Lectures on Sato-Tate distributions of curves

Francesc Fité and Andrew V. Sutherland

February 17–21, 2014

1 Lectures

The goal of this series of talks is to present an approach to the article *Sato-Tate distributions and Galois endomorphism modules in genus* 2 (see [3]). We shall recall some background material and indicate the connection to other works when necessary.

Lecture 1. Introduction to Sato-Tate distributions

Overview of the generalized Sato-Tate conjecture with lots of explicit examples. Preliminary discussion of L-polynomial distributions, Sato-Tate groups, and moment sequences. Presentation of the main results in genus 2.
A.V. Sutherland

Lecture 2. The generalized Sato-Tate conjecture

The general background of [3] will be recalled: the notion of equidistribution (with special emphasis to the case of a compact group), its connection to L-functions (appendix to Chapter I of [11]), the Sato-Tate group and the generalized Sato-Tate conjecture (Chapter 8 of [11]), and the algebraic Sato-Tate conjecture [1].
F. Fité

Lecture 3. Sato-Tate axioms

The *Sato-Tate axioms* for a self-dual motive with rational coefficients and fixed weight ω and Hodge numbers $h^{p,q}$ will be presented (this refers to a set of properties that the Sato-Tate group is conjectured to verify in general). They lead to Lie group classification results for particular choices of ω and the $h^{p,q}$'s. The following cases will be considered:

(i) $\omega = 1$ and $h^{0,1} = h^{1,0} = 1$ (abelian surfaces),

(ii) $\omega = 3$ and $h^{3,0} = h^{2,1} = h^{1,2} = h^{0,3} = 1$.

Case (i) is the content of Chap. 3 of [3]. A sketch of the proof of the considerably easier case (ii) will be given, following [4, Chap. 2].
F. Fité

Lecture 4. The Galois type of an abelian surface

The notion of Galois type of an abelian surface defined over a number field. The dictionary between Galois types and Sato-Tate groups of abelian surfaces defined over number fields [3, Chap. 4]).
F. Fité

Lecture 5. Moment sequences

Moment sequences as a tool for identifying and classifying Sato-Tate distributions. Computing moment sequences of Sato-Tate groups, Weyl integration formulas, comparing moment statistics, distinguishing exceptional distributions with additional statistics.
A.V. Sutherland

Lecture 6. Computing zeta functions

Survey of methods for computing zeta functions of low genus curves (as in [9]), including generic group algorithms, p-adic cohomology, CRT-based methods (Schoof-Pila), and recent average polynomial-time algorithms [6].
A.V. Sutherland

2 Tutorials

2.1 Sato-Tate distributions of $y^2 = x^7 - cx$

The goal of this tutorial is to study the Sato-Tate group of the Jacobian of hyperelliptic curves of the form

$$C_1 : y^2 = x^7 - cx \qquad (c \in \mathbb{Z}), \tag{1}$$

using the trace distribution as a tool for investigation.

In Sage one can use the `frobenius_polynomial` method to compute the trace of Frobenius of C_1 mod p, at any prime p of good reduction, but this is too slow for our purposes. Fortunately, the special form of the curve C_1 allows us to compute the trace of $C_1 \bmod p$ more efficiently.

Definition 2.1. Let p be an odd prime, let $C/\mathbb{F}_p$ be a hyperelliptic curve $y^2 = f(x)$ of genus g, where f is a polynomial of degree $d = 2g+1$ or $d = 2g+2$. The *Hasse-Witt matrix* of C is the $g \times g$ matrix $W = (w_{ij})$ defined by

$$w_{ij} = f_{pi-j}^{(p-1)/2} \qquad (1 \le i, j \le g),$$

where f_m^n denotes the coefficient of x^m in the expansion of $f(x)^n$.

Theorem 2.2. *Let $C/\mathbb{F}_p$ be a hyperelliptic curve. Let $\chi(\lambda)$ be the characteristic polynomial of the Frobenius endomorphism π of $\mathrm{Jac}(C)$ and let W be the Hasse-Witt matrix of C. Then*

$$\chi(\lambda) \equiv (-1)^g \lambda^g \det(W - \lambda I) \bmod p.$$

In particular, $\operatorname{tr} W \equiv \operatorname{tr} \pi \bmod p$.

The Weil bounds imply that $|t_p| \le 2g\sqrt{p}$; thus for all sufficiently large p the trace of W_p uniquely determines the trace of Frobenius.

Exercise 2.3. Let t_p be the trace of the Hasse-Witt matrix of $C_1 \bmod p$. Derive an explicit formula for t_p in terms of c and the binomial coefficients $\binom{n}{n/2}$ and $\binom{n}{n/6}$, where $n = (p-1)/2$ (define $\binom{n}{r} = 0$ for $r \notin \mathbb{Z}$). Prove $t_p \equiv 0 \bmod p$ for all $p \equiv 3 \bmod 4$.

To efficiently apply your formula for t_p, you will need the following congruences for binomial coefficients.

Lemma 2.4. *Let $p = 4m+1 = x^2 + y^2$ be prime, with $x \equiv -(\frac{2}{p}) \bmod 4$. Then*

$$\binom{2m}{m} \equiv 2(-1)^{m+1} x \bmod p.$$

Proof. See [2, Thm. 9.2.2]. □

Lemma 2.5. *Let $p = 12m+1 = x^2 + y^2$ be prime, with $x \equiv -(\frac{2}{p}) \bmod 4$, and define δ to be -1 if $x \equiv 0 \bmod 3$ and $+1$ otherwise. Then*

$$\binom{6m}{m} \equiv 2\delta(-1)^{m+1} x \bmod p.$$

Proof. See [2, Thm. 9.2.10]. □

Exercise 2.6. Using your formula from Exercise 2.3 and the lemmas above, use `sage` (or the programming environment of your choice) to implement a fast algorithm to compute t_p for any prime p of good reduction for C_1. (Recall that Cornacchia's algorithm provides an efficient way to write any prime $p \equiv 1 \bmod 4$ as the sum of two squares). Check your results using `frobenius_polynomial`.

Exercise 2.7. Implement an algorithm to compute the moments of the normalized traces $x_p = t_p/\sqrt{p}$ as p ranges over primes of good reduction up to a given bound N. Use this to provisionally determine the integer values of the 2nd, 4th, and 6th moments of x_p as p varies over good primes up to a bound N tending to infinity. How do the results vary with c?

Exercise 2.8. By restricting to primes $p \equiv 1 \bmod 4$, repeat the exercise above for $C_1/\mathbb{Q}(i)$.

Exercise 2.9. Let $h \in \mathbb{Z}[x]$ be a monic irreducible polynomial. By restricting to primes p for which h has a root modulo p, one can compute moment statistics for C_1/k, where $k = \mathbb{Q}(x)/(h)$, since the normalized traces $x_\mathfrak{p}$ for the degree-1 primes $\mathfrak{p}$ of k account for the overwhelming majority of $x_\mathfrak{p}$ values when enumerating over primes $\mathfrak{p}$ of bounded norm. Using this observation, compute moment statistics for C_1/k over various number fields, and attempt to find number fields where the moment statistics (and the proportion of zero traces) change significantly (with c held fixed).

Exercise 2.10. Say whatever you can about the Sato-Tate group of $C_1/\mathbb{Q}$. For example, how many components does it have? How many of these components have trace zero? What is the identity component?

2.2 Sato-Tate distributions of $y^2 = x^8 + c$

Repeat Exercises 2.1–2.10 for the curve

$$C_2 : y^2 = x^8 + c \qquad (c \in \mathbb{Z}), \tag{2}$$

subject to the following amendments. Prove $t_p \equiv 0 \bmod p$ for $p \equiv 2 \bmod 3$ (rather than $p \equiv 3 \bmod 4$), and your formula for t_p should use the binomial coefficients $\binom{n}{n/2}$ and $\binom{n}{n/4}$. To compute the latter, use the following lemma.

Lemma 2.11. *Let $p = 8m + 1 = x^2 + 2y^2$ be prime, with $x \equiv 3 \bmod 4$. Then*

$$\binom{4m}{m} \equiv 2(-1)^{m+1} x \bmod p.$$

Proof. See [2, Thm. 9.2.8]. □

References

[1] G. Banaszak and K.S. Kedlaya, *An algebraic Sato-Tate group and Sato-Tate conjecture*, arXiv:1109.4449v1 (2011).

[2] B. Berndt, R. Evans, K. Williams, *Gauus and Jacobi Sums*, Wiley, 1998.

[3] F. Fité, K.S. Kedlaya, V. Rotger, and A.V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus* 2, Compositio Mathematica **148** (2012), 1390–1442.

[4] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato-Tate groups of some weight-*3 *motives*, preprint, `http://arxiv.org/abs/1212.0256`.

[5] F. Fité and A.V. Sutherland, *Sato-Tate distributions of twists of* $y^2 = x^5 - x$ *and* $y^2 = x^6 + 1$, Algebra and Number Theory, to appear.

[6] D. Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Annals of Mathematics **179** (2014), 783–803.

[7] C. Johansson, *On the Sato-Tate conjecture for non-generic abelian surfaces*, preprint, `http://arxiv.org/abs/1307.6478`.

[8] N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society, 1999.

[9] K.S. Kedlaya and A.V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic Number Theory 8th International Symposium (ANTS VIII), LNCS **5011**, Springer, 2008, 312–326.

[10] K.S. Kedlaya and A.V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, Arithmetic, Geometry, Cryptography, and Coding Theory (AGCT-11), Contemporary Mathematics **487**, American Mathematical Society, 2000, 119–162.

[11] J.-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, Research Notes in Mathematics **7**, A.K. Peters, 1998.

[12] J.-P. Serre, *Lectures on* $N_X(p)$, Research Notes in Mathematics **11**, CRC Press, 2012.