Computing zeta functions and L-functions
Lecture 4

Andrew V. Sutherland

June 27, 2019

CMI-HIMR Summer School in Computational Number Theory

Arithmetic schemes

Let X be a scheme of finite type over $\operatorname{Spec}\mathbb{Z}$, in other words, an arithmetic scheme.
The Hasse–Weil zeta function (or arithmetic zeta function) of X is defined by

$$\zeta_X(s) := \prod_{x \in X} (1 - N(x)^{-s})^{-1} = \prod \zeta_{X_p}(s) = \prod Z_{X_p}(p^{-s})$$

where the product is taken over closed points x, the norm $N(x) := \#\kappa(x)$ is the cardinality of the residue field $\kappa(x)$ at x, and $X_p := X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}(\mathbb{Z}/p\mathbb{Z})$ is the reduction of X modulo p.
The local zeta function $Z_{X_p}(T)$ is defined by the formal power series

$$Z_{X_p}(T) := \exp\left(\sum_{r \geq 1}^{\infty} \#X_p(\mathbb{F}_{p^r}) \frac{T^r}{r}\right) \in 1 + T\mathbb{Z}[[T]],$$

which is known to lie in $\mathbb{Q}(T)$ (by work of Dwork and Grothendieck).

The set of $\mathbb{F}_{p^r}$-rational points $X_p(\mathbb{F}_{p^r}) := \operatorname{Hom}_{\mathbb{F}_p}(\operatorname{Spec}(\mathbb{F}_{p^r}), X)$ satisfies

$$\#X_p(\mathbb{F}_{p^r}) = \sum_{e \mid r} e \#\{x \in X : \kappa(x) \simeq \mathbb{F}_{p^e}\}.$$

Arithmetic zeta functions and L-functions

If X is a nice curve over $\mathbb{Q}$, by choosing an integral model $\mathcal{X}$ for X we can view $\mathcal{X}$ as an arithmetic scheme. We might then ask about the relationship between $L_X(s)$ and $\zeta_{\mathcal{X}}(s)$.

At all primes p where $\mathcal{X}$ has good reduction we will have $Z_{X_p}(T) = Z_{\mathcal{X}_p}(T)$, and in particular, the L-polynomials $L_{X_p}(T)$ and $L_{\mathcal{X}_p}(T)$ in their numerators will agree.

From our "multiplicity one" perspective, this is all we need; the local zeta functions $Z_{\mathcal{X}_p}(T)$ at primes of good reduction for $\mathcal{X}$ uniquely determine $L_X(s)$ (for any integral model $\mathcal{X}$ of X).

In general the L-polynomial $L_{X_p}(T)$ in the Euler product $L_X(s) = \prod_p L_{X_p}(p^{-s})$ may (but need not) differ from the numerator of the local zeta functions $Z_{\mathcal{X}_p}(T)$ at bad primes.

For example, if X is the elliptic curve `49a1` and $\mathcal{X}$ is the arithmetic scheme defined by its minimal Weierstrass equation $y^2z + xyz = x^3 - x^2z - 2xz^2 - z^3$, then

$$L_{\mathcal{X}_7}(T) = -7T^2 + 1 \neq 1 = L_{X_7}(T).$$

On the other hand, when X is the elliptic curve `11a1` we actually have $L_X(s) = \zeta_{\mathcal{X}}(s)$.

Harvey's results for arithmetic schemes

Theorem (Harvey 2014)

Let X be an arithmetic scheme. The following hold:

1. *There is a deterministic algorithm that, given a prime p, outputs $Z_{X_p} \in \mathbb{Q}[T]$ in $p(\log p)^{1+o(1)}$ time using $O(\log p)$ space.*
2. *There is a deterministic algorithm that, given a prime p, outputs $Z_{X_p} \in \mathbb{Q}[T]$ in $\sqrt{p}\,(\log p)^{2+o(1)}$ time using $O(\sqrt{p}\log p)$ space.*
3. *There is a deterministic algorithm that, given an integer N outputs $Z_{X_p} \in \mathbb{Q}[T]$ for all $p \le N$ in time $N(\log N)^{3+o(1)}$ using $O(N\log^2 N)$ space.*

In these complexity estimates, X is fixed, only p or the bound N are part of the input (the arithmetic scheme X is effectively "hardwired" into the algorithm).

If one constrains X and fixes its representation (a curve with a plane model, for example), one can make the dependence on X completely explicit.

This theorem is not merely an existence statement, its proof involves explicit algorithms.

Hypersurfaces in affine tori

Let $\mathbb{P}^n_{\mathbb{Z}}$ denote n-dimensional projective space over $\mathbb{Z}$. The affine torus $\mathbb{T}^n_{\mathbb{Z}}$ consists of all projective points in $\mathbb{P}^n_{\mathbb{Z}}$ whose coordinates are all nonzero; it is an open subscheme of $\mathbb{P}^n_{\mathbb{Z}}$.

A hypersurface in $\mathbb{T}^n_{\mathbb{Z}}$ is the zero locus of a nonconstant homogeneous polynomial.

Lemma

Let X be an arithmetic scheme. The zeta function $\zeta_X(s)$ can be written as a finite product

$$\zeta_X(s) = \prod_i \zeta_{X_i}(s)^{e_i},$$

where each X_i is a hypersurface in $\mathbb{T}^{n_i}_{\mathbb{Z}}$ and $e_i = \pm 1$. Moreover, for each prime p we have

$$\zeta_{X_p}(s) = \prod_i \zeta_{X_{i,p}}(s)^{e_i}.$$

Proof of the lemma

Proof.

1. Write $X = V_1 \sqcup \cdots \sqcup V_n$ with $V_i = \operatorname{Spec} A_i$ for some $\mathbb{Z}$-algebra A_i by covering X with affine opens $U_1, \ldots, U_n$, setting $V_1 := U_1$, and recursively treating $X' = (U_2 \cup \cdots \cup U_n) \backslash U_1$ covered by $n-1$ affine opens $U_2', \ldots U_n'$, with $U_i' := U_i \backslash U_1$.
2. Now $X = \operatorname{Spec} \mathbb{Z}[x_1, \ldots, x_m]/(F_1, \ldots, F_k)$. For each non-empty $S \subseteq \{1, \ldots, k\}$ define $X_S := \operatorname{Spec} \mathbb{Z}[x_1, \ldots, x_m]/(\prod_{i \in S} F_i)$. Then $\zeta_X(s) = \prod_S \zeta_{X_S}(s)^{e_S}$, where $e_S = \pm 1$ is positive if $|S|$ is odd and negative otherwise (the inclusion/exclusion trick).
3. Assume $X = \operatorname{Spec} \mathbb{Z}[x_1, \ldots, x_m]/(F)$. For each non-empty $S \subseteq \{1, \ldots, m\}$ define $F_S = F(x_i = 0 : i \in S)$ and let X_S be the zero locus of F_S in the affine torus $\mathbb{T}_{\mathbb{Z}}^{|S|}$ with coordinates $\{x_0\} \cup \{x_i : i \in S\}$. Then $\zeta_X(s) = \prod_S \zeta_{X_S}(s)$.

Now note that 1–3 are all compatible with taking Euler products $\square$

Notation

Using $\boldsymbol{x} := (x_0, \ldots, x_n)$ to denote our coordinates and $\boldsymbol{u} := (u_0, \ldots, u_n) \in \mathbb{Z}_{\geq 0}^{n+1}$ to denote an exponent vector, we define the monomial

$$\boldsymbol{x}^{\boldsymbol{u}} := x_0^{u_0} \cdots x_n^{u_n}$$

and let $\deg(u) := u_0 + \cdots + u_n = \deg(\boldsymbol{x}^{\boldsymbol{u}})$.

We define $B_d := \{\boldsymbol{u} : \deg(\boldsymbol{u}) = d\}$, and use $\{\boldsymbol{x}^{\boldsymbol{u}} : \boldsymbol{u} \in B_d\}$ as a $\mathbb{Z}$-basis for the free $\mathbb{Z}$-module $\mathbb{Z}[x]_d$ of rank $\#B_d = \binom{d+n}{n}$ consisting of all homogeneous integer polynomials of degree d in $n+1$ variables.

For $F \in \mathbb{Z}[\boldsymbol{x}]_d$, $\boldsymbol{u} \in B_d$ and $e \in \mathbb{Z}_{\geq 0}$ we define $F_{\boldsymbol{u}}^s$ to be the coefficient of the monomial $\boldsymbol{x}^{\boldsymbol{u}}$ in the polynomial $F^s \in \mathbb{Z}[\boldsymbol{x}]_{ds}$.

The notation $F_{\boldsymbol{u}}^s$ is the multivariate analog of the notation f_u^s that we used in the previous lecture to denote the coefficient of x^u in f^s.

The trace formula

Lemma (Harvey 2014)

Let X be a hypersurface in $\mathbb{T}^n_{\mathbb{Z}}$ defined by $F \in \mathbb{Z}[\boldsymbol{x}]_d$, let r and e be positive integers, and let $p \geq 1 + e/r$ be a prime. Then

$$\#X_p(\mathbb{F}_{p^r}) \equiv (p^r - 1)^n \sum_{s=0}^{e} (-1)^s \binom{e}{s} \operatorname{tr}(M_s^r) \bmod p^e,$$

where M_s is the $m \times m$ integer matrix $M_s := \left[F^{s(p-1)}_{p\boldsymbol{v}-\boldsymbol{u}}\right]_{\boldsymbol{v},\boldsymbol{u}\in B_{ds}}$, with $m = \#B_{ds} = \binom{ds+n}{n}$.

Let $D = 2(4d+4)^n$. To compute $\zeta_{X_p}(s)$ it suffices to compute $\#X(\mathbb{F}_{p^r})$ for all $1 \leq r \leq D$ (by a theorem of Bombieri), and it is enough to compute $\#X(\mathbb{F}_{p^r}) \bmod p^e$ with $e = 2nD$.

If $F(x,y,z) = 0$ is a smooth plane curve of genus g, we only need to consider $1 \leq r \leq g$, and for all sufficiently large p we can take $e = \lceil \frac{g+1}{2} \rceil$ (in general, $e = \lceil \frac{g}{2} \log_p (2\binom{2g}{g}) \rceil$ suffices).
(note that $\lceil \frac{g+1}{2} \rceil = O(g)$ and for $n = 2$ we have $2nD = O(d^2) = O(g)$, so this is an $O(1)$ difference)

Recurrence relations

Fix $s \geq 1$ and $\boldsymbol{v} \in B_{ds}$. We want to compute the $\boldsymbol{v}$th row of M_s.

Fix $h := \max(ds, (d-1)(n+1)+1)$ and $\boldsymbol{w} \in B_h$, and let $m := \#B_h = \binom{h+n}{n}$.
For $k \geq 1$ and $H \in \mathbb{Z}[\boldsymbol{x}]_{kds}$, let $[H]_k$ to be the column vector $(H_{k\boldsymbol{v}+\boldsymbol{w}-\boldsymbol{t}})^{\mathrm{T}}$ indexed by $t \in B_h$.

For each $t \in B_h$, pick i with $t_i \geq d$ and let $t' \in B_{h-d}$ satisfy $t'_i = t_i - d$ and $t'_j = 0$ for $j \neq i$.
Given $F \in \mathbb{Z}[\boldsymbol{x}]_d$, define the matrix $Q \in \mathbb{Z}[k, \ell]^{m \times m}$ as follows: for each $z \in B_h$ let

$$Q_{t,z} := (kv_i + w_i - t'_i - (\ell+1)(z_i - t'_i))F_{z-t'}.$$

Lemma

Let $G := x_0^d + \cdots + x_n^d$, let $F \in \mathbb{Z}[\boldsymbol{x}]_d$, and let Q be defined as above. For all $c \geq 0$ we have

$$[F^{cs}]_c = \frac{1}{d^{cs}(cs)!} Q(c, cs-1) \cdots Q(c, 0)[G^{cs}]_c.$$

The coefficients of $[G^{cs}]_c$ are multinomial coefficients $\binom{n+d}{m_1, \ldots, m_n}$, which are easy to compute.
Using $c = p-1$, we can compute $M_s[\boldsymbol{v}, \boldsymbol{u}] = F^{s(p-1)}_{p\boldsymbol{v}-\boldsymbol{u}}$ as the $\boldsymbol{w} + \boldsymbol{u} - \boldsymbol{v}$ entry of $[F^{cs}]_c$.

Complexity analysis for smooth plane curves

Let $C/\mathbb{Q}$ be a smooth plane curve with an integral plane model $\mathcal{X}\colon F(x,y,z)=0$ of degree d, and X the hypersurface in $\mathbb{T}^2_{\mathbb{Z}}$ defined by F. Assume $d^{O(1)}$ and $\log\|F\|$ are $O(\log p)$

To compute $Z_{C_p}(T)$ at primes of good reduction for $\mathcal{X}$, it suffices to compute $\#C(\mathbb{F}_{p^r})$ for $1\le r\le g=\binom{d-1}{2}$. To do so we compute $\#X(\mathbb{F}_{p^r})$ and then add the number of projective points $(x_0:y_0:z_0)$ satisfying $F(x_0,y_0,z_0)=0$ and $x_0y_0z_0=0$; the latter can be computed in $(\log p)^{2+o(1)})$ time by counting the roots of 3 polynomials over $\mathbb{F}_{p^r}$ and checking 3 points. This means we can compute $Z_{C_p}(T)$ in $g(\log p)^{2+o(1)}$ time given $\#X(\mathbb{F}_{p^r})$ for $1\le r\le g$.

By the Weil bounds, it suffices to compute $\#X(\mathbb{F}_{p^r}) \bmod p^e$ with $e\ge\lceil\frac{r}{2}\log_p(2\binom{2g}{r}\rceil$, which is $\lceil\frac{r+1}{2}\rceil$ for all sufficiently large p, so let us fix $e=\lceil\frac{g+1}{2}\rceil$ (use the same e for all r).

By the trace formula, it suffices to compute $M_s \bmod p^e$ for $0\le s\le e$. We can compute $\operatorname{tr} M_s^r$ for $1\le r\le g$ by computing the charpoly of M_s and applying Newton identities (with $p>g$). Note that M_s has $\#B_{ds}=O((ds)^2)$ rows, which is $O(g^3)$.

Bottom line: given $M_s \bmod p^e$ for $1\le s\le e$ we can compute $Z_{C_p}(T)$ in $g^{11}(\log p)^{2+o(1)}$ time. $(\sum_{0\le s\le e}((ds)^2)^3 e(\log p)^{1+o(1)}=g^{11}(\log p)^{1+o(1)}$ since $e\approx g\approx d^2$).

Complexity analysis for smooth plane curves

There are four ways to compute $M_s \bmod p^e$ for $1 \le s \le e$;

1. Apply $M_s = [F^{s(p-1)}_{p\boldsymbol{v}-\boldsymbol{u}}]$; time $g^5p^2(\log p)^{1+o(1)}$.
   (multivariate Kronecker: $\sum_{0\le s\le e}((dsp)^2)^3 e(\log p)^{1+o(1)} = g^5p^2(\log p)^{1+o(1)}$)
2. Use $Q(k,\ell)$ to compute rows of M_s using matrix-vector mults: time $g^{11}p(\log p)^{1+o(1)}$.
   ($\sum_{0\le s\le e}((ds)^2 p((ds)^2)^2 e(\log p)^{1+o(1)} = g^{11}p(\log p)^{1+o(1)}$)
3. Apply BGS to compute $Q(k,\ell)$ products: time $g^{14}\sqrt{p}(\log p)^{2+o(1)}$.
   (as above, but now we need matrix-matrix mults, dimension is $O(g^3)$)
4. Use an average polynomial time approach for $p \le N$: time $g^{14}N(\log N)^{3+o(1)}$.

Except for 1, these complexities dominate the time to compute $Z_{C_p}(T)$ given the $M_s \bmod p^e$.
In case 1 we obtain a total complexity of $(g^5p^2 + g^{11}\log p)(\log p)^{1+o(1)}$.