sur la localisation des anneaux non commutatifs.*, Séminaire Dubreil. Algèbre et théorie des nombres, tome 24. (1970-1971).

[23] Zhe-Xian Wan, *Quaternary Codes.*, World Scientific. (1997).