THE FANNING METHOD FOR CONSTRUCTING EVEN UNIMODULAR LATTICES. I

Autor(en): **ROEGNER, Katherine**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **48 (2002)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **12.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-66072

L'Enseignement Mathématique, t. 48 (2002), p. 169–187

THE FANNING METHOD FOR CONSTRUCTING EVEN UNIMODULAR LATTICES. I

by Katherine ROEGNER

ABSTRACT. This paper provides a formal study of isofans and discusses their use in the theory of even unimodular lattices. Examples are given that illustrate how isofans simplify the construction of certain types of even unimodular lattices. A classification of isofans concludes the paper.

INTRODUCTION

The history of even unimodular lattices dates back to the 19th century when H. J. S. Smith [Sm] showed the existence of what is known today as the E_8 lattice. The even unimodular lattices have been classified for dimensions 8 [M], 16 [W2], and 24 [N]. The next dimension of interest is 32 due to the fact that even unimodular lattices only occur in dimensions divisible by 8; see e.g. [Sch]. In dimension 32, there are millions of nonisometric even unimodular lattices. Although no classification in this dimension is available, there has been considerable progress. Conway and Pless [CP] determined the doubly-even self-dual binary codes, the results of which can be transformed into a classification statement for even unimodular lattices with complete root systems of a particular type. Within their work, they noted that it is possible to build some codes using known codes by making appropriate substitutions. Kervaire [Ke] classified the remaining cases of complete even unimodular lattices in dimension 32 using a lengthy elimination procedure and a lot of machine testing. Venkov [V] has shown that, except for 15 cases, the even unimodular lattices in dimension 32 can be generated by the roots and vectors with scalar square 4. In that article, Venkov introduced an important operation on lattices, which he called "fanning". It turns out that Venkov's fanning method is comparable to Conway and Pless' substitution method.

The purpose of this article is to provide an indepth study of the fanning method. To do so, Venkov's fanning method is generalized to the isofan, a special isomorphism between rational bilinear form modules associated to root lattices. Some examples are given illustrating the construction of new complete even unimodular lattices from already known ones using isofans. In particular, an easy construction for a lattice that Conway and Pless found using "several processes including divination" is given. A classification of isofans concludes the paper.

The author is indebted to Helmut Koch for the hints and suggestions he has provided. Special thanks are due to Boris Venkov for the many helpful discussions concerning even unimodular lattices and to the referee for suggesting many improvements to the original version of this paper.

1. LATTICES

Let $\mathbf{R}^n$ be n-dimensional euclidean space equipped with the standard scalar product

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \text{ for all } x = (x_1, \ldots, x_n),\ y = (y_1, \ldots, y_n) \in \mathbf{R}^n .$$

A free $\mathbf{Z}$-module $\Lambda \subset \mathbf{R}^n$ of rank $k := \dim_{\mathbf{R}} \mathbf{R} \otimes_{\mathbf{Z}} \Lambda$ is called a *lattice of rank* k. A *basis* of a rank k lattice Λ is a subset $\{\lambda_1, \ldots, \lambda_k\} \subset \Lambda$ that generates Λ over $\mathbf{Z}$.

Let $\Lambda \subset \mathbf{R}^n$ be a lattice. Λ is said to be *integral* if $\lambda_i \cdot \lambda_j \in \mathbf{Z}$ for all $\lambda_i, \lambda_j \in \Lambda$. It is an *even* lattice if, in addition to being integral, $\lambda^2 := \lambda \cdot \lambda \in 2\mathbf{Z}$ for all $\lambda \in \Lambda$. Let $\Lambda^{\#} = \{x \in \mathbf{R}^n \mid x \cdot \lambda \in \mathbf{Z} \text{ for all } \lambda \in \Lambda\}$ denote the *dual lattice*. Clearly, Λ is integral if and only if $\Lambda \subseteq \Lambda^{\#}$. Λ is called *unimodular* if in fact $\Lambda = \Lambda^{\#}$. Thus, an even unimodular lattice is a self-dual lattice such that $\lambda^2 \in 2\mathbf{Z}$ for all $\lambda \in \Lambda$.

Let $\Lambda_1, \ldots, \Lambda_m$ be nontrivial sublattices of the integral lattice Λ whose direct sum is equal to Λ. If $x \cdot y = 0$ for all $x \in \Lambda_i$, $y \in \Lambda_j, i \neq j$, then Λ is called the orthogonal direct sum of the sublattices $\Lambda_1, \ldots, \Lambda_m$ and denoted by $\Lambda = \Lambda_1 \oplus \cdots \oplus \Lambda_m$. Λ is called *decomposable* if there exists such an orthogonal direct sum with $m > 1$, otherwise Λ is said to be *indecomposable*.

The *root system* of an even lattice Λ is the set

$$\Lambda_{\mathrm{rt}} := \{\lambda \in \Lambda \mid \lambda^2 = 2\},$$

the elements of which are called *roots*. Λ is called a *root lattice* if Λ is

generated by its roots. Let $\{e_1, \ldots, e_n\}$ denote the standard basis of $\mathbf{R}^n$. The root system of an even lattice is the orthogonal direct sum of root systems of the following type, corresponding to the indecomposable root lattices [W1]:

$$A_n := \{\pm(e_i - e_j) \mid 1 \le i < j \le n+1,\ n \ge 1\},$$

$$D_m := \{\pm(e_i \pm e_j) \mid 1 \le i < j \le m,\ m \ge 3\},$$

$$E_8 := \Big\{\pm(e_i \pm e_j),\ \frac{1}{2}\sum_{k=1}^{8} \epsilon_k e_k \mid \epsilon_k = \pm 1,\ \prod_{k=1}^{8} \epsilon_k = 1,\ 1 \le i < j \le 8\Big\},$$

$$E_7 := \{v \in E_8 \mid \langle v, e_7 - e_8\rangle = 0\},$$

$$E_6 := \{v \in E_8 \mid \langle v, e_7 - e_8\rangle = 0 \text{ and } \langle v, e_6 - e_7\rangle = 0\}.$$

The root system of an even lattice is said to be *complete* (in Λ) if the lattice generated by Λ_{rt} has finite index in Λ. In this case, we will call Λ a *complete lattice*.

In general, one wants to determine the finitely many isometry classes of even unimodular lattices of a given rank. These isometry classes have been determined for ranks up to 24. Since the rank of even unimodular lattices is known to be divisible by 8, the next rank of interest is 32. There are millions of isometry classes of rank 32 even unimodular lattices. Instead of classifying all isometry classes, several authors have restricted their attention to the isometry classes of *complete* even unimodular lattices of rank 32.

When dealing with complete even unimodular lattices, it is convenient to classify the lattices according to their root systems. Beginning with a candidate root system R, the goal is to construct all isometry classes of even unimodular lattices Λ such that $\Lambda_{\mathrm{rt}} = R$. To do that, it is helpful to associate a code to the lattice generated by Λ_{rt}, which can be achieved in the following manner.

Assume that Λ is a complete integral lattice in $\mathbf{R}^n$. Let $R = \Lambda_{\mathrm{rt}}$, and let $\mathbf{R}$ denote the lattice generated by R. By definition, $\mathbf{R} \subseteq \Lambda$ is a sublattice of finite index and $\mathbf{R} \subseteq \Lambda \subseteq \Lambda^{\#} \subseteq \mathbf{R}^{\#}$. Let $\pi\colon \mathbf{R}^{\#} \to \mathbf{R}^{\#}/\mathbf{R}$ be the natural projection of $\mathbf{R}^{\#}$ onto the *discriminant group* $G(R) := \mathbf{R}^{\#}/\mathbf{R}$, also known as the *word group*. It is a finite abelian group that inherits a nondegenerate, bilinear form

$$b_R\colon \mathbf{R}^{\#}/\mathbf{R} \times \mathbf{R}^{\#}/\mathbf{R} \to \mathbf{Q}/\mathbf{Z};\ b_R(\pi(\xi_1), \pi(\xi_2)) = \xi_1 \cdot \xi_2 \bmod \mathbf{Z}$$

for $\xi_1, \xi_2 \in \mathbf{R}^{\#}$. Thus, the discriminant group is a bilinear form module, which will be denoted by $(G(R), b_R)$ or simply $G(R)$ if no confusion arises.

Next, define a norm

$$\mathbf{n}_{\mathbf{R}}\colon G(R) \to \mathbf{Q}; \qquad \mathbf{n}_{\mathbf{R}}(g) = \min_{\xi \in \mathbf{R}^{\#}} \{\xi^2 \mid \xi = \pi^{-1}(g)\}.$$

An *admissible representative system* $\{r_1, \ldots, r_k\}$ of $G(R)$ is any representative system of $G(R)$ such that $r_i^2 = \mathbf{n_R}(\pi(r_i))$, $1 \leq i \leq k$. The following chart gives the discriminant groups associated to the indecomposable root lattices given earlier. It also provides an admissible representative system for each and includes information on norms.

TABLE 1

R	$G(R) \simeq$	admissible representative system	norm
A_ℓ ($\ell \geq 1$)	$\mathbf{Z}/(\ell+1)\mathbf{Z}$	$a_{\ell,r} = \frac{r}{\ell+1}\sum_{i=0}^{\ell-r} e_i - \frac{\ell+1-r}{\ell+1}\sum_{j=\ell-r+1}^{\ell} e_j$	$\frac{\ell(\ell-r+1)}{\ell+1}$
D_ℓ ($\ell \geq 3$)	$\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (ℓ even) $\mathbf{Z}/4\mathbf{Z}$ (ℓ odd)	$d_{\ell,0} = 0$ $d_{\ell,1} = \frac{1}{2}\sum_{i=1}^{\ell} e_i$ $d_{\ell,2} = e_\ell$ $d_{\ell,3} = \frac{1}{2}\sum_{i=1}^{\ell-1} e_i - \frac{1}{2}e_\ell$	0 $\ell/4$ 1 $\ell/4$
E_8	0	$e_{8,0} = 0$	0
E_7	$\mathbf{Z}/2\mathbf{Z}$	$e_{7,0} = 0$ $e_{7,1} = \frac{1}{4}(e_1 + \cdots + e_6 - 3(e_7 + e_8))$	0 3/2
E_6	$\mathbf{Z}/3\mathbf{Z}$	$e_{6,0} = 0$ $e_{6,1} = \frac{1}{3}(e_1 + \cdots + e_4 - 2(e_5 + e_6))$ $e_{6,2} = -e_{6,1}$	0 4/3 4/3

The nontrivial bilinear forms are as follows:

$$b_{A_\ell}(a_{\ell,j}, a_{\ell,k}) \equiv \frac{j(\ell+1-k)}{\ell+1} \bmod \mathbf{Z},\ 0 \leq j \leq k \leq \ell;$$

$$b_{D_\ell}(d_{\ell,j}, d_{\ell,0}) \equiv 0 \bmod \mathbf{Z},\ 0 \leq j \leq 3, \quad b_{D_\ell}(d_{\ell,k}, d_{\ell,2}) \equiv \frac{1}{2} \bmod \mathbf{Z};\ k = 1, 3,$$

$$b_{D_\ell}(d_{\ell,2}, d_{\ell,2}) \equiv 0 \bmod \mathbf{Z}, \quad b_{D_\ell}(d_{\ell,1}, d_{\ell,3}) \equiv \frac{\ell-2}{4} \bmod \mathbf{Z},$$

$$b_{D_\ell}(d_{\ell,k}, d_{\ell,k}) \equiv \frac{\ell}{4} \bmod \mathbf{Z}, k = 1, 3;$$

$$b_{E_7}(e_{7,j}, e_{7,0}) \equiv 0 \bmod \mathbf{Z},\ j = 0, 1, \quad b_{E_7}(e_{7,1}, e_{7,1}) \equiv \frac{1}{2} \bmod \mathbf{Z};$$

$$b_{E_6}(e_{6,j}, e_{6,0}) \equiv 0 \bmod \mathbf{Z},\ j = 0, 1, 2, \quad b_{E_6}(e_{6,k}, e_{6,k}) \equiv \frac{1}{3} \bmod \mathbf{Z},\ k = 1, 2,$$

$$b_{E_6}(e_{6,1}, e_{6,2}) \equiv \frac{2}{3} \bmod \mathbf{Z}.$$

Note that the index of each root system R in the chart indicates the rank of the indecomposable root lattice $\mathbf{R}$. (To simplify the terminology, set $\operatorname{rk} R := \operatorname{rk} \mathbf{R}$.) It is easy to verify that $(G(D_3), b_{D_3}) \simeq (G(A_3), b_{A_3})$, so that these two bilinear form modules can be identified with one another. Note also that $G(2A_1) \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \simeq G(D_{2k})$. The norms of the elements in $G(2A_1)$ are $0, \frac{1}{2}, 1, \frac{1}{2}$. These would be the norms of the elements of $G(D_2)$ if D_2 existed as a root system. Let $a^1_{1,1}$ denote the nontrivial representative of the first copy of $G(A_1)$ and $a^2_{1,1}$ that of the second copy. Set $d_{2,1} := a^1_{1,1}$, $d_{2,2} := a^1_{1,1} + a^2_{1,1}$, $d_{2,3} := a^2_{1,1}$ It is now easy to check that the bilinear form $b = b_{2A_1}$ for $2A_1$ has the same values as a bilinear form for D_2 would under this identification. Thus, D_2 will often be used to denote $2A_1$ when it is convenient.

If $\Lambda_1, \Lambda_2 \subset \mathbf{R}^n$ are mutually orthogonal, finitely generated $\mathbf{Z}$-submodules of $\mathbf{R}^n$, then $(\Lambda_1 \oplus \Lambda_2)^\# = \Lambda_1^\# \oplus \Lambda_2^\#$, where $\oplus$ denotes the orthogonal direct sum. Thus, the discriminant groups are just orthogonal direct sums of the discriminant groups described above. In particular, if we restrict ourselves to the case of root systems of the form $R = \alpha_1 A_1 + \sum_{i=1}^{k} \delta_{2k} D_{2k} + \varepsilon_7 E_7$, resp. $R = \alpha_2 A_2 + \varepsilon_6 E_6$, then $G(R)$ is isomorphic to $\mathbf{F}_2^n$, resp. $\mathbf{F}_3^n$.

Let Λ be a complete integral lattice, set $H = \pi(\Lambda)$, $H^\perp = \pi(\Lambda^\#)$. Note that

$$H^\perp = \{x \in G(\Lambda_{\mathrm{rt}}) \mid b_{\Lambda_{\mathrm{rt}}}(x, h) = 0 \quad \text{for all } h \in H\}.$$

Because Λ is integral, $H \subseteq H^\perp$. Thus, H is self-orthogonal with respect to the bilinear form b of $G := G(\Lambda_{\mathrm{rt}})$. Furthermore, $H = H^\perp$ if and only if $\Lambda = \Lambda^\#$ (i.e., Λ is unimodular), and in this case H is referred to as an *isotropic subgroup* of G with respect to b, otherwise known as a *metabolizer*. Λ will be an even unimodular lattice if and only if $H = H^\perp$ and $\mathbf{n}(g)$ is an even integer for all $g \in G$.

Beginning with the root system R, each isotropic subgroup $H \subset G(R)$ leads to the even unimodular lattice $\Lambda = \pi^{-1}(H)$. It is not necessary that $\Lambda_{\mathrm{rt}} = R$ because an additional root arises if the norm of some element of H is 2. Since the objective is to construct the even unimodular lattices with a given root system, it is sufficient to consider only those isotropic subgroups H for which $\mathbf{n}(h)$ is an even integer $\neq 2$ for all $h \in H$. Such isotropic subgroups will be called *admissible isotropic subgroups*.

An observation aids in determining the isometry classes of complete even unimodular lattices. Let Λ be a complete even lattice in $\mathbf{R}^n$ and $R = \Lambda_{\mathrm{rt}}$ its root system. Let $\Gamma(R)$ be the subgroup of $\operatorname{Aut} G(R)$ induced by the isometry group of $\mathbf{R}$. There is a one-to-one correspondence between equivalence classes

of even lattices in $\mathbf{R}^n$ with root system R and $\Gamma(R)$-orbits of subgroups H in $G(R)$ with $\mathbf{n}(h) \in 2\mathbf{Z} \setminus \{2\}$ for all $h \in H$. Unimodular lattices correspond to isotropic subgroups.

2. Isofolds and isofans

Given any root system R, we want to determine whether or not a complete even unimodular lattice Λ exists such that $\Lambda_{\mathrm{rt}} = R$. This is equivalent to determining whether or not $(G(R), b_R)$ has an admissible isotropic subgroup. Suppose R' is another root system such that the bilinear form modules $(G(R'), b_{R'})$, $(G(R), b_R)$ are isomorphic. Let φ denote such an isomorphism. As φ is a bilinear form module isomorphism, $b_{R'}(g_1', g_2') = b_R(\varphi(g_1'), \varphi(g_2'))$ for all $g_1', g_2' \in G(R')$. Recall that the bilinear forms have values in $\mathbf{Q}/\mathbf{Z}$, so that

$$\mathbf{n}(g') \equiv \mathbf{n}(\varphi(g')) \bmod \mathbf{Z} \text{ for all } g' \in G(R').$$

If $(G(R'), b_{R'})$ has an isotropic subgroup H', it may be possible to use H' to construct an admissible isotropic subgroup H for $(G(R), b_R)$.

Definition. In the notation above, let

$$\varphi\colon (G(R'), b_{R'}) \to (G(R), b_R)$$

be an isomorphism of bilinear form modules, where $\operatorname{rk} R' < \operatorname{rk} R$. The isomorphism φ is called an *isofan* if

$$\mathbf{n}(g') \equiv \mathbf{n}(\varphi(g')) \bmod 2\mathbf{Z},$$
$$\mathbf{n}(g') \leq \mathbf{n}(\varphi(g'))$$

for all $g' \in G(R')$. The inverse φ^{-1} of the isofan φ is called an *isofold*.

Example 1. The simplest example of an isofan was given by Venkov [V]. Consider the root system D_k, $k \geq 2$, where D_2 is identified with $2A_1$. Recall that an admissible representative system for $(G(D_k), b_{D_k})$ can be given by $d_{k,0}, d_{k,1}, d_{k,2}, d_{k,3}$, the norms of the representatives being $0, \frac{k}{4}, 1, \frac{k}{4}$, respectively. Thus, for any integer k_1 satisfying $k_1 \equiv k \bmod 8$, the norms of $d_{k_1,i}$ and $d_{k,i}$ differ by an integral multiple of 2 for $0 \leq i \leq 3$.

Let φ_{D_k} be the group isomorphism given by

$$\varphi_{D_k}\colon G(D_k) \to G(D_{k+8}); \qquad d_{k,i} \mapsto d_{k+8,i} \quad (0 \leq i \leq 3).$$

This isomorphism preserves the bilinear form in the prescribed manner

$$b_{D_k}(d_{k,i}, d_{k,j}) = b_{D_{k+8}}(\varphi_{D_k}(d_{k,i}), \varphi_{D_k}(d_{k,j})) \quad (0 \le i,j \le 3),$$

so in fact it is an isomorphism of the bilinear form modules. It also preserves norms modulo $2\mathbf{Z}$, as noted above. Moreover, $\mathbf{n}(d_{k,i}) \le \mathbf{n}(\varphi_{D_k}(d_{k,i}))$. Thus φ_{D_k} is an isofan and $\varphi_{D_k}^{-1}$ an isofold.

It is well known that $R' := D_{16}$ is the root system of a complete even unimodular lattice [W2]. An admissible isotropic subgroup for $G(D_{16})$ is given by $H' = \{d_{16,0}, d_{16,1}\}$. Form the subgroup $H := \varphi_{D_{16}}(H') = \{d_{24,0}, d_{24,1}\}$. The map φ preserves the orthogonality relations and the norms modulo $2\mathbf{Z}$, whereby the norms may not decrease under the mapping. Since the group structures are also isomorphic, H is an admissible isotropic subgroup of $G(D_{24})$. Consequently, D_{24} is the root system of a complete even unimodular lattice. By induction, we get a family of complete even unimodular lattices; namely, D_{16+8i} is the root system of the complete even unimodular lattice generated over $\mathbf{Z}$ by D_{16+8i} and the vector $d_{16+8i,1} = \frac{1}{2}\sum_{j=1}^{16+8i} e_j \in \mathbf{R}^{16+8i}$ for $i \in \mathbf{Z}$, $i \ge 0$.

EXAMPLE 2. To find all isometry classes of even unimodular lattices for the root system $E_7+D_4+21A_1$, we will use an application of the fanning method. This root system appears in work of Conway and Pless [CP]; however, they provide no indication as to how an admissible isotropic subgroup, or self-dual doubly-even code, was found for $G(E_7 + D_4 + 21A_1)$.

Begin with the isofold

$$\eta\colon G(E_7 + D_4) \to 3G(A_1)$$
$$e_{7,1} \mapsto a^1 + a^2 + a^3; \quad d_{4,1} \mapsto a^1 + a^2; \quad d_{4,3} \mapsto a^2 + a^3,$$

where a^i refers to $a_{1,1}$ in the ith copy of $G(A_1)$ in $3G(A_1)$. Next, extend η to all of $G(E_7 + D_4 + 21A_1)$ by letting it act on $21G(A_1)$ as $\eta(a^i) = a^{i+3}$, $0 \le i \le 21$. Then $\eta\colon G(E_7+D_4+21A_1) \to 24G(A_1)$ is an isofold. In order to construct an admissible isotropic subgroup for $G(E_7+D_4+21A_1)$, we will apply isofans to isotropic subgroups of $24G(A_1)$.

It is well known that $24A_1$ is the root system of an even unimodular lattice [N]. The only admissible isotropic subgroup, up to equivalence, for its discriminant group can be identified with the self-dual doubly-even binary code of length 24 known as the Golay code. Letting $a^i = a^i_{1,1}$, this isotropic subgroup H' is generated (up to equivalence) by

$$
\begin{aligned}
h'_1 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^5 + a^6 + a^7 + a^8 \\
h'_2 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^9 + a^{10} + a^{11} + a^{12} \\
h'_3 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{13} + a^{14} + a^{15} + a^{16} \\
h'_4 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{17} + a^{18} + a^{19} + a^{20} \\
h'_5 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{21} + a^{22} + a^{23} + a^{24} \\
h'_6 &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^9 + a^{13} + a^{17} + a^{21}
\end{aligned}
\qquad
\begin{aligned}
h'_7 &= a^1 + a^2 + a^3 + a^6 \\
&\quad + a^9 + a^{14} + a^{18} + a^{22} \\
h'_8 &= a^1 + a^2 + a^3 + a^7 \\
&\quad + a^9 + a^{15} + a^{19} + a^{23} \\
h'_9 &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^{10} + a^{14} + a^{19} + a^{24} \\
h'_{10} &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^{11} + a^{15} + a^{20} + a^{22} \\
h'_{11} &= a^2 + a^3 + a^4 + a^5 \\
&\quad + a^9 + a^{14} + a^{20} + a^{23} \\
h'_{12} &= a^1 + a^2 + a^4 + a^5 \\
&\quad + a^9 + a^{15} + a^{18} + a^{24}
\end{aligned}
$$

(see, for example, [Ko]). Applying the isofan

$$\varphi = \eta^{-1} : 24G(A_1) \to G(E_7 + D_4 + 21A_1),$$

obtained from the extended isofold defined above, to the generators of H' yields generators for an admissible isotropic subgroup H:

$$
\begin{aligned}
h'_1 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^5 + a^6 + a^7 + a^8 \\
h'_2 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^9 + a^{10} + a^{11} + a^{12} \\
h'_3 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{13} + a^{14} + a^{15} + a^{16} \\
h'_4 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{17} + a^{18} + a^{19} + a^{20} \\
h'_5 &= a^1 + a^2 + a^3 + a^4 \\
&\quad + a^{21} + e_{7,1} \\
h'_6 &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^9 + a^{13} + a^{17} + a^{21}
\end{aligned}
\qquad
\begin{aligned}
h'_7 &= a^1 + a^2 + a^3 + a^6 \\
&\quad + a^9 + a^{14} + a^{18} + e_{7,1} + d_{4,2} \\
h'_8 &= a^1 + a^2 + a^3 + a^7 \\
&\quad + a^9 + a^{15} + a^{19} + e_{7,1} + d_{4,3} \\
h'_9 &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^{10} + a^{14} + a^{19} + e_{7,1} + d_{4,1} \\
h'_{10} &= a^1 + a^2 + a^3 + a^5 \\
&\quad + a^{11} + a^{15} + a^{20} + e_{7,1} + d_{4,2} \\
h'_{11} &= a^2 + a^3 + a^4 + a^5 \\
&\quad + a^9 + a^{14} + a^{20} + e_{7,1} + d_{4,3} \\
h'_{12} &= a^1 + a^2 + a^4 + a^5 \\
&\quad + a^9 + a^{15} + a^{18} + e_{7,1} + d_{4,1}.
\end{aligned}
$$

This isotropic subgroup represents the only $\Gamma(21A_1+E_7+D_4)$-orbit of subgroups that correspond to even unimodular lattices. If there were another such orbit, there would be an admissible isotropic subgroup $K \subset G(21A_1 + E_7 + D_4)$ not in the orbit of H. This means that $\eta(K)$ is an isotropic subgroup of $24G(A_1)$ in a different orbit than that of H'. Therefore, $\eta(K)$ is inadmissible, meaning that new roots have been created. The resulting root system, however, must still have at least 12 summands of A_1, otherwise some roots of $\eta(K)$ must come from roots in K. Also, the rank of the resulting root system must be 24. The only root system of an even unimodular lattice satisfying these two conditions is $24A_1$.

EXAMPLE 3. This example demonstrates that inequivalent even unimodular lattices can share the same root system; in this case, $4D_8$. Consider the isofold

$$\eta := \eta_{G(4D_8)}\colon 4G(D_8) \to 2G(D_4) + 2G(D_8)$$
$$d^1_{8,j} \mapsto d^1_{4,j} + d^2_{4,2}, \quad d^2_{8,j} \mapsto d^1_{4,2} + d^2_{4,j}, \quad d^3_{8,j} \mapsto d^1_{8,j}, \quad d^4_{8,j} \mapsto d^2_{8,j}, \quad j \in \{1,3\}.$$

There are no even unimodular lattices with root system $2D_4 + 2D_8$ [N]. If $4G(D_8)$ has an admissible isotropic subgroup H, $\eta(H)$ must then be an isotropic subgroup of $G(2D_4 + 2D_8)$ containing at least one element r of norm 2. Since $\mathbf{n}(\eta^{-1}(r)) \geq 4$, the possibilities for r are

$$d^i_{4,j} + d^k_{8,2}, \quad d^1_{4,j} + d^2_{4,\ell}, \quad i,k \in \{1,2\}, \quad j,\ell \in \{1,3\}.$$

The root system has now been changed and must be determined. If a root of the first type occurs, then D_4 joins with D_8 to give D_{12}. Since $D_{12}+D_4+D_8$ is not the root system of a complete even unimodular lattice, we appropriately introduce another root of the first type, resulting in $2D_{12}$, which indeed is the root system of a complete even unimodular lattice. If a root of the second type is introduced, the two D_4 combine to a D_8, so that the new root system is $3D_8$. Each of these root systems, $2D_{12}$ and $3D_8$, has a unique isometry class of even unimodular lattices.

Assume first that two roots of the first type are present. Without loss of generality, these roots may be taken to be $d^1_{4,1} + d^1_{8,2}$ and $d^2_{4,1} + d^2_{8,2}$. There is only one orbit of admissible isotropic subgroups of $2G(D_{12})$. One representative of this orbit is generated by $d^1_{12,1}+d^2_{12,2}$, $d^1_{12,2}+d^2_{12,1}$. From this, we will create an inadmissable isotropic subgroup of $G(2D_4 + 2D_8)$. First, rewrite the generators of the isotropic subgroup in terms of $G(D_4 + D_8 + D_4 + D_8)$, making sure that orthogonality relations between all elements are preserved: $d^1_{12,1}+d^2_{12,2}$ may either be $d^1_{4,2}+d^1_{8,1}+d^2_{8,2}$ or $d^2_{4,3}+d^1_{8,1}+d^2_{8,2}$, and $d^1_{12,2}+d^2_{12,1}$ may be either $d^2_{4,2}+d^1_{8,2}+d^2_{8,1}$ or $d^2_{4,3}+d^1_{8,2}+d^2_{8,1}$. For example,

using the first choices, generators for an inadmissible isotropic subgroup of $G(2D_4 + 2D_8)$ are

$$d^1_{4,2} + d^1_{8,1} + d^2_{8,2}, \quad d^2_{4,2} + d^1_{8,2} + d^2_{8,1}, \quad d^1_{4,1} + d^1_{8,2}, \quad d^2_{4,1} + d^2_{8,2}.$$

Now fan these generators using η^{-1} to get an admissible isotropic subgroup of $G(4D_8)$:

$$d^1_{8,2} + d^3_{8,1} + d^4_{8,2}, \quad d^2_{8,2} + d^3_{8,2} + d^4_{8,1}, \quad d^1_{8,1} + d^2_{8,2} + d^3_{8,2}, \quad d^1_{8,2} + d^2_{8,1} + d^4_{8,2}.$$

Had we used any other choices given above, we would have obtained an equivalent isotropic subgroup. Note that this isotropic subgroup has one word of norm 8.

In a similar fashion, take the generators of a representative of the only orbit of admissible isotropic subgroups of $3G(D_8)$:

$$d^1_{8,2} + d^2_{8,2} + d^3_{8,3}, \quad d^1_{8,2} + d^2_{8,3} + d^3_{8,2}, \quad d^1_{8,3} + d^2_{8,2} + d^3_{8,2}.$$

We shall now break apart the third copy of $G(D_8)$ into $2G(D_4)$ by introducing the root $d^1_{4,1} + d^2_{4,1}$. The next step is to rewrite $d^3_{8,2}$ and $d^3_{8,3}$ in terms of $2G(D_4)$. Since the results will have to be orthogonal to the root, this narrows down the choices considerably. Indeed, $d^3_{8,2}$ will have to be $d^1_{4,1}$ (which is equivalent to $d^2_{4,1}$), whereas, up to equivalence, $d^3_{8,3}$ can be either $d^1_{4,3} + d^2_{4,3}$ or $d^1_{4,2} + d^2_{4,3}$. Using the first choice, form the generators for an inadmissible isotropic subgroup

$$d^1_{4,1} + d^2_{4,1}, \quad d^1_{4,3} + d^2_{4,3} + d^1_{8,2} + d^2_{8,2}, \quad d^1_{4,1} + d^1_{8,2} + d^2_{8,3}, \quad d^1_{4,1} + d^1_{8,3} + d^2_{8,2}$$

for $2G(D_4) + 2G(D_8)$ and fan using η^{-1} to yield generators for an admissible metabolizer of $4G(D_8)$:

$$d^1_{8,3} + d^2_{8,3}, \qquad d^1_{4,1} + d^2_{4,1} + d^3_{8,2} + d^4_{8,2},$$
$$d^1_{8,1} + d^2_{8,2} + d^3_{8,2} + d^4_{8,3}, \qquad d^1_{8,1} + d^2_{8,2} + d^3_{8,3} + d^4_{8,2}..$$

This subgroup has two elements of norm 8, and as such is inequivalent to the admissible isotropic subgroup obtained by breaking apart $2D_{12}$.

On the other hand, if we rewrite $d^3_{8,3}$ as $d^1_{4,2} + d^2_{4,3}$, an inadmissible isotropic subgroup for $2G(D_4) + 2G(D_8)$ is generated by

$$d^1_{4,1} + d^2_{4,1}, \quad d^1_{4,2} + d^2_{4,3} + d^1_{8,2} + d^2_{8,2}, \quad d^1_{4,1} + d^1_{8,2} + d^2_{8,3}, \quad d^1_{4,1} + d^1_{8,3} + d^2_{8,2}.$$

Apply η^{-1} to these to obtain generators for an admissible isotropic subgroup for $4G(D_8)$:

$$d^1_{8,3} + d^2_{8,3}, \quad d^2_{8,3} + d^3_{8,2} + d^4_{8,2}, \quad d^1_{8,1} + d^2_{8,2} + d^3_{8,2} + d^4_{8,3}, \quad d^1_{8,1} + d^2_{8,2} + d^3_{8,3} + d^4_{8,2}.$$

Exchanging $d^i_{8,1}$ for $d^i_{8,3}$ and vice versa for $i = 3, 4$, we recover the same isotropic subgroup as the first one obtained from $2G(D_{12})$. Since all possibilities up to equivalence have been exhausted, there are exactly two distinct isometry classes of complete even unimodular lattices with root system $4D_8$.

EXAMPLE 4. This example deals with a root system of nonzero deficiency; i.e., the maximum number of mutually orthogonal roots is less than the rank of the root lattice. Kervaire [Ke] determined that there is exactly one isometry class of complete even unimodular lattices with the root system $10A_2 + 2E_6$. In his proof, he used results on conference matrices, a topic treated in coding theory. Here, we offer a different proof based on the fanning method.

Define the isofold

$$\eta\colon 10G(A_2) + 2G(E_6) \to 12G(A_2)$$

$$a^i_{2,j} \mapsto a^i_{2,j},\ 1 \le i \le 10,\ j \in \{0,1,2\}, \quad e^1_{6,1} \mapsto a^1_{2,1} + a^2_{2,1}, \quad e^2_{6,1} \mapsto a^1_{2,1} + a^2_{2,2}.$$

Niemeier showed in [N] that there is exactly one isometry class of complete even unimodular lattices with root system $12A_2$. Thus, there is exactly one orbit of admissible isotropic subgroups in $12G(A_2)$. A representative subgroup H' of this orbit is generated by

$$\begin{aligned}
&a^1_{2,1} + a^2_{2,1} + a^3_{2,1} + a^4_{2,1} + a^5_{2,1} + a^6_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^3_{2,2} + a^4_{2,2} + a^7_{2,1} + a^8_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^5_{2,2} + a^6_{2,2} + a^9_{2,1} + a^{10}_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^3_{2,2} + a^5_{2,2} + a^{11}_{2,1} + a^{12}_{2,1}\\
&a^7_{2,1} + a^8_{2,2} + a^9_{2,1} + a^{10}_{2,2} + a^{11}_{2,1} + a^{12}_{2,2}
\end{aligned}$$

The inverse of η acts as the identity on $a^i_{2,j}$ for $1 \le i \le 10$ and $j \in \{0,1,2\}$, while $\eta^{-1}(a^{11}_{2,1}) = e^1_{6,1} + e^2_{6,1}$ and $\eta^{-1}(a^{12}_{2,1}) = e^1_{6,1} + e^2_{6,2}$. Applying η^{-1} to the generators of H' yields generators for an admissible isotropic subgroup H for $10G(A_2) + 2G(E_6)$:

$$\begin{aligned}
&a^1_{2,1} + a^2_{2,1} + a^3_{2,1} + a^4_{2,1} + a^5_{2,1} + a^6_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^3_{2,2} + a^4_{2,2} + a^7_{2,1} + a^8_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^5_{2,2} + a^6_{2,2} + a^9_{2,1} + a^{10}_{2,1}\\
&a^1_{2,1} + a^2_{2,1} + a^3_{2,2} + a^5_{2,2} + e^1_{6,2}\\
&a^7_{2,1} + a^8_{2,2} + a^9_{2,1} + a^{10}_{2,2} + e^2_{6,2}
\end{aligned}$$

If there were an admissible isotropic subgroup J of $10G(A_2)+2G(E_6)$ not in the orbit of H, it would have to fold to an isotropic subgroup J' of $12G(A_2)$ in an orbit different from H'. Necessarily, J' contains roots, and these will have the form $a^i_{2,1\text{ or }2}+a^j_{2,1\text{ or }2}+a^k_{2,1\text{ or }2}$ with distinct $i,j\in\{1,\dots,10\}$ and $k\in\{11,12\}$. These roots can then be seen as roots of E_6. The only root system of a complete even unimodular lattice in dimension 24 with root system containing a summand E_6 is $4E_6$. But to transform $12A_2$ to $4E_6$ would require roots as above in which $k\notin\{11,12\}$. Applying η^{-1} to a root of this kind yields an element of norm 2 in J. Thus, there can be no admissible isotropic subgroup in an orbit different from the one containing H; hence, there is exactly one isometry class of even unimodular lattices with root system $10A_2+2E_6$.

3. Elementary isofans and isofolds

In the previous section, it was shown that φ_{D_k}, $k\geq 2$, is an isofan, as was noted by Venkov [V]. Conway and Pless [CP] found several other isofans that aided them in obtaining some of their codes from already known codes. The associated isofolds for these are:

$$\begin{aligned}
\eta_{2E_7}\colon G(2E_7)\to G(D_6);&\quad e^1_{7,1}\mapsto d_{6,1}\,,\ e^2_{7,1}\mapsto d_{6,3}\,;\\
\eta_{D_6+E_7}\colon G(D_6+E_7)\to G(A_1+D_4);&\quad e_{7,1}\mapsto a_{1,1}+d_{4,2}\,,\\
&\quad d_{6,j}\mapsto a_{1,1}+d_{4,j}\,,\ j\in\{1,3\};\\
\eta_{2D_6}\colon G(2D_6)\to G(4A_1);&\quad d^1_{6,1}\mapsto a^1_{1,1}+a^2_{1,1}+a^3_{1,1}\,,\ d^1_{6,3}\mapsto a^1_{1,1}+a^2_{1,1}+a^4_{1,1}\,,\\
&\quad d^2_{6,1}\mapsto a^1_{1,1}+a^3_{1,1}+a^4_{1,1}\,,\ d^2_{6,3}\mapsto a^2_{1,1}+a^3_{1,1}+a^4_{1,1}.
\end{aligned}$$

There are, however, other isofolds. The purpose of this section is to determine all possible isofolds.

Definition. Let $R=I_1+\cdots+I_l$ be the concatenation of indecomposable root systems I_i, $1\leq i\leq l$. Let $\eta\colon G(R)\to G(R')$ be an isofold for some root system R'. One says that the isofold η is *imprimitive* if there exists an $i\in\{1,\dots,l\}$ such that

$$\eta|_{G(I_i)}(G(I_i))\simeq G(I_i)\quad\text{and}\quad \mathbf{n}(x)=\mathbf{n}(\eta|_{G(I_i)}(x))\ \text{for all}\ x\in G(I_i).$$

In effect, this means that I_i is a summand of R', and η restricted to $G(I_i)$ preserves norms, although it may not be the identity.

If η is not imprimitive, then it is said to be *primitive*. A primitive isofold is called an *elementary isofold* if and only if it is not the composition of two or more primitive isofolds. Finally, two isofolds $\eta_1, \eta_2 : G(R) \to G(R')$ are said to be *equivalent* if and only if there exists a norm preserving automorphism η_3 of $G(R')$ with the property $\eta_3 \circ \eta_2 = \eta_1$ and *inequivalent* otherwise.

As an example, the isofold

$$\eta : G(D_{24}) \to G(D_8); \quad d_{24,i} \mapsto d_{8,i}\,, \ 0 \le i \le 3$$

is primitive since $\mathbf{n}(d_{24,1}) > \mathbf{n}(d_{8,1})$. It is not elementary as it is the composition of two elementary isofolds: $\eta = \varphi_{D_8}^{-1} \circ \varphi_{D_{16}}^{-1}$ (see the previous section for the definition of φ_{D_k}). The isofold

$$\eta' : G(D_{16}) \to G(D_8)$$
$$d_{16,0} \mapsto d_{8,0},\ d_{16,1} \mapsto d_{8,3},\ d_{16,2} \mapsto d_{8,2},\ d_{16,3} \mapsto d_{8,1}$$

is easily seen to be equivalent to $\varphi_{D_8}^{-1}$.

Any primitive isofold that is not elementary is equivalent to the composition of elementary isofolds by definition. The remainder of the section will be devoted to proving the next theorem.

THEOREM 1. *Let $\eta_R : G(R) \to G(R')$ be an elementary isofold. Then η_R is equivalent to one of the elementary isofolds listed in Table 2 (recall that D_2 stands for $2A_1$).*

TABLE 2
Elementary isofolds

R	R'	Definition of η_R $(j \in \{1, 3\})$
$D_{k+8} (k \ge 2)$	D_k	$\eta_{D_{k+8}}(d_{k+8,j}) = d_{k,j}$
$D_{k+4} + D_{\ell+4}$ $(k, \ell \ge 2)$	$D_k + D_\ell$	$\eta_{D_{k+4}+D_{\ell+4}}(d^1_{k+4,j}) = d^1_{k,j} + d^2_{\ell,2}$ $\eta_{D_{k+4}+D_{\ell+4}}(d^2_{\ell+4,j}) = d^1_{k,2} + d^2_{\ell,j}$
$D_{k+2} + E_7$ $(k \ge 2)$	$D_k + A_1$	$\eta_{D_{k+2}+E_7}(d_{k+2,j}) = d_{k,j} + a_{1,1}$ $\eta_{D_{k+2}+E_7}(e_{7,1}) = d_{k,2} + a_{1,1}$
$2E_7$	D_6	$\eta_{2E_7}(e^1_{7,1}) = d_{6,1}$ $\eta_{2E_7}(e^2_{7,1}) = d_{6,3}$
$2E_6$	$2A_2$	$\eta_{2E_6}(e^i_{6,1}) = a^1_{2,1} + a^2_{2,i},\ i = 1, 2$

The proof of the theorem requires several technical lemmata:

1. R has no summand of the form A_i, $i \geq 1$, and R' has no summand of the form A_i, $i \geq 4$;
2. R' has no summand of the form E_6, E_7, E_8;
3. the maximal rank taken over all the indecomposable summands of R is greater than the rank of any indecomposable summand of R';
4. if η is an elementary isofold, there exists an element $g \in G(R)$ such that $\mathbf{n}(g) > \mathbf{n}(\eta(g))$.

The proofs of the lemmata will be deferred until after the proof of the theorem.

Proof. It is a routine exercise to verify that the above mappings are isofolds. They are elementary since the change in rank is 8, whereas the change in rank of the composition of two or more primitive isofolds is at least 16.

Assume the lemmata above hold. By (4), there exists $g \in G(R)$ such that $\mathbf{n}(g) > \mathbf{n}(\eta(g))$. Write g as an orthogonal sum $g = g_1 \perp \cdots \perp g_m$, $m \geq 1$, whereby the g_i are elements of distinct word groups of indecomposable root systems. If $\mathbf{n}(g_i) = \mathbf{n}(\eta(g_i))$, $1 \leq i \leq m$, then $\eta(g_1) + \cdots + \eta(g_m)$ cannot be an orthogonal sum, or the norm does not decrease under η. Thus, either $\mathbf{n}(g_i) > \mathbf{n}(\eta(g_i))$, $1 \leq i \leq m$, or $\mathbf{n}(g_i \perp g_j) > \mathbf{n}(\eta(g_i \perp g_j))$, $1 \leq i < j \leq m$.

Suppose first that $\mathbf{n}(g) > \mathbf{n}(\eta(g))$ with g a representative of the word group of an indecomposable root system. The smallest norm possible for a representative of a word group is $\frac{1}{2}$. Consequently, $\mathbf{n}(g) \geq \frac{5}{2} \equiv \frac{1}{2} \bmod 2\mathbf{Z}$. From this and (1), it follows that $g = d_{k,j} \in G(D_k)$, $k \geq 10$, $j = 1$ or 3. Suppose $g = d_{k,1}$ (the case $g = d_{k,3}$ is analogous). We show that η is equivalent to η_{D_k}.

Set $\eta_1 = \eta_{D_k}$, and extend η_1 to all of $G(R)$ by letting it act as the identity on $G(R \setminus D_k)$. Set $\eta_2|_{G(R\setminus D_k)} = \eta|_{G(R\setminus D_k)}$ and $\eta_2(d_{k-8,j}) = \eta(d_{k,j})$, $j = 0, 1, 2, 3$. Then $\eta = \eta_2 \circ \eta_1$, and $\eta_2 \colon G(R \setminus D_k + D_{k-8}) \to G(R')$ is a group-isomorphism which preserves norms modulo $2\mathbf{Z}$. To show η_2 is an isofold, it remains to check that $\mathbf{n}(h_1) \geq \mathbf{n}(\eta_2(h_1))$ for all $h_1 \in G(R \setminus D_k + D_{k-8})$. Let $h_1 \in G(R \setminus D_k + D_{k-8})$ and $h = \eta_1^{-1}(h_1) \in G(R)$. By the definition of η_1, either $\mathbf{n}(h) = \mathbf{n}(\eta_1(h))$ or $\mathbf{n}(h) - 2 = \mathbf{n}(\eta_1(h))$. If $\mathbf{n}(h) > \mathbf{n}(\eta(h))$, then

$$\mathbf{n}(h_1) \geq \mathbf{n}(h) - 2 \geq \mathbf{n}(\eta(h)) = \mathbf{n}(\eta_2(h_1)).$$

If $\mathbf{n}(h) = \mathbf{n}(\eta(h))$, then by construction $\mathbf{n}(h) = \mathbf{n}(h_1) = \mathbf{n}(\eta_2(h_1))$. Therefore, η_2 is an isofold. Since η, η_1 are both elementary, η_2 must be imprimitive. Therefore, η is equivalent to η_{D_k}.

Next let $g = g_1 \perp g_2$ be the orthogonal sum of representatives of word groups of indecomposable root systems R_1, R_2 whereby $\mathbf{n}(g) > \mathbf{n}(\eta(g))$ and $\mathbf{n}(g_i) = \mathbf{n}(\eta(g_i))$, $i = 1, 2$. There are four possibilities for g, hence η_1 : set

$$\eta_1 := \begin{cases} \eta_{D_k + D_\ell} & \text{if } g = d_{k,j_1} + d_{\ell,j_2},\ j_1, j_2 \in \{1,2,3\}; \\ \eta_{2E_7} & \text{if } g = e^1_{7,1} + e^2_{7,1}; \\ \eta_{D_k + E_7} & \text{if } g = d_{k,j} + e_{7,1},\ j \in \{1,2,3\}; \\ \eta_{2E_6} & \text{if } g = e^1_{6,\pm 1} + e^2_{6,\pm 1}. \end{cases}$$

Extend η_1 to all of $G(R)$ by letting it act as the identity on $G(R \setminus (R_1 + R_2))$. As before, define

$$\eta_2|_{G(R\setminus(R_1+R_2))} := \eta|_{G(R\setminus(R_1+R_2))},\ \eta_2|_{\eta_1(G(R_1+R_2))}.$$

Again, $\eta = \eta_2 \circ \eta_1$ and η_2 is an isofold, hence imprimitive. □

LEMMA 2. *Let η: $G(R) \to G(R')$ be an elementary isofold. Then R contains no summand of the form A_i, $i \geq 1$, and R' contains no summand of the form A_i, $i \geq 4$.*

Proof. Suppose first that R has a summand A_i. Recall that for $i \geq 1$, $G(A_i) \simeq \mathbf{Z}/(i+1)\mathbf{Z}$. Since $\mathbf{n}(a_{i,1}) = \frac{i}{i+1} < 1$, it follows that $\mathbf{n}(\eta(a_{i,1})) = \frac{i}{i+1}$. Moreover, the smallest norm of a representative of any word group is $\frac{1}{2}$. Thus, $\eta(a_{i,1})$ must be a representative of the word group of an indecomposable root system. The norms of representatives from $G(D_k)$, $k \geq 4$, $G(E_6)$, $G(E_7)$ are all at least 1. The norm $\mathbf{n}(a_{\ell,j}) \geq \frac{1}{2}$ is an increasing function in ℓ as well as in j, $0 \leq j \leq \lfloor \frac{\ell}{2} \rfloor$ implies that $\eta(a_{i,1}) = \pm a_{i,1}$. But then η is an equivalence, hence not elementary.

The second statement of the lemma now easily follows. R has no summands of type A_j for all $j \in \mathbf{Z}$, whence $G(R) \simeq (\mathbf{Z}/2\mathbf{Z})^{n_1} \times (\mathbf{Z}/3\mathbf{Z})^{n_2} \times (\mathbf{Z}/4\mathbf{Z})^{n_3}$ for $n_1, n_2, n_3 \in \mathbf{Z}^{\geq 0}$. Since $G(R) \simeq G(R')$, only those A_i with $i \in 1, 2, 3$ are possible summands of R'. □

LEMMA 3. *If η: $G(R) \to G(R')$ is an elementary isofold for root systems R, R', then R' has no summand of type E_i, $i = 6, 7, 8$.*

Proof. E_8 is obvious as it is the only indecomposable root system with trivial word group.

Next, assume that E_7 is a summand of R'. By Lemma 2, R is the orthogonal sum of root systems of type E_j, $j = 6, 7, 8$, and/or D_k, $k \geq 4$. Due to norm considerations, at least one summand must be either E_7 or D_k, $k \equiv 2 \bmod 4$.

Clearly, $\eta^{-1}(e^1_{7,1}) \neq e^2_{7,1}$ or it would be imprimitive. If $\eta^{-1}(e^1_{7,1}) = e^2_{7,1} \perp g$ for some nontrivial g, then $\mathbf{n}(g) \equiv 0 \bmod 2\mathbf{Z}$. Since η is an isofold, $\mathbf{n}(\eta(e^2_{7,1})) = \frac{3}{2}$. Consequently, $\eta(e(7,1)^2)$ cannot contain the orthogonal summand $e^1_{7,1}$, forcing $\eta(g) = e^1_{7,1} \perp h$, for some $h \in G(R')$, $\mathbf{n}(h) \equiv \frac{1}{2} \bmod 2\mathbf{Z}$. On the other hand,

$$e^1_{7,1} = \eta(\eta^{-1}(e_{7,1})) = \eta(e^2_{7,1}) + \eta(g) = \eta(e^2_{7,1}) + e^1_{7,1} + h\,.$$

Since $e^1_{7,1}, e^2_{7,1}$ are of order 2, so is h. But then $h = \eta(e^2_{7,1})$, and $\mathbf{n}(h) \equiv \frac{3}{2} \bmod 2\mathbf{Z}$, a contradiction.

We are now reduced to the case that $\eta^{-1}(e_{7,1}) = d_{k,1} \perp g$, where $k \equiv 2 \bmod 4$ and g may be trivial. Because η is an isofold,

$$1 = \mathbf{n}(d_{k,2}) \geq \mathbf{n}(\eta(d_{k,2})) > 0\,,$$

from which it follows that $\mathbf{n}(\eta(d_{k,2})) = 1$. Since $e_{7,1}$ is of order 2, so is g, so that

$$\eta(d_{k,2}) = \eta(d_{k,1} + d_{k,3} + g + g) = \eta(d_{k,1} + g) + \eta(d_{k,3} + g) = e_{7,1} + h\,,$$

whereby $\eta(d_{k,3} + g) = h$. Since $\mathbf{n}(e_{7,1} + h) = 1$, $h = e_{7,1} \perp h_0$ with $\mathbf{n}(h_0) = 1$; in other words, $\mathbf{n}(h) = \frac{5}{2}$ and $\mathbf{n}(d_{k,3} \perp g) \equiv \frac{1}{2} \bmod 2\mathbf{Z}$. On the other hand, $\mathbf{n}(d_{k,1} \perp g) \equiv \frac{3}{2} \bmod 2\mathbf{Z}$, which would mean that $\mathbf{n}(d_{k,1}) \neq \mathbf{n}(d_{k,3})$, a contradiction.

Finally, assume E_6 is a summand of R'. $G(E_6) \simeq \mathbf{Z}/3\mathbf{Z}$, and the only root system with word group of order divisible by 3 which can appear as a summand of R is E_6. Since η is primitive, $\eta^{-1}(e^1_{6,1}) \neq e_{6,\pm 1}$. Thus, without loss of generality, $\eta^{-1}(e^1_{6,1}) = e^2_{6,1} + e^3_{6,1} + \cdots + e^{3k+2}_{6,1}$, $k \geq 1$.

$$\eta(e^2_{6,1} + e^3_{6,1} + \cdots + e^{3k+2}_{6,1}) = \eta(e^2_{6,1}) + \eta(e^3_{6,1}) + \cdots + \eta(e^{3k+2}_{6,1}) = e^1_{6,1}$$

means that there is some $j \in \{2, \ldots, 3k+2\}$ such that $\eta e^j_{6,1} = e^1_{6,1} \perp h$. Norm requirements force h to be trivial, so that η must be imprimitive. □

LEMMA 4. *Let $\eta\colon G(R) \to G(R')$ be an elementary isofold, and let k, k' denote the maximal ranks of indecomposable summands S, S' of R, R', respectively. Then $k > k'$.*

Proof. Assume that $k \leq k'$. From the previous lemmas, R may not have any summands of the form A_1, A_2, A_3, and R' may not have any of the form A_i, $i \geq 4$, E_6, E_7, E_8. Consequently, $D_{k'}$ is a summand of R' with $k' \geq 4$.

Let $R = I_1 + \cdots + I_m$ be the concatenation of indecomposable root systems I_i, $i \in \{1, \ldots, m\}$. Since η is a group isomorphism, there exists

some $i \in \{1, \ldots, m\}$ such that for some $g_i \in G(I_i)$, $d_{k',1}$ is an orthogonal summand of $\eta(g_i)$. $g_i \neq d_{\ell,j}, j \in \{1,3\}$, for any $\ell (\leq k \leq k')$ because then either $\mathbf{n}(d_{\ell,1}) < \mathbf{n}(d_{k',1})$ or we get an equivalence. $g_i \neq d_{\ell,2}$, since then $k' = 4$, which implies $\ell = 4$, and we have an equivalence. $g_i \neq e_{7,1}$, for then $k' \geq 7$ and

$$\mathbf{n}(e_{7,1}) = \frac{3}{2} < \frac{7}{4} \leq \mathbf{n}(d_{k',1}). \qquad \square$$

LEMMA 5. *Let η: $G(R) \to G(R')$ be an elementary isofold. There exists $g \in G(R)$ such that $\mathbf{n}(\eta(g)) < \mathbf{n}(g)$.*

Proof. We produce a $g \in G(R)$ which satisfies the lemma. By definition, $\mathbf{n}(\eta(h)) \leq \mathbf{n}(h)$ for all $h \in G(R)$. Note that $\mathbf{n}(a_{i,1}) < 1$ for all i, whereas $\mathbf{n}(h) \geq 1$ for all $h \in G(R)$. Thus if A_i is a summand of R', then set $g := \eta^{-1}(a_{i,1})$.

Since R' has no summands of the form $E_j, j = 6, 7, 8$, it suffices to consider $R' := I_1 + \cdots + I_m$, where $I_i, i \in \{1, \ldots, m\}$ is a root system of type $D_{k'}$. $G(I_i)$ is a group of order 4 implies that only summands of type D_k and E_7 are possible for R. Suppose first that E_7 is a summand of R. Since $\mathbf{n}(e_{7,1}) = \frac{3}{2}$, it follows that $\mathbf{n}(\eta(e_{7,1})) = \frac{3}{2}$. The only elements in $G(R')$ of norm $\frac{3}{2}$ are $d_{6,1}, d_{6,3}$. Without loss of generality, $\eta(e_{7,1}) = d_{6,1}$. Let $h = \eta^{-1}(d_{6,3})$, so that

$$\eta^{-1}(d_{6,2}) = \eta^{-1}(d_{6,1}) + \eta^{-1}(d_{6,3}) = e_{7,1} + h.$$

If $h = e_{7,1} \perp h_0$, then $\mathbf{n}(h_0) \equiv 0 \bmod 2\mathbf{Z}$, implying that the norm of $d_{6,2} \neq 1$. Thus, setting $g := e_{7,1} + h$, we see that $\mathbf{n}(g) > \mathbf{n}(\eta(g))$.

We are thus reduced to the case that R, R' contain only summands of type $D_j, j \geq 4$. Let k, respectively k' denote the maximal rank over all summands D_j of R, respectively R'.

$$\eta(d_{k,1}) = y_1 \perp \cdots \perp y_m,\ y_i \in G(I_i),\ i \in \{1, \ldots, m\}.$$

There is at least one $\ell \in \{1, \ldots, m\}$ such that $\eta^{-1}(y_\ell) = d_{k,1} \perp h$ or $\eta^{-1}(y_\ell) = d_{k,3} \perp h$. In any event,

$$\mathbf{n}(y_\ell) \leq \mathbf{n}(d_{k',1}) < \mathbf{n}(d_{k,1}) \leq \mathbf{n}(\eta^{-1}(y_\ell)),$$

so that we may take $g := \eta^{-1}(y_\ell)$. $\square$

A simple corollary of the theorem is stated below.

COROLLARY 6. *A root system of rank n whose word group is not the domain of an isofold must have one of the following forms:*

$$\sum_{i=1}^{n} \alpha_1 A_i + \delta_4 D_4 + \delta_5 D_5 + \delta_j D_j + \varepsilon_6 E_6 ,$$

$$\sum_{i=1}^{n} \alpha_i A_i + \varepsilon_6 E_6 + \varepsilon_7 E_7 ,$$

where the coefficients α_i, δ_4, δ_5 *are arbitrary nonnegative integers and* $\delta_j, \varepsilon_6, \varepsilon_7 \in \{0, 1\}$ *for* $j \in \{6, 7, 8, 9\}$.

REFERENCES

[CP] CONWAY, J.H. and V. PLESS. On the enumeration of self-dual codes. *J. Combin. Theory Ser. A 28* (1980), 26–53.

[CPS] CONWAY, J.H., V. PLESS and N.J.A. SLOANE. The binary self-dual codes of length up to 32: a revised enumeration. *J. Combin. Theory Ser. A 60* (1992), 183–195.

[Ke] KERVAIRE, M. Unimodular lattices with a complete root system. *L'Enseign. Math. (2) 40* (1994), 59–104.

[Ko] KOCH, H. The completeness principle for the Golay codes and some related codes. In: Arslanov et al. (eds.), *Algebra and Analysis.* De Gruyter and Co., Berlin (1996), 75–80.

[M] MORDELL, L.J. The definite quadratic forms in eight variables with determinant unity. *J. Math. Pures Appl. (9) 17* (1938), 41–46.

[N] NIEMEIER, H.-V. Definite quadratische Formen der Dimension 24 und Diskriminante 1. *J. Number Theory 5* (1973), 142–178.

[R] ROEGNER, K. Folding and fanning even unimodular lattices with complete root systems. Thesis, Technische Universität Berlin (1999).

[Sch] SCHARLAU, W. *Quadratic and Hermitian Forms.* Grundlehren der mathematischen Wissenschaften *270*. Springer-Verlag, Berlin (1985).

[Sm] SMITH, H.J.S. On the orders and genera of quadratic forms containing more than three indeterminates. *Proc. Roy. Soc. 16* (1867), 197–208.

[V] VENKOV, B.B. Even unimodular Euclidean lattices of dimension 32. II. *J. Sov. Math. 36*, 21–38 (1987); translation from *Zap. Nauchn. Sem. LOMI 134* (1984), 34–58.

[W1] WITT, E. Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe. *Abh. Math. Sem. Univ. Hamburg 14* (1941), 289–322.

[W2] —— Eine Identität zwischen Modulformen zweiten Grades. *Abh. Math. Sem. Univ. Hamburg 14* (1941), 323–337.

(Reçu le 26 janvier 2001)

Katherine Roegner

Paul-Robeson-Str. 12
D-10439 Berlin
Germany

vide-leer-empty