代数幾何学シンポジウム記録
2011年度 pp.151-151

The Tate-Lichtenbaum pairing on a hyperelliptic curve via hyperelliptic nets

Yukihiro Uchida (Kyoto University)

1 Introduction

Let C be a non-singular projective curve defined over a finite field $\mathbb{F}_q$. Let m be a positive integer with $m \mid (q-1)$. The Tate-Lichtenbaum pairing is a bilinear map

$$\tau_m\colon \mathrm{Pic}^0(C)[m] \times \mathrm{Pic}^0(C)/m\,\mathrm{Pic}^0(C) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m.$$

For cryptographic applications, it is important to find an efficient algorithm to compute the Tate-Lichtenbaum pairing.

The Tate-Lichtenbaum pairing is usually computed by Miller's algorithm. Recently, Stange [3] gave a new algorithm to compute the Tate(-Lichtenbaum) pairing on an elliptic curve. This algorithm is based on elliptic nets, which are also defined by Stange as a generalization of elliptic divisibility sequences.

In this poster, we define hyperelliptic nets as a generalization of elliptic nets to hyperelliptic curves. We also give an expression for the Tate-Lichtenbaum pairing on a hyperelliptic curve in terms of hyperelliptic nets. By using this expression, we obtain an algorithm to compute the Tate-Lichtenbaum pairing on a hyperelliptic curve of genus 2.

2 The hyperelliptic sigma function

Let C be a non-singular projective curve of genus g over $\mathbb{C}$ defined by

$$y^2 = x^{2g+1} + \lambda_{2g}x^{2g} + \cdots + \lambda_1 x + \lambda_0.$$

We use the following notation:

- ∞: the point at infinity of C,
- J: the Jacobian variety of C,
- $\kappa\colon \mathbb{C}^g \to \mathbb{C}^g/\Lambda \cong J(\mathbb{C})$, where we fix a uniformization $\mathbb{C}^g/\Lambda \cong J(\mathbb{C})$,
- $\lambda\colon C \to J$: an embedding with $\lambda(\infty) = O$,
- $\Theta = \lambda(C) + \cdots + \lambda(C)$ ($g-1$ times): the theta divisor.

We write $\boldsymbol{e}(z) = \exp(2\pi\sqrt{-1}\,z)$. We define the theta function with characteristics by

$$\vartheta\begin{bmatrix} a \\ b \end{bmatrix}(z,\tau) = \sum_{n\in\mathbb{Z}^g} \boldsymbol{e}\left(\frac{1}{2}{}^t(n+a)\tau(n+a) + {}^t(n+a)(z+b)\right),$$

where $z \in \mathbb{C}^g$, $\tau \in M_g(\mathbb{C})$ is symmetric, $\mathrm{Im}(\tau)$ is positive definite, and $a, b \in \mathbb{R}^g$.

Definition 1 (cf. [2]). We define the *hyperelliptic sigma function* on $\mathbb{C}^g$ by

$$\sigma(u) = c\exp\left(\frac{1}{2}{}^t u\eta'\omega'^{-1}u\right)\vartheta[\delta](\omega'^{-1}u, \omega'^{-1}\omega''),$$

where $\omega', \omega'' \in M_g(\mathbb{C})$ are period matrices satisfying $\Lambda = \omega'\mathbb{Z}^g + \omega''\mathbb{Z}^g$ and $c \in \mathbb{C}$, $\eta' \in M_g(\mathbb{C})$, and $\delta \in ((1/2)\mathbb{Z})^{2g}$ are certain constants.

If $g = 1$, then $\sigma(u)$ coincides with the Weierstrass sigma function.

The sigma function $\sigma(u)$ has a zero of order 1 along $\kappa^{-1}(\Theta)$.

3 Hyperelliptic nets

Let n be a positive integer.

We first define hyperelliptic nets over $\mathbb{C}$. The following is a straightforward generalization of Stange's definition.

Definition 2. Let $P_1, \ldots, P_n \in J(\mathbb{C}) \setminus \Theta$ with $P_i + P_j \notin \Theta$ for all $1 \le i < j \le n$. Let $u_1, \ldots, u_n \in \mathbb{C}^g$ be points with $\kappa(u_i) = P_i$. We define a map $W_{C,P_1,\ldots,P_n}\colon \mathbb{Z}^n \to \mathbb{C}$ by

$$W_{C,P_1,\ldots,P_n}(v_1,\ldots,v_n) = \frac{\sigma(v_1u_1 + \cdots + v_nu_n)}{\prod_{i=1}^n \sigma(u_i)^{2v_i^2 - \sum_{j=1}^n v_iv_j} \prod_{1\le i<j\le n} \sigma(u_i+u_j)^{v_iv_j}}.$$

We call $W_{C,P_1,\ldots,P_n}$ the *hyperelliptic net associated to* $C, P_1, \ldots, P_n$.

It is easily verified that $W_{C,P_1,\ldots,P_n}$ does not depend on the choice of $u_1, \ldots, u_n$.

Lemma 3. *We assume that C is defined over a subfield $K \subset \mathbb{C}$ and $P_1, \ldots, P_n \in J(K)$. Then, for any $\boldsymbol{v} \in \mathbb{Z}^n$,*

$$W_{C,P_1,\ldots,P_n}(\boldsymbol{v}) \in K.$$

By Lemma 3, we can define hyperelliptic nets over any field of characteristic 0. Furthermore, we can also define hyperelliptic nets over any field of positive characteristic by reduction.

4 Recurrence relations

Theorem 4. *Let $W_{C,P_1,\ldots,P_n}$ be a hyperelliptic net as before. Let $m > 2^g$ be an integer. Let $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(m)} \in ((1/2)\mathbb{Z})^n$ with $\boldsymbol{v}^{(i)} + \boldsymbol{v}^{(j)}, \boldsymbol{v}^{(i)} - \boldsymbol{v}^{(j)} \in \mathbb{Z}^n$ for all $1 \le i, j \le m$. We define a matrix A by*

$$A = \left(W_{C,P_1,\ldots,P_n}(\boldsymbol{v}^{(i)} + \boldsymbol{v}^{(j)})W_{C,P_1,\ldots,P_n}(\boldsymbol{v}^{(i)} - \boldsymbol{v}^{(j)})\right)_{1\le i,j\le m}.$$

Then we have $\det A = 0$. In particular, if $g \equiv 1, 2 \pmod 4$ and m is even, then we have $\mathrm{pf}\, A = 0$, where $\mathrm{pf}\, A$ is the Pfaffian of A.

5 The Tate-Lichtenbaum pairing

Definition 5. The *Tate-Lichtenbaum pairing* is a map

$$\tau_m\colon \mathrm{Pic}^0(C)[m] \times \mathrm{Pic}^0(C)/m\,\mathrm{Pic}^0(C) \to \mathbb{F}_q^\times/(\mathbb{F}_q^\times)^m;$$
$$(\overline{D}, \overline{E}) \mapsto f_D(E) = \prod_{i=1}^r f_D(P_i)^{n_i},$$

where D and E are divisors on C representing $\overline{D}$ and $\overline{E}$ respectively such that D and E have no points in common, f_D is a rational function on C with $\mathrm{div}(f_D) = mD$, and $E = \sum_{i=1}^r n_iP_i$.

It is known that τ_m is bilinear and non-degenerate (cf. [1]).

The Tate-Lichtenbaum pairing is described in terms of hyperelliptic nets.

Theorem 6. *Let P and Q be points associated to $\overline{D}$ and $\overline{E}$ respectively. Then we have*

$$\tau_m(\overline{D}, \overline{E}) = \frac{W_{C,P,Q}(m+1,1)W_{C,P,Q}(1,0)}{W_{C,P,Q}(m+1,0)W_{C,P,Q}(1,1)} \bmod (\mathbb{F}_q^\times)^m.$$

Theorem 6 is a generalization of Stange's result for elliptic curves.

By Theorems 4 and 6, we can compute $\tau_m(\overline{D}, \overline{E})$ for a curve of genus 2.

Corollary 7. *Assume $g = 2$. If (P, Q) is not on a certain divisor on $J \times J$, then $\tau_m(\overline{D}, \overline{E})$ can be computed with $O(\log m)$ operations in $\mathbb{F}_q$.*

Note that the above complexity is the same as that of Miller's algorithm.

6 Example

Let $q = 47$. We consider the following curve and divisors:

- $C/\mathbb{F}_{47}$: $y^2 = x^5 + x + 41$,
- $D = (\alpha_1, 31\alpha_1 + 3) + (\alpha_2, 31\alpha_2 + 3) - 2\infty$,
- $E = (\beta_1, 22\beta_1 + 14) + (\beta_2, 22\beta_2 + 14) - 2\infty$,

where α_1 and α_2 are the roots of the polynomial $x^2 + 6x + 16$ over $\mathbb{F}_{47}$, and β_1 and β_2 are the roots of the polynomial $x^2 + 29x + 24$ over $\mathbb{F}_{47}$.

Let P and Q be the points on J corresponding to $\overline{D}$ and $\overline{E}$ respectively. The following figure shows a part of the net $W_{C,P,Q}$.

	7	12	2	36	19	33	39	18
	14	38	14	10	23	21	36	9
	13	31	32	18	8	2	2	16
	14	15	43	19	44	5	22	42
	25	6	33	11	10	36	21	16
	25	8	2	13	16	32	14	5
↑	1	1	23	4	29	40	43	7
Q	0	1	37	18	36	2	7	45
	$P \to$							

Let $m = 23$. Then m is a divisor of $q - 1 = 46$ and $\overline{D} \in \mathrm{Pic}^0(C)[m]$.

We have

$$W_{C,P,Q}(m+1,1) = 43, \quad W_{C,P,Q}(m+1,0) = 8,$$
$$W_{C,P,Q}(1,0) = W_{C,P,Q}(1,1) = 1.$$

Therefore, by Theorem 6,

$$\tau_m(\overline{D}, \overline{E}) = \frac{43}{8} \bmod (\mathbb{F}_{47}^\times)^{23} = 23 \bmod (\mathbb{F}_{47}^\times)^{23}.$$

References

[1] G. Frey, H.-G. Rück, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Math. Comp. **62** (1994) 865–874.

[2] Y. Ônishi, Determinant expressions for hyperelliptic functions (with an appendix by Shigeki Matsutani), Proc. Edinb. Math. Soc. (2) **48** (2005) 705–742.

[3] K. E. Stange, The Tate pairing via elliptic nets, in *Pairing-Based Cryptography - PAIRING 2007*, Lecture Notes in Computer Science 4575, Springer, Berlin, 2007, 329–348.