Optimal curves of genus 1, 2 and 3

Christophe Ritzenthaler

Institut de Mathématiques de Luminy, CNRS

Leuven, 17-21 May 2010

1. General facts
   - Definitions
   - Bounds

2. Optimal curves of genus $1, 2$ and 3
   - Existence of the isogeny class
   - Existence of an indecomposable principal polarization
   - Serre's obstruction
   - The case $g = 2$

3. Different strategies for $g = 3$
   - Quotients by isogeny
   - Serre's strategy
   - Algebraic interpretation
   - The geometric approach

Maximal curves

- $k = \mathbb{F}_q = \mathbb{F}_{p^n}$ a finite field. K any perfect field;
- C/K a (smooth, projective, absolutely irreducible) curve of genus g over K;
- $N_q(g)$: maximal number of points on a genus g curve over $\mathbb{F}_q$.
- A curve C of genus g over k is maximal if $\#C(k) = N_q(g)$.

Two main directions of research:

- when g is big compared to $q \rightsquigarrow$ asymptotical properties, modular or recursive towers;
- when g is small compared to $q \rightsquigarrow$ tight relationships between the curve and its Jacobian, explicit constructions, massive computations, tricks.

How does the situation look like ?

`www.manypoints.org`

Some bounds

Weil polynomial of C: $\chi_C = \prod_{i=1}^{g}(X^2 + x_i X + q) \in \mathbb{Z}[X]$ with $x_i \in \mathbb{R}$ such that $|x_i| \leq 2\sqrt{q}$.

• $\#C(\mathbb{F}_q) = q + 1 + \sum x_i$.

$\rightarrow N_q(g) \leq 1 + q + \lfloor 2g\sqrt{q} \rfloor$ (Hasse-Weil bound).

Let $m = \lfloor 2\sqrt{q} \rfloor$. Arithmetic-geometric means inequality:

$$\frac{1}{g}\sum(m + 1 - x_i) \geq \left(\prod(m + 1 - x_i)\right)^{1/g} \geq 1$$

$\rightarrow N_q(g) \leq 1 + q + gm$ (Hasse-Serre-Weil bound).

• If $g > (q - \sqrt{q})/2$, the bound can be improved (Oesterlé-Serre-Weil bound) using the fact that the number of places of each degree on a curve is non-negative.

$$\limsup_{g\to\infty} N_q(g)/g \leq \sqrt{q} - 1, \text{ with equality when } q \text{ is a square.}$$

Optimal curves

Definition

A curve is optimal if $\#C(k) = 1 + q + gm$.

Equality in the arithmetic-geometric means inequality $\Rightarrow$ all the $x_i = m$ and so

$$\chi_C = (X^2 + mX + q)^g.$$

Remark: If $p \nmid m$ then $\operatorname{Jac} C \sim E^g$ with E an elliptic curve of trace $-m$. But one can find a simple abelian variety of dimension 9 over $\mathbb{F}_{5^9}$ with this Weil polynomial.

Optimal curves of genus 1, 2 and 3

If C is an optimal curve of genus $1 \leq g \leq 3$ then $\mathrm{Jac}\, C \sim E^g$ with E an elliptic curve of trace $-m$.

• Existence of the isogeny class (Deuring 1941): explained by Honda-Tate theory.

Proposition

There does not exist an elliptic curve with trace $-m$ if and only if $n \geq 3$, n is odd and $p|m$.

$\rightarrow$ This solves the question for optimal genus 1 curves.

The abelian variety $\mathrm{Jac}(C)$ is equipped with an absolutely indecomposable principal polarization.

• Existence of an absolutely indecomposable principal polarization in the class E^g.
This question mainly translates into existence of positive definite indecomposable (quaternion) hermitian forms on $\mathrm{End}(E)$-modules.

- $g = 2$ (Hayashida, Nishi 1965, Serre 1983): no if and only if $q = 4, 9$ or
$$m^2 - 4q \in \{-3, -4, -7\}.$$

- $g = 3$ (Ibukiyama 1993, Lauter, Serre 2002, Nart, R. 2008): no if and only if $q = 4, 16$ or
$$m^2 - 4q \in \{-3, -4, -8, -11\}.$$

The case $g = 2, 3$ (Continued)

For $g \leq 3$, any absolutely indecomposable p.p.a.v. $(A, a)/K$ is the Jacobian of a curve C_0 over $\bar{K}$ (Oort, Ueno 1973).

Theorem (Arithmetic Torelli theorem (Serre 1985))

There is a unique model C/K of C_0 such that:

1. *If C_0 is hyperelliptic, there is an isomorphism*

$$(\mathrm{Jac}\, C, j) \xrightarrow{\sim} (A, a).$$

2. *If C_0 is not hyperelliptic, there is a unique quadratic character ε of $\mathrm{Gal}(\bar{K}/K)$, and a unique isomorphism*

$$(\mathrm{Jac}\, C, j) \xrightarrow{\sim} (A, a)_\varepsilon$$

where $(A, a)_\varepsilon$ is the twist of A by ε.

The case $g = 2$ (end)

For $g = 2$, the previous results give the answer. Actually (Serre 1983) gives the value $N_q(2)$.

Remark (Howe, Nart, R. 09): one characterizes the isogeny classes of abelian surfaces which contain a Jacobian in terms of their Weil polynomial.

Serre's obstruction for genus 3 curve

Serre's observation (1983): "Le théorème de Torelli s'applique de façon moins satisfaisante (on doit extraire une mystérieuse racine carrée . . .)"

Serre's Question (letter to Top 2003): how to compute the character ε ?

1. Explicit quotients by isogeny (Partial results);
2. Serre's analytic strategy, also followed by S. Meagher (Well understood);
3. Algebraic interpretation of this strategy (Work in progress);
4. Geometric strategy (Soon on Arxiv).

Quotients by isogeny

Key idea: use families with explicit elliptic isogeny factors and reverse the process to see when you can glue them together in this way.

Example: a non hyperellliptic family with geometric automorphism group $(\mathbb{Z}/2\mathbb{Z})^2$ in char. 2

$$C : (a(x^2 + y^2) + cz^2 + xy + ez(x + y))^2 = xyz(x + y + z)$$

with involutions $(y, x, z), (x + z, y + z, z), (y + z, x + z, z)$.
For the first involution: $X = x + y$, $Y = xy$ and

$$E_1 : (aX^2 + c + Y + eX)^2 = Y(X + 1).$$

Then $\mathrm{Jac}(C) \sim E_1 \times E_2 \times E_3$ where

$$\begin{aligned} E_1 &: y^2 + xy &&= x^3 + ex^2 + a^2(a + c + e)^2 \\ E_2 &: y^2 + xy &&= x^3 + ex^2 + c^2(a + c + e)^2 \\ E_3 &: y^2 + xy &&= x^3 + ex^2 + c^2a^2. \end{aligned}$$

If one wants to glue $E_i : y^2 + xy = x^3 + ex^2 + 1/j_i$.
If $q > 2$ then $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(e) = 0$ if and only if $\mathrm{Tr}(E_i) \equiv 1 \pmod 4$.

Let $s_i^4 = 1/j_i$. Then

$$\begin{aligned} a &= \frac{s_1 s_3}{s_2} \\ c &= \frac{s_2 s_3}{s_1} \\ e &= \frac{s_1 s_3}{s_2} + \frac{s_2 s_3}{s_1} + \frac{s_1 s_2}{s_3}. \end{aligned}$$

$\longrightarrow$ Serre's obstruction is a condition on the trace of

$$\frac{s_1 s_3}{s_2} + \frac{s_2 s_3}{s_1} + \frac{s_1 s_2}{s_3}.$$

- (Nart, R. 2009) : if n is odd and $m = \lfloor 2\sqrt{2^n} \rfloor \equiv 1, 5, 7 \pmod 8$ there is an optimal curve over $\mathbb{F}_{2^n}$.
- (Nart, R. 2008): if $n \geq 6$ is even then there is an optimal curve over $\mathbb{F}_{2^n}$.
- (Howe, Leprevost, Poonen 2002) in characteristic different from 2. Easiest case: if $3\alpha + \beta \in k^2$ then there exists C/k such that $\mathrm{Jac}(C) \sim E^3$ with $E/k : y^2 = x(x - \alpha)(x - \beta)$;

Rem: (Mestre 2009) works with the family with geometric automorphism group S_3.

Main result (Lachaud, R., Zykin 2009)

Let $A = (A, a)/K$ be a p.p.a.t. defined over a field K with $\operatorname{char} K \neq 2$. Assume that a is absolutely indecomposable. There exists a unique geometric Siegel modular form of weight 18 defined over $\mathbb{Z}$, denoted χ_{18}, such that

- (A, a) is a hyperelliptic Jacobian if and only if $\chi_{18}(A, a) = 0$.
- (A, a) is a non hyperelliptic Jacobian if and only if $\chi_{18}(A, a)$ is a non-zero square.

Moreover, if $K \subset \mathbb{C}$, let

- $(\omega_1, \omega_2, \omega_3)$ be a basis of $\Omega^1_K[A]$;
- $\gamma_1, \ldots \gamma_6$ be a symplectic basis (for a);
- $\Omega_a := [\Omega_1\ \Omega_2] = [\int_{\gamma_j} \omega_i]$ with $\tau_a := \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$.

Then (A, a) is a Jacobian if and only if

$$\chi_{18}((A, a), \omega_1 \wedge \omega_2 \wedge \omega_3) := \frac{(2\pi)^{54}}{2^{28}} \cdot \frac{\prod_{[\varepsilon] \text{ even}} \theta[\varepsilon](\tau_a)}{\det(\Omega_2)^{18}}$$

is a square in K.

Ingredients of the proof and consequences

- Result of (Ichikawa 1996): let $t : \mathrm{M}_3 \to \mathrm{A}_3$ be the Torelli map. There exists a Teichmüller modular form of weight 9 defined over $\mathbb{Z}$, denoted μ_9, such that $t^*(\chi_{18}) = \mu_9^2$.
- General result on the action of twists on geometric Siegel modular forms.
- Link between analytic and geometric Siegel modular forms.

By-products:

- Klein's formula: $\mu_9 = \pm\,\mathrm{Disc}$;
- cannot work for g even;
- need forms of weight h such that $h/2$ is odd;
- cannot take χ_h.

How to use it for optimal curves ?

R. 2010 : worked out the procedure in the case $A = E^3$ where E is an elliptic curve with CM.

- $\exists$? optimal curve $C/\mathbb{F}_{47}$: $A = \mathrm{Jac}\, C \sim E^3$ with E CM by $\mathcal{O} = \mathbb{Z}[\tau]$ where $\tau = (1 + \sqrt{-19})/2$.
- $Cl(\mathcal{O}) = 1 \Rightarrow A = E^3$.
- a_0 the product polarization on A:

$$\{a \text{ p.p. on } A\} \longleftrightarrow \{M = a_0^{-1} a \in M_3(\mathcal{O}) \text{ hermitian positive definite of determinant } 1\}.$$

- computation by (Schiemann 1998) of such matrices. There is only one –up to equivalence–, which is indecomposable:

$$M = \begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}.$$

- lift E as a CM curve over $\overline{\mathbb{Q}}$: $\tilde{E} : y^2 = x^3 - 152x - 722$;
- find a period matrix associated to $(\tilde{E}^3, a_0 M)$.
- compute an analytic approximation of

$$\chi_{18}((\tilde{E}^3, a_0 M), \omega_0) = (2^{19} \cdot 19^7)^2;$$

- since it is a square (over $\mathbb{F}_{47}$), such an optimal curve C exists.

(Guàrdia 2009):

$$\tilde{C} : x^4 + \frac{1}{9}y^4 + \frac{2}{3}x^2y^2 - 190y^2 - 570x^2 + \frac{152}{9}y^3 - 152x^2y = 1083.$$

Values of $\chi = \chi_{18}((\tilde{E}^3, a_0 M), \omega_0)$

$\tilde{E}$: Gross' models with discriminant d^3 (when the class number is 1).

d	M, $\tau = (1+\sqrt{d})/2$	χ	$\#\,\mathrm{Aut}(\tilde{E}^3, a)$
-7	$\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & \overline{\tau} \\ 1 & \tau & 2 \end{pmatrix}$	$(7^7)^2$	$2 \cdot 168$
-19	$\begin{pmatrix} 2 & 1 & -1 \\ 1 & 3 & -2+\tau \\ -1 & -2+\overline{\tau} & 3 \end{pmatrix}$	$(2^5 \cdot 19^7)^2 \cdot (-2)$	$2 \cdot 6$
-43	$\begin{pmatrix} 3 & 1 & 1-\overline{\tau} \\ 1 & 4 & 2 \\ 1-\tau & 2 & 5 \end{pmatrix}$	$(2^6 \cdot 43^7)^2 \cdot (-47 \cdot 79 \cdot 107 \cdot 173)$	$2 \cdot 1$
-67	$\begin{pmatrix} 2 & 0 & -1 \\ 0 & 3 & -2+\overline{\tau} \\ -1 & -2+\tau & 7 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 67^7)^2 \cdot (-2 \cdot 7 \cdot 31)$	$2 \cdot 6$
-163	$\begin{pmatrix} 2 & 1 & -\overline{\tau} \\ 1 & 2 & 1-\overline{\tau} \\ -\tau & 1-\tau & 28 \end{pmatrix}$	$(2^5 \cdot 7^4 \cdot 11^4 \cdot 163^7)^2 \cdot (-2 \cdot 7 \cdot 11 \cdot 19 \cdot 127)$	$2 \cdot 6$
-15	$\begin{pmatrix} 2 & -1 & -1+\overline{\tau} \\ -1 & 2 & 1-\overline{\tau} \\ -1+\tau & 1-\tau & 3 \end{pmatrix}$	$22769095299822142340569171645771726299/4+$ $1018252260302083448486308515124432267 5 \cdot \sqrt{5}/4+$ $44626409093538218819956956474294768 69 \cdot \sqrt{-15}/4$ $+997833061792288644382398275511420244 5 \cdot \sqrt{-3}$	$2 \cdot 24$

Consequences (with $d = -19$): optimal curve for $q = 47, 61, 137, 277$ but not for 311 (see Top 2003, Alekseenko et al. 2009).

Algebraic interpretation of χ

Idea: interpret $\mathfrak{p}|\chi$ in terms of the geometric nature of $(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$.

So far, very basic results about primes that appear because of decomposable polarizations.

Question: how to detect hyperelliptic reduction ?
Ex. for $d = -15$ with $\mathfrak{p}|19$:

$\sqrt{-3}$	$\sqrt{5}$	$(\tilde{E}^3, a_0 M) \pmod{\mathfrak{p}}$ is the Jacobian of a
-4	9	non hyperelliptic curve with $1 + q + 3m - 3$ points
-4	-9	non hyperelliptic curve with $1 + q + 3m - 3$ points
4	-9	non hyperelliptic curve with $1 + q - 3m + 3$ points
4	9	hyperelliptic curve

Worse: how to control the (parity of the) exponents ?

The geometric approach (work in progress with A. Beauville)

Let $(A, a)/k$ be a p.p.a.t. with an absolutely indecomposable polarization and char $k \neq 2$. We assume that (A, a) is geometrically non hyperelliptic.

- There exists a symmetric theta divisor Θ defined over k.

Let Σ be the union of $2_*\Theta$ and of the unique divisor in $|2\Theta|$ with multiplicity ≥ 4 at 0.

Proposition

Let $\alpha \in A(\bar{k}) \setminus \{0\}$. The curve $\tilde{X}_\alpha = \Theta \cap (\Theta + \alpha)$ is smooth and connected iff $\alpha \in A(\bar{k}) \setminus \Sigma$.

Assume so, then $X_\alpha = \tilde{X}_\alpha/(z \mapsto \alpha - z)$ is a smooth genus 4 curve.

Proposition

The curve X_α is non hyperelliptic and its canonical model in $\mathbb{P}^3$ lies on a quadric Q_α which is smooth.

Theorem

Assume there exists $\alpha \in A(k) \setminus \Sigma$. Then (A, a) is a Jacobian if and only if $\delta = \mathrm{Disc}\, Q_\alpha \in k^2$.

Remark: when $\alpha \in A[2](k) \setminus \Sigma$, this is a geometric interpretation of Howe-Leprevost-Poonen construction.

Question: can we compute δ for $A = E^3$ and $a = a_0 M$?