3. Elementary isofans and isofolds

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **20.09.2024**

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:

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

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 $\eta_1, \eta_2 \colon G(R) \to G(R')$ 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

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

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

$$\eta'\colon G(D_{16}) \to G(D_8)$$

$$d_{16,0} \mapsto d_{8,0},\ d_{16,1} \mapsto d_{8,3},\ d_{16,2} \mapsto d_{8,2},\ d_{16,3} \mapsto d_{8,1}$$

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 $\eta_R\colon G(R) \to G(R')$ 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 $(j \in \{1, 3\})$
$D_{k+8} (k \geq 2)$	D_k	$\eta_{D_{k+8}}(d_{k+8,j}) = d_{k,j}$
$D_{k+4} + D_{\ell+4}$ $(k, \ell \geq 2)$	$D_k + D_\ell$	$\eta_{D_{k+4}+D_{\ell+4}}(d^1_{k+4,j}) = d^1_{k,j} + d^2_{\ell,2}$ $\eta_{D_{k+4}+D_{\ell+4}}(d^2_{\ell+4,j}) = d^1_{k,2} + d^2_{\ell,j}$
$D_{k+2} + E_7$ $(k \geq 2)$	$D_k + A_1$	$\eta_{D_{k+2}+E_7}(d_{k+2,j}) = d_{k,j} + a_{1,1}$ $\eta_{D_{k+2}+E_7}(e_{7,1}) = d_{k,2} + a_{1,1}$
$2E_7$	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

$$\eta_1 := \begin{cases} \eta_{D_k+D_\ell} & \text{if } g = d_{k,j_1} + d_{\ell,j_2}, j_1, j_2 \in \{1,2,3\}; \\ \eta_{2E_7} & \text{if } g = e^1_{7,1} + e^2_{7,1}; \\ \eta_{D_k+E_7} & \text{if } g = d_{k,j} + e_{7,1}, j \in \{1,2,3\}; \\ \eta_{2E_6} & \text{if } g = e^1_{6,\pm1} + e^2_{6,\pm1}. \end{cases}$$

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 η: $G(R) \to G(R')$ 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* δ_j, ε_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.