A generalisation of Turyn's construction of self-dual codes

Numerical Methods of Research in Vertex Operator Algebras, Finite Groups and Combinatorics

Author(s)
Nebe, Gabriele

Citation
数理解析研究所講究録 (2011), 1756: 51-59

Issue Date
2011-08

URL
http://hdl.handle.net/2433/171294

Type
Departmental Bulletin Paper

Textversion
publisher

Kyoto University
A generalisation of Turyn's construction of self-dual codes.

Gabriele Nebe

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

ABSTRACT. In [17] Turyn constructed the famous binary Golay code of length 24 from the extended Hamming code of length 8 (see also [10, Theorem 18.7.12]). The present note interprets this construction as a sum of tensor products of codes and uses it to construct certain new extremal (or at least very good) self-dual codes (for example an extremal doubly-even binary code of length 80). The lattice counterpart of this construction has been described by Quebbemann [13]. It was used recently to construct an extremal even unimodular lattice in dimension 72 ([12]).

1 Introduction.

A linear code is a subspace $C$ of $F_q^n$, where $F_q$ denotes the field with $q$ elements. The vector space $F_q^n$ is equipped with the standard inner product $(x,y):=\sum_{i=1}^{n}x_iy_i$. We call this the standard Euclidean inner product to distinguish it from the Hermitian inner product $h(x,y):=\sum_{i=1}^{n}x_i\overline{y}_i$ where $x \mapsto \overline{x} = x^r$ is the field automorphism of $F_q$ of order 2 and $q = r^2$. For $C \subseteq F_q^n$ the dual code is

$$C^\perp := \{x \in F_q^n \mid (x,c) = 0 \text{ for all } c \in C\}.$$ 

Analogously the hermitian dual code $C^{\perp,h}$ is the orthogonal space with respect to $h$. The code $C$ is called (hermitian) self-orthogonal if $C \subseteq C^{\perp,h}$ and (hermitian) self-dual if $C = C^{\perp,h}$.

For $x \in F_q^n$ the weight of $x$ is $wt(x) := |\{i \mid x_i \neq 0\}|$ the number of non-zero entries in $x$. The error correcting properties of a code $C$ are measured by the minimum weight $d(C) := \min\{wt(c) \mid 0 \neq c \in C\}$. A code $C$ is called $m$-divisible, if the weight of any codeword is a multiple of $m$. For $q = 2,3$ the square of any non-zero element in $F_q$ is 1 and hence any self-orthogonal code in $F_q^n$ is $q$-divisible. Similarly $x\overline{x} = 1$ for any $0 \neq x \in F_4$ so any hermitian self-orthogonal code in $F_4^n$ is 2-divisible. The Gleason-Pierce theorem shows that there are essentially four interesting families of self-dual $m$-divisible linear codes over finite fields: The self-dual binary codes (Type I codes) with $m = 2$, the self-dual ternary codes (Type III codes) with $m = 3$, the hermitian self-dual quaternary codes (Type IV codes) with $m = 2$ and the doubly-even self-dual binary codes (Type II codes) with $m = 4$. 

Invariant theory of finite complex matrix groups gives the following bounds on the minimum weight of Type $T$ codes of length $n$:

$$d(C) \leq \begin{cases} 2 + 2\lfloor \frac{n}{8} \rfloor & \text{if } T=I \\ 4 + 4\lfloor \frac{n}{24} \rfloor & \text{if } T=II \\ 3 + 3\lfloor \frac{n}{12} \rfloor & \text{if } T=III \\ 2 + 2\lfloor \frac{n}{6} \rfloor & \text{if } T=IV \end{cases}$$

Using the notion of the shadow of a code, Rains [14] improved the bound for Type I codes

$$d(C) \leq 4 + 4\lfloor \frac{n}{24} \rfloor + a$$

where $a = 2$ if $n \pmod{24} = 22$ and $0$ otherwise. Self-dual codes that achieve these bounds are called extremal. The monograph [11] gives a framework to define the notion of a Type of a self-dual code in much more generality and shows how to apply invariant theory to find upper bounds on the minimum weight of codes of a given Type.

Motivated by the article [13] and the construction of extremal 80-dimensional even unimodular lattices in [2] a generalisation of a construction used by Turyn to construct the Golay code of length 24 from the Hamming code of length 8 is given in this paper. The new codes discovered in this paper are an extremal Type II code of length 80 (at least 15 such codes have been known before) and 5 Euclidean self-dual codes in $F_4^{36}$ with minimum weight 11. All computations are done with MAGMA [4].

2 A construction for self-dual codes.

**Theorem 2.1.** Let $C = C^\perp$, $D = D^\perp \leq F_q^n$ and $X \leq F_q^m$ such that $X \cap X^\perp = \{0\}$. Then

$$T := T(C, D, X) := C \otimes X + D \otimes X^\perp \leq F_q^{nm} = F_q^n \otimes F_q^m$$

is a self-dual code.

If $q = 2$ and $C$ and $D$ are doubly-even, then $T$ is also doubly-even.

**Proof.** Let $c, c' \in C$, $d, d' \in D$, $x, x' \in X$ and $y, y' \in X^\perp$. Then

$$(c \otimes x, c' \otimes x') = 0 \quad \text{since } C \subseteq C^\perp$$

$$(d \otimes y, d' \otimes y') = 0 \quad \text{since } D \subseteq D^\perp$$

$$(c \otimes x, d \otimes y) = 0 \quad \text{since } x \in X, y \in X^\perp$$

so $T \subseteq T^\perp$. Moreover

$$\dim(T) = \dim(C \otimes X) + \dim(D \otimes X^\perp) - \dim(C \otimes X \cap D \otimes X^\perp) = nm/2 - 0$$

since $X \cap X^\perp = \{0\}$. This implies that $T$ is self-dual.

If $C$ and $D$ are doubly-even, then the weights of all generators of $T$ are multiples of 4 and so also $T$ is doubly-even.

\[ \blacksquare \]
Remark 2.2. A similar result holds for hermitian self-dual codes: Let $C = C^{\perp, h}, D = D^{\perp, h} \leq \mathbb{F}_q^n$ and $X \leq \mathbb{F}_q^n$ such that $X \cap X^{\perp, h} = \{0\}$. Then

$$T_h := T_h(C, D, X) := C \otimes X + D \otimes X^{\perp, h} \leq F_q^{nm} = F_q^n \otimes F_q^m$$

is a hermitian self-dual code.

Remark 2.3. Clearly $X + X^{\perp} = F_q^m$ has minimum weight 1 and therefore $d(T(C, D, X)) \leq d(C \cap D)$. For $q = 2$, any self-dual code contains the all-one vector $1$, so the maximum possible minimum weight for binary codes is $d(T(C, D, X)) \leq d(C \cap D) \leq d(\langle 1 \rangle) = n$.

Example 2.4. (binary codes)

1) Turyn’s construction of the Golay-code ([17], see [10, Theorem 18.7.12]).

Let $C \cong D \cong h_8 = h_8^\perp \leq F_2^8$ both to be equivalent to the extended Hamming code $h_8$ of length 8, the unique doubly-even binary self-dual code of length 8. Up to the action of $S_8$ there is a unique such pair satisfying $C \cap D = \langle 1 \rangle$. Let $X := \langle (1, 1, 1) \rangle$. Then $T(C, D, X)$ is a doubly-even self-dual code of length 24. From the explicit description

$$T(C, D, X) = \{(c + d_1, c + d_2, c + d_3) \mid c \in C, d_i \in D, d_1 + d_2 + d_3 \in C \cap D = \langle 1 \rangle\}$$

one easily sees that the minimum weight of $T(C, D, X)$ is $\geq 8$, so $T(C, D, X)$ is equivalent to the Golay code: Any non-zero word $w \in T(C, D, X)$ has either

1) 1 non-zero component: Then up to permutation $w$ is of the form $(d, 0, 0)$ with $d = 1 \in F_2^8$ and has weight 8.

2) 2 non-zero components: Then $w$ is equivalent to $(d_1, d_2, 0)$ with non-zero $d_1, d_2 \in D \cong h_8$ and has weight $\geq d(h_8) + d(h_8) = 4 + 4 = 8$.

3) 3 non-zero components: Since all components of $w$ lie in $C + D = \langle 1 \rangle^\perp$ they all have even weight, so $wt(w) \geq 2 + 2 + 2 = 6$. The code $T$ is doubly-even, so the weight of $w$ is a multiple of 4, therefore $wt(w) \geq 8$.

2) Let $X \leq F_2^{10}$ be the code with generator matrix

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

(see [1]). Then $X$ is equivalent to its dual code, $X \cap X^\perp = \langle 1 \rangle$ and the minimum weight of $X$ (and of $X^\perp$) is 4. Let $C$ and $D$ be as in 1) and put

$$T := X \otimes C + X^\perp \otimes D \leq F_2^{10}.$$
Then $T$ is self-orthogonal of dimension
\[
\dim(X \otimes C) + \dim(X^\perp \otimes D) - \dim((X \otimes C) \cap (X^\perp \otimes D)) = 20 + 20 - 1 = 39.
\]
The three codes $T_1, T_2, T_3$ with $T \subseteq T_i \subseteq T^\perp$ are all self-dual, two of them are doubly-even and one of these doubly-even self-dual codes has minimum weight 16, hence is an extremal doubly-even code of length 80. Its automorphism group is isomorphic to $PSL_2(7) \times S_6 : 2$, which can be seen as follows:
Let $S$ be stabiliser of $D$ in $\text{Aut}(C)$. Then $S \cong PSL_2(7)$. The two codes $C$ and $D$ are the only self-dual $S$-invariant submodules of $F_2^{10}$, they are interchanged by the normalizer of $S$ in $S_8$ which is isomorphic to $PGL_2(7)$. Hence there is $\tau \in S_8$ interchanging $C$ and $D$.

The automorphism group $A$ of $X$ is isomorphic to $S_6$, it also fixes the dual code $X^\perp$. The two codes $X$ and $X^\perp$ are the only $A$-invariant subspaces of $F_2^{10}$ which have dimension 5, therefore they are interchanged by the normalizer of $A$ in $S_{10}$, which contains $A$ of index 2. So there is $\sigma \in S_{10}$ with $\sigma(X) = X^\perp$ and $\sigma(X^\perp) = X$. One therefore gets an obvious action of

\[
H := \langle A \otimes S, \sigma \otimes \tau \rangle \cong PSL_2(7) \times S_6 : 2
\]
on $T$. Since the three self-dual codes $T_1, T_2, T_3$ are not equivalent, the automorphism group of $T$ also stabilizes all codes $T_i$. With MAGMA one checks that $\text{Aut}(T_1) = H$.

To the author's knowledge this code is not described before in the literature.

**Example 2.5. Ternary codes:**
Let $C \leq F_3^{12}$ be the linear ternary self-dual code with generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0 & 1
\end{pmatrix}
\]
Then $C$ is equivalent to the ternary Golay code of length 12. Let $h \in S_{12}$ be the permutation $(1, 4, 6, 12, 3, 9, 8)(2, 11, 7, 10)$ and let $D = h(C)$. Then $C \cap D$ is of dimension 1 and minimum weight 12.

Choose $X = \langle (1, 1) \rangle \leq F_3^2$. Then $T(C, D, X)$ is a self-dual code of minimum weight 9. The extremal ternary codes of length 24 are classified in [8]. There are two such codes, one of them is the extended quadratic residue code, the other one is equivalent to $T(C, D, X)$.

**Example 2.6. Euclidean self-dual quaternary codes:**
Let $C \leq F_4^{12}$ be the code with generator matrix
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & 1 & 1 & \omega & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & \omega^2 & \omega & \omega^2 \\
0 & 0 & 1 & 0 & 0 & 0 & \omega & \omega^2 & \omega & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & \omega & \omega^2 & \omega & 1 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & \omega^2 & \omega & 1 & 0 & \omega^2 & \omega \\
0 & 0 & 0 & 0 & 0 & 1 & \omega^2 & 1 & 1 & \omega & 1 & 1
\end{pmatrix}
\]
Then $C$ is a euclidean self-dual code equivalent to the extended quadratic residue code of length 12 over $\mathbb{F}_4$. Putting $D = \pi(C)$ for permutations $\pi \in S_{12}$ running through a right transversal of Aut($C$) in $S_{12}$, $X = \langle (1, \omega) \rangle \leq \mathbb{F}_4^2$ and $X^\perp = \langle (1, \omega + 1) \rangle$ one constructs 20 monomially inequivalent euclidean self-dual codes in $\mathbb{F}_4^{24}$ with minimum weight 8. Taking $X = \langle (1,1,1) \rangle$ one obtains five monomially inequivalent euclidean self-dual codes in $\mathbb{F}_4^6$ with minimum weight 11: $T_1, T_2$ (108 minimum words) and $T_3, T_4$ and $T_5$ (1188 minimum words each). These codes are not equivalent to the ones given in [3]. Permutations $\pi_i$ yielding these codes $T_i$ are

$$
\begin{align*}
\pi_1 &= (1, 10, 7, 2, 11, 8, 5)(3, 4, 12, 9) \\
\pi_2 &= (1, 10, 6, 4, 12, 9, 5)(2, 11, 8, 7) \\
\pi_3 &= (1, 3, 4, 5, 7, 8, 9, 11)(2, 10, 12) \\
\pi_4 &= (1, 6, 11)(2, 5, 8, 12, 4, 7, 10)(3, 9) \\
\pi_5 &= (1, 10, 2, 8)(3, 11, 12, 6)(4, 7, 5, 9)
\end{align*}
$$

The permutation groups are $S_3 \times A_5$ for $T_i$ (i=1,2,3,4) and $S_3 \times PSL_2(11)$ for $T_5$.

### 3 An application to lattices.

In [13] Quebbemann describes a construction of integral lattices that is the lattice counterpart of the construction described in the last section. Here a lattice $(L, Q)$ is 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

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

contains $L$ and the finite abelian group $L^\#/L =: D(L, Q)$ is called the discriminant group. $L$ is called unimodular, if $L = L^\#$. Note that unimodular quadratic lattices are usually called even unimodular lattices. They correspond to regular positive definite integral quadratic forms.

The minimum of a lattice $(L, Q)$ is

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

which is half of the usual minimum of the lattice.

The theory of modular forms allows to show that the minimum of a unimodular quadratic lattice of dimension $n$ is always

$$\min(L, Q) \leq \left\lfloor \frac{n}{24} \right\rfloor + 1.$$

Lattices achieving this bound are called extremal.
For any prime $p$ not dividing the order of $D(L, Q)$ the quadratic form $Q$ induces a non-degenerate quadratic form

$$\overline{Q} : L/pL \to \mathbb{Z}/p\mathbb{Z}, \overline{Q}(\ell + pL) := Q(\ell) + p\mathbb{Z}.$$  

From the theory of integral quadratic forms (see for instance [15]) it is well known that this quadratic space $(L/pL, \overline{Q})$ is hyperbolic, so there are maximal isotropic subspaces $A = A^\perp$ and $A' = (A')^\perp$ such that

$$L/pL = A \oplus A', \overline{Q}(A) = \overline{Q}(A') = \{0\}.$$  

If $M$ and $N$ are the full preimages of $A$ and $A'$, then $L = M + N, pL = N \cap M$ and $(M, \frac{1}{p}Q)$ and $(N, \frac{1}{p}Q)$ are again integral lattices with the same discriminant group as $L$. 

The pair $(M, N)$ is called a polarisation of $L$ (for the prime $p$).

**Theorem 3.1.** ([13, Proposition]) Let $(L, Q), p, A, A'$ be as above and let $B \leq A^n$ be a subgroup of $A^n$. Put

$$B' := (A')^n \cap B^\perp = \{z = (z_1, \ldots, z_n) \in (A')^n | \sum_{i=1}^{n} (b_i, z_i) = 0 \text{ for all } (b_1, \ldots, b_n) \in B\}.$$  

Then $C := B \oplus B' \leq (L/pL)^n$ satisfies $\overline{Q^n}(C) = \{0\}$ and $C = C^\perp$. The lattice

$$\Lambda := \Lambda(L, A, A', B) := \{\ell \in L^n | \overline{\ell} \in C\}$$

is integral with respect to $\tilde{Q} := \frac{1}{p}Q^n$ and satisfies $D(\Lambda, \tilde{Q}) \cong D(L, Q^n)$.

Of particular interest is the case where

$$B = \{(x, \ldots, x) | x \in A\}$$

is the diagonal subgroup of $A^n$. Then

$$B' = \{(z_1, \ldots, z_n) | z_i \in A' \text{ and } \sum z_i = 0\}$$

and $\Lambda(L, A, A', B)$ will be denoted by $\Lambda(L, A, A', n)$ or equivalently $\Lambda(L, M, N, n)$, where $M, N$ are the full preimages of $A, A'$ respectively.

**Lemma 3.2.** 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

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

**Proof.** The lattice $\Lambda := \Lambda(L, M, N, 3)$ has the following description

$$\Lambda = \{(m + n_1, m + n_2, m + n_3) | m \in M, n_1, n_2, n_3 \in N, n_1 + n_2 + n_3 \in 2L\}.$$  

We write any element of $\Lambda$ of $\lambda = (a, b, c)$ and distinguish according to the number of non-zero components:
1) One non-zero component: Then \( \lambda = (a, 0, 0) \) with \( a = 2\ell \in 2L \) so \( \bar{Q}(\lambda) = \frac{1}{2}Q(2\ell) = 2Q(\ell) \geq 2d \).

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

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

Examples for \( p = 2 \) and \( n = 3 \)

1) Take \((L, Q) = E_8\) the unique (even) unimodular lattice of dimension 8. Then for \( p = 2 \), the quadratic space \( L/2L \) has a unique polarisation \( L/2L = A \oplus A' \) up to the action of the orthogonal group of \( L \). By Lemma 3.2 the lattice \( \Lambda(E_8,A,A',3) \) is an even unimodular lattice of minimum 2, therefore isomorphic to the Leech lattice, the unique unimodular lattice of dimension 24 with minimum 2. This has been remarked independently in [16], [9], [13].

2) Take \( L = \Lambda_{24} \) to be the Leech lattice and take a polarization \( L = M+N, M \cap N = 2L \) such that \( \Lambda(M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24} \). Bob Griess [7] remarked that \( \Lambda(M, L, N, 3) \) is a 72-dimensional unimodular lattice of minimum 3 or 4 (this also follows from Lemma 3.2). In [6] the number of sublattices \( M \leq \Lambda_{24} \) such that \( (M, \frac{1}{2}Q) \cong \Lambda_{24} \) is computed. There are \( 5,163,643,468,800,000 \) such sublattices, about \( 1/68107 \) of all maximal isotropic subspaces. Each maximal isotropic subspace \( A \) has \( 2^{86} \) complements (the number of alternating \( 12 \times 12 \) matrices over \( \mathbb{F}_2 \)). Assuming that approximately \( 1/68107 \) of these complements correspond to lattices that are similar to the Leech lattice, the number of pairs \((M, N)\) such that \( M + N = \Lambda_{24}, M \cap N = 2\Lambda_{24} \) and \( (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong \Lambda_{24} \) is about \( 5.6 \times 10^{40} \). Dividing by the order of the Conway group, \( \text{Aut}(\Lambda_{24})/\{\pm 1\} \), one gets a rough estimate of \( 10^{12} \) orbits of such polarisations of the Leech lattice. Presumably most of these orbits will give rise to lattices of minimum 3. In [12] I found one lattice \( \Gamma := \Lambda(\Lambda_{24},M,N,3) \) to be an extremal unimodular lattice of dimension 72. Here the sublattices \( M = \alpha \Lambda_{24} \) and \( N = (\alpha+1)\Lambda_{24} \) are obtained using a hermitian structure of the Leech lattice over the ring of integers \( \mathbb{Z}[\alpha] \) in the imaginary quadratic number field of discriminant \(-7\), where \( \alpha^2 + \alpha + 2 = 0 \). The Leech lattice has nine such Hermitian structures and one of them defines a polarisation giving rise to an extremal unimodular lattice. \( \Gamma \) can also be constructed as the tensor product of the Leech lattice with the unique unimodular \( \mathbb{Z}[\alpha] \)-lattice \( P_b \) or dimension 3, \( \Gamma = \Lambda_{24} \otimes_{\mathbb{Z}[\alpha]} P_b \). This construction allows to find the subgroup \( \text{SL}_2(25) \times \text{PSL}_2(7) : 2 \) of the automorphism group of \( \Gamma \). For more details on this lattice see my preprint [12].

The extremal 72-dimensional lattice \( \Gamma \) described above is constructed using a polarizaion \((M, N)\) of \( \Lambda_{24} \) that is invariant under \( \text{SL}_2(25) \). This group contains an element \( g \) of order 13, acting as a primitive 13th root of unity on \( L/2L \) and it is interesting to investigate all \( g \)-invariant polarisations:
Remark 3.3. Take \( L := \Lambda_{u} \) to be the Leech lattice and let \( g \in \text{Aut}(L) \) be an element of order 13 (there is a unique conjugacy class of such elements). Then \( g \) acts fixed point free on \( L/2L \) and hence there are \( 2^{12} + 1 \) subspaces of dimension 12 that are invariant under \( \langle g \rangle \). The preimage \( M \) in \( L \) of 41 of these invariant subspaces is similar to the Leech lattice. The normalizer \( G \) in \( \text{Aut}(L) \) of \( \langle g \rangle \) acts on these lattices with orbits of length 36, 4, and 1. In total we obtain 31 representatives \( (M, N) \) of \( G \)-orbits on the ordered polarizations \( (M, N) \) of \( L \) modulo 2 such that

\[
gN = N, gM = M, (M, \frac{1}{2}Q) \cong (N, \frac{1}{2}Q) \cong (L, Q) \cong \Lambda_{24}.
\]

Only one such pair yields a lattice \( L(M, N, 3) \) that has minimum 4. This lattice is necessarily isometric to \( \Gamma \).

I did a similar computation for an element \( g \in \text{Aut}(\Lambda_{24}) \) acting as a primitive 21st root of 1. All 71 orbits of the normalizer on the ordered "good" polarisations \( (M, N) \) yield lattices \( L(M, N, 3) \) that contain vectors of norm 3.

Example.

In [2] we used the code \( X \leq F_{2}^{10} \) from example 2.4 2) to construct two 80-dimensional extremal unimodular lattices from the \( E_{8} \)-lattice.

References


