COMPUTING ZETA FUNCTIONS AND L-FUNCTIONS OF CURVES
CMI-HIMR SUMMER SCHOOL IN COMPUTATIONAL NUMBER THEORY (2019)

ANDREW V. SUTHERLAND

OVERVIEW

Let X be a nice (smooth projective geometrically integral) curve of genus g over a field k. When k is a finite field $\mathbb{F}_q$, the curve X has an associated zeta function

$$Z_X(T) := \exp\left(\sum_{r\geq 1} \frac{\#X(\mathbb{F}_{q^r})}{r} T^r\right) = \frac{L_X(T)}{(1-T)(1-qT)},$$

where the L-polynomial $L_X \in \mathbb{Z}[T]$ has the form

$$L_X(T) = q^g T^{2g} + q^{g-1}a_1 T^{2g-1} + \cdots + qa_{g-1}T^{g+1} + a_g T^g + a_{g-1}T^{g-1} + \cdots + a_1 T + 1$$

and roots $\alpha_1, \ldots, \alpha_{2g}$ that satisfy $|\alpha_i| = q^{-1/2}$.

When k is a number field K, the curve X has an associated L-function

$$L_X(s) := \prod_{\mathfrak{p}} L_{X_\mathfrak{p}}(|\mathfrak{p}|^{-s})^{-1},$$

where $\mathfrak{p}$ ranges over the primes of K (nonzero prime ideals of $\mathcal{O}_K$) and $X_\mathfrak{p}$ denotes the reduction of X to the residue field $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$. For all but finitely many primes $\mathfrak{p}$ (the good primes), $X_\mathfrak{p}$ is a nice curve of genus g and the polynomial $L_{X_p}(T)$ is the numerator of the zeta function $Z_{X_\mathfrak{p}}(T)$. Under the widely believed assumption that $L_X(s)$ satisfies the functional equation required by the Langlands correspondence, the polynomials $L_{X_\mathfrak{p}}(T)$ at bad $\mathfrak{p}$ can be explicitly computed given sufficiently many $L_{X_\mathfrak{p}}(T)$ at good $\mathfrak{p}$, so we shall restrict our attntion to good primes.

The zeta functions $Z_X(T)$ and the L-functions $L_X(T)$ are canonical invariants of the isogeny class of the Jacobian of X, an abelian variety of dimension g, and the main objects of some of the most important theorems and conjectures in arithmetic geometry, including generalizations of the modularity theorem, the Sato-Tate conjecture, and the conjecture of Birch and Swinnerton-Dyer. The goal of this lecture series is to describe some explicit methods for computing them.

COURSE OUTLINE

Lecture 1. Introduction. (slides)

- Zeta functions and L-functions of curves and their Jacobians
- Strong multiplicity one
- Mumford representation
- Cantor's algorithm

Lecture 2. Generic and ℓ-adic algorithms. (slides)

- Mestre's approach
- Birthday paradox algorithms
- Schoof's algorithm
- Generalizations to higher genus

Lecture 3. An average polynomial-time algorithm. (slides)

- The Hasse invariant
- Linear recurences
- An $p^{1/2+o(1)}$ time algorithm
- An average polynomial-time

Lecture 4. p-adic and average polynomial-time algorithms. (slides)

- Reduction to hypersurfaces in affine tori
- The trace formula
- Recursion formulas
- Implementation

Exercises

Exercises for Lecture 1. Let $X/\mathbb{F}_p$ be a nice curve of genus g with zeta function

$$Z(T) := \exp\left(\sum_{r\geq 1}\frac{N_r}{r}T^r\right) = \frac{L(T)}{(1-T)(1-qT)},$$

where $N_r := \#X(\mathbb{F}_{p^r})$.

(1) Prove that $L(T) = p^g T^{2g} + p^{g-1}a_1 T^{2g-1} + \cdots a_g T^g + \cdots a_1 T + 1$ is completely determined by the integers $N_r := \#X(\mathbb{F}_{p^r})$ for $1 \leq r \leq g$ and work out explicit formulas for $a_1, \ldots, a_g$ and N_{g+1} in terms of $N_1, \ldots N_g$ for $g \leq 3$.

(2) Prove that $\#\operatorname{Jac}(X)(\mathbb{F}_p) = L_X(1)$, and more generally, that

$$\#\operatorname{Jac}(X)(\mathbb{F}_{p^r}) = \prod_{n=1}^{r} L(e^{2\pi i n/r}).$$

Show that if X is a hyperelliptic curve and $\tilde{X}$ is a non-isomorphic quadratic twist then $\#\operatorname{Jac}(X)(\mathbb{F}_{p^2}) = \#\operatorname{Jac}(X)(\mathbb{F}_p)\#\operatorname{Jac}(\tilde{X})(\mathbb{F}_p)$ (assume $p \neq 2$ if you wish). Then show that for $g \leq 3$ and all sufficiently large p the zeta function $Z(T)$ is completely determined by the integers $\#\operatorname{Jac}(X)(\mathbb{F}_p)$ and $\#\operatorname{Jac}(\tilde{X})(\mathbb{F}_p)$.

(3) Assume X is defined by $y^2 = f(x)$ with f monic, square-free, of degree $2g+1$ ($p \neq 2$). Show that the 2-torsion field of $\operatorname{Jac}(X)$ is the splitting field of $f(x)$ and prove that

$$\#\operatorname{Jac}(X)(\mathbb{F}_p)[2] = 2^{n-1},$$

where n is the number of irreducible factors of f in $\mathbb{F}_p[x]$. From this, conclude that $\operatorname{Jac}(X)(\overline{\mathbb{F}}_p)[2] \simeq (\mathbb{Z}/2\mathbb{Z})^{2g}$.

(4) Assume X is an elliptic curve $y^2 = f(x)$ with f a monic cubic, and $O := (0:1:0)$. If we identify points $P \in X(\mathbb{F}_p)$ with divisor classes $[P - O]$ in $\mathrm{Jac}(X)(\mathbb{F}_p)$ (this is the isomorphism induced by the Abel-Jacobi map), then Cantor's algorithm reduces to the usual group law on X (three points on a line sum to O). Work this out explicitly for the case of adding two distinct reduced divisors (corresponding to distinct points on X).

(5) Assume X has genus 2. Show that (1) and (2) imply

$$\#\,\mathrm{Jac}(X)(\mathbb{F}_p) = \frac{N_2 + N_1^2}{2} - p.$$

Give a bijective combinatorial proof of this formula in the case that X has a rational Weierstrass point by using the Mumford representation for $\mathrm{Jac}(X)$ to express the LHS in terms of the RHS. Which divisors counted by the first term on the RHS are being removed by the second term on the RHS to obtain the LHS?

Day 2.

(1) Modify the Sage implementation of Schoof's algorithm presented in lecture (click here) to compute the order of the Frobenius action on $\mathrm{End}(E[\ell])$. Give an explicit example of isogenous elliptic curves E_1 and E_2 over a finite field for which $E_1(\mathbb{F}_p)[5] \simeq E_2(\mathbb{F}_p)[5]$ (as abelian groups), but the Frobenius actions on $E_1[5]$ and $E_2[5]$ have different orders.

(2) Modify the Sage implementation of Schoof's algorithm presented in lecture (click here) to use Elkies optimization, that is, use precomputed modular polynomials (available here) to determine which primes are Elkies primes and for these primes compute the Elkies kernel polynomial using [9, Alg. 28, p. 555].

(3) Mestre's approach to computing $\#\,\mathrm{Jac}(X)(\mathbb{F}_p)$ for elliptic curves $X/\mathbb{F}_p$ relies on the fact that for all sufficiently large primes p at least one of $\lambda(\mathrm{Jac}(X)(\mathbb{F}_p))$ or $\lambda(\mathrm{Jac}(\tilde{X})(\mathbb{F}_p))$ has a unique multiple in the Hasse-Weil interval (here $\tilde{X}$ denotes the quadratic twist). Prove that this approach is doomed to fail in genus 2 by showing that for every prime p there is a genus 2 curve $X/\mathbb{F}_p$ such that neither $\lambda(\mathrm{Jac}(X)(\mathbb{F}_p))$ nor $\lambda(\mathrm{Jac}(\tilde{X})(\mathbb{F}_p))$ has a unique multiple in the Hasse-Weil interval $[(\sqrt{p}-1)^4, (\sqrt{p}+1)^4]$.

(4) Let G be a finite abelian group with exponent $\lambda(G)$. Show that for uniformly distributed independent random elements $\alpha, \beta \in G$ we have

$$\mathrm{Prob}[\mathrm{lcm}(|\alpha|, |\beta|) = \lambda(G)] > \frac{6}{\pi^2} = 0.607927\ldots$$

Day 3. Free day! But feel free to do any of the problems from days 1 and 2.

Day 4. The file ZetaPlaneCurvesProblem.m contains the skeleton of the code that was demonstrated in lecture. Your task is to fill in missing bodies of the functions `mat`, `pts`, and `zeta`:

- The function `mat` computes the matrix $M_s \bmod p^e$ for the hypersurface in the affine torus $\mathbb{T}^2_{\mathbb{Z}}$ defined by f; you can do this naïvely by directly applying the definition of M_s.
- The function `pts` uses `mat` to evaluate the trace formula to compute $\#X(\mathbb{F}_{p^r}) \bmod p^e$ by first viewing f as defining a hypersurface in an affine torus, and then adding missing points (using the provided function `MissingPoints`) to get the correct count for the nice curve $X/\mathbb{F}_p$ defined by $f(x,y,z) = 0$.

- The function `zeta` uses `pts` to compute the L-polynomial of X using the point counts computed by `pts`. Use the provided function `TracesToLPolynomial` to convert the list of integers $p+1-\#X(\mathbb{F}_{p^r})$ for $1 \le r \le g$ to the corresponding L-polynomial.

Once you have implemented your function, test it on the provided polynomials f_3 and f_4 at small good primes $p > 1 + e/r$ (you can compare your results with the provided functions `Pts` and `Zeta`). Then compute the L-polynomials of the plane quintic curve defined by f_5 at primes $p = 7, \ldots, 29$ (or as far as you can go).

For reference the running times for $p = 7, 11, 13, 17, 19, 23, 29$ using the code I showed in lecture are $13, 35, 38, 88, 124, 174, 357$ seconds on my laptop (but your mileage may vary).

References

[1] S. Abelard, Counting points on hyperelliptic curves in large characteristic: algorithms and complexity, Université de Lorraine, 2018. HAL archives-ouvert: tel-01876314f.

[2] S. Abelard, P. Gaudry, and P.-J. Spaenlehauer, *Counting points on genus 3 hyperelliptic curves with explicit real multiplication*, in *Thirteenth Algorithmic Number Theory Symposium (ANTS XIII)*, Open Book Series **2** (2019), 1–22.

[3] J. D. Achter and E. W. Howe, *Hasse–Witt and Cartier–Manin matrices: A warning and a request*, in *Arithmetic Geometry: Computation and Applications* (Y. Aubry, E. W. Howe, and C. Ritzenthaler, eds.), Contemp. Math. **722** (2019), American Mathematical Society, 1–18.

[4] L. M. Adleman and M.-D. Huang, *Counting points on curves and abelian varieties over finite fields*, J. Symbolic Comput. **32** (2001), 171–189.

[5] Ju. I. Manin, *The Hasse-Witt matrix of an algebraic curve*, AMS Translations, Series 2 **45** (1965), 245–264.

[6] A. Bostan, P. Gaudry, and E. Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier-Manin operator on hyperelliptic curves*, Finite Fields and Applications (2003), 43–58.

[7] A. Bostan, P. Gaudry, and E. Schost, *Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator*, SIAM J. Comput. **36** (2007), 1777–1806.

[8] D.G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp. **45** (1987), 95–101.

[9] S.D. Galbraith, *Mathematics of Public Key Cryptography, Version 2*, 2018.

[10] S.D. Galbraith, M. Harrison, and D.J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors* in *Algorithmic Number Theory 8th International Symposium (ANTS VIII)*, Lecture Notes in Comput. Sci. **5011**, Springer, 2008, 342–356.

[11] P. Gaudry and E. Schost, *Genus 2 point counting over prime fields*, J Symbolic Computation **47** (2012), 368–400.

[12] D. Harvey, *Kedlaya's algorithm in larger characteristic*, International Mathematics Research Notices **2007**.

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

[14] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proceedings of the London Mathematical Society **111** (2015), 1379–1401.

[15] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, in *Algorithmic Number Theory 11th International Symposium (ANTS XI)*, LMS Journal of Computation and Mathematics **17** (2014), 257–273.

[16] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*, in *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, Contemporary Mathematics **663** (2016), AMS, 127–148

[17] K.S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, Journal of the Ramanujan Mathematical Society **16** (2001), 323–338.

[18] K.S. Kedlaya, *Computing zeta functions via p-adic cohomology*, in *Algorithmic Number Theory 6th International Symposium (ANTS VI)*, Lecture Notes in Computer Science **3076**, Springer 2004, 1–17.

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

[20] D. Kohel, Pierrick Gaudry, and Eric Schost, *Counting points on genus 2 curves with real multiplication*, Advances in Cryptology – ASIACRYPT (2011), 504–519.

[21] J. Pila, *Frobenius Maps of Abelian Varieties and Finding Roots of Unity in Finite Fields*, Math. Comp. **55** (1990), 745–763.

[22] B. Poonen, *Computational aspects of curves of genus at least* 2, in *Algorithmic Number Theory 2nd International Symposium (ANTS II)*, Lecture Notes in Computer Science **1122**, Springer 1996, 283–306.

[23] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1995), 483–494.

[24] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Théorie des Nombres de Bordeaux **7** (1995), 219–254.

[25] I. Shparlinski and A.V. Sutherland, *On the distribution of Atkin and Elkies primes, on average*, LMS J. Comp. Math. **18** (2015) 308–322.

[26] K.-O. Stöhr and José Felipe Voloch, *A formula for the Cartier operator on plane algebraic curves*, J. Reine Angew. Math. **377** (1987), 49–64.

[27] A.V. Sutherland, *Structure computation and discrete logarithms in finite abelian p-groups*, Mathematics of Computation **80** (2011), 477–500.

[28] A.V. Sutherland *Fast Jacobian arithmetic for hyperelliptic curves of genus* 3, in *Thirteenth Algorithmic Number Theory Symposium (ANTS XIII)*, Open Book Series **2** (2019), 425–442.

[29] N. Yui, *On the Jacobian varieties of hyperelliptic curves over fields of characteristic $p > 2$*, J. Algebra **52** (1978), 378–410.