Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 48 (2002)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE FANNING METHOD FOR CONSTRUCTING EVEN UNIMODULAR LATTICES. I

Autor: ROEGNER, Katherine

Kapitel: 2. ISOFOLDS AND ISOFANS

DOI: https://doi.org/10.5169/seals-66072

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

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

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, $k \ge 2$, 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 $0 \le i \le 3$.

Let φ_{D_k} be the group isomorphism given by

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

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

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

(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 :

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

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

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

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

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

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 $3G(D_8)$:

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

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

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

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

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

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 $d_{8,3}^3$ as $d_{4,2}^1+d_{4,3}^2$, an inadmissible isotropic subgroup for $2G(D_4)+2G(D_8)$ is generated by

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

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

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

Exchanging $d_{8,1}^i$ for $d_{8,3}^i$ 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

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

$$a_{2,j}^i \mapsto a_{2,j}^i,\ 1 \le i \le 10,\ j \in \{0,1,2\}, \quad e_{6,1}^1 \mapsto a_{2,1}^1 + a_{2,1}^2, \quad e_{6,1}^2 \mapsto a_{2,1}^1 + a_{2,2}^2.$$

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

$$\begin{gathered}
a_{2,1}^1 + a_{2,1}^2 + a_{2,1}^3 + a_{2,1}^4 + a_{2,1}^5 + a_{2,1}^6 \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^3 + a_{2,2}^4 + a_{2,1}^7 + a_{2,1}^8 \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^5 + a_{2,2}^6 + a_{2,1}^9 + a_{2,1}^{10} \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^3 + a_{2,2}^5 + a_{2,1}^{11} + a_{2,1}^{12} \\
a_{2,1}^7 + a_{2,2}^8 + a_{2,1}^9 + a_{2,2}^{10} + a_{2,1}^{11} + a_{2,2}^{12}
\end{gathered}$$

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

$$\begin{gathered}
a_{2,1}^1 + a_{2,1}^2 + a_{2,1}^3 + a_{2,1}^4 + a_{2,1}^5 + a_{2,1}^6 \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^3 + a_{2,2}^4 + a_{2,1}^7 + a_{2,1}^8 \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^5 + a_{2,2}^6 + a_{2,1}^9 + a_{2,1}^{10} \\
a_{2,1}^1 + a_{2,1}^2 + a_{2,2}^3 + a_{2,2}^5 + e_{6,2}^1 \\
a_{2,1}^7 + a_{2,2}^8 + a_{2,1}^9 + a_{2,2}^{10} + e_{6,2}^2
\end{gathered}$$

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 $a^i_{2,1\,\mathrm{or}\,2}+a^j_{2,1\,\mathrm{or}\,2}+a^k_{2,1\,\mathrm{or}\,2}$ 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:

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

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.