APPLICATIONS OF CODING THEORY TO THE CONSTRUCTION OF MODULAR LATTICES

BY CHRISTINE BACHOC

Recherche effectuée au sein de l'Unitée Mixte
C.N.R.S.–Enseignement supérieur U.R.M. 9936

28 March 1996

ABSTRACT. We study self-dual codes over certain finite rings which are quotients of quadratic imaginary fields or of totally definite quaternion fields over $\mathbb{Q}$. A natural weight taking two different non zero values is defined over these rings ; using invariant theory, we give a basis for the space of invariants to which belongs the three variables weight enumerator of a self-dual code. A general bound for the weight of such codes is derived. We construct a number of extremal self-dual codes, which are the codes reaching this bound, and derive some extremal lattices of level $l = 2, 3, 7$ and minimum $4, 6, 8$.

1. Introduction

Most of the lattices known for their good density share the following property : they are l-modular for a certain level l equal to 1 or a prime number. This means, following [Q4], that they are even lattices such that a similarity of rate $\sqrt{l}$ sends their dual lattice to themselves. This definition includes the even unimodular lattices, and also famous lattices like the Coxeter-Todd lattice of dimension 12 and level 3 and the Barnes-Wall lattices which are, after rescaling, alternatively 2-modular or unimodular.

Such lattices appear naturally in the following situation : let K be either a number field with complex multiplication, or a quaternion field defined over a totally real number field with all its infinite places ramified in K. We denote by $x \to \overline{x}$ the canonical conjugation on K. Let V be a (left) K-vector space of finite dimension, endowed with a non degenerate hermitian form $h(x, y)$. Most often, $V = K^n$ and $h(x, y) = \sum_{i=1}^{n} x_i \overline{y_i}$, or a multiple of it. Let $\mathfrak{O}_K$ be a maximal order of K, and let L be an $\mathfrak{O}_K$-lattice contained in V. The hermitian dual of L is defined by : $L_h^* = \{x \in V / h(x, V) \in \mathfrak{O}_K\}$.

Then L is a $\mathbb{Z}$-lattice for the scalar product : $x.y = \mathrm{Trace}_{K/\mathbb{Q}}(h(x, y))$, where $\mathrm{Trace}_{K/\mathbb{Q}}$ is respectively the trace form of $K/\mathbb{Q}$ when K is a number field, and the compositum of

Key words and phrases. code, lattice, modular lattice, extremal lattice.

I wish to thank Jacques Martinet and Heinz-Georg Quebbemann for helpful discussions and their encouragements .

the reduced trace of K with the trace form of its center when K is a quaternion field. We denote it by $L_{\mathbb{Z}}$. Its dual is given by $L_{\mathbb{Z}}^* = \mathcal{D}_{K/\mathbb{Q}}^{-1} L_h^*$, where $\mathcal{D}_K$ is the different of K. This shows that, if this ideal is principal, and if L is hermitian unimodular, then the lattice $L_{\mathbb{Z}}$ is modular of level $|d_K| = \mathrm{Norm}_{K/\mathbb{Q}}(\mathcal{D}_K)$ (the similarity being the left multiplication by a generator of the different).

On the other hand, it is shown in [Q4] that one gets a l-modular lattices of smallest dimension by taking $(\mathfrak{O}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$, where K is either the quadratic imaginary field of discriminant l if $l \equiv 3 \mod 4$, or the quaternion field over $\mathbb{Q}$ ramified at l and ∞ if $l = 2$ or $l \equiv 1 \mod 4$. It is then natural to focus on lattices which are unimodular over these structures. Previous work was already done in this direction in [B], [Q1], [Q2], [Q3], [F], [BQS] ; in these papers the main tools used to construct or classify such lattices are mass formula and Kneser neighbouring.

Some previous constructions make use of codes, like in [Q3], [B] ; we want here to generalize these constructions by defining codes over finite involution algebras which are quotients of these maximal orders. Then self-dual codes give by "construction A" (i.e. by taking their preimage in $\mathfrak{O}_K^n$) hermitian unimodular lattices. A suitable weight over these finite rings permits to measure the minimum of the corresponding lattices. In section 3, we set MacWilliams identities for these codes and derive with the help of invariant theory Gleason-type theorems for the corresponding weight enumerator polynomial. Here the results are very similar to those concerning self-dual codes over $\mathbb{Z}_4$ (see [CS3]). This leads to a bound for the minimal weight, and to the notion of extremal codes, which are the codes meating this bound.

In section 4, we construct extremal codes in some special cases, which give rise to some extremal modular lattices of level 2, 3 and 7 of minimum 4, 6, 8, some of which were not yet known.

2. Codes over $\mathfrak{O}_K/p\mathfrak{O}_K$. Definitions.

We take the following notations for the rest of the paper : K is either an imaginary quadratic field, or a quaternion field of center $\mathbb{Q}$ ramified at ∞. We denote by $x \to \overline{x}$ the canonical involution on K. We fix a maximal order $\mathfrak{O}_K$ of K (it is not unique if K is a quaternion field, see [V]).

Let p be a prime number. We want to define codes over the finite ring $\mathfrak{O}_K/p\mathfrak{O}_K$, which is a $\mathbb{F}_p$-algebra endowed with an involution $x \to \overline{x}$ deduced from the one on K. We first look at its structure :

Proposition 2.1. *The $\mathbb{F}_p$-algebra with involution $\mathfrak{O}_K/p\mathfrak{O}_K$ is isomorphic to the following algebra A :*

(1) *K is a quaternion field and p is split in K. Then*

$$A = \mathcal{M}_2(\mathbb{F}_p) \quad \forall x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \overline{x} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

(2) *K is a quaternion field and p is ramified in K. Then*

$$A = \mathbb{F}_{p^2} + u\mathbb{F}_{p^2} \text{ with } u^2 = 0 \text{ and } au = ua^p \text{ for all } a \in \mathbb{F}_{p^2}$$

$$\forall x = a + ub, \quad \overline{x} = a^p - ub$$

(3) *K is an imaginary quadratic field and p is split in K. Then*

$$A = \mathbb{F}_p \times \mathbb{F}_p \quad \forall x = (a, b) \quad \overline{x} = (b, a)$$

(4) *K is an imaginary quadratic field and p is ramified in K. Then*

$$A = \mathbb{F}_p + u\mathbb{F}_p \text{ with } u^2 = 0 \text{ and } au = ua \text{ for all } a \in \mathbb{F}_p$$

$$\forall x = a + ub, \quad \overline{x} = a - ub$$

(5) *K is an imaginary quadratic field and p is inert in K. Then*

$$A = \mathbb{F}_{p^2} \quad \overline{x} = x^p$$

Proof. It is obvious once K is completed at p. See [V] for the quaternionic case. □

The case (5) is covered by the classical coding theory. We assume in the rest of the paper that A is one of the algebras defined in the previous proposition, and we will refer to it by its number. The cases (2) and (4) will most often be treated together, by setting $A = \mathbb{F}_q + u\mathbb{F}_q$ with $q = p, p^2$; it is the ramified case, while the cases (1) and (3) are the so-called split cases.

A code C of length n over A is then a left submodule of A^n. Orthogonality is defined with respect to the form $\sum_{i=1}^n x_i\overline{y_i}$. The code C is said to be self-dual if $C = C^\perp$.

Two codes are said to be equivalent if a monomial transformation sends one of them on the other. Such a transformation is a permutation matrix where the ones can be replaced by invertible elements of A, acting on A^n from the right. We summarize in the following the group A^* of invertible elements of A :

Lemma 2.2.

(1) $A = \mathcal{M}_2(\mathbb{F}_p)$; $A^* = \mathcal{G}l_2(\mathbb{F}_p)$
(2) $A = \mathbb{F}_{p^2} + u\mathbb{F}_{p^2}$; $A^* = \{x = a + bu \mid a \neq 0\}$
(3) $A = \mathbb{F}_p \times \mathbb{F}_p$; $A^* = \{(a, b) \mid a \neq 0, b \neq 0\}$
(4) $A = \mathbb{F}_p + u\mathbb{F}_p$; $A^* = \{x = a + bu \mid a \neq 0\}$
(5) $A = \mathbb{F}_{p^2}$; $A^* = \mathbb{F}_{p^2}^*$

Examples 2.3. Let A be one of the algebras (1)-(4). The following construction is the translation in terms of codes of the lattices U defined in [M1], [M2,Chap.VIII]. Let I be a left ideal of A, distinct from $\{0\}$ and A. If $A = \mathcal{M}_2(\mathbb{F}_p)$, there are $p + 1$ such ideals, and the group of units of A is doubly transitive on them. If $A = \mathbb{F}_q + u\mathbb{F}_q$, there is only one which is $u\mathbb{F}_q$. If $A = \mathbb{F}_p \times \mathbb{F}_p$ there are two of them, namely $\mathbb{F}_p \times \{0\}$ and $\{0\} \times \mathbb{F}_p$, which are conjugate.

We set $C_1 = I$. Then C_1 is a self-dual code of length one over A. In case (1), C_1 is unique up to equivalence ; in case (3), the two ideals define conjugate codes.

If A is (1) or (3), let I' be a second non trivial ideal, distinct from I. If A is (2) or (4), let $I' = \{0\}$. We set, for $n \geq 2$:

$$C_n = \{(x_1, .., x_n) \in A^n \mid \quad \forall i \neq j \quad x_i \equiv x_j \mod I \text{ and } \sum_{i=1}^{n} x_i \equiv 0 \mod I'\}.$$

Then, with the additional condition $n \equiv 0 \mod p$ in cases (2) and (4), C_n is a self-dual code over A. In order to prove this, let us remark that the choice of (I, I') has no importance because of the previous remarks on the ideals of A. Let $x = (x_1, .., x_n)$ and $y = (y_1, .., y_n)$ be two elements of C_n. Then $x.y = \sum_{i=1}^n x_i\overline{y_i} = \sum_{i=1}^n (x_i - x_1)(\overline{y_i} - \overline{y_1}) + (\sum_{i=1}^n x_i)\overline{y_1} + x_1(\sum_{i=1}^n \overline{y_i}) - nx_1\overline{y_1}$. The first sum belongs to $I\overline{I}$, which is reduced to $\{0\}$; in cases (2) and (4), we see that $C_n \subset C_n^\perp$ is equivalent to $n \equiv 0 \mod p$. In cases (1) and (3), we can assume that $I = Ae$, $I' = A\overline{e}$ with $e^2 = e$. Then $e + \overline{e} = 1$ and $e\overline{e} = 0$. Writing $x_1\overline{y_1} = x_1(e + \overline{e})\overline{y_1}$, $(\sum_{i=1}^n x_i)\overline{y_1} + x_1(\sum_{i=1}^n \overline{y_i}) - nx_1\overline{y_1} = (\sum_{i=1}^n (x_i - x_1))\overline{e}\,\overline{y_1} + x_1 e \sum_{i=1}^n (\overline{y_i} - \overline{y_1})$ which is zero because $x_i - x_1 \in Ae$ and $\overline{y_i} - \overline{y_1} \in \overline{e}A$. In all cases we have proved the inclusion $C_n \subset C_n^\perp$, which turns to be an equality because the number of elements of C_n is exactly $\sqrt{|A|}^n$.

The previous definition and proof have the advantage to be uniform. If we denote by $\mathbf{1}$ the code over $\mathbb{F}_p$ generated by $(1, 1, .., 1)$ and by PC its dual the parity-check code, it is easy to see that in cases (2) and (4), $C_n = \mathbf{1} + uPC$, and in case (3) $C_n = \mathbf{1} \times PC$, with evident notations.

3. Lattices and weights

Assume that K and A are as in Proposition 2.1. To a code C of length n over A we associate the following lattice :

$$L_C = \{(x_1, .., x_n) \in \mathfrak{O}_K \mid x_1..x_n \mod p \in C\}$$

with the hermitian form : $h(x, y) = 1/p \sum_{i=1}^n x_i\overline{y_i}$, and the scalar product : $x.y = \mathrm{Trace}_{K/\mathbb{Q}}(h(x, y))$. (Notice that a code over a given ring A can be lifted to various fields K).

Now we want to define a weight on A which measures well the minimum of the lattice L_C. We have, for x in $\mathfrak{O}_K$, $x.x = \frac{2}{p}x\overline{x}$. If x belongs to an ideal $\mathfrak{p}$ satisfying $p\mathfrak{O}_K \subset \mathfrak{p} \subset \mathfrak{O}_K$, then $x\overline{x}$ is always a multiple of p. So, as the union of the proper ideals of A is the complementary set of A^*, it is natural to set :

Definition 3.1. *Let A be one of the rings defined in (1) ... (5). The weight w on A is defined by :*

$$\begin{cases} w(0) = 0 \\ w(x) = 1 \text{ if } x \in A^* \\ w(x) = p \text{ if } x \in A \backslash (A^* \cup \{0\}) \end{cases}$$

Remark. *It is the Hamming weight in case (5).*

We extend it to A^n in the standard way by setting $w(x_1,..,x_n) = \sum_{i=1}^n w(x_i)$. The weight of a code C is the minimum of the weights of its non zero elements. If K is a field with the quotient $\mathfrak{O}_K/p\mathfrak{O}_K$ isomorphic to A, we denote by $s_K : \mathfrak{O}_K \to A$ the canonical surjection and extend it componentwise to $\mathfrak{O}_K^n$. We have then, for all $x = (x_1,..,x_n) \in \mathfrak{O}_K^n$, $x.x \geq \frac{2}{p} w(s_K(x))$. This minoration may not be optimal, unless it coincides with the length function l_K which is defined on A by :

$$\forall a \in A, l_K(a) = \min\{x\overline{x} \mid s_K(x) = a\}$$

Of course, l_K depends on K while w does not. For all a in A, $w(a)$ is a divisor of $l_K(a)$. Before we look at the cases where they coincide, we will study a weaker condition, trivially verified by l_K, which is the following one :

$$(*) \qquad \forall x \in A, w(x) \equiv x.x \mod p$$

This congruence is true in the classical coding theory cases, i.e. for the Hamming weight over $\mathbb{F}_2$, $\mathbb{F}_3$ with the form $\sum x_i y_i$, or over $\mathbb{F}_4$ with the form $\sum x_i \overline{y_i}$. It is worth remarking here that, if (*) holds, then a self-orthogonal code has all its weights divisible by p.

Proposition 3.2. *The condition (*) holds for the weight w if and only if $A = \mathcal{M}_2(\mathbb{F}_2)$, $\mathbb{F}_q + u\mathbb{F}_q$ with $q = 2, 3, 4$, $\mathbb{F}_2 \times \mathbb{F}_2$, or $\mathbb{F}_q$ with $q = 2, 3, 4$.*

Proof. Assume $A = \mathcal{M}_2(\mathbb{F}_p)$. Let x be an element of A ; then $x.x = x\overline{x} = \det(x)$. Then, if (*) holds, every invertible matrix should have determinant 1, which implies $p = 2$. Assume that $A = \mathbb{F}_q + u\mathbb{F}_q$, and let $x = a + ub$ be an element of A. Then, in the two cases (2) and (4), $x.x = x\overline{x} = a\overline{a}$ where $\overline{a} = a$ or a^p. Then (*) implies that $a\overline{a} \equiv 1 \mod p$ for all $a \in \mathbb{F}_q^*$, and so $q = 2, 3, 4$. Finally, if $A = \mathbb{F}_q \times \mathbb{F}_q$ and $x = (a, b)$ then $x.x = (ab, ab)$ and we need $p = 2$.

Conversely, (*) holds in those cases. □

Examples 3.3. Computation of the weight of the codes C_n : the code C_1 has of course weight 1.

In case $A = \mathbb{F}_q + u\mathbb{F}_q$, let $x \in C_n$. We set $x = (x_1,..,x_n)$ with $x_i = a + ub_i$, $\sum_{i=1}^n b_i = 0$. If $a \neq 0$, $w(x) = n$, and if $a = 0$, $w(x) = p.wt(a) \geq 2p$ where wt is the Hamming weight. Hence $w(C_n) = min(2p, n)$. In the case $A = \mathbb{F}_p \times \mathbb{F}_p$, $x_i = (a, b_i)$ with $\sum_{i=1}^n b_i = 0$; if $a = 0$, w(x)=p.wt(b) and if $a \neq 0$, $w(x) = wt(b) + p(n - wt(b)$. Hence $w(C_n) = min(2p, n)$ if $n \equiv 0 \mod 2$ and $w(C_n) = min(2p, n+p-1)$ if $n \equiv 1 \mod 2$. In the case $A = \mathcal{M}_2(\mathbb{F}_p)$, we take $e = (\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix})$ so that $x_i = (\begin{smallmatrix} a & b_i \\ c & d_i \end{smallmatrix})$ with $\sum_{i=1}^n b_i = \sum_{i=1}^n d_i = 0$. The det function $x \mapsto (\det(x_i))_i = (ad_i - cb_i)_i$ sends C_n to the parity-check code over $\mathbb{F}_p$. If $a = c = 0$, $w(x) \geq 2p$, and if a or c is non zero, $w(x) = wt(\det(x)) + p(n - wt(\det(x)))$. Again we find the same result as for the previous case.

The following proposition tells us when l_K and w coincide. These are the interesting cases for the construction of lattices.

Proposition 3.4. *We have $w = l_K$ if and only if :*

(1) $K = \mathbb{Q}_{3,\infty}$, $p = 2$, $A = \mathcal{M}_2(\mathbb{F}_2)$
(2) $K = \mathbb{Q}_{2,\infty}$, $p = 2$, $A = \mathbb{F}_4 + u\mathbb{F}_4$
(3) $K = \mathbb{Q}(\sqrt{-7})$, $p = 2$, $A = \mathbb{F}_2 \times \mathbb{F}_2$
(4) $K = \mathbb{Q}(i)$, $i^2 = -1$, $p = 2$, $A = \mathbb{F}_2 + u\mathbb{F}_2$
(5) $K = \mathbb{Q}(\omega)$, $\omega^2 + \omega + 1 = 0$, $p = 2$, $A = \mathbb{F}_4$, *or* $p = 3$, $A = \mathbb{F}_3 + u\mathbb{F}_3$

Proof. A necessary condition for w to be equal to l_K is that the image of $\mathfrak{O}_K^*$ under s_K is all of A^*. Of course, we are in one of the cases of the previous proposition. We make use of the following well-known result : if K is a quadratic imaginary field, then $\mathfrak{O}_K^* = \{\pm 1\}$, unless $K = \mathbb{Q}(i)$, for which $\mathfrak{O}_K^* = \{\pm 1, \pm i\}$ is cyclic of order 4, or $K = \mathbb{Q}(\omega)$, for which $\mathfrak{O}_K^* = \{\pm 1, \pm\omega, \pm\omega^2\}$ is cyclic of order 6 ; if K is a quaternion field over $\mathbb{Q}$ ramified at ∞, then $\mathfrak{O}_K^*$ is cyclic of order 2,4,6, except in two cases : $K = \mathbb{Q}_{2,\infty}$ the quaternion field ramified at 2 and ∞, defined by $i^2 = -1$, $j^2 = -1$, $ij = -ji$; the maximal order is unique up to conjugation and equal to the so-called Hurwitz order $\mathbb{Z}[1, i, j, (1 + i + j + k)/2]$. Its units are $\{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$, a group of order 24 isomorphic to $\tilde{A}_4$ (the non trivial central extension of the alternating group A_4 by $\{\pm 1\}$). The other case is $K = \mathbb{Q}_{3,\infty}$ the quaternion field ramified at 3 and ∞, defined by $i^2 = -1$, $j^2 = -3$; the maximal order is unique up to conjugation and equals $\mathbb{Z}[1, i, \omega = (-1 + j)/2, i\omega]$. Its units are $\{\pm 1, \pm\omega, \pm\omega^2, \pm i, \pm i\omega, \pm i\omega^2\}$ and form a quaternionic group of order 12. (The proof goes through the classification of the finite subgroups of the real Hurwitz quaternions. See [M,Appendice 2] or [V]).

Case (3) reduces to $K = \mathbb{Q}(\sqrt{-7})$ because it is the only quadratic imaginary field in which 2 is split and the ideals above 2 are principal.

It is now easy to see that the condition $s_K(\mathfrak{O}_K^*) = A^*$ leaves the only possibilities listed in the proposition, and that in those cases we do have $l_K = w$. $\square$

Remark 3.5. Of course, most often, we have $l_K \neq w$. For example, if $K = \mathbb{Q}_{3,\infty}$, the function l_K over $\mathfrak{O}_K/3\mathfrak{O}_K$ takes five different non zero values. Another example is in [Q3] with $A = \mathbb{F}_9 \times \mathbb{F}_9$.

The lattice L_C has the following properties :

Proposition 3.6. *The lattice $(L_C, h(x, y))$ is hermitian unimodular if and only if $C = C^\perp$. Under this condition, the $\mathbb{Z}$-lattice $L_\mathbb{Z} = (L_C, x.y)$ is even, of determinant $|d_K|^{n[K/\mathbb{Q}]/2}$, where $|d_K|$ is the discriminant of the field K. Moreover, if the different of K is principal and L_C is unimodular, then $L_\mathbb{Z}$ is a $|d_K|$-modular lattice. The minimum of $L_\mathbb{Z}$ is bounded by :*

$$\min(L_Z) \geq \min(2p, \frac{2}{p} w(C))$$

with equality if we are in one of the cases of proposition 3.4.

Proof. It is immediate with the following properties : $(L_C)_h^* = L_{C^\perp}$ and $L_\mathbb{Z}^* = \mathcal{D}_{K/\mathbb{Q}}^{-1} L_h^*$ (see [B]). If $x \in L_C$, $x.x = \mathrm{Trace}_{K/\mathbb{Q}}(h(x, x)) = 2h(x, x) \in 2\mathbb{Z}$ since $h(x, x) \in \mathfrak{O}_K$, and L_C is even. If the different is principal generated by α, let $f(x) = \alpha x$. Then $L =$

$\mathcal{D}_{K/\mathbb{Q}} L_{\mathbb{Z}} = f(L_{\mathbb{Z}})$ and $f(x).f(y) = \mathrm{Trace}_{K/\mathbb{Q}}(h(\alpha x, \alpha y)) = \mathrm{Trace}_{K/\mathbb{Q}}(\alpha\overline{\alpha} h(x,y)) = |d_K| x.y$ since $\alpha\overline{\alpha} = |d_K|$; hence a hermitian unimodular lattice is $|d_K|$-modular.

Let x be an element of L_C. If x belongs to $p\mathfrak{O}_K^n$, then $x.x \geq \min(p\mathfrak{O}_K^n) = 2p$. If x doesn't belong to $p\mathfrak{O}_K^n$, then $s_K(x) \neq 0$ and $x.x \geq \frac{2}{p} w(C)$. Since in the cases of proposition 3.4 we have $w = l_K$, the previous inequality is an equality. □

Remark 3.7. In the cases of proposition 3.4, the maximal order (which is unique up to conjugation) is principal. The lattice $L_{C_1} \simeq (\mathfrak{O}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$ is isometric repectively to : (1) $\mathbb{A}_2 \perp \mathbb{A}_2$, (2) $\mathbb{D}_4$, (3) the lattice with Gram matrix $\begin{pmatrix} 2 & 1 \\ 1 & 4 \end{pmatrix}$, (4) $\mathbb{A}_1 \perp \mathbb{A}_1$, (5) $\mathbb{A}_2$ with the standard notations for the root lattices.

Remark 3.8. If $K = \mathbb{Q}(\sqrt{-d})$ where d has no square factor and $-d \equiv 2, 3 \mod 4$, then $d_K = -4d$ and $L_C/\sqrt{2}$ is still an integral lattice. It is d-modular but not necessarily even. It is the case if $K = \mathbb{Q}(i)$, where we get unimodular lattices. The study of the codes over the corresponding algebra $\mathbb{F}_2 + u\mathbb{F}_2$ reduces trivially to binary codes by the following transformation : $\phi : \mathbb{F}_2 + u\mathbb{F}_2 \to \mathbb{F}_2 \times \mathbb{F}_2$ defined by $\phi(x + yu) = (x + y, y)$ which preserves the weight.

4. MacWilliams identities and invariant theory

In this section, we study the weight enumerator polynomials related to the codes over the algebras defined in proposition 2.1. More generally, if $A = \{w_0 = 0, w_1, .., w_{d-1}\}$ is a ring with an involution $x \to \overline{x}$ satisfying $\overline{xy} = \overline{y}\,\overline{x}$, the complete weight enumerator of a code C of length n over A is defined by ([MWS]) :

$$W_C^c(z_0, z_1, .., z_{d-1}) = \sum_{u \in C} z_o^{s_o(u)} z_1^{s_1(u)} .. z_{d-1}^{s_{d-1}(u)},$$

where, for all i, $0 \leq i \leq d-1$, $s_i(u)$ is the number of coordinates of u equal to w_i.

The MacWilliams identity is then :

Theorem 4.1.
Let $\chi : (A, +) \to (\mathbb{C}^*, \times)$ be a character of the additive group of A whose restriction to any non zero left ideal of A is non trivial. Then :

$$W_{C^\perp}^c(z_0, z_1, .., z_{d-1}) = \frac{1}{\mathrm{Card}(C)} W_C^c(M(z_0, z_1, .., z_{d-1})),$$

where

$$M = (\chi(w_i \overline{w_j}))_{\substack{0 \leq i \leq d-1 \\ 0 \leq j \leq d-1}}.$$

(The matrix M operates on the d-tuples in the usual way).

Proof. It is a consequence of [D, Chap. 6]. It also can be proved directly as in the classical case ([MWS, Chap.5]) using the Poisson summation formula.

Let us go back to the cases we are interested in. For most of them, the size of A is too large to allow us to handle the complete weight enumerator ; in view of the weight defined in 3.1, it is natural to specialize it to the following three variables polynomial :

$$W_C(X,Y,Z) = \sum_{u \in C} X^{t_0(u)} Y^{t_1(u)} Z^{t_2(u)},$$

where $t_0(u)$ is the number of coordinates of u equal to zero, $t_1(u)$ is the number of invertible coordinates of u, $t_2(u)$ is the number of non zero, non invertible coordinates of u. Moreover, in the cases of proposition 3.4, the theta series of the lattice L_C expresses through W_C :

Proposition 4.2. *Let C be a code of length n over A. In the cases of proposition 3.4, we have*

$$\theta_{L_C} = W_C(\theta_0, \theta_1, \theta_2)$$

where

$$\begin{aligned} \theta_0 &= \sum_{x \in p\mathfrak{O}_K} q^{x\overline{x}/p} \\ \theta_1 &= \sum_{x \in 1+p\mathfrak{O}_K} q^{x\overline{x}/p} \\ \theta_2 &= \sum_{x \in \alpha+p\mathfrak{O}_K} q^{x\overline{x}/p}, \text{ where } \alpha \in \mathfrak{O}_K \text{ and } \alpha\overline{\alpha} = p \end{aligned}$$

Proof. The theta series of a lattice L is defined by $\theta_L = \sum_{x \in L} q^{x.x/2}$ where $q = e^{2i\pi z}$. Since $w = l_K$, for each $u \in A$ we can choose $v \in \mathfrak{O}_K$ such that $s_K(v) = u$ and $v\overline{v} = w(u)$. Hence we have :

$$\begin{aligned} \theta_{L_C} &= \sum_{x \in L_C} q^{x.x/2} = \sum_{u \in C} \sum_{x, s_K(x) = u} q^{h(x,x)} \\ &= \sum_{u \in C} \sum_{x \in v + p\mathfrak{O}_K} q^{1/p \sum x_i \overline{x_i}} = \sum_{u \in C} \prod_{i=1}^{n} \Big(\sum_{x \in v_i + p\mathfrak{O}_K} q^{\frac{x_i\overline{x_i}}{p}} \Big). \end{aligned}$$

In the cases of proposition 3.4, it is easy to see that the sum $\sum_{x \in v_i + p\mathfrak{O}_K} q^{\frac{x_i\overline{x_i}}{p}}$ only depends on $w(u_i)$ (see Example 2.3). With the notations of the proposition,

$$\theta_{L_C} = \sum_{u \in C} {\theta_0}^{t_0(u)} {\theta_1}^{t_1(u)} {\theta_2}^{t_2(u)} = W_C(\theta_0, \theta_1, \theta_2).$$

□

We forget about the case (5) which leads to the usual MacWilliams identity in two variables over a finite field ([MWS]). Then we get :

Theorem 4.2. *Let A be one of the algebras defined in proposition 2.1. Let C be a code of length n over A. Then*

$$W_{C^\perp}(X,Y,Z) = \frac{1}{\mathrm{Card}(C)} W_C(M(X,Y,Z))$$

with

(1) *If $A = \mathbb{F}_q + u\mathbb{F}_q$*

$$M = \begin{pmatrix} 1 & q(q-1) & q-1 \\ 1 & 0 & -1 \\ 1 & -q & q-1 \end{pmatrix}.$$

(2) *If $A = \mathcal{M}_2(\mathbb{F}_p)$*

$$M = \begin{pmatrix} 1 & (p^2-1)(p^2-p) & (p^2-1)(p+1) \\ 1 & p & -(p+1) \\ 1 & -p(p-1) & p(p-1)-1 \end{pmatrix}.$$

(3) *If $A = \mathbb{F}_p \times \mathbb{F}_p$*

$$M = \begin{pmatrix} 1 & (p-1)^2 & 2(p-1) \\ 1 & 1 & -2 \\ 1 & -(p-1) & p-2 \end{pmatrix}.$$

Examples 4.3. The weight enumerator polynomial of the codes C_n. The code $C_1 = I$ doesn't contain any invertible element, so

$$W_{C_1}(X,Y,Z) = X + (\sqrt{|A|}-1)Z.$$

We recall that the Hamming weight enumerators of $\mathbf{1}$ and PC over $\mathbb{F}_q$ are $W_{\mathbf{1}}(x,y) = x^n + (q-1)y^n$ and $W_{PC}(x,y) = \frac{1}{q}W_{\mathbf{1}}(x+(q-1)y, x-y) = \frac{1}{q}((x+(q-1)y)^n + (q-1)(x-y)^n)$.

Let $A = \mathbb{F}_q + u\mathbb{F}_q$. We have $C_n = \mathbf{1} + uPC$. The words $x = a + ub$ with $a \neq 0$ give a Y^n in the enumerator polynomial and those with $a = 0$ give $W_{PC}(X,Z)$. We get

$$W_{C_n} = (q-1)q^{n-1}Y^n + \frac{1}{q}((X+(q-1)Z)^n + (q-1)(X-Z)^n).$$

Let $A = \mathbb{F}_p \times \mathbb{F}_p$. Following [MWS], let $J_{A,B}(a,b,c,d)$ denote the joint weight enumerator of two codes A, B. Then, because $C_n = \mathbf{1} \times PC$,

$$\begin{aligned} W_{C_n}(X,Y,Z) =& J_{\mathbf{1},PC}(X,Z,Z,Y) \\ =& \frac{1}{p}((X+(p-1)Z)^n + (p-1)(Z+(p-1)Y)^n) \\ &+ \frac{p-1}{p}((X-Z)^n + (p-1)(Z-Y)^n). \end{aligned}$$

Let $A = \mathcal{M}_2(\mathbb{F}_p)$. Let $x = (x_1, .., x_n)$ be an element of C_n with $x_i = (\begin{smallmatrix} a & b_i \\ c & d_i \end{smallmatrix})$, $\sum b_i = \sum d_i = 0$. If $a = c = 0$, then the coordinates of x are never invertible, and the contribution is $J_{PC,PC}(X, Z, Z, Z)$. If a or c is non zero, all the coordinates are non zero. We fix such a couple (a, b). If we set $\det : C_n \to \mathbb{F}_p^n$, defined by $\det(x) = (ad_i - bc_i)_{1 \le i \le n}$, then the kernel of det is of dimension $n - 1$ and the image is the code PC. The contribution of x is $Y^{wt(\det(x))} Z^{n-wt(\det(x))}$. We get when (a, b) varies $(p^2 - 1)p^{n-1} W_{PC}(Z, Y)$. Finaly

$$\begin{aligned} W_{C_n}(X, Y, Z) =& \frac{1}{p^2}(X + (p^2 - 1)Z)^n + \frac{p^2 - 1}{p^2}(X - Z)^n \\ &+ (p^2 - 1)p^{n-2}((Z + (p - 1)Y)^n + (p - 1)(Z - Y)^n). \end{aligned}$$

We now assume that condition (*) holds for the algebra A. Let C be a self-dual code of length n. Then the weight of any element of C is a multiple of p ; it is also congruent modulo p to $t_1(u)$, which proves that the weight enumerator polynomial W_C is invariant under the matrix

$$P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \zeta_p & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

where ζ_p is a root of unity of order p. One can compute the group G generated by $\frac{1}{\sqrt{|A|}} M$ and P and its Molien series, which leads to the structure of the corresponding algebra of invariants $\mathcal{I}_G$ (for more about invariant theory, see [MWS], [S]). It turns out that it is always a polynomial ring.

The results are summarized in the following proposition.

Theorem 4.4. *Assume A is one of the algebras given in proposition 3.2, but not a field. The weight enumerator polynomial W_C of a self-dual code C of length n is invariant under the group G generated by M and P, which has the following structure and Molien series $\Phi_G(\lambda)$:*

(1) *If $A = \mathbb{F}_2 \times \mathbb{F}_2$ or if $A = \mathcal{M}_2(\mathbb{F}_2)$, G is a dihedral group of order 6 ; its Molien series is $\Phi_G(\lambda) = \frac{1}{(1-\lambda)(1-\lambda^2)(1-\lambda^3)}$. The algebra of invariants is the polynomial ring generated by W_{C_1}, W_{C_2}, W_{C_3}, or equivalently by*

if $A = \mathbb{F}_2 \times \mathbb{F}_2$

$$\begin{cases} P_1 = X + Z \\ P_2 = 2XZ - (Y^2 + Z^2) \\ P_3 = Z(X^2 - Y^2) \end{cases}$$

if $A = \mathcal{M}_2(\mathbb{F}_2)$

$$\begin{cases} P_1 = X + 3Z \\ P_2 = XZ - Y^2 \\ P_3 = Z((X + Z)^2 - 4Y^2) \end{cases}$$

(2) *If $A = \mathbb{F}_q + u\mathbb{F}_q$, G is respectively a dihedral group of order 6 if $q = 2$, a group of order 18 isomorphic to $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ if $q = 3$, a dihedral group of order 8 if $q = 4$; in all cases, the Molien series is $\Phi_G(\lambda) = \frac{1}{(1-\lambda)(1-\lambda^p)(1-\lambda^{2p})}$. The algebra of invariants is the polynomial ring generated by W_{C_1}, W_{C_p}, $W_{C_{2p}}$, or equivalently by*

if $q = 2$

$$\begin{cases} Q_1 = X + Z \\ Q_2 = XZ - Y^2 \\ Q_4 = Y^2(X - Z)^2 \end{cases}$$

if $q = 3$

$$\begin{cases} R_1 = X + 2Z \\ R_3 = 3Y^3 - Z(X^2 + XZ + Z^2) \\ R_6 = Y^3(X - Z)^3 \end{cases}$$

if $q = 4$

$$\begin{cases} S_1 = X + 3Z \\ S_2 = 2Y^2 - Z(X + Z) \\ S_4 = Y^2(X - Z)^2 \end{cases}$$

Proof. The Molien series, which is the generating series of the dimensions of the homogeneous components of $\mathcal{I}_G$ is computed using the formula ([MWS], [S])

$$\Phi_G(\lambda) = \frac{1}{|G|} \sum_{M \in G} \frac{1}{\det(I - \lambda M)}.$$

The polynomials given in the theorem belong to $\mathcal{I}_G$, are algebraically independent, and have the right degree. Hence they generate it, and $\mathcal{I}_G$ is a ring of polynomials.

5. A bound for the minimum weight of self-dual codes

Theorem 4.4 allows us to introduce the notion of an extremal self-dual code, as in the case of codes over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$. A self-dual code over A is said to be extremal if it has the best possible weight, under the constraint that its weight enumerator polynomial should belong to $\mathcal{I}_G$. Let us look at the first case, $A = \mathbb{F}_2 \times \mathbb{F}_2$. The others work the same way. If C is a self-dual code of length n over A, then

$$W_C = \sum_{2a+3b \leq n} \lambda_{a,b} P_1^{n-2a-3b} P_2^a P_3^b.$$

If we set $y' = Y^2/X$ and $z = Z/X$, and develop this expression, we get

$$\sum_{2a+3b\leq n} \lambda_{a,b}(1+z)^{n-2a-3b}(2z-y'-z^2)^a(z(1-y))^b = \sum_{\alpha,\beta\geq 0} \gamma_{\alpha,\beta}{y'}^{\alpha}z^{\beta}.$$

The code contains words of weight $2d$ if and only if one of the $\gamma_{\alpha,\beta}$ with $\alpha+\beta=d$ is non zero. Each $\gamma_{\alpha,\beta}$ is a linear combination of the $\lambda_{a,b}$ with $a+b\leq\alpha+\beta$ and $b\leq\beta$. Moreover, if $a+b=\alpha+\beta=d$, then the terms of weight d come from $\sum_{a+b=d,\, b\leq\beta}\lambda_{a,b}(2z-y')^a z^b$, and the coefficient of $\lambda_{d-\beta,\beta}$ is $(-1)^{d-\beta}$.

Hence the linear system given by the equations $\gamma_{0,0}=1$, $\gamma_{\alpha,\beta}=0$ for all $1\leq\alpha+\beta\leq d$ is triangular in the unknowns $\lambda_{a,b}$ arranged in the lexicographic order of $(a+b,b)$ as long as $a+b\leq d \Rightarrow 2a+3b\leq n$. We can go up to $d=[n/3]$.

An extremal code is a code which enumerator polynomial is a solution of this system. Its weight is at least $2([n/3]+1)$; but its weight enumerator is not uniquely determined in general. In order to prove that the weight of an extremal code is exactly equal to $2([n/3]+1)$, we could go further and add the set of equations $\gamma_{\alpha,\beta}=0$ for all $\alpha+\beta=[n/3]+1$, $\beta\leq n-2[n/3]-2$. Now the solution is unique and we would have to prove that one of its $\gamma_{\alpha,\beta}$ with $\alpha+\beta=[n/3]+1$ is non zero. But the classical expression of such a coefficient using the Lagrange formula involves here series expansions with two variables ; such formulas exist in several variables but are not so nice unless the new variables expansion are diagonal, which is not the case here. In order to avoid such heavy computations, we prefer to go through the theta series of the related lattice L_C, which will allow us to stay in the one-variable case. We closely follow the proof of [MOS2].

Theorem 5.1. *Let C be a self-dual code of length n over A. Then*

(1) *If $A=\mathbb{F}_2\times\mathbb{F}_2$ or $A=\mathcal{M}_2(\mathbb{F}_2)$, $w(C)\leq 2([n/3]+1)$.*
(2) *If $A=\mathbb{F}_3+u\mathbb{F}_3$, $w(C)\leq 3([n/6]+1)$*
(3) *If $A=\mathbb{F}_4+u\mathbb{F}_4$, $w(C)\leq 2([n/4]+1)$*

Proof. We will make use of the results proved in [Q4] on l-modular lattices. Let Λ be such a lattice, and let θ_Λ be its theta series. We assume that $1+l$ divides 24, and set $k_1=24/(1+l)$. Let $\Delta=(\eta(z)\eta(lz))^{k_1}=q(\prod_{n\geq 1}(1-q^n)\prod_{n\geq 1}(1-q^{ln}))^{k_1}$ and let θ be the theta series of a l-modular lattice of lowest dimension. We denote by k_0 the weight of θ, which is respectively 4 if $l=1$, 2 if $l=2$ or $l\equiv 1 \mod 4$, 1 if $l\equiv 3 \mod 4$. Then ([Q4, theorem 7]) θ_Λ belongs to $\mathbb{C}[\Delta,\theta]$ (and an extremal lattice is a lattice having the highest minimum with respect to this property).

Let C be a self-dual code of length n over A. We consider the lattice L_C defined by lifting C to the field K of proposition 3.4. The lattice L_C is then l-modular, with the following values for the parameters k_1, k_0, k, the last one being the weight of θ_{L_C}. Moreover, we set $k/k_1=n/a$, which is the number appearing in the integer part of the bound.

	l	k_1	k_0	k	a
$\mathbb{F}_2 \times \mathbb{F}_2$	7	3	1	n	3
$\mathcal{M}_2(\mathbb{F}_2)$	3	6	1	$2n$	3
$\mathbb{F}_3 + u\mathbb{F}_3$	3	6	1	n	6
$\mathbb{F}_4 + u\mathbb{F}_4$	2	8	2	$2n$	4

We set

$$\theta_{L_C} = \sum_{\mu=0}^{[k/k_1]} a_\mu \theta^{k/k_0 - \mu k_1/k_0} \Delta^\mu = \sum_{r \geq 0} \alpha_r q^r.$$

Each α_r is a linear combination of the a_μ with $\mu \leq r$, and a_r appears with the coefficient 1 because the term of lowest degree of Δ is q and that of θ is 1.

Let $L_0 = (p\mathfrak{O}_K)^n$. It is a sublattice of L_C, preimage of zero by the application s_K defined in §3. Using the fact that $w = l_K$, the minimal weight $w(C)$ of C is the smallest integer such that L_C contains a vector x not belonging to L_0 of norm $x.x = 2w(C)/p$. If we set

$$\theta_{L_0} = \sum_{r \geq 0} \beta_r q^r$$

and

$$\theta_{L_C} = \theta_{L_0} + \sum_{r \geq w(C)/p} \gamma_r q^r$$

the highest weight is obtained if θ_{L_C} is a solution of the linear system ($\alpha_i = \beta_i$ for all $0 \leq i \leq [k/k_1]$). Since it is triangular with ones on the diagonal, this solution is unique, denoted by

$$\theta^* = \sum_{\mu=0}^{[k/k_1]} {a^*}_\mu \theta^{k/k_0 - \mu k_1/k_0} \Delta^\mu = \theta_{L_0} + \sum_{r \geq [k/k_1]+1} {\gamma^*}_r q^r;$$

now

$$w(C) \leq p([k/k_1] + 1) \Leftrightarrow {\gamma^*}_{[k/k_1]+1} \neq 0.$$

If $\phi = \Delta/\theta^{k_1/k_0}$, we have

$$\sum_{\mu=0}^{[k/k_1]} {a^*}_\mu \phi^\mu = \theta^{-k/k_0}\theta_{L_0} + \theta^{-k/k_0} \sum_{r\geq [k/k_1]+1} {\gamma^*}_r q^r$$

which shows that, if we develop $\theta^{-k/k_0}\theta_{L_0}$ in powers of ϕ, and set $\theta^{-k/k_0}\theta_{L_0} = \sum_{s\geq 0} b_s\phi^s$, then

$$\gamma^*_{[k/k_1]+1} = -b_{[k/k_1]+1}.$$

Lagrange formula gives

$$b_s = \frac{1}{s!}\frac{d^{s-1}}{dq^{s-1}}(\frac{d}{dq}(\theta^{-k/k_0}\theta_{L_0})(q/\phi)^s)_{\{q=0\}}.$$

For any ideal $\mathfrak{A}$ of K, we denote by $\theta_{\mathfrak{A}}$ the theta series of the lattice $(\mathfrak{A}, \mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$. Hence $\theta_{\mathfrak{A}} = \sum_{x\in\mathfrak{A}} q^{x\overline{x}}$. Let $\mathfrak{P}$ be a left ideal of K of norm p. It exists in every case since p is either split or ramified in K, and it is principal. We can take the ideal generated by $1+i$ in the quaternionic case, $\sqrt{-3}$ and $(1+\sqrt{-7})/2$ in the others. The lattice $(\mathfrak{P}, \mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$ is isometric to $(p\mathfrak{O}_K, \frac{1}{p}\mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$, so $\theta_{L_0} = \theta_{\mathfrak{P}}^n$. On the other hand, $\theta_{\mathfrak{O}_K} = \theta$ in every case except for $A = \mathcal{M}_2(\mathbb{F}_2)$ where $(\mathfrak{O}_K, \mathrm{Trace}_{K/\mathbb{Q}}(x\overline{y}))$ is the orthogonal sum of two hexagonal lattices and hence $\theta_{\mathfrak{O}_K} = \theta^2$, see remark 3.7. We obtain :

$$\begin{aligned} b_s &= \frac{1}{s!}\frac{d^{s-1}}{dq^{s-1}}(\frac{d}{dq}((\theta_{\mathfrak{O}_K}/\theta_{\mathfrak{P}})^{-n})((q/\Delta){\theta_{\mathfrak{O}_K}}^a)^s)_{\{q=0\}} \\ &= \frac{1}{s!}\frac{d^{s-1}}{dq^{s-1}}(-n({\theta_{\mathfrak{O}_K}}^{as-n-1}\theta_{\mathfrak{P}}^{n-1}(\theta_{\mathfrak{P}}\frac{d\theta_{\mathfrak{O}_K}}{dq} - \theta_{\mathfrak{O}_K}\frac{d\theta_{\mathfrak{P}}}{dq})(q/\Delta)^s)_{\{q=0\}}. \end{aligned}$$

Since q/Δ has strictly positive coefficients, since for $s = [n/a]+1$, $as-n-1 \geq 0$, and since $\theta_{\mathfrak{O}_K}$ has positive coefficients, it is enough to show that $\theta_{\mathfrak{P}}^{n-1}(\theta_{\mathfrak{P}}\frac{d\theta_{\mathfrak{O}_K}}{dq} - \theta_{\mathfrak{O}_K}\frac{d\theta_{\mathfrak{P}}}{dq})$ has positive coefficients up to the index $[n/a]$.

In every case, the quotient $\mathfrak{O}_K/\mathfrak{P}$ has representatives of reduced norm one, so $\theta_{\mathfrak{O}_K} = \theta_{\mathfrak{P}} + (N\mathfrak{P}-1)\theta_{1+\mathfrak{P}}$, where $N\mathfrak{P} = [\mathfrak{O}_K : \mathfrak{P}]$. Now

$$\begin{aligned} \theta_{\mathfrak{P}}^{n-1}(\theta_{\mathfrak{P}}\frac{d\theta_{\mathfrak{O}_K}}{dq} - \theta_{\mathfrak{O}_K}\frac{d\theta_{\mathfrak{P}}}{dq}) &= (N\mathfrak{P}-1)\theta_{\mathfrak{P}}^{n-1}(\theta_{\mathfrak{P}}\frac{d\theta_{1+\mathfrak{P}}}{dq} - \theta_{1+\mathfrak{P}}\frac{d\theta_{\mathfrak{P}}}{dq}) \\ &= (N\mathfrak{P}-1)\theta_{\mathfrak{P}}^{n-1}\sum_{\substack{y\in 1+\mathfrak{P}\\ x\in\mathfrak{P}}}(y\overline{y}-x\overline{x})q^{x\overline{x}+y\overline{y}-1} \\ &= (N\mathfrak{P}-1)\sum_{\substack{y\in 1+\mathfrak{P}\\ x,x_1,..,x_{n-1}\in\mathfrak{P}}}(y\overline{y}-x\overline{x})q^{x\overline{x}+y\overline{y}+x_1\overline{x_1}+..+x_{n-1}\overline{x_{n-1}}-1} \end{aligned}$$

If we fix an integer r and put together the terms for which $x\overline{x}+y\overline{y}+x_1\overline{x_1}+..+x_{n-1}\overline{x_{n-1}} = r$, the coefficient of q^{r-1} is a sum of expressions $ny\overline{y}-(x\overline{x}+x_1\overline{x_1}+..+x_{n-1}\overline{x_{n-1}}) = (n+1)y\overline{y}-r$ which is at least $n+1-r$ since $y\in 1+\mathfrak{P}$ is non zero, and hence positive up to the index n which is more than what is needed. $\square$

Remark 5.2. *The same method should prove, as in the classical cases, that extremal codes do not exist when the dimension goes beyond a certain value by showing that the next coefficient is negative.*

Examples 5.3. From the previous computations, we see that the codes C_n are extremal codes in the split cases for $n = 2, 3, 4, 5$; if $A = \mathbb{F}_3 + u\mathbb{F}_3$ for $n = 3, 6$; if $A = \mathbb{F}_4 + u\mathbb{F}_4$ for $n = 2, 4, 6$. The corresponding lattices L_{C_n} have minimum 4 and are extremal in the following level and dimension : in level $l = 2$, dimension 16 and 24, these are the Barnes-Wall lattice and the lattice named R_{24} in [B] ; in level 3, and dimension 12, this is the Coxeter-Todd lattice, found once over $\mathbb{Z}[\omega]$ (it is the construction of [CS2]) and once over $\mathbb{Q}_{3,\infty}$ (it is the construction of [M1]). We find two more extremal lattices of minimum 4 over $\mathbb{Q}_{3,\infty}$ in dimension 16 and 20. In level 7, we find three such lattices in dimension 6, 8, 10.

6. Constructions of extremal self-dual codes and lattices

In this section, we construct extremal codes over A for small length in the four cases (1)-(4). The problem of the complete classification of these codes of a given length can be solved by hand in small length but is better handled using mass formulas and computer programs. Mass formulas are settled in the case $A = \mathbb{F}_q + u\mathbb{F}_q$ in [G].

Next we study the lattices L_C defined over the maximal orders of the fields of proposition 3.4. For $p = 2$, the minimum of the lattice L_C cannot be better than 4 (proposition 3.6). If C is an extremal code of weight greater than 4, we try to construct a lattice of minimum $w(C)$ as a neighbour of L_C. This is a standard technique in lattice theory going back to Kneser which extends easily to lattices over number fields or quaternion fields (see [B], [SH]). For $p = 3$, L_C is extremal up to minimum 6.

6.1. The case $A = \mathbb{F}_2 \times \mathbb{F}_2$

Let C be a code of length n over A. Let C_1 and C_2 be the two binary codes which are the projections of C on the two components of $\mathbb{F}_2 \times \mathbb{F}_2$. Since C is an A-module, $(1, 0)C \subset C$, and $C = C_1 \times C_2$. Moreover, it is easy to see from the definition of the scalar product that C is self-dual if and only if $C_2 = C_1^\perp$. For example, the codes $C_n = \mathbf{1} \times PC$ provide extremal codes of weight 4 in length 3, 4, 5. We now look for codes of weight 6.

Lemma 6.1. *Let $C = C_1 \times C_1^\perp$ be a self-dual code over $A = \mathbb{F}_2 \times \mathbb{F}_2$. Then*

$$w(C) \geq 6 \Longleftrightarrow \begin{cases} wt(C_1) \geq 3 \\ wt(C_1^\perp) \geq 3 \\ wt(C_1 \cap C_1^\perp) \geq 6 \end{cases}$$

Proof. Let x be an element of C_1. Then $(x, 0)$ is an element of C of weight $2wt(x)$. If x also belongs to $C_1^\perp$, then (x, x) is an element of C of weight $wt(x)$. Hence the conditions of the right hand side of the equivalence are necessary. Conversely, since the weight of (x, y)

is greater than the Hamming weight of each component, and since C is self-dual, the first two conditions imply that $w(C) \geq 4$. As an element of weight 4 can only be of the type (x, x) with $wt(x) = 4$, the last condition suffices to show that $w(C) \geq 6$. $\square$

Theorem 6.2. *There is no extremal code of length 6 and 7 over $A = \mathbb{F}_2 \times \mathbb{F}_2$. There is at least one of length 8 which is $C = C_1 \times C_1^{\perp}$ where C_1 is the binary code of generating matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Its weight enumerator is

$$\begin{aligned} W_C(X,Y,Z) = & X^8 + 8X^3Y^4Z + 4Z^2(2X^4Y^2 + 5X^2Y^4) + 8Z^3(X^5 + 4X^3Y^2 + 2XY^4) \\ & + 2Z^4(5X^4 + 28X^2Y^2 + 2Y^4) + 8Z^5(X^3 + 6XY^2) + 4Z^6(3X^2 + 4Y^2) \\ & + 8XZ^7 + Z^8 \end{aligned}$$

Proof. Let k be the dimension of C_1. Since $C_1^{\perp}$ has weight at least 3, the columns of a matrix of C_1 should be distinct and non zero, hence $k = 3$. If $n = 6$, the columns are all the elements of $\mathbb{F}_2^3 \backslash \{0\}$ except one ; we can extend C_1 to the orthogonal of the Hamming code. If $n = 7$, it is equivalent to it. In both cases, this implies that $C_1 \cap C_1^{\perp}$ contains words of weight 4.

The code of length 8 given in the proposition is the first of a series of quasicyclic codes satisfying lemma 6.1. Let D_{2n} be the code of length $2n$ with generating matrix $[I_n|A]$ where A is the circulant matrix of first line 1100...0. Then it is easy to see that D_{2n} is equivalent to its dual, that its weight is three since any line of its matrix has weight 3 and the sum of two lines has weight 4 or 6 ; moreover, $D_{2n} \cap D_{2n}^{\perp}$ is $\{0\}$ if n is prime to 3 and is of dimension 2 and weight $4n/3$ if 3 divides n. $\square$

Now we look at the lengths 9, 10, where the bound for the weight is 8.

Theorem 6.3. *There is no extremal code of length 9 over $A = \mathbb{F}_2 \times \mathbb{F}_2$. There is at least one of length 10 which is $C = C_1 \times C_1^{\perp}$ where C_1 is the binary double circulant code of generating matrix*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Its weight enumerator is

$$\begin{aligned} W_C(X,Y,Z) = & X^{10} + Y^{10} + 90X^4Y^4Z^2 + 30Z^4(X^6 + 6X^4Y^2 + X^2Y^4 + Y^6) \\ & + 30Z^6(X^4 + 12X^2Y^2 + Y^4) + 45Z^8(X^2 + Y^2) + 2Z^{10}. \end{aligned}$$

Proof. Let C_1 be a code of length 9 such that $C_1 \times C_1^\perp$ has weight 8. Then both C_1 and $C_1^\perp$ have Hamming weight at least 4. Hence we can assume that the dimension of C_1 is 4. If a generating matrix of C_1 has the shape $[I_4|M]$, then the columns of M should be of weight 3 or 4 otherwise $C_1^\perp$ would contain a word of weight 3. Up to equivalence, the only possibility is to take all of them, but $C_1^\perp$ still contains words of weight 3 since the all-one column decomposes as the sum of a column of weight one and a column of weight 3.

The binary code given in the proposition is a $[10, 5, 4]$ double circulant code (see [MWS, table 16.7). It is equivalent to its dual and its intersection with its dual is the code **1**. It is easy to check that $C_1 \times C_1^\perp$ has weight 8. □

The norm of a modular lattice of level 7 and dimension m is bounded by $2([m/6] + 1)$. While up to dimension 10 a lattice reaching this bound exists (see example 5.3), it is shown in [SH] that there is no lattice of minimum 6 and dimension 12 by a complete exploration of the genus. A lattice of level 7, dimension 20, minimum 8 connected to the Mathieu group M_{22} is known from [A], [NP] ; we rediscover it here as a neighbour of the lattice L_C constructed from the code of proposition 6.3 (it is clearly the same lattice from the generators given in [A]).

More precisely, let $K = \mathbb{Q}(\sqrt{-7})$. We set $\alpha = (1 + \sqrt{-7})/2$ and have $\mathfrak{O}_K = \mathbb{Z}[\alpha]$. This element generates one of the two ideals of K above 2 ; we set $\mathfrak{p} = \mathfrak{O}_K\alpha$. Since the all one word belongs to C, the vector $e = (1, 1, .., 1)$ belongs to L_C. Let $L_C^e = \{y \in L_C \text{ s.t. } h(y, x) \in \mathfrak{p}\}$ and let

$$\Lambda = L_C^e + \mathfrak{O}_K \frac{\alpha^2}{2} e.$$

Theorem 6.4. *The lattice Λ has minimum 8.*

Proof. From proposition 3.6 and 6.3, the elements of L_C have norm at least 8 apart from the norm 4 elements equal to $(2, 0, 0, .., 0)$ up to a permutation of the coordinates and a sign. These elements don't belong to L_C^e ; hence the minimum of L_C^e is 8. The hermitian dual of L_C^e is $(L_C^e)^* = L_C + \mathfrak{O}_K \frac{\alpha}{2} e$; since $\mathrm{Norm}_{K/\mathbb{Q}}(z + \alpha/2) \geq 1/2$ for all $z \in \mathfrak{O}_K$, we have $x.x \geq 5$ for all $x \in (L_C^e)^*$. Let us show that this lattice doesn't contain any vector of norm 6. Such a vector would indeed have either eight coordinates of norm 1/2 and two of norm 1, or nine coordinates of norm 1/2 and one of norm 3/2. But it is easy to check that, if z belongs to $\mathfrak{O}_K$, then $\mathrm{Norm}_{K/\mathbb{Q}}(z + \alpha/2) = 1/2$ if and only if $z = 0, -\alpha$, $\mathrm{Norm}_{K/\mathbb{Q}}(z + \alpha/2) = 1$ if and only if $z = -1, 1 - \alpha$ and that $\mathrm{Norm}_{K/\mathbb{Q}}(z + \alpha/2) = 3/2$ is impossible. Since the code C has weight 4, a vector of L_C cannot have eight coordinates congruent to 0 modulo $\mathfrak{p}$ and two coordinates congruent to 1 modulo $\mathfrak{p}$.

Since Λ is $\mathfrak{O}_K$-unimodular, it is even and contained in $(L_C^e)^*$, and hence has minimum 8.

□

No extremal level 7 lattice is known in dimensions 14 and 18 ; in dimension 16, such a lattice exists and can be constructed from the real quadratic field $\mathbb{Q}(\sqrt{2})$ ([S]), but no hermitian construction is known for it. The lattice L_C constructed from the extremal code of proposition 6.2 has no 2-neighbour of minimum 6, since any sublattice of the form L_C^e contains vectors of norm 4.

6.2. The case $A = \mathcal{M}_2(\mathbb{F}_2)$

Codes over $\mathcal{M}_2(\mathbb{F}_2)$ reduce to codes over $\mathbb{F}_4$ in the following way : Let us call ω an element of $\mathcal{M}_2(\mathbb{F}_2)$ of characteristic polynomial x^2+x+1, for example $\omega = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ an element of order 2 satisfying $i\omega = \overline{\omega} i$. Then $\mathbb{F}_2[\omega] \simeq \mathbb{F}_4$ and $\mathcal{M}_2(\mathbb{F}_2) = \mathbb{F}_2[\omega] + \mathbb{F}_2[\omega]i$. Let us call ϕ the induced isomorphism of $\mathbb{F}_4$ left vector spaces $\phi : \mathbb{F}_4 \times \mathbb{F}_4 \to \mathcal{M}_2(\mathbb{F}_2)$. The non invertible elements of $\mathcal{M}_2(\mathbb{F}_2)$ correspond through ϕ to the pairs (a,b) with a and b non zero. Hence ϕ preserves the weight, if $\mathbb{F}_4 \times \mathbb{F}_4$ is endowed with the Hamming weight wt. We extend ϕ to n-tuples ; if C is a code of length n over $\mathcal{M}_2(\mathbb{F}_2)$, then $\phi(C)$ is a code of length $2n$ over $\mathbb{F}_4$.

Lemma 6.5. *The map ϕ induces a bijection between the set of codes of length n over $\mathcal{M}_2(\mathbb{F}_2)$ and the set of couples (C_1, σ) where C_1 is a code of length $2n$ over $\mathbb{F}_4$ and σ is a permutation of the $2n$ coordinates which is a product of n disjoint transpositions satisfying $\sigma(C_1) = \overline{C_1}$. Self-dual codes over $\mathcal{M}_2(\mathbb{F}_2)$ correspond to self-dual codes over $\mathbb{F}_4$ (for the form $\sum x_i \overline{y_i}$). Moreover we have $w(C) = wt(\phi(C))$.*

Proof. If a, b belong to $\mathbb{F}_2[\omega]$ then $i(a+bi) = \overline{b} + \overline{a} i$. The left multiplication by i induces the permutation σ of the $2n$ coordinates with the prescribed properties. The reciprocal is evident.

From $(a+bi)\overline{(a'+b'i)} = a\overline{a}' + b\overline{b}' + (ab' + ba')i$, we see that $C \subset C^\perp$ implies $\phi(C) \subset \phi(C)^\perp$. Reciprocally, if $\phi(C) = C_1$, since $\sigma(C_1) = \overline{C_1}$, we have both $C_1.C_1 = 0$ and $C_1.\overline{\sigma(C_1)} = 0$. □

Different choices of the permutation σ associated to a code over $\mathbb{F}_4$ may provide non equivalent codes over $\mathcal{M}_2(\mathbb{F}_2)$, unless they are conjugate by an element of the permutation group of the code.

Self-dual codes over $\mathbb{F}_4$ are classified up to length 16 in [CPS]. The smallest length where a weight 6 code exists is length 14 (there is no extremal code of length 12, as well as there is no extremal $\mathbb{Z}[\omega]$-unimodular lattice in dimension 24 by Feit's classification [F]), and it is an extended quadratic residue code.

This family of codes provides self-dual codes over $\mathcal{M}_2(\mathbb{F}_2)$. If l is a prime, $l \equiv 5 \mod 8$ and $\mathcal{Q}_{l+1}$ is the extended quadratic residue code over $\mathbb{F}_4$, then it is preserved by the group $PSl_2(\mathbb{F}_l)$ acting on the projective line identified with the $l+1$ coordinates, while the elements of $PGl_2(\mathbb{F}_l)$ of non square determinant exchange $\mathcal{Q}_{l+1}$ and $\overline{\mathcal{Q}_{l+1}}$ ([AM]). Such an element has order two if and only if its characteristic polynomial has the form $T^2 - a$, $a \notin (\mathbb{F}_l^*)^2$, and has no eigenvector. Hence it induces a permutation which is a product of

$(l+1)/2$ disjoint transpositions. Moreover, two such elements of $PGl_2(\mathbb{F}_l)$ are conjugate by an element of $PSl_2(\mathbb{F}_l)$. The first examples are the codes $\mathcal{Q}_6$, $\mathcal{Q}_{14}$, $\mathcal{Q}_{30}$ which provide extremal codes of weight 4, 6, 12.

An extremal code over A of length 8 is provided by the $\mathbb{F}_4$-code number 52 of [CPS] of minimal weight 6 where the existence of the permutation σ is noticed in [CPS, §E]. We denote this $\mathbb{F}_4$-code by C_{16}. It is tempting to try the code S_{18} of [MOS1] in length 9, but a computer search has shown the non existence of the permutation σ.

Now we study the corresponding lattices over the quaternion field ramified at 3 and ∞ over $\mathbb{Q}$. We keep the notations of proposition 3.4 and fix the maximal order $\mathfrak{O}_K = \mathbb{Z}[\omega] + i\mathbb{Z}[\omega]$ where $\omega = (-1+j)/2$. The three left ideals above 2 are $\mathfrak{p} = \mathfrak{O}_K(1+i)$, $\mathfrak{p}\omega$, $\mathfrak{p}\omega^2$.

Theorem 6.6. *The lattice L_C constructed from the quaternary code $\mathcal{Q}_6$ is the Coxeter-Todd lattice, while the lattices L_C constructed from the quaternary codes $\mathcal{Q}_{14}$ and C_{16} have neighbours of minimum 6 which are $\mathfrak{O}_K$-unimodular lattices and hence extremal lattices of level 3 and dimension respectively 28 and 32.*

Proof. Since $L_{\mathcal{Q}_6}$ is a $\mathfrak{O}_K$-unimodular lattice of minimum 4, it is the Coxeter-Todd lattice (it is easy to see that the neighbouring graph over $\mathfrak{O}_K$ has only two vertices. See [B] for an analogous argument over the Hurwitz order).

The codes $\mathcal{Q}_{14}$ and C_{16} contain the all-one word which lifts to the vector $e = (1+i, .., 1+i)$ of L_C. We set

$$L_C^{\omega e} = \{y \in L_C \text{ s.t. } h(y, \omega e) \in \mathfrak{p}\}.$$

The only elements of norm 4 of L_C are, up to a permutation of the coordinates and the multiplication by a unit of $\mathfrak{O}_K$, equal to $y = (2, 0, .., 0)$. Since $h(y, \omega e) = (1-i)\overline{\omega} \notin \mathfrak{p}$, this lattice has minimum 6. If $\alpha = \frac{(1+i)\omega(1+i)}{2}$, its hermitian dual is

$$(L_C^{\omega e})^* = \{y \in K^n \text{ s.t. } h(y, L_C^{\omega e}) \in \mathfrak{O}_K\} = L_C + \mathfrak{O}_K(\alpha, .., \alpha).$$

The lattice L_C has two neighbours over $\mathfrak{O}_K$ containing $L_C^{\omega e}$ which are both contained in its dual. We look at the vectors of norm 4 of $L_C + \mathfrak{O}_K(\alpha, .., \alpha)$. If such a vector is not in L_C, then, up to the multiplication by a unit, we can assume that it has the form $Z = y + (\alpha, .., \alpha)$ with $y \in L_C$. If $\mathrm{Norm}_{K/\mathbb{Q}}$ is the norm of K, it is easy to see that, for $x \in \mathfrak{O}_K$, $\mathrm{Norm}_{K/\mathbb{Q}}(\alpha - x)$ belongs to $\mathbb{N}/2$, is equal to $1/2$ if and only if $x = \omega, -\overline{\omega}$, and is equal to 1 if and only if $x = 0, -i, 1+2\omega, 1-i+2\omega, -\overline{\omega}i, -\omega i, -\overline{\omega}i+1+2\omega, -\omega i+1+2\omega$; we notice that all these elements are distinct modulo 2.

In the case of dimension 32, the rank over K is 8 and we have $Z.Z \geq 8/2 = 4$, with equality if and only if the coordinates of y are $-\omega$ or $\overline{\omega}$. The image of y modulo 2 is then a word of weight 8 of C_{16} with zeros at the coordinates of even index. Since this code has weight 6, two words of weight 8 with the same support are proportional. Hence Z is unique up to a unit and at least one of the neighbours of L_C has minimum 6.

In the case of dimension 7, $Z.Z = 4$ if and only if six of the seven coordinates of y is at distance $1/2$ from α and the remaining one is at distance 1. Again the image of y modulo 2 is a word of weight 6 or 8 which is uniquely determined by the code $\mathcal{Q}_{14}$. Modulo the units, we get 7 vectors of norm 4 which are congruent modulo $L_C^{\omega e}$ and hence belong to the same neighbour. $\square$

6.3. The case $A = \mathbb{F}_q + u\mathbb{F}_q$, $q = 3, 4$

As described in [B], [G], a code C of length n over $\mathbb{F}_q + u\mathbb{F}_q$ is a triple (C_1, C_2, f) where C_1 and C_2 are codes of length n over $\mathbb{F}_q$ such that $C_1 \subset C_2$ and $f : C_1 \to \mathbb{F}_q^n/C_2$ is a morphism satisfying $C = \{x + uy | x \in C_1 \text{ and } y \in f(x)\}$. C_1 is the image of C modulo u and C_2 is given by the elements of C annihilated by u. Moreover, C is self-dual if and only if $C_2 = C_1^\perp$ and f is symmetric (relatively to the form $\sum x_i\overline{y_i}$ over $\mathbb{F}_q$, where $\overline{x} = x$ if $q = 3$ and $\overline{x} = x^2$ if $q = 4$).

Since $uC_2 \subset C$, if wt is the Hamming weight over $\mathbb{F}_q$ and p the characteristic of A, the weight of C satisfies

$$\min(wt(C_1), p\,wt(C_2)) \leq w(C) \leq p\,wt(C_2)$$

and a suitable choice of f can make $w(C)$ become strictly greater than $wt(C_1)$, as in [B]. The case $f = 0$ is the code $C = C_1 + uC_2$; for example the codes C_n previously defined are of this form.

Theorem 6.7.

Extremal self-dual codes exist over $A = \mathbb{F}_3 + u\mathbb{F}_3$ in length $n = 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 16, 17$. The corresponding lattice L_C is an extremal 3-modular lattice of dimension $2n$. There is no extremal code in length 7 and 12.

Extremal self-dual codes exist over $A = \mathbb{F}_4 + u\mathbb{F}_4$ in length $n \leq 12$. The corresponding lattice L_C is an extremal 2-modular lattice of dimension $4n$ if $n \leq 7$; if $8 \leq n \leq 12$, there exists an extremal 2-modular lattice Λ deduced from L_C by at most two successive neighbourings.

Proof. We start with $p = 3$. Extremal codes have weight 6 in length 6 to 11. The code $C = \mathbf{1} + uPC$ provides such a code in length 6 and 9. In length 8, 10, 11, it is easy to find a code $C_1 \subset C_1^\perp$ of dimension 2 and weight 6 such that $C_1^\perp$ has weight 2. We can take respectively

$$C_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 & 0 & 1 & 2 & 1 \end{pmatrix}.$$

$$C_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}.$$

$$C_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 2 & 1 & 2 & 1 & 1 \end{pmatrix}.$$

Let us show that there is no extremal code in length 7. Since 7 is odd, the dimension of C_1 is at least 2, and C_1 contains at least one word x of weight 3. Let us show that C_1 contains necessarily another word of weight 3 disjoint from x. Let $\sup(x)$ be the support of the word x and let p_x be the projection on the complementary set of $\sup(x)$:

$p_x(y) = (y_i)_{i \notin \sup(x)}$. We need a morphism f such that, for all $y \in f(x)$, $x+uy$ has weight at least 6, which means that $p_x(y)$ is non zero modulo $p_x(C_1^\perp)$, if we go back to the definition of w. Hence we need $p_x(C_1^\perp) \neq \mathbb{F}_3^4$. But, the dual of $p_x(C_1^\perp)$ being the set of words of C_1 disjoint from x, it is either $\{0\}$ or $\mathbb{F}_3 x'$ if C_1 contains a word x' of weight 3 disjoint from x. Since the subcode $\mathbb{F}_3 x + \mathbb{F}_3 x'$ has one zero coordinate, the dimension of C_1 is at least 3 ; up to equivalence C_1 is generated by

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

But, for the four words of weight 3 generated by the first two lines, $p_x(C_1^\perp)$ is of codimension 1, defined by $x_5 + x_6 + x_7 = 0$, so, since f needs to be a morphism, any choice of f will leave words of weight 3 in the $\mathbb{F}_3 + u\mathbb{F}_3$ code.

We know from Feit's classification [F] that there is no code of weight 9 over A in length 12, otherwise the lattice L_C would be $Z[\omega]$-unimodular of minimum 6 and dimension 24. In [N1], G. Nebe has constructed a 3-modular lattice of minimum 6 in this dimension, which turns to be a non integral $\mathbb{Z}[\omega]$-lattice. We will construct here extremal codes of weight 9 in length $n = 13, 14, 16, 17$. The corresponding lattices L_C are $\mathbb{Z}[\omega]$-unimodular and extremal of level 3 and minimum 6.

In order to guess the code C_1, we proceed has follows. If the Hamming weight enumerators of C_1 and $C_2 = C_1^\perp$ are : $W_{C_1}(X) = A_0 + A_3X^3 + A_6X^6 + .. + A_{3[n/3]}X^{3[n/3]}$ and $W_{C_2}(X) = B_0 + B_1X + B_2X^2 + .. + B_nX^n$, the linear conditions $S = (B_0 = 1, B_1 = B_2 = 0)$ lead through the MacWilliams identity ([MWS]) to three linear conditions on the A_{3i}. Hence we can add to S the extra conditions $A_0 = 1, A_3 = .. = A_{3([n/3]-3)}$ which has now a unique solution W depending on the dimension k of C_1. For each length n we take the lowest value of k for which the coefficients of W are positive and integral and try to construct a code C_1 having such a weight enumerator. We find :

* $n = 13$, $k = 4$, $W = 1 + 26X^9$. We recognize the weight enumerator of the dual of the Hamming code H_3 of length $(3^3-1)/(3-1) = 13$. Since its minimal weight is 9, the code $C = H_3^\perp + uH_3$ has weight 9. This construction was first communicated to me by H.-G. Quebbemann.

* $n = 14$, $k = 4$, $W = 1 + 4X^6 + 60X^9 + 16X^{12}$. The unknown code C_1 has modulo ± 1 two words of weight 6. We will then need a non trivial morphism f. The same discussion as in length 7 about $p_x(C_1^\perp)$ shows that this implies that the two words of weight 6 have disjoint supports. Then it is not difficult to show that, up to equivalence, the only code of weight enumerator W with, modulo ± 1, two words of weight 6 with disjoint supports is :

$$C_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 \\ 0 & 1 & 1 & 2 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Reciprocally, since $p_{x_1}(C_1^\perp)$ is the parity-check code, the symmetric morphism defined by $f(1^6 0^8) = 0^6 1 0^7$, $f(0^6 1^6 0^2) = 1 0^{13}$, and zero on the last two lines, is such that $(C_1, C_1^\perp, f)$ is a code of weight 9 over A.

* $n = 15$, $k = 4$, $W = 1 + 50X^9 + 30X^{12}$. Here the method doesn't work since one can show that W is not the weight enumerator of a code.
* $n = 16$, $k = 4$, $W = 1 + 32X^9 + 48X^{12}$. We easily construct a code of weight enumerator W using the tetracode of generating matrix

$$T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

We can take

$$C_1 = \begin{pmatrix} T & T & T & 0 \\ 0 & T & 2T & T \end{pmatrix}.$$

Since the minimal weight of C_1 is 9, the code $C_1 + uC_1^\perp$ has minimum weight 9.
* $n = 17$, $k = 4$, $W = 1 + 18X^9 + 58X^{12} + 4X^{15}$. This code was obtained by shortening an extended Reed-Solomon code of length 9 over $\mathbb{F}_9$. Its weight enumerator is equal to W.

$$C_1 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 2 & 2 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 2 & 1 & 1 & 0 & 1 & 1 & 0 & 2 & 1 & 2 & 2 & 0 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 & 1 & 0 & 2 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 2 \end{pmatrix}.$$

Since the minimal weight of C_1 is 9, the code $C_1 + uC_1^\perp$ has minimum weight 9.

Now we consider the case of $q = 4$. An extremal code over $\mathbb{F}_4 + u\mathbb{F}_4$ has weight 4 up to $n = 7$. If n is even, $C = \mathbf{1} + uPC$ is convenient. For $n = 5$ and 7, we can take respectively

$$C_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & \omega & \overline{\omega} & 1 \end{pmatrix}.$$

and the dual of the Hamming code with parameters $[7, 3, 4]$; then $C = C_1 + uC_1^\perp$ has weight 4.

When the length n is greater than 7, we proceed as in characteristic 3 in order to guess the weight enumerator W of C_1. We find
* $n = 8$, $k = 3$, $W = 1 + 6X^4 + 48X^6 + 9X^8$. A code C of weight 6 with C_1 having a weight enumerator equal to W and the related 2-modular (although not integral over the Hurwitz order) extremal lattice are constructed in [B].
* $n = 9$, $k = 3$, $W = 1 + 36X^6 + 27X^8$. We can take

$$C_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & \omega & \omega & 0 & \overline{\omega} & \overline{\omega} \\ 1 & 0 & 1 & \overline{\omega} & 0 & \overline{\omega} & \omega & 0 & \omega \end{pmatrix}.$$

The code $C = C_1 + uC_1^\perp$ has weight 6. The lattice L_C over the Hurwitz order has vectors of norm 4 which are, up to a permutation of the coordinates and the multiplication by a unit, equal to $(2, 0, 0, .., 0)$. Moreover, since the length is odd, any vector of L_C has at least one coordinate in $\mathfrak{P} = \mathfrak{O}_K(1 + i)$ the ideal above 2 in the Hurwitz quaternions. Hence any sublattice of L_C of index $\mathfrak{P}$ contains vectors of norm 4. We construct a lattice Λ such that $L_C/L_C\cap\Lambda$ is isomorphic to $\mathfrak{O}_K/\mathfrak{P}\times\mathfrak{O}_K/\mathfrak{P}$, or equivalently as the preimage of a self-dual code over $\mathfrak{O}_K/4\mathfrak{O}_K$, connected to the sequence of codes $C_0\subset C_1\subset C_1^\perp\subset C_0^\perp$ where C_0 is the subcode of C_1 generated by the first two lines. Since this lattice is the result of a computer search, we simply give a set of generators. If we call e_1, e_2, e_3, the lines of C_1 given above, $\sqrt{2}\Lambda$ is generated modulo 4 by $f_1=e_1+(0,0,0,0,0,0,u^2\overline{w},u^3\overline{\omega},u^3\omega)$, $f_2=e_2+(0,0,0,0,0,0,0,u^3\overline{\omega},u^2+u^3\omega)$, ue_3, $u^2C_1^\perp$ and $u^3C_0^\perp$. It is $\mathfrak{O}_K$-unimodular and has minimum 6 ; this last statement was verified using PARI. The lattice $\sqrt{2}\Lambda\cap\sqrt{2}L_C$ is generated modulo 4 by uf_1, uf_2, ue_3, $u^2C_1^\perp$ and $u^3C_0^\perp$.

* $n=10$, $k=3$, $W=1+15X^6+45X^8+3X^{10}$. We can take

$$C_1=\begin{pmatrix}1&1&1&1&1&1&1&1&1&1\\0&1&\omega&\overline{\omega}&0&0&1&\omega&\overline{\omega}&0\\0&1&\overline{\omega}&\omega&1&\omega&0&0&0&\overline{\omega}\end{pmatrix}.$$

The code $C=C_1+uC_1^\perp$ has weight 6. Since the all-one word belongs to C_1, the lattice L_C contains $e=(1,1,..,1)$. The sublattice L_C^e has minimum 6 and its hermitian dual is $L_C+\mathfrak{P}^{-1}e$. Since $\min_{x\in\mathfrak{O}_K}\mathrm{Norm}_{K/\mathbb{Q}}((1+i)/2-x)=1/2$, any vector z belonging to $L_C+\mathfrak{P}^{-1}e$ but not to L_C satisfies $z.z\geq 10/2=5$; hence a neighbour of L_C containing L_C^e is of minimum 6.

* $n=11$, $k=3$, $W=1+3X^6+45X^8+15X^{10}$. We can take

$$C_1=\begin{pmatrix}1&1&1&1&1&1&1&1&0&0&0\\0&0&0&1&1&1&\omega&\overline{\omega}&1&1&1\\0&1&\omega&0&1&\omega&0&0&0&1&\omega\end{pmatrix}.$$

The code $C=C_1+uC_1^\perp$ has weight 6. We proceed as in length 9 to construct Λ, using the subcode generated by the two first lines e_1 and e_2 of C_1. One can take the lattice Λ generated by $e_1+(0,0,-2,0,-2,0,0,0,0,0,u^3)$, $e_2+(0,0,0,0,0,0,0,u^3,0,-2,-2)$, ue_3, $u^2C_1^\perp$ and $u^3C_0^\perp$.

* $n=12$, $k=4$, $W=1+6X^6+135X^8+90X^{10}+24X^{12}$. If we denote by e_6 a generating matrix of the hexacode,

$$e_6=\begin{pmatrix}1&0&0&1&\omega&\omega\\0&1&0&\omega&1&\omega\\0&0&1&\omega&\omega&1\end{pmatrix}.$$

we can take for C_1

$$C_1=\begin{pmatrix}e_6&e_6\\1\dots1&0\dots0\end{pmatrix}.$$

Since this code has, modulo units, two words of weight 6 with disjoint supports, the morphism f defined by $f(1^60^6)=10^510^5$ and $f(x|x)=0$ for all $x\in e_6$ is symmetric and the code defined by $(C_1,C_1^\perp,f)$ has weight 8. We can construct a lattice Λ of minimum 8 of the form $L_C^e+\mathfrak{P}^{-1}y$ which is 2-modular ; but a more elegant construction, communicated to me by H.-G. Quebbemann, is the following : take the Leech lattice L with its structure over the Hurwitz order (see [Q1]), and take $\Lambda = \{(x,y) \in L \times L \text{ s.t. } x \equiv y \mod \mathfrak{P}L\}$. Then Λ is $\mathfrak{O}_K$-unimodular of minimum 8. The explicit construction of the Leech lattice over the Hurwitz order, which makes use of the e_6 code, shows that Λ and L_C share a sublattice of index $\mathfrak{P}^2$. $\square$

Remarks 6.8. The method developped in the previous proof fails to give an extremal code over $\mathbb{F}_3 + u\mathbb{F}_3$ in length 18 since one can show that any code $(C_1, C_1^{\perp}, f)$ such that the weight enumerator polynomial of C_1 equals the candidate W has weight at most 9.

We have constructed an extremal lattice of level 3 in all dimensions $26 \leq 2n \leq 34$, except the dimension 30 ; such a lattice exists and is constructed in [N2, theorem 9.1].

Bibliography

[**AM**] E.F. Assmus,H.F. Mattson, *New 5-designs*, J. Comb. Theory **6** (1969), 122-151.

[**A**] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[**B**] C. Bachoc, *Voisinages au sens de Kneser pour les réseaux quaternioniens*, Comm. Math. Helvet. **70** (1995), 350–374.

[**BQS**] C. Batut, H-G. Quebbemann, R. Scharlau, *Computations of cyclotomic lattices.*, Exp. Math., à paraître.

[**CPS**] J.H. Conway, V. Pless, N.J.A. Sloane, *Self-dual codes over GF(3) and GF(4) of length not exceeding 16*, IEEE Trans. Inf. Th. 3 **IT-25** (1979), 312-322.

[**CS1**] J.H. Conway N.J.A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Heidelberg, 1988.

[**CS2**] J.H. Conway, N.J.A. Sloane, *The Coxeter-Todd lattice, the Mitchell group, and related sphere packings*, Math. Proc. Cambridge Phil. Soc. **93** (1983), 421–440.

[**CS3**] J.H. Conway, N.J.A. Sloane, *Self-dual codes over the integers modulo 4*, J. Comb. Th. **Series A 62** (1993), 30-45.

[**D**] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements.

[**F**] W. Feit, *Some lattices over* $\mathbb{Q}(\sqrt{-3})$, J. Algebra **52** (1978), 248–263.

[**G**] P. Gaborit, *Mass formula for self-dual codes over* $\mathbb{Z}_4$ *and* $\mathbb{F}_q + u\mathbb{F}_q$ *rings*, to appear.

[**MOS1**] F.J. MacWilliams, A.M. Odlysko, N.J.A. Sloane, *Self-dual codes over* $\mathbb{F}_4$, J. Comb. Th. A **25** (1978), 288-318.

[**MOS2**] C.L. Mallows A.M. Odlysko N.J.A. Sloane, *Upper bounds for modular forms, lattices and codes*, J. Algebra **36** (1975), 68-76.

[**MWS**] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical library, 1977.

[**Mar1**] J. Martinet, *Structures algébriques sur les réseaux*, Number Theory, S. David éd. (Séminaire de Théorie des Nombres de Paris, 1992-93), Cambridge University Press, Cambridge, 1995, pp. 167–186.

[**M2**] J. Martinet, *Les réseaux parfaits des espaces euclidiens (livre en préparation).*

[**N1**] G. Nebe, *Endliche rationale Matrixgruppen vom Grad* 24, *Aachener Beiträge zur Mathematik*, Verlag der Augustinus Buchhandlung, 1995.

[**N2**] G. Nebe, *Finite subgroups of* $Gl_n(\mathbb{Q})$ *for* $25 \leq n \leq 31$., Communications of Algebra, à paraître.

[**NP**] G. Nebe, W. Plesken, *Finite rational matrix groups*, *Memoirs A.M.S.*, vol. 116(556), 1995.

[**Q1**] H.-G. Quebbemann, *An application of Siegel's formula over quaternion orders*, Mathematika **31** (1984), 12–16.

[**Q2**] H.-G. Quebbemann, *A construction of integral lattices*, Mathematika **31** (1984), 138–141.

[**Q3**] H.-G. Quebbemann, *Lattices with theta-functions for* $G(\sqrt{2})$ *and linear codes*, J. Algebra **105** (1987), 443–450.

[**Q4**] H.-G. Quebbemann, *Modular Lattices in Euclidean Spaces*, J. Number Theory **54** (1995), 190-202.

[**S**] N.J.A. Sloane, *Error-correcting codes and invariant theory : New applications of a nineteenth century technique*, Amer. Math. Monthly **84** (1977), 82-107.

[**SH**] R. Scharlau, B. Hemkemeier, *Classification of integral lattices with large class number*, to appear.

[**V**] M.-F. Vigneras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800** (1980), Springer-Verlag.

Laboratoire d'Algorithmique Arithmétique 351, cours de la Libération F-33405 Talence