

CHRISTINE BACHOC

PHILIPPE GABORIT

On extremal additive \mathbb{F}_4 codes of length 10 to 18

Journal de Théorie des Nombres de Bordeaux, tome 12, n° 2 (2000),
p. 255-271

http://www.numdam.org/item?id=JTNB_2000__12_2_255_0

© Université Bordeaux 1, 2000, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

On extremal additive \mathbb{F}_4 codes of length 10 to 18

par CHRISTINE BACHOC et PHILIPPE GABORIT

*À Jacques Martinet,
Grâce à qui les empilements déferlent,
Les kissing numbers montent,
Et qui nous donna le nom de décodeurs.
Merci.*

RÉSUMÉ. Dans cet article nous considérons les codes \mathbb{F}_4 -additifs autoduaux pairs et extrémaux. Nous en donnons une classification complète en longueur 10. Avec l'hypothèse qu'au moins deux mots de poids minimal ont le même support, nous classifions les codes de longueur 14, et montrons en longueur 18 qu'un tel code est équivalent à l'unique code \mathbb{F}_4 -linéaire hermitien autodual de paramètres $[18, 9, 8]$.

ABSTRACT. In this paper we consider the extremal even self-dual \mathbb{F}_4 -additive codes. We give a complete classification for length 10. Under the hypothesis that at least two minimal words have the same support, we classify the codes of length 14 and we show that in length 18 such a code is equivalent to the unique \mathbb{F}_4 -hermitian code with parameters $[18, 9, 8]$. We construct with the help of them some extremal 3-modular lattices.

1. Introduction

An additive code C over \mathbb{F}_4 of length n is an additive subgroup of \mathbb{F}_4^n . We will denote by C an $(n, 2^k)$ additive code of length n with 2^k codewords. Additive codes over \mathbb{F}_4 were introduced in [4] as a way to describe a certain subclass of quantum codes. Such codes can also be used to construct modular of level 3 lattices, as it will be discussed in Section 5.

Let $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$ where $\bar{\omega} = \omega^2 = 1 + \omega$. The trace map $Tr : \mathbb{F}_4 \rightarrow \mathbb{F}_2$ is defined by

$$Tr(x) = x + x^2.$$

The space \mathbb{F}_4^n is endowed with the *trace inner product* defined for two vectors $\mathbf{x} = x_1x_2 \cdots x_n$ and $\mathbf{y} = y_1y_2 \cdots y_n$ in \mathbb{F}_4^n by:

$$\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^n \text{Tr}(x_i \overline{y_i}).$$

If C is an additive code, its *dual* C^\perp is defined by $C^\perp = \{\mathbf{x} \in \mathbb{F}_4^n \mid \mathbf{x} \cdot \mathbf{c} = 0\}$. If C is an $(n, 2^k)$ code, then C^\perp is an $(n, 2^{2n-k})$ code. As usual, an additive code C is *self-orthogonal* if $C \subseteq C^\perp$ and *self-dual* if $C = C^\perp$. In particular, a Hermitian self-dual \mathbb{F}_4 -linear code is also self-dual for the trace inner product, when considered as an additive code.

The *weight* $wt(\mathbf{c})$ of $\mathbf{c} \in C$ is the usual Hamming weight over \mathbb{F}_4 which counts the number of nonzero components of \mathbf{c} and the minimal weight d of C is the smallest weight of any nonzero codeword in C . We shall often make use of the following identity linking the weight and the trace inner product:

$$\text{For all } u, v \in \mathbb{F}_4^n, u \cdot v = wt(u + v) - wt(u) - wt(v) \pmod 2$$

(meaning that the weight modulo 2 is a quadratic form on \mathbb{F}_4^n viewed as a binary space with associated symplectic form $u \cdot v$.)

Two additive codes C_1 and C_2 are *equivalent* provided there is a map from $S_3^n \times S_n$ sending C_1 onto C_2 , with S_n the permutation group of the n coordinates and S_3 the permutation group on the elements $\{1, \omega, \overline{\omega}\}$. The *automorphism group* of C , denoted $\text{Aut}(C)$, consists of all the elements of $S_3^n \times S_n$ which stabilize C .

An additive self-dual code is *Type II* if all its codewords have even weight and *Type I* else. Type II codes are known to exist only in even lengths. A bound on the minimal weight of an additive self-dual code was given by Rains in [12, Theorem 33]. If we let d_I or d_{II} be the minimal distance of an additive self-dual Type I or Type II code, then:

$$(1) \quad d_I \leq \begin{cases} 2 \lfloor \frac{n}{6} \rfloor + 1 & \text{if } n \equiv 0 \pmod 6 \\ 2 \lfloor \frac{n}{6} \rfloor + 3 & \text{if } n \equiv 5 \pmod 6 \\ 2 \lfloor \frac{n}{6} \rfloor + 2 & \text{otherwise} \end{cases}$$

$$(2) \quad d_{II} \leq 2 \lfloor \frac{n}{6} \rfloor + 2.$$

A code that meets the appropriate bound is called *extremal*. Type II codes meeting the bound d_{II} have a uniquely determined weight enumerator.

The classification of self-dual additive codes was done by Hohn in [7] up to length 7 for Type I-II codes and up to length 8 for Type II codes. In [6], Gaborit, Kim, Huffman and Pless pushed the classification of extremal Type I codes to the lengths 8, 9 and 11. They also gave a written proof

of the uniqueness of the extremal Type II code of length 12, the so called dodecacode.

The computation of the mass of Type II codes (see [7]) shows that the number of classes of such codes is greater than 1.72 times 10^6 for length 14, greater than 1.02 times 10^{10} for length 16 and greater than 8.9 times 10^{16} for length 18, so that a complete classification is unrealistic.

In this paper we only consider extremal Type II codes and we extend the classification to length 10, for which we find 19 inequivalent extremal codes. Under the restrictive hypothesis $s(C) > 0$ that we shall explain in Section 2, we find 490 inequivalent extremal codes for length 14 and only one extremal code for length 18, the unique \mathbb{F}_4 -linear hermitian [18,9,8] code. We did not consider length 16 since the number of extremal Type II codes will be even larger than for length 14. Section 2 explains the method we used, Sections 3 and 4 list the numerical results we obtained, eventually we give in the Appendix the complete list of the 19 extremal Type II codes of length 10 and also 5 particular codes of length 14. Section 5 examines the lattices constructed from these codes. All the computations were done with the Magma system [3].

2. The method

In this section, C denotes an extremal, Type II code of length n and minimal weight d . Let u be a codeword of weight d . Let $S = S(u)$ denote the support of u . Two cases arise: either u is the only word in C with support S , or exactly three words in C have S as support. In this last case, we can assume up to equivalence that these three words are $1^d 0^{n-d}$, $\omega^d 0^{n-d}$, $\bar{\omega}^d 0^{n-d}$. (This is clear from the following observations: If the code C contains another element v with the same support as u , then the nonzero coordinates of u and v are pairwise different otherwise $u + v$ would be of weight strictly lower than d . And $u + v$ itself is also a weight d codeword with the same support as u and v .) It is worth noticing that, if C is equivalent to a linear code, then the first case never happens since wu and w^2u provide codewords with the same support as u . Hence the following invariant of C measures how far the code is to be linear:

$$(3) \quad s(C) := \text{card} \left\{ S \subset \{1 \dots n\} \mid |S| = d \right. \\ \left. \text{and } \text{card}\{u : u \in C \mid S(u) = S\} > 1 \right\}.$$

We shall see later that it is much more difficult to classify the codes with $s(C) = 0$. Note that, when the code C is \mathbb{F}_4 linear, $s(C) = \frac{1}{3} \text{card}\{x \in C \mid wt(x) = d\}$.

Again, let $u \in C$ be a minimal word. Let

$$(4) \quad C_0(u) := \{v : v \in C \mid S(v) \cap S(u) = \emptyset\}.$$

This is a subcode of C . The classification of the possible $C_0(u)$ for the lengths under consideration will be discussed in next section. We can then describe a general form for a generating matrix of an extremal code.

Lemma 2.1. *The extremal code C has, up to equivalence, a generating matrix of the form:*

1. If $s(C) = 0$

$$\begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \hline & & 0 & & & C_0 \\ \hline 1 & & & 0 & & \\ & \ddots & & \vdots & & s_1 \\ & & 1 & 0 & & \\ \hline \omega & & & \omega & & \\ & \ddots & & \vdots & & s_2 \\ & & \omega & \omega & & \end{bmatrix}$$

where C_0 is an additive code of length $n - d$ and dimension $n - 2d + 1$.

Here s_i denote matrices of size $(d - 1) \times (n - d)$.

2. If $s(C) > 0$

$$\begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \omega & \dots & \omega & 0 & \dots & 0 \\ \hline & & 0 & & & C_0 \\ \hline 0 & 1 & & 1 & & \\ \vdots & & \ddots & \vdots & & s_1 \\ 0 & & 1 & 1 & & \\ \hline 0 & \omega & & \omega & & \\ \vdots & & \ddots & \vdots & & s_2 \\ 0 & & & \omega & \omega & \end{bmatrix}$$

where C_0 is an additive code of length $n - d$ and dimension $n - 2d + 2$.

Here s_i denote matrices of size $(d - 2) \times (n - d)$.

Proof. See [6].

□

In order to enumerate the extremal codes, we have then to fulfil two steps: The first step is the enumeration of the possibilities for the subcode C_0 . It is an additive code with parameters $(n - d, 2^{n-2d+1}, d)$ if $s(C) = 0$, or $(n - d, 2^{n-2d+2}, d)$ if $s(C) > 0$. This is left to next section, where we shall make use of the fact that in some cases ($n = 14, 18$ and $s(C) > 0$), its weight enumerator can be computed. The Second step is to run over

the possibilities for (s_1, s_2) . Therefore, we discuss some properties of these matrices.

Let $V := C_0^\perp/C_0$. This \mathbb{F}_2 -vector space is endowed with a weight w_V defined by

$$(5) \quad w_V(x) := \min\{wt(u) : u \in x\}$$

and with a non degenerate binary quadratic form q_V

$$(6) \quad q_V(x) := w_V(x) \pmod{2}.$$

We denote by b_V the associated symplectic form, which is nothing else than the bilinear form induced by the inner product on C_0 . Note that the isomorphism class of the symplectic space (V, b_V) and of the quadratic space (V, q_V) are determined by $\dim(V)$ since the quadratic space has index $\dim(V)/2$ as will be proved in Lemma 2.2. Clearly, the rows of the matrices s_i are defined modulo C_0 and belong to C_0^\perp since C is assumed to be self-dual. For $i = 1, 2$, we denote by S_i the subspace of V spanned by the rows of s_i . These rows are specific vectors of S_i and must satisfy certain weight conditions, so that the whole row of the generating matrix has weight at least d . Hence we take the following notations: a set $\{e_1, \dots, e_s\} \subset V$ is said to satisfy condition (C1), respectively (C2), (C3) if

$$(C1) \quad \text{For all } 1 \leq k \leq s/2, \quad \begin{cases} w_V(\sum_{2k-1} e_i) \geq \max(d - 2k, 2k) \\ w_V(\sum_{2k} e_i) \geq \max(d - 2k, 2k) \end{cases}$$

$$(C2) \quad \text{For all } 1 \leq k \leq s, \quad w_V(\sum_k e_i) \geq \max(d - k, k)$$

$$(C3) \quad \text{For all } 1 \leq k \leq s/2, \quad \begin{cases} w_V(\sum_{2k-1} e_i) \geq d - 2k \\ w_V(\sum_{2k} e_i) \geq d - 2k \end{cases}$$

where $\sum_k e_i$ means any sum over k distinct indices i .

We denote by I the unit matrix and by J the matrix

$$(7) \quad J = \begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & \dots & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \dots & 1 & 0 & 1 \\ 1 & \dots & 1 & 1 & 0 \end{pmatrix}.$$

Lemma 2.2. • *If $s(C) = 0$ and for a generating matrix as in 1. of Lemma 2.1, the quadratic space V has dimension $2(d - 1)$, the subspace S_2 is maximal and totally isotropic for q_V , while S_1 is maximal and totally isotropic for b_V . Moreover, $S_1 \cap S_2 = \{0\}$, S_1 has*

a basis $b_1 = (e_1, \dots, e_{d-1})$ satisfying (C2) and S_2 has a unique basis $b_2 = (f_1, \dots, f_{d-1})$ such that $(b_V(e_i, f_j))_{i,j} = I$, and both b_2 and $(e_1 + f_1, \dots, e_{d-1} + f_{d-1})$ satisfy (C3).

- If $s(C) > 0$ and for a generating matrix as in 2. of lemma 2.1, the quadratic space V has dimension $2(d-2)$ and the subspaces S_i are maximal and totally isotropic for q_V . Moreover, $S_1 \cap S_2 = \{0\}$ and one can find in S_1 a basis $b_1 = (e_1, \dots, e_{d-2})$ such that S_2 has a unique basis $b_2 = (f_1, \dots, f_{d-2})$ with $(b_V(e_i, f_j))_{i,j} = J$, and b_1, b_2 and $(e_1 + f_1, \dots, e_{d-2} + f_{d-2})$ satisfy (C1).

Proof. We assume $s(C) > 0$ and we consider a generating matrix as in 2. of lemma 2.1. The dimension of the quadratic space V follows from the dimension of C_0 . If the sum of some rows of s_i was zero, it would give rise to a word in C with support strictly contained in $\{1, \dots, d\}$ which would contradict the hypothesis. So $\dim(S_i) = d-2$. Clearly the rows of s_i are pairwise orthogonal for b_V and isotropic for q_V , so the S_i are maximal totally isotropic subspaces of V . In the same way, a sum of some of the rows of s_1 or s_2 cannot be 0, which means that $S_1 \cap S_2 = \{0\}$.

The conditions satisfied by $w_V(\sum_k e_i)$ follow easily from the fact that d is the minimal weight of C . The computation of $b_V(e_i, f_j)$ where e_i are the rows of s_1 and f_i are the rows of s_2 follows from the form of the generating matrix. The basis $(e_1 + f_1, \dots, e_{d-2} + f_{d-2})$ corresponds to the subcode with matrix

$$\begin{bmatrix} 0 & \bar{w} & & \bar{w} & e_1 + f_1 \\ \vdots & & \ddots & \vdots & \vdots \\ 0 & & & \bar{w} & \bar{w} & e_{d-2} + f_{d-2} \end{bmatrix}$$

and hence has the same properties as the other two.

The arguments in the case $s(C) = 0$ are similar. \square

Let us assume that $s(C) > 0$. The method that we have followed to classify the extremal codes goes through the following algorithmic steps:

Step 1: List the possible C_0 . There are few possibilities in each case; see next section for the explicit list of possibilities for $n = 10, 14, 18$.

Step 2: Fix C_0 . List the maximal totally isotropic subspaces in V . This can be easily done by applying the orthogonal group of the quadratic form to a specific one, as long as the number of such spaces is not too large. Compute the orbits of this set under the action of $\text{Aut}(C_0)$.

Step 3: List the subset \mathcal{S}_1 of the representatives of these orbits which contain at least one basis satisfying (C1). For all $S_1 \in \mathcal{S}_1$, list the set $B(S_1)$ of the basis of S_1 satisfying (C1). Therefore, we make use of the joint action of the symmetric group on the first d coordinates and of the stabilizer of S_1 in $\text{Aut}(C_0)$ on the set of ordered basis of S_1 .

$\dim(V)$	orthogonal geometry of index $\dim(V)/2$	symplectic geometry
6	30	135
8	270	2295
10	4590	75735
12	151470	4922775
14	9845550	635037975

TABLE 1. The number of totally isotropic spaces

Step 4: For each $S_1 \in \mathcal{S}_1$, compute the set $\mathcal{S}_2 = \{S_2 \mid S_2 \cap S_1 = \{0\}\}$ where S_2 is maximal totally isotropic for q_V . For each basis $(e_1, \dots, e_{d-2}) \in B(S_1)$, compute the unique basis (f_1, \dots, f_{d-2}) of S_2 such that $(b_V(e_i, f_j))_{i,j} = J$. Test if (f_1, \dots, f_{d-2}) and $(e_1 + f_1, \dots, e_{d-2} + f_{d-2})$ satisfy (C1). If so, store the matrix

$$\begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \\ \omega & \dots & \omega & 0 & \dots & 0 \\ \hline & 0 & & & C_0 & \\ \hline 0 & 1 & & 1 & & e_1 \\ \vdots & & \ddots & \vdots & & \vdots \\ 0 & & & 1 & 1 & e_{d-2} \\ \hline 0 & \omega & & \omega & & f_1 \\ \vdots & & \ddots & \vdots & & \vdots \\ 0 & & & \omega & \omega & f_{d-2} \end{bmatrix}.$$

Step 5: Test equivalence between the codes with generating matrices stored in Step 4.

In the case when $s(C) = 0$, the modifications are :

Step 2: Note that, the dimension of V is increased by 2. Moreover, we need to list the larger set of maximal totally isotropic subspaces for b_V .

Step 3: Replace condition (C1) by (C2).

Step 4: Replace J by I and condition (C1) by (C3).

Remark 2.3. One of the limits of the method is that it requires the exhaustive list of all the maximal totally isotropic subspaces of V for respectively the quadratic form or the symplectic form. We give in Table 1 their number as a function of $\dim(V)$; it explains why we have limited our search to the case $s(C) > 0$ for $n = 18$.

3. The subcode C_0

In this section, we discuss the classification of the subcode C_0 . We first assume that $C_0 = C_0(u)$ where u is a minimal weight word in C of the second type, i.e. such that its support $S(u)$ is shared by two other codewords. Then, C_0 has parameters $(n-d, 2^{n-2d+2}, d)$. In the case $n = 18$, the weight enumerator of C_0 has the form $W_{C_0} = x^{10} + (15-k)x^2y^8 + ky^{10}$; applying MacWilliams transform to it shows that $k = 0$. In the case $n = 14$, the same argument shows that $W_{C_0} = x^8 + (15-k)x^2y^6 + ky^8$ with $k = 1, 3$. The computations on the harmonic weight enumerators of C worked out in [1] show that $k = 3$ is the only possibility. In the case $n = 10$, we have again $W_{C_0} = x^6 + (15-k)x^2y^4 + ky^6$ with $k = 0, 2, 4, 6$. When $s(C) = 0$, there is no support of minimal weight word shared by two other codewords. We then consider a code C_0 of the first type with parameters $(n-d, 2^{n-2d+1}, d)$. Both cases have to be considered to complete the classification.

Proposition 3.1. • *Let C_0 be an even $(6, 2^4)$ quaternary additive code with minimal weight 4. Then C_0 is equivalent to one of the seven following codes:*

$$\begin{bmatrix} 1 & 1 & 0 & 0 & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & 0 & 0 & 1 & \bar{\omega} & 1 \\ 0 & \bar{\omega} & \bar{\omega} & \omega & 0 & \omega \\ 0 & 0 & 1 & 1 & \omega & \omega \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & \omega & 0 & \bar{\omega} & 0 & \bar{\omega} \\ 0 & 0 & 1 & 1 & \omega & \omega \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & 0 & \bar{\omega} & 1 & 1 & 0 \\ 0 & \bar{\omega} & 0 & \omega & \omega & \bar{\omega} \\ 0 & 0 & 1 & 1 & \omega & \omega \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & 1 & 0 & 1 & 0 & \omega \\ 0 & 0 & 1 & 1 & \omega & \omega \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & \bar{\omega} & 1 & \omega \\ 0 & 1 & 0 & \bar{\omega} & \omega & 1 \\ 0 & 0 & 1 & 1 & \omega & \omega \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & 0 & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & \bar{\omega} & 0 & 0 & \omega & \omega \\ 0 & 0 & 1 & 1 & \omega & \omega \\ 0 & 0 & \bar{\omega} & \bar{\omega} & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ \omega & \omega & \omega & \omega & 0 & 0 \\ 0 & 1 & \omega & \bar{\omega} & 1 & 0 \\ 0 & \omega & \bar{\omega} & 1 & \omega & 0 \end{bmatrix}.$$

The automorphism groups of these codes are of order 12, 96, 72, 16, 64, 288, 2160 respectively, and the last two are the only ones which are equivalent to \mathbb{F}_4 -linear codes.

- Let C_0 be an even $(6, 2^3)$ quaternary additive code with minimal weight 4. Then C_0 is equivalent to one of the seven following codes:

$$\begin{bmatrix} 1 & \bar{\omega} & 1 & 0 & 0 & \bar{\omega} \\ \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 0 & \omega & 0 & 1 & 1 & \omega \end{bmatrix}, \begin{bmatrix} 1 & \bar{\omega} & 1 & 0 & 0 & \omega \\ 0 & \omega & 0 & 1 & 1 & \bar{\omega} \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ \bar{\omega} & \omega & 1 & \omega & \omega & 1 \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 & \bar{\omega} & \bar{\omega} & 0 \\ 0 & 0 & 1 & \omega & \omega & 1 \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 0 & 0 & \omega & \bar{\omega} & 1 \\ 0 & 1 & 1 & \bar{\omega} & \omega & 0 \\ 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & \omega & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ \omega & \omega & \omega & \omega & 0 & 0 \\ 0 & 1 & \omega & \bar{\omega} & 1 & 0 \end{bmatrix}.$$

The automorphism groups of these codes are of order 48, 24, 192, 128, 32, 768, 288 respectively, and since these codes have 2^3 codewords, they are not \mathbb{F}_4 -linear.

Proof. The codes were obtained by exhaustive search. □

Proposition 3.2. • Let C_0 be an even quaternary additive code with weight enumerator $W_{C_0} = x^8 + 12x^2y^6 + 3y^8$. Then C_0 is equivalent to one of the following five codes:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega & \omega & \omega & \omega & \omega & \omega & \omega \\ 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} & 0 & 0 \\ \omega & \omega & 0 & 0 & \bar{\omega} & \bar{\omega} & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega & \omega & \omega & \omega & \omega & \omega & \omega \\ 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} & 0 & 0 \\ \bar{\omega} & \omega & 0 & \omega & 0 & \bar{\omega} & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \omega & \omega & \omega & \omega & \omega & \omega & \omega & \omega \\ 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} & 0 & 0 \\ 0 & \bar{\omega} & \omega & 1 & 0 & \bar{\omega} & \omega & 1 \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega & \omega & \omega & \omega \\ \omega & \omega & 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} \\ \bar{\omega} & 0 & 1 & \bar{\omega} & \omega & 1 & \omega & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega & \omega & \omega & \omega & \omega & \omega \\ \omega & \omega & 1 & 1 & \omega & \omega & \bar{\omega} & \bar{\omega} \\ 1 & \bar{\omega} & \omega & 0 & 0 & 1 & \bar{\omega} & \bar{\omega} \end{bmatrix}$$

The automorphism groups of these codes are of order 1152, 72, 48, 4, 24 respectively, and the first one is the only one which is equivalent to a \mathbb{F}_4 -linear one.

• Let C_0 be an even quaternary additive code with weight enumerator $W_{C_0} = x^{10} + 15x^2y^8$. Then C_0 is equivalent to one of the following five codes:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ \omega & \omega & \omega & \omega & \omega & \omega & \omega & \omega & 0 & 0 \\ \omega & \omega & \bar{\omega} & \bar{\omega} & 0 & 0 & 1 & 1 & 1 & \omega \\ \bar{\omega} & \bar{\omega} & 1 & 1 & 0 & 0 & \omega & \omega & \omega & \bar{\omega} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & \omega & \omega & \omega & \omega & 0 & 0 & 1 & 1 \\ \omega & \omega & 1 & \omega & \bar{\omega} & \bar{\omega} & 0 & \omega & 0 & \omega \\ 1 & 0 & 1 & \bar{\omega} & 0 & \omega & \omega & \omega & \omega & \bar{\omega} \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & \omega & \omega & \omega & \omega & 0 & 0 & 1 & 1 \\ \omega & \omega & 1 & \omega & \bar{\omega} & \bar{\omega} & 0 & \omega & 0 & \omega \\ 0 & \omega & 0 & \omega & 1 & \omega & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} \end{bmatrix},$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & \omega & \omega & \omega & \omega & 0 & 0 & 1 & 1 \\ \omega & \omega & 1 & \omega & \bar{\omega} & \bar{\omega} & 0 & \omega & 0 & \omega \\ 0 & 0 & \omega & \omega & 1 & 1 & \omega & \bar{\omega} & \bar{\omega} & \omega \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & \omega & \omega & \omega & \omega & 0 & 0 & 1 & 1 \\ \omega & \omega & 1 & \omega & \bar{\omega} & \bar{\omega} & 0 & \omega & 0 & \omega \\ \bar{\omega} & 1 & \bar{\omega} & \omega & 0 & 0 & \bar{\omega} & 1 & \bar{\omega} & \omega \end{bmatrix}$$

The automorphism groups of these codes are of order 11520, 24, 120, 288, 96 respectively. The first one is the only one which is equivalent to a \mathbb{F}_4 -linear one.

Proof. The codes were obtained by exhaustive search. □

Remark 3.3. It is worth noticing that the last four codes of length 10 that appear in previous proposition are not linear and not equivalent to constant weight codes. Hence Bonisoli result [2] on constant weight codes over fields does not extend to quaternary additive codes.

4. Numerical results

4.1. Length 10. Here $d = 4$ and the extremal even self-dual codes have weight enumerator

$$(8) \quad W_C(x, y) = x^{10} + 30x^6y^4 + 300x^4y^6 + 585x^2y^8 + 108y^{10}.$$

Applying the algorithm described in Section 2, for the two possible types of C_0 , we obtain:

Proposition 4.1. *There are exactly 19 non equivalent even self-dual, extremal quaternary additive codes C of length 10.*

Two of these codes (QC_{10r} and QC_{10s}) are linear and were already classified as \mathbb{F}_4 linear self-dual hermitian codes in [9] and five non-linear codes (QC_{10a}, b, c, d, e) were found in [6], the 12 others are new. Table 2 lists the 19 codes with their automorphism group orders and the value of $s(C)$. The generator matrices of the codes are listed in the appendix.

Code	n	d	$ \text{Aut}(C) $	$s(C)$
QC_{10a}	10	4	48	0
QC_{10b}	10	4	32	0
QC_{10c}	10	4	1440	0
QC_{10d}	10	4	256	2
QC_{10e}	10	4	18	0
QC_{10f}	10	4	48	1
QC_{10g}	10	4	48	1
QC_{10h}	10	4	144	1
QC_{10i}	10	4	64	2
QC_{10j}	10	4	20	0
QC_{10k}	10	4	720	0
QC_{10l}	10	4	16	0
QC_{10m}	10	4	768	2
QC_{10n}	10	4	320	0
QC_{10o}	10	4	12	0
QC_{10p}	10	4	1152	4
QC_{10q}	10	4	240	0
QC_{10r}	10	4	11520	10
QC_{10s}	10	4	43200	10

TABLE 2. Extremal Type II codes of length 10

4.2. Length 14. Here $d = 6$ and the extremal even self-dual codes have weight enumerator

$$(9) \quad W_C(x, y) = x^{14} + 273x^8y^6 + 2457x^6y^8 + 7098x^4y^{10} + 6006x^2y^{12} + 549y^{14}.$$

card $Aut(C)$	1	2	3	4	6	8	12	18	24	28	36	48	84	6552
C	273	133	10	25	17	9	5	1	12	1	1	1	1	1

TABLE 3. The number of codes C of length 14 with card $Aut(C) = k$

$s(C)$	1	2	3	4	5	6	7	8	9	10	11	12	14	15	17	21	91
C	274	115	42	18	21	4	2	3	3	1	1	1	1	1	1	1	1

TABLE 4. The number of codes C of length 14 with $s(C) = k$

Applying the algorithm described in Section 2, we obtain:

Proposition 4.2. *There are exactly 490 non-equivalent even self-dual, extremal quaternary additive codes C of length 14 with $s(C) > 0$.*

Only one of them is equivalent to a \mathbb{F}_4 -linear one, as was previously known from [9]. It has an automorphism group of order 6552.

Because of the huge number of codes found in this case, we have not explored the other case $s(C) = 0$, although it should be possible to do it (see Table 1).

We give in Table 3 the number of codes found with the corresponding number of automorphisms, and in Table 4 the number of codes found with the corresponding value for the invariant $s(C)$. Matrices for the five new codes which are characterized by the number of their automorphisms (respectively 18, 28, 36, 48, 84) are given in the Appendix. The others can be found at <http://www.math.u-bordeaux.fr/~bachoc>.

4.3. Length 18. Here $d = 8$ and the extremal even self-dual codes have weight enumerator

$$(10) \quad W_C(x, y) = x^{18} + 2754x^{10}y^8 + 18360x^8y^{10} + 77112x^6y^{12} + 110160x^4y^{14} + 50949x^2y^{16} + 2808y^{18}.$$

There is up to equivalence only one extremal \mathbb{F}_4 -linear Hermitian code ([8]), denoted by S_{18} . Our search seems to indicate that it is also unique as a quaternary additive code, but we could not handle the case $s(C) = 0$ because of the huge number of totally isotropic spaces in dimension 14 (see Table 1).

Applying the algorithm described in Section 2, we obtain:

Proposition 4.3. *Up to equivalence, the code S_{18} is the unique even self-dual, extremal quaternary additive code C of length 18 with $s(C) > 0$.*

5. From codes to lattices

In this section, we discuss the lattices that can be constructed from the codes previously studied. Let A_2 denote as usual the 2-dimensional hexagonal lattice. The quadratic space $(A_2/2A_2, q)$ where $q(x) := (x.x)/2$ and $x.x$ denotes the inner product of the underlying Euclidean space, is clearly isomorphic to $(\mathbb{F}_4, Tr(x\bar{y}))$. Hence the \mathbb{F}_4 -additive codes of length n can be lifted into A_2^n ; this construction is usually called ‘‘Construction A’’ from [5]. The lattice A_2 is modular of level 3 in the sense of [11], which means that there exists $\sigma : A_2 \rightarrow A_2^*$ a similarity of rate $1/\sqrt{3}$ between A_2 and its dual. Hence, even self-dual codes give rise to $2n$ -dimensional lattices which are also modular of level 3. We explicit this construction in the next proposition. We again denote by $\sigma : A_2^n \rightarrow (A_2^*)^n$ the map $(x_1, \dots, x_n) \mapsto (\sigma(x_1), \dots, \sigma(x_n))$.

Proposition 5.1. *Let C be a \mathbb{F}_4 -additive code of length n , with $C \subset C^\perp$ and C even. Let L_C be the lattice defined by*

$$(11) \quad L_C := \{(x_1, \dots, x_n) \in A_2^n \mid (x_1, \dots, x_n) \pmod{2A_2} \in C\}.$$

Then, $(L_C, 1/2 \sum_{i=1}^n x_i.y_i)$ is an even lattice of dimension $2n$. Its dual lattice is $(L_C)^ = \sigma(L_{C^\perp})$. In particular, if C is a self-dual code, then L_C is modular of level 3. As a consequence, its determinant is equal to 3^n . Its minimum is given by*

$$(12) \quad \min(L_C) = \min(4, wt(C)).$$

Proof. The formula $(L_C)^* = \sigma(L_{C^\perp})$ is clear from the fact that the inner product on \mathbb{F}_4 is the one induced by the scalar product on A_2 . The computation of the minimum of the lattice follows from the two observations: $\min((2A_2)^n, 1/2 \sum_{i=1}^n x_i.y_i) = 4$ and, if u denotes the image of (x_1, \dots, x_n) in $A_2/2A_2$ identified with \mathbb{F}_4 , $\min((x_1, \dots, x_n) + (2A_2)^n, 1/2 \sum_{i=1}^n x_i.y_i) = wt(u)$. This last property follows from the fact that the roots of A_2 , i.e. the vectors x with $x.x = 2$ are representatives of the non zero classes of A_2 modulo $2A_2$. □

The study of the theta series of modular lattices of level 3 leads in [11] to the definition of extremal lattices. These are the lattices meeting the bound

$$(13) \quad \min(L) \leq 2[\dim(L)/12] + 2.$$

See [13] for a survey on the notion of extremal lattices. From Proposition 5.1, the lattices L_C are extremal only up to dimension 20 (i.e. length 10 for the codes). For higher dimensions, it is usual to proceed to Kneser

neighborings to get rid of the norm 4 vectors arising from the sublattice $((2A_2)^n, 1/2 \sum_{i=1}^n x_i.y_i)$. Clearly two neighborings are necessary to do so; however, this procedure fails to produce an extremal lattice from the dodecacode of length 12. Nevertheless, it is known that such a lattice exists since a 24-dimensional lattice, extremal and modular of level 3 is constructed in [10] from matrix groups. The genus of modular lattices of level 3 is completely classified up to dimension 16. Computations in the Magma system allow us to prove the following:

Proposition 5.2. *The 19 extremal type II codes of length 10 give rise to 19 non isometric 20-dimensional extremal modular lattices of level 3.*

Proof. Direct verification. Among these lattices, 13 are generated by their minimal vectors, for one of them the minimal vectors span a sublattice of index 2 and for other five, the index is 4. The automorphism groups have non-equal orders, except for the lattices obtained from the codes QC_{10f} and QC_{10g} . The two codes have an automorphism group of order 48 and the two lattices have an automorphism group of order $2^{14}.3^2$ but are not isometric. \square

Appendix

- The 19 extremal Type II codes of length 10.

$$QC_{10a} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \bar{\omega} & 1 & 0 & 0 & \bar{\omega} \\ 0 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & \omega \\ 1 & 0 & 0 & 0 & 0 & \bar{\omega} & 1 & \omega & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & \bar{\omega} & 1 & 0 & \omega & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & \omega & \bar{\omega} \\ \omega & 0 & 0 & \omega & 0 & 0 & 0 & \bar{\omega} & 0 & \bar{\omega} \\ 0 & \omega & 0 & \omega & 0 & \bar{\omega} & \bar{\omega} & 1 & 0 & 1 \\ 0 & 0 & \omega & \omega & 0 & 0 & \bar{\omega} & 1 & \bar{\omega} & 1 \end{bmatrix}, QC_{10b} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \bar{\omega} & 1 & 0 & 0 & \bar{\omega} \\ 0 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 0 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & \omega \\ 1 & 0 & 0 & 0 & 0 & 0 & \omega & 0 & \bar{\omega} & 1 \\ 0 & 1 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} & 1 & \bar{\omega} & \omega \\ 0 & 0 & 1 & 0 & 0 & 0 & \bar{\omega} & 0 & \omega & 1 \\ \omega & 0 & 0 & \omega & 0 & \bar{\omega} & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 0 & \omega & 0 & \omega & 0 & \bar{\omega} & 0 & \bar{\omega} & 0 & 0 \\ 0 & 0 & \omega & \omega & 0 & \bar{\omega} & 0 & 0 & \bar{\omega} & 0 \end{bmatrix}$$

$$QC_{10c} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \bar{\omega} & \omega & 1 & \omega & \omega & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ \omega & 0 & 0 & \omega & 0 & \bar{\omega} & 0 & 0 & \bar{\omega} & 0 \\ 0 & \omega & 0 & \omega & 0 & \bar{\omega} & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 0 & 0 & \omega & \omega & 0 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} \end{bmatrix}, QC_{10d} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & \bar{\omega} & \omega & 1 & \omega & \omega & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \bar{\omega} & \bar{\omega} & \bar{\omega} & \bar{\omega} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & \omega & 1 & \bar{\omega} \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & \omega & \bar{\omega} \\ 0 & 0 & 1 & 0 & 0 & \bar{\omega} & 1 & 1 & 1 & \omega \\ \omega & 0 & 0 & \omega & 0 & 1 & 0 & \bar{\omega} & \omega & 1 \\ 0 & \omega & 0 & \omega & 0 & 1 & 0 & \omega & \bar{\omega} & 1 \\ 0 & 0 & \omega & \omega & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

References

- [1] C. BACHOC, *Harmonic weight enumerators of nonbinary codes and MacWilliams identities*. Preprint (1999).
- [2] A. BONISOLI, *Every equidistant linear code is a sequence of dual hamming codes*. *Ars Comb.* **18** (1983), 181–186.
- [3] W. BOSMA, J. CANNON, *Handbook of Magma functions*. Sydney (1995).
- [4] A.R. CALDERBANK, E.M. RAINS, P.W. SHOR, N.J.A. SLOANE, *Quantum error correction via codes over $GF(4)$* . *IEEE Trans. Inform. Theory* **IT-44** (1998), 1369–1387.
- [5] J. CONWAY, N.J.A. SLOANE, *Sphere packings, Lattices and Groups*. Springer-Verlag (1988).
- [6] P. GABORIT, W. C. HUFFMAN, J.-L. KIM, V. PLESS, *On the classification of extremal additive codes over $GF(4)$* . to appear in: Proceedings of the 37th Allerton Conference on Communication, Control, and Computing (1999), UIUC.
- [7] G. HÖHN, *Self-dual codes over the Kleinian four group*. Preprint (1996).
- [8] W.C. HUFFMAN, *On extremal self-dual quaternary codes of lengths 18 to 28*. *IEEE Trans. Inform. Theory* **36** (1990), 651–660.
- [9] F.J. MACWILLIAMS, A.M. ODLYZKO, N.J.A. SLOANE, H.N. WARD, *Self-Dual Codes over $GF(4)$* . *J. Comb. Theory* **25** (1978), 288–318.
- [10] G. NEBE, *Finite subgroups of $GL(24, \mathbb{Q})$* . *Exp. Math.* **5** (1996), 2341–2397.
- [11] H.-G. QUEBBEMANN, *Modular Lattices in Euclidean Spaces*. *J. Number Theory* **54** (1995), 190–202.
- [12] E.M. RAINS, N.J.A. SLOANE, *Self-dual codes*. In: *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, 1998, pp. 177–294.
- [13] R. SCHARLAU, R. SCHULZE-PILLOT, *Extremal Lattices*, *Algorithmic Algebra and Number Theory* (Heidelberg 1997), 139–170, Springer, Berlin, 1999.

Christine BACHOC
A2X, Université Bordeaux I
351, cours de la Libération
33405 Talence cedex
France
E-mail : bachoc@math.u-bordeaux.fr

Philippe GABORIT
LACO, Université de Limoges
87000 Limoges
France
E-mail : gaborit@unilim.edu