On extremal even unimodular 72-dimensional lattices.

Gabriele Nebe[1] and Richard Parker[2]

Abstract. By computer search we show that the lattice Γ from [9] is the unique extremal even unimodular 72-dimensional lattices that can be constructed as proposed in [6].
Keywords: extremal even unimodular lattice.
MSC: primary: 11H06, secondary: 11H31, 11H50, 11H55, 11H56, 11H71

1 Introduction.

In this paper a lattice (L,Q) is always an even unimodular positive definite lattice, i.e. a free $\mathbb{Z}$-module L equipped with an integral positive definite quadratic form $Q : L \to \mathbb{Z}$ of determinant 1. The minimum of L is the minimum of the quadratic form on the non-zero vectors of L

$$\min(L) = \min(L,Q) = \min\{Q(\ell) \mid 0 \neq \ell \in L\}^3.$$

From the theory of modular forms it is known that the minimum of an even unimodular lattice of dimension n is at most $\lfloor \frac{n}{24} \rfloor + 1$. Lattices achieving equality are called extremal. Of particular interest are extremal unimodular lattices in the "jump dimensions" - the multiples of 24. There are five extremal even unimodular lattices known in the jump dimensions, the Leech lattice Λ_{24}, the unique even unimodular lattice in dimension 24 without roots,[4] three lattices called P_{48p}, P_{48q}, P_{48n},[5] of dimension 48 which have minimum 3 [2], [8] and one lattice Γ in dimension 72 [9].

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. We call (M,N) a **polarisation** of L.

Definition 1.1. *([6], [10, Construction I], [9]) Given such a polarisation (M,N) of the even unimodular lattice (L,Q) let*

$$\begin{aligned} \mathcal{L}(M,N) &:= \{(a,b,c) \in L \perp L \perp L \mid a+b+c \in M, a+b \in N, a+c \in N\} \\ &= \{(x+m, y+m, z+m) \in L \perp L \perp L \mid m \in M, x,y,z \in N, x+y+z \in 2L\}. \end{aligned}$$

[1]Corresponding author, Gabriele Nebe, Lehrstuhl D für Mathematik, RWTH Aachen university, 52056 Aachen, Germany, nebe@math.rwth-aachen.de
[2]Parker's visit to Aachen was financed by the DFG (GRK 1632)
[3]In our definition the minimum is half the usual minimum of a lattice.
[4]Roots are norm 1 vectors in L. The reflection along a root defines an automorphism of L.
[5]See [3, Corollary 4.2] for a construction of P_{48n} from a polarisation of the Leech lattice mod 3.

Then the lattice $(\mathcal{L}(M,N),\tilde{Q})$ is an even unimodular lattice where

$$\tilde{Q}(a,b,c) := \frac{1}{2}(Q(a)+Q(b)+Q(c)).$$

Lemma 1.2. *(see [9]) Let (M,N) be a polarisation of L and assume that $d = \min(L,Q) = \min(N, \frac{1}{2}Q) = \min(M, \frac{1}{2}Q)$. Then*

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

The vectors of norm $\frac{3d}{2}$ in $\mathcal{L}(M,N)$ are exactly those triples (a,b,c) where $a,b,c \in \mathrm{Min}(L)$ satisfy $a+N = b+N = c+N$ and $a+b+c \in M$.

Proof. Let $\lambda = (a,b,c) \in \mathcal{L}(M,N)$. 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

$$\tilde{Q}(\lambda) = \frac{1}{2}Q(2\ell) = 2Q(\ell) \geq 2d.$$

2) Two non-zero components: Then $\lambda = (a,b,0)$ with $a,b \in N$ so $\tilde{Q}(\lambda) = \frac{1}{2}(Q(a)+Q(b)) \geq 2d$.

3) Three non-zero components: Then $\tilde{Q}(\lambda) = \frac{1}{2}(Q(a)+Q(b)+Q(c)) \geq \frac{3}{2}d$.

If $\tilde{Q}(\lambda) = \frac{3d}{2}$ then $\lambda = (a,b,c)$ has three non-zero components and $Q(a) = Q(b) = Q(c) = \frac{d}{2}$. By construction all components of λ lie in the same coset of N and their sum is in M. □

Example 1.3. *(see [5], [7], [10]) Let $L = \mathbb{E}_8$ be the unique even unimodular lattice of dimension 8. Then $\mathrm{Aut}(L)$ has a unique orbit on the polarisations (M,N) of L, so there is up to isometry just one lattice $\mathcal{L}(M,N)$ with $L = \mathbb{E}_8$. This lattice is an even unimodular lattice of dimension 24 with minimum 2, so it is isometric to the Leech lattice Λ_{24}. We use this construction of Λ_{24} to fix a Gram matrix F of the Leech lattice. Let $\alpha \in \mathrm{End}(\mathbb{E}_8)$ be such that $\alpha^2 - \alpha + 2 = 0$ (there is a unique $\mathrm{Aut}(\mathbb{E}_8)$ conjugacy class of such endomorphisms). Then $\mathbb{Z}[\alpha] \cong \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $\beta := (1-\alpha)$ satisfies $\alpha\beta = 2$. Put $M := \alpha L$ and $N := \beta L$. Then a Gram matrix of $\Lambda_{24} = \mathcal{L}(M,N)$ is given by the matrix product*

$$\mathcal{F} := \frac{1}{2}\begin{pmatrix} \alpha & \alpha & \alpha \\ \beta & \beta & 0 \\ 0 & \beta & \beta \end{pmatrix} \mathrm{diag}(F,F,F) \begin{pmatrix} \alpha & \alpha & \alpha \\ \beta & \beta & 0 \\ 0 & \beta & \beta \end{pmatrix}^{tr} = \begin{pmatrix} 3F & X & X \\ X^{tr} & 2F & F \\ X^{tr} & F & 2F \end{pmatrix}$$

where F is a Gram matrix of $\mathbb{E}_8$ and $X = \alpha F(1-\alpha)^{tr}$:

$$F = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}, \quad X = \begin{pmatrix} -3 & 0 & 2 & -1 & 1 & 1 & -2 & 0 \\ 0 & -3 & 0 & 1 & 0 & 1 & -1 & 2 \\ 1 & 0 & -3 & 1 & 1 & -1 & 2 & -1 \\ 1 & 2 & 2 & -3 & 1 & -1 & 0 & 0 \\ -1 & 0 & -1 & 2 & -3 & 2 & 0 & 0 \\ -1 & -1 & 1 & 1 & 1 & -3 & 1 & 0 \\ 2 & 1 & -2 & 0 & 0 & 2 & -3 & 1 \\ 0 & -2 & 1 & 0 & 0 & 0 & 2 & -3 \end{pmatrix}$$

Starting with a suitable polarisation (M_0, N_0) of $L = \Lambda_{24}$ the extremal even unimodular lattice $\Gamma = \mathcal{L}(M_0, N_0)$ of dimension 72 was constructed in [9]. This paper reports on a computer demonstration that Γ is the unique extremal even unimodular lattice of dimension 72 that can be constructed by this tripling construction. The main result is

Theorem 1.4. *Let (M, N) be a polarisation of $L = \Lambda_{24}$ such that $\mathcal{L}(M, N)$ has minimum 4. Then there is some $g \in \mathrm{Aut}(\Lambda_{24})$ such that $M = gM_0$, $N = gN_0$ and hence $\mathcal{L}(M, N) \cong \Gamma$.*

As already remarked in [6] if (M, N) is a polarisation of Λ_{24} such that $\mathcal{L}(M, N)$ is extremal, then $(M, \frac{1}{2}Q)$ and $(N, \frac{1}{2}Q)$ are both isometric to the Leech lattice. We call such sublattices **good**. A polarisation (M, N) of Λ_{24} is called **good**, if both sublattices N and M are good. A good polarisation (M, N) is called **extremely good**, if $\mathcal{L}(M, N)$ is extremal. The strategy to find orbit representatives of all extremely good polarisations of Λ_{24} starts by constructing representatives of all orbits of $\mathrm{Aut}(\Lambda_{24})$ on the set of good sublattices. It turns out that there are 16 orbits, so there are 16 candidates for the second entry N in the (extremely) good polarisations (M, N).

2 Orbit representatives of the subspaces.

In this section we list the orbits of the automorphism group of the Leech lattice Λ_{24} on the good sublattices N of Λ_{24} Such a sublattice N necessarily contains $2\Lambda_{24}$ and hence corresponds to a totally singular subspace $E = N/2\Lambda_{24} \leq \Lambda_{24}/2\Lambda_{24}$.

Definition 2.1. *Let N be a good sublattice of Λ_{24}. Then any nonzero class $0 \neq f + N \in \Lambda_{24}/N$ contains exactly 24 pairs $\{\pm v_1, \ldots, \pm v_{24}\}$ of minimal vectors in Λ_{24} (so $Q(v_i) = 2$ for all i). The set*

$$B(N, f) := \{(v_i + v_j + v_k) + 2\Lambda_{24} \mid 1 \leq i, j, k \leq 24\} \subset \Lambda_{24}/2\Lambda_{24}$$

is called the set of **bad vectors** *for N and f. Their union*

$$B(N) := \bigcup_{0 \neq f + N \in \Lambda_{24}/N} B(N, f)$$

is called the set of **bad vectors** *for N. The* **profile** *of N is the multiset*

$$\mathit{prof}(N) := \{|B(N, f)| \mid 0 \neq f + N \in \Lambda_{24}/N\}.$$

Theorem 2.2. *The automorphism group $\mathrm{Aut}(\Lambda_{24}) = 2.Co_1$ has exactly 16 orbits on the good sublattices as given in the table below.*

Proof. We first construct enough totally isotropic subspaces $E = N/2\Lambda_{24}$ of $\Lambda_{24}/2\Lambda_{24}$ such that the full preimage N of E is similar to the Leech lattice. [6] We then compute the stabiliser

[6] The number of good sublattices N is given in [4], their proportion in the set of all maximal totally singular subspaces is about 1/68107. Some of the subspaces are found by guessing large subgroups of their stabiliser, the first 7 orbits are already known from [9]. Other subspaces (in particular the large orbits) are found by constructing a large number of isotropic subspaces using a variant of Kneser's neighboring method. For the last orbit (a small orbit with a soluble stabiliser) we know the exact order of the stabiliser and constructed it as a sublattice invariant under a suitable subgroup of order 36 of stabiliser number 6.

and profile of these subspaces which turn out to distinguish the orbits. The sum of the orbit lengths is the number of good sublattices N given in [4] which proves the completeness of our list. $\square$

The stabilisers of orbit representatives of good sublattices

	$\mathrm{Stab}_{Co_1}(E)$	$\lvert \mathrm{Stab}_{2.Co_1}(E) \rvert$	$\mathrm{prof}(N)$
1	$PSL_2(25):2$	$2^5 3 \cdot 5^2 13$	$64^{65}, 256^{650}, 1024^{3380}$
2	$A_7 \times PSL_2(7)$	$2^7 3^3 5 \cdot 7^2$	$256^{2625}, 1024^{1470}$
3	$S_3 \times PSL_2(13)$	$2^4 3^2 7 \cdot 13$	$256^{1365}, 1024^{2730}$
4	$3.A_6 \times A_5$	$2^7 3^4 5^2$	$256^{225}, 1024^{3870}$
5	$PSL_2(7) \times PSL_2(7)$	$2^7 3^2 7^2$	$32^7, 128^{196}, 512^{2548}, 2048^{1344}$
6	$A_5 \times$ soluble	$2^{16} 3^3 5$	$64^{63}, 256^{960}, 1024^{3072}$
7	$G_2(4) \times A_4$	$2^{16} 3^4 5^2 7 \cdot 13$	64^{4095}
8	$PSL_2(23)$	$2^4 3 \cdot 11 \cdot 23$	$128^{253}, 512^{2530}, 2048^{1312}$
9	soluble	$2^{12} 3$	$32, 128^{30}, 512^{2784}, 2048^{1280}$
10	soluble	$2^{13} 3^2$	$64^{15}, 256^{240}, 1024^{3840}$
11	soluble	$2^9 3 \cdot 7$	$64^7, 256^{80}, 1024^{3808}$
12	soluble	$2^{12} 3^2$	$32, 128^{286}, 512^{1504}, 2048^{2304}$
13	$3.A_7.2$	$2^5 3^3 5 \cdot 7$	$64^{63}, 256^{1260}, 1024^{2772}$
14	soluble	$2^{10} 3 \cdot 5$	$64^{15}, 256^{1200}, 1024^{2880}$
15	soluble	$2^9 3 \cdot 7$	$32, 128^{14}, 512^{1904}, 2048^{2176}$
16	soluble	$2^{15} 3^3$	$64^{159}, 256^{2400}, 1024^{1536}$

Bases for good subspaces

1	1465	938	3283	3558	1133	2623	2648	802	1901	2171	539	2029
2	4447	2579	2509	2265	4760	45	569	868	483	6407	6695	-2747
3	717	2761	10347	2206	10348	10730	8271	725	9189	2800	-1617	-2718
4	762	67421	66339	2025	67054	779	66906	-30808	-16145	-7871	-4075	-1954
5	279159	278691	16921	279303	16470	-114417	-65128	-16052	-24146	-11304	-5897	-2512
6	213	450	82	6484	2863	2555	5117	961	6601	4432	2779	-2314
7	4541	4541	1075	5383	1275	381	256	1333	6139	1018	4422	-690
8	1014	352	1657	1830	2504	608	2081	3373	4	2144	3720	761
9	4485	4155	599	5910	6113	1336	4098	193	638	6021	5071	-102
10	1107	110	4206	4439	1115	164	1929	221	10	5229	1960	-1614
11	11139	10899	10760	10713	985	890	2178	939	2179	2120	-1375	-2929
12	1589	2157	548	2012	870	3451	3827	327	817	1972	1172	3533
13	1094	434	1173	9609	12557	313	5360	5550	13418	442	-6028	-3571
14	12835	12896	498	12619	8300	526	5024	8293	4173	531	-6027	-2135
15	1051	10197	8547	9983	1559	990	8868	9428	9727	9747	-2665	-980
16	34128	38064	1413	32913	32832	33981	4438	33013	-16351	-8085	-4733	-3109

To encode a basis of representatives of these 16 orbits in the table above we work with respect to a basis B with Gram matrix $\mathcal{F}$ of Λ_{24} given in Example 1.3. Any $v \in \Lambda_{24}/2\Lambda_{24}$

has a unique expression $v = \sum_{i=1}^{24} a_i \overline{B_i}$ with $a_i \in \{0,1\}$. Then $\mathrm{num}(v) := \sum_{i=1}^{24} a_i 2^{24-i} \in \{0,\ldots,2^{24}-1\}$ A basis of the subspace $E = \langle e_1,\ldots,e_{12}\rangle_{\mathbb{F}_2} \leq \Lambda_{24}/2\Lambda_{24}$ is encoded by giving the numbers $\mathrm{num}(e_i) - 2^{24-i}$. Apart from this renormalisation we did not pay any attention to find small numbers (by choosing either a better basis or a different orbit representative). Explicit generator matrices are available from the first author's homepage.

3 The extremely good polarisations.

The key observation to find all extremely good polarisations by an exhaustive computer search is the following easy lemma.

Lemma 3.1. *Let N be a good sublattice of Λ_{24}. The polarisation (M,N) of Λ_{24} is extremely good if and only if $(M/2\Lambda_{24}) \cap B(N) = \emptyset$.*

Proof. The polarisation (M,N) is good, if $\min(M,Q) = 4$. By assumption $(M, \frac{1}{2}Q)$ is an even unimodular lattice so the condition that $\min(M,Q) = 4$ is equivalent to the fact that M does not contain any minimal vectors of Λ_{24}. Each of these $4095 \cdot 48$ minimal vectors belongs to exactly one frame $\{\pm v_1,\ldots,\pm v_{24}\} \subset f+N$ and by construction their classes mod $2\Lambda_{24}$ belong to $B(N,f)$. By Lemma 1.2 the vectors of norm 3 in $\mathcal{L}(M,N)$ are triples (a,b,c) where $a,b,c \in \mathrm{Min}(\Lambda_{24})$ belong to the same class modulo N. The sum $a+b+c$ of all such triples is included in the set $B(N)$ of bad vectors of N. Therefore a necessary and sufficient condition for (M,N) to be an extremely good polarisation is that $B(N) \cap M/2\Lambda_{24} = \emptyset$.
□

Corollary 3.2. *Let $N \leq \Lambda_{24}$ be good sublattice of Λ_{24}. If $2048 \in$ prof(N), then there is no extremely good polarisation (M,N) containing N as second entry.*

Proof. Assume that there is an extremely good polarisation (M,N). Then $F := M/2\Lambda_{24}$ is a complement of $E := N/2\Lambda_{24}$ in $\Lambda_{24}/2\Lambda_{24}$. In particular F consists of a system of isotropic representatives of all classes $f+N \in \Lambda_{24}/N$. Any nonzero class $f+E$ contains exactly $2^{11} = 2048$ isotropic vectors (if f is isotropic, then all isotropic vectors in $f+E$ are $\{f+e \mid e \in E \cap f^{\perp}\}$). By construction all elements of $B(N,f)$ are isotropic elements in $f+E$. If there is one class $f+E$ in which all isotropic elements are bad, then $F \cap B(N,f) \neq \emptyset$, contradicting the assumption that (M,N) is extremely good. □

Now the procedure to find all extremely good polarisations (M,N) is as follows: We fix one of the 16 orbit representatives of good sublattices as the second entry N, compute $B(N)$, put $E := N/2\Lambda_{24}$ and work in $\mathbb{F}_2^{24} \cong \Lambda_{24}/2\Lambda_{24}$. We fix some basis $(e_1,\ldots,e_{12})$ of E and the dual basis $(f_1,\ldots,f_{12})$ of some totally singular complement F_0 of E. Any M corresponds to a totally singular complement F of E and this complement has a unique basis $(b_1,\ldots,b_{12})$ such that $(b_i,e_j) = \delta_{ij}$. Then $b_i = f_i + \sum_{j=1}^{12} x_{ij} e_j$ where $(x_{ij}) = (x_{ij})^{tr} \in \mathbb{F}_2^{12\times 12}$ satisfies $x_{ii} = 0$ for all i. Now (M,N) is an extremely good polarisation, if and only if $F \cap B(N) = \emptyset$.

We recursively build the basis $(b_1,\ldots,b_{12})$ of F by running through

$$\{b_1 \in f_1 + E \mid b_1 \text{ isotropic }\} \setminus B(N,f_1).$$

If $(b_1, \ldots, b_k)$ are chosen put $U := \langle b_1, \ldots, b_k \rangle$. Then the candidates for b_{k+1} are those isotropic elements in $f_{k+1} + E$ that are perpendicular to U and for which $(b_{k+1} + U) \cap B(N) = \emptyset$. It is very helpful to order the basis vectors $(e_1, \ldots, e_{12})$ such that $|B(N, f_i)|$ is as big as possible for the first few values of i.

There is still an action of $S := \mathrm{Stab}_{Co_1}(E)$ on the complements F of E which we use in the hard cases: If the program has proven that there is no extremely good complement F that contains the vector b_1, we can exclude the full orbit Sb_1 and replace $B(N)$ by $B(N) \cup Sb_1$. For the case $S \cong G_2(4) \times A_4$ we even had to use the action of the stabiliser S_1 of b_1 in S on the candidates for b_2.

To simplify and speed up the computations we precompute a list of 2^{24} entries 0 or 1, where 1 means "bad" and 0 means "good". For a given N, the $8,386,560$ anisotropic vectors in $\mathbb{F}_2^{24}$ have a flag 1 as well as the vectors in $B(N)$. The resulting 0-1 sequence is then the input of a C-program that performs the recursive procedure described above, by successively changing a 0 flag for the vector v to 1, if $v + U$ contains a bad vector, i.e. a vector labelled by 1. Hence the output of the C-program is simply all subspaces $M + 2L$, where all 2^{12} vectors have their flag $0 =$"good".

We use the action of the stabilizer S of N by letting the C-program exclude the vector b_1. Then we change all 0s in the orbit Sb_1 to 1s and thus create the new input for the C-program.

We let this program run for all 11 orbit representatives N of good sublattices where $2048 \notin \mathrm{prof}(N)$. For the first possibility of N, where $S = \mathrm{PSL}_2(25) : 2$, we found two extremely good polarisations (M, N) which belong to the same orbit under S. They both give rise to the lattice Γ constructed in [9]. For the other ten orbit representatives N, no extremely good polarisation (M, N) was found.

References

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

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

[3] R. Coulangeon, G. Nebe, Dense lattices as Hermitian tensor products. Proceedings of the BIRS workshop "Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms,", Contemporary Mathematics (to appear)

[4] C. Dong, H. Li, G. Mason, S. P. Norton, Associative subalgebras of the Griess algebra and related topics. in: Ferrar, J. (ed.) et al., The Monster and Lie algebras. Proceedings of a special research quarter at the Ohio State University, Columbus, OH, USA, May 1996. Berlin: de Gruyter. Ohio State Univ. Math. Res. Inst. Publ. **7**, 27-42

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

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

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

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

[9] G. Nebe, An even unimodular 72-dimensional lattice of minimum 8. J. Reine und Angew. Math. (to appear)

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