Counting points on hyperelliptic curves with geometrically split Jacobians

Semyon Novoselov

Immanuel Kant Baltic Federal University, Russia

Abstract

For genus 2 curves of type $y^2 = x^5 + ax^3 + bx$ there is a fast algorithm [*Satoh'09*] for computing the Jacobian order and the explicit formulae [*Guillevic-Vergnaud'12*].
In this work we extend these results to higher genera.

Basic definitions

Hyperelliptic curves

$$C : y^2 = f(x),$$

$f \in \mathbb{F}_q[x]$, f is square-free, $\deg f \in \{2g+1, 2g+2\}$, $\mathrm{char}(\mathbb{F}_q) = p > 2$.

Geometrically split Jacobians

$$\mathrm{Jac}_C(\mathbb{F}_{q^k}) \sim \mathrm{Jac}_{X_1} \times \mathrm{Jac}_{X_2},$$

$\mathrm{Jac}_C(\mathbb{F}_q)$ is simple or contains simple abelian varieties A.
For $g = 2$ it is known that $k \le 6$ [*Chou-Kani'14*].

Zeta-function

$$Z(C/\mathbb{F}_q; T) = exp\left(\sum_{k=1}^{\infty} \frac{\#C(\mathbb{F}_{q^k})}{k} T^k\right) = \frac{L_{C,q}(T)}{(1-T)(1-qT)}.$$

Here, $L_{C,q}(T) = T^{2g}\chi_{C,q}(\frac{1}{T})$ where $\chi_{C,q}(T)$ is the characteristic polynomial of the Frobenius endomorphism.

$$\#\mathrm{Jac}_C(\mathbb{F}_q) = \chi_{C,q}(1).$$

Our goal is to derive fast methods for computing $\chi_{C,q}$.

Legendre-Satoh curves

$$C : y^2 = x^{2g+1} + ax^{g+1} + bx$$

- g – odd, $\mathrm{Jac}_C(\mathbb{F}_q[\sqrt[2g]{b}]) \sim E_1 \times \mathrm{Jac}^2_{X_1}$. Splits as $E_1 \times A$ over $\mathbb{F}_q$.
- g – even, $\mathrm{Jac}_C(\mathbb{F}_q[\sqrt[4g]{b}]) \sim \mathrm{Jac}^2_{X_2}$. Can be simple over $\mathbb{F}_q$.

Chebyshev-Dickson curves

$$X_1 : y^2 = D_g(x, \sqrt[g]{b}) + a,$$
$$X_2 : y^2 = (x + 2\sqrt[2g]{b})(D_g(x, \sqrt[g]{b}) + a).$$

- $D_g(x, \alpha)$ is a Dickson polynomial of degree g.
- $\mathrm{Jac}_{X_1}, \mathrm{Jac}_{X_2}$ are generically absolutely simple (for prime g).
- X_1 is a curve with explicit RM.

General complexity

Computing χ_{X_i,q^k}

- $\tilde{O}(\log^{cg_i} q^k)$, general algorithm for h.e.c., [*Abelard-Gaudry-Spaenlehauer'19*].
- $O(\log^9 q^k)$, h.e.c. with explicit RM, [*Abelard'19*].
- $O(\log^8 q^k)$, $g = 2$, h.e.c, [*Gaudry-Schost'12*].

Descend

- solving polynomial equation systems over $\mathbb{Z}$ in g variables of total degree $\le \max\{k_i\}$.
- exponential in $\log q$ (general case).
- $g = 2$: polynomial time via resultants [*Satoh'09*] and explicit formulae [*Guillevic-Vergnaud'12*].

Outline of general algorithm

Input: A curve C s.t. $\mathrm{Jac}_C(\mathbb{F}_{q^k}) \sim \mathrm{Jac}_{X_1} \times \mathrm{Jac}_{X_2}$.
Output: $\chi_{C,q}$ for simple Jac_C.

1. Compute χ_{X_1,q^k} and χ_{X_2,q^k}.
2. $\chi_{C,q^k} \leftarrow \chi_{X_1,q^k} \times \chi_{X_2,q^k}$.
3. Factor $k = k_1 \cdot \ldots \cdot k_m$.
4. Descend on the tower

$$\mathbb{F}_q \subset \mathbb{F}_{q^{k_1}} \subset \mathbb{F}_{q^{k_1k_2}} \subset \ldots \subset \mathbb{F}_{q^k},$$

step-by-step by computing the chain

$$\chi_{C,q^k} \mapsto \ldots \mapsto \chi_{C,q^{k_1k_2}} \mapsto \chi_{C,q^{k_1}} \mapsto \chi_{C,q}$$

of characteristic polynomials.

New explicit formulae [2, 3]

General via Cartier-Manin

For Legendre-Satoh curves:

Table 1: Characteristic polynomials for curve C.

g	conditions	$\chi_p(T) \bmod p$
2	$p \equiv 1 \bmod 4$	$T^2(T - P_{\lfloor \frac{p}{4} \rfloor})^2$
2	$p \equiv 3 \bmod 4$	$T^2(T^2 - P^2_{\lfloor \frac{p}{4} \rfloor})$
3	$p \equiv 1 \bmod 3$	$T^3(T - P_{\lfloor \frac{p}{2} \rfloor})(T - P_{\lfloor \frac{p}{6} \rfloor})^2$
3	$p \equiv 2 \bmod 3$	$T^3(T - P_{\lfloor \frac{p}{2} \rfloor})(T^2 - P^2_{\lfloor \frac{p}{6} \rfloor})$
4	$p \equiv 1 \bmod 8$	$T^4(T - P_{\lfloor \frac{p}{8} \rfloor})^2(T - P_{\lfloor \frac{3p}{8} \rfloor})^2$
4	$p \equiv 3,5 \bmod 8$	$T^4(T^2 - P_{\lfloor \frac{p}{8} \rfloor} P_{\lfloor \frac{3p}{8} \rfloor})^2$
4	$p \equiv 7 \bmod 8$	$T^4(T^2 - P^2_{\lfloor \frac{p}{8} \rfloor})(T^2 - P^2_{\lfloor \frac{3p}{8} \rfloor})$

Here, $P_n := P_n(-a/2)$ is the Legendre polynomial of degree n. This table is for $b = 1$. For $b \ne 1$ see [2].

Complexity

- $P_{\lfloor \frac{p}{2} \rfloor}$, $P_{\lfloor \frac{p}{4} \rfloor}$, $P_{\lfloor \frac{p}{6} \rfloor}$ = Frobenius traces of the elliptic curves [2]. Computation takes $\tilde{O}(\log^4 p)$ using SEA.
- General case has exponential time complexity.

Analogous table for Chebyshev-Dickson curve X_1 from the Jacobian decomposition:

For Chebyshev-Dickson curves

Table 2: Characteristic polynomials for X_1.

genus	conditions	$\chi_p(T) \bmod p$
2	$p \equiv 1,4 \bmod 5$	$T^2(T - P_{\lfloor \frac{3p}{10} \rfloor})(T - P_{\lfloor \frac{p}{10} \rfloor})$
2	$p \equiv 2,3 \bmod 5$	$T^2(T^2 - P_{\lfloor \frac{3p}{10} \rfloor} P_{\lfloor \frac{p}{10} \rfloor})$
3	$p \equiv 1,6 \bmod 7$	$T^3(T - P_{\lfloor \frac{5p}{14} \rfloor})(T - P_{\lfloor \frac{3p}{14} \rfloor})(T - P_{\lfloor \frac{p}{14} \rfloor})$
3	$p \equiv 2,3,4,5 \bmod 7$	$T^3(T^3 - P_{\lfloor \frac{5p}{14} \rfloor} P_{\lfloor \frac{3p}{14} \rfloor} P_{\lfloor \frac{p}{14} \rfloor})$

For genus 3 via Descend

For any curve

Let $\mathrm{Jac}_C \sim E_1 \times A$ over $\mathbb{F}_q$ and $\mathrm{Jac}_C \sim E_1 \times E_2 \times \tilde{E}_2$ over $\mathbb{F}_{q^3}$ where E_2 is ordinary. Then $\chi_C = \chi_{E_1,q} \times \chi_{A,q}$ where $\chi_{A,q}$ is one of the following.

- $(T^2 - t_2T + q)(T^2 \pm t_2T + q)$;
- $T^4 \pm t_2T^3 + (t_2^2 - q)T^2 \pm t_2qT + q^2$.

For specialized formulae for Legendre-Satoh curves see [3].

Special algorithms

Genus 3

$$C : y^2 = x^7 + ax^4 + bx$$

Computing $\chi_{C,q}$

- Curve over prime field $\Longrightarrow$ Cartier-Manin method (Table 1) is polynomial time.
- General case $\Longrightarrow$ explicit formulae for genus 3.

New complexity

Computing $\chi_{C,q}$ for genus 3 Legendre-Satoh curve takes time $\tilde{O}(\log^4 q)$. General case: $\tilde{O}(\log^{14} q)$.

Genus 4

$$C : y^2 = x^9 + ax^5 + bx$$

- $\mathrm{Jac}_C \sim \mathrm{Jac}^2_{X_2}$ over $\mathbb{F}_q[\sqrt[16]{b}]$.

Computing $\chi_{C,q}$

- Use twist of X_2 defined over $\mathbb{F}_q[\sqrt{b}]$:

$$\tilde{X}_2 : y^2 = (x+2)(x^4 - 4x^2 + 2 + a/\sqrt{b}).$$

- Compute $\chi_{\tilde{X}_2,q^2}(T)$ and derive $\chi_{X_2,q^{16}}(T)$ from it.
- Descend = factoring univariate polynomial [2] of degree 16.
- Most expensive operation is a computing $\chi_{\tilde{X}_2,q^2}(T)$ for genus 2 curve.

New complexity

Computing $\chi_{C,q}$ for genus 4 Legendre-Satoh curve takes time $\tilde{O}(\log^8 q)$.

Experimental results

We implemented the algorithms in Sage 8.9. Source code is available at [4]. Computations were done on Xeon E-2146G, 3.50GHz. For $g = 3$ the runtime is given for a curve with simple factor A of Jacobian. For $g = 4$ the runtime is given for a curve with simple Jacobian.

Table 3: Computations for curves over prime fields.

g	curve	group size	method	time
3	L/S	958 bit	SEA+Cartier-Manin	39 min.
3	L/S	1535 bit	SEA+exp.formulae	6 min.
4	L/S	163 bit	hypellfrob+descend	18 min.

References

[1] S. Novoselov, Hyperelliptic curves, Cartier-Manin matrices and Legendre polynomials, http://mi.mathnet.ru/pdm593

[2] S. Novoselov, Counting points on hyperelliptic curves of type $y^2 = x^{2g+1} + ax^{g+1} + bx$, https://arxiv.org/abs/1902.05992

[3] S. Novoselov, Y. Boltnev, Characteristic polynomials of the curve $y^2 = x^7 + ax^4 + bx$ over finite fields, http://mi.mathnet.ru/pdma427

[4] https://crypto-kantiana.com/semyon.novoselov

Contact
snovoselov@kantiana.ru