January 11, 2011

Diagonal lattices and rootless EE_8 pairs

Robert L. Griess Jr.
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109 USA
rlg@umich.edu

Ching Hung Lam
Institute of Mathematics
Academia Sinica
Taipei 10617, Taiwan
chlam@math.sinica.edu.tw

Abstract

Let E be an integral lattice. We first discuss some general properties of an SDC lattice, i.e., a sum of two diagonal copies of E in $E \perp E$. In particular, we show that its group of isometries contains a wreath product. We then specialize this study to the case of $E = E_8$ and provide a new and fairly natural model for those rootless lattices which are sums of a pair of EE_8-lattices. This family of lattices was classified in [7]. We prove that this set of isometry types is in bijection with the set of conjugacy classes of rootless elements in the isometry group $O(E_8)$, i.e., those $h \in O(E_8)$ such that the sublattice $(h-1)E_8$ contains no roots. Finally, our model gives new embeddings of several of these lattices in the Leech lattice.

Keywords: integral lattice, rootless lattice, isometry, E_8-lattice, Leech lattice
AMS subject classification: 20C10 Integral representations of finite groups; 11H56 Automorphism groups of lattices

Contents

1 Introduction

In this article, *lattice* means a finitely generated free abelian group with a rational valued symmetric bilinear form.

We begin by defining the main construction used in this article.

Notation 1.1. *Suppose that we are given an integral lattice, E, and an isometry $h \in O(E)$. In $E \perp E$, we have two sublattices*

$$M := \{(x, x) \mid x \in E\} \quad \text{and} \quad N := \{(x, hx) \mid x \in E\}.$$

Clearly, $M \cong N \cong \sqrt{2}E$ (where $\cong$ indicates isometry of quadratic spaces). Define $L := L(E, h) := M + N$. We call L an SDC-lattice or, more precisely, an $SCD(E, h)$-lattice or $SDC(E)$-lattice, meaning a sum of diagonal copies (of the fixed input lattice, E, using the isometry h).

Clearly, L is integral (since it is a sublattice of $E \perp E$) and even (since the generating set $M \cup N$ has only even norm vectors). Our first main result shows that L has a large group of isometries (1.2).

Theorem 1.2. *Let L, h be as in (1.1), where h has order n. Then $O(L)$ contains a chain of subgroups $\langle t_M, t_N \rangle \leq W_{M,N} \cong \mathbb{Z}_n \wr \mathbb{Z}_2$. Furthermore, each of t_M, t_N is a wreathing involution of $W_{M,N}$.*

Some lattices of great interest have this form. One has for instance the Barnes-Wall lattices (for which M, N are scaled copies of smaller rank Barnes-Wall lattices and $h^2 = -1$). Additional examples are listed in Section 5. One should note the trivial cases $h = 1$, for which $M = N$, and $h = -1$, for which $M + N = M \perp N$.

The term EE_8*-lattice* means a lattice isometric to $\sqrt{2}E_8$ [7].

We now consider rootless integral lattices spanned by a pair of EE_8-lattices. They were studied and classified in [7]. Recently, we realized that they may be expressed as SDC-lattices (1.3). The next two main results shows how they may be expressed as SDC-lattices (1.3).

Theorem 1.3. *All rootless EE_8 pairs listed in [7, Table 1] can be embedded into $E_8 \perp E_8$ as $SDC(E_8)$-lattices (1.1).*

Theorem 1.4. *There is a bijection between the conjugacy classes of rootless elements in $O(E_8)$ and the isometry classes of rootless EE_8 pairs.*

An application of modeling the lattices of [7] as $SDC(E_8)$-lattices is that one can see relatively natural embeddings of some of them into the Leech lattice; see Section A. Such embeddings were first demonstrated in [7], but the proofs were rather technical.

Conventions. Group actions will be on the left. Notations are generally standard. We mention the relatively new notations EE_8 for $\sqrt{2}E_8$ [7], RSSD and SSD (2.1). For background on groups and lattices, see [6].

2 About SDC lattices

In this section, E is an arbitrary integral lattice. Later in this article, we shall specialize to the case $E = E_8$.

Definition 2.1. *A sublattice X of an integral lattice Y is called RSSD if $2Y \leq X + ann(X)$. If X is RSSD, the orthogonal transformation t_X which is -1 on X and 1 on $ann(X)$ takes Y to itself, whence $t_X \in O(Y)$.*

The lattice X is called SSD if $2X^* \leq X$. An SSD lattice X contained in the integral lattice Y is RSSD in Y. See [5, 7, 6].

We use the notations of (1.1).

Lemma 2.2. *As maps on $E \perp E$, $t_M : (x, y) \mapsto (-y, -x)$ and $t_N : (x, y) \mapsto (-h^{-1}y, -hx)$.*

Proof. Direct calculation. Here is an argument for t_M. Write $(x, y) = (\frac{1}{2}(x + y), \frac{1}{2}(x + y)) + (\frac{1}{2}(x - y), -\frac{1}{2}(x - y))$ and note that the first summand on the right side is in M and the second is in $ann(M)$. Therefore, t_M negates the first summand and fixes the second.

To verify the formula for t_N, notice that this map negates N and fixes all $(w, -hw)$, $w \in L$. Then use the decomposition

$(x, y) = (\frac{1}{2}(x + h^{-1}y), \frac{1}{2}(hx + y)) + (\frac{1}{2}(x - h^{-1}y), \frac{1}{2}(-hx + y))$. □

Notation 2.3. *Define sublattices $N' := \{(x, h^{-1}x) \mid x \in E\}$ and $L' := M + N'$.*

Define the following elements of $O(E \perp E)$:

$\beta : (x, y) \mapsto (hx, y)$;

$\gamma : (x, y) \mapsto (x, hy)$;

$\delta : (x, y) \mapsto (hx, hy)$;

$\delta' : (x, y) \mapsto (h^{-1}x, hy)$.

These maps satisfy $\delta = \beta\gamma = \gamma\beta$ and $\delta' = \beta^{-1}\gamma = \gamma\beta^{-1}$.

We denote by $W(E, h)$ the group $\langle t_M, t_N, \beta, \gamma \rangle$. It is a subgroup of $O(E \perp E)$ (but we shall see that it embeds in $O(L)$ (2.11)).

Lemma 2.4. *(i) $t_N t_M = \delta'$;*

(ii) $\beta = t_M \gamma t_M = t_N \gamma t_N$;

(iii) $W(E, h)$ is generated by any three of t_M, t_N, β, γ. Furthermore, $W(E, h) = (\langle \beta \rangle \times \langle \gamma \rangle)\langle t_M \rangle$ is isomorphic to the wreath product $\mathbb{Z}_{|h|} \wr \mathbb{Z}_2$;

(iv) $\langle \beta, \gamma \rangle$ contains $\langle \delta, \delta' \rangle$ with index $(2, |h|)$.

(v) In $W(E, h)$, the stabilizer of M is $\langle t_M \rangle \times \langle \delta \rangle$ and the stabilizer of N is $\langle t_N \rangle \times \langle \delta \rangle$.

Proof. (i) Direct calculation.

(ii) One may check the first equality by direct calculation. For the second, note that $t_N = \delta' t_M = t_M(\delta')^{-1}$ and that δ' and γ commute.

(iii) Let V be the subgroup of $W(E,h)$ generated by three of the generators and let $H := \langle\beta\rangle \times \langle\gamma\rangle$. Then V covers $W(E,h)/H \cong 2$, i.e., $W(E,h) = HV$. If V includes generators β, γ, then $V \geq H$ and we are done. If not, V contains both t_M and t_N, whence also δ'. Clearly, H is generated by any two of β, γ, δ' and so we conclude that $V = W(E,h)$.

(iv) Clearly, $\langle\beta,\gamma\rangle$ contains $\langle\delta,\delta'\rangle$. The latter equals $\langle\beta^2,\gamma^2,\delta\rangle$ and has index $(2,|h|)$ in $\langle\beta,\gamma\rangle$.

(v) Let S be the stabilizer of M in $W(E,h)$. We have $\langle t_M\rangle \leq S$. Since $W(E,h) = \langle t_M\rangle H$, the Dedekind law implies that $S = \langle t_M\rangle(S \cap H)$. Clearly, $(S \cap H) = \langle\delta\rangle$. This completes the analysis for M. The argument for N is similar. □

Lemma 2.5. *$\gamma(M) = N$, $\gamma(N') = M$ and $\gamma(L') = L$.*

Lemma 2.6. *(i) $2L \leq M + ann(M)$;*

(ii) $2L' \leq M + ann(M)$.

Proof. (i) It suffices to prove that $2N \leq M + ann(M)$. An element of N has shape (x, hx) for some $x \in E$. We have $2(x,hx) = (x+hx, x+hx) + (x-hx, -x+hx)$. The first summand is in M and the second is in $ann(M)$.

(ii) Use (i) with h replaced by h^{-1}. □

Lemma 2.7. *$2L \leq N + ann(N)$.*

Proof. Apply γ to the containment (2.6) (ii).

Corollary 2.8. *$\langle t_M, t_N\rangle$ maps L to itself.*

Proof. We have shown that M and N are RSSD lattices. Therefore the isometries t_M and t_N map L to itself. □

Remark 2.9. *The isometry group of L contains an isomorphic copy $C(E,h)$ of $C_{O(E)}(h)$, acting diagonally on $E \perp E$. We have $\langle -1, \delta\rangle \leq C(E,h)$ and $C(E,h)$ centralizes $\langle t_M, t_N\rangle$.*

Lemma 2.10. *We have*

(i) $L \cap (E \perp 0) = Im(h-1) \perp 0$; and

(ii) $L \cap (0 \perp E) = 0 \perp Im(h-1)$.

Proof. (i) Consider $a, b \in E$. Then $(a,a) + (b,hb) \in E \perp 0$ if and only if $a = -hb$ if and only if $a + b = (1-h)b$. This proves $L \cap (E \perp 0) \leq Im(h-1) \perp 0$. Conversely, suppose that $c \in E$. Then by (2.2), $((1-h)c, 0) = (c,c) + (-hc, -c) = t_M(-(c,c) + (c,hc)) \in t_M(M+N) = M+N$ (2.8). This proves $L \cap (E \perp 0) \geq Im(h-1) \perp 0$.

(ii) This follows from (i) and use of t_M (2.2), (2.8). □

Proposition 2.11. *(i) $W(E,h)$ stabilizes L.*

(ii) The action of $W(E,h)$ on L is faithful, so restriction gives an embedding of $W(E,h)$ in $O(L)$.

Proof. (i) In view of (2.4)(iii) and (2.8), it suffices to prove that γ is in $O(L)$. By (2.5), it suffices to prove that $\gamma(N) \leq L$. We take $a \in E$ and calculate $\gamma(a, ha) = (a, h^2a) = (a, ha) + (0, h^2a - ha))$. Obviously, $(a, ha) \in N \leq L$. We have $(0, h^2a - ha)) = (0, (h-1)ha)$, which is in $L \cap (0 \perp E)$ by (2.10), so we are done.

(ii) Let K be the kernel of the action of $W(E,h)$ on L. We may assume that $E \neq 0$. By (2.4)(v), $K \leq \langle t_M, \delta \rangle$.

We shall argue that $K \leq \langle \delta \rangle$. Suppose otherwise. Consider an integer i so that $z := \delta^i t_M \in K$. Then z takes (x,x) to $(-h^ix, -h^ix)$ which is (x,x) since $z \in K$. It follows that $h^i = -1$ on E. By (2.2), z takes (x, hx) to (hx, x), which must equal (x, hx), for all $x \in E$. We conclude that $h = 1$. Since $E \neq 0$, this incompatible with $h^i = -1$.

We have $K \leq \langle \delta \rangle$. Since the group $\langle \delta \rangle$ acts faithfully on M, it acts faithfully on L and we conclude that $K = 1$. □

Lemma 2.12. *Let M and N be defined as above. Then*

$$ann_N(M) = \{(\alpha, -\alpha) \mid \alpha \in E \text{ and } h\alpha = -\alpha\}, \quad \text{and}$$
$$ann_M(N) = \{(\alpha, \alpha) \mid \alpha \in E \text{ and } h\alpha = -\alpha\}.$$

Proof. We prove the first equality. The proof of the second is similar.

Let $(\alpha, h\alpha) \in N$. Then

	$(\alpha, h\alpha)$ annihilates M
if and only if	$(\alpha, \beta) + (h\alpha, \beta) = 0$ for all $\beta \in E$
if and only if	$(h\alpha + \alpha, \beta) = 0$ for all $\beta \in E$
if and only if	$h\alpha = -\alpha$.

Thus, $ann_N(M) = \{(\alpha, -\alpha) \in E \perp E \mid \alpha \in E$ and $h\alpha = -\alpha\}$ as desired. □

Remark 2.13. *(i) Given a pair of isometric doubly even lattices, M, N in Euclidean space, such that $M+N$ is integral and M, N are RSSD in $M+N$, when is there a representation of $M+N$ in the form of (1.1)? One would need to define a suitable h. The following example indicates a caution.*

Let the lattice L have basis u, v and Gram matrix $\begin{pmatrix} 2a & b \\ b & 2a \end{pmatrix}$, for integers $a \geq 1$ and b. For positive definiteness, we require $4a^2 - b^2 > 0$. The A_2-lattice is such an example.

Let E be the rank 1 lattice with Gram matrix (a). Then $M := span\{u\}$ and $N := span\{v\}$ are sublattices of L isometric to $\sqrt{2}E$ and their sum is L. The condition that M and N be RSSD in L is $a|b$.

If L were isometric to $SDC(E, h)$ with M, N as in (1.1), then $h = \pm 1$ and so $b \in 2a\mathbb{Z}$, which implies the RSSD condition $a|b$. The necessary condition $b \in 2a\mathbb{Z}$ implies that L is not positive definite if $b \neq 0$, so the above L are not $SDC(E, h)$ if $b \neq 0$.

(ii) A study of SDC lattices was carried out by Paul Lewis in his 2010 undergraduate research project [8]. For many cases of familiar input lattice E and isometry h, the resulting $SDC(E, h)$ is another familiar lattice, but there are surprises.

3 About rootless isometries

We continue to use the notations (1.1).

Definition 3.1. *We say $h \in O(E)$ is rootless if $(h-1)E$ contains no roots.*

Lemma 3.2. *Let E be an even lattice. The sum $M+N$ is rootless if and only if h is rootless.*

Proof. Let $x = (\alpha + \beta, \alpha + h\beta) \in M + N$, where $\alpha, \beta \in E$. If both $\alpha + h\beta$ and $\alpha + \beta$ are non-zero, then $(x, x) \geq 2 + 2 = 4$.

If $\alpha + \beta = 0$, then $x = (0, (h-1)\beta)$ and if $\alpha + h\beta = 0$, then $x = (-(h-1)\beta, 0)$. Thus, $(x, x) > 2$ if $(h-1)E$ is rootless.

On the other hand, $(0, (h-1)\alpha) \in M + N$ for any $\alpha \in E$. Therefore, $(h-1)E$ is rootless if $M+N$ is. □

We now take E to be E_8 and begin determination of those h for which the conditions of (3.2) hold.

Lemma 3.3. *Suppose that $h \in O(E)$ and h is rootless. Then so is h^i for all $i \in \mathbb{Z}$.*

Proof. We may assume that $i \geq 1$. Since $h^i - 1 = (h-1)(1 + h + h^2 + \cdots + h^{i-1})$, this is clear. □

Notation 3.4. *Recall that if g is a group element of finite order mn, with $(m, n) = 1$, then g is uniquely expressible as $g = hk$, where h has order m and k has order n and $hk = kh$. Such h, k lie in $\langle g \rangle$. If m is a power of the prime p, we call h, k the p-part, p'-part of g, respectively. Denote by $g_p, g_{p'}$ be the p-part, p'-part of g, respectively.*

Corollary 3.5. *If $h \in O(E)$ is rootless, then so are the p-parts of h, for all primes p.*

Corollary 3.6. *Suppose that E contains roots, that $h \in O(E)$ is rootless and that p, q are distinct primes so that $pq||h|$. Then at most one of h_p, h_q has no eigenvalue 1.*

Proof. If h_p has no eigenvalue 1, $(h_p - 1)E$ has index a power of p. If h_q has no eigenvalue 1, $(h_q - 1)E$ has index a power of q. If both of these statements are true then $(h-1)E$ contains $(h_p - 1)E + (h_q - 1)E$, which by relative primeness has index 1 in E. This contradicts the rootless property of h. □

3.1 Root lattice of type A

We shall review some basic properties of the root lattices of type A_n.

We use the *standard model* for A_n, i.e.,

$$A_n = \left\{ (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} \;\middle|\; \sum_{i=1}^{n+1} x_i = 0 \right\}.$$

Then the roots of A_n are given by

$$\{\pm(e_i - e_j) \mid 1 \leq i < j \leq n+1\},$$

where $\{e_1 = (1, 0, \ldots, 0), \ldots, e_{n+1} = (0, 0, \ldots, 1)\}$ is the standard basis of $\mathbb{Z}^{n+1}$.

Notation 3.7. *Recall that* $(A_n^*)/A_n \cong \mathbb{Z}_{n+1}$. *Let* $\gamma_{A_n}(0) = 0$ *and*

$$\gamma_{A_n}(j) = \frac{1}{n+1}\left(-(n+1-j)\sum_{i=1}^{j} e_i + j\sum_{i=j+1}^{n+1} e_i\right), \text{ for } j = 1, \dots, n.$$

Then $\gamma_{A_n}(j) \in A_n^*$. *In fact,* $\{\gamma_{A_n}(0), \gamma_{A_n}(1), \dots, \gamma_{A_n}(n)\}$ *forms a transversal of* A_n *in* A_n^* *[2, Chapter 4]. We also note that the norm of* $\gamma_{A_n}(j)$ *is equal to* $j(n+1-j)/(n+1)$ *for all* $j = 0, \dots, n$.

Notation 3.8. *Let* h_{A_n} *be an* $(n+1)$*-cycle in* $Weyl(A_n) \cong Sym_{n+1}$.

Lemma 3.9. *For* $j = 1, \dots, n$, $(h_{A_n} - 1)(\gamma_{A_n}(j))$ *is a root.*

Proof. By definition, $(h_{A_n} - 1)(\gamma_{A_n}(j)) = e_1 - e_{j+1}$ is a root. □

Lemma 3.10. $(h_{A_n} - 1)A_n$ *is rootless.*

Proof. We may assume h_{A_n} is the cyclic permutation of the $n+1$-coordinates.

Suppose $(h_{A_n} - 1)\alpha$ is a root for some $\alpha = (x_1, x_2, \dots, x_{n+1}) \in A_n$. Without loss, we may assume $(h_{A_n} - 1)\alpha = e_1 - e_j$ for some $j \geq 2$.

Then we have

$$x_{n+1} - x_1 = 1,\ x_{j-1} - x_j = -1,\ x_1 = \cdots = x_{j-1} \text{ and } x_j = \cdots = x_{n+1}.$$

That implies $x_{n+1} = 1 + x_1$. Moreover, $x_1 + \cdots + x_{n+1} = 0$. Thus, we have $(j-1)x_1 + (n+2-j)(x_1+1) = 0$ or $x_1 = -\frac{n+2-j}{n+1}$, which is not an integer since $2 \leq j \leq n+1$, a contradiction. □

Lemma 3.11. *Let* A_n^* *be the dual lattice of* A_n. *Then* $(h_{A_n} - 1)A_n^* = A_n$

Proof. *First proof:* Again, we shall use the standard model for A_n. Then A_n^* is the $\mathbb{Z}$-span of

$$\frac{1}{n+1}(1,1,1,\dots,1,-n), \frac{1}{n+1}(1,1,\dots,-n,1), \dots, \frac{1}{n+1}(1,-n,1,\dots,1,1).$$

Note that

$$(h_{A_n} - 1)\left(\frac{1}{n+1}(1,1,1,\dots,1,-n)\right) = (1,0,\dots,0,-1) \in A_n.$$

Similarly, we can show that $(h_{A_n} - 1)A_n^* \leq A_n$.

On the other hand, the set

$$\{(1,0,\ldots,0,-1),(0,0,\ldots,-1,1),\ldots,(0,-1,1,\ldots,0)\}$$

spans A_n and hence $(h_{A_n}-1)A_n^* = A_n$.

Second proof: Since $(h-1)A_n^* = (h-1)\mathbb{Z}^{n+1} = span\{e_i - e_{i+1} \mid i = 1,2\ldots\}$, this is clear. □

Lemma 3.12. *Let X be a type A_m lattice contained in E_8. Then X is a direct summand unless $m = 8$.*

Proof. If X is properly contained in a summand, S, of E_8, then there exists an integer $d \geq 2$ so that $d^2 | det(X)$. Since $det(X) = m+1$ and $m \leq 8$, $m = 3$ or $m = 8$. If $m = 3$, $d = 2$ and so $det(S) = 1$, whence $S \cong \mathbb{Z}^4$, which is an odd lattice, a contradiction. Therefore, $m = 8$. □

Lemma 3.13. *Identify $Q := A_{i_1} \perp \cdots \perp A_{i_\ell}$ with a rank 8 sublattices of E_8. For any $1 \leq k \leq \ell$, define $h := h_k := h_{A_{i_1}} \oplus \cdots \oplus h_{A_{i_k}} \oplus id \oplus \cdots \oplus id$.*

(a) Suppose that for any $x \in E_8 \setminus Q$, $(h-1)x$ is either 0 or has non-zero projections to at least two of the A_i's. Then $(h-1)E_8$ is rootless.

(b) Suppose there exists an element $x \in E_8 \setminus Q$ such that $(h-1)x$ has non-zero projections to exactly one of the A_i's. Then $(h-1)E_8$ has a root.

Proof. (a) By Lemma 3.10, it is clear that $(h-1)Q$ has no roots. Now let $x \in E_8 \setminus Q$. Then by our assumption and Lemma 3.11, $(h-1)x$ is either 0 or has norm $\geq 2 \times 2$. Hence, $(h-1)E_8$ has no roots.

(b) Let $x \in E_8 \setminus Q$ such that $(h-1)x$ has non-zero projections to exactly one of the A_i's, say to A_{i_1}.

Let a be the projection of x to $A_{i_1}^*$. Then there exists $j \in \{1,\ldots,i_1\}$ such that a is in the coset $\gamma_{A_{i_1}}(j) + A_{i_1}$ (cf. Notation 3.7). Thus, there exists $b \in A_{i_1}$ such that $a + b = \gamma_{A_{i_1}}(j)$. In this case,

$$(h-1)(x+b) = (h_{A_{i_1}}-1)(a+b) = (h_{A_{i_1}}-1)(\gamma_j),$$

which is a root by Lemma (3.9). □

4 Eliminating cases

We begin to study the cases where h is p-element for some prime p. Recall that $O(E_8)$ has order $2^{14}{\cdot}3^5{\cdot}5^2{\cdot}7$.

Convention. When we consider an embedding of lattices $X \leq Y$, we may describe it informally as containment of isometry types, for example "$A_1^8 \leq E_8$" or "$A_2^3 \leq E_6$". Given such a containment, one may use notations for isometries of the sublattice and make use of their unique extensions to overlattices. This informally should not cause confusion.

4.1 The prime 7

Lemma 4.1. *There is no rootless element of order* 7 *in* $O(E_8)$.

Proof. By Sylow's theorem, there is only one conjugacy class of order 7 subgroups in $O(E_8)$. Without loss, we may assume

$$h = h_{A_6} \oplus id_B,$$

where $B = ann_{E_8}(A_6)$. However, $(h-1)E_8$ has roots by Lemma 3.9. □

4.2 The prime 5

Theorem 4.2. *A rootless element of order* 5 *is fixed point free and is conjugate to* $h_{A_4} \oplus h_{A_4}$.

Proof. Let h be an order 5 in $O(E_8)$. Then there is a root α such that $h\alpha \neq \alpha$ since E_8 is generated by roots. Then, $(h^4 + h^3 + h^2 + h + 1)(\alpha) = 0$ and $((h^4+h^3+h^2+h+1)(\alpha), \alpha) = 0$. This implies $(h\alpha, \alpha) + (h^2\alpha, \alpha) = -1$ since $(h\alpha, \alpha) = (h^4\alpha, \alpha)$, $(h^2\alpha, \alpha) = (h^3\alpha, \alpha)$ and $(\alpha, \alpha) = 2$. By Cauchy-Schwarz inequality, we have $|(h\alpha, \alpha)| < 2$ and $|(h^2\alpha, \alpha)| < 2$ and thus $(h\alpha, \alpha) = -1$, $(h^2\alpha, \alpha) = 0$ or $(h\alpha, \alpha) = 0$, $(h^2\alpha, \alpha) = -1$. Therefore, $K = span\{h^i\alpha \mid 0 \leq i \leq 3\} \cong A_4$ since the Gram matrix of K is given by

$$\begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix}.$$

Then $ann_{E_8}(K) \cong A_4$ [6, (5.3.2)] and h stabilizes both K and $ann_{E_8}(K)$.

Case 1: h fixes $ann_{E_8}(K)$ pointwise. Then h is conjugate to $h_{A_4} \oplus id_{A_4}$, which is not rootless by (3.13) (b).

Case 2: There exists a root $\beta \in ann_{E_8}(K)$ such that $h\beta \neq \beta$. Then $ann_{E_8}(K) = span\{h^i\beta \mid 0 \leq i \leq 4\} \cong A_4$. In this case, h is fixed point free and lies in $Weyl(K) \times Weyl(ann_{E_8}(K)) \cong Sym_5 \times Sym_5$. Such elements form a single conjugacy class, so h is conjugate to $h_{A_4} \oplus h_{A_4}$ and h is rootless (3.11). □

4.3 The prime 3

Order 3

Notation 4.3. *Let h be an element of order 3 in $O(E_8)$. Let F be the fixed point sublattice of h in E_8. Let $J := ann_{E_8}(F)$.*

By the analysis in [7], $\mathcal{D}(F) \cong 3^s$ for some integer s. Thus, by [7, Lemma D.9], $F \cong 0, A_2, A_2 \perp A_2$, or E_6. Note that in each case, F contains an orthogonal direct sum of A_2's with finite index.

We have $J \cong E_8, E_6, A_2 \perp A_2$ and A_2, respectively and h is fixed point free on J. Recall that the fixed point free elements of order 3 in $O(E_8)$ form one conjugacy class and they are conjugate to $h_{A_2}^{\oplus 4}$ in $O(E_8)$. The fixed point free elements of order 3 also form one conjugacy class in $O(E_6)$ and they are conjugate to $h_{A_2}^{\oplus 3}$ (see for example [1]). Therefore, in each case, there exists a sublattice of E_8 which we may identify with A_2^4 such that $h = h_{A_2}^{\oplus 4-k} \oplus id_{A_2}^{\oplus k}$, where $k = \frac{1}{2} dim F$. Recall that E_8/A_2^4 can be identified with the tetracode $\mathcal{C}_4$, which is a self-dual code of length 4, minimal weight 3 [2, 3]. Now, by Lemma 3.13, we have the theorem.

Theorem 4.4. *Let h be an element of order 3 in $O(E_8)$. Then h is rootless if and only if $F = Fix(h) = 0$ or $\cong A_2$. Identify A_2^4 with a sublattice of E_8. Then, h is conjugate to $h_{A_2}^{\oplus 4}$ if $F = 0$ and $h_{A_2}^{\oplus 3} \oplus id_{A_2}$ if $F \cong A_2$.*

Order 9

Notation 4.5. *Let h be an element of order 9 in $O(E_8)$. Let $g := h^3$ and $F := Fix(h^3) = Ker(h^3 - 1)$. Let $J := ann_{E_8}(F)$.*

Then the minimal polynomial of h on J is divisible by the irreducible cyclotomic polynomial $x^6 + x^3 + 1$ and the minimal polynomial for h on F is $x - 1$ or $x^2 + x + 1$. Hence, $rank(F) = 2$ (whence $F \cong A_2$) and $rank(J)$ is 6. Since h stabilizes both F and $J = ann_{E_8}(F) \cong E_6$, $h|_F$ defines an element of order 1 or 3 in $O(F)$ and $h|_J$ is an order 9 element in $O(J)$.

Lemma 4.6. *In $\mathbb{Z}_p \wr \mathbb{Z}_p$, there are $(p-1)^2$ conjugacy classes of elements of order p^2. More precisely, we let $B = B_1 \times \cdots \times B_p$ where each factor B_i has order p and the order p automorphism g acts on B by cyclically permuting the p factors. Thus the semidirect product $B\langle g\rangle$ is isomorphic to $\mathbb{Z}_p \wr \mathbb{Z}_p$. The classes of order p^2 are represented by ${u_i}^k g^i$, $i = 1, 2, \ldots, p-1$, $k = 1, \ldots, p-1$, where for each i, u_i is a generator for B as a $\langle g\rangle$-module.*

Proof. We count. Two such elements $u_i^k g^i$ and $u_j^\ell i g^j$ can not be conjugate if $i \neq j$ or $k \neq \ell$ since their images modulo $(B\langle g\rangle)'$ are distinct. The conjugacy class of such an element has cardinality p^{p-1} since B is a free module for $B\langle g\rangle/B$. Therefore, we have accounted for $(p-1)(p^p - p^{p-1})$ elements of $B\langle g\rangle$. The p^p elements of B have order 1 or p. If $i = 1, 2, \ldots, p-1$ and $v \in B$ does not generate B as a $\langle g\rangle$-module, then vg^i has order 1 or p. This latter category accounts for the remaining $(p-1)p^{p-1}$ elements of $B\langle g\rangle$. □

Corollary 4.7. *In $O(E_6)$, there is just one conjugacy class of elements of order 9.*

Proof. We view the E_6 lattice as an overlattice of A_2^3, defined by glue vector $(1,1,1)$. From this viewpoint, it is obvious that we have a group of automorphisms $H := Weyl(A_2) \wr Sym_3$. The analysis of (4.6) shows that we have exactly four conjugacy classes of elements of order 9 in a Sylow 3-subgroup of H. These classes are fused in a Sylow 3-normalizer in H. □

Theorem 4.8. *There are no rootless elements of order 9 in $O(E_8)$.*

Proof. Let $h' = h|_J \in O(E_6)$ be an element of order 9. Recall that E_6 contains a sublattice of type A_2^3 and we may assume

$$E_6 = span\{A_2^3, (\gamma, \gamma, \gamma)\}$$

where $\gamma = \frac{1}{3}(1, 1, -2) \in A_2^*$.

Note that there is only one conjugacy class of order 9 in $O(E_6)$ (4.7). Thus, we may assume that $h' = \tau\sigma$, where $\sigma = h_{A_2} \oplus id_{A_2} \oplus id_{A_2}$ and τ is a cyclic permutation of the 3 copies of A_2.

Let $\alpha = (\gamma, \gamma, \gamma) = \frac{1}{3}(1, 1, -2; 1, 1, -2; 1, 1, -2)$. Then

$$h'(\alpha) = \frac{1}{3}(1, 1, -2; -2, 1, 1; 1, 1, -2) \text{ and } (h' - 1)\alpha = (0, 0, 0; 1, 0, -1; 0, 0, 0),$$

which is a root. □

There are no elements of order 27 in $O(E_8)$, by (4.6) and the fact that $Weyl(E_6) \times Weyl(A_2)$ embeds with index prime to 3 in $O(E_8)$. Therefore, we have treated all cases of 3-elements in $O(E_8)$.

4.4 The prime 2

Order 2

Suppose $h \in O(E_8)$ has order 2. Then the (-1)-eigenlattice $L^-(h)$ of h is a RSSD sublattice of E_8. By the classification of RSSD lattices in E_8 [7, Lemma D.2], there are nine possible cases up to conjugation and $L^-(h) \cong A_1^k, k \leq 4, D_4, D_4 \perp A_1, D_6, E_7$ or E_8. For each case, there exists a sublattice $A_1^8 < E_8$ such that $h = h_{A_1}^{\oplus k} \oplus id_{A_1}^{\oplus(8-k)}$, where $k = dimL^-(h)$ (proof: each of the above RSSD lattices contains an orthogonal direct sum of A_1s with finite index).

Theorem 4.9. *Suppose $h \in O(E_8)$ has order 2. Then h is rootless if and only if $L^-(h) \cong D_4, D_6, E_7$ or E_8.*

Proof. Suppose $dim(L^-(h)) = k$. Then there exists $\alpha_1, \dots, \alpha_k \in L^-(h)$ such that $(\alpha_i, \alpha_j) = 2\delta_{i,j}$ for $i, j = 1, \dots, k$. Take $\alpha_{k+1}, \dots, \alpha_8 \in ann_{E_8}(L^-(h))$ such that

$$A = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_8 \cong A_1^8.$$

Then the quotient group E_8/A can be identified with the Hamming $[8, 4, 4]$ code H_8.

Case 1: $L^-(h) \cong A_1^k$, $1 \leq k \leq 4$. By identifying a codeword with its support, we know that $\{1, \dots, k\} \notin H_8$ since the minimal weight of H_8 is 4 and $L^-(h) \cong D_4$ if $\{1, 2, 3, 4\} \in H_8$. Hence there exists $a \in H_8$ such that $|\{1, \dots, k\} \cap a|$ is odd. Without loss, we may assume a has weight 4. Then $|\{1, \dots, k\} \cap a| = 1$ or 3.

If $|\{1, \dots, k\} \cap a| = 1$, let $\alpha_a = \frac{1}{2}\sum_{i \in a} \alpha_i$. Then $(h-1)\alpha_a = -\alpha_j$ is a root, where $\{j\} = \{1, \dots, k\} \cap a$. If $|\{1, \dots, k\} \cap a| = 3$, let $\bar{a} = \{1, \dots, 8\} \setminus a$. Then $|\{1, \dots, k\} \cap \bar{a}| = 1$ and we get a contradiction as before. We conclude that h is not rootless.

Case 2: $L^-(h) \cong D_4 \oplus A_1$. Then $k = 5$. There exists $\{i_1, i_2, i_3, i_4\} \subset \{1, \dots, 5\}$ such that $\{i_1, i_2, i_3, i_4\} \in H_8$. Let $a = \{1, \dots, 8\} \setminus \{i_1, i_2, i_3, i_4\}$. Then $|a \cap \{1, \dots, 5\}| = 1$ and $(h-1)\alpha_a$ is a root.

Case 3: $L^-(h) \cong D_4$. Then $k = 4$ and $\{1, 2, 3, 4\} \in H_8$. Since H_8 is a self dual code, for any $a \in H_8$, $|a \cap \{1, 2, 3, 4\}|$ is even. Hence, for any $\alpha \in E_8 \setminus A$, $(h-1)\alpha$ is either 0 or has 2 or 4 non-zero projections to the A_1's. Thus, by Lemma (3.13) (a), h is rootless.

Case 4: $L^-(h) \cong D_6, E_7$ or E_8. Then $k \geq 6$. Since the minimal weight of H_8 is 4, we have $|a \cap \{1, \dots, k\}| \geq 2$ for any nonzero element $a \in H_8$. Hence, h is rootless by Lemma (3.13) (a). □

Order 4

Notation 4.10. *Let h be a rootless element of order 4 and set $J := Ker(h^2 + 1)$.*

Then J has even rank and h^2 is also rootless. Since $det(h^2) = 1$, (4.9) implies that $J \cong D_4, D_6$, or E_8.

Lemma 4.11. *Let $h \in O(D_{2n})$ be an element of order 4 and $h^2 = -1$. Then there exists an orthogonal set of roots $\{\alpha_1, \dots, \alpha_{2n}\} \subset D_{2n}$ such that $h(\alpha_{2i-1}) = \alpha_{2i}$ and $h(\alpha_{2i}) = -\alpha_{2i-1}$ for all $i = 1, \dots, n$.*

Proof. We shall use the standard model for D_{2n}, i.e.,

$$D_{2n} = \{\sum_{i=1}^{2n} x_i e_i \mid x_1 + \cdots + x_{2n} \equiv 0 \mod 2\},$$

where $\{e_1, \dots, e_{2n}\}$ is the standard basis of $\mathbb{Z}^{2n}$.

Then up to conjugacy in $O(D_{2n})$, we may assume that $h = DP$, where P is a matrix associated to a permutation $\sigma \in Sym_{2n}$ and D is a diagonal matrix with diagonal entries 1 or -1. Note that

$$P = \sum_{i=1}^{2n} E_{\sigma i, i},$$

where $E_{i,j}$ is a matrix whose (i, j)-entry is 1 and all other entries are 0.

Let $\epsilon_1, \dots, \epsilon_{2n}$ be the diagonal entries of D. Then

$$DPD = \sum_{i=1}^{2n} \epsilon_{\sigma i} \epsilon_i E_{\sigma i, i}$$

and

$$(DP)(DP) = (DPD)P = \sum_{1 \le i,j \le 2n} \epsilon_i \epsilon_{\sigma_i} \delta_{i, \sigma_j} E_{\sigma i, j}.$$

By $h^2 = -1$, we have $(DP)(DP) = (DPD)P = -I$. This implies $\sigma^2 = 1$ and $\epsilon_{\sigma_i} \epsilon_i = -1$. Therefore, by rearranging the indices if necessary, the matrix of h with respect to the standard basis is given by

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & -1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & -1 & 0 \end{pmatrix}.$$

Now define $\alpha_{2i-1} = e_{2i-1} - e_{2i}$ and $\alpha_{2i} = e_{2i-1} + e_{2i}$ for $i = 1, \dots n$. Then $\{\alpha_1, \alpha_2, \dots, \alpha_{2n-1}, \alpha_{2n}\}$ satisfies the required properties. □

We now treat the order 4 case according to the three types of J (4.10).

Notation 4.12. *Let $F := ann_{E_8}(J)$. Note that h^2 acts trivially on F.*

Case 1: $J \cong E_8$. Then h is fixed point free and h^2 acts as -1 on E_8. Such elements form one conjugacy class (4.11).

Case 2: $J \cong D_6$. Then $F \cong A_1 \perp A_1$. Then by Lemma 4.11, there exists $\{\alpha_1, \alpha_2, \dots, \alpha_6\} \subset J$ such that $h(\alpha_{2i-1}) = \alpha_{2i}$, $h(\alpha_{2i}) = -\alpha_{2i-1}$ for $i = 1, 2, 3$ and

$$J = span_{\mathbb{Z}}\{\alpha_1, \dots, \alpha_6, \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4), \frac{1}{2}(\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6)\}.$$

Let $\{\alpha_7, \alpha_8\}$ be a basis of F. Then we may also arrange indexing so that

$$E_8 = span_{\mathbb{Z}} \left\{ \begin{array}{c} \alpha_1, \dots, \alpha_8, \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4), \frac{1}{2}(\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6), \\ \frac{1}{2}(\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8), \frac{1}{2}(\alpha_1 + \alpha_3 + \alpha_5 + \alpha_7) \end{array} \right\}.$$

Next we shall study the action of h on F.

Lemma 4.13. *In above notation, $h(\alpha_7) \in span_{\mathbb{Z}}\{\alpha_8\}$.*

Proof. Suppose $h(\alpha_7) \notin span_{\mathbb{Z}}\{\alpha_8\}$. Then $h(\alpha_7) = \pm\alpha_7$ and $h(\alpha_8) = \pm\alpha_8$.
In this case, we have

$$(h-1)\frac{1}{2}(\alpha_1+\alpha_3+\alpha_5+\alpha_7) = \frac{1}{2}(-\alpha_1+\alpha_2-\alpha_3+\alpha_4-\alpha_5+\alpha_6-\alpha_7+\epsilon\alpha_7), \quad \epsilon = \pm 1,$$

which has norm 3 or 5. It is a contradiction since E_8 is even. □

By the lemma above, we may assume $h(\alpha_7) = \alpha_8$ and $h(\alpha_8) = \alpha_7$ (by replacing α_8 by $-\alpha_8$ if necessary). Then

$$(h-1)\frac{1}{2}(\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8) = \alpha_5,$$

which is a root. Thus, h is not rootless.

Case 3: $J \cong D_4$ and $F \cong D_4$. This will lead to two cases for h.

Notation 4.14. *Let $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\} \subset J$ such that $h(\alpha_1) = \alpha_2, h(\alpha_2) = -\alpha_1, h(\alpha_3) = \alpha_4, h(\alpha_4) = -\alpha_3$ (cf. Lemma (4.11)).*

Let $\{\alpha_5, \alpha_6, \alpha_7, \alpha_8\} \subset F$ such that $(\alpha_i, \alpha_j) = 2\delta_{i,j}$.

We may reindex to assume

$$E_8 = span_{\mathbb{Z}} \left\{ \begin{array}{c} \alpha_1, \ldots, , \alpha_8, \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4), \frac{1}{2}(\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6), \\ \frac{1}{2}(\alpha_5 + \alpha_6 + \alpha_7 + \alpha_8), \frac{1}{2}(\alpha_1 + \alpha_3 + \alpha_5 + \alpha_7) \end{array} \right\}.$$

Lemma 4.15. *If h is rootless, then $h(\alpha_i) = \pm\alpha_i$ for all $i = 5, \ldots, 8$.*

Proof. Suppose $h(\alpha_k) = \epsilon\alpha_\ell$ for some $\epsilon = \pm 1$, $k \neq \ell$ and $k, \ell \in \{5, 6, 7, 8\}$. Then $h(\epsilon\alpha_\ell) = h^2(\alpha_k) = \alpha_k$ since $\alpha_k \in F$.

Take $i, j \in \{1, 2, 3, 4\}$ with $i < j$ such that

$$\frac{1}{2}(\alpha_i + \alpha_j + \alpha_k + \epsilon\alpha_\ell) \in E_8.$$

Then

$$\begin{aligned} & h\left(\frac{1}{2}(\alpha_i + \alpha_j + \alpha_k + \epsilon\alpha_\ell)\right) \\ = & \begin{cases} \frac{1}{2}(\alpha_i - \alpha_j + \alpha_k + \epsilon\alpha_\ell) & \text{if } h(\alpha_i) \in span_{\mathbb{Z}}(\alpha_j), \\ \frac{1}{2}(\pm\alpha_{i'} \pm \alpha_{j'} + \alpha_k + \epsilon\alpha_\ell) & \text{if } h(\alpha_i) \notin span_{\mathbb{Z}}(\alpha_j), \end{cases} \end{aligned}$$

where $\{\alpha_i, \alpha_j, \alpha_i', \alpha_j'\} = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$.

In either case, $(h-1)\frac{1}{2}(\alpha_i + \alpha_j + \alpha_k + \epsilon\alpha_\ell)$ is a root. □

Lemma 4.16. *Let Y be the fixed point sublattice of h on F. Then $\operatorname{rank} Y \leq 1$.*

Proof. Suppose $rank\, Y \geq 2$. Then by the previous lemma, h fixes α_k and α_ℓ for some $k \neq \ell$ and $k, \ell \in \{5, 6, 7, 8\}$. Take $i, j \in \{1, 2, 3, 4\}$ with $i < j$ such that

$$\frac{1}{2}(\alpha_i + \alpha_j + \alpha_k + \alpha_\ell) \in E_8.$$

Then by the same argument as in Lemma 4.15, $(h-1)\frac{1}{2}(\alpha_i + \alpha_j + \alpha_k + \alpha_\ell)$ is a root. $\square$

Since $h(\alpha_i) = \pm\alpha_i$ for $i = 5, \ldots, 8$ and $rank\, Y \leq 1$, $\{\alpha_5, \alpha_6\}$ or $\{\alpha_7, \alpha_8\}$ is contained in the (-1)-eigenspace of h.

By reindexing, we may assume α_5, α_6 are in the (-1)-eigenspace of h. Define

$$\begin{aligned} \beta_1 &:= \frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_5 + \alpha_6), \\ \beta_1' &:= \frac{1}{2}(\alpha_3 + \alpha_4 + \alpha_5 - \alpha_6) = \frac{1}{2}(\alpha_3 + \alpha_4 + \alpha_5 + \alpha_6) - \alpha_6. \end{aligned}$$

Then by our convention (4.14), β_1 and β_1' are in E_8. Let

$$\beta_2 := h(\beta_1) = \frac{1}{2}(-\alpha_1 + \alpha_2 - \alpha_5 - \alpha_6), \quad \beta_3 := h^2(\beta_1) = \frac{1}{2}(-\alpha_1 - \alpha_2 + \alpha_5 + \alpha_6),$$

$$\beta_2' := h(\beta_1') = \frac{1}{2}(-\alpha_3 + \alpha_4 - \alpha_5 + \alpha_6), \quad \beta_3' := h^2(\beta_1') = \frac{1}{2}(-\alpha_3 - \alpha_4 + \alpha_5 - \alpha_6).$$

Then $\beta_2, \beta_3, \beta_2', \beta_3'$ are also in E_8 since $h \in O(E_8)$.

Let $A := span\{\beta_1, \beta_2, \beta_3\}$ and $A' := span\{\beta_1', \beta_2', \beta_3'\}$. Then $A \cong A' \cong A_3$ and $(A, A') = 0$. By identifying A, A' with A_3, $h|_A$ and $h|_{A'}$ are identified with h_{A_3}.

Let $X := ann_F(span\{\alpha_5, \alpha_6\})$. Then $X \cong A_1 \oplus A_1$ and $Y = Fix_F(h) < X$. Note also that $(X, A) = (X, A') = 0$.

If $Y = 0$, then $h|_X = -id_X$. If $Y \cong A_1$, then h acts trivially on Y and acts as -1 on $X' := ann_X(Y) \cong A_1$. Thus, h may be identified with

$$\begin{cases} h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus h_{A_1} & \text{if } Y = Fix(h) = 0, \\ h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus id_{A_1} & \text{if } Y = Fix(h) \cong A_1. \end{cases}$$

Let $Q \cong A_3 \oplus A_3 \oplus A_1 \oplus A_1$ be a sublattice of E_8. Then $|E_8/Q| = 8$ and any element in $E_8 \setminus Q$ has non-zero projections to at least three A_i's. If $h = h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus h_{A_1}$ or $h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus id_{A_1}$, then $(h-1)x$, $x \in E_8 \setminus Q$, has at least two non-zero projections to the A_i's. Therefore, they are rootless by (3.13).

As a summary, we have

Theorem 4.17. *Let h be a rootless element of order 4. Then $J = Ker(h^2 + 1) \cong D_4$ or E_8.*

(1) If $J \cong D_4$, then h conjugate to $h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus h_{A_1}$ or $h_{A_3} \oplus h_{A_3} \oplus h_{A_1} \oplus id_{A_1}$.

(2) If $J \cong E_8$, then h is fixed point free and h^2 acts as -1 on E_8. Such elements form one conjugacy class.

Order 8

Theorem 4.18. *There is no rootless element of order* 8.

Proof. Suppose h is a rootless element of order 8. Then $g = h^2$ is a rootless element of order 4. By the analysis of order 4 elements, $Ker(g^2 + 1) \cong D_4$ or E_8 (cf. Theorem 4.17).

In either case, there exists a D_4 sublattice of E_8 which h acts (cf. Lemma 4.11).

Recall that $O(D_4)$ has the shape $(2^3{:}Sym_4).Sym_3$ (see (4.3.12) in [6]) Since h has order 8, h acts on D_4 as a product of a 4-cycle in Sym_4 and an outer involution with respect to the standard model of D_4. Therefore, there exists $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ such that $(\alpha_i, \alpha_j) = 2\delta_{i,j}$ for $i = 1, 2, 3, 4$ and

$$h(\alpha_1) = \alpha_2,\ h(\alpha_2) = \alpha_3,\ h(\alpha_3) = \alpha_4,\ h(\alpha_4) = -\alpha_1.$$

However,

$$(h-1)\frac{1}{2}(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4) = -\alpha_1,$$

which is root, a contradiction. □

4.5 Rootless elements of composite orders

Order 6

Let h be a rootless element of order 6. Let $g := h^2$ and $t := h^3$. Then, g has order 3 and t has order 2.

Let $L^+(t)$ and $L^-(t)$ be the $(+1)$ and (-1)-eigenlattice of t on E_8.

Lemma 4.19. *If h is rootless of order 6, then $L^+(t) \cong D_4$.*

Proof. First, we note that $g = h^2$ acts on both $L^+(t)$ and $L^-(t)$.

By the order 2 analysis, $L^+(t) \cong 0, A_1, A_1^2$, or D_4.

Case 1: $L^+(t) = 0$ and thus t acts as -1 on E_8. Therefore,

$$h = tg^2 = -g^2,$$

By the order 3 analysis, we may identify g^2 with either $h_{A_2}^{\oplus 4}$ or $h_{A_2}^{\oplus 3} \oplus id_{A_2}$.

In either case, let $\hat{\gamma} = (\gamma_1, \gamma_2, \gamma_3, 0)$ be a root in E_8, where $\gamma_1, \gamma_2, \gamma_3 \in A_2^*$ and have norm $2/3$. Since $1 + h_{A_2} + h_{A_2}^2 = 0$ on A_2^*, $(-h_{A_2} - 1)\gamma_i = h_{A_2}^2 \gamma_i$ also has norm $2/3$ for $i = 1, 2, 3$. Therefore,

$$(h-1)(\hat{\gamma}) = ((-h_{A_2} - 1)\gamma_1, (-h_{A_2} - 1)\gamma_2, (-h_{A_2} - 1)\gamma_3, 0)$$

has norm 2 and is a root.

Case 2: $L^+(t) \cong A_1$. Then g acts trivially on $L^+(t)$. Thus, $Fix(g) \neq 0$ and hence $Fix(g) \cong A_2$ and g^2 may be identified with $h_{A_2}^{\oplus 3} \oplus id_{A_2}$ by Theorem 4.4. Note that $L^+(t) < Fix(g)$. Therefore, $ann_{E_8}(Fix(g)) < ann_{E_8}(L^+(t)) = L^-(t)$ and we have

$$h|_{ann_{E_8}(Fix(g))} = -g^2.$$

Let $\hat{\gamma} = (\gamma_1, \gamma_2, \gamma_3, 0)$ be a root in $ann_{E_8}(Fix(g)) \cong E_6$, where $\gamma_1, \gamma_2, \gamma_3 \in A_2^*$ have norm $2/3$. Then, as in Case 1,

$$(h-1)\hat{\gamma} = ((-h_{A_2} - 1)\gamma_1, (-h_{A_2} - 1)\gamma_2, (-h_{A_2} - 1)\gamma_3, 0)$$

is a root.

Case 3: $L^+(t) \cong A_1 \oplus A_1$. Then g acts trivially on $L^+(t)$ since $O(A_1 \oplus A_1)$ has no elements of order 3. This is impossible since $Fix(g) \cong A_2$ does not contain a sublattice of type $A_1 + A_1$.

Therefore, the only possible case is $L^+(t) \cong D_4$. □

Since $L^+(t) \cong D_4$, we also have $L^-(t) = ann_{E_8}(L^+(t)) \cong ann_{E_8}(D_4) \cong D_4$ [6, (5.3.1)]. Note that g acts on both $L^+(t)$ and $L^-(t)$.

Lemma 4.20. *Let $Fix_{L^\pm(t)}(g)$ be the fixed points of g on $L^\pm(t)$. Then the rank of $Fix_{L^\pm(t)}(g)$ is even.*

Proof. Note that the minimal polynomial of g on $ann_{L^\pm(t)}(Fix_{L^\pm(t)}(g))$ is $x^2 + x + 1$, which is irreducible. Thus $rank(ann_{L^\pm(t)}(Fix_{L^\pm(t)}(g)))$ is even and so is $rank(Fix_{L^\pm(t)}(g))$. □

Lemma 4.21. *We use the same notation as in (4.20). Then* $Fix_{L^-(t)}(g) \neq 0$.

Proof. Suppose g is fixed point free on $L^-(t)$. Then $span\{\alpha, g\alpha\} \cong A_2$ for any root $\alpha \in L^-(t)$. Now choose a root $\alpha \in L^-(t)$ and define $A := span\{\alpha, g\alpha\}$.

Let $B := ann_{L^-(t)}(A)$. Then $B \cong \sqrt{2}A_2$. Thus, we obtain a sublattice $A \oplus B \cong A_2 \oplus \sqrt{2}A_2$ in $L^-(t)$ and g acts fixed point freely on the indecomposable direct summands.

By the previous lemma, $Fix_{L^+(t)}(g)$ has even rank and hence $Fix_{L^+(t)}(g) \cong A_2$ or 0. We shall first obtain information in these two cases, then finally a contradiction to prove this lemma.

Case 1: $X := Fix_{L^+(t)}(g) \cong A_2$. Then $C := ann_{L^+(t)}(X) \cong \sqrt{2}A_2$ and g acts fixed point freely on C. Thus, we obtain a sublattice

$$X \oplus A \oplus B \oplus C \cong A_2 \oplus A_2 \oplus \sqrt{2}A_2 \oplus \sqrt{2}A_2$$

in E_8 such that g acts on each indecomposable summand and is fixed point free on B and C.

Notice that $B \oplus C < ann_{E_8}(X \oplus A) \cong A_2 \oplus A_2$ and

$$|ann_{E_8}(X \oplus A)/(B \oplus C)| = 2^2.$$

Since $ann_{E_8}(X \oplus A) \cong A_2 \oplus A_2$ has roots, there exist $\beta \in B$ and $\gamma \in C$ with $(\beta, \beta) = (\gamma, \gamma) = 4$ such that $\frac{1}{2}(\beta + \gamma)$ is a root in $ann_{E_8}(X \oplus A)$. Then we also have $\frac{1}{2}(g\beta + g\gamma) \in ann_{E_8}(X \oplus A)$. Recall that the 2-part of $\mathcal{D}(\sqrt{2}A_2) = (\sqrt{2}A_2)^*/\sqrt{2}A_2$ is generated by the elements of the form $\frac{1}{2}\delta + \sqrt{2}A_2$ for $\delta \in \sqrt{2}A_2$ with $(\delta, \delta) = 4$.

By comparing the determinants, we have

$$ann_{E_8}(X \oplus A) = span\{B \oplus C, \frac{1}{2}(\beta + \gamma), \frac{1}{2}(g\beta + g\gamma)\} \cong A_2 \oplus A_2.$$

Let $A^+ = span\{\frac{1}{2}(\beta+\gamma), \frac{1}{2}(g\beta+g\gamma)\}$ and $A^- = span\{\frac{1}{2}(-\beta+\gamma), \frac{1}{2}(-g\beta+g\gamma)\}$. Then A^+ and A^- are sublattices of $ann_{E_8}(X \oplus A)$. Since g satisfies $x^2 + x + 1 = 0$ on $ann_L(X)$, we have $(v, gv) = -\frac{1}{2}(v, v)$ for all $v \in ann_L(X)$. It follows that $A^+ \cong A^- \cong A_2$ and $(A^+, A^-) = 0$. Moreover, g stabilizes each of A^+ and A^-.

Note that t commutes with g and $h = tg^2$. Since $X, C < L^+(t)$ and $A, B < L^-(t)$, we have

$$h|_X = id_X, \quad h|_A = -g^2|_A,$$

$$h(\frac{1}{2}(\beta+\gamma)) = \frac{1}{2}(-g^2\beta + g^2\gamma), \quad h(\frac{1}{2}(-\beta+\gamma)) = \frac{1}{2}(g^2\beta + g^2\gamma).$$

Thus we have $h(A^+) = A^-$ and $h(A^-) = A^+$. Note that

$$t(\frac{1}{2}(\beta+\gamma)) = \frac{1}{2}(-\beta+\gamma) \text{ and } t(\frac{1}{2}(g\beta+g\gamma)) = \frac{1}{2}(-g\beta+g\gamma).$$

Therefore, h acts on $A^+ \oplus A^-$ and t interchanges A^+ and A^-.

By identifying $X \oplus A \oplus A^+ \oplus A^-$ with A_2^4 and g^2 with h_{A_2} on A, A^+ and A^-, h is conjugate to $\sigma\tau$, where

$$\sigma = id_{A_2} \oplus (-h_{A_2}) \oplus h_{A_2} \oplus h_{A_2}$$

and τ performs a transposition on the 3rd and 4th copies of A_2 and is the identity on the first two summands.

Case 2: $Fix_{L^+(t)}(g) = 0$. Then g acts fixed point freely on $Fix_{L^+(t)}(g)$. Let $\alpha \in L^+(t)$ be a root. Then $X' := span\{\alpha, g\alpha\} \cong A_2$. Let $C' := ann_{L^+(t)}(X)$. Then $C' \cong \sqrt{2}A_2$ and we obtain a sublattice $X' \oplus A \oplus B \oplus C' \cong A_2 \oplus A_2 \oplus \sqrt{2}A_2 \oplus \sqrt{2}A_2$ in E_8 such that g acts fixed point freely on X', A, B and C'. Then by an argument as in case 1, one can show that h is conjugate to $\sigma'\tau$, where

$$\sigma' = h_{A_2} \oplus (-h_{A_2}) \oplus h_{A_2} \oplus h_{A_2}$$

and τ is a transposition on the 3rd and 4th copies of A_2.

We now get a contradiction to both Case 1 and Case 2. We take a sublattice A_2^4 of E_8 so that g preserves each summand and h has the form $\sigma\tau$, $\sigma'\tau$, as described in the two cases. Let $\eta := \frac{1}{3}(0, a, b, c)$ be a root in E_8 where $a, b, c \in A_2$ have norm 6. Then, $h\eta = \frac{1}{3}(0, -h_{A_2}a, h_{A_2}c, h_{A_2}b)$ and

$$(\eta, h\eta) = \frac{1}{9}\left(3 + (b, h_{A_2}c) + (c, h_{A_2}b)\right) = \frac{1}{9}(3 - (b, c))$$

since $(1 + h_{A_2} + h_{A_2}^2)b = 0$ and $(c, h_{A_2}b) = (b, h_{A_2}^2 c)$.

Since η is a root, $(\eta, h\eta) = 0, \pm 1$ or ± 2. Thus, we have $(b, c) = -6$ or 3 because $|(b, c)| \le 6$ and $\frac{1}{9}(3 - (b, c)) \in \mathbb{Z}$. It implies $c = -b$ or $-h_{A_2}^i b$ for $i = 1, 2$.

Since h_{A_2} stabilizes all cosets of A_2 in A_2^*, we also have $\frac{1}{3}(0, a, b, h_{A_2}^i c) \in E_8$ for all $i = 1, 2$. Thus, by replacing c by $h_{A_2}^i c$ if necessary, we may assume $c = -b$. Then

$$(h-1)\eta = -\frac{1}{3}(0, (h_{A_2}+1)a, (h_{A_2}+1)b, (h_{A_2}+1)c).$$

Recall that $(h_{A_2}\alpha, \alpha) = -\frac{1}{2}(\alpha, \alpha)$ for $\alpha = a, b, c$ (cf. [7, Lemma 3.2]) Thus, $(h_{A_2}+1)a, (h_{A_2}+1)b$ and $(h_{A_2}+1)c$ have norm 6 and $(h-1)\eta$ is a root. This final contradiction proves that $Fix_{L^-(t)}(g) \neq 0$. □

Lemma 4.22. *We use the same notation as in (4.20) and (4.21). Then* $Fix_{L^-(t)}(g) \cong A_2$ *and* g *acts fixed point freely on* $L^+(t)$.

Proof. We first note that $Fix_L(g) \cong A_2$ or 0 (see (4.4)). Since $Fix_{L^-(t)}(g) \neq 0$ and has even rank, we have $Fix_{L^-(t)}(g) \cong A_2$ and $Fix_{L^+(t)}(g) = 0$. □

By the same argument as in Lemma (4.21), we have the following.

Lemma 4.23. *Let* h *be a rootless element of order* 6. *Then* h *is conjugate to* $\sigma\tau = \tau\sigma$, *where* $\sigma = (-id_{A_2}) \oplus h_{A_2} \oplus h_{A_2} \oplus h_{A_2}$ *and* τ *is an involution which interchanges the 3rd and 4th copies of* A_2.

Proof. Let $P := Fix_{L^-(t)}(g) \cong A_2$ and $R := ann_{L^-(t)}(P)(\cong \sqrt{2}A_2)$. Take a root $\alpha \in L^+(t)$. Then $Q := span\{\alpha, g\alpha\} \cong A_2$ since g acts fixed point freely on $L^+(t)$. Also, $S := ann_{L^+(t)}(Q) \cong \sqrt{2}A_2$. Thus we obtain a sublattice $P \oplus Q \oplus R \oplus S \cong A_2 \oplus A_2 \oplus \sqrt{2}A_2 \oplus \sqrt{2}A_2$ in E_8 such that g acts trivially on P and fixed point freely on Q, R and S. Again, we have $R \oplus S < ann_{E_8}(P \oplus Q) \cong A_2 \oplus A_2$. Thus, by the same argument as in Lemma (4.21), one can show that h is conjugate to $\sigma\tau$, where $\sigma = (-id_{A_2}) \oplus h_{A_2} \oplus h_{A_2} \oplus h_{A_2}$ and τ is an involution which interchanges the 3rd and 4th copies of A_2.□

Let σ and τ be as in Lemma 4.23 and assume $h = \sigma\tau$. Then we determine a sublattice $(A_2)^4$ in E_8.

Let $\eta := \frac{1}{3}(\beta, 0, \gamma, \gamma') \in (A_2^*)^4$ be a root in E_8, where β, γ and γ' have norm 6. Then $h(\eta) = \frac{1}{3}(-\beta, 0, h_{A_2}\gamma', h_{A_2}\gamma)$ and

$$(\eta, h\eta) = \frac{1}{9}\left((\beta, -\beta) + (\gamma, h_{A_2}\gamma') + (\gamma', h_{A_2}\gamma)\right) = \frac{1}{9}(-6 - (\gamma, \gamma')).$$

Since $(\eta, h\eta) = 0, \pm 1$ or ± 2, we have $(\gamma, \gamma') = 3$ or -6 and hence $\gamma' = -h_{A_2}^i\gamma$ for $i = 0, 1, 2$. Without loss, we may assume $\gamma' = -h_{A_2}\gamma$ since h_{A_2} stabilizes all cosets of A_2 in A_2^*.

Then, we have $\eta = \frac{1}{3}(\beta, 0, \gamma, -h_{A_2}\gamma)$ and

$$\begin{aligned} h\eta &= \frac{1}{3}(-\beta, 0, -h_{A_2}^2\gamma, h_{A_2}\gamma), \\ h^2\eta &= \frac{1}{3}(\beta, 0, h_{A_2}^2\gamma, -\gamma), \\ h^3\eta &= \frac{1}{3}(-\beta, 0, -h_{A_2}\gamma, \gamma), \\ h^4\eta &= \frac{1}{3}(\beta, 0, h_{A_2}\gamma, -h_{A_2}^2\gamma). \end{aligned}$$

Thus we have $(h\eta, \eta) = (h^{-1}\eta, \eta) = -1$, $(h^2\eta, \eta) = (h^{-2}\eta, \eta) = 0$ and $(h^3\eta, \eta) = 0$. It implies that $A = span\{h^i\eta \mid i = 0, \dots, 5\} \cong A_5$ and $\{\eta, h\eta, h^2\eta, h^3\eta, h^4\eta\}$ is a fundamental set of simple roots. By identifying A with A_5, we may identify $h|_A$ with h_{A_5}.

Let B be the second summand isometric to A_2 and $C := ann_{L^-(h)}(\beta)$. Then $C \cong A_1$ and h acts as -1 on C. Thus we have a rank 8 sublattice $A \oplus B \oplus C$ in E_8 such that $A \cong A_5$, $B \cong A_2$, $C \cong A_1$. Moreover, we may identify $h|_A$ with h_{A_5}, $h|_B$ with h_{A_2} and $h|_C = -id_C$. The following theorem now follows.

Theorem 4.24. *Let h be a rootless element of order 6. Then h is conjugate to $h_{A_5} \oplus h_{A_2} \oplus h_{A_1}$.*

Other composite orders

Theorem 4.25. *There is no rootless element of order 12.*

Proof. Let h be a rootless element of order 12. Then $g = h^4$ has order 3, $f = h^3$ has order 4 and both are rootless. By the analysis of rootless order 6 elements, we have $Fix_{L^-(f^2)}(g) \cong A_2$ (see (4.22)). Since f commutes with g, f also acts on $Fix_{L^-(f^2)}(g)$. For any root $\alpha \in L^-(f^2)$, we have

$$(f\alpha, \alpha) = (f^2\alpha, f\alpha) = -(\alpha, f\alpha).$$

Hence $(f\alpha, \alpha) = 0$ and $span\{\alpha, f\alpha\} \cong A_1 \oplus A_1$. Since A_2 does not contain any sublattice isometric to $A_1 \oplus A_1$, f cannot stabilize any A_2-sublattice in $L^-(f^2)$, which is a contradiction. □

Lemma 4.26. *If $h \in O(L)$ is rootless, $|h|$ is not 10 or 15.*

Proof. Let h be rootless and have order 10 or 15. We use the notations in (3.4). Since h_5 is fixed point free, if q is the other prime dividing $|h|$, the q-part has eigenvalue 1. This means if $q = 3$, then h_3 has rank 2 fixed point sublattice, which is impossible since h_5 does not leave invariant a rank 2 sublattice. Now suppose that $q = 2$. Since the fixed point sublattice F of h_2 is nonzero and is h-invariant, $rank(F) = 4$. However, no rank 4 RSSD sublattice of L has an automorphism of order 5, contradiction. $\square$

5 How the surviving cases give all rootless EE_8 pairs

Each of the 11 lattices from the main result of [7] has the form $M+N$, where $M \cong N \cong EE_8$ and is denoted by some notation $DIH_{2k}(d, \cdots)$, where d is the rank and $2k = |\langle t_M, t_n\rangle|$. Their structures are summarized in Table 1. We shall prove that each of the 11 cases occurs as some SDC-lattice $L(E_8, h)$ by using the rootless h, which we classified in preceding sections.

We exclude the case $h = 1$, which is indeed rootless, but for which $M = N = L$.

Table 1: **Integral rootless lattices which are sums of EE_8s**

Name	$\langle t_M, t_N\rangle$	Isometry type of L (contains)	$\mathcal{D}(L)$	In Leech?
$DIH_4(12)$	Dih_4	$\geq DD_4^{\perp 3}$	$1^4 2^6 4^2$	Yes
$DIH_4(14)$	Dih_4	$\geq AA_1^{\perp 2} \perp DD_6^{\perp 2}$	$1^4 2^8 4^2$	Yes
$DIH_4(15)$	Dih_4	$\geq AA_1 \perp EE_7^{\perp 2}$	$1^2 2^{14}$	No
$DIH_4(16)$	Dih_4	$\cong EE_8 \perp EE_8$	2^{16}	Yes
$DIH_6(14)$	Dih_6	$\geq AA_2 \perp A_2 \otimes E_6$	$1^7 3^3 6^2$	Yes
$DIH_6(16)$	Dih_6	$\cong A_2 \otimes E_8$	$1^8 3^8$	Yes
$DIH_8(15)$	Dih_8	$\geq AA_1^{\perp 7} \perp EE_8$	$1^{10} 4^5$	Yes
$DIH_8(16, DD_4)$	Dih_8	$\geq DD_4^{\perp 2} \perp EE_8$	$1^8 2^4 4^4$	Yes
$DIH_8(16, 0)$	Dih_8	$\cong BW_{16}$	$1^8 2^8$	Yes
$DIH_{10}(16)$	Dih_{10}	$\geq A_4 \otimes A_4$	$1^{12} 5^4$	Yes
$DIH_{12}(16)$	Dih_{12}	$\geq AA_2 \perp AA_2 \perp A_2 \otimes E_6$	$1^{12} 6^4$	Yes

$X^{\perp n}$ denotes the orthogonal sum of n copies of the lattice X.

There are 11 rootless nonidentity conjugacy classes. If we form the associated 11 SDC lattices, it suffices to argue that they give 11 distinct EE_8-pairs. Notice that the dihedral group $\langle t_M, t_N\rangle$ has order $2|h|$ (2.4).

We now prove the bijection by use of Table 2. In column 1, we list the possibilities for rootless h. Columns 2 and 3 are consequences of our classification of rootless elements of $O(E_8)$. Our intended correspondence is expressed in column 4, which we shall now justify.

Table 2: **Rootless classes in** $O(E_8)$

Notation for h	Order of $\langle t_M, t_N\rangle$	$rank(M+N)$	Lattice name in [7]
$h_{A_1}^8$	4	16	$DIH_4(16)$
$h_{A_1}^7 \oplus id_{A_1}$	4	15	$DIH_4(15)$
$h_{A_1}^6 \oplus id_{A_1^2}$	4	14	$DIH_4(14)$
$h_{A_1}^4 \oplus id_{A_1}$	4	12	$DIH_4(12)$
$h_{A_2}^4$	6	16	$DIH_6(16)$
$h_{A_2}^3 \oplus id_{A_2}$	6	14	$DIH_6(14)$
$h_{A_3}^2 \oplus h_{A_1}^2$	8	16	$DIH_8(16, DD_4)$
$h_{A_3}^2 \oplus h_{A_1} \oplus id_{A_1}$	8	15	$DIH_8(15)$
$h^2 = -1$	8	16	$DIH_8(16, 0)$
$h_{A_4}^2$	10	16	$DIH_{10}(16)$
$h_{A_5} \oplus h_{A_2} \oplus h_{A_1}$	12	16	$DIH_{12}(16)$

We observe that two lattices which occur for different entries in column 1 of Table 1 are distinguished by the orders of the dihedral groups and their ranks, with the exception of the two cases of rank 16 lattices when the dihedral group has order 8. The latter two lattices are distinguished by $ann_M(N)$, which can be 0 or DD_4. By Lemma 2.12, $ann_N(M) = \{(\alpha, -\alpha) \mid \alpha \in E \text{ and } h\alpha = -\alpha\}$. Therefore, $ann_M(N) \cong DD_4$ when h has form $h_{A_3}^2 \oplus h_{A_1}^2$ (Theorem 4.17 (1)) and $ann_M(N) = 0$ when h satisfies $h^2 = -1$. Our set of rootless classes in $O(E_8)$ therefore gives 11 distinct SDC lattices, which must be the 11 types listed in [7] and which appear in column 4 of Table 2.

The main theorems (1.2), (1.3), (1.4) of this article are now proved. The rest of this article demonstrates new embeddings of a few of the above lattices into the Leech lattice.

A Embeddings of EE_8 pairs in the Leech lattice

As usual, Λ denotes a copy of the Leech lattice.

In this appendix, we shall construct several lattices $\mathcal{E} \cong E_8 \perp E_8$ in $\Lambda \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $\mathcal{E} \cap \Lambda$ is an $SDC(E_8)$-lattice. This will give relatively easy embeddings of some rootless EE_8 pairs into the Leech lattice. An account of embeddings for all cases of EE_8-pairs was given in [7].

A.1 Order 2

Let Ω be a 24-set and let $\mathcal{G}$ be the extended Golay code of length 24 indexed by Ω.

For explicit calculations, we shall use some 4×6 arrays to denote the codewords of the Golay code and the vectors in the Leech lattice. For each codeword in $\mathcal{G}$, 0 and 1 are indicated by an empty and filled space, respectively, at the corresponding positions in the array.

The following is a standard construction of the Leech lattice.

Definition A.1 ([2, 3]). *Let* $e_i := \frac{1}{\sqrt{8}}(0, \dots, 4, \dots, 0)$ *for* $i \in \Omega$. *Then* $(e_i, e_j) = 2\delta_{i,j}$. *Denote* $e_X := \sum_{i \in X} e_i$ *for* $X \in \mathcal{G}$. *The standard Leech lattice* Λ *is a lattice of rank 24 generated by the vectors:*

$$\frac{1}{2} e_X \,, \quad \text{where } X \text{ runs over all codewords of the Golay code } \mathcal{G};$$
$$\frac{1}{4} e_\Omega - e_1 \,;$$
$$e_i \pm e_j \,, \ i, j \in \Omega.$$

Let $\mathcal{D}$ be the subcode of $\mathcal{G}$ generated by

$$\mathcal{O}_1 = \left|\begin{array}{cc|cc|cc} * & & * & & & \\ * & & * & & & \\ * & & * & & & \\ * & & * & & & \end{array}\right| , \qquad \mathcal{O}_2 = \left|\begin{array}{cc|cc|cc} & * & & * & & \\ & * & & * & & \\ & * & & * & & \\ & * & & * & & \end{array}\right| ,$$

$$\mathcal{O}_3 = \left|\begin{array}{cc|cc|cc} * & * & * & * & & \\ * & * & * & * & & \\ & & & & & \\ & & & & & \end{array}\right| , \qquad \mathcal{O}_4 = \left|\begin{array}{cc|cc|cc} * & * & * & * & & \\ & & & & & \\ * & * & * & * & & \\ & & & & & \end{array}\right| .$$

Note that $\mathcal{D}$ is supported at $\mathcal{O}_1 \cup \mathcal{O}_2$ and is isomorphic to $d(H_8)$, where H_8 is the Hamming $[8, 4, 4]$-code and $d : \mathbb{Z}_2^8 \to \mathbb{Z}_2^{16}$ is defined by $d(\alpha) = (\alpha, \alpha)$.

Remark A.2. *Recall that $A_1^* = \frac{1}{2}A_1$, $A_1^*/A_1 \cong \mathbb{Z}_2$ and the root lattice E_8 can be constructed by A_1^8 and H_8 as follows [2, 6].*

Let $\rho : (A_1^*)^8 \to (A_1^*/A_1)^8 \cong \mathbb{Z}_2^8$ be the natural map. Then $\rho^{-1}(0) = Ker\rho = A_1^8$ and $\rho^{-1}(H_8) \cong E_8$.

Let

$$A = \frac{4}{\sqrt{8}}\left\{ \begin{array}{|cc|cc|cc|} \hline a & b & a & b & & \\ c & d & c & d & & \\ e & f & e & f & & \\ g & h & g & h & & \\ \hline \end{array} \;\middle|\; a,b,c,d,e,f,g,h \in \mathbb{Z} \right\}.$$

and denote $M = spanA \cup \{\frac{1}{2}e_X \mid X \in \mathcal{D}\}$. Then $A \cong AA_1^8$ and $M \cong EE_8$. Note that both A and M are sublattices of Λ.

Let

$$\mathcal{O} = \begin{array}{|cc|cc|cc|} \hline * & * & & & & \\ * & * & & & & \\ * & * & & & & \\ * & * & & & & \\ \hline \end{array}, \qquad \hat{\mathcal{O}} = \begin{array}{|cc|cc|cc|} \hline & & * & * & & \\ & & * & * & & \\ & & * & * & & \\ & & * & * & & \\ \hline \end{array}$$

and denote by $P_{\mathcal{O}}$ and $P_{\hat{\mathcal{O}}}$ the natural projections to $\mathcal{O}$ and $\hat{\mathcal{O}}$, respectively.

Let $E^1 = P_{\mathcal{O}}(M)$ and $E^2 = P_{\hat{\mathcal{O}}}(M)$. Then $E^1 \cong E^2 \cong E_8$ and $E^1 \perp E^2$. Moreover, $E^1 \perp E^2 < \frac{1}{2}\Lambda$. By identifying E^1 with E^2, we have

$$M = \{(\alpha, \alpha) \mid \alpha \in E^1\}.$$

Case 1: Now let $h_1 = \varepsilon_{\hat{\mathcal{O}}}$, i.e., h_1 acts as -1 on the basis vectors indexed by $\hat{\mathcal{O}}$ and as 1 on the basis vectors indexed by $\Omega \setminus \hat{\mathcal{O}}$.

Then h_1 acts as -1 on E^2 and fixes E^1 pointwise. Then $N = h_1(M) = \{(\alpha, h_1\alpha) \mid \alpha \in E^1\} < E^1 \perp E^2$ is also a diagonal copy. In this case, $M \perp N$ and $M + N \cong EE_8 \perp EE_8$.

Case 2: Let

$$\mathcal{O}' = \begin{array}{|cc|cc|cc|} \hline & & * & * & * & * \\ & & * & * & * & * \\ & & & & & \\ & & & & & \\ \hline \end{array}$$

and define $h_2 = \varepsilon_{\mathcal{O}'}$. Then $|\mathcal{O} \cap \mathcal{O}'| = 0$ and $|\hat{\mathcal{O}} \cap \mathcal{O}'| = 4$. Thus, h_2 may be identified with $h_{A_1}^4 \oplus id_{A_1}^4$ on E^2

and fixes E^1 pointwise. Let $N = h_2(M)$. Then $N \cap M \cong DD_4$ and $M + N \cong DIH_4(12)$.

A.2 Order 3

First, we recall the ternary construction of the Leech lattice Λ [2]. Let Δ be a 12-set and let $\mathcal{TG}$ be a ternary Golay code with index set Δ.

We also use the standard model for A_2, i.e.,

$$A_2 = \{(a, b, c) \in \mathbb{Z}^3 \mid a + b + c = 0\}.$$

Let $\gamma_0 := 0$, $\gamma_1 := \frac{1}{3}(1, 1, -2)$ and $\gamma_2 := \frac{1}{3}(-1, -1, 2)$ be elements in A_2^*.

Let $\mathcal{A}^i, i \in \Delta$, be isometric copies of A_2 and $\mathcal{X} := \oplus_{i\in\Delta}\mathcal{A}_i$ an orthogonal sum of 12 copies of A_2. Then the dual lattice $\mathcal{X}^* = \oplus_{i\in\Delta}\mathcal{A}_i^*$ and $\mathcal{D}(\mathcal{X})$ has a natural identification with $\mathbb{F}_3^{12}$.

For each codeword $x = (x_1, \dots, x_{12}) \in \mathcal{TG}$, let $\gamma_x = (\gamma_{x_1}, \dots, \gamma_{x_{12}}) \in \mathcal{X}^*$ be some vector which modulo $\mathcal{X}$ gives the codeword x. Then

$$\mathcal{N} := \mathit{span}\, \mathcal{X} \cup \{\gamma_x \mid x \in \mathcal{TG}\}$$

is isometric to the Niemeier lattice of type A_2^{12}.

Let $\delta := \frac{1}{3}(1, 0, -1)$ be in the standard model of A_2 and $\hat{\delta} := (\delta, \dots \delta)$. Then

$$\mathcal{N}^0 = \{\alpha \in N \mid (\alpha, \hat{\delta}) \in \mathbb{Z}\}$$

is a sublattice of index 3 and has no roots.

Let $\beta = (-1, 1, 0) \in A_2$. Then $(\beta, 0, 0 \dots, 0) + \hat{\delta}$ has norm 4 and the lattice $\mathcal{N}^0 + \mathbb{Z}((\beta, 0, 0 \dots, 0) + \hat{\delta})$ is even unimodular and has no root. Hence, it is isometric to the Leech lattice Λ [2, Chapter 24].

Next, we construct some EE_8 sublattices of $\mathcal{N}^0 < \Lambda$. We shall arrange the 12-set Δ into a 3×4 array. For each codeword in $\mathcal{TG}$, 0, 1 and 2 are marked by a blank space and + and − signs, respectively, at the corresponding positions in the array.

Let TD be the subcode of $\mathcal{TG}$ generated by

$$X = \begin{array}{|c|c|c|c|} \hline & + & - & \\ & + & - & \\ & + & - & \\ \hline \end{array}, \qquad Y = \begin{array}{|c|c|c|c|} \hline + & + & & \\ - & - & - & \\ & & + & \\ \hline \end{array}.$$

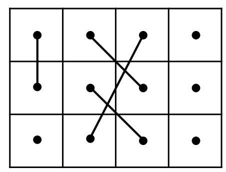
Let

$$\Omega_1 = \begin{array}{|c|c|c|c|} \hline * & * & & \\ & * & & \\ & * & & \\ \hline \end{array}, \qquad \Omega_2 = \begin{array}{|c|c|c|c|} \hline & & * & \\ * & & * & \\ & & * & \\ \hline \end{array}$$

be subsets of Δ and let P_{Ω_1} and P_{Ω_2} be the natural projections, from $\mathbb{F}_3^{\Delta}$ to $\mathbb{F}_3^{\Omega_1}$, $\mathbb{F}_3^{\Omega_2}$, respectively.

Then $P_{\Omega_1}(TD)$ and $P_{\Omega_2}(TD)$ are both isomorphic to the tetracode $\mathcal{C}_4$ since they are self-orthogonal and have dimension 2 and length 4.

Define a permutation φ of Δ by



Then $\varphi(\Omega_1) = \Omega_2$ and φ induces an isomorphism between $P_{\Omega_1}(TD)$ and $P_{\Omega_2}(TD)$.

Let

$$B = \left\{ \begin{array}{|c|c|c|c|} \hline a & b & -d & \\ -a & c & -b & \\ & d & -c & \\ \hline \end{array} \ \middle| \ a, b, c, d \in A_2 \right\} < \mathcal{X}$$

and $M = span\ B \cup \{\gamma_x \mid x \in TD\} < \mathcal{X}^*$. Then $B \cong AA_2^4$.

For any subset $S \subset \Delta$, let $\tilde{P}_S : \mathcal{X}^* \to \oplus_{i \in S} \mathcal{A}_i^*$ be the natural projection. Then $\tilde{P}_{\Omega_1}(B) \cong \tilde{P}_{\Omega_2}(B) \cong A_2^4$. Moreover, we have $\tilde{P}_{\Omega_1}(M) \cong \tilde{P}_{\Omega_2}(M) \cong E_8$ since $P_{\Omega_1}(TD) \cong P_{\Omega_2}(TD) \cong \mathcal{C}_4$, the tetracode.

Let $E^1 := \tilde{P}_{\Omega_1}(M)$ and $E^2 := \tilde{P}_{\Omega_2}(M)$. Then $(E^1, E^2) = 0$ and $E^1 \perp E^2 < \frac{1}{3}\Lambda$. Note that the permutation φ also induces a map on $\mathcal{X}^*$ by permutating the $\mathcal{A}_i^*$'s. Then we have $\varphi(E^1) = E^2$ and $M = \{(\alpha, -\varphi\alpha) \mid \alpha \in E^1\} < E^1 \perp E^2$. By identifying E^1 with E^2 using φ, we have $M = \{(\alpha, -\alpha) \mid \alpha \in E^1\} \cong EE_8$.

Let $h := h_X := h_{A_2}^{x_1} \oplus \cdots \oplus h_{A_2}^{x_{12}}$. Note that h defines an isometry of $\mathcal{N}$ and Λ [2, 3]. Moreover, h acts on $E^1 \perp E^2$ as $g \oplus g^{-1}$, where $g = h_{A_2}^3 \oplus id_{A_2} \in O(E_8)$. Then

$$N = h(M) = \{(g\alpha, g^{-1}\alpha) \mid \alpha \in E^1\} = \{(\alpha, g\alpha) \mid \alpha \in E^1\}.$$

In this case, $M \cap N \cong AA_2$ and $M + N \cong DIH_6(14)$.

A.3 Order 5

First we recall a construction of the Leech lattice from A_4^6 [2].

Let S_i, $i = 1, \ldots, 6$, be isometric copies of A_4 and $S = \oplus_{i=1}^6 S_i$ an orthogonal sum of six copies of A_4's. Then the dual lattice $S^* = \oplus_{i=1}^6 S_i^*$.

Let $\mathcal{C}$ be the subcode of $\mathbb{Z}_5^6$ generated by

$$(1,0,1,4,4,1),\ (1,1,0,1,4,4),\ (1,4,1,0,1,4).$$

Then $\mathcal{C}$ is a self-dual code over $\mathbb{Z}_5$ and is a glue code associated to the construction of $N(A_4^6)$ from A_4^6 [2, Chapter 16].

Let $a[1] := \frac{1}{5}(1,1,1,1,-4), a[2] := \frac{1}{5}(2,2,2,-3,-3), a[3] := -a[2], a[4] := -a[1]$ in A_4^* and $a[0] := 0$. For each $\alpha = (\alpha_1,\ldots,\alpha_6) \in \mathcal{C}$, let

$$\gamma_\alpha := (a[\alpha_1], a[\alpha_2], \ldots, a[\alpha_6]).$$

Define

$$\mathcal{N} := span_{\mathbb{Z}}(\, S \cup \{\gamma_\alpha \mid \alpha \in \mathcal{C}\}) < S^*$$

Then $\mathcal{N}$ is isometric to the Niemeier lattice of type A_4^6.

Let $\eta := \frac{1}{5}(2,1,0,-1,-2)$ and $\hat{\eta} := (\eta,\eta,\eta,\eta,\eta,\eta)$. Then

$$\mathcal{N}^0 = \{\alpha \in \mathcal{N} \mid (\alpha, \hat{\eta}) \in \mathbb{Z}\}$$

is an index 5 sublattice of $\mathcal{N}$ and has no roots.

Let

$$\Lambda := span_{\mathbb{Z}}(\mathcal{N}^0 \cup \{(\beta,0,0,0,0,0) + \hat{\eta}\}),$$

where $\beta := (-1,1,0,0,0) \in A_4$.

Then Λ is even unimodular and has no roots. That means Λ is isometric to the Leech lattice [2, Chapter 24].

Next we shall construct some EE_8's in Λ. Let

$$K := \{(0,a,0,-a,-b,b) \mid a,b \in A_4\} < S$$

and

$$M := span_{\mathbb{Z}}(\ K \cup \{(0,a[1],0,-a[1],-a[2],a[2])\}).$$

Then $K \cong AA_4 \perp AA_4$ and $M \cong EE_8$.

Note that

$$(0,1,0,-1,-2,2) = (1,0,1,4,4,1) - (1,4,1,0,1,4) \in \mathcal{C}$$

and hence $M < \mathcal{N}^0 < \Lambda$.

Let $P_1 : S^* \to S_2^* \oplus S_6^*$ and $P_2 : S^* \to S_4^* \oplus S_5^*$ be the natural projections.

Let $E^1 := P_1(M)$ and $E^2 := P_2(M)$. Then $E^1 \cong E^2 \cong E_8$ and $(E^1, E^2) = 0$. By identifying S_2 with S_4 and S_6 with S_5, we may identify E^1 with E^2. Then, we have $M = \{(\alpha, -\alpha) \mid \alpha \in E^1\}$.

Let $h := (1, h_{A_4}, 1, h_{A_4}^{-1}, h_{A_4}^{-2}, h_{A_4}^{2}) \in O((A_4^*)^6)$. Since $(0,1,0,-1,-2,2) \in \mathcal{C}$, one can verify that $h(\Lambda) = \Lambda$ (see [1] or [2]). Note that h acts as $h_{A_4} \oplus h_{A_4}^2$ on E^1 and as $h_{A_4}^{-1} \oplus h_{A_4}^{-2}$ on E^2.

Let $N := h(M)$ and let $g := h|_{E^1}$. Then by the identification of E^2 to E^1, we may identify $h|_{E^2}$ with g^{-1}. Hence, we have

$$N = h(M) = \{(g\alpha, -g^{-1}\alpha) \mid \alpha \in E^1\} = \{(\alpha, -g^{-2}\alpha) \mid \alpha \in E^1\}.$$

In this case, $M \cap N = 0$ and $M + N$ is an SDC lattice and is isometric to $DIH_{10}(16)$.

Acknowledgements. The authors thank Kavili Institute of Theoretical Physics in Beijing for hospitality during July and August, 2010.

The first author thanks the US National Science Foundation (DMS-0600854) and the US National Security Agency for financial support (H98230-10-1-0201) and the Academia Sinica for hospitality during his visit in Taipei, August 2010.

The second author thanks National Science Council (NSC 97-2115-M-006-015-MY3) and National Center for Theoretical Sciences, Taiwan for financial support and University of Michigan for hospitality during a visit, March 2010.

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of finite groups*, Clarendon Press, Oxford, 1985.

[2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd Edition, Springer, New York, 1999.

[3] R. L. Griess, Jr., *Twelve Sporadic Groups*, Springer Verlag, 1998.

[4] R. L. Griess, Jr., Pieces of Eight, *Adv. Math.*, 148, 75-104 (1999).

[5] R. L. Griess, Jr., Positive definite lattices of rank at most 8, *J. Number Theory*, 103 (2003), 77-84.

[6] R. L. Griess, Jr., *An introduction to groups and lattices: finite groups and positive definite rational lattices*, Higher Education Press (in China) and by the International Press (2010).

[7] R. L. Griess, Jr. and C. H. Lam, Dihedral groups and EE_8 lattices, *Pure Appl. Math. Q.*, Volume 7, Number 3 (Special Issue: In honor of Professor Jacques Tits) 621–743, 2011.

[8] P. Lewis, Sums of isometric pairs of lattices, arXiv:1009.0060.