New results on curves of genus 4 (updated slides, including new results)

Everett W. Howe

Center for Communications Research, La Jolla

Arithmetic, Geometry, and Coding Theory
Luminy, 14 March 2011

Motivation

Curves with many points

- Used in coding theory...
- ... but also a source of interesting math problems.
- $N_q(g) =$ max. number of points on a genus-g curve $/\mathbb{F}_q$

manypoints.org

- Gathers best known results on $N_q(g)$ for small q and g
- Lower bounds from: Class field theory, fiber products, special curves, guided searches, ...
- Upper bounds from: Weil-Serre bound, Oesterlé bound, analysis of isogeny classes, ...

Curves of small genus

Know $N_q(1)$ and $N_q(2)$ for all q

In fact, know exactly which polynomials occur as characteristic polynomials of Frobenius. . .

- for elliptic curves (Deuring/Waterhouse);
- for genus-2 curves (H.-Nart-Ritzenthaler).

Know $N_q(3)$ for all q in manypoints table

Values filled in by Serre, Auer-Top, Top, others.

But there are 23 values of $q < 100$ for which $N_q(4)$ is unknown. (As of February 2011.)

This talk

1. Improve upper and lower bounds for $N_q(4)$ for $q < 100$

- Zaytsev's results on Jacobians isomorphic to E^g
- Double covers of elliptic curves
- Double covers of genus-2 curves
- Hermitian forms over non-maximal quadratic orders
- Hermitian forms over $\mathbb{Z}[\zeta_5]$

2. Genus-4 curves with isomorphic Jacobians

- Idea suggested by examples of curves with many points
- First explicit examples
- Can show: One can find arbitrarily many genus-4 curves sharing same (unpolarized) Jacobian.

Part 1: Improving bounds on $N_q(4)$

Zaytsev's work

Consider a curve $C/\mathbb{F}_q$ with...

- Jac $C \cong E^g$, with g not too big
- End E a maximal order $\mathcal{O}$ of class number 1
- E ordinary

Schiemann: Calculated unimodular Hermitian forms on $\mathcal{O}^g$.

Zaytsev: Deduces existence of automorphisms of C, uses these to obtain contradictions.

Genus 4 Weil-Serre bound not reached for these $q < 100$

new: 11, 17, 23, 37, 47, 59, 61, 83
previously eliminated: 8, 13, 31, 32, 43, 73

Real Weil polynomials

$C =$ a genus-g curve over $\mathbb{F}_q$
$f =$ the characteristic polynomial of Frobenius for C
a.k.a. the *Weil polynomial* of C

The real Weil polynomial

We can write

$$f(x) = x^g\, h(x + q/x)$$

for a polynomial h of degree g, the *real Weil polynomial* of C.

All complex roots of h are real, in interval $[-2\sqrt{q}, 2\sqrt{q}]$.

h^2 is characteristic polynomial of Frobenius $+$ Verschiebung.

Producing possible real Weil polynomials

IsogenyClasses.magma

- Magma package, from H.-Lauter papers
- Given q, g, N, produces list of polynomials that includes the real Weil polynomials of all genus-g curves over $\mathbb{F}_q$ with N points
- For each polynomial, can sometimes deduce properties of curves with that real Weil polynomial (if any exist)
- Example: Sometimes deduce that C must be a double cover of an elliptic curve E in a known isogeny class

Genus-4 double covers of elliptic curves

Given E over $\mathbb{F}_q$ with q odd.

Normal forms for genus-4 double covers of E

Take equation for E, together with $z^2 = f$, where

- f is a function on E,
- $\operatorname{div} f = P_1 + \cdots + P_6 + 2Q - 8\infty$,
- Q taken from representatives of $E(\mathbb{F}_q)/3E(\mathbb{F}_q)$ modulo automorphisms of E.
- (Need only look at set of f's modulo squares in $\mathbb{F}_q^*$.)

Example: $q = 31$

Weil-Serre bound is 76. Older methods: $N_{31}(4) \leq 73$.

For $N = 73$, IsogenyClasses.magma says:

- Only one possible polynomial: $(x + 8)(x + 11)^3$.
- Using techniques of H.-Lauter: Must be a double cover of an elliptic curve with real Weil polynomial $x + 11$.

$$y^2 = x^3 + 3, \quad z^2 = c_6x^3 + c_5xy + c_4x^2 + c_3y + c_2x + c_1$$

Enumerate these covers

No curves with 73 points. But some have 72. So $N_{31}(4) = 72$.

Example: $y^2 = x^3 + 3, \quad z^2 = 3x^3 - 9$

Other possible deductions from real Weil polynomial

Things one might deduce:

- Curve must be a double cover of a genus-2 curve.
  - Enumeration will determine whether curve exists.
- Curve *cannot* be a double-cover of a genus-2 curve.
  - . . . so don't bother enumerating them!
- Sometimes, can deduce neither.
  - It can't hurt to look. . .

Genus-4 double covers of genus-2 curves

Let X be a genus-2 curve over $\mathbb{F}_q$, with q odd.

Normal form for genus-4 double covers of X

Take equation for X, together with $z^2 = f$, where

- f is a function on X with $\operatorname{div} f = P_1 + P_2 + 2D - 6\infty$,
- D effective, degree 2.

To enumerate double covers:

- Loop over D.
- Loop over f in Riemann-Roch space $L(6\infty - 2D)$.
- Count points on $z^2 = f$.
- (Need only look at f up to squares in $\mathbb{F}_q^*$.)

Example: $q = 47$

Zaytsev eliminates $N = 100$ (Weil-Serre bound).
Older techniques eliminate $N = 99$.

For $N = 98$, IsogenyClasses.magma says:

- Two possible polynomials:
  $(x + 11)(x + 13)^3$ and $(x^2 + 25x + 155)^2$.
- First: Must be double cover of $x + 11$, eliminate by search.
- Second: Maybe a double cover of $x^2 + 25x + 155$?
- Unique genus-2 curve to consider.

Find example!

$$y^2 = x^5 + 5x^3 + 12x^2 + 37x + 32$$
$$5z^2 = y + 11x^3 + 46x^2 + 42x + 27$$

So $N_{47}(4) = 98$.

Hermitian forms over quadratic orders

Suppose $\psi : E^4 \to \mathrm{Jac}\, C$ is isogeny of degree n, where End E is an order $\mathcal{O}$ in quadratic field.

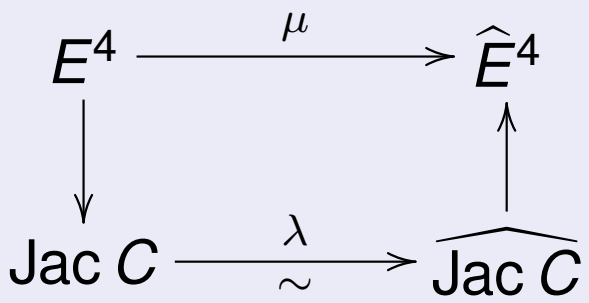
Pull back polarization to E

- Pull back principal polarization λ on Jac C to get μ on E^4.
- Degree of μ is $(\deg \psi)^2$.
- View μ as Hermitian form on $\mathcal{O}^4$.
- Suppose $\gamma = (\alpha_1, \ldots, \alpha_4) \in \mathcal{O}^4$ has squared-length m.
- Consider map $\Gamma : E \to E^4$ determined by γ.
- $\Gamma^* \mu$ is m times the canonical polarization on E.

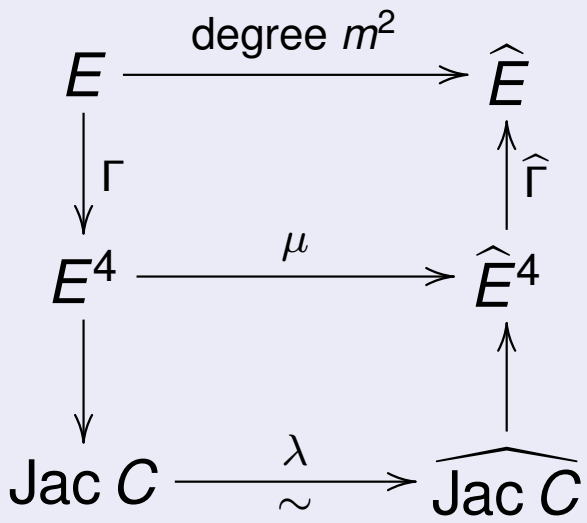
Getting a degree-m map $C \to E$ from a diagram

$$\operatorname{Jac} C \xrightarrow[\sim]{\lambda} \widehat{\operatorname{Jac} C}$$

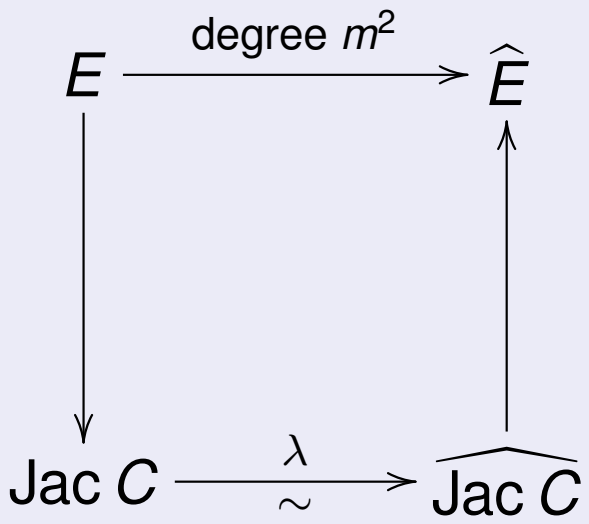
Getting a degree-m map $C \to E$ from a diagram



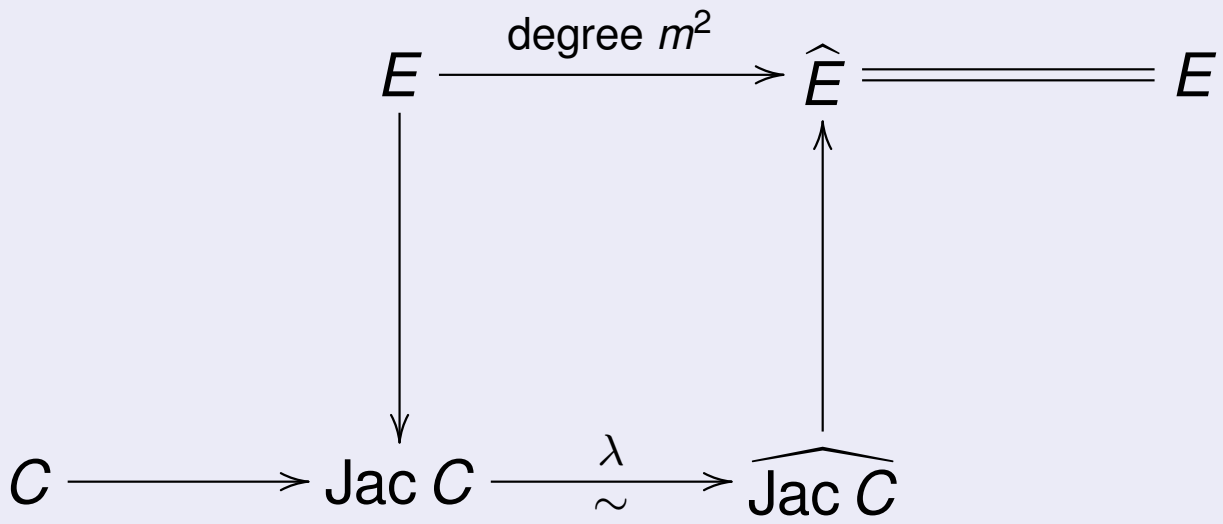
Getting a degree-m map $C \to E$ from a diagram



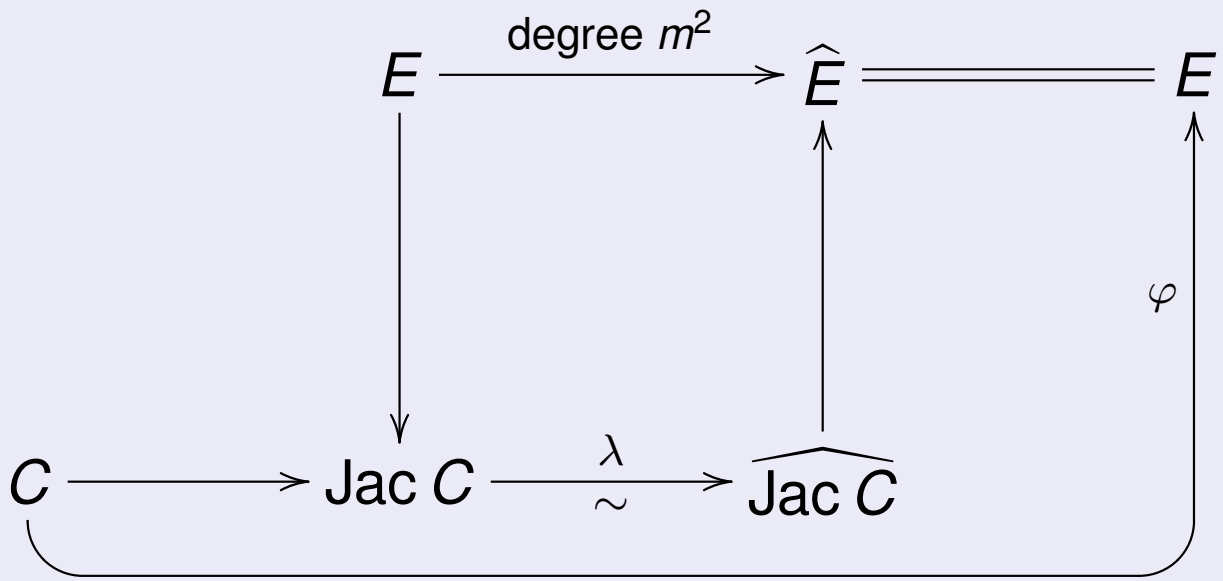
Getting a degree-m map $C \to E$ from a diagram



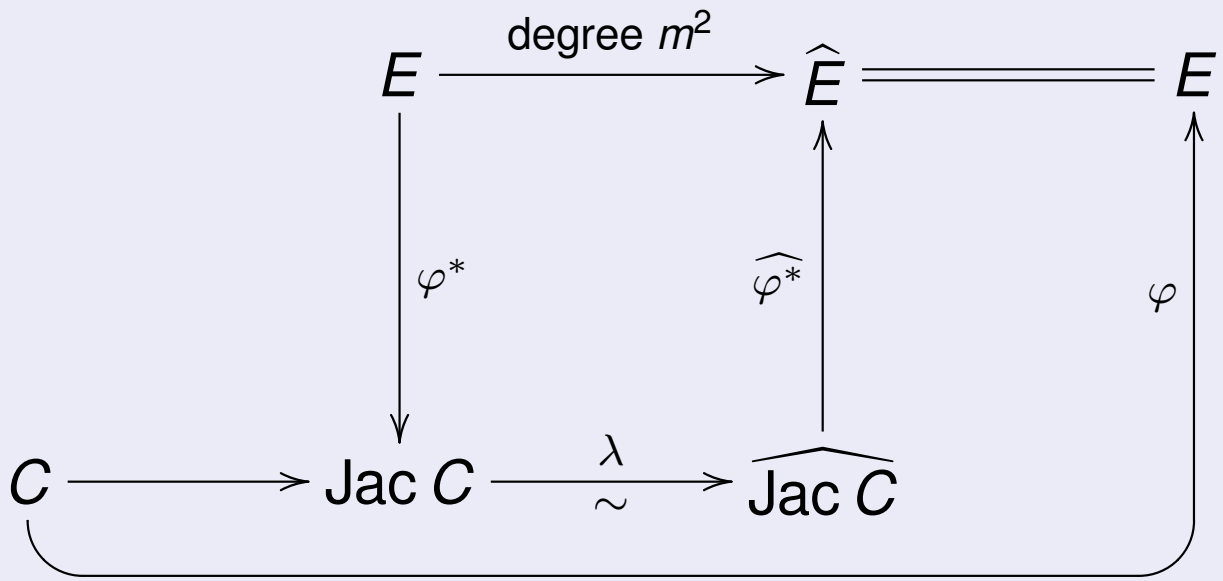
Getting a degree-m map $C \to E$ from a diagram



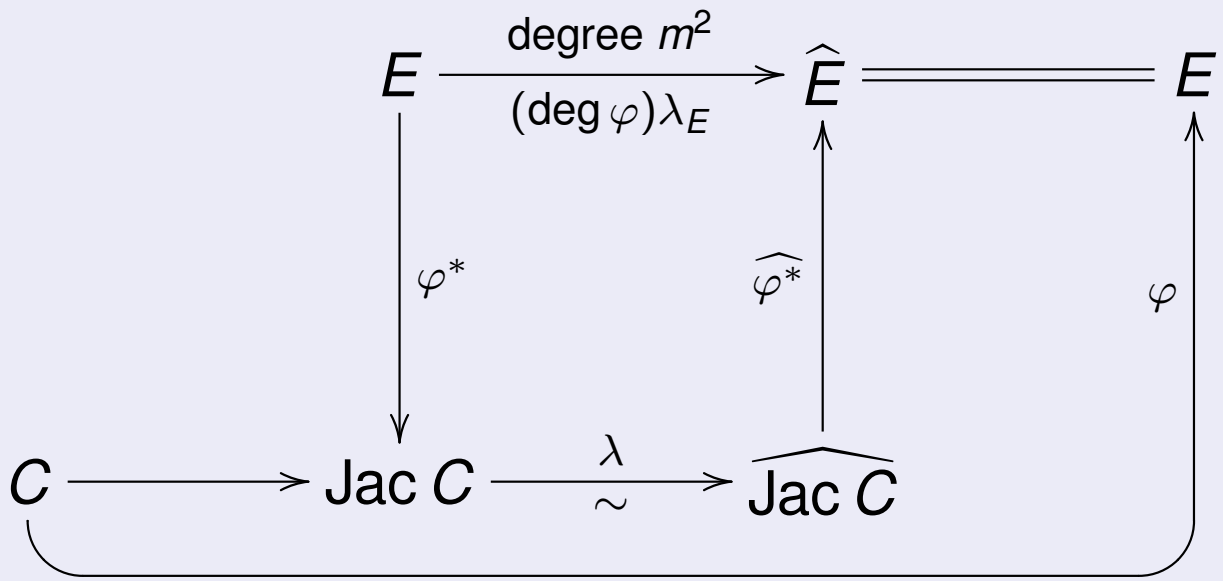
Getting a degree-m map $C \to E$ from a diagram



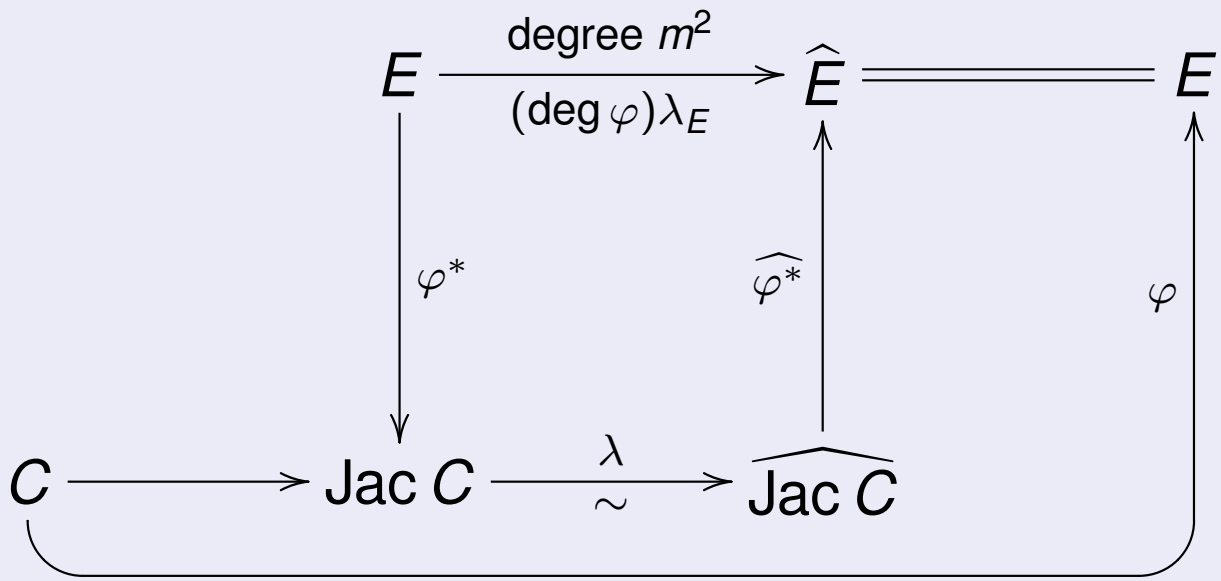
Getting a degree-m map $C \to E$ from a diagram



Getting a degree-m map $C \to E$ from a diagram



Getting a degree-m map $C \to E$ from a diagram



So $\deg \varphi = m$.

We would like bounds on the length of the shortest vector in a Hermitian lattice with a given Gram determinant.

Bounds on short vectors

Suppose $\operatorname{disc} \mathcal{O} = \Delta$ and we want to enumerate Hermitian forms on $\mathcal{O}^4$ with Gram determinant D.

If D and Δ are small:

- Can enumerate directly.
- Each form has a sublattice given by Hermitian matrix with
  - product of diagonal elements bounded by $D\Delta^2$
  - non-diagonals bounded by positive definiteness
- Can be quite slow.

If $\mathcal{O}$ maximal and a PID, and D is a norm from $\mathcal{O}$:

Build forms from unimodular forms, listed by Schiemann.
This is *much* more efficient.

Example: Weil-Serre bound for $q = 19$.

Only real Weil polynomial for C is $(x + 8)^4$.

Two elliptic curves with real Weil polynomial $x + 8$:

- E with CM by $\mathcal{O} = \mathbb{Z}[(1 + \sqrt{-3})/2]$,
- F with CM by $\mathbb{Z}[\sqrt{-3}]$.

- Jac C is one of E^4, $E^3 \times F$, $E^2 \times F^2$, $E \times F^3$, F^4.
- Pull back polarization to E^4.
- Hermitian form on $\mathcal{O}^4$ with Gram determinant 1, 2, 4, 8, 16.
- Short vectors of length at most 1, 1, 2, 2, 3.

So: Double cover of E unless Jac $C \cong F^4$.

Eliminating final case

We have a problem if principal polarization on F^4 pulls back to polarization of degree 16^2 on E^4 with short vector of length 3.

Enumerate Hermitian matrices in $M_4(\mathcal{O})$ of determinant 16.

Look at those with short vector of length 3.

Verify that none of these gives polarization with kernel containing a maximal isotropic subgroup G with $E^4/G \cong F^4$.

Results

No curve attaining Weil-Serre bound for $q = 19$ and $q = 67$.

Other nonmaximal quadratic orders

Can make similar arguments for $\Delta = -16$ and $\Delta = -28$.

Results

No curve attaining Weil-Serre bound for $q \in \{23, 53, 71\}$.

Hermitian forms over $\mathbb{Z}[\zeta_5]$

Zaytsev and other methods show $N_{11}(4) \leq 34$.
$N = 34$: Only possible polynomial is $(x^2 + 11x + 29)^2$.

Observations/deductions

- Jac C is isogenous to A^2 for some abelian surface A.
- From Weil polynomial, determine that End $A = \mathbb{Z}[\zeta_5]$.
- $\mathbb{Z}[\zeta_5]$ is PID, so A unique in isogeny class, and Jac $C \cong A^2$.
- Polarizations on $A^2 \longleftrightarrow$ rank-2 unimodular Hermitian forms over $\mathbb{Z}[\zeta_5]$
- Strong form of Euclidean algorithm on $\mathbb{Z}[\zeta_5]$ gives reduction theory on Hermitian forms.
- Only unimodular Hermitian form is trivial one.
- No polarization on A^2 gives a Jacobian.

Results from Hermitian forms over $\mathbb{Z}[\zeta_5]$

$q = 11$

- Hermitian forms over $\mathbb{Z}[\zeta_5]$ show: $N_{11}(4) < 34$.
- Find a double cover of genus-2 curve with $N = 33$.
- So $N_{11}(4) = 33$.

$q = 61$

- If $N = 120$, IsogenyClasses.magma gives two polynomials: $(x + 13)(x + 15)^3$ and $(x^2 + 29x + 209)^2$.
- First: Double cover of an elliptic curve. Eliminated.
- Second: Once again Jac $C \cong A^2$ with End $A = \mathbb{Z}[\zeta_5]$.
- Hermitian forms over $\mathbb{Z}[\zeta_5]$ show: $N_{61}(4) < 120$.
- Find many double covers of elliptic curves with $N = 118$.
- So $118 \leq N_{61}(4) \leq 119$.

Final results

q	old	new
2	8	8
3	12	12
4	15	15
5	18	18
7	24	24
8	25	25
9	30	30
11	−34	33
13	−39	38
16	45	45
17	−48	46
19	−52	48 − 50

q	old	new
23	−58	57
25	66	66
27	64	64
29	−70	67 − 68
31	−73	72
32	71 − 72	71 − 72
37	−84	82
41	−90	88
43	−93	92
47	−98	98
49	−106	102 − 106
53	−110	108

q	old	new
59	−118	116
61	−120	118 − 119
64	129	129
67	−132	129
71	132 − 136	134
73	−139	138
79	−148	148
81	154	154
83	−154	152
89	−162	160 − 162
97	−174	174

Table: Old and new ranges for $N_q(4)$, for $q < 100$.

(The old ranges include Zaytsev's improvements.)

The manypoints.org tables will be updated when I finish double-checking the values that rely on computer searches.

Part 2: Curves of genus 4 with isomorphic Jacobians

Curves with isomorphic Jacobians

Question

Can an abelian variety A have two non-isomorphic principal polarizations λ_1 and λ_2, with (A, λ_1) and (A, λ_2) Jacobians?

More generally: How many curves C can have $\mathrm{Jac}\, C \cong A$?

Today, let's restrict attention to the complex numbers $\mathbb{C}$.

History: Genus 2

- Humbert (1900): There are simple A with two principal polarizations. (And simple polarized surfaces are Jacobians.)
- Hayashida-Nishi (1965): If E has CM, E^2 can have many non-isomorphic polarizations coming from curves.
- Explicit equations: For non-simple Jacobians, H. (1995). For simple Jacobians, defined over $\mathbb{Q}$, H. (2005).

History: Genus 3

- Generalize Humbert and Hayashida-Nishi. Use fact that principally polarized threefolds are (usually) Jacobians.
- Explicit non-simple examples over $\mathbb{C}$: H. (2000).
- Explicit non-simple examples over $\mathbb{Q}$: H. (2005).

History: Genus 4

Much more difficult: A principally polarized abelian fourfold is usually *not* a Jacobian.

Ciliberto-van der Geer (1994):

- Showed there are simple A that are Jacobians in two ways.
- Used A with real multiplication.
- Argument shows that a certain moduli space has positive dimension.
- Does not provide explicit examples.

Today: Will give explicit non-simple examples.

A family of genus-4 curves

For every t define a genus-4 curve

$$D_t: \quad y^3 = 2x(x^2 - 2t + 2)(x^2 - 2t - 2).$$

Let $\Delta < 0$ be fundamental discriminant divisible by 24,

$$H = \text{Hilbert class polynomial of } \Delta$$

$$g(x) = \text{numerator of } H\left(2^4 3^3 \frac{(4x-5)^3}{(x-1)(x+1)^3}\right)$$

$$f(x) = \gcd(g(x), g(-x))$$

Theorem

If s and t are distinct positive real roots of f, then D_s and D_t are non-isomorphic, and yet have isomorphic Jacobians.

A family of genus-4 curves

If s and t are distinct positive real roots of f, then D_s and D_t are non-isomorphic, and yet have isomorphic Jacobians.

Number of examples

Number of positive real roots is half the size of the 2-torsion subgroup of the class group of Δ.

Example

With $\Delta = -120$, can take

$$s = \frac{\sqrt{1235 + 70\sqrt{10}}}{27} \qquad t = \frac{\sqrt{1235 - 70\sqrt{10}}}{27}$$

Fields of definition

I think the theorem remains true over any field that contains all of the roots of $z^3 + 1/z^3 + 2s = 0$ and $z^3 + 1/z^3 + 2t = 0$.

Where does this theorem come from?

We get the curves D_t as double covers of genus-2 curves C_t with automorphisms of order 3.

Genus-2 curves with automorphisms of order 3

Suppose C is a genus-2 curve with order-3 automorphism

- Can write C as $C_t : y^2 = x^6 + tx^3 + 1$.
- Extra involution: $(x, y) \mapsto (1/x, y/x^3)$.
- Get map from C to elliptic curve, so Jacobian is not simple.

Decomposition of Jacobian

- Given a 3-isogeny $\varphi : E \to E'$, let $A = E \times E'$.
- Take $\lambda = \begin{bmatrix} 2 & \widehat{\varphi} \\ \varphi & 2 \end{bmatrix}$, $\alpha = \begin{bmatrix} -2 & \widehat{\varphi} \\ -\varphi & 1 \end{bmatrix}$.
- α is automorphism of (A, λ), and $\alpha^2 + \alpha + 1 = 0$.
- All order-3 automorphism of PPAS's arise in this way.
- Jac $C_t = E_t \times E'_t$.

Genus-2 curves with isomorphic Jacobians

- Let K be a quadratic field in which 3 is not inert.
- Let $\mathcal{O}$ be the maximal order of K.
- Let $\mathfrak{P}$ be a prime of $\mathcal{O}$ over 3.
- For every ideal $\mathfrak{A}$, the elliptic curves given by the lattices $\mathfrak{A}$ and $\mathfrak{AP}$ in $\mathbb{C}$ are 3-isogenous.

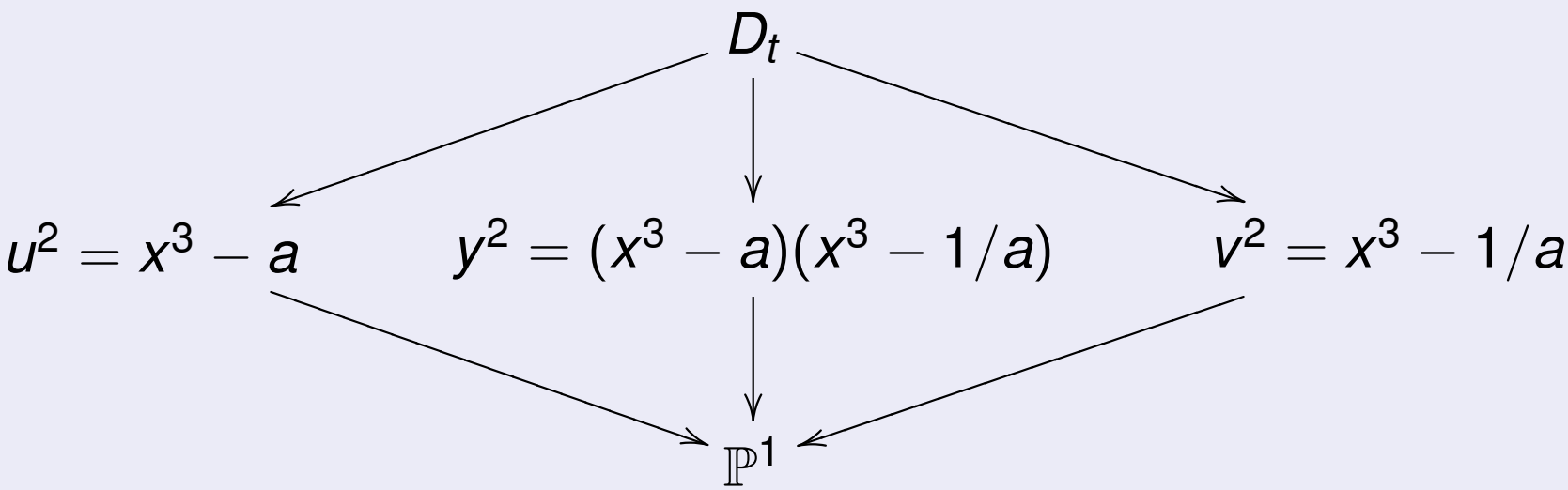
Finding s and t with Jac $C_s =$ Jac C_t

- Choose s that gives isogeny $\mathbb{C}/\mathfrak{A} \to \mathbb{C}/(\mathfrak{AP})$.
- Choose t that gives isogeny $\mathbb{C}/\mathfrak{B} \to \mathbb{C}/(\mathfrak{BP})$.
- If $\mathfrak{A}^2 = \mathfrak{B}^2$ in class group, then $E_s \times E_s' \cong E_t \times E_t'$.

Double covers of C_t

Write $x^6 + tx^3 + 1 = (x^3 - a)(x^3 - 1/a)$.

Kummer extension:



Left and right hand curves are elliptic curves with $j = 0$.

Kani-Rosen

$\operatorname{Jac} D_t \sim \operatorname{Jac} C_t \times E_0^2 = E_t \times E_t' \times E_0 \times E_0$.

Not hard to determine the kernel of $E_t \times E_t' \times E_0 \times E_0 \to \operatorname{Jac} D_t$.

Bootstrapping

So if C_s and C_t have isomorphic Jacobians, then D_s and D_t have isogenous Jacobians.

By keeping track of kernels of isogenies, can determine when Jac D_s and Jac D_t are isomorphic.

Source of construction

Several curves found in searches for curves with many points had this form. Analyzing their Jacobians led to this construction.

Have tried to make variants of this construction to get higher-genus examples. No success yet.