Hypergeometric L-functions in average polynomial time

David Roe
(joint with Edgar Costa and Kiran Kedlaya)

Department of Mathematics
Massachusetts Institute of Technology

Joint Mathematics Meetings
AMS Special Session on Modular Forms,
Hypergeometric Functions, and Related Topics
January 9, 2025

Hasse-Weil L-functions

Let X be a nice algebraic variety over $\mathbb{Q}$. For $w = 0, \ldots, 2\dim(X)$, we get an associated **(incomplete) Hasse-Weil L-function** built out of **Euler factors**:

$$L_w(X, s) = \prod_p L_p(X, p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \qquad L_p(X, T) := \det(1 - T\,\mathrm{Frob}_p, H^w_{\mathrm{et}}(X, \mathbb{Q}_\ell)^{I_p}).$$

We can similarly define $L(M, s)$ for M a **motive** factor of $H^w(X)$; we refer to w as the **weight** of M and $r = \dim(M)$ as the **degree**. A prime p is **good** if I_p acts trivially, and **bad** otherwise. We have $\deg(L_p(X, T)) \leq r$, with equality iff p is good. One can define the conductor N as a certain product of powers of the bad primes, and the **completed L-function** $\Lambda(M, s)$ as the product of $L(M, s)$ with $N^{s/2}$ and a certain product of Gamma factors.

Goal

Gather numerical data for such L-functions: zero distribution, special values, analytic continuation and functional equation, murmurations. Want a diverse source of motives where $L(M, s)$ is computable, with varying weight, degree, and Hodge numbers.

Hypergeometric data

A **hypergeometric datum** over $\mathbb{Q}$ of degree r is defined by two disjoint tuples

$$(\alpha_1, \ldots, \alpha_r), (\beta_1, \ldots, \beta_r) \text{ over } \mathbb{Q} \cap [0, 1)$$

which are each **Galois-stable**: the multiplicity of any reduced fraction depends only on its denominator. For example

$$\alpha = (\tfrac{1}{4}, \tfrac{1}{2}, \tfrac{1}{2}, \tfrac{3}{4}),\ \beta = (\tfrac{1}{3}, \tfrac{1}{3}, \tfrac{2}{3}, \tfrac{2}{3}).$$

This datum defines a family of hypergeometric motives $M_z^{\alpha,\beta}$ over $z \in \mathbb{Q} \setminus \{0, 1\}$, and a family of degree r L-functions, where $F_p(T) := L_p\big(M_z^{\alpha,\beta}, T\big) = 1 - a_p T + \cdots \in \mathbb{Z}[T]$ is of degree at most r. The Hodge vector and motivic weight can be read from the **zigzag function**

$$Z_{\alpha,\beta}(x) := \#\{j : \alpha_j \leq x\} - \#\{j : \beta_j \leq x\}.$$

Hypergeometric families in the wild

- Legendre Family: $E_t\colon y^2 = x(1-x)(x-t)$

$$\mathrm{H}^1(E_t,\mathbb{Q}) \simeq M_t^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{2},\tfrac{1}{2}),\ \beta = (1,1).$$

- Dwork family: $X_\lambda\colon x^4+y^4+z^4+w^4-4\lambda xyzw = 0 \subset \mathbb{P}^3$

$$\mathrm{H}^2(X_\lambda,\mathbb{Q}) = Pic(X_\lambda)\oplus T_\lambda \quad (22 = 19+3)$$
$$T_\lambda \simeq M_{\lambda^4}^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{4},\tfrac{1}{2},\tfrac{3}{4}),\ \beta = (1,1,1).$$

- K3 family with Picard rank 16: $X_\lambda\colon x^3y+y^4+z^4+w^4-12\lambda xyzw = 0 \subset \mathbb{P}^3$

$$\mathrm{H}^2(X_\lambda,\mathbb{Q}) = Pic(X_\lambda)\oplus T_\lambda \qquad (22 = 16+6)$$
$$T_\lambda \simeq M_{2^{10}3^6\lambda^{12}}^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{12},\tfrac{1}{6},\tfrac{5}{12},\tfrac{7}{12},\tfrac{5}{6},\tfrac{11}{12}),$$
$$\beta = (0,0,0,\tfrac{1}{3},\tfrac{1}{2},\tfrac{2}{3}).$$

L-functions of hypergeometric motives

$$L(M_z^{\alpha,\beta}, s) = \prod_p F_p(p^{-s}) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

The primes p of **bad reduction** (i.e., $\deg F_p < r$) have the following forms.

- p is **wild** if $v_p(\gamma) < 0$ for some $\gamma \in \alpha \cup \beta$ (e.g., 2 and 3 in our last example).
- p is **tame** if it is not wild, and either $v_p(z) \neq 0$ or $v_p(z-1) \neq 0$.

Completing the L-function gives

$$\Lambda(s) := N^{s/2} \cdot \Gamma_{\alpha,\beta}(s) \cdot L\big(M_z^{\alpha,\beta}, s\big).$$

We expect Λ to satisfy the functional equation

$$\Lambda(s) = \pm\Lambda(w+1-s)$$

To numerically study the analytic properties of $\Lambda(s)$ and check its functional equation one needs to know

$$a_n \leq B, \text{ where } B = O(\sqrt{N}).$$

The Good, the Tame and the Wild

$$L(M_z^{\alpha,\beta}, s) = \prod_p F_p(p^{-s}) = \sum_{n\geq 1} \frac{a_n}{n^s} = L_{\mathrm{good}}(s)\cdot L_{\mathrm{tame}}(s)\cdot L_{\mathrm{wild}}(s)$$

We do not yet have formulas for F_p at the wild primes.
There is a recipe for F_p at the tame primes.
For p a good prime (neither wild nor tame), $F_p(T) = \det(1 - T\,\mathrm{Frob}_p \,|\, M_z^{\alpha,\beta})$ may be recovered from a trace formula of the shape

$$\mathrm{Tr}(\mathrm{Frob}_q) = H_q\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right) := \frac{1}{1-q}\sum_{m=0}^{q-2} \pm p^{\xi(m)}\left(\prod_{j=1}^{r}\frac{(\alpha_j)_m^*}{(\beta_j)_m^*}\right)[z]^m,$$

where $[z]$ is the multiplicative lift of $z \bmod p$ and $(\gamma)_m^*$ is a p-adic variant of the Pochhammer symbol $(\gamma)_m = \gamma(\gamma+1)\cdots(\gamma+m-1)$.

Hypergeometric L-functions in average polynomial time

$$a_p = H_p\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right) := \frac{1}{1-p}\sum_{m=0}^{p-2} \pm p^{\xi(m)} \left(\prod_{j=1}^{r} \frac{(\alpha_j)_m^*}{(\beta_j)_m^*}\right) [z]^m,$$

where $[z]$ is the multiplicative lift of $z \bmod p$ and $(\gamma)_m^*$ is a p-adic variant of the Pochhammer symbol $(\gamma)_m = \gamma(\gamma+1)\cdots(\gamma+m-1)$.

Theorem (Costa–Kedlaya–R, 2024)

We exhibit an algorithm to compute a_p for all primes $p \leq X$.
For fixed α, β, and z the time and space complexities are both $\widetilde{O}(X)$.

Our initial algorithm (2020) allowed computation of L-functions with motivic weight 1; the 2024 version dropped the restriction on weight.

`github.com/edgarcosta/amortizedHGM`

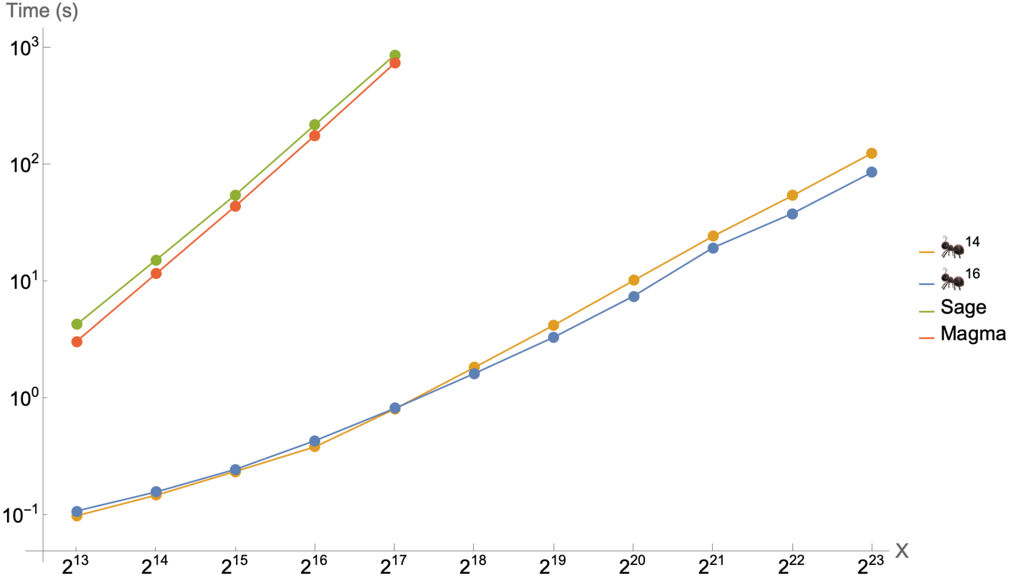
Amortization over primes

$$a_p = H_p\left(\begin{matrix}\alpha \\ \beta\end{matrix}\middle| z\right) := \frac{1}{1-p}\sum_{m=0}^{p-2} \pm p^{\xi(m)} \left(\prod_{j=1}^{r} \frac{(\alpha_j)_m^*}{(\beta_j)_m^*}\right) [z]^m,$$

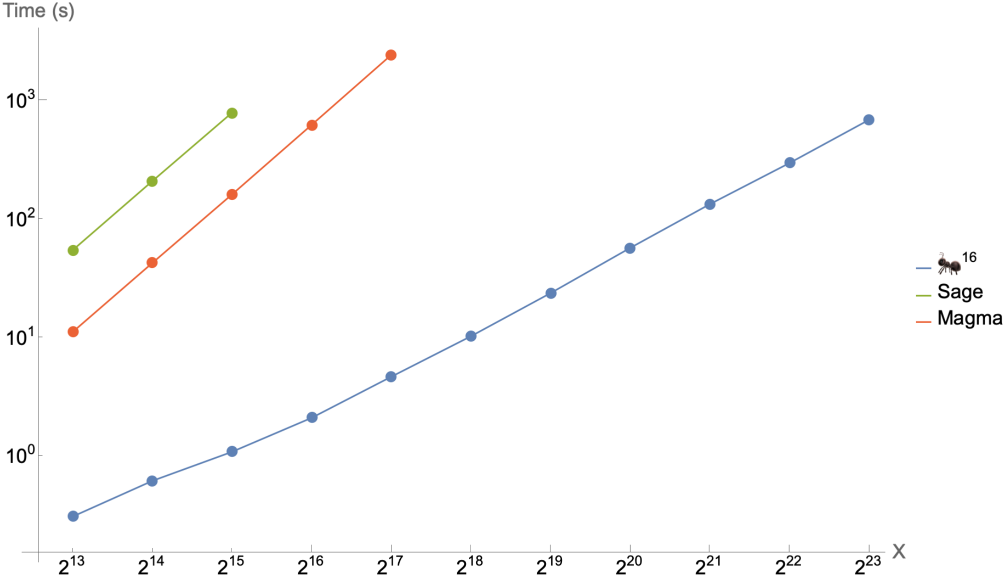
where $[z]$ is the multiplicative lift of $z \bmod p$ and $(\gamma)_m^*$ is a p-adic variant of the Pochhammer symbol $(\gamma)_m = \gamma(\gamma+1)\cdots(\gamma+m-1)$.

The implementations in `Magma` and `Sage` compute a_p one p at a time. Since the sum is over $O(p)$ terms, computing all prime Dirichlet coefficients up to X requires $\widetilde{O}(X^2)$ arithmetic operations.
The shape of the formula makes it feasible to amortize this complexity over p, thus requiring $\widetilde{O}(X)$ arithmetic operations.

Timings: working $\pmod{p^1}$, degree $= 4$, weight $= 1$



Timings: working $\pmod{p^3}$, degree $= 6$, weight $= 5$



Amortization ingredients

- Overall approach is via accumulating remainder trees, following Costa, Gerbicz, Harvey, and Sutherland;
- Use a generic prime, with computations in $\mathbb{Z}[P]/P^e$ amortized with polynomial arithmetic and then substituting $P = \frac{p}{1-p}$ afterward;
- Break amortization up by dividing $[0, p-2]$ into pieces based on locations of α and β;
- Divide primes into arithmetic progressions modulo the denominators from α and β;
- Precompute various p-adic gamma factors using a similar amortization method (independent of z, only mild dependence on α and β)
- Extract the desired sum from a product of block triangular matrices, using accumulating remainder trees to compute the product modulo all necessary p.

Accumulating remainder trees: Wilson primes

The Alhazen–Wilson theorem states that $(p-1)! \equiv -1 \pmod{p}$ for all primes p. A **Wilson prime** is one so that $(p-1)! \equiv -1 \pmod{p^2}$. The only known examples are $p = 5, 13, 563$.

Costa–Gerbicz–Harvey computed $(p-1)! + 1 \pmod{p^2}$ for all $p \le X = 2 \times 10^{13}$ using a new technique that reduced the overall complexity from $\widetilde{O}(X^2)$ to $\widetilde{O}(X)$.

The idea is to replace the separate computation of $(p-1)! + 1 \pmod{p^2}$ with the serial computation of

$$n! \pmod{\prod_{n<p\le X} p^2} \qquad \text{for } n = 0, \dots, X-1.$$

To make this work, this serialization must be balanced against making the moduli so large that they slow down the computation. Harvey–Sutherland generalized this process into **accumulating remainder trees**.

Accumulating remainder trees

Given integers (or matrices) $A_0, \ldots, A_{b-1}$ and integers $m_0, \ldots, m_{b-1}$, we want to compute simultaneously

$$C_j := A_0 \ldots A_{j-1} \pmod{m_j} \qquad (j = 0, \ldots, b-1).$$

For simplicity, assume $b = 2^\ell$. Form a complete binary tree of depth ℓ with nodes (i, j) where $i = 0, \ldots, \ell$ and $j = 0, \ldots, 2^i - 1$. By computing from the leaves to the root, we can compute products over diadic ranges:

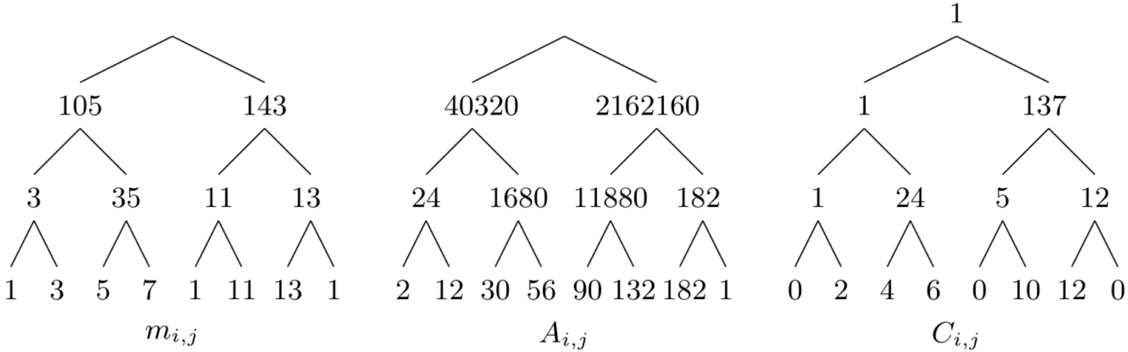
$$m_{i,j} := m_{j2^{\ell-i}} \ldots m_{(j+1)2^{\ell-i}-1},$$
$$A_{i,j} := A_{j2^{\ell-i}} \ldots A_{(j+1)2^{\ell-i}-1}.$$

Then from the root to the leaves, we compute the products $C_{i,j} := A_{i,0} \ldots A_{i,j-1} \pmod{m_{i,j}}$ by writing $C_{0,0} = 1$ and

$$C_{i,j} = \begin{cases} C_{i-1,\lfloor j/2 \rfloor} \pmod{m_{i,j}} & j \equiv 0 \pmod 2 \\ C_{i-1,\lfloor j/2 \rfloor} A_{i,j-1} \pmod{m_{i,j}} & j \equiv 1 \pmod 2. \end{cases}$$

Example: $(p-1)! \pmod{p}$ (Harvey–Sutherland 2014)

- Set $m_0, \ldots, m_7$ to be the first 8 odd numbers, with composites replaced by 1
- $A_i = (i+1)(i+2)$.
- $C_{i,j} = \begin{cases} C_{i-1,\lfloor j/2 \rfloor} \pmod{m_{i,j}} & j \equiv 0 \pmod 2 \\ C_{i-1,\lfloor j/2 \rfloor} A_{i,j-1} \pmod{m_{i,j}} & j \equiv 1 \pmod 2. \end{cases}$



Next steps

We want to add a bunch of interesting hypergeometric L-functions to the LMFDB. Two main obstacles:

1. We need to choose good specialization points z. In order to keep the conductor small, we want both z and $z-1$ to only have small prime factors. We can achieve this by solving S-unit equations, but this approach won't practically be able to ever guarantee all L-functions in a family below a certain conductor bound.
2. The wild L-factors are still not pinned down. Ongoing work by Roberts–Rodriguez Villegas may help, and we can numerically check possible factors using the functional equation.

Thank you!