Eisenstein lattices, Galois rings and quaternary codes

Philippe Gaborit*, Ann Marie Natividad†, Patrick Solé‡

Abstract

Self-dual codes over the Galois Ring $GR(4,2)$ are investigated. Of special interest are quadratic double circulant codes. Euclidean self-dual codes yield self-dual $\mathbb{Z}_4$-codes by projection on a trace orthogonal basis. Hermitian self-dual codes also give self-dual $\mathbb{Z}_4$-codes by the cubic construction, as well as Eisenstein lattices by Construction A. Applying a suitable Gray map to self-dual codes over the ring gives formally self-dual $\mathbb{F}_4$-codes, most notably in length 12 and 24.

Extremal unimodular lattices in dimension 38, 42 and the first extremal $3-$modular lattice in dimension 44 are constructed.

Keywords: Eisenstein lattices, Galois rings, $\mathbb{Z}_4$-codes, $\mathbb{F}_4$-codes

1 Introduction

The Galois ring $GR(4,2)$ of order 16 and characteristic 4 shares, as a coding alphabet, properties of both the ring $\mathbb{Z}_4$ and the field $\mathbb{F}_4$. Like $\mathbb{F}_4$ [11], it is endowed with a trace orthogonal basis which gives self-dual codes on the base ring $\mathbb{Z}_4$ by projection from a self-dual code on the extension. Like $\mathbb{Z}_4$ it affords a Gray map to the cartesian product of the residue field with itself; it is also, like $\mathbb{Z}_4$, a quotient of the ring $\mathbb{Z}$, a fact which allows to build Euclidean lattices by construction A.

We explore self-dual codes of length n over $GR(4,2)$ with four types of applications in mind

*LACO,Université de Limoges, 123 rue Albert Thomas, 87 Limoges, France `gaborit@unilim.fr`

†Department of Mathematics, University of the Philippines, Diliman, 1101 Quezon City, Philippines, `ann@math.upd.edu.ph`

‡CNRS, I3S ESSI, BP 145 Route des Colles 06 903 Sophia Antipolis, France, `ps@essi.fr`

- self-dual $\mathbb{Z}_4$-codes of length $2n$ by projection on a trace orthogonal basis
- quasi-cyclic self-dual $\mathbb{Z}_4$-codes of length $3n$ by the cubic construction
- modular lattices of dimension $2n$ by Construction A
- formally self-dual $\mathbb{F}_4$-codes of length $2n$ by Gray map

The coding applications will require either an euclidean or an hermitian scalar product, while the lattice application will require an hermitian scalar product. The construction technique is based on a generalization over $GR(4,2)$ of Quadratic Double Circulant codes over fields [8].

The material is organized in the following way. The next section contains the necessary definitions. Section III studies Quadratic Double Circulant Codes over $GR(4,2)$. Section IV develops in four successive subsections the four applications above.

2 Definitions and Notations

2.1 Lattices

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 [15, Th. 1] that the norm of an unimodular $n-$dimensionnal lattice is at most

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

for $n \neq 23$. An unimodular lattice meeting that bound is called **extremal**. Similarly, it was proved in [15, Th. 2] that the norm of a $3-$modular $n-$dimensionnal 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 [6, 15].

2.2 $\mathbb{Z}_4$-codes

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 $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$.

The Lee weight of a vector $x = (x_1, x_2, \ldots, x_n)$ is $\sum_{i=1}^n \min\{|x_i|,\ |(2k - x_i)|\}$. A self-dual code is Type II if all vectors in the code have Euclidean weights which are 0 (mod 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

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

It is shown in [3] 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 $\min\{4, \frac{d_E}{4}\}$.

2.3 $GR(4, 2)$-codes

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 $\mathbb{F}_4$. Let $\mathbb{T}$ denote the Teichmuller representatives of the cosets of $2R$ into R.

$$\mathbb{T} = \{0, 1, \alpha, \alpha^2\}.$$

For convenience let $\mathbb{T}^* = \mathbb{T} \setminus 0$. Define $\mathbb{T}_1 = \pm\mathbb{T}^*,\ \mathbb{T}_2 = 2\mathbb{T}_1,\ \mathbb{T}_3 = (\alpha - 1)\mathbb{T}_1$. 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 $z \in R$ downto $\mathbb{Z}_4$ by $T(z) := z + \overline{z}$.

By a code of length n over R we shall mean an $R-$submodule of R^n. A code is **Euclidean (resp. Hermitian) self-dual** if it is equal to its dual w.r.t. the form

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

respectively

$$x.y = \sum_i x_i \overline{y_i}$$

For $x \in R$ define $w_3(x) = 1, 4, 9$ if $x \in \mathbb{T}_1,\ \mathbb{T}_2,\ \mathbb{T}_3$ respectively, and zero otherwise. Extend it componentwise to R^n. The lattice weight on R^n is obtained by adding the contribution of each coordinate

$$w_3(x) = \sum_i w_3(x_i)$$

The minimum weight of a code C is

$$w_3(C) := \min\{w_3(x) \mid x \in C \ \&\ x \neq 0\}.$$

The composition of a vector $x \in R^n$ say $n_i(x)\, i = 0, 1, 2, 3$ is the number of entries in x of T_i. For instance $w_L(x) = n_1(x) + 4n_2(x) + 3n_3(x)$. The symmetrized weight enumerator (swe) of a code C is then defined as

$$swe_C(a, b, c, d) = \sum_{x \in C} a^{n_0(x)} b^{n_1(x)} c^{n_2(x)} d^{n_3(x)}$$

For Euclidean self-dual codes we recall the notion of Type II code introduced in [2]. Let $\overline{x}$ denote an arbitrary lift from $GR(4, 2)$ into $GR(8, 2)$. It was shown in [2], that, given x, $\overline{x}^2$ is unique. An Euclidean self-dual code is Type II iff each one of its codewords c satisfies

$$\sum_{i=1}^{n} \overline{c_i}^2 = 0,$$

or the equivalent condition

$$\sum_{i=1}^{n} T_8(\overline{c_i}^2) = 0,$$

where T_8 denotes the Trace from $GR(8, 2)$ downto $\mathbb{Z}_8$.

3 Quadratic Double Circulant Codes

Let q denote an odd prime power and $\epsilon = (-1)^{(q-1)/2}$. Let Q (resp. N) denote the matrices indexed by $\mathbb{F}_q$ and $Q_{i,j} = 1$ (resp. $N_{i,j} = 1$) if $j - i$ is a quadratic residue (resp. a non-residue) and $Q_{i,j} = 0$ (resp. $N_{i,j} = 0$) otherwise. If $r, s, t \in GR(4, 2)$ define

$$Q_q(r, s, t) := rI + sQ + tN.$$

This matrix can be bordered by adding one row and one column as

$$S_q(r, s, t) = \begin{pmatrix} u & v \\ w & Q_q(r, s, t) \end{pmatrix}$$

where $u, v, w \in GR(4,2)$. We shall always assume that $w = \epsilon v$. We can now define the *pure* QDC code by its generator matrix $P_q := (I, Q_q(r,s,t))$, and the *bordered* QDC code by its generator matrix $B_q := (I, S_q(r,s,t))$. Finally define the *twisted* QDC code by its generator matrix $(\beta I, \gamma I + S_q(r,s,t))$, where $\beta, \gamma \in GR(4,2)$. The notation $'XQ_q'$ means an extension of one column of the matrix Q_q such that the code generated by the matrix XQ_q is self-dual (Euclidean or Hermitian depending on the context). We mention, without proof [8], some basic facts on the matrices Q and N.

Lemma 3.1 *Let q be an odd prime power, and put $\epsilon = (-1)^{(q-1)/2}$. If $\epsilon = 1$ then*

- $Q = Q^t$ *and* $N = N^t$
- $QQ^t = 2kI + (k-1)Q + kN$
- $QN^t = NQ^t = kJ - kI$
- $NN^t = kQ + (k-1)N + 2kI$

while if $\epsilon = -1$

- $Q = Q^t$ *and* $Q + N + I = J$
- $QQ^t = (k+1)I + kJ$
- $QN^t = kQ + (k+1)N$
- $NQ^t = (k+1)Q + kN$
- $NN^t = (k+1)I + kJ$

The following result, essentially in [8], is needed to construct QDC Euclidean self-dual codes over R.

Theorem 3.2 *Let q be an odd prime power, and put $\epsilon = (-1)^{(q-1)/2}$. If $\epsilon = 1$ and $q = 4k+1$ then*

$$Q_q(a,b,c)Q_q(a,b,c)^t = Q_q(a^2 + 2k(b^2+c^2),\ 2ab - b^2 + k(b+c)^2,\ 2ac - c^2 + k(b+c)^2)$$

while if $\epsilon = -1$ and $q = 4k+3$

$$Q_q(a,b,c)Q_q(a,b,c)^t =$$

$$Q_q(a^2 + (2k+1)(b^2+c^2),\ ab + ac + k(b^2+c^2) + (2k+1)bc,\ ab + ac + k(b^2+c^2) + (2k+1)bc)$$

The next result is needed to construct QDC Hermitian self-dual codes over R, and follows from Lemma 3.1 after some algebra.

Theorem 3.3 *Let a, b, c be arbitrary in R, of conjugates a', b', c' Let q be an odd prime power, and put $\epsilon = (-1)^{(q-1)/2}$. If $\epsilon = 1$ and $q = 4k+1$ then*

$$Q_q(a,b,c)\overline{Q_q(a,b,c)}^t =$$

$$Q_q(aa'+2k(bb'+cc'), ab'+a'b+(k-1)bb'+k(cc'+b'c+bc'), ac'+a'c+kbb'+(k-1)cc'+k(bc'+b'c))$$

while if $\epsilon = -1$ and $q = 4k+3$

$$Q_q(a,b,c)\overline{Q_q(a,b,c)}^t =$$

$$Q_q(aa'+(2k+1)(bb'+cc'), ac'+a'b+kbc'+(k+1)cb'+k(bb'+cc'), k(b+b')(c+c')+bc'+ca'+ab')$$

Proof: If $q = 4k+1$ then

$$\begin{aligned}
Q_q(a,b,c)\overline{Q_q(a,b,c)}^t &= (aI + bQ + cN)(\overline{a}I + \overline{b}Q^t + \overline{c}N^t) \\
&= a\overline{a}I + a\overline{b}Q^t + a\overline{c}N^t + \overline{a}bQ + b\overline{b}QQ^t + b\overline{c}QN^t + \overline{a}cN + \overline{b}cNQ^t + c\overline{c}NN^t onumber \qquad (2) \\
&= a\overline{a}I + a\overline{b}Q + a\overline{c}N + \overline{a}bQ + b\overline{b}(2kI + (k-1)Q + kN) + b\overline{c}(kJ - kI) \\
&\quad + \overline{a}cN + \overline{b}c(kJ - kI) + c\overline{c}(kQ + (k-1)N + 2kI) \\
&= (a\overline{a} + 2kb\overline{b} - kb\overline{c} - k\overline{b}c + 2kc\overline{c})I + (a\overline{b} + \overline{a}b + (k-1)b\overline{b} + kc\overline{c})Q \\
&\quad + (a\overline{c} + kb\overline{b} + \overline{a}c + (k-1)c\overline{c})N + (kbnec + k\overline{b}c)J. \\
&= (a\overline{a} + 2k(b\overline{b} + c\overline{c}))I + (a\overline{b} + \overline{a}b + (k-1)b\overline{b} + kc\overline{c} + k(b\overline{c} + \overline{b}c))Qr \qquad (3) \\
&\quad + (a\overline{c} + \overline{a}c + kb\overline{b} + (k-1)c\overline{c} + k(b\overline{c} + \overline{b}c))N.
\end{aligned}$$

The case when $q = 4k+3$ can be proved similarly.

As corollaries, we derive infinite families of self-dual QDC code over $GR(4,2)$.

Corollary 3.4 *Let $q = 4k+3$ be a power of an odd prime. Then the code over $\mathbf{Z}_4[\omega] = GR(4,2)$ with generator matrix $P_q(2\omega+1, \omega, 3\omega+2)$ is Hermitian self-dual.*

Proof. : Using the corollary, $Q_q(2\omega+1,\omega,3\omega+2)\overline{Q_q(2\omega+1,\omega,3\omega+2)}^t = 3I$. Therefore the code with generator matrix $P_q(2\omega+1,\omega,3\omega+2)$ is Hermitian self-dual.

Corollary 3.5 *Let $q = 4k+1$ be a power of an odd prime. Then the code over $\mathbf{Z}_4[\omega] = GR(4,2)$ with generator matrix $P_q(2\omega+3, \omega, 3\omega+2)$ is Hermitian self-dual.*

Proof. : Using the corollary, $Q_q(2\omega+3,\omega,3\omega+2)\overline{Q_q(2\omega+3,\omega,3\omega+2)}^t = 3I$. Therefore the code with generator matrix $P_q(2\omega+3,\omega,3\omega+2)$ is Hermitian self-dual.

Corollary 3.6 *Let $q = 4k + 1$ be a power of an odd prime. Then the code over $\mathbf{Z}_4[\omega] = GR(4, 2)$ with generator matrix $B_q(0, 2 + 3\omega, 2 + \omega)$ is Hermitian self-dual, $u = 0, v = 2 + \omega$.*

Proof. : Using the corollary, $B_q(0, 2 + 3\omega, 2 + \omega)\overline{B_q(0, 2 + 3\omega, 2 + \omega)} = J - I$. Therefore the code with generator matrix $B_q(0, 2 + 3\omega, 2 + \omega)$ is Hermitian self-dual.

Corollary 3.7 *Let $q = 4k + 3$ be a power of an odd prime. Then the code over $\mathbf{Z}_4[\omega] = GR(4, 2)$ with generator matrix $B_q(2, 2 + 3\omega, 2 + \omega)$ is Hermitian self-dual, $u = 2, v = 1$, $\beta = 1, u = 1 + 2\omega$.*

Proof. : Using the corollary, $B_q(2, 2+3\omega, 2+\omega)\overline{B_q(2, 2 + 3\omega, 2 + \omega)} = 3J - 3I$. Therefore the code with generator matrix $B_q(2, 2 + 3\omega, 2 + \omega)$ is Hermitian self-dual.

Corollary 3.8 *Let $q = 4k + 3$ be a power of an odd prime and $k \equiv 0(mod\ 4)$. Then the code over $\mathbf{Z}_4[\omega] = GR(4, 2)$ with generator matrix $Q_q(3\omega + 3, 2\omega + 3, 3\omega)$ is Euclidean self-orthogonal and self-orthogonal by rank inspection.*

Proof. Using the theorem, $Q_q(3\omega + 3, 2\omega + 3, 3\omega)Q_q(3\omega + 3, 2\omega + 3, 3\omega)^t = 0$. Therefore the code with generator matrix $Q_q(3\omega + 3, 2\omega + 3, 3\omega)$ is Euclidean self-orthogonal and self-orthogonal by rank inspection.

Corollary 3.9 *Let $q = 4k + 1$ be a power of an odd prime and $3k \equiv 1(mod\ 4)$. Then the code over $\mathbf{Z}_4[\omega] = GR(4, 2)$ with generator matrix $Q_q(0, \omega + 1, \omega)$ is Hermitian self-dual.*

Proof. : Using the corollary, $Q_q(0, \omega + 1, \omega)\overline{Q_q(0, \omega + 1, \omega)}^t = 0$. Therefore the code with generator matrix $Q_q(0, \omega + 1, \omega)$ is Hermitian self-orthogonal and self-orthogonal by rank inspection.

4 Applications

4.1 A trace-orthogonal basis

Let $\gamma = \alpha$ and $\delta = \alpha^2 + 2\alpha = \alpha + 3$. Then a straighforward calculation shows that $T(\gamma^2) = T(\delta^2) = -1$ and that $T(\gamma\delta) = 0$. Note that ω, ω^2 is the unique trace orthogonal basis of $\mathbb{F}_4$ over $\mathbb{F}_2$. Define a bijective map ν say which maps $c\gamma + d\delta \in R$ onto $(c, d) \in \mathbb{Z}_4^2$. This map is extended componentwise to codes. The main motivation for considering such an object is the following result.

Theorem 4.1 *If $C \subseteq R^n$ is a euclidean self-dual code then $\nu(C)$ is a self-dual $\mathbb{Z}_4$ code. Furthermore $\nu(C)$ is Type II iff C is.*

Proof. The first statement is clear by trace orthogonality of the basis. The second statement follows by the following property of the trace of an arbitrary scalar $x \in GR(4,2)$

$$\overline{T(x)}^2 \equiv T_8(\overline{x}^2) \pmod 8,$$

extended to an arbitrary vector of $GR(4,2)^n$

$$\sum_{i=1}^{n} \overline{T(x_i)}^2 \equiv T_8(\sum_{i=1}^{n} \overline{x_i}^2) \pmod 8.$$

Examples:

length 8 Take C to be the code $XQ_3(1+\omega, 2+3\omega, 2\omega)$ $R-$code of generator matrix

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

Then $\nu(C)$ is the celebrated octacode O_8, [6, 3, 12], the unique Type II $\mathbb{Z}_4-$code of length 8 and minimum Lee weight 6., that occurs in one of the "holy" constructions of the Leech lattice [6], and whose Gray image is the Nordtrom-Robinson code [12]. It would be interesting to see if a similar construction holds for other extended quadratic residue $\mathbb{Z}_4-$codes [3] in higher lengths.

length 16 Let C be the R-code with generator matrix $XQ_7(2, 1+3\omega, 2\omega)$, then $\nu(C]$ is a Type I self-dual $\mathbb{Z}_4-$code of length 16, Lee distance 6 and Eucliden distance 8. Let C be the R-code with generator matrix $XQ_7(\omega, 2+3\omega, 1+2\omega)$, then $\nu(C]$ is a Type II self-dual $\mathbb{Z}_4-$code of length 16, sum of two lattices E_8.

length 38 Let C be the $R-$ span of $Q_{19}(3\alpha+3, 2\alpha+3, 3\alpha))$. (a Supplemented Quadratic Residue Code in the terms of [3]). Then $\nu(C]$ is a self-dual $\mathbb{Z}_4-$code of length 38, Lee distance 14 and Euclidean distance 16. Its generator matrix G is

$$G = \left[\begin{array}{c}
10000000000000000010303222333330003231 \\
01000000000000000011311100102021221112 \\
00100000000000000010230110101112121122 \\
00010000000000000010122011101021211123 \\
00001000000000000011111201201012120123 \\
00000100000000000011210120211011211023 \\
00000010000000000011220012112011120113 \\
00000001000000000011221001302111111022 \\
00000000100000000010221100221121110113 \\
00000000010000000011121110113022110022 \\
00000000001000000010211111102212210013 \\
00000000000100000011120111201131220012 \\
00000000000010000010211011211023121012 \\
00000000000001000010120101212012311112 \\
00000000000000100010111010212111230122 \\
00000000000000010010110101112121122023 \\
00000000000000001011110010202122111213 \\
00000000000000000111210001111122210132 \\
00000000000000000020220000202022220020 \\
00000000000000000022222222222222222222
\end{array}\right]$$

This code beats the d_L and d_E of the self-dual code of the same length in [10], it leads to an extremal unimodular lattice of dimension 38 of norm 4. Although an extremal lattice already exists in dimension 38 ([9]), this is the first extremal lattice in length 38 constructed from codes over $\mathbb{Z}_4$.

Using the $\mathbb{Z}_4$ Gray map yields a distance invariant formally self-dual binary code of length 76 comparable to an extremal binary self-dual code of that length, and a best-known linear $[76, 38]$ binary code [4].

length 40 Take C to be the code $XQ_{19}(1+\omega, 2+3\omega, 2\omega)$ then $\nu(C]$ is a Type II self-dual $\mathbb{Z}_4-$code of length 40 and Euclidean distance 16.

The symmetrized weight enumerator of $\nu(C)$ can be obtained by specialization from the cwe of an $R-$code.

Proposition 4.2 *If C is an arbitrary $R-$code then*

$$swe_{\nu(C)}(a, b, c) = cwe_C(a^2, b^2, c^2, b^2, ab, bc, bc, ab, ac, b^2, ab, ab, bc, bc)$$

4.2 Cubic Construction

By [13], every ℓ-quasi-cyclic code C over $\mathbb{Z}_4$ of length 3ℓ decomposes into a pair (C_1, C_2), where C_1 is a code over $\mathbb{Z}_4$ of length ℓ and C_2 is a code of length ℓ over $GR(4,2)$. Furthermore, if both C_1 and C_2 are self-dual so is C [13]. This correspondence is given by

$$C = \{(\mathbf{x} + 2\mathbf{a}' - \mathbf{b}' | \mathbf{x} - \mathbf{a}' + 2\mathbf{b}' | \mathbf{x} - \mathbf{a}' - \mathbf{b}') \mid \mathbf{x} \in C_1,\ \mathbf{a}' + \alpha\mathbf{b}' \in C_2\},$$

where $\alpha \in GR(4,2)$ satisfies $\alpha^2 + \alpha + 1 = 0$. Equivalently, by the Trace formula of [13] we have

$$C = \{(x + Tr(y) | x + Tr(\alpha^2 y) | x + Tr(\alpha y)) | \ \mathbf{x} \in C_1,\ y \in C_2\}$$

Proposition 4.3 *With the notation of the above subsection, let d, d_1, d_2 denote the minimum Lee weights of, respectively, C, C_1, $\nu(C_2)$. We then have*

$$d \leq 3d_1, \quad d \leq 8d_2.$$

Proof. Let $x \in C_1$ achieving d_1. Since $(x, x, x) \in C_1$ the first bound follows.

Similarly, let $a + \alpha b \in C_2$, such its ν image has Lee weight d_2. Since $(2a - b, -a + 2b, -a - b) \in C$, the bound follows after some algebra.

Examples:

length 30: Using this construction with

C1 —length 10, $[10, 4] - d10a$ [7]

C2 —Pure QDC parameters $(3w + 1, w, w + 2)$

Under the cubic construction, the resulting 10-quasi-cyclic code of length 30 is the self-dual $\mathbb{Z}_4-$code with generator matrix

$$G_{30} := \begin{bmatrix} 100000000000000122003232131032 \\ 010000000000000101130123220212 \\ 001000000000000130111312133221 \\ 000100000000000111230013202122 \\ 000010000000000131123323311230 \\ 0000010000000001013300032030120 \\ 0000001000000001032232203110322 \\ 0000000100000001021233302200211 \\ 0000000010000001020130230331022 \\ 0000000001000001020021323100103 \\ 000000000010001102013222130201 \\ 000000000001001012210100321003 \\ 000000000000101003230210320301 \\ 000000000000011020112003100231 \\ 000000000000002000022000202220 \\ 000000000000000222222222200000 \end{bmatrix}$$

length 30, Lee distance 10 and Euclidean distance 12. Construction A_4 yields an optimal unimodular lattice in dimension 30.

length 42: C_1 is the self-dual code over $\mathbb{Z}_4$ of length 14 referred to in [7] as $[14,6]-e_7+e_7$ C_2 is pure QDC over GR(4,2) of length 14 with generator matrix $P_7(2w+1, w, 3w+2)$. Under the cubic construction, the resulting 14-quasi-cyclic code of length 42 is the self-dual code with generator matrix

$$
G_{42} := \left[\begin{array}{c}
100000000000001000000300021021333011231 1131 \\
010000000000010000003000130111300301213311 \\
001000000000010000003000231311112201103133 \\
000100000000010000003000023013333011310333 \\
000010000000010000003000333013100211331013 \\
000001000000010000003000320013121331333121 \\
000000100000010000003000323111301221111110 \\
000000010000010000322000230001133321200101 \\
000000001000010000310000233203022012320111 \\
000000000100010000111000213311033100032310 \\
000000000010010000212000223011121120203013 \\
000000000001010000303000232100021230220002 \\
000000000000110000033000201100020332000202 \\
000000000000020000002000202000020202222222 \\
000000000000001000323000323103320031222303 \\
000000000000000100311000202201023332122311 \\
000000000000000010112000323111200100030332 \\
000000000000000001213000121311131332221013 \\
000000000000000000001001132100113200000000 \\
000000000000000000000102333010233300000000 \\
000000000000000000000011321001132100000000 \\
000000000000000000000000000222222222222222
\end{array}\right]
$$

The minimum Lee weight of **C** is 12 and the minimum Euclidean weight is 16. Construction A_4 yields an extremal unimodular lattice in dimension 42.

Below is a list of the codes we derived from the cubic construction having C_1 and C_2 as their component codes:

N	C_1	C_2	d_L	d_E
30	[10,4]-d10a	$P_5(3\omega+1,\omega,\omega+2)$	10	12
36	5-d4pe8e-12	$B_5(0,\omega,3\omega)$	12	12
39	3-d4-13	$Q_{13}(0,\omega+1,\omega)$	10	12
42	[14,6]-e7+e7	$P_7(2\omega+1,\omega,3\omega+2)$	12	16

Summary of l-quasi-cyclic self-dual codes of length 3l.

4.3 Eisenstein lattices

Let A_2 denote the hexagonal lattice scaled to have norm 2. In particular A_2 is 3-modular. In other words $A_2 = \sqrt{2}E$ where $E := \mathbb{Z}[\rho]$ stands for the ring of Eisenstein integers (here ρ is a complex third root of unity $\rho = \exp(2\pi\sqrt{-1}/3)$). In arithmetic terms A_2 is obtained as E equipped with the quadratic form $Tr(x\overline{y})$. Its Gram matrix as per the basis $(1, \rho)$ is

$$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$$

Observe that $A_2 = \sqrt{3}A_2^*$. To every $R-$code we attach an E-lattice by the following rule. Define construction A_3 in Forney symbolic notation as

$$A_3(C) = \frac{1}{\sqrt{2}}(C + 4A_2^n).$$

Then the properties that we need are summarized in the following statement.

Theorem 4.4 *If C is an hermitian self-dual $R-$code of length n then the real image of $A_3(C)$ is a $3-$modular $\mathbb{Z}-$lattice of dimension $2n$ and of norm*

$$\min(8, w_3(C)/2).$$

It is proven in [15] that 3-modular lattices exist for even dimensions n and that their norm μ is bounded by :

$$\mu \leq 2[\frac{n}{12}] + 2.$$

Lattices which satisfies this bound are said to be extremal.

By the preceding theorem it is therefore possible to construct extremal 3-modular lattices up to dimension 46.

Note that it is also possible to construct Eisenstein lattices from codes over $GF(4)$, but their norm is bounded by 4 then. In [1] extremal 3-modular lattices are constructed from Eisenstein lattices for dimensions higher than 24 but through a neighbouring construction and not directly by Construction A. The highest known extremal 3-modular lattice (in dimension 40) is constructed in [**?**]. A table of known such extremal lattices can be found in [14].

We now apply the preceding theorem to construct 3-modular lattices from self-dual Hermitian codes over R. We summarize these results in Table [**?**], where μ corresponds to the norm of the constructed lattices and K_{12} stands for the Coxeter-Todd lattice..

One lattice of norm 6 (the highest known norm for this dimension) was also constructed in [14]. The lattice of dimension 44 is new and extremal. The lattice of dimension 48 has the highest known norm for this dimension.

The following statement summarizes the main result of [5].

n	C	L	dim L	μ	upper bound
6	$P_3(2\omega+1,\omega,3\omega+2)$	K_{12}	12	4	4
10	$P_5(2\omega+3,\omega,3\omega+2)$	L_{20}	20	4	4
12	$B_5(0,2\omega+3,2+\omega)$	L_{24}	24	4	6
18	$P_9(2\omega+1,\omega,3\omega+2)$	L_{36}	36	6	8
20	$B_9(2,2\omega+3,2+\omega)$	L_{40}	40	6	8
22	$P_{11}(2\omega+3,\omega,3\omega+2)$	L_{44}	44	8	8
24	$B_{11}(0,2\omega+3,2+\omega)$	L_{48}	48	8??	10

Table 1: 3-modular lattices constructed from codes over R

Theorem 4.5 *If C is an hermitian self-dual $R-$code of length n with symmetrized weight enumerator $swe_C(X,Y,Z,T)$, then the real image of $A_3(C)$ has theta series $swe_C(\theta_0,\theta_1,\theta_2,\theta_3)(\sqrt{q})$ where the θ_i's are defined in [5] by*

$$\begin{aligned}
\theta_0(q) &= \sum_{x\in 4E} q^{x\overline{x}} \\
\theta_1(q) &= \sum_{x\in 1+4E} q^{x\overline{x}} \\
\theta_2(q) &= \sum_{x\in 2+4E} q^{x\overline{x}} \\
\theta_3(q) &= \sum_{x\in 2+\rho+4E} q^{x\overline{x}}
\end{aligned}$$

and are given up to $O(q^{50})$ by

$$\begin{aligned}
\theta_0 &= 1+6q^{16}+6q^{48} \\
\theta_1 &= q+q^9+2q^{13}+2q^{21}+q^{25}+2q^{37}+3q^{49} \\
\theta_2 &= 2q^4+2q^{12}+4q^{28}+2q^{36} \\
\theta_3 &= q^3+2q^7+2q^{19}+q^{27}+2q^{31}+2q^{39}+2q^{43}
\end{aligned}$$

4.4 Quaternary Codes

We consider the following Gray map ϕ

$$z = A+2B \mapsto (b, a+b)$$

from $GR(4,2)$ into $\mathbb{F}_4^2$. Here $A,B\in\mathbb{T}$ and a,b are their images under reduction modulo 2. It is easy to check that the Hamming weight of $\phi(x)$ is constant on $x\in\mathbb{T}_i$ of respective value $0,1,2,2$. For instance $\mathbb{T}_1$ consists of elements of the form $\pm A$, $\mathbb{T}_2$ consists of elements

n	R-code	sd	$\to$	$2n$	F4-code	num	d
6	$P_3(\omega, 3\omega+1, 3\omega+1)$	H		12	C_{12}	4^6	6
8	$XQ_7(1, 1+2\omega, 1+3\omega)$	H		16	C_{16}	4^8	6
12	$XQ_{11}(0, 1+2\omega, 1+3\omega)$	E		24	C_{24}	4^{12}	9

Table 2: Non-linear $\mathbb{F}_4$ codes

of the form $2B$, and so on. The Hamming weight enumerator of $\phi(C)$ can therefore be easily obtained from its swe:

$$W_{\phi(C)}(x,y) = swe_C(x^2, xy, y^2, y^2).$$

For convenience one can define a super symmetrized weight enumerator

$$sswe_C(X,Y,Z) := swe_C(X,Y,Z,Z).$$

With this notation

$$W_{\phi(C)}(x,y) = sswe_C(x^2, xy, y^2).$$

Proposition 4.6 *If C is either hermitian or euclidean self-dual then $\phi(C)$ is distance invariant formally self-dual for the Hamming weight enumerator.*

Proof. The distance invariance follows by the linearity of C and the isometry property of the Gray map. It can be shown, combining the MacWilliams identity for the cwe with Lemma 4.2, that the *sswe* enjoys the following MacWilliams relation

$$sswe_{C^\perp}(X,Y,Z) = \frac{1}{|C|} sswe_C(X+2Y+Z, X-Z, X-2Y+Z)$$

The result follows by the binomial theorem and the relation between $W_{\phi(C)}$ and the *sswe*.

We construct in particular three interesting non-linear codes over $GF(4)$. The Table 2 summarizes their construction, 'sd' in the table stands for the type of self-duality 'H', Hermitian, or 'E', Euclidean, and 'num' stands for the number of codewords.

By construction the codes constructed over $\mathbb{F}_4$ are *a priori* non-linear but their weight enumerators satisfy the same properties than fsd codes.

The weight enumerator of C_{12} is:

$$1 + 360\, y^6 + 216\, y^7 + 945\, y^8 + 720\, y^9 + 1440\, y^{10} + 216\, y^{11} + 198\, y^{12}$$

Note that only 2 $(12, 4^6, 6)$ codes are known (besides C_{12}), the extended quadratic residue code of length 11 over $\mathbb{F}_4$, which is linear, and the non-linear additive $\mathbb{F}_4$ dodecacode. It can be checked in Magma that C_{12} is 1-homogeneous, i.e. each weight class holds a $1-$design.

The weight enumerator of C_{16} is :

$$1 + 336\,y^6 + 90\,y^8 + 6720\,y^9 + 5376\,y^{10} + 12096\,y^{11} + 10920\,y^{12} + 20160\,y^{13} + 5040\,y^{14} + 4032\,y^{11} + 765\,y^{16}$$

Many linear $(16, 4^8, 6)$ codes are known, C_{16} has the particularity of having no words of weight 7.

The weight enumerator of C_{24} is:

$$1 + 2112\,y^9 + 7920\,y^{10} + 23760\,y^{11} + 877714\,y^{12} + 242424\,y^{13} + \ldots$$

Presently no $(24, 4^{12}, 9)$ Euclidean self-dual is known and Hermitian self-dual codes over $\mathbb{F}_4$ have distance, upper bounded by 8. Linear $(24, 4^{12}, 9)$ can be constructed from XQ_{29} but they have no reason to be fsd.

References

[1] C. Bachoc, Applications of Coding Theory to the Construction of Modular Lattices, *Jour. Comb. Th. (A)*, **(78)**, (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., submitted (2003).

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

[4] `http://homepages.cwi.nl/htbin/aeb/lincodbd/`

[5] K-S. Chua, P. Solé, Eisenstein lattices, Galois rings, and theta series, European J. of Combinatorics in press.

[6] J. H. Conway, N.J. A. Sloane, *Sphere Packings, Lattices and Groups* Springer (1993).

[7] J. Fields, P. Gaborit, J. Leon and V. Pless, All self-dual Z4 codes of length 15 or less are known, *IEEE Trans. Inform. Theory*, **44**, (1998), pp. 311 - 322, (`http://www2.math.uic.edu/ fields/z4/index.html`).

[8] . P. Gaborit, Quadratic Double Circulant Codes over Fields, J. Comb. Theory Ser. A 97 (2002) 85–107.

[9] . P. Gaborit, Construction of new extremal unimodular lattices, *to appear in Eur. Jour. Comb.*

[10] Philippe Gaborit and Ayoub Otmani, *Experimental constructions of codes over rings and construction of an optimal unimodular lattice in dimension 43*, Preprint(2003).

[11] Philippe Gaborit, Vera Pless, Patrick Solé and Oliver Atkin, Type II Codes over $\mathbb{F}_4$, Finite Fields and Their Applications, Volume 8, Issue 2, April 2002, Pages 171-183

[12] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4-$Linearity of Kerdock, Preparata, Goethals and Related Codes, IEEE Trans. Information Theory, 40 (1994), pp. 301-31

[13] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, Designs, Codes and Cryptography **30** (1) (2003) 113–130.

[14] G. Nebe and N. J. A. Sloane, *A catalogue of lattices* http://www.research.att.com/~njas/lattices

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