Effective Computation of Hodge Cycles

Edgar Costa (MIT)

November 28, 2024, University of Sydney

Slides available at edgarcosta.org.
Joint work with Nicholas Mascot, Jeroen Sijsling, John Voight, and Emre Can Sertöz

Endomorphism ring of an abelian variety

Let A be an abelian variety defined over k.

Goal

Given A compute the endomorphism ring $\operatorname{End} A$.

Endomorphism ring of an abelian variety

Let A be an abelian variety defined over k.

Goal

Given A compute the endomorphism ring $\operatorname{End} A$.

- Over a finite field, Honda–Tate theory tells us

$$\det(1 - t\,\mathrm{Frob}|H^1(A, \mathbb{Q}_\ell)) \in 1 + t\mathbb{Z}[t]$$

  determines the k-isogeny class and the isomorphism class of $\operatorname{End}(A) \otimes \mathbb{Q}$.
  If $A = \operatorname{Jac}(C)$, then we can compute this via `LPolynomial`.

Endomorphism ring of an abelian variety

Let A be an abelian variety defined over k.

Goal

From the equations of A determine a basis for $\operatorname{End} A$ and their equations in $A \times A$.

- Over a finite field, Honda–Tate theory tells us

$$\det(1 - t\operatorname{Frob}|H^1(A, \mathbb{Q}_\ell)) \in 1 + t\mathbb{Z}[t]$$

  determines the k-isogeny class and the isomorphism class of $\operatorname{End}(A) \otimes \mathbb{Q}$.
  If $A = \operatorname{Jac}(C)$, then we can compute this via `LPolynomial`.
- There are several in principle algorithms to do this over a number field.
  These involve, a day/night algorithm:
  - by day: search for reasonable morphisms;
  - by night: restrict your search space.

Our setup

Let C be a nice (smooth, projective, geometrically integral) curve over k of genus g given by equations. Let J be the Jacobian of C.

Goal

Given the equations of C, compute the endomorphism ring $\operatorname{End} J^{\mathrm{al}}$.

Our setup

Let C be a nice (smooth, projective, geometrically integral) curve over k of genus g given by equations. Let J be the Jacobian of C.

Goal

Given the equations of C, compute the endomorphism ring $\operatorname{End} J^{\mathrm{al}}$.

But why?

- It is an interesting challenge [*citation needed*].
- If $\operatorname{End} J$ contains non-trivial idempotents, we can hope to decompose J into abelian varieties of smaller dimension.
- If $\operatorname{End} J$ is non-trivial, then this allows us to find a modular form that describes the arithmetic properties of J and C.

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g/\Lambda,$$

where we pick an k basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model `BigPeriodMatrix(RiemannsSurface(f, σ))`.

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick an k basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model `BigPeriodMatrix(RiemannsSurface(f, σ))`.
  Picking a projection that works is sometimes a challenge.

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick an k basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model `BigPeriodMatrix(RiemannsSurface(f,` σ`))`. Picking a projection that works is sometimes a challenge.
- Using Λ, we can hope to understand J analytically...

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$ and a projection into $\mathbb{P}^2$, we can consider C as a Riemann surface, and

$$J_{\mathbb{C}} = H^0(C, \Omega_C)^\vee / H_1(C, \mathbb{Z}) = \mathbb{C}^g / \Lambda,$$

where we pick an k basis for $H^0(C, \Omega_C) = k\omega_1 \oplus \ldots \oplus k\omega_g$, hence,

$$\Lambda = \left\{ \left(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_g \right) \in \mathbb{C}^g \ : \ \gamma \in H_1(C, \mathbb{Z}) \right\} \cong \mathbb{Z}^{2g}.$$

In other words, J is a complex torus (plus a polarization).

- We can calculate Λ numerically by taking a plane model `BigPeriodMatrix(RiemannsSurface(f,` σ`))`. Picking a projection that works is sometimes a challenge.
- Using Λ, we can hope to understand J analytically...
- and perhaps even to be able to transfer these results to the algebraic setting.

Heuristic solution

By picking a k-basis for $H^0(C, \Omega_C)$, we have

$$\mathbf{End}(J) = \{T \in M_g(k) \mid T\Lambda \subset \Lambda\}$$

Hence, if Π is a period matrix for C, i.e., $\Lambda = \Pi\mathbb{Z}^{2g}$, then we are reduced to finding a $\mathbb{Z}$-basis of the solutions (T, R) to

$$T\Pi = \Pi R, \qquad T \in M_g(k^{\mathrm{al}}), \quad R \in M_{2g}(\mathbb{Z}).$$

Heuristically, via lattice reduction algorithms, we can find such a $\mathbb{Z}$-basis.

The Galois module structure of $\mathbf{End}(J)$ is given via $T \in M_g(k^{\mathrm{al}})$.

There is no obvious way to prove that our guesses are actually correct.

The reconstruction of $T \in M_g(k^{\mathrm{al}})$ can be quite finicky, this lead to a whole library to work with $k \subset \mathbb{C}$ with fixed embedding.

Representing endomorphisms

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \longmapsto \{Q_1, \ldots, Q_g\} \Longleftrightarrow \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

Representing endomorphisms

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \longmapsto \{Q_1, \ldots, Q_g\} \iff \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

Given $\alpha \in \mathrm{M}_g(k^{\mathrm{al}})$ this divisor is a certificate of containment 

for $\alpha \in \mathrm{End}\, J^{\mathrm{al}}$.

Representing endomorphisms

$$\alpha_C : C \xrightarrow{AJ} J \xrightarrow{\alpha} J \dashrightarrow \mathrm{Sym}^g(C)$$

$$P \longmapsto \{Q_1, \ldots, Q_g\} \Longleftrightarrow \alpha([P - P_0]) = \left[\sum_{i=1}^{g} Q_i - P_0\right]$$

This traces out a divisor on $C \times C$, which determines α.

Given $\alpha \in \mathrm{M}_g(k^{\mathrm{al}})$ this divisor is a certificate of containment  for $\alpha \in \operatorname{End} J^{\mathrm{al}}$.

Theorem (C–Mascot–Sijsling–Voight)

We give an algorithm for

$$\mathrm{M}_g(k^{\mathrm{al}}) \ni \alpha \mapsto \begin{cases} \texttt{true} & \text{if } \alpha \in \operatorname{End} J^{\mathrm{al}}, \text{ and a certificate} \\ \texttt{false} & \text{if } \alpha \notin \operatorname{End} J^{\mathrm{al}} \end{cases}$$

By interpolation via α_C or by locally solving a differential equation on $C \times C$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* ✓.

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.

$$\mathrm{M}_g(k^{\mathrm{al}}) \ni \alpha \mapsto \begin{cases} \texttt{true} & \text{if } \alpha \in \operatorname{End} J^{\mathrm{al}}, \text{ and a certificate} \\ \texttt{false} & \text{if } \alpha \notin \operatorname{End} J^{\mathrm{al}} \end{cases}$$

- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* .

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

$$\{L_{p_1}(t) := \det(1 - t \operatorname{Frob}_p | H^1), L_{p_2}(t), \ldots, L_{p_i}(t)\} \longmapsto \text{upper bounds on } \operatorname{End} J^{\mathrm{al}}$$

  - The $L_p(t)$ polynomials are as random as $\operatorname{End} J^{\mathrm{al}}$ allows it.
  - Two polynomials $L_p(t)$ and $L_q(t)$ suffice to obtain a sharp upperbound.
  - For (p, q) in a set of positive density, but unknown apriori.

Rigorous Endomorphism ring

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight, C–Sertöz)

We give an algorithm that computes $\operatorname{End} J^{\mathrm{al}}$ *with a certificate* ✓.

This is a day/night algorithm:

- By day, we compute $\Lambda \subset \mathbb{C}^g$ numerically and then certify $B \subseteq \operatorname{End} J^{\mathrm{al}}$.
- By night, we search for evidence that $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

$$\operatorname{Frob}_p \bmod p^N \circlearrowright H^1_{\mathrm{crys}}(C, \mathbb{Z}_p) \longmapsto \text{upper bounds on } \operatorname{End} J^{\mathrm{al}}$$

- $\operatorname{Frob}_p \bmod p^N$ is a byproduct of computing $L_p(t) = \det(1 - t \operatorname{Frob}_p | H^1_{MW})$.
- We check what correspondences $C \rightsquigarrow C \bmod p$ lift to $C \rightsquigarrow C \bmod p^N$.

Examples

- Our method works just as well for isogenies and projections.
- We have verified, decomposed and matched the 66,158 curves over $\mathbb{Q}$ of genus 2 in the *L-functions and modular form database* (LMFDB).
- The algorithms verify that the plane quartic

$$C : x^4 - x^3y + 2x^3z + 2x^2yz + 2x^2z^2 - 2xy^2z + 4xyz^2 - y^3z + 3y^2z^2 + 2yz^3 + z^4 = 0$$

  has complex multiplication.
- Try it:

  https://github.com/edgarcosta/endomorphisms

  contains friendly button-push algorithms.

“Dans la seconde partie de mon rapport, il s’agit des variétés kählériennes dites K3, ainsi nommées en l’honneur de Kummer, Kähler, Kodaira et de la belle montagne K2 au Cachemire.” —André Weil *(Photo credit: Waqas Anees)*

What is a K3 surface?

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

What is a K3 surface?

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

e.g. Fermat quartic surface $x^4 + y^4 + z^4 + w^4 = 0$.

What is a K3 surface?

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

e.g. Fermat like surface $w^2 = x^6 + y^6 + z^6$.

What is a K3 surface?

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

- Kummer surfaces, $\mathrm{Kummer}(A) := \widetilde{A/\pm}$, with A an abelian surface.

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{NS} X^{\mathrm{al}} \simeq \operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Plays a similar role as $\operatorname{End}(A)$ for an abelian variety A

$$\operatorname{NS}(A) \otimes \mathbb{Q} \simeq \{\phi \in \operatorname{End}(A) \otimes \mathbb{Q} : \phi^{\dagger} = \phi\},$$

where † denotes the Rosati involution.

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\mathrm{NS}\, X^{\mathrm{al}} \simeq \mathrm{Pic}\, X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Plays a similar role as $\mathrm{End}(A)$ for an abelian variety A

$$\mathrm{NS}(A) \otimes \mathbb{Q} \simeq \{\phi \in \mathrm{End}(A) \otimes \mathbb{Q} : \phi^{\dagger} = \phi\},$$

where $\dagger$ denotes the Rosati involution.

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\mathrm{Pic}\, X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z}) \subsetneq H^2(X, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

Thus, $1 \leq \mathrm{rk}\, \mathrm{Pic}\, X^{\mathrm{al}} \leq 20 = \dim H^{1,1}(X)$. A generic K3 surface has $\mathrm{rk}\, \mathrm{Pic}\, X^{\mathrm{al}} = 1$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\mathrm{NS}\, X^{\mathrm{al}} \simeq \mathrm{Pic}\, X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Plays a similar role as $\mathrm{End}(A)$ for an abelian variety A

$$\mathrm{NS}(A) \otimes \mathbb{Q} \simeq \{\phi \in \mathrm{End}(A) \otimes \mathbb{Q} : \phi^\dagger = \phi\},$$

where $\dagger$ denotes the Rosati involution.

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\mathrm{Pic}\, X^{\mathrm{al}} \simeq H^{1,1}(X) \cap H^2(X, \mathbb{Z}) \subsetneq H^2(X, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

Thus, $1 \leq \mathrm{rk}\, \mathrm{Pic}\, X^{\mathrm{al}} \leq 20 = \dim H^{1,1}(X)$. A generic K3 surface has $\mathrm{rk}\, \mathrm{Pic}\, X^{\mathrm{al}} = 1$

“New and interesting” Galois representations arise from $T(X)$.

$$H^2(X, \mathbb{Q}) \simeq Pic(X^{\mathrm{al}})_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

"The evaluation of ρ for a given surface presents in general grave difficulties." — Zariski

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X \rangle / \langle \text{linear equivalences} \rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

"The evaluation of ρ for a given surface presents in general grave difficulties." — Zariski

Useful for studying the existence rational points, precisely, via a potential Brauer–Manin obstruction on X, as

$$H^1(\operatorname{Gal}(k^{\mathrm{al}}/k), \operatorname{Pic} X^{\mathrm{al}}) \simeq \operatorname{Br}_1(X)/Br_0(X).$$

Picard lattice of a K3 surface

Let X be a K3 surface defined over $k \subset \mathbb{C}$. We view X also as a complex manifold.

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

Useful for studying the existence rational points, precisely, via a potential Brauer–Manin obstruction on X, as

$$H^1(\operatorname{Gal}(k^{\mathrm{al}}/k), \operatorname{Pic} X^{\mathrm{al}}) \simeq \operatorname{Br}_1(X)/Br_0(X).$$

Over a finite field, Tate conjecture (proven) gives us $\operatorname{rk} \operatorname{Pic} X$ from

$$\det(1 - t \operatorname{Frob} | H^2(X, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$$

and Artin–Tate conjecture (proven) also gives $\operatorname{disc} \operatorname{Pic} X^{\mathrm{al}}$ modulo squares.
Acessible via `WeilPolynomialOfDegree2K3Surface(`$w^2 = f(x,y,z)$`)`

Picard lattice of a K3 surface

$$\operatorname{Pic} X^{\mathrm{al}} \simeq \mathbb{Z}\langle \text{algebraic curves in } X\rangle / \langle \text{linear equivalences}\rangle \subset H_2(X, \mathbb{Z})$$

Goal

From the equations of X, compute $\operatorname{Pic} X^{\mathrm{al}} \subset H_2(X, \mathbb{Z})$ as a $\operatorname{Gal}(k^{\mathrm{al}}/k)$-module.

Over a finite field, Tate conjecture (proven) gives us $\operatorname{rk} \operatorname{Pic} X$ from

$$\det(1 - t \operatorname{Frob} | H^2(X, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$$

and Artin–Tate conjecture (proven) also gives $\operatorname{disc} \operatorname{Pic} X^{\mathrm{al}}$ modulo squares.
Acessible via `WeilPolynomialOfDegree2K3Surface(`$w^2 = f(x, y, z)$`)`

Over a number field there are several in principle algorithms to compute $\operatorname{rk} \operatorname{Pic} X$ or even $\operatorname{Pic} X$. These involve, a day/night algorithm:

- by day: find curve classes in $\operatorname{Pic} X$;
- by night: restrict the ambient space for $\operatorname{Pic} X \subset H^2(X, \mathbb{Z})$.

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathsf{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

- Π can be computed:
    - rigorously as a ball via deformation for projective hypersurfaces (Sertöz)
    - heuristically for degree 2 surfaces branched over 6 lines (Elsenhans–Jahnel)

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

- Π can be computed:
  - rigorously as a ball via deformation for projective hypersurfaces (Sertöz)
  - heuristically for degree 2 surfaces branched over 6 lines (Elsenhans–Jahnel)
- Heuristically, via lattice reduction algorithms, we can find $\Lambda \subset H_2(X, \mathbb{Z})$.
- There is no obvious way to prove that our guesses are actually correct.

An analytic approach

Lefschetz (1,1) theorem

A homology class $\gamma \in H_2(X, \mathbb{Z})$ is in $\operatorname{Pic} X^{\mathrm{al}}$ if and only if $\int_\gamma \omega_X = 0$, where ω_X is the nonzero holomorphic 2-form ω_X on X, unique up to scaling.

Hence, if $\Pi = [\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})} \in \mathbb{C}^{22}$ is the period vector for ω_X, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in H_2(X, \mathbb{Z}) \simeq \mathbb{Z}^{22}.$$

- Π can be computed:
  - rigorously as a ball via deformation for projective hypersurfaces (Sertöz)
  - heuristically for degree 2 surfaces branched over 6 lines (Elsenhans–Jahnel)
- Heuristically, via lattice reduction algorithms, we can find $\Lambda \subset H_2(X, \mathbb{Z})$.
- There is no obvious way to prove that our guesses are actually correct.
- Nonetheless, given Π as a ball, one can compute $B \gg 0$ such that such that

$$\operatorname{Pic}(X^{\mathrm{al}})_{|B} := \mathbb{Z}\langle \gamma \in \operatorname{Pic} X^{\mathrm{al}} \mid -\gamma_{\mathrm{prim}}^2 < B \rangle \subseteq \Lambda \qquad \text{(Lairez–Sertöz).}$$

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
  - The Picard rank of a K3 surface over $\mathbb{F}_p^{\mathrm{al}}$ is always even.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
  - The Picard rank of a K3 surface over $\mathbb{F}_p^{\mathrm{al}}$ is always even.
  - If p and q are two primes of good reduction, such that

$$\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} = \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} = 20 \text{ and } \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} \neq \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} \implies \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} < 20.$$

    this can be deduced from $\det(1 - t\,\mathrm{Frob}_\bullet | H^2(X, \mathbb{Q}_\ell))$. (van Luijk)

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
  - The Picard rank of a K3 surface over $\mathbb{F}_p^{\mathrm{al}}$ is always even.
  - If p and q are two primes of good reduction, such that

    $$\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} = \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} = 20 \text{ and } \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} \neq \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} \Longrightarrow \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} < 20.$$

    this can be deduced from $\det(1 - t\,\mathrm{Frob}_\bullet | H^2(X, \mathbb{Q}_\ell))$. (van Luijk)
  - Use p-adic variational Hodge conjecture to show that only at most 19 classes lift to characteristic zero. One needs $\mathrm{Frob}_p \bmod p^N \circlearrowright H^1_{\mathrm{crys}}(C, \mathbb{Z}_p)$ (C–Sertöz)

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3 z + yw^3 + z^3 w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
  - The Picard rank of a K3 surface over $\mathbb{F}_p^{\mathrm{al}}$ is always even.
  - If p and q are two primes of good reduction, such that

    $$\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} = \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} = 20 \text{ and } \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_p} \neq \operatorname{disc}\operatorname{Pic} X^{\mathrm{al}}_{\mathbb{F}_q} \implies \operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} < 20.$$

    this can be deduced from $\det(1 - t\,\mathrm{Frob}_\bullet | H^2(X, \mathbb{Q}_\ell))$. (van Luijk)
  - Use p-adic variational Hodge conjecture to show that only at most 19 classes lift to characteristic zero. One needs $\mathrm{Frob}_p \bmod p^N \circlearrowright H^1_{\mathrm{crys}}(C, \mathbb{Z}_p)$ (C–Sertöz)
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \stackrel{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut}\Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut}\Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.
- No small rational curves: There are no lines, no conics, no twisted cubics.
- The “smallest” non-trivial curves that appear are smooth rational quartics.

A running example inspired by Klein–Mukai

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

- It is a fiber in a pencil that has generic rank 19, thus $\operatorname{rk}\operatorname{Pic} X^{\mathrm{al}} \geq 19$.
- Matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes $\Lambda \simeq \mathbb{Z}^{19}$ such that

$$\Pi\Lambda \approx 0 \qquad \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}.$$

- We can compute $\operatorname{Aut}\Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2,7)$.
- No small rational curves: There are no lines, no conics, no twisted cubics.
- The “smallest” non-trivial curves that appear are smooth rational quartics.
- Lattice computations with Λ predict that there are

  133056

  smooth rational quartics spanning Λ.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon H_2(X,\mathbb{Z}) \times H^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1 H^2_{\mathrm{dR}}(X/k)$.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon H_2(X,\mathbb{Z}) \times H^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1 H^2_{\mathrm{dR}}(X/k)$.

Theorem (Movasati–Sertöz)

If $\gamma = [C] \in H_2(X,\mathbb{Z})$ for a curve $C \subset X$ then from $\frac{1}{2\pi i}(\int_\gamma \omega)_{\omega\in F^1}$ one can construct an ideal I_γ such that $I(C) \subsetneq I_\gamma$.

In favorable circumstances we expect low order equations in I_γ to span $I(C)$.

For example, smooth rational curves of degree up to 4 in K3s.

Reconstructing isolated curves from their Hodge classes

Turns out one can compute a bit more for hypersurfaces

$$\varphi\colon H_2(X,\mathbb{Z}) \times H^2_{\mathrm{dR}}(X/k) \to \mathbb{C} \qquad (\gamma,\omega) \longmapsto \int_\gamma \omega$$

Note, if $\gamma \in \operatorname{Pic} X^{\mathrm{al}}$, then $\frac{1}{2\pi i}\int_\gamma \omega \in k^{\mathrm{al}}$ for $\omega \in F^1 H^2_{\mathrm{dR}}(X/k)$.

Theorem (Movasati–Sertöz)

If $\gamma = [C] \in H_2(X,\mathbb{Z})$ for a curve $C \subset X$ then from $\frac{1}{2\pi i}(\int_\gamma \omega)_{\omega\in F^1}$ one can construct an ideal I_γ such that $I(C) \subsetneq I_\gamma$.

In favorable circumstances we expect low order equations in I_γ to span $I(C)$.
For example, smooth rational curves of degree up to 4 in K3s.

Theorem (Cifani–Pirola–Schlesinger)

For a smooth rational quartic curve $C \subset X$ we have that the equation of the quadric surface containing C generates $I_{[C],2}$, i.e., $I(C)_2 = I_{[C],2}$.

Reconstructing quadric surfaces

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

$$\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

Reconstructing quadric surfaces

$$X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$$

$$\mathrm{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \mathrm{Pic}\, X^{\mathrm{al}}$$

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

- Fortunately, there is a small $\mathrm{Aut}(\Lambda)$ orbit of size 336 (Elkies).

Reconstructing quadric surfaces

$$X : x^4 + xyzw + y^3 z + yw^3 + z^3 w = 0 \subset \mathbb{P}^3$$

$$\mathrm{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \mathrm{Pic}\, X^{\mathrm{al}}$$

Goal

Reconstruct the quadric surfaces containing some of the 133056 smooth rational quartics in X using the curve classes.

- Fortunately, there is a small $\mathbf{Aut}(\Lambda)$ orbit of size 336 (Elkies).
- For each quartic curve $C \subset X$, we can compute

  $$I_{[C],2} = \langle a_0 x^2 + \cdots \sigma(a_9) w^2 \rangle_{\mathbb{C}}$$

  that defines a quadric surface Q, such that $Q \cap X = C \cup \overline{C}$.
  Hence, we expect an orbit of 168 quadrics each containing a pair of quartics.
- We aim reconstruct the ten (algebraic!) coefficients of these quadrics.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.
- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 10014013832542203812872613924739x^{161}$$
$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$
$$- 1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$
$$+ 23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313 \cdots$$

- Every computation must be done extremely selectively!

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- Considering all the embeddings, and clearing denominators when possible one can reconstruct each $\prod_\sigma (x - \sigma(a_i)) \in \mathbb{Q}[x]$ independently.
- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 1001401383254220381287261392 4739x^{161}$$

$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$

$$-1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$

$$+23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313\cdots$$

- Every computation must be done extremely selectively!
- We are presented with same 168 degree field L in 9 different ways.

Reconstructing quadric surfaces

Goal

Reconstruct the ten coefficients a_i of these quadrics in a Galois orbit of size 168.

- The minimal polynomials have large height about 9k characters, e.g.:

$$x^{168} - 1001401383254220381287261392 4739x^{161}$$
$$+ 171047690745503707515328576627906817785436888130925209472262244x^{154}$$
$$- 1268317331496745879603035032448157273146519836562713924560050631153969519297207668270922371313x^{147}$$
$$+ 23237703563539410755436556575134206593366430461423708193774287327245213403024087108979694756912313 \cdots$$

- Every computation must be done extremely selectively!
- We are presented with same 168 degree field L in 9 different ways.
  The abstract isomorphism problem feels hopeless. 

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \ldots, a_9) = \mathbb{Q}(a_0)$.

One approach is to compute the roots of the minimal polynomial of a_i in L.

In many situations, particularly if $\deg L \gg \deg \mathbb{Q}(a_k)$, it is wiser to factor the defining polynomial of L over $\mathbb{Q}(a_k)$. This is what `PARI/GP` does.

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \dots, a_9) = \mathbb{Q}(a_0)$.

One approach is to compute the roots of the minimal polynomial of a_i in L.

In many situations, particularly if $\deg L \gg \deg \mathbb{Q}(a_k)$, it is wiser to factor the defining polynomial of L over $\mathbb{Q}(a_k)$. This is what `PARI/GP` does.

In our case, we have all the compatible embeddings

$$\sigma_i : \mathbb{Q}(a_k) \hookrightarrow L \hookrightarrow \mathbb{C}$$

Thus the isomorphisms is given is the solution of the following linear system

$$\{\sigma_i(a_k)^j\}_{i,j} \cdot v = \{\sigma_i(a_0)\}_i, \qquad v \in \mathbb{Q}^{168}$$

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \ldots, a_9) = \mathbb{Q}(a_0)$.

One approach is to compute the roots of the minimal polynomial of a_i in L.

In many situations, particularly if $\deg L \gg \deg \mathbb{Q}(a_k)$, it is wiser to factor the defining polynomial of L over $\mathbb{Q}(a_k)$. This is what `PARI/GP` does.

In our case, we have all the compatible embeddings

$$\sigma_i : \mathbb{Q}(a_k) \hookrightarrow L \hookrightarrow \mathbb{C}$$

Thus the isomorphisms is given is the solution of the following linear system

$$\{\sigma_i(a_k)^j\}_{i,j} \cdot v = \{\sigma_i(a_0)\}_i, \qquad v \in \mathbb{Q}^{168}$$

This is numerically stable, as $\{\sigma_i(a_k)^j\}_{i,j}$ is a Vandermonde matrix.

The denominators of v are bounded.

Isomorphism problem

Goal

Construct $\mathbb{Q}(a_k) \hookrightarrow L$, where $L = \mathbb{Q}(a_0, \ldots, a_9) = \mathbb{Q}(a_0)$.

One approach is to compute the roots of the minimal polynomial of a_i in L.
In many situations, particularly if $\deg L \gg \deg \mathbb{Q}(a_k)$, it is wiser to factor the defining polynomial of L over $\mathbb{Q}(a_k)$. This is what `PARI/GP` does.

In our case, we have all the compatible embeddings

$$\sigma_i : \mathbb{Q}(a_k) \hookrightarrow L \hookrightarrow \mathbb{C}$$

Thus the isomorphisms is given is the solution of the following linear system

$$\{\sigma_i(a_k)^j\}_{i,j} \cdot v = \{\sigma_i(a_0)\}_i, \qquad v \in \mathbb{Q}^{168}$$

This is numerically stable, as $\{\sigma_i(a_k)^j\}_{i,j}$ is a Vandermonde matrix.
The denominators of v are bounded.
In practice, it is faster to iteratively refine the complex embeddings, as their height is smaller than theoretically possible: 4k vs 120k digits.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive! Linear algebra 😰

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive! Linear algebra 😰 Gröbner basis 😱

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!
  Linear algebra 😰 Gröbner basis 😱
  One needs to compute S by hand, and clear denominators before that.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!
  Linear algebra 😰 Gröbner basis 😱
  One needs to compute S by hand, and clear denominators before that.
- Working over $\mathbb{F}_p$ we find 10 distinct points.
  Hence, S is zero-dimensional and reduced, and $\deg S \leq 10$.

Intersecting the quadric surfaces with the K3 surface

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

Goal

Show that $Q \cap X$ decomposes into two quartic curves.

- It suffices to show that the singular locus S of $Q \cap X$ consists of 10 distinct reduced points.
- Hopeless to do this directly! Operations in L are seriously expensive!
  Linear algebra 😰 Gröbner basis 😱
  One needs to compute S by hand, and clear denominators before that.
- Working over $\mathbb{F}_p$ we find 10 distinct points.
  Hence, S is zero-dimensional and reduced, and $\deg S \leq 10$.
- We conclude $\deg S = 10$ via Gotzmann regularity theorem, by checking that $\dim L[x, y, z, w]_\bullet / I_\bullet = 10$ for $\bullet = 6, 7$, where $V(I) = S$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0 x^2 + a_1 xy + \cdots + a_9 w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X, \, \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0 x^2 + a_1 xy + \cdots + a_9 w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\, \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.
- Certify that these correspond to the original classes.
  Showing that there are at most 66528 distinct quadrics. Can be done over $\mathbb{C}$.
  This establishes a bijection between these quadric surfaces and the 168 pairs of quartic curve classes that they correspond to.

Certifying $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$

$$\Lambda_Q := \langle [C] : C \subset \sigma(Q) \cap X,\ \sigma : L \hookrightarrow \mathbb{C} \rangle \subseteq \operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$$

The inclusion $\Lambda_Q \subseteq \Lambda$ is not explicit!

Nonetheless, $\operatorname{Pic} X^{\mathrm{al}}$ and Λ are saturated in $H_2(X, \mathbb{Z})$.

Hence, it is sufficient to show that $\operatorname{rk} \Lambda_Q = \operatorname{rk} \Lambda = 19$.

We can do this in two ways:

- Compute the intersections of these 336 curves with each other over $\mathbb{F}_p$.
- Certify that these correspond to the original classes.
  Showing that there are at most 66528 distinct quadrics. Can be done over $\mathbb{C}$.
  This establishes a bijection between these quadric surfaces and the 168 pairs of quartic curve classes that they correspond to.

$$\operatorname{Pic} X^{\mathrm{al}} = \Lambda$$

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega\in F^1} \in K^{21}$.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega \in F^1} \in K^{21}$.

These can be reconstructed in the same fashion as we reconstructed a_i.

Unclear how to certify this step! What are the denominators of $\frac{1}{2\pi i}\int_C \omega$?

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

Via the identification with the original classes we have $\frac{1}{2\pi i}\left(\int_C \omega\right)_{\omega \in F^1} \in K^{21}$.

These can be reconstructed in the same fashion as we reconstructed a_i.

Unclear how to certify this step! What are the denominators of $\frac{1}{2\pi i}\int_C \omega$?

Can one compute K using geometry without Gröbner basis?

To try: For a generic hyperplane $Q \cap X \cap H$ is a degree 8 reduced scheme.
The number field K is the quadratic extension where we observe two orbits.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

The direct computation of $\mathrm{Gal}(K/\mathbb{Q})$ looks hopeless.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

The direct computation of $\mathrm{Gal}(K/\mathbb{Q})$ looks hopeless.

We guess that $K = F(\sqrt[14]{u})$ for a unit u of where F is defined by

$$\begin{aligned} x^{24} &+ x^{22} - 24x^{21} - 84x^{20} - 205x^{19} - 155x^{18} - 770x^{17} - 500x^{16} + 18916x^{15} \\ &+ 36988x^{14} + 109234x^{13} + 387901x^{12} + 373961x^{11} - 18170x^{10} + 75132x^{9} + 10381x^{8} \\ &- 123071x^{7} + 108274x^{6} - 41580x^{5} + 39936x^{4} - 21911x^{3} + 4032x^{2} + 1428x + 616 \end{aligned}$$

and $\mathrm{Gal}(F/\mathbb{Q}) = C_3 \times \mathrm{PGL}(2,7)$. $\#\,\mathrm{Gal}(F/\mathbb{Q})$ is 14 times smaller than $\#\,\mathrm{Aut}\,\mathrm{Pic}\,X^{\mathrm{al}}$.

Computing the Galois action

$$Q : a_0x^2 + a_1xy + \cdots + a_9w^2 = 0 \subset \mathbb{P}^3, \quad [L := \mathbb{Q}(\{a_i\}_i) : \mathbb{Q}] = 168$$

$Q \cap X$ decomposes into a pair of quartics over K a quadratic extension of L.

Goal

Compute K and $\mathrm{Gal}(K/\mathbb{Q})$ acting on Λ_Q.

The direct computation of $\mathrm{Gal}(K/\mathbb{Q})$ looks hopeless.

We guess that $K = F(\sqrt[14]{u})$ for a unit u of where F is defined by

$$\begin{aligned} x^{24} &+ x^{22} - 24x^{21} - 84x^{20} - 205x^{19} - 155x^{18} - 770x^{17} - 500x^{16} + 18916x^{15} \\ &+ 36988x^{14} + 109234x^{13} + 387901x^{12} + 373961x^{11} - 18170x^{10} + 75132x^{9} + 10381x^{8} \\ &- 123071x^{7} + 108274x^{6} - 41580x^{5} + 39936x^{4} - 21911x^{3} + 4032x^{2} + 1428x + 616 \end{aligned}$$

and $\mathrm{Gal}(F/\mathbb{Q}) = C_3 \times \mathrm{PGL}(2,7)$. $\#\,\mathrm{Gal}(F/\mathbb{Q})$ is 14 times smaller than $\#\,\mathrm{Aut}\,\mathrm{Pic}\,X^{\mathrm{al}}$. Can we compute $\mathrm{Gal}(K/\mathbb{Q})$? $\mathrm{Gal}(K/\mathbb{Q}) \stackrel{?}{=} \mathrm{Aut}\,\Lambda$? $H^1(\mathrm{Gal}(k^{\mathrm{al}}/k), \mathrm{Pic}\,X^{\mathrm{al}}) =?$

Summary

Theorem (C–Sertöz)

The quartic surface $X : x^4 + xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3$ has $\operatorname{Pic} X^{\mathrm{al}} = \Lambda$, generated by quartics over a quadratic extension of $L := \mathbb{Q}(\{a_i\}_i)$.

We are hoping to streamline this method and also figure out its applications/limitations.

Hopefully, also be able handle families, e.g.,

$$X : x^4 + \lambda xyzw + y^3z + yw^3 + z^3w = 0 \subset \mathbb{P}^3(\mathbb{Q}(\lambda))$$

Do you have a challenge K3 surface for us?