Effective Computation of Hodge Cycles

Edgar Costa (MIT)

August 27, 2024, Simons Symposium on Geometry of Non-Closed Fields

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

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

determines the k-isogeny class and the isomorphism class of $\operatorname{End}(A) \otimes \mathbb{Q}$.

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 $\mathbf{End}\, A$ and their equations in $A \times A$.

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

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

  determines the k-isogeny class and the isomorphism class of $\mathrm{End}(A) \otimes \mathbb{Q}$.
- 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 $\mathrm{End}\, J^{\mathrm{al}}$.

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 $\mathbf{End}\, J^{\mathrm{al}}$.

But why?

- It is an interesting challenge [*citation needed*].
- If $\mathbf{End}\, J$ contains non-trivial idempotents, we can hope to decompose J into abelian varieties of smaller dimension.
- If $\mathbf{End}\, J$ is non-trivial, then this allows us to find a modular form that describes the arithmetic properties of J and C.
- An algorithm to decide transcendence of 1-periods using Huber–Wüstholz theory (Ouaknine–Worrell–Sertöz)

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$, 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.
- Using Λ, we can hope to understand J analytically...

An analytic description of the Jacobian

Via a chosen embedding of k into $\mathbb{C}$, 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.
- 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

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

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.

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

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.

Representing endomorphisms

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

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

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

Theorem (C–Mascot–Sijsling–Voight)

We give an algorithm for

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

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–Voigt, C–Lombardo–Voigt, C–Sertöz)

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

This is a day/night algorithm:

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

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 $B \subseteq \operatorname{End} J^{\mathrm{al}}$.

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

- 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 $\operatorname{End} J^{\mathrm{al}} \subseteq B$.

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

  - 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

$$\begin{aligned} C : x^4 - x^3y + 2x^3z + 2x^2yz + 2x^2z^2 - 2xy^2z + 4xyz^2 \\ - y^3z + 3y^2z^2 + 2yz^3 + z^4 = 0 \end{aligned}$$

  has complex multiplication.
- Try it:

  https://github.com/edgarcosta/endomorphisms

  contains friendly button-push algorithms.

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

Given X compute $\operatorname{Pic} X^{\mathrm{al}}$.

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

Given X compute $\operatorname{Pic} X^{\mathrm{al}}$.

- Over finite field, Tate conjecture tells us that $\det(1 - t \operatorname{Frob} | H^2(X, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$ gives us the rank of $\operatorname{Pic} X$.

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.

- Over finite field, Tate conjecture tells us that $\det(1 - t\,\mathrm{Frob}|H^2(X, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$ gives us the rank of $\operatorname{Pic} X$.
- There are several in principle algorithms to compute $\operatorname{rk} \operatorname{Pic} X$ or even $\operatorname{Pic} X$ over a number field.
  These involve, a day/night algorithm:
  - by day: find curve classes in $\operatorname{Pic} X$;
  - by night: restrict the ambient space for $\operatorname{Pic} X \subset H^2(X, \mathbb{Z})$.

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

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 Π is the period vector for ω_X, i.e., $[\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})}$, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in \mathbb{Z}^{22}.$$

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 Π is the period vector for ω_X, i.e., $[\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})}$, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in \mathbb{Z}^{22}.$$

- Π can be computed via deformation for projective hypersurfaces (Sertöz).
- Heuristically, via lattice reduction algorithms, we can find Λ.
- 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 Π is the period vector for ω_X, i.e., $[\int_\gamma \omega_X]_{\gamma \in H_2(X,\mathbb{Z})}$, then we are reduced to finding a lattice $\Lambda \subset H_2(X, \mathbb{Z})$ of solutions

$$\Pi R = 0, \qquad R \in \mathbb{Z}^{22}.$$

- Π can be computed via deformation for projective hypersurfaces (Sertöz).
- Heuristically, via lattice reduction algorithms, we can find Λ.
- There is no obvious way to prove that our guesses are actually correct...
- Nonetheless, a posteriori, one can compute $B \gg 0$ 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 and 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 and matching upper bounds can be deduced by positive characteristic methods.
- 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 and matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes Λ such that $\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$.
- We can compute $\operatorname{Aut} \Lambda$, the isomorphism class seems to be $F_7 \times \mathrm{PGL}(2, 7)$.

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 and matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes Λ such that $\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$.
- 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 and matching upper bounds can be deduced by positive characteristic methods.
- No known explicit descriptions of $\operatorname{Pic} X^{\mathrm{al}}$.
- Heuristically, one computes Λ such that $\operatorname{Pic}(X^{\mathrm{al}})_{|B} \subseteq \Lambda \overset{?}{\subseteq} \operatorname{Pic} X^{\mathrm{al}}$.
- 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 $\gamma = [Y] \in H_2(X,\mathbb{Z})$ for a curve $Y \subset X$ then from $\frac{1}{2\pi i}(\int_\gamma \omega)_{\omega \in F^1}$ one can construct an ideal I_γ such that $I(Y) \subsetneq I_\gamma$.

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

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

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

Theorem (Cifani–Pirola–Schlesinger)

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

Reconstructing quadric equations

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

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

Goal

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

Reconstructing quadric equations

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

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

Goal

Reconstruct the quadrics 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.

Reconstructing quadric equations

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

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

Goal

Reconstruct the quadrics 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.
- 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 equations

Goal

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

- Considering all the embeddings and by clearing denominators when possible, one can reconstruct each coefficient independently.

Reconstructing quadric equations

Goal

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

- Considering all the embeddings and by clearing denominators when possible, one can reconstruct each coefficient independently.
- The minimal polynomials of these elements have incredibly large height.

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

- Every computation must be done very selectively.

Reconstructing quadric equations

Goal

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

- Considering all the embeddings and by clearing denominators when possible, one can reconstruct each coefficient independently.
- The minimal polynomials of these elements have incredibly large height.

$$x^{168} - 1001401383254220381287261392473 9x^{161} + 1710476907455037075153285766279068177854368881309252094722622 44x^{154}$$
$$- 12683173314967458796030350324481572731465198365627139245600506311539695192972076682709223713 13x^{147} + \cdots$$

- Every computation must be done very selectively.
- We solve the isomorphism problem between the different presentations by refining the complex embeddings and inverting a Vandermonde matrix. The abstract isomorphism problem feels hopeless otherwise.

Intersecting the quadric with X

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

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 with X

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

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!
- 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 with X

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

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

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

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

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

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

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

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

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

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

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 quadrics and the 168 pairs of quartic curve classes that they correspond to.

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 such heuristic guesses!

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 such heuristic guesses!

Even if given the order $\mathcal{O} \subset K$ over which the quartics are defined over, no obvious control over denominators of $\frac{1}{2\pi i}\int_C \omega$.

Can one compute K using geometry without Gröbner basis?

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

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

and $\mathrm{Gal}(F/\mathbb{Q}) = C_3 \times \mathrm{PGL}(2,7)$ (with size 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

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

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

Do we have $\mathrm{Gal}(K/\mathbb{Q}) \stackrel{?}{=} \mathrm{Aut}\,\Lambda$? Can we compute $\mathrm{Gal}(K/\mathbb{Q})$ by hand?

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.

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

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

Do you have a challenge K3 surface for us?