Inverse Jacobian and related topics for certain superelliptic curves

Somoza Henares, A.

Stellingen

behorend bij het proefschrift

Inverse Jacobian and related topics for certain superelliptic curves

1. The Picard curve $y^3 = x^4 - x$ satisfies the generalized Sato-Tate conjecture.

2. There exist exactly 4 cyclic plane quintic curves defined over $\mathbb{Q}$ whose Jacobians have complex multiplication (CM) by a maximal order.

3. There is an algorithm that, given the period matrix of a Picard curve, returns a numerical approximation of the defining equation of the curve.

4. There is an analogous algorithm for cyclic plane quintic curves.

The following definitions are used in Propositions 5 and 6. We define a *principally polarized* $\mathbb{Z}[\zeta_5]$*-lattice* to be a pair $(\mathcal{M}, T)$ with $\mathcal{M}$ a free $\mathbb{Z}[\zeta_5]$-module of rank 3 and $T : \mathcal{M} \times \mathcal{M} \to \mathbb{Q}(\zeta_5)$ an antihermitian form such that the alternating $\mathbb{Z}$-bilinear form $E = \mathrm{tr}_{\mathbb{Q}(\zeta_5)/\mathbb{Q}} \circ T : \mathcal{M} \times \mathcal{M} \to \mathbb{Q}$ satisfies $E(\mathcal{M}, \mathcal{M}) \subset \mathbb{Z}$ and has determinant 1.

Let $\phi_1, \phi_2 : \mathbb{Q}(\zeta_5) \to \mathbb{C}$ be the embeddings given by $\phi_i(\zeta_5) = \exp(2\pi i/5)^i$.

The *signature* of T is the integer pair $\mathrm{sign}(T) = (r_1, r_2)$ with $0 \le r_1, r_2 \le 3$ if for every $\nu = 1, 2$ there exists an invertible matrix $W_\nu \in \mathbb{C}^{3\times 3}$ that satisfies

$$\phi_\nu(T) = {}^t\overline{W_\nu} \begin{pmatrix} i\mathbf{1}_{r_\nu} & 0 \\ 0 & -i\mathbf{1}_{3-r_\nu} \end{pmatrix} W_\nu.$$

We also define the fractional $\mathbb{Z}[\zeta_5]$-ideal

$$[\mathbb{Z}[\zeta_5]^3/\mathcal{M}] = (\det(\alpha) : \alpha \in \mathbb{Q}(\zeta_5)^{3\times 3} \text{ such that } \alpha\mathbb{Z}[\zeta_5]^3 \subseteq \mathcal{M}).$$

5. Every principally polarized $\mathbb{Z}[\zeta_5]$-lattice $(\mathcal{M}, T)$ satisfies

$$\mathrm{N}_{K/K_+}([\mathbb{Z}[\zeta_5]^3/\mathcal{M}]) = (\det(\delta T)^{-1})\mathbb{Z}[\zeta_5^4 + \zeta_5].$$

6. There is a unique isomorphism class of principally polarized $\mathbb{Z}[\zeta_5]$-lattices $(\mathcal{M}, T)$ with $\mathrm{sign}(T) = (3, 2)$.

In Propositions 7 and 8, we refer as the *fractional approximation* R_f of a polynomial $f \in \mathbb{F}_q[x]$ given by

$$f(x) = \Big(\ldots\big((a_0x + a_1)^{q-2} + a_2\big)^{q-2} \cdots + a_n\Big)^{q-2} + a_{n+1} \qquad (\star)$$

to the rational function $R_f(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ with matrix form

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_0 & a_1 \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2}.$$

7. Let $f \in \mathbb{F}_q[x]$ be as in $(\star)$, and let $c \in \mathbb{F}_q^\times$ and $1 \leq k < q-1$ be such that both $x \mapsto f(x)$ and $x \mapsto f(x) + cx^k$ are bijections from $\mathbb{F}_q$ to $\mathbb{F}_q$. Suppose that the fractional approximation R_f of f satisfies $\gamma \neq 0$ and $\delta = 0$. If $k+1$ and $q-1$ are coprime, then $k \geq (q-n)/(n+3)$ holds.
8. Consider the polynomial $f = (((x+a)^{q-2}+b)^{q-2}+c)^{q-2}$ with $f(0) = 0$ and $a(b^2+4) \neq 0$. Let $R_f^{(m)}$ be the fractional approximation of the mth iterate of f. Then we have $R_f^{(m)}(x) = x$ if and only if b is a root of the polynomial
$$A_m(T) = \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m-j-1}{j} T^{m-2j-1} .$$
In particular we have $\mathrm{ord}(R_f) = \min\{m : A_m(b) = 0\}$.
9. When a publication contains computational results, it is a good habit to share the implementation, preferably using only open source software.
10. In the situation of Proposition 9, writing that it is *available upon request* does not count as sharing.

Propositions 1 and 3 are based on joint work with Lario. Propositions 7 and 8 are based on joint work with Anbar, Oduzak, Patel, Quoos and Topuzoğlu.