K3 surfaces, entropy and glue

Curtis T. McMullen

13 September, 2009

Contents

Research supported in part by the NSF.

1 Introduction

In this paper we use the gluing theory of lattices to construct K3 surface automorphisms with small entropy.

Algebraic integers. A *Salem number* $\lambda > 1$ is an algebraic integer which is conjugate to $1/\lambda$, and whose remaining conjugates lie on S^1. There is a unique minimum Salem number λ_d of degree d for each even d. The smallest known Salem number is *Lehmer's number*, λ_{10}. These numbers and their minimal polynomials $P_d(x)$, for $d \leq 14$, are shown in Table 1.

		$P_d(x)$
λ_2	2.61803398	$x^2 - 3x + 1$
λ_4	1.72208380	$x^4 - x^3 - x^2 - x + 1$
λ_6	1.40126836	$x^6 - x^4 - x^3 - x^2 + 1$
λ_8	1.28063815	$x^8 - x^5 - x^4 - x^3 + 1$
λ_{10}	1.17628081	$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$
λ_{12}	1.24072642	$x^{12} - x^{11} + x^{10} - x^9 - x^6 - x^3 + x^2 - x + 1$
λ_{14}	1.20002652	$x^{14} - x^{11} - x^{10} + x^7 - x^4 - x^3 + 1$

Table 1. The smallest Salem numbers by degree, and their minimal polynomials.

Surface dynamics. Now let $F : X \to X$ be an automorphism of a compact complex surface. It is known that the topological entropy $h(F)$ is determined by the spectral radius of F^* acting on $H^*(X)$. More precisely, we have

$$h(F) = \log \rho(F^*|H^2(X)), \tag{1.1}$$

and if $h(F) > 0$, then a minimal model for X is either a K3 surface, an Enriques surface, a complex torus or a rational surface [Ca]. The lower bound

$$h(F) \geq \log \lambda_{10} \tag{1.2}$$

holds for all surface automorphisms of positive entropy, by [Mc3].

In this paper, we will show that the lower bound (1.2) can be achieved on a K3 surface.

Theorem 1.1 *There exists an automorphism of a K3 surface with entropy* $h(F) = \log \lambda_{10}$.

Although the entropy in Theorem 1.1 is the minimum possible, the associated K3 surface is not projective. For projective surfaces, we will show:

Theorem 1.2 *There exists an automorphism of a projective K3 surface with entropy* $h(F) = \log \lambda_6$.

As a complement, we note:

Theorem 1.3 *There exists an automorphism of a complex torus* $\mathbb{C}^2/\Lambda$ *with* $h(F) = \log \lambda_6$*, and an automorphism of an Abelian surface with* $h(F) = \log \lambda_4$. *In each case, no smaller positive entropy is possible.*

In particular, the automorphisms provided by Theorems 1.1 and 1.2 have lower entropy than any example that can be obtained from a complex torus automorphism by passing to the associated Kummer surface (cf. [Mc2, §4]).

Proof of Theorem 1.3. For the first example, let $A \in \mathrm{SL}_4(\mathbb{Z})$ be a matrix with $\det(xI - A) = x^4 + x + 1$. Then A gives an automorphism F of $X = \mathbb{R}^4/\mathbb{Z}^4$ preserving a complex structure, since the roots of P occur in conjugate pairs; and the characteristic polynomial of $\wedge^2 A$ is $P_6(x)$, so $h(F) = \log \lambda_6$ (compare [Mc2, §5]). No smaller entropy can arise, since $\exp h(F)$ must be a Salem number of degree at most $\dim H^2(X) = 6$.

For the second example, let $\zeta_d = \exp(2\pi i/d)$, let $E = \mathbb{C}/\mathbb{Z}[\zeta_3]$, let $X = E \times E$, and let $A \in \mathrm{M}_2(\mathbb{Z}[\zeta_3])$ be any matrix with $(\operatorname{tr} A, \det A) = (1, \zeta_6)$. Then the largest eigenvalue of A satisfies $|\lambda|^2 = \lambda_4$. It follows that the induced automorphism $F : X \to X$ has entropy $h(F) = \log \lambda_4$. No smaller entropy is possible because, in the projective case, the entropy is given by the log of the leading eigenvalue of F^* acting on the Néron-Severi group $\mathrm{NS}(X) \subset H^2(X, \mathbb{Z})$, and the rank of $\mathrm{NS}(X)$ is at most four. ■

It is known that the lower bound (1.2) can be realized on a rational surface [BK, Appendix], [Mc3], but not on an Enriques surface [Og, Thm 1.2]. At present there is no known automorphism F of a projective K3 surface with $0 < h(F) < \log \lambda_6$.

Glue groups. To explain how the examples underlying Theorems 1.1 and 1.2 were found, suppose $F : X \to X$ is a K3 surface automorphism of positive entropy, and let $f = F^*$ acting on the even unimodular lattice $L = H^2(X, \mathbb{Z})$ of signature $(3, 19)$. Then we can write $S(x) = \det(xI - f) = S_1(x)S_2(x)$, where $S_1(x)$ is a Salem polynomial and $S_2(x)$ is a product of cyclotomic polynomials $C_n(x)$. There is a corresponding splitting $f = f_1 \oplus f_2$, leaving invariant a sum of lattices $L_1 \oplus L_2$ with finite index in L. Passing to the *glue groups* $G(L_i) = L_i^\vee / L_i$, we obtain an isomorphism

$$\phi : G(L_1) \to G(L_2)$$

intertwining the quotient actions of f_1 and f_2. If these glue groups happen to be nontrivial vector spaces over $\mathbb{F}_p$, then $S_1(x)$ and $S_2(x)$ must have a common factor when reduced $\bmod p$. (Compare [Og, §4]).

In these terms, Theorems 1.1 and 1.2 were suggested by the fact that, when reduced modulo $p = 3$, the Salem polynomial $P_{10}(x)$ is divisible by $C_3(x) = x^2 + x + 1$, and $P_6(x)$ divides $C_{13}(x) = (x^{13} - 1)/(x - 1)$.

To actually construct examples, in §2–§4 we develop the general theory of equivariant gluing, Coxeter groups and twists. These results provide tools for producing a model $f : L \to L$ of the desired lattice automorphism $F^* : H^2(X, \mathbb{Z}) \to H^2(X, \mathbb{Z})$. Care must be taken to construct a candidate for the Kähler cone of X (§5). Then the strong Torelli theorem and surjectivity of the period map (reviewed in §6) show one can realize $f : L \to L$ by a holomorphic automorphism $F : X \to X$ of a K3 surface. Detailed constructions adapted to the Salem numbers λ_{10} and λ_6 are given in §7 and §8.

Many variations on these constructions, adapted to other Salem numbers and to other properties of the resulting K3 surface, remain to be explored.

Notes and references. This paper is a sequel to [Mc2] and [GM], and was inspired by Oguiso's recent example of a K3 surface automorphism with entropy $\log \lambda_{14}$ [Og]. I would like to thank B. Gross for many useful discussions, and for pointing out the positive automorphism of $A_2 \oplus A_2$ used in §7.

2 Lattices and glue

We begin by reviewing the construction of lattices and their automorphisms using glue groups. This technique goes back to Witt and Kneser [Kn]; for more details see e.g. [CoS].

Lattices. A *lattice* L of rank r is a free abelian group $L \cong \mathbb{Z}^r$, equipped with a nondegenerate inner product $\langle x, y \rangle$ taking values in $\mathbb{Z}$. The inner product determines natural inclusions

$$L \subset L^\vee \subset L \otimes \mathbb{Q} \tag{2.1}$$

where

$$L^\vee = \mathrm{Hom}(L, \mathbb{Z}) \cong \{x \in L \otimes \mathbb{Q} \, : \, \langle x, L \rangle \subset \mathbb{Z}\}.$$

We say L has signature (p, q) if the associated quadratic form

$$x^2 = \langle x, x\rangle$$

on $L \otimes \mathbb{R}$ is equivalent to

$$x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2. \tag{2.2}$$

The glue group. The finite abelian group $G(L) = L^\vee/L$ is the *glue group* of L. It comes equipped with a nondegenerate *fractional form* $\langle\langle x, y\rangle\rangle$ taking values in $\mathbb{Q}/\mathbb{Z}$, characterized by

$$\langle\langle x, y\rangle\rangle = \langle \widetilde{x}, \widetilde{y}\rangle \bmod 1$$

for any $\widetilde{x}, \widetilde{y} \in L^\vee$ representing $x, y \in G(L)$.

Concretely, if (e_i) is an integral basis for L with Gram matrix $B_{ij} = \langle e_i, e_j\rangle$, and $d_i \in G(L)$ are the classes represented by a dual basis for $L^\vee$, then the glue group has order

$$|G(L)| = \det(L) = |\det B_{ij}|,$$

and its fractional form is given by

$$\langle\langle d_i, d_j\rangle\rangle = (B^{-1})_{ij} \bmod 1.$$

Primary decomposition The glue group can be written canonically as an orthogonal direct sum of p-groups,

$$G(L) = \bigoplus G(L)_p,$$

where p ranges over the primes dividing $\det(L)$. The fractional form on $G(L)_p$ takes values in $\mathbb{Z}[1/p^e]/\mathbb{Z}$ for some e.

In the special case where every element of $G(L)_p$ has order p, we can regard $G(L)_p$ as a vector space over $\mathbb{F}_p$, and consider the fractional form as an inner product with values in $\mathbb{Z}[1/p]/\mathbb{Z} \cong \mathbb{F}_p$; see §3.

Extensions of L. The glue group provides a useful description of all the lattices $M \supset L$ such that M/L is finite. Indeed, since M pairs integrally with L, any such extension can be regarded as a subgroup of $L^\vee$; and the condition that the inner product on M is integral is equivalent to the condition that

$$\overline{M} = M/L \subset G(L)$$

is *isotropic*, i.e. $\langle\!\langle x, y\rangle\!\rangle = 0$ for all $x, y \in \overline{M}$. Thus we have a bijective correspondence:

$$\left\{ \begin{array}{c} \text{Lattices } M \text{ with} \\ L \subset M \subset L^\vee \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Isotropic subgroups } \overline{M} \text{ with} \\ 0 \subset \overline{M} \subset G(L) \end{array} \right\}.$$

Note that $[M : L] = |\overline{M}|$, $\det(M) = \det(L)/[M : L]^2$, and the glue group of the extension is given by

$$G(M) \cong \overline{M}^{\perp}/\overline{M}.$$

Gluing a pair of lattices. Now suppose $L = L_1 \oplus L_2$. A *gluing map* is an isomorphism $\phi : H_1 \to H_2$ between a pair of subgroups $H_i \subset G(L_i)$, $i = 1, 2$, satisfying

$$\langle\!\langle x, y\rangle\!\rangle = -\langle\!\langle \phi(x), \phi(y)\rangle\!\rangle. \tag{2.3}$$

This condition guarantees that

$$\overline{M} = \{(x, \phi(x)) : x \in H_1\} \subset G(L_1) \oplus G(L_2) = G(L)$$

is isotropic, and hence ϕ determines a lattice

$$M = L_1 \oplus_\phi L_2$$

obtained by *gluing* L_1 and L_2 along $H_1 \cong H_2$. The extension $L_1 \oplus L_2 \subset M$ is *primitive* in the sense that $L_i = M \cap (L_i \otimes \mathbb{Q})$, or equivalently M/L_i is torsion-free. Any primitive extension arises in this way, and hence we also have a natural correspondence:

$$\left\{ \begin{array}{c} \text{Primitive extensions} \\ L_1 \oplus L_2 \subset M \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Gluing maps } \phi : H_1 \to H_2 \text{ between} \\ \text{subgroups of } G(L_1) \text{ and } G(L_2) \end{array} \right\}.$$

Even lattices. A lattice L is *even* if $\langle x, x\rangle \in 2\mathbb{Z}$ for all $x \in L$. In this case we have a natural quadratic form $q : G(L) \to \mathbb{Q}/\mathbb{Z}$ defined by

$$q(x) = (1/2)\langle \widetilde{x}, \widetilde{x}\rangle \bmod 1. \tag{2.4}$$

An extension $L \subset M$ is even iff $q|\overline{M} = 0$; similarly, a gluing $M = L_1 \oplus_\phi L_2$ of even lattices is even iff $q(x) + q(\phi(x)) = 0$ for all $x \in H_1$.

Note that $M \supset L$ is even whenever L is even and $d = [M : L]$ is odd, for in this case we have $(dx)^2 = x^2 \bmod 2$.

Since $q(x+y) = q(x) + q(y) + \langle\langle x, y \rangle\rangle$, the fractional form determines $q|G(L)_p$ for all odd primes p (but not for $p = 2$).

Extending isometries. A bijective map from one lattice to another is an *isometry* if it preserves the inner product and group structure.

The *orthogonal group* $\mathrm{O}(L)$ consists of the isometries $f : L \to L$. For simplicity, we also use f to denote its linear extensions to $L^\vee, L \otimes \mathbb{R}, L \otimes \mathbb{C}$, etc. We let $\overline{f}$ denote the induced isometry of $G(L)$.

An isometry $f \in \mathrm{O}(L)$ extends to $M \supset L$ iff $\overline{f}(\overline{M}) = \overline{M}$. Similarly, equivariant gluing maps allow one to glue together isometries; we have a natural correspondence:

$$\left\{ \begin{array}{c} \text{Extensions } f \in O(M) \text{ of} \\ f_1 \oplus f_2 \in \mathrm{O}(L_1 \oplus L_2) \end{array} \right\} \leftrightarrow \left\{ \begin{array}{c} \text{Gluing maps } \phi : H_1 \to H_2 \\ \text{satisfying } \phi \circ f_1 = f_2 \circ \phi \end{array} \right\}.$$

Roots and the Weyl group. A vector $e \in L$ is a *root* if $\langle e, e \rangle = \pm 1$ or ± 2. Any root determines an isometric reflection $s \in \mathrm{O}(L)$ by the formula

$$s(x) = x - \frac{2\langle x, e \rangle}{\langle e, e \rangle} e.$$

The subgroup generated by all such reflections is the *Weyl group* $W(L) \subset \mathrm{O}(L)$. Note that $s(x) - x$ is an integral multiple of e for all $x \in L^\vee$. This shows:

The Weyl group acts trivially on the glue group.

Root lattices. We say L is a *root lattice* if it has an integral basis of roots. We conclude with some examples of root lattices that will be useful later. For more details, see [CoS], [Hum].

Odd unimodular lattices. Let $\mathbb{Z}^{p,q}$ denote $\mathbb{Z}^n$ with the inner product associated to the quadratic form (2.2). This is an odd unimodular root lattice, so it has trivial glue group.

Coxeter diagrams. Let Γ be a graph with vertices labeled $1, 2, \dots n$. Then Γ determines a symmetric form with matrix

$$B_{ij} = \langle e_i, e_j \rangle = \begin{cases} 2 & \text{if } i = j, \\ -1 & \text{if } i \text{ and } j \text{ are joined by an edge, and} \\ 0 & \text{otherwise.} \end{cases}$$

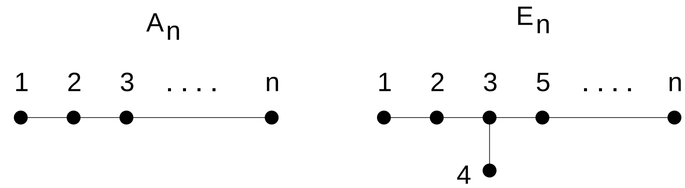

Figure 2. Diagrams for the root lattices A_n and E_n.

Provided $\det B_{ij} \neq 0$, this form makes $L = \oplus \mathbb{Z} e_i$ into an even root lattice of rank n. The product of the basic reflections s_i determined by e_i yields the *Coxeter element*

$$f = s_1 s_2 \cdots s_n \in \mathrm{W}(L) \subset \mathrm{O}(L).$$

If Γ is a tree, then the conjugacy class of f is independent of the ordering of the vertices of Γ. Since f lies in the Weyl group, $\overline{f}$ acts trivially on $G(L)$.

***A_n* and *E_n*.** The diagrams for the lattices A_n and E_n are shown in Figure 2. The A_n lattice can be regarded as the sublattice of $\mathbb{Z}^{n+1}$ defined by the equation $\sum x_i = 0$. Equivalently, A_n is the orthogonal complement of $v_n = (1, 1, \ldots, 1)$. Since $\mathbb{Z}^{n+1}$ is unimodular, this shows

$$\mathbb{Z}^{n+1} = A_n \oplus_\phi (\mathbb{Z} v_n)$$

where $\phi : G(A_n) \to G(\mathbb{Z} v_n)$ is an isomorphism. Since $\langle v_n, v_n \rangle = n + 1$, this implies

$$G(A_n) \cong G(\mathbb{Z} v_n) \cong \mathbb{Z}/(n+1).$$

Similarly, E_n can be regarded as the sublattice of $\mathbb{Z}^{n,1}$ perpendicular to

$$k_n = (1, 1, 1, \ldots, 1, -3).$$

(This vector represents the canonical class on the blowup of $\mathbb{P}^2$ at n points; cf. [Mc3, §3].) Note that $\langle k_n, k_n \rangle = n - 9$. Excluding the case $n = 9$ (since the bilinear form on E_9 is degenerate), we find that

$$G(E_n) \cong \mathbb{Z}/|9 - n|.$$

The signature of E_n is $(n, 0)$ for $n \leq 8$ and $(n-1, 1)$ for $n \geq 10$.

Even unimodular lattices. The inner product $\langle e_i, e_j \rangle = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ on $\mathbb{Z}^2$ gives the unique even unimodular lattice H of signature $(1, 1)$. More generally, for any $p, q \geq 1$ with $p \equiv q \bmod 8$, there is a unique even unimodular lattice $\mathrm{II}_{p,q}$ of signature (p, q) [MH], [Ser, §5].

We have just seen that E_8 and E_{10} are unimodular, so we have $E_{10} \cong E_8 \oplus H \cong \mathrm{II}_{9,1}$; and in general $\mathrm{II}_{p,q} \cong aE_8 \oplus bH$ for suitable integers a, b.

3 Isometries over finite fields

In this section we give a criterion for certain lattice automorphisms to automatically glue together.

Theorem 3.1 *Let $f_i \in \mathrm{O}(L_i)$, $i = 1, 2$ be a pair of lattice isometries, and let p be a prime. Suppose*

1. *Each glue group $G(L_i)_p$ is a vector space over $\mathbb{F}_p$;*
2. *The maps $\overline{f}_i$ on $G(L_i)_p$ have the same characteristic polynomial $S(x)$; and*
3. *$S(x) \in \mathbb{F}_p[x]$ is a separable polynomial, with $S(1)S(-1) \neq 0$.*

Then there is a gluing map $\phi : G(L_1)_p \to G(L_2)_p$ such that $f_1 \oplus f_2$ extends to $L_1 \oplus_\phi L_2$.

The proof is based on general properties of isometries over finite fields.

Inner products spaces. Let k be a field. An *inner product space* over k is a finite-dimensional vector space V equipped with nondegenerate, symmetric bilinear form $\langle x, y\rangle : V \times V \to k$. With respect to a basis, the form is given by a symmetric matrix $B_{ij} = \langle e_i, e_j\rangle$; and the class

$$\det(V) = [\det B_{ij}] \in k^*/(k^*)^2$$

is an invariant of V.

Example. The sum $W = V \oplus V^\vee$ of a vector space with its dual carries a natural *split* inner product with $\det(W) = (-1)^{\dim V}$. Its matrix with respect to a pair of dual bases is given by $\left(\begin{smallmatrix} 0 & I \\ I & 0 \end{smallmatrix}\right)$.

Polynomials. Given a degree d monic polynomial $S \in k[x]$ with $S(0) \neq 0$, let

$$S^*(x) = x^d S(x^{-1})/S(0).$$

This is again a monic polynomial, whose roots are the inverses of the roots of S. If $S = S^*$ we say S is a *reciprocal* polynomial. In this case $S(0) = \pm 1$. If $S(1)S(-1) \neq 0$, then the degree $d = 2e$ of S is even, and there is a unique *trace polynomial* R (of degree e) such that

$$S(x) = x^e R(x + x^{-1}).$$

Isometries. Let $f : V \to V$ be an isometry. Then $f^\vee = f^{-1}$, and hence the characteristic polynomial $S(x) = \det(xI - f)$ is reciprocal. Similarly

$$(\operatorname{Ker} P(f))^\perp = \operatorname{Im}(P(f)^\vee) = \operatorname{Im} P^*(f) \tag{3.1}$$

for any $P \in k[x]$.

Finite fields. Now let $f : V \to V$ be an isometry of an inner product space over a *finite* field k.

We first note that V is almost determined, up to isometry, by its dimension. In fact:

1. If $\operatorname{char} k$ is odd, then V is uniquely determined by $\dim(V)$ and by $\det(V) \in k^*/(k^*)^2 \cong \mathbb{Z}/2$; while
2. If $\operatorname{char} k$ is 2, then V is uniquely determined by $\dim(V)$ and the parity of V (which is even if $\langle x, x\rangle = 0$ for all $x \in V$, and otherwise odd). Even forms exists only in even dimensions.

See e.g. [MH, App. 2], [Ger, §2.8].

We now turn to the problem of classifying the *pair* (V, f) up to isometry.

Proposition 3.2 *If $S(x) = \det(xI - f)$ is irreducible and $\dim V > 1$, then (V, f) is determined up to isometry by S.*

Proof. We claim (V, f) is isometric to (K, g), where $K = k[t]/S(t)$, $g(x) = tx$ and the inner product on K is given by $\langle x, y\rangle_K = \operatorname{Tr}_k^K(xy')$. Here $x \mapsto x'$ is the Galois involution on K sending t to t^{-1}, whose existence is guaranteed by the fact that $S(t)$ is a reciprocal polynomial.

To make this identification, first observe that $t \mapsto f$ gives an isomorphism $K \cong k[f] \subset \operatorname{End}_k(V)$ sending the Galois involution to the adjoint involution (since $f^\vee = f^{-1}$). Upon choosing a nonzero vector $v \in V$, we obtain an isomorphism $V \cong Kv \cong K$ sending f to g. By nondegeneracy of the trace form, there is then a unique k-linear map $\xi : K \to K$ such that

$$\langle x, y\rangle = \operatorname{Tr}_k^K(\xi(x)y').$$

Using the fact that $\langle f(x), f(y)\rangle = \langle x, y\rangle = \langle y, x\rangle$, we find that $\xi(x) = bx$ where $b = b' \in K$. Since $\deg(S) > 1$, the Galois involution is nontrivial, and hence $b = aa'$ for some $a \in K$ (as a counting argument shows). But then we can simply replace v by av to obtain a new identification $V \cong Kav \cong K$ such that $\langle x, y\rangle = \operatorname{Tr}_k^K(xy')$. ∎

Proposition 3.3 *If $\det(xI - f) = Q(x)Q^*(x)$, where $Q(x)$ and $Q^*(x)$ are distinct irreducible monic polynomials, then (V, f) is determined up to isometry by $Q(x)$.*

Proof. In this case $V = \operatorname{Ker} Q(f) \oplus \operatorname{Ker} Q^*(f) = W \oplus W^\vee$, where the inner product identifies the second summand with the dual of the first. Since the linear map $f|W$ is determined by $Q(x)$, the pair (V, f) is determined up to isometry by the same information. ■

Proposition 3.4 *If $S(x) = \det(xI - f)$ is separable and $S(1)S(-1) \neq 0$, then (V, f) is determined up to isometry by S.*

Proof. Since S is a separable, reciprocal polynomial, it factors as a product of distinct irreducible polynomials

$$S(x) = S_1(x) \cdots S_r(x) Q_1(x) Q_1^*(x) \cdots Q_s(x) Q_s^*(x)$$

where $S_i = S_i^*$. Thus V splits as an f-invariant orthogonal direct sum

$$V = \left(\bigoplus_1^r \operatorname{Ker} S_i(f) \right) \oplus \left(\bigoplus_1^s \operatorname{Ker} Q_i(f) Q_i^*(f) \right).$$

(Orthogonality follows from (3.1).) The assumption $S(1)S(-1) \neq 0$ insures $\dim \operatorname{Ker} S_i(f) > 1$ for each i. Thus the preceding two propositions can be applied, term to term, to show that (V, f) is determined up to isometry by S. ■

Proof of Theorem 3.1. The fractional form makes $G(L_i)_p$ into an inner product space over $\mathbb{F}_p \cong \mathbb{Z}[1/p]/\mathbb{Z}$. Since $\overline{f}_i$ acts isometrically, we may applying the preceding result (after reversing the sign of one of the forms) to obtain the desired gluing map ϕ. ■

The glue group of $\boldsymbol{A_{p-1}}$. In the absence of an automorphism, the isometry type of a glue group may need to be determined directly. For later use, we record a particular case:

Proposition 3.5 *The fractional form makes $V = G(A_{p-1})$ into an inner product space over $k = \mathbb{F}_p$ with $\det(V) = [-1] \in k^*/(k^*)^2$.*

Proof. The vector $x = (1, 1, \ldots, 1, 1-p)/p \in A_{p-1}^\vee \subset \mathbb{R}^p$ satisfies $\langle x, x \rangle = (p-1)/p = -1/p \bmod 1$. ■

Notes and references. The results above can be regarded as special cases of the fact that a Hermitian space over a finite field is determined up to isomorphism by its dimension; see [MH, App. 2].

4 Twists

In this section we discuss the twists of a lattice L by a self-adjoint endomorphism $a : L \to L$. Twisting allows one to adjust the signature and glue group of L while respecting the action of a given isometry.

Twisting lattices. Let L be a lattice of rank r. Suppose $a \in \mathrm{End}(L)$ satisfies $a = a^\vee$ and $\det(a) \neq 0$. Then

$$\langle x, y \rangle_a = \langle ax, y \rangle$$

defines a new inner product on L, giving us a new lattice $L(a)$ called the *twist* of L by a.

It is easy to see that $G(L(a)) = L^\vee / aL$ and $\det(L(a)) = \det(L)|\det(a)|$. More precisely, we have an exact sequence

$$0 \to L/aL \to G(L(a)) \to G(L) \to 0, \tag{4.1}$$

which splits if $\det(a)$ and $\det(L)$ are relatively prime.

Twisting isometries. Now suppose L is equipped with an isometry $f : L \to L$. Let $\mathbb{Z}[f] \subset \mathrm{End}(L)$ be the ring generated by f, and suppose $a \in \mathbb{Z}[f + f^{-1}]$ and $\det(a) \neq 0$. Then $a = a^\vee$ and $af = fa$, so $f \in O(L(a))$ as well. Thus we can regard L, $L(a)$ and their glue groups as modules over $\mathbb{Z}[f]$. With this understanding, (4.1) is an exact sequence of $\mathbb{Z}[f]$-modules.

Proposition 4.1 *If $a \in \mathbb{Z}[f + f^{-1}]$ and L is even, then so is $L(a)$.*

Proof. Write $a = \sum_0^n a_i (f^i + f^{-i})$ with $a_i \in \mathbb{Z}$, and observe that $\langle f^{-1}x, x \rangle = \langle fx, x \rangle$; thus for all $x \in L$, we have

$$\langle ax, x \rangle = a_0 \langle x, x \rangle + \sum_1^n 2 \langle f^i x, x \rangle \in 2\mathbb{Z}.$$

■

Primes and divisors. For more detailed results, we fix a prime p not dividing $\det(L)$, and let $P \mapsto \overline{P}$ denote the natural map $\mathbb{Z}[x] \to \mathbb{F}_p[x]$. Then the twist $M = L(p)$ of a lattice of rank r satisfies

$$G(M)_p \cong \mathbb{F}_p^r \quad \text{and} \quad \det(xI - \overline{f} | G(M)_p) = \overline{S}(x),$$

where $S(x) = \det(xI - f)$.

By twisting with a divisor of p in the ring $\mathbb{Z}[f + f^{-1}]$, we can sometimes arrange that the characteristic polynomial of $\overline{f}|G(M)_p$ is a given divisor of $\overline{S}(x)$. To state a result in this direction, assume that:

1. The polynomial $\overline{S}(x) \in \mathbb{F}_p[x]$ is separable; and
2. We have $pL \subset aL$, where $a \in \mathbb{Z}[f + f^{-1}]$.

Then the result of twisting by a can be described as follows.

Theorem 4.2 *The lattice $M = L(a)$ has glue group*

$$G(M) \cong G(M)_p \oplus G(L) \tag{4.2}$$

as a $\mathbb{Z}[f]$-module. Moreover $G(M)_p$ is a vector space over $\mathbb{F}_p$, and the characteristic polynomial of $\overline{f}|G(M)_p$ is given by

$$\overline{Q}(x) = \gcd(\overline{A}(x), \overline{S}(x)) \ \in \mathbb{F}_p[x],$$

where $a = A(f) \in \mathbb{Z}[f]$.

Proof. Since $pL \subset aL$, $\det(a)$ is a power of p; and since p does not divide $\det(L)$, the exact sequence (4.1) splits, which gives (4.2). The assumption $pL \subset aL$ also implies that $G(M)_p \cong L/aL$ is a quotient of $V = L/pL \cong \mathbb{F}_p^r$, so it is a vector space over $\mathbb{F}_p$. By separability, we have $V \cong \mathbb{F}_p[x]/(\overline{S})$, and hence

$$G(M)_p \ \cong \ V/aV \ \cong \ \mathbb{F}_p[x]/(\overline{A}, \overline{S}) \ \cong \ \mathbb{F}_p[x]/(\overline{Q})$$

as modules over $\mathbb{Z}[f]$. ■

Dedekind domains. The existence of a desired twist is guaranteed in certain situations by the following result.

Theorem 4.3 *Suppose $\mathcal{O} = \mathbb{Z}[f + f^{-1}]$ is a Dedekind domain of class number one,*

$$\overline{S}(x) = \det(xI - f) \bmod p$$

is separable, $\overline{S}(1)\overline{S}(-1) \neq 0$ and $\gcd(p, \det L) = 1$. Let $\overline{S}_1(x)$ be a reciprocal factor of $\overline{S}(x)$. Then there exists a twist $M = L(a)$, with $a \in \mathbb{Z}[f + f^{-1}]$ dividing p, such that

$$\overline{S}_1(x) = \det(xI - \overline{f}|G(M)_p). \tag{4.3}$$

Proof. Let $R(y)$ be the trace polynomial associated to $S(x)$, so $S(x) = x^e R(x + x^{-1})$. Let $\overline{R} = \overline{R}_1 \overline{R}_2$ be the factorization of $\overline{R}$ corresponding to the given factorization $\overline{S} = \overline{S}_1 \overline{S}_2$. Then $\mathcal{O} \cong \mathbb{Z}[y]/(R)$, so by basic number theory (see e.g. [La, I, §8]), there is a factorization $p = a_1 a_2$ in $\mathcal{O}$ such that

$$\mathcal{O}/(a_i\,\mathcal{O}) \cong \mathbb{F}_p[y]/(\overline{R}_i)$$

for $i = 1, 2$. Equivalently, if $a_i = A_i(f + f^{-1})$ with $A_i \in \mathbb{Z}[y]$, then $(\overline{A}_i) = (\overline{R}_i)$ as ideals in $\mathbb{F}_p[y]/(\overline{R})$.

Now we can also write $a_1 = A(f)$, since $\mathbb{Z}[f^{-1}] = \mathbb{Z}[f]$. Then $A(x) = A_1(x + x^{-1})$ in the ring $\mathbb{Z}[x]/(S)$. Consequently

$$(\overline{A}(x)) = (\overline{A}_1(x + x^{-1})) = (\overline{R}_1(x + x^{-1})) = (\overline{S}_1(x))$$

as ideals in $\mathbb{F}_p[x]/(\overline{S})$, and hence $\overline{S}_1 = \gcd(\overline{A}, \overline{S})$, which gives (4.3) for $M = L(a_1)$. ■

Signature. To conclude, we relate the signatures of L and $L(a)$.

Let $f : L \to L$ be an isometry of a lattice of signature (p, q) such that $S(x) = \det(xI - f)$ is separable and $S(1)S(-1) \neq 0$.

Since $S(x)$ is reciprocal, it has $2s$ roots outside S^1 and $2t$ roots on S^1. The map $\lambda \mapsto \lambda + \lambda^{-1}$ sends the roots on S^1 to a set $T \subset (-2, 2)$ with $|T| = t$. As in [GM], we define the *sign invariant* $\epsilon_L : T \to \langle \pm 1 \rangle$ by

$$\epsilon_L(\tau) = \begin{cases} +1 & \text{if } E_\tau \text{ has signature } (2,0), \\ -1 & \text{if } E_\tau \text{ has signature } (0,2), \end{cases}$$

where

$$E_\tau = \operatorname{Ker}(f + f^{-1} - \tau I) \subset L \otimes \mathbb{R} \cong \mathbb{R}^{p,q}.$$

Then the signature of L is given by

$$(p, q) = (s, s) + \sum_T \begin{cases} (2,0) & \text{if } \epsilon_L(\tau) = +1, \\ (0,2) & \text{if } \epsilon_L(\tau) = -1. \end{cases} \tag{4.4}$$

Now for any twisting parameter $a = A(f + f^{-1}) \in \mathbb{Z}[f + f^{-1}]$, define $\epsilon_a : T \to \langle \pm 1 \rangle$ so that $\epsilon_a(\tau) A(\tau) > 0$. We then have

$$\epsilon_{L(a)}(\tau) = \epsilon_L(\tau) \epsilon_a(\tau), \tag{4.5}$$

and by (4.4) this determines the signature of $L(a)$.

5 Positivity

In this section we discuss the notion of a positive automorphism of a Euclidean or Lorentzian lattice. (The Lorentzian case is not needed until §8).

The Euclidean case. To begin with, assume L is an even, positive-definite lattice. Let

$$\Phi = \{y \in L \,:\, y^2 = 2\} \tag{5.1}$$

be the finite set of roots in L. We say $\Phi^+ \subset \Phi$ is a *system of positive roots* if there is an $x \in L$ such that

$$\Phi = \Phi^+ \cup (-\Phi^+) \quad \text{and} \quad \langle x, y \rangle > 0 \; \forall y \in \Phi^+. \tag{5.2}$$

Such an x exists iff the convex hull of Φ^+ does not contain the origin.

We say an isometry $f \in \mathrm{O}(L)$ is *positive* if it preserves a system of positive roots.

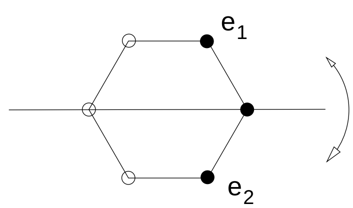

Figure 3. Reflection through the x-axis preserves a set of positive roots in the A_2 lattice.

Example. The hexagonal root lattice A_2 admits a positive involution f which interchanges the basic roots e_1 and e_2; see Figure 3. This map is not in the Weyl group $W(L)$; it comes from a symmetry of the A_2 diagram. We have $\overline{f}(x) = -x$ on the glue group $G(A_2) \cong \mathbb{Z}/3$, and in fact f generates $\mathrm{O}(L)/W(L) \cong \mathbb{Z}/2$.

Basic properties. If $L = L_1 \oplus L_2$, and $f_i \in \mathrm{O}(L_i)$ are positive, then so is $f = f_1 \oplus f_2$. This is because every root of L lies in L_1 or L_2.

So long as L has at least one root, any positive map $f \in \mathrm{O}(L)$ has 1 as an eigenvalue, since f must fix $\sum\{y \,:\, y \in \Phi^+\}$. By splitting along this eigenspace, we can present (L, f) as a gluing $(L_1 \oplus_\phi L_2, f_1 \oplus f_2)$ where f_1 is the identity map and L_2 has no roots. Conversely, any map of this form is positive.

The Lorentzian case. We now turn to the case where L is an even lattice of signature $(n, 1)$.

In this case we say Φ^+ is a *positive root system* if it satisfies (5.2) for some $x \in L$ with $x^2 < 0$. Geometrically, the roots $y \in \Phi$ define a locally finite system of hyperplanes $y^\perp$ in the hyperbolic space $\mathbb{H}^n \subset \mathbb{P}(L \otimes \mathbb{R})$, cutting it into open chambers. The choice of a positive root system (up to sign) is the same as the choice of one of those chambers; and a chamber can be specified by giving a representative point $[x] \in \mathbb{H}^n$ satisfying $\langle x, \Phi^+ \rangle > 0$.

Note that Φ excludes any roots of L with $y^2 = -2$.

Example. Let L be the Lorentz lattice $\mathbb{Z}^2$ with $(a,b)^2 = 2(a^2 + ab - b^2)$. Its roots Φ include the Fibonacci pairs $(1,1), (2,3), (5,8)$, etc. Let $e_1 = (1,0), e_2 = (0,1)$, and let $\Phi_i = \{y \in \Phi : \langle e_i, y \rangle > 0\}$. Then Φ_2 is a positive root system but Φ_1 is not, essentially because $e_2^2 < 0$ but $e_1^2 > 0$.

The light cone condition. In the Lorentzian case, we say $f : L \to L$ is *positive* if it preserves a positive root system *and* it stabilizes each component of the light cone defined by $x^2 < 0$ in $L \otimes \mathbb{R} \cong \mathbb{R}^{n,1}$. (Thus $f(x) = -x$ is never positive).

Gluing. Let $L = L_1 \oplus_\phi L_2$ be an even lattice obtained by gluing a Lorentzian lattice L_1 to a Euclidean lattice L_2. We wish to investigate when an automorphism $f = f_1 \oplus f_2$ of L is positive.

We remark that the timelike vectors in any Lorentzian lattice satisfy a reverse Cauchy-Schwarz inequality:

$$x^2, y^2 \le 0 \implies |x^2 y^2| \le |\langle x, y \rangle|^2, \tag{5.3}$$

as is easily verified by reducing to the case $x = e_{n+1}$ in $\mathbb{R}^{n,1}$.

Theorem 5.1 *Suppose $x^2 \in 2a_i\mathbb{Z}$ for all $x \in L_i$, $a_i > 1$, $bL \subset L_1 \oplus L_2$, and $b^2 \notin \mathbb{Z}_+ a_1 + \mathbb{Z}_+ a_2$. Then $f_1 \oplus f_2$ is a positive automorphism of L provided f_1 has an eigenvalue $\lambda > 1$.*

Here $\mathbb{Z}_+ = \{1, 2, 3 \ldots\}$ denotes the set of positive integers.

Proof. Let $y \in \Phi$ be a root of L. Then $y = (y_1, y_2) \in L_1^\vee \oplus L_2^\vee$ satisfies $y^2 = y_1^2 + y_2^2 = 2$, and $by \in L_1 \oplus L_2$. Therefore

$$(by)^2 = 2b^2 = (by_1)^2 + (by_2)^2 = 2(a_1 n_1 + a_2 n_2)$$

with $n_1, n_2 \in \mathbb{Z}$ and $n_2 \ge 0$. By assumption, this equation has no solutions with $n_1, n_2 > 0$. Our assumptions also imply that L_1 and L_2 have no roots, so we cannot have $n_1 = 0$ or $n_2 = 0$. Thus we must have $n_1 < 0$ and hence $y_1^2 < 0$; more precisely, we have $y_1^2 \le -a_1/b^2$.

Pick any $x_1 \in L_1$ with $x_1^2 < 0$. Then by (5.3), we have

$$|\langle x_1, y\rangle|^2 = |\langle x_1, y_1\rangle|^2 \geq |x_1^2 y_1^2| \geq a_1|x_1^2|/b_2 > 0 \;\; \forall y \in \Phi.$$

Thus $\Phi^+ = \{y \in \Phi \,:\, \langle x_1, y\rangle > 0\}$ is a positive root system for L. It consists exactly of the roots which project into the component of the light cone of $L_1 \otimes \mathbb{R}$ as x_1. Since f_1 has an eigenvalue $\lambda > 1$, it preserves this component, and hence f preserves Φ^+ and is positive. ■

Geometrically, the proof shows that the inclusion $L_1 \subset L$ determines an f-invariant hyperbolic subspace $\mathbb{H}^{n_1} \subset \mathbb{H}^n$ lying completely inside one of the chambers defined by Φ.

Theorem 5.2 *Suppose f_1 and f_2 are positive, and every root $(y_1, y_2) \in L$ which is not in $L_1 \oplus L_2$ satisfies $y_2^2 \geq 2$. Then $f_1 \oplus f_2$ is a positive automorphism of L.*

Proof. Let Φ denote the roots of L, let $\Phi_i = \Phi \cap L_i$ for $i = 1, 2$, and let

$$\Phi_3 = \{(y_1, y_2) \in \Phi \,:\, y_1^2 \leq 0, y_1 \neq 0\}.$$

Consider any root $y = (y_1, y_2)$ of L that is not in $\Phi_1 \cup \Phi_2$. Since L_1 and L_2 are primitive, neither y_1 nor y_2 is zero. If $(y_1, y_2) \in L_1 \oplus L_2$, this implies $y_1^2 = 2 - y_2^2 \leq 0$; and the same is true, by assumption, if $(y_1, y_2) \notin L_1 \oplus L_2$. Therefore

$$\Phi = \Phi_1 \cup \Phi_2 \cup \Phi_3.$$

Let $\Phi_i^+ \subset \Phi_i$ be an f_i-invariant system of positive roots for $i = 1, 2$, and choose $x_i \in L_i$ such that $\langle x_i, y\rangle > 0$ for all $y \in \Phi_i^+$. We may assume $x_1^2 < 0$.

Note that any $(y_1, y_2) \in \Phi_3$ satisfies $\langle x_1, y_1\rangle \neq 0$, since $y_1^2 \leq 0$ and $y_1 \neq 0$. Let

$$\Phi_3^+ = \{(y_1, y_2) \in \Phi_3 \,:\, \langle x_1, y_1\rangle > 0\}.$$

This subset just consists of the elements of Φ_3 that project to the component of the lightcone in $L_1 \otimes \mathbb{R}$ that contains $-x_1$. Since f_1 preserves this component, we have $f(\Phi_3^+) = \Phi_3^+$.

We claim that $\Phi_+ = \Phi_1^+ \cup \Phi_2^+ \cup \Phi_3^+$ is a positive root system for L. Since $f(\Phi_+) = \Phi_+$, this will complete the proof of positivity of $f = f_1 \oplus f_2$.

Evidentally $\Phi^+ \cup (-\Phi^+) = \Phi$. Let $x = (Mx_1, x_2)$ for some integer $M > 0$. For all M large enough, we have $x^2 < 0$. It remains only to show that for all M large enough, we also have $\langle x, y\rangle > 0$ for all $y \in \Phi^+$.

The desired inequality is immediate for all $y \in \Phi_1^+ \cup \Phi_2^+$. Now suppose $y = (y_1, y_2) \in \Phi_3^+$. Choose $d > 0$ such that $dL \subset L_1 \oplus L_2$. Then $dy_1 \in L_1$, and hence $\langle x_1, y_1 \rangle \geq 1/d$. Similarly, we have $|y_1^2| \geq 1/d^2$ provided $y_1^2 \neq 0$.

We claim that

$$y_2^2 \leq (2d^2 + 1)\langle x_1, y_1 \rangle^2 \tag{5.4}$$

for all $(y_1, y_2) \in \Phi_3^+$. Indeed, if $y_1^2 \neq 0$ then $|y_1^2| \geq 1/d^2$ and hence

$$y_2^2 = 2 + |y_1^2| \leq (2d^2 + 1)|y_1^2|.$$

The reverse Cauchy-Schwarz inequality together with the fact that $|x_1^2| \geq 1$ then gives

$$|y_1^2| \leq |x_1^2 y_1^2| \leq \langle x_1, y_1 \rangle^2,$$

which yields (5.4). For the case $y_1^2 = 0$ we just observe that $\langle x_1, y_1 \rangle^2 \geq 1/d^2$, and hence

$$y_2^2 = 2 \leq 2d^2 \langle x_1, y_1 \rangle^2,$$

so (5.4) holds in this case as well.

Now the usual Cauchy-Schwarz inequality implies

$$\langle x_2, y_2 \rangle^2 \leq x_2^2 y_2^2 \leq x_2^2 (2d^2 + 1)\langle x_1, y_1 \rangle^2.$$

So for any M large enough that $M^2 > (2d^2 + 1)x_2^2$, we have $\langle Mx_1, y_1 \rangle > |\langle x_2, y_2 \rangle|$, and hence $\langle x, y \rangle = \langle Mx_1, y_1 \rangle + \langle x_2, y_2 \rangle > 0$ for all $y = (y_1, y_2) \in \Phi_3^+$. Thus Φ^+ is a positive, f-invariant root system, and f is a positive automorphism of L. ■

6 Automorphisms of K3 surfaces

In this section we relate automorphisms of lattices to automorphisms of K3 surfaces.

K3 structures. Fix an even, unimodular lattice L of signature $(3, 19)$. A *K3 structure* on L consists of following data:

1. A *Hodge decomposition*

   $$L \otimes \mathbb{C} = L^{2,0} \oplus L^{1,1} \oplus L^{0,2}$$

   such that $L^{i,j} = \overline{L^{j,i}}$, and the Hermitian spaces $L^{1,1}$ and $L^{2,0} \oplus L^{0,2}$ have signatures $(1, 19)$ and $(2, 0)$ respectively;

2. A *positive cone* $\mathcal{C} \subset L^{1,1} \cap (L \otimes \mathbb{R})$, forming one of the two components of the locus $x^2 > 0$; and

3. A set of *effective roots*

$$\Psi^+ \subset \Psi = \{x \in L \cap L^{1,1} \,:\, x^2 = -2\},$$

satisfying $\Psi = \Psi^+ \cup (-\Psi^+)$.

We require that the *Kähler cone*

$$\mathcal{C}^+(L) = \{x \in \mathcal{C} \,:\, \langle x, y\rangle > 0 \ \forall y \in \Psi^+\}$$

defined by this data is nonempty.

Realizability. A K3 structure on L is *realized* by a K3 surface X if there exists an isomorphism

$$\iota : L \to H^2(X, \mathbb{Z})$$

sending $L^{i,j}$ to $H^{i,j}(X)$ and sending $\mathcal{C}^+(L)$ to the Kähler cone in $H^{1,1}(X, \mathbb{R})$. Similarly, an isometry $f : L \to L$ is *realized* an automorphism $F : X \to X$ if ι can be chosen so that the diagram

$$\begin{array}{ccc} L & \xrightarrow{\iota} & H^2(X,\mathbb{Z}) \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle F^*} \\ L & \xrightarrow{\iota} & H^2(X,\mathbb{Z}) \end{array}$$

commutes.

The following fundamental theorem [BPV, VIII] encapsulates the strong Torelli theorem for K3 surfaces as well as surjectivity of the period map:

Theorem 6.1 *Any K3 structure on L is realized by a unique K3 surface X, and any $f \in \mathrm{O}(L)$ preserving a given K3 surface structure is realized by a unique automorphism $F : X \to X$.*

Remarks. The Hodge structure on L determines X up to isomorphism, while the Kähler cone $\mathcal{C}^+(L)$ pins down the isomorphism ι. The Néron-Severi group $\mathrm{NS}(X) \cong \mathrm{Pic}(X) \subset H^2(X, \mathbb{Z})$ is given by

$$\mathrm{NS}(X) = \iota(L \cap L^{1,1}).$$

To conclude, we address the problem of finding an f-invariant K3 structure.

Theorem 6.2 *Let $f \in \mathrm{O}(L)$ be an isometry with spectral radius $\rho(f) > 1$. Suppose $\rho(f)$ is an eigenvalue of f, and there is a unique $\tau \in (-2,2)$ such that*

$$E_\tau = \mathrm{Ker}(f + f^{-1} - \tau I) \subset L \otimes \mathbb{R}$$

has signature $(2,0)$. Then f is realizable by a K3 surface automorphism iff $f|M(-1)$ is positive, where $M = L \cap E_\tau^\perp$.

Proof. Our assumptions imply there is an f-invariant Hodge structure with $L^{2,0} \oplus L^{0,2} \cong E_\tau \otimes \mathbb{C}$. Moreover, this is the unique f-invariant Hodge structure of K3 type, up to interchanging the roles of $L^{2,0}$ and $L^{0,2}$. In particular, $L^{1,1}$ is uniquely determined, as is the candidate Néron-Severi group

$$M = L \cap L^{1,1} = L \cap E_\tau^\perp$$

and the set of roots $\Psi = \{x \in M \,:\, x^2 = -2\}$.

Suppose $f|M(-1)$ is positive. Let $\Psi^+ \subset \Psi$ be a system of positive roots preserved by f. If M has signature $(1,n)$, then (by the definitions in §5, taking into account the reversal of signs) there is an $x \in M$ with $x^2 > 0$ such that $\langle x, y\rangle > 0$ for all $y \in \Psi^+$. Choose $\mathcal{C}$ so $x \in \mathcal{C}^+$; then $\mathcal{C}^+$ is nonempty, and $f(\mathcal{C}) = \mathcal{C}$ because the leading eigenvalue of f is positive. Thus f is realizable. If M has signature $(0,n)$, then the same argument applies, except $x^2 < 0$. But we can then simply replace x with $x' = x + z$, where $z \in L^{1,1} \cap M^\perp$ and $z^2 + x^2 > 0$; then $(x')^2 > 0$, so $\mathcal{C}^+ \neq \emptyset$, and hence f is realizable in this case as well.

Conversely, if f is realizable by $F : X \to X$, then F preserves the Kähler cone in $H^{1,1}(X, \mathbb{R})$, and hence f preserves the dual system of positive roots $\Psi^+ \subset \mathrm{NS}(X)(-1) \cong M(-1)$, so it is positive. ∎

The proof shows the pair (X, F) realizing f is unique up to complex conjugation, and that $M \cong \mathrm{NS}(X)$.

7 Minimum entropy

In this section we will show:

Theorem 7.1 *There exists an automorphism $F : X \to X$ of a non-algebraic K3 surface with entropy $h(F) = \log \lambda_{10} \approx \log 1.17628$.*

Building blocks. To exhibit F, we will construct a lattice automorphism $f : L \to L$ with characteristic polynomial

$$\det(xI - f) = P_{10}(x)(x-1)^9(x+1)(x^2+1)$$

satisfying the realizability criterion stated in Theorem 6.2. The pair (L, f) will in turn be obtained as a gluing of (L_1, f_1) and (L_2, f_2). We begin by describing these two constituents of f.

The Salem factor. Recall from §2 that E_{10} is an even, unimodular lattice of signature $(9, 1)$. The Salem polynomial $P_{10}(x)$ arises naturally as the characteristic polynomial

$$S_1(x) = P_{10}(x) = \det(xI - f_1)$$

of the Coxeter automorphism $f_1 : E_{10} \to E_{10}$ (see e.g. [Mc1]). Reducing $\bmod p$ for $p = 3$, we find

$$\overline{S}_1(x) = \left(x^2+1\right)\left(x^8 + x^7 + 2x^6 + x^5 + x^3 + 2x^2 + x + 1\right) \tag{7.1}$$

in $\mathbb{F}_3[x]$. This factorization suggests that with suitable twisting, we may be able to arrange that $\overline{f}_1$ acts with characteristic polynomial (x^2+1) on a glue group isomorphic to $\mathbb{F}_3^2$. And indeed this is the case: if we let

$$a = 2(f_1 + f_1^{-1}) + 3 \in \mathrm{End}(E_{10}),$$

then $|\det(a)| = 9$ and $3E_{10} \subset aE_{10}$, as can be checked by a matrix computation (e.g. $3a^{-1}$ is integral). It then follows from Theorem 4.2 that for $L_1 = E_{10}(a)$, we have

$$G(L_1) \cong \mathbb{F}_3^2 \quad \text{and} \quad \overline{Q}_1(x) = \det(xI - \overline{f}_1) = (x^2+1) \bmod 3.$$

To determine the signature of L_1, let $R_1(y) = y^5 + y^4 - 5y^3 - 5y^2 + 4y + 3$ be the trace polynomial of $S_1(x)$, and let

$$T = \{\tau_1, \tau_2, \tau_3, \tau_4\} \approx \{-1.886, -1.468, -0.584, 0.913\}$$

denote the roots of $R_1(y)$ which lie in $(-2, 2)$. The associated eigenspaces of $f + f^{-1}$ all have signature $(2, 0)$, since E_{10} has signature $(9, 1)$ (see equation 4.4). On the other hand, the polynomial $P(y) = 2y + 3$ is negative for $y = \tau_1$ but positive for $y = \tau_2, \tau_3, \tau_4$; since $a = P(f + f^{-1})$, this implies $L_1 = E_{10}(a)$ has signature $(7, 3)$ (by equation 4.5). Finally L_1 is an even lattice, by Proposition 4.1.

The cyclotomic factor. Now recall from §5 that there is a positive automorphism $g : A_2 \to A_2$ such that $\overline{g}$ acts with order two on $G(A_2) \cong \mathbb{F}_3$. Let $L_2 = E_8 \oplus A_2 \oplus A_2$. Note that L_2 has signature $(12, 0)$, and every root of L_2 lies in one of its summands. It follows that the order four map $f_2 : L_2 \to L_2$ given by

$$f_2(x, y, z) = (x, g(z), y)$$

is also positive. Its characteristic polynomial is given by

$$S_2(x) = (x-1)^9(x+1)(x^2+1),$$

while its action on $G(L_2) \cong \mathbb{F}_3^2$ has characteristic polynomial

$$\overline{Q}_2(x) = \det(xI - \overline{f}_2) = x^2 + 1.$$

Proof of Theorem 7.1. Since $\overline{Q}_1(x) = \overline{Q}_2(x) = x^2 + 1 \in \mathbb{F}_3[x]$ is a separable polynomial, nonvanishing at $x = \pm 1$, there is a gluing map $\phi : G(L_1) \to G(L_2)$ conjugating $\overline{f}_1$ to $\overline{f}_2$ by Theorem 3.1.

Let $L = (L_1 \oplus_\phi L_2)(-1)$. This is a lattice of signature $(3, 7) + (0, 12) = (3, 19)$. Since we are gluing at the odd prime $p = 3$, L is still even. By construction, $f_1 \oplus f_2$ extends to an isometry $f : L \to L$, with characteristic polynomial $S(x) = S_1(x)S_2(x)$.

Since $S_1(x)$ is a Salem polynomial and $S_2(x)$ is a product of cyclotomic polynomials, the spectral radius

$$\rho(f) = \max\{|\lambda| \,:\, S(\lambda) = 0\} = \lambda_{10}$$

is an eigenvalue of f. Moreover, the twist by a provides us with a unique eigenspace

$$E_\tau = \mathrm{Ker}(f + f^{-1} - \tau I) \subset L_1 \otimes \mathbb{R} \cong \mathbb{R}^{3,19}$$

with signature $(2, 0)$, coming from $\tau = \tau_1$.

Since $S_1(x)$ is irreducible, no element of L_1 lies in $E_\tau^\perp$; thus $M = L \cap E_\tau^\perp = L_2(-1)$. By construction, $f_2|L_2 \cong f|M(-1)$ is positive. Thus by Theorem 6.2 there is a K3 surface automorphism $F : X \to X$ realizing f; and $h(F) = \rho(f) = \lambda_{10}$ by equation (1.1). ■

Remarks.

1. We have $\mathrm{NS}(X)(-1) \cong E_8 \oplus A_2 \oplus A_2$. Thus by Grauert's criterion [BPV, III.2], the exceptional curves on X can be blown down to yield a singular complex manifold Y with no curves at all. The map F descends to an automorphism of Y which exchanges its two singular points of type A_2, and fixes its unique singular point of type E_8.

2. The ring $\mathbb{Z}[f_1 + f_1^{-1}]$ is in fact a Dedekind domain of class number one, so by Theorem 4.3, the existence of the desired twist of E_{10} is automatic once one has the factorization (7.1).

3. Oguiso gives an example of a K3 surface automorphism with entropy $\log \lambda_{14} \approx \log 1.20002$ [Og]. This example is analogous to the one above, but with $L_1 = \mathrm{II}_{11,3}$ and $L_2 = E_8$. Here both lattices are unimodular, so no glue is necessary, and one can take $f_2(x) = x$. The existence of an $f_1 \in \mathrm{O}(L_1)$ with characteristic polynomial $P_{14}(x)$ is guaranteed by [GM].

4. Many examples of K3 surface automorphisms based on Salem numbers of degree 22 are given in [Mc2]. In these examples no gluing takes place (there is no cyclotomic factor), and positivity is automatic, because the Néron-Severi group is trivial.

5. We remark that gluing theory is also useful for describing the Kummer surface X associated to a complex torus A: indeed, $H^2(X,\mathbb{Z})$ is obtained by gluing $H^2(A,\mathbb{Z})(2)$ along $\mathbb{F}_2^6$ to a fixed lattice of rank 16 (see [BPV, VIII.5]).

8 A projective example

In this section we will show:

Theorem 8.1 *There exists an automorphism $F : X \to X$ of a projective K3 surface with entropy $h(F) = \log \lambda_6 \approx \log 1.40126$.*

For the proof, we will construct a model for $F|H^2(X,\mathbb{Z})$ by gluing together four lattice automorphisms $f_i : L_i \to L_i$, $i = 1, \ldots, 4$ (see Figure 4), and twisting by -1. The result will be an automorphism $f : L \to L$ of an even, unimodular lattice of signature $(3, 19)$ with characteristic polynomial

$$S(x) = P_6(x)C_{13}(x)(x^2 + x + 1)(x - 1)^2, \tag{8.1}$$

where $P_6(x)$ is the Salem polynomial for λ_6 (see Table 1) and $C_{13}(x) = (x^{13} - 1)/(x - 1)$. Theorem 6.2 will imply that f is realizable.

We now turn to the construction of the building blocks $f_i : L_i \to L_i$. For each i we will determine the signature of L_i, the glue group $G(L_i)$, and the characteristic polynomial

$$\overline{Q}_{i,p}(x) = \det(xI - \overline{f}_i|G(L_i)_p) \in \mathbb{F}_p[x]$$

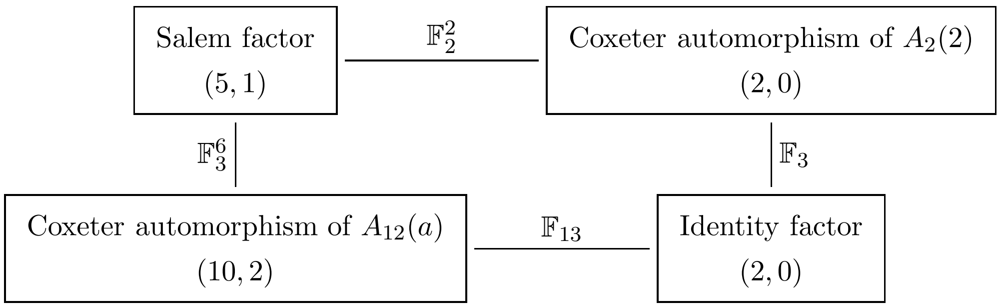

Figure 4. Assembly of an algebraic K3 automorphism with entropy $\log \lambda_6$.

of $\overline{f}_i$ for each prime p where it is nontrivial.

1. The Salem factor. Let $W = \wedge^2 \mathbb{Z}^4$, with the natural inner product

$$\langle \alpha, \beta \rangle = \alpha \wedge \beta \in \wedge^4 \mathbb{Z}^4 \cong \mathbb{Z}.$$

Then $W \cong \mathrm{II}_{3,3}$ is an even, unimodular lattice of signature $(3,3)$, and any $g \in \mathrm{SL}_4(\mathbb{Z})$ gives rise to an isometry $f = \wedge^2 g \in \mathrm{O}(W)$. In particular, if we take $g = g_1$ to be the companion matrix for $x^4 + x + 1$, then we obtain a map $f_1 \in \mathrm{O}(W)$ with characteristic polynomial

$$S_1(x) = \det(I - f_1) = P_6(x).$$

(This is related to the fact that $\log \lambda_6$ can be realized as the entropy of an automorphism of a complex 2-torus [Mc2, §5].) Reducing mod $p = 2$, we find

$$\overline{S}_1(x) = (1 + x + x^2)(1 + x + x^2 + x^3 + x^4)$$

in $\mathbb{F}_2[x]$. This factorization suggests we can find a twist $W(a)$ such that

$$G(W(a)) = \mathbb{F}_2^2 \quad \text{and} \quad \det(xI - \overline{f}_1 | W(a)) = (1 + x + x^2).$$

Indeed, this is the case for $a = -(1 + f + f^{-1})$, as can be verified with the help of Theorem 4.2. Similarly, if we set $L_1 = W(3a)$, then we find

$$\begin{aligned} G(L_1) &= G(L_1)_2 \oplus G(L_1)_3 = \mathbb{F}_2^2 \oplus \mathbb{F}_3^6, \\ \overline{Q}_{1,2}(x) &= (1 + x + x^2) \quad \text{and} \\ \overline{Q}_{1,3}(x) &= (2 + x + x^2 + x^3)(2 + 2x + 2x^2 + x^3). \end{aligned}$$

(Note that $\overline{Q}_{1,3}(x)$ is a reciprocal polynomial, even though its irreducible factors are not). Since W is even, and we have twisted by $3a$, we have $\langle x,x\rangle \in 6\mathbb{Z}$ for all $x \in L_1$. In particular, L_1 is an even lattice with *no roots*. It signature is $(5,1)$, as can be checked using equation (4.5).

2. The order 13 factor. Next consider the Coxeter automorphism $f_2 : A_{12} \to A_{12}$. This map has order 13, so its characteristic polynomial is given by $S_2(x) = C_{13}(x)$, which factors modulo $p = 3$ as

$$\overline{S}_2(x) = (2+x+x^2+x^3)(2+2x+2x^2+x^3)(2+2x+x^3)(2+x^2+x^3).$$

The map $\overline{f}_2|G(A_{12}) \cong \mathbb{Z}/13$ is the identity, since f_2 belongs to the Weyl group of A_{12} (see §2). If we set $L_2 = A_{12}(a)$ where $a = 1 + (f_2 + f_2^{-1}) - (f_2 + f_2^{-1})^3$, then $aA_{12} \subset 3A_{12}$ and we find

$$\begin{aligned} G(L_2) &= G(L_2)_3 \oplus G(L_1)_{13} = \mathbb{F}_3^6 \oplus \mathbb{F}_{13}, \\ \overline{Q}_{2,3}(x) &= (2+x+x^2+x^3)(2+2x+2x^2+x^3), \quad \text{and} \\ \overline{Q}_{2,13}(x) &= (x-1). \end{aligned}$$

(Note that we have chosen a so that $\overline{Q}_{1,3} = \overline{Q}_{2,3}$.) In this case L_2 is an even lattice of signature $(10,2)$.

The action of $\overline{f}_2$ determines the fractional form on $G(L_2)_3$, but not on $G(L_2)_{13}$ (where it acts by the identity). For later use we note:

The determinant of $G(L_2)_{13}$ is not a square.

That is, the nonzero values of the form $13\langle\langle x,x\rangle\rangle$ consist of the non-square numbers $\{2,4,6,7,8,11\} \bmod 13$. This can be verified by a direct matrix computation, or by noting that $\det G(A_{12}) = -1$ (as computed in Proposition 3.5) is a square mod 13 but 8 is not, and $ax = 8x$ for $x \in G(A_{12})$, since $\overline{f}_2(x) = x$.

3. The order 3 factor. Let $f_3 : A_2 \to A_2$ be the Coxeter automorphism, and let $L_3 = A_2(2)$. Then the characteristic polynomial of f_3 is given by $S_3(x) = x^2 + x + 1$, and $\overline{f}_3|G(A_2)$ is the identity. It follows that

$$\begin{aligned} G(L_3) &= G(L_3)_2 \oplus G(L_3)_3 = \mathbb{F}_2^2 \oplus \mathbb{F}_3, \\ \overline{Q}_{2,2}(x) &= x^2+x+1, \quad \text{and} \\ \overline{Q}_{2,3}(x) &= (x-1). \end{aligned}$$

The lattice L_2 has signature $(2,0)$, and $\langle x,x\rangle \in 4\mathbb{Z}$ for all $x \in L_2$. Since -1 is not a square mod 3, and neither is the twisting parameter 2, using Proposition 3.5 again we find:

The determinant of $G(L_3)_3$ *is a square.*

4. The identity factor. Finally let $L_4 \cong \mathbb{Z}^2$ be the even lattice of signature $(2,0)$ and determinant 39 with inner product matrix $B = \left(\begin{smallmatrix} 2 & 1 \\ 1 & 20 \end{smallmatrix}\right)$. Then

$$G(L_4) = G(L_4)_3 \oplus G(L_4)_{13} = \mathbb{F}_3 \oplus \mathbb{F}_{13}.$$

To control later gluings, the following two properties are important.

If $x \in L_4^\vee$ *projects to a nontrivial element of* $\mathbb{F}_3 \subset G(L_4)$*, then* $x^2 > 2$*.*

In fact, $(1,1)/3$ and $(-1,-1)/3$ are the minimal norm vectors in $L_4^\vee$ representing the nonzero elements of $\mathbb{F}_3$, and each satisfies $x^2 = 8/3$.

Neither $\det G(L_4)_3$ *nor* $\det G(L_4)_{13}$ *is a square.*

To see this, note that $2/39$ appears on the diagonal of B^{-1}. Thus $\langle\langle x,x\rangle\rangle = 2/39 \bmod 1$ for some x in $G(L_4)$; this implies $\det G(L_4)_3 = [3\langle\langle 13x, 13x\rangle\rangle] = [2 \bmod 3]$ and $\det G(L_4)_{13} = [13\langle\langle 3x, 3x\rangle\rangle] = [6 \bmod 13]$, and neither class is a square.

As an automorphism of L_4, we simply take $f_4(x) = x$.

Assembly. By construction, we have gluing isometries

$$\begin{aligned} \phi_{12} &: G(L_1)_3 \to G(L_2)_3 \cong \mathbb{F}_3^6, \\ \phi_{13} &: G(L_1)_2 \to G(L_3)_2 \cong \mathbb{F}_2^2, \\ \phi_{24} &: G(L_2)_{13} \to G(L_4)_{13} \cong \mathbb{F}_{13}, \quad \text{and} \\ \phi_{34} &: G(L_3)_3 \to G(L_4)_3 \cong \mathbb{F}_3, \end{aligned}$$

satisfying $\phi_{ij}\overline{f}_i = \overline{f}_j\phi_{ij}$. The first glue map ϕ_{12} exists by Theorem 3.1, since $\overline{Q}_{1,3} = \overline{Q}_{2,3}$. Similar reasoning applies to the second. The third map ϕ_{24} exists because both the domain and range have non-square determinant, and because (-1) is a square mod 13. (Recall that a gluing map must reverse the sign of the bilinear form.) The last map exists because its domain has square determinant, while its range does not, and because -1 is *not* a square mod 3.

Let $\bigoplus_\phi L_i$ denote the unimodular lattice of signature $(19,3)$ obtained by gluing together all four lattices, as shown Figure 4. Let $L = (\bigoplus_\phi L_i)(-1)$, and let $f : L \to L$ denote the linear extension of $\oplus f_i$. Then the characteristic polynomial of f is given by $S(x) = \prod_1^4 S_i(x)$, which agrees with equation (8.1).

Evenness. We claim L is even. This is almost automatic, since its constituents L_i are even and since almost all the gluings take place over groups of odd order. The one exception comes from ϕ_{13}. To verify evenness, we must check that the $\mathbb{Q}/\mathbb{Z}$-valued quadratic forms $q_i(x)$ on $G(L_i)_2$, $i = 1, 3$, defined by equation (2.4), satisfy $q_1(x) + q_3(\phi_{13}(x)) = 0 \bmod 1$. But q_i is invariant under $\overline{f}_i$, which cyclically permutes the three nonzero vectors in $G(L_i)_2 \cong \mathbb{F}_2^2$. This easily implies that $q_i(x) = 1/2$ for all $x \neq 0$, so the sum vanishes and hence L is even.

Proof of Theorem 8.1. Clearly $\rho(f) = \lambda_6 > 1$, since all other roots of $S(x)$ are inside or on the unit circle. By construction, $f + f^{-1}$ has a unique eigenspace of signature $(2, 0)$, namely

$$E_\tau = \mathrm{Ker}(f + f^{-1} - \tau I) \subset L_2 \otimes \mathbb{R}$$

where $\tau = 2\cos(2\pi/13)$. Since the action of f on L_2 is irreducible over $\mathbb{Q}$, the candidate Néron-Severi group $M = L \cap E_\tau^\perp$ satisfies

$$M(-1) = L_1 \oplus_{\phi_{13}} L_3 \oplus_{\phi_{34}} L_4.$$

We claim $f_{13} = f_1 \oplus f_3$ is positive on the Lorentzian lattice

$$L_{13} = L_1 \oplus_{\phi_{13}} L_3.$$

Indeed, we have $x^2 \in 2a_i\mathbb{Z}$ for all $x \in L_i$, where $a_1 = 3$ and $a_3 = 2$; and $bL \subset L_1 \oplus L_3$ for $b = 2$, since we are gluing along $\mathbb{F}_2^2$. Since $b^2 = 4 \notin \mathbb{Z}_+ a_1 + \mathbb{Z}_+ a_3$, positivity follows from Theorem 5.1.

Note that, since f_4 is the identity, it gives a positive automorphism of the Euclidean lattice L_4.

We now claim that the sum of positive automorphisms, $f_{134} = f_{13} \oplus f_4$, is positive on $L_{134} = L_{13} \oplus_{\phi_{34}} L_4 = M(-1)$. Here the gluing takes place over $\mathbb{F}_3$. In fact, the desired positivity follows from Theorem 5.2. For if $(x, y) \in L_{134}$ is a root but $(x, y) \notin L_{13} \oplus L_4$, then $y \in L_4^\vee$ represents a nonzero element $[x_4] \in \mathbb{F}_3 \subset G(L_4)$, and hence (as we have seen above) $y^2 \geq 8/3 > 2$.

Thus $f|M(-1)$ is positive. By Theorem 6.2, there is a K3 surface automorphism $F : X \to X$ realizing $f : L \to L$; by construction, $h(F) = \log \rho(f) = \log \lambda_6$; and since $M \cong \mathrm{NS}(X)$ has signature $(1, 9)$, X is projective. ∎

Remarks.

1. Since $P_6(x)$ is an *unramified* Salem polynomial, the fact that it can be realized by an isometry $f_1 \in \mathrm{O}(\mathrm{II}_{3,3})$ also follows from general results [GM].

2. The existence of the twists producing L_1 and L_2 can, as in §7, be explained by the fact that $\mathbb{Z}[f_1 + f_1^{-1}]$ and $\mathbb{Z}[f_2 + f_2^{-1}]$ are Dedekind domains of class number one.

3. We note that $\mathrm{NS}(X)$ has signature $(1, 9)$ and determinant $3^6 \cdot 13 = 9477$, and $F^*|H^{2,0}(X)$ has order 13.

4. The Coxeter polynomial for Eh_8 (the 'hyperbolic extension of E_6', with diagram $Y_{3,3,4}$) is the same as the characteristic polynomial for $f|L_1 \oplus L_3$, namely $P_6(x)(1 + x + x^2)$ (see [Mc1, Table 5]). In fact the Coxeter automorphism of Eh_8 could have been taken as the starting point for the construction of f, just as the Coxeter automorphism of E_{10} (the hyperbolic extension of E_8) was the starting point for the construction in §7.

References

[BPV] W. Barth, C. Peters, and A. van de Ven. *Compact Complex Surfaces.* Springer-Verlag, 1984.

[BK] E. Bedford and K. Kim. Periodicities in linear fractional recurrences: Degree growth of birational surface maps. *Michigan Math. J.* **54**(2006), 647–670.

[Ca] S. Cantat. Dynamique des automorphismes des surfaces projectives complexes. *CRAS Paris Sér. I Math.* **328**(1999), 901–906.

[CoS] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups.* Springer-Verlag, 1999.

[Ger] L. J. Gerstein. *Basic Quadratic Forms.* American Mathematical Society, 2008.

[GM] B. Gross and C. McMullen. Automorphisms of even unimodular lattices and unramified Salem numbers. *J. Algebra* **257**(2002), 265–290.

[Hum] J. E. Humphreys. *Reflection Groups and Coxeter Groups.* Cambridge University Press, 1990.

[Kn] M. Kneser. Klassenzahlen definiter quadratischer Formen. *Arch. Math.* **8**(1957), 241–250.

[La] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970.

[Mc1] C. McMullen. Coxeter groups, Salem numbers and the Hilbert metric. *Publ. Math. IHES* **95**(2002), 151–183.

[Mc2] C. McMullen. Dynamics on K3 surfaces: Salem numbers and Siegel disks. *J. reine angew. Math.* **545**(2002), 201–233.

[Mc3] C. McMullen. Dynamics on blowups of the projective plane. *Publ. Math. IHES* **105**(2007), 49–89.

[MH] J. Milnor and D. Husemoller. *Symmetric Bilinear Forms.* Springer, 1973.

[Og] K. Oguiso. The third smallest Salem number in automorphisms of K3 surfaces. *Preprint, 2009.*

[Ser] J. P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

Mathematics Department
Harvard University
1 Oxford St
Cambridge, MA 02138-2901