# An even unimodular 72-dimensional lattice of minimum 8.

Gabriele Nebe

Lehrstuhl D für Mathematik, RWTH Aachen University
52056 Aachen, Germany
nebe@math.rwth-aachen.de

ABSTRACT. An even unimodular 72-dimensional lattice $\Gamma$ having minimum 8 is constructed as a tensor product of the Barnes lattice and the Leech lattice over the ring of integers in the imaginary quadratic number field with discriminant $-7$. The automorphism group of $\Gamma$ contains the absolutely irreducible rational matrix group $(\mathrm{PSL}_2(7) \times \mathrm{SL}_2(25)) : 2$.
Keywords: extremal even unimodular lattice, Hermitian tensor product.
MSC: primary: 11H06, secondary: 11H31, 11H50, 11H55, 11H56, 11H71

## 1 Introduction.

In this paper a lattice $(L, Q)$ is always an even positive definite lattice, i.e. a free $\mathbb{Z}$-module $L$ equipped with a quadratic form $Q : L \to \mathbb{Z}$ such that the bilinear form

$$(\cdot, \cdot) : L \times L \to \mathbb{Z}, (x, y) := Q(x + y) - Q(x) - Q(y)$$

is positive definite on the real space $\mathbb{R} \otimes L$. The dual lattice is

$$L^{\#} := \{x \in \mathbb{R} \otimes L \mid (x, \ell) \in \mathbb{Z} \text{ for all } \ell \in L\}$$

and $L$ is called unimodular, if $L = L^{\#}$. The minimum of $L$ is twice the minimum of the quadratic form on the non-zero vectors of $L$

$$\min(L) = \min(L, Q) = \min\{(\ell, \ell) \mid 0 \neq \ell \in L\}.$$

From the theory of modular forms it is known ([23], [12]) that the minimum of an even unimodular lattice of dimension $n$ is always $\leq 2\lfloor \frac{n}{24} \rfloor + 2$. Lattices achieving this bound are called extremal. Of particular interest are extremal unimodular lattices in the so called "jump dimensions", these are the multiples of 24. There are four even unimodular lattices known in the jump dimensions, the Leech lattice $\Lambda$, the unique even unimodular lattice in dimension 24 without roots, and three lattices called $P_{48p}$, $P_{48q}$, $P_{48n}$, of dimension 48 which have minimum 6 [4], [16].

It was a long standing open problem whether there exists an extremal 72-dimensional unimodular lattice ([21, p. 151], [20, Section 3.4]). Many people tried to construct such a lattice, or to prove its non-existence. Most of these attempts are not documented, all constructed lattices contained vectors of norm 6. In [1] Christine Bachoc and I discovered two extremal lattices in dimension 80 of which we could prove extremality using a classical construction that we learned from [18]. Given a binary code $C \leq \mathbb{F}_2^d$ and an even lattice $L \leq \mathbb{R}^n$ of odd determinant together with a polarisation $L/2L = T_1 \oplus T_2$ by isotropic subspaces the new lattice $\mathcal{L}(T_1, T_2, C)$ of dimension $dn$ is constructed as the preimage in $L^d$ of $T_1 \otimes C \oplus T_2 \otimes C^{\perp} \leq (L/2L)^d$. Inspired by [5] Christine and I used polarisations coming from Hermitian $\mathbb{Z}[\alpha]$-structures (where $\alpha^2 - \alpha + 2 = 0$) of $L$.

Bob Griess' article [6] analyses this construction for certain polarisations of the Leech lattice $\Lambda$ and $C = \langle (1,1,1) \rangle \leq \mathbb{F}_2^3$ for which he describes a strategy to prove extremality of the resulting lattice. This motivated me to try the nine $\mathbb{Z}[\alpha]$-structures of $\Lambda$ calculated in [8]. I computed the minimum of all nine 72-dimensional lattices using four different strategies: A combination of lattice reduction programs applied directly to the 72-dimensional lattice found vectors of norm 6 for all but one lattice. I then went on to compute the super offenders as described in [6, Section 4] and computed the number of norm 6 vectors in the lattices as given in Table 1. Using the $\mathbb{Z}[\alpha]$ structure of $\Lambda$ this computation may be reduced to a computation within the set of minimal vectors of the Leech lattice. The result of these computations agreed with the ones applying the methods described in Section 4.

Using the explicit matrices for this extremal lattice $\Gamma$ and the action of the subgroup $G$ of $\mathrm{Aut}(\Gamma)$ as constructed in Section 2 Mark Watkins (personal communication) succeeded in listing representatives of all $G$-orbits of the vectors of norm 8 in $\Gamma$ using the method described in [22]. From the stored information one verifies that $\Gamma$ has $6,218,175,600$ minimal vectors which gives an independent proof of the extremality of $\Gamma$ (see also Theorem 3.3 for an explicit description of the kissing configuration of $\Gamma$).

## 2 An Hermitian tensor product construction of $\Gamma$.

Throughout the paper let $\alpha$ be a generator of the ring of integers $\mathbb{Z}[\alpha]$ in the imaginary quadratic number field of discriminant $-7$, with $\alpha^2 - \alpha + 2 = 0$ and $\beta := \overline{\alpha} = 1 - \alpha$ its complex conjugate. Then $\mathbb{Z}[\alpha]$ is a principal ideal domain and $(\alpha)$ and $(\beta)$ are the two maximal ideals of $\mathbb{Z}[\alpha]$ that contain 2.

Let $(P, h)$ be an Hermitian $\mathbb{Z}[\alpha]$-lattice, so $P$ is a free $\mathbb{Z}[\alpha]$-module and $h : P \times P \to \mathbb{Z}[\alpha]$ a positive definite Hermitian form. One example of such a lattice is the Barnes lattice

$$P_b = \langle (\beta, \beta, 0), (0, \beta, \beta), (\alpha, \alpha, \alpha) \rangle = \langle (1, 1, \alpha), (0, \beta, \beta), (0, 0, 2) \rangle \leq \mathbb{Z}[\alpha]^3$$

with the half the standard Hermitian form

$$h : P_b \times P_b \to \mathbb{Z}[\alpha], h((a_1, a_2, a_3), (b_1, b_2, b_3)) = \frac{1}{2} \sum_{i=1}^{3} a_i \overline{b_i}.$$

Then $P_b$ is Hermitian unimodular, $P_b = P_b^* := \{v \in \mathbb{Q}P_b \mid h(v, \ell) \in \mathbb{Z}[\alpha] \text{ for all } \ell \in P_b\}$. The automorphism group of the $\mathbb{Z}[\alpha]$-lattice $P_b$ is isomorphic to $\pm \mathrm{PSL}_2(7)$

$$\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_b) := \{g \in \mathrm{GL}(P_b) \mid h(gv, gw) = h(v, w) \text{ for all } v, w \in P_b\} \cong \pm \mathrm{PSL}_2(7).$$

From any such Hermitian $\mathbb{Z}[\alpha]$-lattice $(P, h)$ one obtains an even $\mathbb{Z}$-lattice

$$L(P, h) := (L, (,)) := (P, \mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}} \circ h)$$

by restricting scalars. Since $h$ is Hermitian $h(\ell,\ell)\in\mathbb{Z}=\mathbb{Z}[\alpha]\cap\mathbb{R}$ for all $\ell\in P$ and hence

$$Q(\ell):=\frac{1}{2}\mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(h(\ell,\ell))=h(\ell,\ell)\in\mathbb{Z}.$$

The dual lattice of $L(P,h)$ is the product of $P^*$ with the different of $\mathbb{Z}[\alpha]$:

$$L(P,h)^{\#}:=\{v\in\mathbb{Q}P\mid \mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(h(\ell,v))\in\mathbb{Z}\text{ for all }\ell\in P\}=\frac{1}{\sqrt{-7}}P^*.$$

Michael Hentschel [8] classified all Hermitian $\mathbb{Z}[\alpha]$-structures on the even unimodular $\mathbb{Z}$-lattices of dimension 24 using the Kneser neighbouring method [10] to generate the lattices and checking completeness with the mass formula. In particular there are exactly nine such $\mathbb{Z}[\alpha]$ structures $(P_i,h)$ $(1\le i\le 9)$ such that $(P_i,\frac{1}{7}\mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}}\circ h)\cong\Lambda$ is the Leech lattice. The 36-dimensional Hermitian $\mathbb{Z}[\alpha]$-lattice $R_i$ is defined as

$$(R_i,h):=P_b\otimes_{\mathbb{Z}[\alpha]}P_i,\ \text{so}\ \mathrm{Aut}_{\mathbb{Z}[\alpha]}(R_i)\supseteq \mathrm{PSL}_2(7)\times\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_i).$$

**Definition 2.1.** For $1\le i\le 9$ let $(\Gamma_i,(,)):=L(R_i,\frac{1}{7}h):=(R_i,\frac{1}{7}\mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}}\circ h)$ where the quadratic form is $Q(\ell)=\frac{1}{14}\mathrm{trace}_{\mathbb{Z}[\alpha]/\mathbb{Z}}(h(\ell,\ell))$ for all $\ell\in\Gamma_i=R_i$.

All $\Gamma_i$ are even unimodular lattices of dimension 72.

The table below lists these nine Hermitian structures of the Leech lattice. The first column gives the structure of the automorphism group $\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_i)$ followed by its order and then the number of vectors of norm 6 in the lattice $\Gamma_i$ (computed in Section 4 below).

Table 1

| | group | order | norm 6 vectors |
|---|---|---|---|
| 1 | $\mathrm{SL}_2(25)$ | $2^4 3\cdot 5^2 13$ | 0 |
| 2 | $2.A_6\times D_8$ | $2^7 3^2 5$ | $2\cdot 20,160$ |
| 3 | $\mathrm{SL}_2(13).2$ | $2^4 3\cdot 7\cdot 13$ | $2\cdot 52,416$ |
| 4 | $(\mathrm{SL}_2(5)\times A_5).2$ | $2^6 3^2 5^2$ | $2\cdot 100,800$ |
| 5 | $(\mathrm{SL}_2(5)\times A_5).2$ | $2^6 3^2 5^2$ | $2\cdot 100,800$ |
| 6 | soluble | $2^9 3^3$ | $2\cdot 177,408$ |
| 7 | $\pm\mathrm{PSL}_2(7)\times(C_7:C_3)$ | $2^4 3^2 7^2$ | $2\cdot 306,432$ |
| 8 | $\mathrm{PSL}_2(7)\times 2.A_7$ | $2^7 3^3 5\cdot 7^2$ | $2\cdot 504,000$ |
| 9 | $2.J_2.2$ | $2^9 3^3 5^2 7$ | $2\cdot 1,209,600$ |

**Remark 2.2.** (a) The groups number 1, 3, 4, 5, and 9 are maximal finite quaternionic matrix groups with endomorphism algebra the definite quaternion algebra with center $\mathbb{Q}$ and discriminant $5^2$ $(1,4,5,9)$ resp. $13^2$ (group number 3) (see [17]). For the group number 4 resp. 5, the endomorphism ring of the lattice is not the maximal order.
(b) The group number 8 is a maximal finite symplectic matrix group over $\mathbb{Q}[\alpha]$ as defined in [9], it is globally irreducible in the sense of [7].
(c) The groups number 2 and 7 are reducible.

The Hermitian structures number 4 and 5 are just Galois conjugate to each other, whereas all the others are Galois invariant. For these seven lattices the automorphism group of the $\mathbb{Z}$-lattice $\Gamma_i$ hence contains an extension of $\mathrm{Aut}_{\mathbb{Z}[\alpha]}(R_i)$ by the Galois automorphism. For the extremal lattice $\Gamma:=\Gamma_1$ this is a split extension.

**Theorem 2.3.** *The lattice* $\Gamma$ *is an extremal even unimodular lattice of dimension* 72*. Its automorphism group* $\mathrm{Aut}(\Gamma)$ *contains the subgroup* $\mathcal{U} := (\mathrm{PSL}_2(7) \times \mathrm{SL}_2(25)) : 2$*.*

Two proofs that the minimum of $\Gamma$ is 8 are given below.

**Remark 2.4.** The natural $\mathbb{C}\mathcal{U}$-module $\mathbb{C}\otimes\Gamma$ contains no $\mathcal{U}$-invariant submodules, so $\mathrm{Aut}(\Gamma)$ is an absolutely irreducible subgroup of $\mathrm{GL}_{72}(\mathbb{Q})$. In fact $\mathcal{U}$ is almost a globally irreducible representation in the sense of [7]. More precisely $\mathbb{F}_p \otimes \Gamma$ is also absolutely irreducible except for $p = 5$ and $p = 7$, where the module has a unique non-trivial submodule, which is of dimension 36. For both primes $p = 5$ and $p = 7$ there is an element $x_p \in N_{\mathrm{GL}_{72}(\mathbb{Q})}(\mathcal{U})$, the rational normaliser of $\mathcal{U}$, mapping $\Gamma$ to the unique sublattice of index $p^{36}$, which is therefore isometric to $(\Gamma, pQ)$ (see [14]). Therefore $\mathrm{Aut}(\Gamma)$ is a maximal finite subgroup of $\mathrm{GL}_{72}(\mathbb{Q})$.

**Remark 2.5.** Since $\mathrm{Aut}(\Gamma)$ contains an element of order 91 the lattice $\Gamma$ is an ideal lattice in the cyclotomic field $\mathbb{Q}[\exp(2\pi i/91)]$ in the sense of [2]. It would be interesting to determine the ideal class of this lattice.

## 2.1 An elementary linear algebra construction.

This section just repeats the construction above in elementary linear algebra (understood by computer algebra systems).

Let $(b_1, \ldots, b_{24})$ be a $\mathbb{Z}$-basis of the Leech lattice $\Lambda$ and $F := ((b_i, b_j)) \in \mathbb{Z}^{24\times 24}_{sym}$ denote its Gram matrix. Then an Hermitian structure over $\mathbb{Z}[\alpha]$ is given by a matrix $A \in \mathbb{Z}^{24\times 24}$ such that $AFA^{tr} = 2F$ and the $F$-adjoint $FA^{tr}F^{-1} = 1 - A =: B$. Mapping $\alpha$ to the right multiplication by $A$ then defines the Hermitian $\mathbb{Z}[\alpha]$-structure on the $\mathbb{Z}$-lattice $\Lambda$.

That there are exactly nine such $\mathbb{Z}[\alpha]$ structures of the Leech lattice means that there are nine such matrices $A_1, \ldots, A_9$ up to conjugation under the automorphism group of $\Lambda$.

For any of these nine structures the even unimodular lattice $\Gamma_i$ of dimension 72 is constructed as a sublattice of $\Lambda \perp \Lambda \perp \Lambda$ with Gram matrix $\frac{1}{2}\,\mathrm{diag}(F, F, F)$ generated by the rows of the block matrix

$$\begin{pmatrix} A_i & A_i & A_i \\ B_i & B_i & 0 \\ 0 & B_i & B_i \end{pmatrix} \text{ or equivalently } \begin{pmatrix} 1 & 1 & A_i \\ 0 & B_i & B_i \\ 0 & 0 & 2 \end{pmatrix} =: T_i$$

If $U$ denotes the subgroup of $\mathrm{GL}_{72}(\mathbb{Z})$ obtained by replacing $\alpha$ by $A_i$ in the group $\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_b) \le \mathrm{GL}_3(\mathbb{Z}[\alpha])$ isomorphic to $\mathrm{PSL}_2(7)$ then $\mathrm{Aut}(\Gamma_i)$ contains the matrix group

$$\langle \{\mathrm{diag}(g, g, g) \mid g \in \mathrm{Aut}(\Lambda), gA_i = A_i g\} \cup U \rangle \cong \mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_i) \times \mathrm{PSL}_2(7).$$

A matrix for the additional Galois automorphism with respect to the basis given by $T_i$ above can be constructed from an isometry

$$Y_i \in \mathrm{GL}_{24}(\mathbb{Z}), \quad Y_i F Y_i^{\mathrm{tr}} = F, \quad Y_i A_i Y_i^{-1} = B_i$$

(this only exists for $i \neq 4, 5$) as the block matrix

$$\begin{pmatrix} Y_i & -Y_i & A_i Y_i \\ 0 & -B_i Y_i & Y_i \\ -AY_i & 0 & Y_i \end{pmatrix}.$$

The shape of the matrix was obtained from an isometry between $(P_b, h)$ and $(P_b, \overline{h})$.

## 2.2 A classical coding theory construction.

The lattices $\Gamma_i$ can be obtained using a special case of a classical construction with codes: If $(L, Q)$ is an even unimodular lattice, then $L/2L$ becomes a non-degenerate quadratic space over $\mathbb{F}_2$ with quadratic form $q(\ell+2L) := Q(\ell)+2\mathbb{Z}$. This has Witt defect 0, so there are totally isotropic subspaces $U, V \leq (L/2L, q)$ such that $L/2L = U \oplus V$. Let $2L \leq M, N \leq L$ denote the preimages of $U, V$, respectively. Then $(M, \frac{1}{2}Q)$ and $(N, \frac{1}{2}Q)$ are again even unimodular lattices.

**Definition 2.6.** *([6], [18, Construction I])* Given such a polarisation $(M, N)$ of the even unimodular lattice $(L, Q)$ and some $k \in \mathbb{N}$ let

$$L(M, N, k) := \{(x_1+y, x_2+y, \ldots, x_k+y) \mid y \in N, x_1, \ldots, x_k \in M \text{ and } x_1+\ldots+x_k \in M \cap N\}.$$

Then the lattice $(L(M, N, k), \tilde{Q})$ is an even unimodular lattice ([18, Proposition]) where

$$\tilde{Q}(x_1 + y, x_2 + y, \ldots, x_k + y) := \frac{1}{2} \sum_{i=1}^{k} Q(x_i + y).$$

Of particular interest for this paper is the case where $k = 3$.

**Lemma 2.7.** *Let $(N, M)$ be a polarisation of $L$ modulo 2 and assume that $d = \min(L, Q) = \min(N, \frac{1}{2}Q) = \min(M, \frac{1}{2}Q)$. Then*

$$\lceil \frac{3d}{2} \rceil \leq \min(L(M, N, 3), \tilde{Q}) \leq 2d.$$

Proof. Let $\lambda = (a, b, c) \in L(M, N, 3)$. According to the number of non-zero components one gets up to permutation:
**1)** One non-zero component: Then $\lambda = (a, 0, 0)$ with $a = 2\ell \in 2L$ so

$$(\lambda, \lambda) = 2\tilde{Q}(\lambda) = Q(2\ell) = 4Q(\ell) = 2(\ell, \ell) \geq 2d.$$

**2)** Two non-zero components: Then $\lambda = (a, b, 0)$ with $a, b \in N$ so $(\lambda, \lambda) = 2\tilde{Q}(\lambda) = Q(a) + Q(b) \geq 2d$.
**3)** Three non-zero components: Then $(\lambda, \lambda) = 2\tilde{Q}(\lambda) = Q(a) + Q(b) + Q(c) \geq \frac{3}{2}d$. □

If $(L, Q) \cong (N, \frac{1}{2}Q) \cong (M, \frac{1}{2}Q) \cong \mathbb{E}_8$ is the unique even unimodular lattice of dimension 8, then Lemma 2.7 immediately implies that $L(M, N, 3) \cong \Lambda$ is the Leech lattice (see [11]). Starting with the Leech lattice one obtains the following Remark.

**Remark 2.8.** *([6, Theorem 4.10])* Assume that $L = \Lambda \cong (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q)$ is the Leech lattice. Then $L(M, N, 3)$ has minimum 6 or 8. The vectors of norm 6 in $L(M, N, 3)$ are of the form $(w + x, w + y, w + z)$ with $w \in N$, $x, y, z \in M$, $x + y + z \in 2\Lambda$ and $Q(w + x) = Q(w + y) = Q(w + z) = 2$.

If the sublattices $M$ and $N$ are defined by an Hermitian structure of $L$ as in Section 2, then the lattice $L(M, N, 3)$ is an Hermitian tensor product as one easily sees from the explicit basis of the Barnes lattice given in Section 2.

**Remark 2.9.** Assume that the lattice $L$ has an Hermitian structure over $\mathbb{Z}[\alpha]$ as defined in Section 2. Then $M := \alpha L$ and $N := \beta L$ defines a polarisation of $L$ such that $L(M, N, 3) \cong P_b \otimes_{\mathbb{Z}[\alpha]} L$.

## 3 The vectors of norm 6 and 8 in $L(M,N,3)$.

Let $(\Lambda, Q)$ be the Leech lattice and fix a polarisation $(M,N)$ of $\Lambda$ such that $(M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda$.

The following property of the Leech lattice is well known.

**Lemma 3.1.** *The nontrivial classes of $\Lambda/2\Lambda$ are represented by vectors $v \in \Lambda$ of norm $(v,v) = 4, 6$ and $8$. In particular all classes of $M/2\Lambda$ and $N/2\Lambda$ are represented by vectors of norm $8$. If $K = v + 2\Lambda$ contains a vector of norm $8$, then $\{k \in K \mid (k,k) \leq 8\} = \{\pm k_1, \ldots, \pm k_{24}\}$ with $(k_i, k_j) = 8\delta_{ij}$. If $K = v + 2\Lambda$ contains a vector $v$ of norm $4$ or $6$ then $\{k \in K \mid (k,k) \leq 8\} = \{\pm v\}$.*

Proof. Let $(v,v) = 4$ or $(v,v) = 6$ and assume that there is some $\pm v \neq k \in v + 2\Lambda$ such that $(k,k) \leq 8$. Then one of $v \pm k \in 2\Lambda$ has norm $\leq 6 + 8 < 16 = \min(2\Lambda)$ which is a contradiction. Similarly one sees that for $(v,v) = 8$ the vectors of norm 8 in $v + 2\Lambda$ form a frame. Now

$$\frac{|\Lambda_4|}{2} + \frac{|\Lambda_6|}{2} + \frac{|\Lambda_8|}{48} = 2^{24} - 1$$

so all nonzero classes of $\Lambda/2\Lambda$ are represented by vectors of norm $\leq 8$. □

**Proposition 3.2.** *Fix some $w \in \Lambda \setminus M$ with $(w,w) = 8$. Then*

*(a) $W_3(w) := \{x \in M \mid Q(x+w) = 3\}$ has cardinality $2 \cdot 2048$.*

*(b) $W_2(w) := \{x \in M \mid Q(x+w) = 2\}$ has cardinality $2 \cdot 24$.
The set $\{x + w \mid x \in W_2(w)\}$ is the rescaled root system $24\mathbb{A}_1$.*

Proof. (a) If $x \in M$ such that $Q(w+x) = 3$ then the class $K_x := x + 2\Lambda$ is not perpendicular to $K_w$. Since $K_w \notin M/2\Lambda = (M/2\Lambda)^\perp$ there are $2^{11} = 2048$ classes $x + 2\Lambda \in M/2\Lambda$ that are not perpendicular to $K_w$. So there are 2048 possibilities for the class $K_{w+x} = K_x + K_w = (x+w) + 2\Lambda$. Such a class is necessarily anisotropic and therefore contains exactly 2 vectors of norm 6 by Lemma 3.1.
(b) Let $v_1 \neq \pm v_2 \in w + M$ with $(v_i, v_i) = 4$ $(i = 1,2)$. Then again $v_1 \pm v_2 \in M$ implies $(v_1, v_2) = 0$, and hence every class in $\Lambda/M$ contains at most 48 vectors of norm 4. Since $|\Lambda_4|/48 = 2^{12} - 1$ all non-zero classes in $\Lambda/M$ contain exactly 24 pairs of orthogonal vectors of norm 4. Now $W_2(w)$ is the set of minimal vectors in the class $w + M$ and therefore of cardinality 48. □

**Theorem 3.3.** *The vectors of norm 6 and 8 in $L(M,N,3)$ are of the form $(w+x, w+y, w+z)$ with $w \in M$, $x,y,z \in N$, $x+y+z \in 2\Lambda$ such that $Q(w+x) + Q(w+y) + Q(w+z) = 6$ or $8$. For norm 6 the only possibility is $Q(w+x) = Q(w+y) = Q(w+z) = 2$. Let $b_6$ denote the number of such vectors. For norm 8 one has the possible types*

*(a) $(8,0,0)$ with $196560 \cdot 3$ vectors.*

*(b) $(4,4,0)$ with $196560 \cdot 48 \cdot 3$ vectors.*

*(c) $(3,3,2)$ with $4095 \cdot 48 \cdot 2048 \cdot 2 \cdot 2 \cdot 3$ vectors.*

*(d)* $(4,2,2)$ *with* $4095 \cdot 48 \cdot 48 \cdot 48 \cdot 3 - 72b_6$ *vectors.*

Proof. Clearly these are the only possibilities for vectors of norm 6 or 8 in $L(M,N,3)$. The vectors of type $(8,0,0)$ correspond to the minimal vectors in the sublattice $2\Lambda \perp 2\Lambda \perp 2\Lambda$. The vectors of type $(4,4,0)$ are of the form $(x,y,0)$ with $x,y \in M$, $(x,x) = (y,y) = 8$ such that $x+2\Lambda = y+2\Lambda$, so one has 196560 possibilities for $x$ and for each such $x$ one may choose all 48 minimal vectors $y \in x+2\Lambda$. The additional factor 3 counts the possible permutations $(x,y,0), (x,0,y)$, and $(0,x,y)$.
**(c)** By Lemma 3.1 all anisotropic classes in $\Lambda/2\Lambda$ are represented by vectors of norm 6. For a fixed representative $w$ of one of the 4095 classes of $N/2\Lambda$ of norm $(w,w) = 8$ the vectors $z$ and $w$ run through all $z \in W_2(w)$ and $y \in W_3(w)$. Then the condition that $x+y+z \in 2\Lambda$ means that $w+x+2\Lambda = y+z+2\Lambda$, so $w+x$ is one of the 2 vectors of norm 6 in this anisotropic class.
**(d)** Again, fixing some $w$ as above the elements $y$ and $z$ are in $W_2(w)$. There are 48 possibilities of each of them. Then $w+x \in w+y+z+2\Lambda$ is in an isotropic class of $\Lambda/2\Lambda$. This class is either of minimum 4 or 8. If it has minimum 4, then there are 2 vectors of norm 4 in this class which give vectors of norm 6 in $L(M,N,3)$. It is has minimum 8, then there are 48 possibilities for $w+x$ such that $Q(w+x) = 4$. □

**Remark 3.4.** From Theorem 3.3 the number of vectors of norm 8 in $L(M,N,3)$ is $6,218,175,600 - 72b_6$, where $b_6$ is the number of norm 6 vectors in this lattice. This can also be seen from the theory of modular forms.

# 4 Two proofs that the minimum of $\Gamma$ is 8

## 4.1 Counting the norm 6 vectors in $L(M,N,3)$

Let $W := \{w_1, \ldots, w_{4095}\}$ denote a fixed set of representatives of the classes in $N/2\Lambda$ consisting of vectors of norm 8. The vectors of norm 6 in $\Gamma$ are of the form $(w+x, w+y, w+z)$ where $w \in W$, $x,y,z \in W_2(w)$ and $x+y+z \in 2\Lambda$.

**Remark 4.1.** To count the vectors of norm 6 and 8 in $\Gamma_i$ let $w \in W$ run through representatives of the $\mathrm{Aut}_{\mathbb{Z}[\alpha]}(P_i)$-orbits on $N/2\Lambda$.
For each such $w$ compute the set $W_2(w) = \{s - w \mid s \in \langle w, M\rangle, (s,s) = 4\}$. Then run through the pairs $(x,y) \in W_2(w) \times W_2(w)$ and compute the vectors of norm 4 in the lattice $\langle 2\Lambda, w+x+y\rangle$. This lattice either has two vectors of norm 4 contributing to the vectors of norm 6 in $\Gamma_i$ or it has minimum 8 and then it contains 48 vectors of norm 8 contributing to the vectors of norm 8 in $\Gamma_i$.
Using this method I found the number of vectors of norm 6 in $\Gamma_i$ as given in Table 1.

## 4.2 Using orthogonal decomposition $(24,48)$.

The idea (see [15]) is to embed the lattice $\Gamma_i$ from Section 2 $(i = 1,\ldots,9)$ into an orthogonally decomposable lattice $I_1 \perp I_2$ such that the minimal vectors of $I_1$ and the minimum of sublattices of $I_2$ can be computed. The even unimodular lattice $\Gamma_i$ has basis matrix $T_i$

given in Section 2.1 with respect to the Gram matrix $\frac{1}{2}\operatorname{diag}(F,F,F)$. Let $\pi$ denote the orthogonal projection onto the first 24 components, $K_1 := \ker(1-\pi) \subset I_1 := \operatorname{im}(\pi) = K_1^{\#}$, and $K_2 := \ker(\pi) \subset I_2 := \operatorname{im}(1-\pi) = K_2^{\#}$. Then

$$K_1 \perp K_2 \subset \Gamma_i \subset I_1 \perp I_2.$$

So the even unimodular lattice $\Gamma_i$ contains the sublattice $K_1 \perp K_2$ of index $2^{24}$ and is contained in $I_1 \perp I_2$ also of index $2^{24}$. Moreover $I_1 \cong \frac{1}{\sqrt{2}}\Lambda$ and $K_1 \cong \sqrt{2}\Lambda$ are similar to the Leech lattice of minimum 2 respectively 8. $I_2$ is a non integral lattice of dimension 48, with $(\ell,\ell) \in \mathbb{Z}$ for all $\ell \in I_2$. A computer calculation shows that $\min(I_2) = 4$ and $\min(K_2) = 8$. In particular

**Remark 4.2.** The vectors of norm 6 in $\Gamma_i$ are of the form $x+y$ with $x \in I_1$ of norm 2 and $y \in I_2$ of norm 4.

For all $i = 1,\ldots,9$ I computed representatives $v$ of the orbits of $\operatorname{Aut}_{\mathbb{Z}[\alpha]}(P_i)$ on the minimal vectors of $I_1$. For each $v$ there is some $w \in I_2$ such that $v + w \in \Gamma_i$, moreover $w$ is unique modulo $K_2$. So it remains to check that the minimum of the 48 dimensional lattice

$$I(w) := \langle K_2, w\rangle \leq I_2$$

is $\geq 6$. This is done by enumerating all vectors of norm 4 in this lattice.

**Remark 4.3.** For $\Gamma_2,\ldots,\Gamma_9$ the lattice $I(w)$ contains vectors of norm 4 for some $w$, summing up to the number of vectors of norm 6 in $\Gamma_i$ given in Table 1. Only for the lattice $\Gamma = \Gamma_1$ the representatives $w$ of all 15 orbits of $\mathrm{SL}_2(25)$ provide lattices $I(w)$ of minimum $> 4$.

# 5 Related lattices.

## 5.1 The polarisations defined by fourvolutions.

**Remark 5.1.** As proposed by Bob Griess in [6, Lemma B.3] I checked all pairs $f, g \in \operatorname{Aut}(\Lambda)$ with $f^2 = g^2 = -1$ such that $x := fg$ is an element of odd prime order $p$ with irreducible minimal polynomial. Then $p = 3, 5, 7, 13$ and the conjugacy class of $x$ in $2.Co_1$ is unique. To enumerate all such pairs, I computed the normaliser $N$ of $\langle x\rangle$ in $2.Co_1$ and went through all conjugacy classes of elements $f$ of $N$ such that $f^2 = -1$. For each such $f$ that satisfies $x^f = x^{-1}$ I put $g := f^{-1}x$. The centraliser in $2.Co_1$ acts on the situation. All six lattices $L(\Lambda(f-1), \Lambda(g-1), 3)$ contain vectors of norm 6.

Table 2

| $x$ | centraliser order | norm 6 vectors |
|---|---|---|
| 3 | $2^8 3^3 5^2 7$ | $2 \cdot 1,209,600$ |
| $5a$ | $2^8 3^3 5^2 7$ | $2 \cdot 1,209,600$ |
| $5b$ | $2^8 3 \cdot 5$ | $2 \cdot 103680$ |
| 7 | $2^3 3 \cdot 5$ | $2 \cdot 11520$ |
| 13 | $2^3 3$ | $2 \cdot 57600$ |

### 5.2 3-modular lattices.

For the construction in Definition 2.6 it is enough to assume that $L$ is an even lattice of odd determinant to obtain an even lattice $L(M,N,k)$ of determinant $\det(L)^k$ (see [18]). Interesting classes of lattices are the $p$-modular lattices as defined in [19] where a completely analogous theory of modular forms allows to define extremality as for unimodular lattices. In particular for $p = 7$ and $p = 3$ the "jump-dimensions" for the $p$-modular lattices are the multiples of 6 respectively 12. In dimension 6 respectively 12 there is a unique extremal $p$-modular lattice, the Barnes lattices $P_6$ and the Coxeter-Todd lattice $K_{12}$. Applying the construction to these lattices one hence finds 7-modular lattices of dimension 18 and 3-modular ones of dimension 36 that have minimum 6 or 8, where 8 would be extremal:

**Remark 5.2.** (a) The Barnes lattice $L$ has a unique polarisation $M, N$ such that $M$ and $N$ are similar to $L$. The lattice $L(M,N,3)$ has minimum 6, kissing number 336 and its automorphism group is a maximal finite matrix group ([13, p.44]).
(b) The automorphism group of the Coxeter-Todd lattice $L := K_{12}$ has five orbits on the set of polarisations $(M,N)$ of $L$ such that $(M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong L$. The lattices $L(M,N,3)$ all have minimum 6 and kissing number 576, 2016, 2880, 4320 respectively 12096.

# References


[1] Christine Bachoc, Gabriele Nebe, Extremal lattices of minimum 8 related to the Mathieu group $M_{22}$. J. reine angew. Math. 494 (1998) 155-171.

[2] Eva Bayer-Fluckiger, Ideal lattices. Proc. of the conference in honor of Alan Baker, Number Theory and Diophantine Geometry, Cambridge Univ. Press (2002) 168-184.

[3] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235-265, 1997

[4] J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups.* Springer Grundlehren 290, 1993.

[5] N. Elkies, B. Gross, The exceptional cone and the Leech lattice, Int. Math. Res. Notices 14 (1996) 665-698.

[6] Robert L. Griess Jr., Rank 72 high minimum norm lattices. J. Number Theory 130 (2010) 1512-1519.

[7] B. Gross, Group representations and lattices. J. Amer. Math. Soc. 3 (1990) 929-960.

[8] M. Hentschel, On Hermitian theta series and modular forms. Thesis RWTH Aachen 2009. http://darwin.bth.rwth-aachen.de/opus/volltexte/2009/2903/

[9] M. Kirschmer, Finite symplectic matrix groups. Thesis RWTH Aachen 2009, Exp. Math. (to appear)

[10] M. Kneser, Klassenzahlen definiter quadratischer Formen. Archiv der Math. 8 (1957) 241-250.

[11] J. Lepowsky, A. Meurman, An $\mathbb{E}_8$-approach to the Leech lattice and the Conway group. J. Algebra 77 (1982) 484-504.

[12] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, Upper Bounds for Modular Forms, Lattices, and Codes. J. Algebra 36 (1975) 68-76.

[13] G. Nebe, W. Plesken, Finite Rational Matrix Groups. Memoirs of the AMS 556 (1995)

[14] G. Nebe, The normaliser action and strongly modular lattices. L'Ens. Math., 43 (1997) 67-76

[15] G. Nebe, Construction and investigation of lattices with matrix groups. in *Integral Quadratic Forms and Lattices* edited by Myung-Hwan Kim, J. S. Hsia, Y. Kitaoka, R. Schulze-Pillot, Contemporary Mathematics **249** (1999), 205-220.

[16] G. Nebe, Some cyclo-quaternionic lattices, J. Alg. 199 (1998) 472-498.

[17] G. Nebe, Finite quaternionic matrix groups. Represent. Theory 2 (1998) 106-223.

[18] H.-G. Quebbemann, A construction of integral lattices. Mathematika, 31 (1984) 137-140.

[19] H.-G. Quebbemann, Modular lattices in euclidean spaces. J. Number Th. 54 (1995) 190-202.

[20] R. Scharlau, R. Schulze-Pillot, Extremal lattices. Algorithmic algebra and number theory (Heidelberg, 1997), Springer (1999) 139-170.

[21] N. J. A. Sloane, Binary Codes, Lattices, and Sphere-Packings. in *Combinatorial Surveys: Proceedings of the Sixth British Combinatorial Conference*, P. J. Cameron (editor), Academic Press, NY (1977) 117-164.

[22] D. Stehlé, M. Watkins, On the Extremality of an 80-Dimensional Lattice. ANTS 2010: 340-356.

[23] C.L. Siegel, Berechnung von Zetafunktionen an ganzzahligen Stellen. Göttinger Nach. 10 (1969) 87-102.