Extremal lattices of minimum 8 related to the Mathieu group M_{22}.

Christine Bachoc [*] Gabriele Nebe [†]

dedicated to Martin Kneser

Abstract

In this paper, we construct three new extremal lattices of minimum 8; one is 3-modular and of dimension 40, the two others are unimodular of dimension 80. They are strongly connected to the 20-dimensional lattice with automorphism group isomorphic to $2.M_{22}.2$.

1 Introduction

An even, unimodular lattice can only exist in dimensions n which are multiples of 8, and one knows, from the modular properties of its theta series, that its minimum is bounded by $2([n/24]+1)$ (see [CoS 88]). A lattice attaining this bound is said to be extremal. Extremal lattices are known up to dimension 64; the most wanted would be a 72-dimensional lattice of minimum 8, which is not yet proved to exist. In this paper, we construct two extremal lattices in dimension 80. One of them belongs to a series of three lattices of minimum 8, in dimension 20, 40, 80, which are modular of level 7, 3, respectively 1.

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

[†]supported by the DFG

1991 Mathematics Subject Classification: 11H31, 11H56, 94B05

An even lattice is said to be modular if it is similar to its dual. The norm of the similarity is then called the level of the lattice. In particular, its determinant is equal to the level to the power $n/2$. The modular properties of the theta series of such lattices, studied in [Que 95] lead to the notion of extremal lattices; if the level l is a prime number such that $1+l$ divides 24, an extremal lattice has minimum $2([n/k]+1)$, where $k = 2 \cdot 24/(1+l)$. For the levels $7, 3, 1$, we get $k = 24, 12, 6$, which means that the "jump dimensions" (which are the dimensions where the minimum may increase) for level 1 (resp. 3) is twice the "jump dimensions" for level 3 (resp. 7). In order to shift from one level to another, we can take the tensor product of a lattice with suitable elementary lattices. An example of such a situation is the following, and was communicated to the first author by B. Gross: let α satisfy the equation $\alpha^2 - \alpha + 2 = 0$; then $\mathbb{Z}[\alpha]$ is the ring of integers of the imaginary quadratic field of discriminant -7. This ring embeds into any maximal order $\mathfrak{M}$ of the quaternion field $\mathbb{Q}_{3,\infty}$ over $\mathbb{Q}$ ramified at 3 and ∞, as follows. We set $i^2 = -1$, $j^2 = -3$, $ij = k$ so that $\mathbb{Q}_{3,\infty} = \mathbb{Q}(i,j)$ and choose $\mathfrak{M} = \mathbb{Z}[1, i, (1+j)/2, (i+k)/2]$. Then $\alpha = (1+i+j+k)/2 \in \mathfrak{M}$. It embeds also in a maximal order of the octonions over $\mathbb{Q}$, as described in ([Gro 96], §4). Then the hermitian matrix $E = \begin{pmatrix} 2 & \alpha & -1 \\ \overline{\alpha} & 2 & \alpha \\ -1 & \overline{\alpha} & 2 \end{pmatrix}$ defines over these three rings a lattice for the scalar product $x.y = \mathrm{trace}(x^t E \overline{y})$, where trace is the reduced trace on each algebra, which is isometric to the Barnes lattice P_6, the Coxeter-Todd lattice K_{12}, respectively the Leech lattice Λ_{24}. In other words, if P_6 is the Barnes lattice considered with its hermitian structure over $\mathbb{Z}[\alpha]$, then we have the isometries $\mathbb{A}_2^2 \otimes_{\mathbb{Z}[\alpha]} P_6 \sim K_{12}$ and $\mathbb{E}_8 \otimes_{\mathbb{Z}[\alpha]} P_6 \sim \Lambda_{24}$ (together with the scalar product $\mathrm{trace}(x\overline{y})$, the previous maximal orders define respectively the root lattices $\mathbb{A}_2^2$ and $\mathbb{E}_8$).

We point out the existence of a similar series of three extremal lattices of minimum 8. The first one is a 20-dimensional even lattice of level 7, which is a $\mathbb{Z}[\alpha]$-unimodular lattice; its automorphism group is the group $2.M_{22}.2$, as shown in [PlN 95], [CCNPW 85]. Its structure as a $\mathbb{Z}[\alpha]$-lattice is explicitly given in [CCNPW 85]. Then $L_{40} = \mathbb{A}_2^2 \otimes_{\mathbb{Z}[\alpha]} L_{20}$ and $L_{80} = \mathbb{E}_8 \otimes_{\mathbb{Z}[\alpha]} L_{20}$ are of level 3 respectively unimodular; from this definition we determine their automorphism groups in §3. As shown in §2, one can easily get a Gram matrix for these lattices from a Gram matrix of L_{20}, following a general procedure that constructs modular Gram matrices (and we give several examples of

such constructions); but this is of no use in order to compute the minimum of the 80-dimensional lattices, which might become lower than 8, since the algorithms designed to compute the minimum of a lattice are by this time limited to the dimensions around 60. In §4 we show that these lattices are special cases of a general construction using a $(10, 5, 4)$-binary code, which allows us to compute their minimum. It moreover gives two non-isometric lattices in dimension 80.

A few constructions were already proposed for an 80-dimensional unimodular extremal lattice. The most natural would perhaps be a lattice invariant under $SL_2(79)$, in connection with the corresponding quadratic residue code; see [Sch 93]. In fact, there is a unique even unimodular $SL_2(79)$-invariant lattice of dimension 80 which remains a candidate to be extremal. In [Neb 97] resp. [BQS 95] three other candidates are constructed, which provide the groups $SL_2(41) \otimes \tilde{S}_3$ resp. $C_4 \times C_{41} : C_{40}$ as subgroups of their automorphism groups. None of them can overcome the problem of the determination of its minimum (although LLL-reduction doesn't give any vector of norm 6).

It is worth noticing that the center density of an 80-dimensional unimodular lattice of minimum 8 is equal to 2^{40}, which is slightly less than the one of the lattice of the same dimension constructed independently by Elkies and Shioda which has center density $2^{40.14..}$ ([Shi 91]).

2 A convenient construction

In this section we give a convenient construction for modular lattices. In particular Gram matrices for the lattices L_{40} and L_{80} may easily be obtained from a Gram matrix of L_{20}, the latter being given in [PlN 95] (cf. also [CCNPW 85]).

Proposition 2.1 *Let K be either $\mathbb{Q}$ or an imaginary quadratic number field and $F \in K^{n \times n}$ a hermitian positive definite matrix. Let $a, d \in \mathbb{Q}$, $b \in K$, such that $a, d, ad - b\bar{b} > 0$. Then the matrix*

$$Q(F, a, b, d) := \begin{pmatrix} aF & bI_n \\ \bar{b}I_n & dF^{-1} \end{pmatrix}$$

is a positive definite hermitian matrix of determinant $(ad - b\bar{b})^n$. The map $g \to \begin{pmatrix} g & 0 \\ 0 & g^{-tr} \end{pmatrix}$ embeds $Aut(F)$ into $Aut(Q(F, a, b, d))$.

If $K = \mathbb{Q}$ then $Q(F, a, b, d)$ is $ad - b^2$-modular with respect to the symplectic similarity $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$.

Proof: Straightforward, using

$$(\star) \quad Q(F, a, b, d) = \begin{pmatrix} 1 & 0 \\ 0 & F^{-1} \end{pmatrix} \left(\begin{pmatrix} a & b \\ \bar{b} & d \end{pmatrix} \otimes F \right) \begin{pmatrix} 1 & 0 \\ 0 & F^{-1} \end{pmatrix}.$$

□

Remark: *Let B be a basis of the lattice L in the hermitian space (K^n, ϕ_0) with Gram matrix F and B^* the dual basis of B which is a lattice basis of the dual lattice L^*. Then $Q(F, a, b, d)$ is the Gram matrix of the lattice $L \oplus L^*$ in the hermitian space $(K^n \oplus K^n, \phi)$ with respect to the basis (B, B^*), where the hermitian form $\phi : K^n \oplus K^n \to K$ is given by*

$$\phi(l_1 + l_1', l_2 + l_2') = a\phi_0(l_1, l_2) + b\phi_0(l_1, l_2') + \bar{b}\phi_0(l_1', l_2) + d\phi_0(l_1', l_2')$$

for all $l_1, l_2, l_1', l_2' \in K^n$.

Many well known lattices can be described as above:

For example the root lattices $\mathbb{D}_4 = Q(\mathbb{A}_2, 1, 1, 3)$ and $\mathbb{E}_8 = Q(\mathbb{D}_4, 1, 1, 2) = Q(\mathbb{A}_4, 1, 2, 5)$, but also the Coxeter Todd lattice $K_{12} = Q(P_6, 1, 2, 7)$ can be constructed in this way.

Examples: Some extremal 2-modular lattices:

(i) The Barnes-Wall lattice (cf. [CoS 88] p.129) $BW_{16} = Q(\mathbb{A}_2 \otimes \mathbb{D}_4, 1, 2, 6)$.

(ii) The 2 known extremal 2-modular lattices of dimension 20 (cf. [PlN 95] p. 49) may be obtained from the Craig lattices (cf. [CoS 88] p.222) in dimension 10: $[2.M_{12}.2]_{20} = Q(A_{10}^{(2)}, 1, 3, 11)$ and $[SU_5(2) \overset{2(2)}{\circ} SL_2(3)]_{20} = Q(A_{10}^{(3)}, 1, 3, 11)$.

(iii) The extremal 2-modular lattice of dimension 24 with maximal finite automorphism group ([Neb 95], [Neb 96]): $[6.U_4(3).2 \overset{2}{\boxtimes}_{\sqrt{-3}} SL_2(3)]_{24} = Q(K_{12}, 1, 1, 3)$.

(iv) Applying this construction to a Gram matrix F of the 6-modular lattices of minimum 8 belonging to the maximal finite subgroups 16 and 17 of $GL_{24}(\mathbb{Q})$ (in [Neb 95] and [Neb 96]) one obtains extremal 2-modular lattices $Q(F,1,2,6)$ of dimension 48.

(v) If F is a Gram matrix of the 6-modular lattice of minimum 6 in dimension 16 with maximal finite automorphism group number 9 of [NeP 95] then $Q(F,1,2,6)$ is a non extremal 2-modular lattice of dimension 32. So this construction does i.g. not preserve the minimum.

It should be noted, that the construction Q only depends on the lattice and not on the choice of the Gram matrix. For unimodular F, the lattice $Q(F,a,b,d)$ is simply the tensor product $\begin{pmatrix} a & b \\ b & d \end{pmatrix} \otimes F$. For arbitrary integral F, the construction Q is a natural way to obtain a (modular) overlattice of this tensor product, which is also invariant under the automorphism group $Aut(F)$.

Let F be a Gram matrix of L_{20}. Then the corresponding bilinear form is of the form trace $\circ f$, where L_{20} is a 10-dimensional $\mathbb{Z}[\alpha]$-module and f is a unimodular hermitian form $L_{20} \times L_{20} \to \mathbb{Z}[\alpha]$.

Proposition 2.2 *(i)* $Q(F,1,2,7) \in \mathbb{Z}^{40\times 40}$ *is a Gram matrix of the* $\mathbb{Z}$*-lattice* L_{40}*.*

(ii) $g := Q(f,1,\frac{2}{\sqrt{-7}},1) \in \mathbb{Z}[\alpha]^{20\times 20}$ *is a Gram matrix of the hermitian* $\mathbb{Z}[\alpha]$*-lattice* L_{40}*.*

(iii) $Q(g,1,\frac{-\alpha}{\sqrt{-7}},3) \in \mathbb{Z}[\alpha]^{40\times 40}$ *is a Gram matrix of the hermitian* $\mathbb{Z}[\alpha]$*-lattice* L_{80}*.*

Proof: (ii) Let $\mathfrak{M}$ be the maximal order of $\mathbb{Q}_{3,\infty}$. As described in the introduction, $\mathfrak{M}$ is a hermitian $\mathbb{Z}[\alpha]$-lattice. With respect to the $\mathbb{Z}[\alpha]$-basis $(\frac{i-k}{2},1)$, the form trace$(x\overline{y})$ on $\mathfrak{M}$ has the hermitian Gram matrix

$$h := \begin{pmatrix} 1 & \frac{2}{\sqrt{-7}} \\ -\frac{2}{\sqrt{-7}} & 1 \end{pmatrix}.$$

The $\mathbb{Z}[\alpha]$-hermitian form on $L_{40} = L_{20} \underset{\mathbb{Z}[\alpha]}{\otimes} \mathfrak{M}$ is given by the Gram matrix $h \otimes f$. Since f is unimodular, one finds (ii) using $(\star)$.

(i) may be deduced from (ii) by blowing up the matrix g: Let $(b_1, \ldots, b_{10})$ be a basis of the $\mathbb{Z}[\alpha]$-lattice L_{20} with Gram matrix f and $(b_1^*, \ldots, b_{10}^*)$ the corresponding dual basis (i.e. $f(b_i, b_j^*) = \delta_{ij}$). A $\mathbb{Z}$-basis of L_{20} is given by $B := (b_1, \alpha b_1, \ldots, b_{10}, \alpha b_{10})$. Let F be the corresponding Gram matrix of trace $\circ f$. Then the dual basis is $B^* = (\frac{1}{7}(4-\alpha)b_1^*, \frac{1}{7}(1-2\alpha)b_1^*, \ldots, \frac{1}{7}(4-\alpha)b_{10}^*, \frac{1}{7}(1-2\alpha)b_{10}^*)$ (with Gram matrix F^{-1}). To get integral scalar products we multiply the elements of B^* by $\sqrt{-7}$ and compute $\mathrm{trace}(g(b_i, \frac{4-\alpha}{\sqrt{-7}}b_j^*)) = \delta_{ij}(\mathrm{trace}(-\frac{2}{\sqrt{-7}}\frac{4-\bar{\alpha}}{\sqrt{-7}})) = 2\delta_{ij}$, etc.. Therefore trace $\circ\, g = Q(F, 1, 2, 7)$.

(iii) The matrix

$$o := \begin{pmatrix} 1 & \frac{2}{\sqrt{-7}} & \frac{-\alpha}{\sqrt{-7}} & 0 \\ -\frac{2}{\sqrt{-7}} & 1 & 0 & \frac{-\alpha}{\sqrt{-7}} \\ \frac{\bar{\alpha}}{\sqrt{-7}} & 0 & 1 & -\frac{2}{\sqrt{-7}} \\ 0 & \frac{\bar{\alpha}}{\sqrt{-7}} & \frac{2}{\sqrt{-7}} & 1 \end{pmatrix}$$

is a Gram matrix of the $\mathbb{Z}[\alpha]$-lattice $\mathbb{E}_8$. Hence (iii) follows from the equation

$$\begin{pmatrix} I_{10} & 0 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & 0 & I_{10} \end{pmatrix} Q(g, 1, \frac{-\alpha}{\sqrt{-7}}, 3) \begin{pmatrix} I_{10} & 0 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & f & 0 \\ 0 & 0 & 0 & I_{10} \end{pmatrix} = o \otimes f.$$

□

3 The automorphism groups

In this section we deduce the automorphism groups $Aut(L)$, i.e. the group of all orthogonal transformations mapping the lattice L into itself, of the two lattices $L = L_{40}$ and $L = L_{80}$. Since L_{40} only has 360360 minimal vectors, it might be possible to compute $Aut(L_{40})$ with the computer program described in [PlS 97]. But L_{80} has 1250172000 vectors of length 8 (which moreover cannot be found directly by computer), so here this method will fail. We use the classification of finite simple groups to show that the automorphism groups of both lattices are the tensor products of $Aut(L_{20}) = 2.M_{22}.2$ with the automorphism groups of the hermitian lattices $\mathbb{A}_2^2$ respectively $\mathbb{E}_8$.

Proposition 3.1 *(i) The hermitian automorphism group of the $\mathbb{Z}[\alpha]$-lattice $\mathbb{A}_2^2$ is the unit group of the maximal order $\mathfrak{M}$ of $\mathbb{Q}_{3,\infty}$, isomorphic to $\tilde{S}_3$.*

(ii) The hermitian automorphism group of the $\mathbb{Z}[\alpha]$-lattice $\mathbb{E}_8$ is $2.Alt_7$.

(iii) $Aut(L_{20}) = 2.M_{22}.2$ is an extension of the double cover $2.M_{22}$ of the Mathieu group M_{22} by the outer automorphism of order 2. This group is also the hermitian automorphism group of the $\mathbb{Z}[\alpha]$-lattice L_{20}.

Proof: (i) The automorphism group of the integral lattice $\mathbb{A}_2^2$ is $D_{12} \wr C_2$ the wreath product of the dihedral group of order 12 by C_2. The hermitian automorphism group $U \leq GL_4(\mathbb{Z}[\alpha])$ of this lattice may be regarded as a subgroup of $D_{12} \wr C_2$ commuting with an element $\alpha \in GL_8(\mathbb{Q})$ with $\alpha^2 - \alpha + 2 = 0$. By construction, U contains the unit group $\tilde{S}_3$ of $\mathfrak{M}$. Since 7 does not divide the order of U, the commuting algebra $C_{\mathbb{Q}^{8\times 8}}(U)$ of U in $\mathbb{Q}^{8\times 8}$ contains $\mathbb{Q}[\alpha]$ properly. One concludes that $C_{\mathbb{Q}^{8\times 8}}(U) = C_{\mathbb{Q}^{8\times 8}}(\tilde{S}_3) \cong \mathbb{Q}_{3,\infty}$. Therefore U embeds into $\mathbb{Q}_{3,\infty}$ and hence $U = \tilde{S}_3$.
(ii) Let $U \leq GL_4(\mathbb{Z}[\alpha])$ be the hermitian automorphism group of $\mathbb{E}_8$. Then $U \leq Aut(\mathbb{E}_8) = 2.O_8^+(2).2$ is contained in the stabilizer of a maximal totally singular subspace $T_1 = \alpha\mathbb{E}_8/2\mathbb{E}_8$. By [CCNPW 85] this subspace is unique up to the action of $2.O_8^+(2).2$ and its stabilizer is $2_+^{1+6}.Alt_8$. One computes the centralizer of α in this group to be the subgroup $2.Alt_7$ of index 512.
(iii) Follows from [CCNPW 85] p. 39 (cf. also [PlN 95] Chapter IX). □

Theorem 3.2 *The automorphism group of L_{80} is $G := Aut(L_{80}) = 2.Alt_7 \otimes_{\sqrt{-7}} 2.M_{22}.2$ and a maximal finite subgroup of $GL_{80}(\mathbb{Q})$. The G-invariant lattices in $\mathbb{Q}^{1\times 80}$ are of the form cL_{80}, where $0 \neq c \in C_{\mathbb{Q}^{80\times 80}}(G) \cong \mathbb{Q}[\alpha]$ is an invertible element in the commuting algebra of G (i.e. G is a GIR in the sense of [Gro 90]).*

Proof: Let $U := 2.Alt_7 \otimes_{\sqrt{-7}} 2.M_{22}.2$. By construction U is a subgroup of $Aut(L_{80}) = G$. The commuting algebra of U is isomorphic to $\mathbb{Q}[\alpha]$ and U fixes up to isomorphism only one lattice (cf. [CCNPW 85] and [JLPW 95]). So we only have to show that $G = U$. Since L_{80} is orthogonally indecomposable, G is a maximal finite primitive subgroup of $GL_{80}(\mathbb{Q})$.

Assume first, that $2.M_{22} \trianglelefteq G$ is a normal subgroup of G. Then $C := C_G(2.M_{22})$ embeds into $GL_4(\mathbb{Q}[\alpha])$ and contains $2.Alt_7$. Since $2.Alt_7$ is the full automorphism group of its up to isomorphism unique lattice in $\mathbb{Q}[\alpha]^{1\times 4}$ this implies that $C = 2.Alt_7$ and G contains $2.Alt_7 \otimes_{\sqrt{-7}} 2.M_{22}$ of index $\leq 2 = |Out(2.M_{22})|$. Hence $G = U$. The same conclusion holds under

the assumption that $2.Alt_7$ is a normal subgroup of G, because then $C := C_G(2.Alt_7)$ is $2.M_{22}.2$, a maximal finite subgroup of $GL_{20}(\mathbb{Q})$. Therefore $2.M_{22} \trianglelefteq G$ and $G = U$.

Hence we may assume that none of the two groups is a normal subgroup of G. Let $F := Fit(G) = \prod_{p||G|} O_p(G)$ be the Fitting group of G. The primitivity of G implies that all abelian characteristic subgroups of F are cyclic. A Theorem of P. Hall, which classifies those p-groups, all of which abelian characteristic subgroups are cyclic (cf. [Hup 67], p. 357), yields only rather restricted possibilities for F: If $p \neq 2, 5$, then $O_p(G)$ is cyclic, for $p = 5$, one additionally has the possibility $O_5(G) \cong 5_+^{1+2}$ and $O_2(G)$ embeds into $GL_{16}(\mathbb{Q})$, leaving many possibilities (cf. [NeP 95]). None of the possible groups F have an outer automorphism group the order of which is divisible by 11.

Therefore one concludes that $S := G^{(\infty)}/Z(G)$ is a finite simple group containing $U^{(\infty)}/Z(U)$. An inspection of the orders and character tables of the 26 sporadic finite simple groups in [CCNPW 85] shows that S is a finite Chevalley group. Bounds for the minimal degrees of the projective representation of the finite Chevalley groups are given in [SeZ 93] (cf. also [LaS 74]). Using the fact, that the minimal degree of a faithful projective modular representation of $U^{(\infty)}/Z(U)$ is $3 \cdot 6 = 18$ (cf. [JLPW 95]), one immediately excludes the case that S is a classical group. The bounds in [SeZ 93] now only leave the possibilities that S is one of $F_4(2)$, $G_2(2)$, $G_2(3)$, $G_2(4)$, $Sz(8)$, $Sz(32)$, ${}^2G_2(3)$, ${}^2G_2(27)$, ${}^3D_4(2)$, or ${}^2F_4(2)$. But none of these 10 groups is of order divisible by 11, contradicting the assumption that $M_{22} \leq S$. □

Using the same arguments one shows the following

Theorem 3.3 *The automorphism group of L_{40} is $G := Aut(L_{40}) = \tilde{S}_3 \otimes_{\sqrt{-7}} 2.M_{22}.2$ and a maximal finite subgroup of $GL_{40}(\mathbb{Q})$. The G-invariant lattices in $\mathbb{Q}^{1\times 40}$ are of the form cL_{40} or $cL_{40}^{\#}$, where $0 \neq c \in C_{\mathbb{Q}^{40\times 40}}(G) \cong \mathbb{Q}[\alpha]$ is an invertible element in the commuting algebra of G.*

4 The minimum

In order to prove that the minimum of L_{20}, L_{40}, L_{80} is 8, we shall reconstruct them using codes. This general construction, of which a special case is already

described in [Bac 97] for the lattice of dimension 20, also shows the existence of a second unimodular lattice of minimum 8 in dimension 80.

The first step is a special case of [Que 84]. Let $(L_0, b(x,y))$ be an even, integral lattice of odd determinant and of dimension k; then the quotient $(L_0/2L_0, \overline{b})$ admits an hyperbolic decomposition $L_0/2L_0 = T_1 \oplus T_2$ (i.e. $T_i^{\perp} = T_i$ for the induced non degenerate form $\overline{b}$). For $i = 1, 2$, we denote by L_i the sublattice of L_0 which is the preimage of T_i. We again denote by $b, \overline{b}$ the forms over L_0^n, $(L_0/2L_0)^n$ deduced from the previous ones.

The Hamming weight of a word $x \in {\mathbb{F}_2}^n$ is the number $wt(x)$ of its non zero coordinates. We denote by $x.y$ the usual scalar product $x.y = \sum_{i=1}^n x_i y_i$ in ${\mathbb{F}_2}^n$. Let C be a binary linear code of length n (see [MWS 77]), and let

$$\mathcal{C} = T_1 \otimes_{\mathbb{F}_2} C \oplus T_2 \otimes_{\mathbb{F}_2} C^{\perp} \subset (L_0/2L_0)^n.$$

For $x \in L_0$ (respectively $x \in L_0/2L_0$), and $u \in {\mathbb{F}_2}^n$, we denote by $x \otimes u \in L_0^n$ (respectively $x \otimes u \in (L_0/2L_0)^n$) the n-tuple which i-th coordinate is equal to x if i belongs to the support of u and is zero otherwise.

The n-tuple of ${\mathbb{F}_2}^n$ with all coordinates equal to 1 (resp. 0) is denoted by $\mathbf{1}$ (resp. $\mathbf{0}$).

Proposition 4.1 *With the previous notations, we have*

(i) $\mathcal{C}^{\perp} = \mathcal{C}$.

(ii) Let $L_{\mathcal{C}}$ be the preimage of $\mathcal{C}$ in L_0^n, endowed with the form $x.y = \frac{1}{2} b(x,y)$. It is an integral lattice of determinant $det(L_{\mathcal{C}}) = det(L_0)^n$.

(iii) If moreover $\frac{1}{\sqrt{2}} L_i$ is even, or if the codes C and $C^{\perp}$ are even (i.e. the Hamming weight takes even values on them), then $L_{\mathcal{C}}$ is even.

Proof:
(i) The $\mathbb{F}_2$-vector space $\mathcal{C}$ is generated by elements of the form $t \otimes u$, where either u belongs to C and t to T_1, or u belongs to $C^{\perp}$ and t to T_2. Since $\overline{b}(t \otimes u, s \otimes v) = (u.v)\overline{b}(t,s)$, this is zero in all cases. Hence $\mathcal{C} \subset \mathcal{C}^{\perp}$; equality holds from the equality of the dimensions.
(ii) follows from (i) and [Que 84].
(iii) The lattice $L_{\mathcal{C}}$ is generated by $(2L_0)^n$ which is obviously even with respect to $\frac{1}{2} b(x,y)$, and by the $x \otimes u$, where u belongs to C (resp $C^{\perp}$) and x

to L_1 (resp to L_2). Since $(x \otimes u).(x \otimes u) = wt(u)b(x,x)/2$, the lattice $L_{\mathcal{C}}$ is even under the hypothesis of the proposition. □

In order to measure the norm of the lattice $L_{\mathcal{C}}$, we define a weight w on $L_0/2L_0$ by the following:

Definition 4.2 *We set, for $t_1 \in T_1$ and $t_2 \in T_2$,*

$$w(t_1+t_2) = \begin{cases} 0 & \text{if } t_1 = t_2 = 0 \\ 1 & \text{if } \overline{b}(t_1,t_2) \neq 0 \\ 2 & \text{if } \overline{b}(t_1,t_2) = 0 \text{ and } (t_1,t_2) \neq (0,0) \end{cases}$$

We extend the function w to $(L_0/2L_0)^n$ by setting $w(x) = \sum_{i=1}^n w(x_i)$. If $\mathcal{C} \subset (\mathcal{L}_\prime/\in\mathcal{L}_\prime)^\setminus$, the weight of $\mathcal{C}$ is defined by

$$w(\mathcal{C}) = \min\{w(t) \mid t \in \mathcal{C} \setminus \{0\}\}.$$

Lemma 4.3 *If L_0 is one of the lattices $\mathbb{Z}[\alpha]$, $\mathbb{A}_2^2$, $\mathbb{E}_8$, we can choose a decomposition $L_0/2L_0 = T_1 \oplus T_2$ as above with L_i isometric to $\sqrt{2}L_0$; then*

$$\forall\, t \in L_0/2L_0,\ w(t) = \min\{b(x,x)/2 \mid x \in t\}.$$

Proof: The fact that these three lattices are $\mathbb{Z}[\alpha]$-modules shows the existence of such a decomposition: one can take $L_1 = \alpha L_0$, $L_2 = \overline{\alpha}L_0$ (see the Introduction). In all three cases it is well known that the classes of L_0 modulo $2L_0$ are represented by the vectors of norm 2 and 4 (see [CoS 88], [Bac 97]) and that one class doesn't contain elements of the two types. For $x_i \in L_i$, the equality $b(x_1+x_2, x_1+x_2) = b(x_1,x_1) + b(x_2,x_2) + 2b(x_1,x_2)$ shows that

$$(\star)\ 2w(t) \equiv b(x,x) \pmod 4\ \forall\, t \in L_0/2L_0,\ \forall\, x \in t$$

which concludes the proof. □

Now we apply the construction described in Proposition 4.1 to the three lattices L_0 of Lemma 4.3, which show that, in those cases, the weight w is the right one to be considered in order to determine the minimum of the lattice $L_{\mathcal{C}}$.

Example. If C is the length 3 code generated by **1**, it is easy to see that the corresponding $\mathcal{C}$ has weight 4; from Lemma 4.3 and the fact that $2L_0$ has

minimum 4, the lattices $L_{\mathcal{C}}$ have minimum 4. We recover B. Gross constructions of the Coxeter-Todd and Leech lattices described in the Introduction.

In ([Bac 97], Theorem 6.3), a code $C \times C^{\perp}$ over $\mathbb{F}_2 \times \mathbb{F}_2$ of weight 8 and length 10 is defined; this is the case $L_0 = \mathbb{Z}[\alpha]$, where $\mathbb{Z}[\alpha]/2\mathbb{Z}[\alpha]$ is identified with $\mathbb{F}_2 \times \mathbb{F}_2$. We prove here that the extension of this code to the two other quotients $L_0/2L_0$ keeps the weight 8 (clearly $\mathcal{C} = L_0/2L_0 \otimes_{\mathbb{F}_2 \times \mathbb{F}_2} (C \times C^{\perp})$). We start by the definition of the code C and some of its properties which will be of later use. We identify an element of ${\mathbb{F}_2}^n$ and the set of its non zero coordinates.

Lemma 4.4 *Let C be the binary code of length 10 generated by the rows of the matrix*

$$\begin{array}{cccccccccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array}$$

(i) It is a cocyclic code, equivalent to its dual; it contains 15 words of weight 4, 15 words of weight 6, and one word of weight 10.

(ii) $C \cap C^{\perp} = \{\mathbf{0}, \mathbf{1}\}$.

(iii) A word of weight 6 of C contains exactly three words of weight 4 of $C^{\perp}$, which are, up to permutation, in the following position:

$$\begin{array}{cccccc} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \end{array} .$$

and this is a one to one correspondence between the words of weight 6 of C and the sets of three words of weight 4 of $C^{\perp}$ in the previous position.

Proof: Straightforward from the definition of C. □

Proposition 4.5 *If C is the binary code defined in Lemma 4.4, in all three cases $\mathcal{C}$ has weight 8.*

Proof: We set $(e_1, \ldots, e_k)$ a basis of $L_0/2L_0$ such that the $k/2$ first vectors generate T_1, while the $k/2$ last vectors generate T_2 and satisfy $\overline{b}(e_i, e_{k/2+j}) = \delta_{i,j}$. We write $x = e_1 \otimes u_1 + \ldots + e_k \otimes u_k$ a non zero element of $\mathcal{C}$, with $u_1, \ldots, u_{k/2} \in C$ and $u_{k/2+1}, \ldots, u_k \in C^\perp$. Up to a change of basis, we can assume that $\{u_1, \ldots, u_{k/2}\}$ are distinct. ¿From $(\star)$ and the fact that $(L_\mathcal{C}, \frac{1}{2}b(x,y))$ is even (Proposition 4.1), the weight is even on $\mathcal{C}$ and we only need to prove that $w(x) \geq 7$. Obviously $w(x) \geq \text{card}(\cup u_i)$, so we can assume that $\text{card}(\cup u_i) \leq 6$. If at least one of the words u_i has weight 6, for example u_1, the others are contained in it. Since $wt(C) = 4$, $u_2, \ldots, u_{k/2} = \mathbf{0}$. ¿From the definition of w, $w(x) = 6$ if and only if $u_{k/2+1} = u_1$, which is not possible since $C \cap C^\perp = \{\mathbf{0}, \mathbf{1}\}$.

The last case to consider is the case where all the non zero u_i have weight 4. Two distinct weight 4 words of $C \cup C^\perp$ intersect on zero, one, or two coordinates. Since we assume $\text{card}(\cup u_i) \leq 6$, we only need to consider the case where the intersections have cardinality 2. If at most one of the $\{u_1, \ldots, u_{k/2}\}$ and at most one of the $\{u_{k/2+1}, \ldots, u_k\}$ is non zero, then clearly at least four coordinates belong to $T_1 \cup T_2 \setminus \{0\}$ and have weight 2. If at least two of the $\{u_1, \ldots, u_{k/2}\}$ are weight 4 words, they are in the position of Lemma 4.4 and define a weight 6 word of $C^\perp$. Under our assumption, this means that $u_{k/2+1}, \ldots, u_k = 0$, and the nonzero coordinates of x all have weight 2. □

We have the following estimate of the norm of the lattice $L_\mathcal{C}$:
• It contains $(2L_0)^n$, which has norm 4, attained on the vectors of the form $(x, 0, \ldots, 0)$ up to permutation, where x is a minimal vector of L_0. The next value of the norm on this lattice is 8.
• $\min(L_\mathcal{C} \setminus (2L_0)^n) = w(\mathcal{C})$.

The goal of the second step of the construction, in the case of the code C given in Lemma 4.4, is to get rid of the norm 4 vectors of $L_\mathcal{C}$. Therefore, we define a sublattice L' of $L_\mathcal{C}$ not containing them, and show the existence of an even overlattice Λ of L', with the same index, and of minimum 8. This must be understood as a "neighbouring" procedure. The lattice L' is easy to define:

$$L' = \{x = (x_1, \ldots, x_n) \in L_\mathcal{C} \mid \sum_{i=1}^{n} x_i \in 2L_1\}.$$

We also set

$$L'' = L_{\mathcal{C}} + \{\frac{1}{2}(z, z, \ldots, z) \mid z \in L_1\}.$$

Proposition 4.6 *Assume that* $n \equiv 2 \pmod 4$, $\mathbf{1} \in C \cap C^{\perp}$ *and that* $w(\mathcal{C}) = 8$. *Then*

(i) $\min(L') = 8$.

(ii) The map $\psi : x \to \sum_{i=1}^{n} x_i$ *induces an isometry of the* $\mathbb{F}_2$*-quadratic spaces* $(L''/L', \frac{1}{2}b(x,x))$ *and* $(L_1/2L_1, \frac{1}{4}b(x,x))$. *Moreover* $\psi(L_{\mathcal{C}}/L') = 2L_0/2L_1$.

Proof:
(i) Clearly, the norm 4 vectors of $L_{\mathcal{C}}$, previously defined, don't belong to L' because the minimum of L_1 is 4.
(ii) With the previous notations, a vector y of $L_{\mathcal{C}}$ can be written $y = \sum l_1 \otimes u + \sum l_2 \otimes v + 2t$ where $u \in C$, $v \in C^{\perp}$, $l_i \in L_i$ for $i = 1, 2$, and $t \in L_0^n$. Then $\sum y_i = \sum wt(u) l_1 + \sum wt(v) l_2 + 2\sum t_i \in 2L_0$, and, if $x = y + \frac{1}{2}(z, \ldots, z)$, $\psi(x) = \sum x_i = \sum y_i + \frac{n}{2} z \equiv \sum y_i + z \pmod{2L_1}$ belongs to $2L_1$, if and only if $x \in L'$. Clearly, $\psi(x) \in 2L_0$ if and only if $x \in L_{\mathcal{C}}$, i.e. $z \in 2L_1$.

Since the lattice $L_{\mathcal{C}}$ is even for $\frac{1}{2}b(x,y)$, one has for $y \in L_{\mathcal{C}}$, $b(y,y) \equiv 0 \pmod 4$. Hence $b(x,x) = b(y + \frac{1}{2}(z, \ldots, z), y + \frac{1}{2}(z, \ldots, z)) \equiv b(\sum y_i, z) + 2(b(z,z)/4) \pmod 4$ is even and $\frac{1}{2}b(\psi(x), \psi(x)) = \frac{1}{2}b(\sum y_i + z, \sum y_i + z) \equiv b(\sum y_i, z) + \frac{1}{2}b(z,z) \pmod 4$ since $\sum y_i \in 2L_0$, which shows that ψ is an isometry of the quadratic forms. □

The last step of the construction shows that certain overlattices of L' keep the minimum 8.

Theorem 4.7 *Let* C *be the binary code defined in Lemma 4.4, and let* $L_{\mathcal{C}}$, L' *be the lattices previously defined from it. Let* B *be a maximal totally singular subspace of the* $\mathbb{F}_2$*-quadratic space* L''/L', *which is a complement of* $L_{\mathcal{C}}/L'$ *and let* $\Lambda(B)$ *be the sublattice of* L'' *which is the preimage of* B. *Then the minimum of* $\Lambda(B)$ *is* 8.

Proof: Let B be a fixed maximal totally singular subspace as in the Theorem and $\Lambda := \Lambda(B)$. From the definition of Λ, $\Lambda \cap L_{\mathcal{C}} = L'$ which has minimum 8, and $\Lambda \subset L_{\mathcal{C}} + \{\frac{1}{2}(z, \ldots, z) \mid z \in L_1\}$. For $y \in L_0$ and $z \in L_1 \setminus 2L_0$, since $L_1 \sim$

$\sqrt{2}L_0$, $b(y+z/2, y+z/2) = b(y,y)+b(y,z)+b(z,z)/4 \in \mathbb{N}_{\geq 1}$. Hence a vector X in $L_{\mathcal{C}} + \frac{1}{2}(z,\dots,z)$ satisfies $X.X \geq 5$ (recall that $X.X = b(X,X)/2 \in \mathbb{N}$ from Proposition 4.6(ii)). We shall prove that such a translate of $L_{\mathcal{C}}$ doesn't contain any vector of norm 6, which is enough to prove that Λ has minimum 8. We fix $z \in L_1 \setminus 2L_0$. For $i = 1, 2, 3$ we set

$$S_i = \{y \in L_0 \mid b(y + z/2, y + z/2) = i\}.$$

Then a vector $Y \in L_{\mathcal{C}}$ such that $X = Y + \frac{1}{2}(z,\dots,z)$ has norm 6 would have either 8 coordinates in S_1 and 2 in S_2, or 9 coordinates in S_1 and one in S_3. We need a precise description of these sets. The case $L_0 = \mathbb{Z}[\alpha]$ is treated in [Bac 97] (in this case, $S_3 = \emptyset$), so we now concentrate on the two other cases.

Lemma 4.8 *With the previous notations,*

(i) If $L_0 = \mathbb{A}_2^2$, there are $\epsilon_i \in \frac{1}{2}L_0$, $1 \leq i \leq 4$, such that $2\epsilon_i$ belongs to the class of z modulo $2L_0$, and $b(\epsilon_i, \epsilon_i) = 1$ for $i = 1, 2$, $b(\epsilon_i, \epsilon_i) = 3$ for $i = 3, 4$, and $b(\epsilon_i, \epsilon_j) = 0$ for $i \neq j$, such that

$$\begin{array}{ll} S_1 & = \{-\frac{z}{2} \pm \epsilon_i \mid i = 1, 2\} \\ S_2 & = \{-\frac{z}{2} + \frac{1}{2}\sum_{i=1}^4 k_i\epsilon_i \mid k_i = \pm 1,\ \sum_{i=1}^4 k_i \equiv 0 \pmod 4\} \\ S_3 & = \{-\frac{z}{2} \pm \epsilon_i \mid i = 3, 4\} \end{array}$$

(ii) If $L_0 = \mathbb{E}_8$, there are $\epsilon_i \in \frac{1}{2}L_0$, $1 \leq i \leq 8$, such that $2\epsilon_i$ belongs to the class of z modulo $2L_0$, and $b(\epsilon_i, \epsilon_j) = \delta_{i,j}$ for all i, j, such that

$$\begin{array}{ll} S_1 & = \{-\frac{z}{2} \pm \epsilon_i \mid 1 \leq i \leq 8\} \\ S_2 & = \{-\frac{z}{2} + \frac{1}{2}\sum_{i=1}^8 k_i\epsilon_i \mid k_i = \pm 1,\ \sum_{i=1}^8 k_i \equiv 0 \pmod 4\} \\ S_3 & = \{-\frac{z}{2} \pm \epsilon_i \pm \epsilon_j \pm \epsilon_l \mid 1 \leq i, j, l \leq 8 \text{ pairwise distinct }\} \end{array}$$

Proof: In the case $L_0 = \mathbb{E}_8$, $z/2$ is a deep hole and its class modulo $2L_0$ contains an orthogonal frame denoted by $(2\epsilon_i)_{1\leq i\leq 8}$ ([CoS 88], p.169). In the case $L_0 = \mathbb{A}_2^2$, it is easy to check that any class modulo $2L_0$ which doesn't contain a minimal vector, contains such an orthogonal set.

In both cases, the vectors $\epsilon_i \pm \epsilon_j$ generate a sublattice of index 2 in L_0 (isometric to $\mathbb{D}_8$ in the case $L_0 = \mathbb{E}_8$). So we may assume (up to a change of

signs) that $(\epsilon_1 + \ldots + \epsilon_k)/2 \in L_0$. We set $y + x/2 = (\sum_{i=1}^{8} k_i \epsilon_i)/2$, where the k_i are integers with the same parity, and find the announced solutions. $\square$

Now we need to study the decomposition of the elements of the sets S_i in $L_0/2L_0 = T_1 \oplus T_2$. We set p_i the projection on T_i. Since $T_1 \oplus T_2$ is a hyperbolic decomposition, for all $x, y \in L_0/2L_0$, $\overline{b}(x, y) = \overline{b}(p_1(x), p_2(y)) + \overline{b}(p_2(x), p_1(y))$. Moreover, we can choose z arbitrarily in its class modulo $2L_0$, so we take $z = -2\epsilon_1$. We fix a basis $(e_1, \ldots, e_{k/2})$ of T_1 such that $e_{k/2} = 2\epsilon_i \pmod{2L_0}$ for all i, and choose for $(e_{k/2+1}, \ldots, e_k)$ its dual basis in T_2, defined by the conditions $\overline{b}(e_i, e_{k/2+j}) = \delta_{i,j}$. If $-z/2 \pm \epsilon_i$ and $-z/2 \pm \epsilon_j$ are two distinct elements of S_1, $p_1(-x/2 \pm \epsilon_i) - p_1(-x/2 \pm \epsilon_j) = p_1(\pm\epsilon_i \pm \epsilon_j) \neq 0$, since, for $i \neq j$, $\pm\epsilon_i \pm \epsilon_j$ has norm 2, hence cannot belong to L_1, and, for $i = j$, $p_1(2\epsilon_i) = e_{k/2}$. So, in both cases, the map p_1 is a bijection from S_1 to T_1. Since $p_2(2\epsilon_i) = 0$, the image of S_1 under p_2 is half of T_2. More precisely, we have $b(2\epsilon_1, \epsilon_1 \pm \epsilon_i) \equiv 0 \pmod 2$, so $\overline{b}(e_{k/2}, p_2(s)) = 0$ for all $s \in S_1$, and $p_2(S_1) = \mathbb{F}_2 e_{k/2+1} + \ldots + \mathbb{F}_2 e_{k-1}$.

Let now s belong to S_2. We have $\overline{b}(e_{k/2}, p_2(s)) \equiv b(2\epsilon_1, \epsilon_1 + \sum_{i=1}^{k} k_i \epsilon_i)/2 \equiv 1 \pmod 2$, which proves that $p_2(s)$ has a non zero coordinate on e_k. Then it is not possible for Y to have 8 coordinates in S_1 and 2 in S_2, since the code $C^\perp$ doesn't contain any word of weight 2.

We now consider the case where Y has exactly one coordinate in S_3. If $s \in S_3$, $\overline{b}(e_{k/2}, p_2(s)) = 0$, and the coordinates of Y don't have any component on e_k. In order to deal with this case, we need to know the exact decomposition of S_1 on the basis $\{e_1, \ldots, e_k\}$, i.e., since S_1 is in a one-to-one correspondence with T_1, we need to know the map $\phi : {\mathbb{F}_2}^{k/2} \to {\mathbb{F}_2}^{k/2-1}$ such that for all $s \in S_1$, and for all $x \in {\mathbb{F}_2}^{k/2}$, $p_1(s) = \sum_{i=1}^{k/2} x_i e_i \iff p_2(s) = \sum_{i=k/2+1}^{k-1} (\phi(x))_{i-k/2} e_i$. In general, this map is not linear. ¿From the previous remarks, we have $\phi(0) = 0$ and $\phi(x + e_{k/2}) = \phi(x)$; hence we only need to know $\phi|_{<e_1,\ldots,e_{k/2-1}>}$, again denoted by ϕ. In the case $L_0 = \mathbb{A}_2^2$, $k = 4$, and ϕ is already determined by these conditions: the only possibility is $\phi(x_1 e_1) = x_1 e_3$. In the case $L_0 = \mathbb{E}_8$, we need to take into account the mutual scalar products of the elements of S_1. Since, for $1 \neq i \neq j \neq 1$, $\overline{b}(\epsilon_1 \pm \epsilon_i, \epsilon_1 \pm \epsilon_j) = 1$, we have $\forall x, x' \in {\mathbb{F}_2}^{k/2-1} \setminus \{0\} \mid x \neq x',\ x^t \phi(x') + {x'}^t \phi(x) = 1$. This set of affine conditions leaves eight solutions for ϕ, which are transitively permuted by changes of the base $\{e_1, \ldots, e_{k/2-1}\}$. One of them is:

$$
\begin{array}{rc}
x & \left\{\begin{array}{cccccccc} 0&0&0&0&1&1&1&1 \\ 0&0&1&1&0&0&1&1 \\ 0&1&0&1&0&1&0&1 \end{array}\right. \begin{array}{c} e_1 \\ e_2 \\ e_3 \end{array} \\
 & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\phi(x) & \left\{\begin{array}{cccccccc} 0&0&0&1&1&1&1&0 \\ 0&0&1&1&1&0&0&1 \\ 0&1&1&0&1&0&1&0 \end{array}\right. \begin{array}{c} e_5 \\ e_6 \\ e_7 \end{array} \\
 & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
C_i & \begin{array}{cccccccc} 1&2&4&6&8&5&7&3 \end{array}
\end{array}
$$

where each column contains $x \in {\mathbb{F}_2}^{k/2-1}$ and $\phi(x)$.

Lemma 4.9 *For all $t \in S_3$, there is a unique $s \in S_1$ such that $t = s + l_1$, where $l_1 \in L_1$ and $p_1(l_1) \notin \mathbb{F}_2 e_{k/2}$.*

Proof: In both cases, since $x \in L_1$, the vectors $2\epsilon_i$ belong to L_1 for all i. Since $b(x,y) \in 2\mathbb{Z}$ for all $x, y \in L_1$, we have the inclusion $L_1 \subset \oplus_{i=1}^{k} \mathbb{Z}\epsilon_i$. Then, from the isometries $L_1 \sim \sqrt{2}L_0$:
If $L_0 = \mathbb{A}_2^2$, $\forall\, i = 3, 4, \exists!\, j(i) \in \{1,2\} \mid \epsilon_i \pm \epsilon_{j(i)} \in L_1$. Clearly $\epsilon_i \pm \epsilon_{j(i)} \not\equiv 2\epsilon_i \pmod{2L_0}$.
If $L_0 = \mathbb{E}_8$, $\forall 1 \leq i \neq j \neq l \leq 8, \exists!\, s = s(i,j,l) \mid \epsilon_i \pm \epsilon_j \pm \epsilon_l \pm \epsilon_s \in L_1$. (The unicity of s in this case comes from the fact that the words of the Hamming code form a 3-design ([MWS 77]).) Again, $\epsilon_i \pm \epsilon_j \pm \epsilon_l \pm \epsilon_s \not\equiv 2\epsilon_i \pmod{2L_0}$. □

Now we conclude in the case $L_0 = \mathbb{A}_2^2$: if Y has nine coordinates in S_1 and one in S_3, say Y_{i_0}, from Lemma 3.4, $Y_{i_0} = s + l_1$, with $p_1(l_1) \notin \mathbb{F}_2 e_2$. Then $Y = e_1 \otimes u_1 + e_2 \otimes u_2 + e_3 \otimes u_3 \pmod{2L_0}$ with $u_1, u_2 \in C$ and $u_3 \in C^\perp$; the determination of ϕ shows that $u_1 = u_3$ up to the coordinate i_0 which is different since $p_1(l_1) \notin \mathbb{F}_2 e_2$. Hence they cannot be even at the same time.

Let $L_0 = \mathbb{E}_8$ and $Y = \sum_{i=1}^{7} e_i \otimes u_i$, with $u_1, \ldots, u_4 \in C$ and $u_5, \ldots u_7 \in C^\perp$. We arrange the elements of ${\mathbb{F}_2}^3$ in the lexicographic order:
${\mathbb{F}_2}^3 = \{C_1, C_2, \ldots, C_8\}$, $C_1 = (0,0,0)$, $C_2 = (0,0,1)$, $C_3 = (0,1,0)$,…,$C_8 = (1,1,1)$ and set, for $1 \leq i \leq 8$, $A_i = \{j \mid (u_{5,j}, u_{6,j}, u_{7,j}) = C_i\}$. Moreover, we set $a_i = \mathrm{card}(A_i) \pmod 2$. Then, the determination of ϕ in this case shows that, up to the coordinate i_0 where $Y_{i_0} \in S_3$, we have for $i = 1, 2, 3$, $u_i = v_i$, where:

$$\begin{cases} v_1 &= A_3 \cup A_5 \cup A_6 \cup A_8 \\ v_2 &= A_3 \cup A_4 \cup A_6 \cup A_7 \\ v_3 &= A_2 \cup A_3 \cup A_5 \cup A_7 \end{cases}$$

More precisely, since C is even, $u_i = v_i$ if and only if v_i is even.
Case 1: $u_5.u_6 = 0$. Then, from the parity of $C^\perp$,

$$\begin{cases} a_1 + a_2 = 0 \\ a_3 + a_4 = 0 \\ a_5 + a_6 = 0 \\ a_7 + a_8 = 0 \\ a_1 + a_3 + a_5 + a_7 = 0 \end{cases}$$

and $wt(v_3) \equiv a_2 + a_3 + a_5 + a_7 = a_1 + a_2 = 0 \pmod 2$, which shows that the component of $p_1(l_1)$ over e_3 is zero and hence that $v_3 \in C$. Then the scalar product of this word with u_5, u_6, u_7 must be zero which leads to the additional conditions:

$$\begin{cases} a_5 + a_7 = 0 \\ a_3 + a_7 = 0 \\ a_2 = 0 \end{cases}$$

This implies that $a_i = 0$ for all $1 \leq i \leq 8$, which means that $p_1(l_1) \in \mathbb{F}_2 e_4$, in contradiction with Lemma 3.4.
Case 2: $u_5.u_6 = 1$. Now we have the conditions

$$\begin{cases} a_1 + a_2 = 1 \\ a_3 + a_4 = 1 \\ a_5 + a_6 = 1 \\ a_7 + a_8 = 1 \\ a_1 + a_3 + a_5 + a_7 = 0 \end{cases}$$

which imply

$$\begin{cases} wt(v_1) \equiv a_3 + a_7 \pmod 2 \\ wt(v_2) \equiv a_5 + a_7 \pmod 2 \\ wt(v_3) \equiv a_1 + a_2 = 1 \pmod 2 \end{cases}$$

If $a_3 + a_7 = 0$, then $v_1 \in C$ which is in contradiction with $v_1.u_6 = a_3 + a_8 = 1$.
If $a_5 + a_7 = 0$, then $v_2 \in C$ which is in contradiction with $v_2.u_5 = a_6 + a_7 = 1$.

If $a_3 + a_7 = a_5 + a_7 = 1$, since $v_3.u_5 = a_5 + a_7 = 1$ and $v_3.u_6 = a_3 + a_7 = 1$, $i_0 \in A_7$ and $v_3.u_7 = a_2 = 0$. Then $a_2 = a_3 = a_5 = a_8 = 0$ and $a_1 = a_4 = a_6 = a_7 = 1$. But $v_1 + v_2 \in C$ which is in contradiction with $(v_1 + v_2).u_5 = a_5 + a_7 + a_8 = 1$. □

The group $S := Stab_{Aut(L_{\mathcal{C}})}(L')$ acts on the set of maximal totally singular subspaces B of L''/L' which are complements of $L_{\mathcal{C}}/L'$, as defined in Theorem 4.7. From Proposition 4.6(ii), L''/L' is a non-singular $\mathbb{F}_2$-quadratic space of dimension $k = dim(L_0)$ and Witt defect 0. Let $k = 2m$; there are $2^{m(m-1)/2}$ such subspaces B. If L_0 is one of $\mathbb{Z}[\alpha]$, $\mathbb{A}_2^2$, or $\mathbb{E}_8$ we find using the notation of Theorem 4.7.

Proposition 4.10 *(i) If $L_0 = \mathbb{Z}[\alpha]$, then B, hence $\Lambda(B)$, is unique and $\Lambda(B)$ is isometric to L_{20}.*

(ii) If $L_0 = \mathbb{A}_2^2$, then the two subspaces B lie in one orbit under the action of S. Hence also in this case one gets a unique lattice $\Lambda(B)$, which is isometric to L_{40}.

(iii) If $L_0 = \mathbb{E}_8$, the 64 subspaces B fall into 2 orbits under the action of S of length 8 and 56 with representatives say B and B'. The two lattices $\Lambda(B) \cong L_{80}$ and $\Lambda(B')$ are non isometric.

Proof: The group $S_0 := Aut(L_0) \cap Aut(L_1) \cap Aut(L_2)$ acts on the set of maximal totally singular subspaces of $L_1/2L_1$ which are complements of $2L_0/2L_1$. They correspond bijectively to the set of subspaces B as in Theorem 4.7. by the isometry $\psi : L''/L' \to L_1/2L_1$ as defined in Proposition 4.6. (ii). The action of S_0 is induced by the action of a subgroup of S on L''/L'. One calculates $S_0 = \{\pm 1\}$, $D_8 \leftthreetimes S_3$, resp. $2.Alt_8$ and the decomposition of the set of $\psi(B)$ into 1, 1, resp. 2 orbits under S_0 of lengths 1, 2, resp. 8 and 56. The stabilizers of representatives of the last two orbits are the two maximal subgroups $2.Alt_7$ resp. $(SL_2(5) \times C_3).2$ of $2.Alt_8$. To show the proposition, we have to show that the lattices defined by the latter two subspaces B are non isometric and that the lattices L_{20}, L_{40}, and L_{80} as defined in the Introduction are of the form $\Lambda(B)$.

The explicit description of the lattice L_{20} given in [CCNPW 85] shows that L_{20} is isometric to the lattice Λ of ([Bac 97], Theorem 6.4), which clearly satisfies the conditions of Theorem 4.7. (with the notations of [Bac 97],

$L' = L_C^e$). Let us denote by a superscript $^{(20)}$ the previous constructions when applied to the first case $L_0 = \mathbb{Z}[\alpha]$. It was already noticed that, for the three cases $L_0 = \mathbb{Z}[\alpha]$, $\mathbb{A}_2^2$, $\mathbb{E}_8$,

$$\mathcal{C} = L_0/2L_0 \otimes_{\mathbb{F}_2 \times \mathbb{F}_2} \mathcal{C}^{(20)}.$$

Hence we also have

$$L_{\mathcal{C}} \simeq L_0 \otimes_{\mathbb{Z}[\alpha]} L_{\mathcal{C}}^{(20)}$$

and clearly

$$L' \simeq L_0 \otimes_{\mathbb{Z}[\alpha]} L'^{(20)}.$$

Then, if L_{20} defines the maximal self-orthogonal subspace $B^{(20)}$ of $L''^{(20)}/L'^{(20)}$, the even lattice $L_0 \otimes_{\mathbb{Z}[\alpha]} L_{20}$ defines the maximal self-orthogonal subspace $B = L_0/2L_0 \otimes_{\mathbb{F}_2 \times \mathbb{F}_2} B^{(20)} \subset L_0/2L_0 \otimes_{\mathbb{F}_2 \times \mathbb{F}_2} L''^{(20)}/L'^{(20)} \simeq L''/L'$ (notice that this is the 2-torsion part of $(L')^*/L'$) which is a complement of $L_{\mathcal{C}}/L'$. Therefore the lattices L_{20}, L_{40}, and L_{80} are isometric to $\Lambda(B)$ in the respective cases.

It remains to consider the dimension 80. The lattice L_{80} corresponds to the orbit of length 8 with stabilizer $2.Alt_7 = Aut_{\mathbb{Z}[\alpha]}(L_0)$. Since the stabilizer of a representative B' of the orbit of length 56 has endomorphism ring $\cong \mathbb{Z}[\beta := \frac{-1+\sqrt{-15}}{2}]$, it is natural to construct the lattice $M_{80} := \Lambda(B')$ replacing $\mathbb{Z}[\alpha]$ by $\mathbb{Z}[\beta]$.

Let $L_{\mathcal{C}}$ be the $\mathbb{Z}[\beta]$-lattice in $\mathbb{Q}[\beta]^{10}$ constructed as in Proposition 4.1. from $L_0 = \mathbb{Z}[\beta]$, $L_0/2L_0 = \wp/(2) \oplus \overline{\wp}/(2)$, and the binary code of Lemma 4.4, where $\wp := (\beta, 2)$ is a prime ideal of $\mathbb{Z}[\beta]$ containing 2. Let

$$M_{20} := \{(x_1, \ldots, x_{10}) \in L_{\mathcal{C}} \mid \sum x_i \in 2\wp\} + \frac{\wp^2}{2}(1, \ldots, 1).$$

Lemma 4.11 *(i) The lattice M_{20} is a $\mathbb{Z}[\beta]$-unimodular lattice which as $\mathbb{Z}$-lattice has minimum 8, 180 minimal vectors, and automorphism group $Aut_{\mathbb{Z}}(M_{20}) = Aut_{\mathbb{Z}[\beta]}(M_{20}) = 2^5 : S_6$ (a maximal subgroup of $2.M_{22}.2$).*

(ii) Let $M_{80} := M_{20} \otimes_{\mathbb{Z}[\beta]} \mathbb{E}_8$, where $Aut_{\mathbb{Z}[\beta]}(\mathbb{E}_8) = (SL_2(5) \times C_3).2$ as above. Then M_{80} is an even unimodular lattice not isometric to L_{80}.

Proof: (i) May be calculated with the computer ([PlS 97]). Note that the minimal vectors of M_{20} are up to permutation of the coordinates the vectors

$(\pm 2, \pm 2, 0, \ldots, 0) \in 2\mathbb{Z}[\beta]^{10}$. In particular, the automorphism group of M_{20} fixes $L_{\mathcal{C}}$. This can be seen from the fact that the weight w to be defined on $L_0/2L_0$ in order to satisfy the equality of Lemma 4.3. takes the values 0, 1, 4 (cf. Definition 4.2) since the ideal $\wp$ is not principal. Hence one can show that the minimum $\min(L_{\mathcal{C}} \setminus 2\mathbb{Z}[\beta]^{10})$ is 10.
(ii) M_{80} is clearly an even unimodular lattice. By construction its automorphism group contains the subgroup $(SL_2(5) \otimes C_3).2 \otimes 2^5.S_6$, which is not a subgroup of $Aut(L_{80}) = 2.Alt_7 \otimes_{\mathbb{Z}[\alpha]} 2.M_{22}.2$ (cf. [CCNPW 85]). Therefore M_{80} is not isometric to L_{80}. □

As above one now concludes that M_{80} is of the form $\Lambda(B')$ and hence of minimum 8 by Theorem 4.7. Since M_{80} is not isometric to L_{80}, the subspace $B' \leq L''/L'$ belongs to a second orbit (of length 56) under S. □

References

[Bac 97] C. Bachoc, *Applications of coding theory to the construction of modular lattices.* J. Comb. Theory, Series A **78** (1997), 92-119

[CCNPW 85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *Atlas of finite groups.* Oxford University Press 1985

[BQS 95] C. Batut, H-G. Quebbemann, R. Scharlau, *Computations of cyclotomic lattices.* Exp. Math. vol. 4, no 3 (1995) 175-179

[CoS 88] J. H. Conway, N. J. A. Sloane, *Sphere Packings, Lattices, and Groups.* Springer-Verlag 1988

[Gro 90] B. Gross, *Group representations and Lattices.* J. AMS **3** (1990), 929-960

[Gro 96] B. Gross, *Groups over* $\mathbb{Z}$. Invent. Math. **124** (1996), 263-279

[Hup 67] B. Huppert, *Endliche Gruppen I.* Springer-Verlag (1967)

[JLPW 95] C. Jansen, K. Lux, R. A. Parker, R. A. Wilson, *An atlas of Brauer Characters.* Clarendon Press, Oxford 1995

[LaS 74] V. Landazuri, G.M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups.* J. Algebra **32** (1974), 418-443

[MWS 77] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes.* North-Holland Mathematical library (1977)

[Neb 95] G. Nebe, *Endliche rationale Matrixgruppen vom Grad 24.* Dissertation, RWTH Aachen (1995), Aachener Beiträge zur Mathematik **12**, Verlag der Augustinus Buchhandlung Aachen (1995)

[Neb 96] G. Nebe, *Finite rational matrix groups of degree 24.* Exp. Math. vol.5, no 3 (1996), 163-191

[Neb 97] G. Nebe, *Some cyclo-quaternionic lattices.* J. Algebra (to appear)

[NeP 95] G. Nebe, W. Plesken, *Finite rational matrix groups of degree 16.* AMS-Memoirs, vol. 116, No 556 (1995)

[PlN 95] W. Plesken, G. Nebe, *Finite rational matrix groups.* AMS-Memoirs, vol. 116, No 556 (1995)

[PlS 97] W. Plesken, B. Souvignier, *Computing isometries of lattices.* J. Symb. Computation 24, no 3-4 (1997)

[Que 84] H.-G. Quebbemann, *A construction of integral lattices.* Mathematika **31** (1984), 138-141

[Que 95] H.-G. Quebbemann, *Modular Lattices in Euclidean Spaces.* J. Number Theory **54** (1995), 190-202

[Sch 93] R. Schulze-Pillot, *Quadratic residue codes and cyclotomic lattices.* Arch. Math. **60** (1993), 40-45

[SeZ 93] G. M. Seitz, A. E. Zalesskii, *On the minimal degrees of projective representations of the finite Chevalley Groups II.* J. Algebra **158** (1993), 233-243

[Shi 91] T. Shioda, *Mordell-Weil lattices and sphere packings.* Amer. J. Math. 113 (1991), 931-948

C. Bachoc, Laboratoire d'Algorithmique Arithmétique,
351, cours de la Libération, F-33405 Talence
bachoc@math.u-bordeaux.fr

G. Nebe, Lehrstuhl B für Mathematik, RWTH Aachen,
Templergraben 64, D-52062 Aachen
gabi@math.rwth-aachen.de