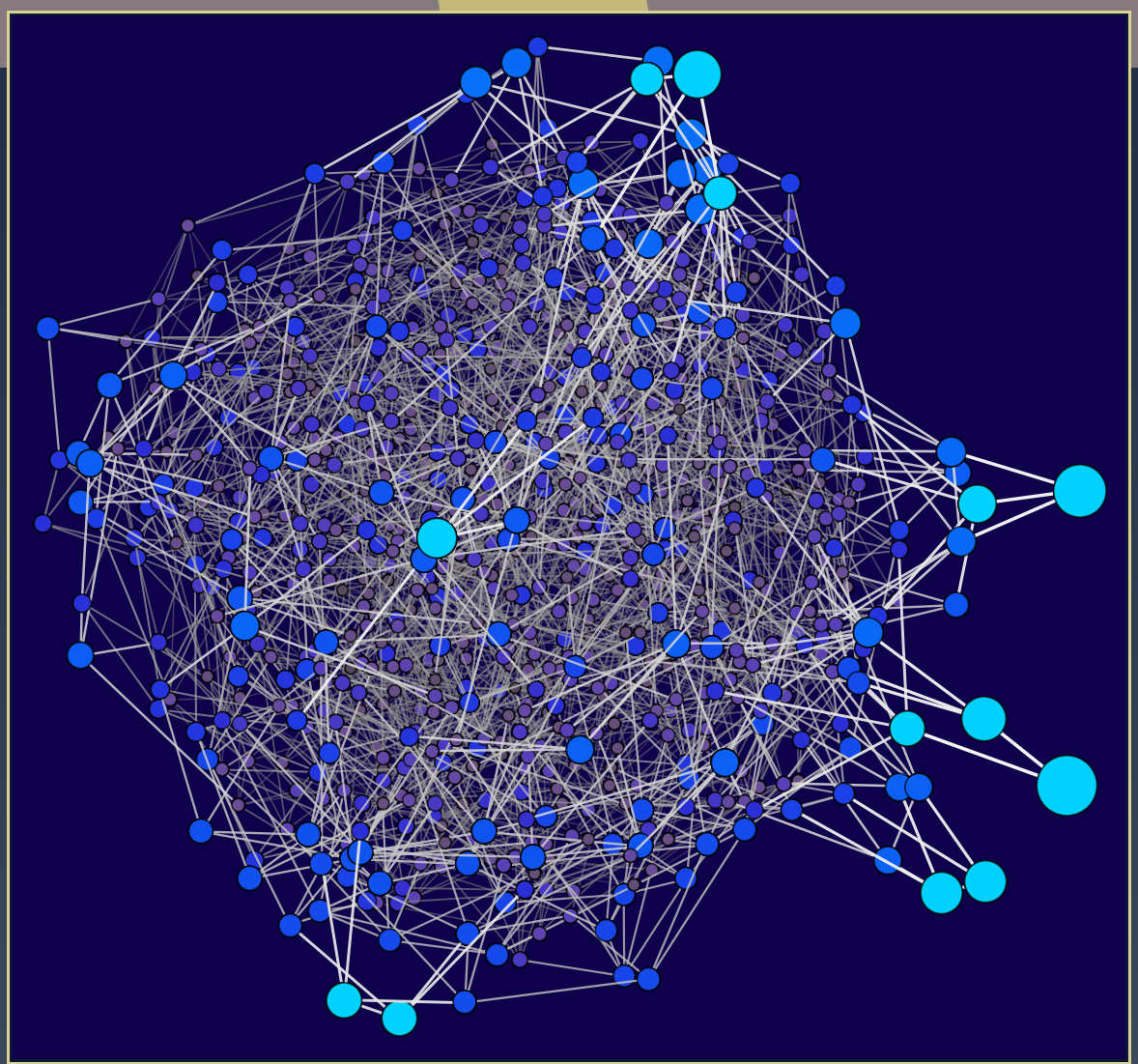
THE OPEN BOOK SERIES 4

ANTS XIV
Proceedings of the Fourteenth Algorithmic Number Theory Symposium

Hypergeometric L-functions in average polynomial time

Edgar Costa, Kiran S. Kedlaya, and David Roe



msp

THE OPEN BOOK SERIES **4** (2020)
Fourteenth Algorithmic Number Theory Symposium
https://doi.org/10.2140/obs.2020.4.143

Hypergeometric L-functions in average polynomial time

Edgar Costa, Kiran S. Kedlaya, and David Roe

We describe an algorithm for computing, for all primes $p \leq X$, the mod-p reduction of the trace of Frobenius at p of a fixed hypergeometric motive in time quasilinear in X. This combines the Beukers–Cohen–Mellit trace formula with average polynomial time techniques of Harvey et al.

1. Introduction

In the past, computation of arithmetic L-functions has largely been limited to familiar classes of low-dimensional geometric objects, such as hyperelliptic curves or K3 surfaces [CHK19]. Recently, it has emerged that families of motives whose associated (Picard–Fuchs) differential equation is a hypergeometric equation also have L-functions which can be computed at large scale. Such motives provide accessible examples of arithmetic L-functions with diverse configurations of Hodge numbers, some of which arise in heretofore unanticipated applications. For example, certain hypergeometric motives appear among families of Calabi–Yau threefolds, where they give rise to arithmetic manifestations of mirror symmetry (as in [DKS+18]).

Using finite hypergeometric sums in the manner of Greene [Gre87], Katz [Kat90], and especially McCarthy [McC13], an explicit formula for the L-function of a hypergeometric motive was given by Beukers, Cohen and Mellit [BCM15]. It was then modified by Cohen and Rodriguez Villegas, using the Gross–Koblitz formula [GK79] to replace classical Gauss sums with the Morita p-adic gamma function. That work is unpublished, but is documented in the manuscript [Wat15]; the resulting formula appears in [Coh15, §8] and [FKS16, §7.1]; it is implemented in PARI/GP [PAR19], Magma [Magma], and SageMath [SageMath]; and it is being used to tabulate hypergeometric L-functions in the L-functions and modular forms database [LMFDB]. (For an alternative approach using the p-adic Frobenius structure on a hypergeometric equation, see [Ked19].)

The purpose of this paper is to describe a preliminary adaptation of *average polynomial time* techniques for computation of L-functions to the setting of hypergeometric motives. Such techniques, based on

Costa and Roe were supported by the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation via Simons Foundation grant 550033. Kedlaya was supported by NSF (DMS-1802161) and UCSD (Warschawski Professorship).
MSC2010: primary 11Y16, 33C20; secondary 11G09, 11M38, 11T24.
Keywords: hypergeometric L-functions, average polynomial time.

accumulating remainder trees, were introduced by Costa, Gerbicz and Harvey [CGH14] for the problem of finding Wilson primes; adapted to computing L-functions by Harvey [Har14; Har15]; and further elaborated (and made practical in particular cases) by Harvey and Sutherland [HS14; HS16] and Harvey, Massierer and Sutherland [HMS16].

To simplify matters, we consider here only a limited form of the problem: given a hypergeometric motive over $\mathbb{Q}$ and a bound X, for each prime $p \leq X$, we compute the reduction modulo p of the trace of Frobenius at p in time quasilinear in X. This eliminates some technical issues that would arise when computing the mod-p^e reduction for $e > 1$, such as the computation of multiplicative lifts and evaluation of the Morita p-adic gamma function in average polynomial time. Modulo p, the trace formula at p for a parameter value t is a polynomial in t of degree $O(p)$ whose coefficients are essentially ratios of Pochhammer symbols. Computing the Pochhammer symbols themselves in average polynomial time is a straightforward adaptation of the corresponding computation for factorials done in [CGH14]; this approach can then be modified to include the polynomial evaluation.

At the end of the paper, we discuss the prospects of lifting our present restrictions of working modulo p (rather than a higher power) and of computing only the trace of the p-power Frobenius (rather than a higher power). Eliminating both restrictions would yield an average polynomial time algorithm for computing arbitrary hypergeometric L-series. However, the restricted computation described here is already of significant value for hypergeometric motives of weight 1, for which the trace of the p-power Frobenius is determined uniquely by its reduction modulo p (except when p is very small). Since the formula for the trace of the q-power Frobenius involves a summation over $q-1$ terms, our method reduces the complexity of computing the first X terms of the L-series from X^2 to $X^{3/2}$ (see Theorem 2.29).

We end this introduction by asking (as in [Ked19]) whether a similar trace formula exists for *A-hypergeometric systems* in the sense of Gelfand, Kapranov and Zelevinsky [GKZ08]. Such a formula might unlock even more classes of previously inaccessible L-functions.

2. Background

2A. ***The p-adic* Γ *function.*** For a detailed development of the following material, we recommend [Rob00, §7.1] and [RV07, §6.2].

Definition 2.1. The (Morita) p-adic gamma function is the unique continuous function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$ which satisfies

$$\Gamma_p(n+1) = (-1)^{n+1} \prod_{\substack{i=1 \\ (i,p)=1}}^{n} i = (-1)^{n+1} \frac{\Gamma(n+1)}{p^{\lfloor n/p \rfloor} \Gamma(\lfloor n/p \rfloor + 1)} \tag{2.2}$$

for all $n \in \mathbb{Z}_{\geq 0}$. For $p \geq 3$, it is Lipschitz continuous with $C = 1$; i.e.,

$$|\Gamma_p(x) - \Gamma_p(y)|_p \leq |x - y|_p. \tag{2.3}$$

There is also a functional equation analogous to the one for the complex Γ function:

$$\Gamma_p(x+1) = \omega(x)\Gamma_p(x), \qquad \omega(x) := \begin{cases} -x & \text{if } x \in \mathbb{Z}_p^\times \\ -1 & \text{if } x \in p\mathbb{Z}_p. \end{cases} \tag{2.4}$$

Remark 2.5. It was originally observed by Dwork (writing pseudonymously in [Boy80], as corroborated in [KT99]; see [RV07, §6.2] for the formulation given here) that Γ_p admits an easily computable Mahler expansion on any mod-p residue disc:

$$\Gamma_p(-a+px) = \sum_{k\geq 0} p^k c_{a+kp}(x)_k, \tag{2.6}$$

where $(x)_k := x(x+1)\cdots(x+k-1)$ is the usual Pochhammer symbol, and c_n is defined by the recursion

$$nc_n = c_{n-1} + c_{n-p}, \qquad c_0 = 1,\ c_n = 0 \ \text{ for } n < 0. \tag{2.7}$$

Thus, one may compute $\Gamma_p(x)$ modulo p^f using $O(pf)$ ring operations.

2B. ***Hypergeometric motives and their L-functions.*** While the following discussion is needed to put our work in context, the reader is encouraged to skip ahead to (2.22), as the essential content of the paper is the computation of that formula.

Definition 2.8. A *hypergeometric datum* is a pair of disjoint tuples $\alpha = (\alpha_1, \ldots, \alpha_r)$ and $\beta = (\beta_1, \ldots, \beta_r)$ valued in $\mathbb{Q} \cap [0, 1)$ which are *Galois-stable* (or *balanced*): any two reduced fractions with the same denominator occur with the same multiplicity.

Remark 2.9. There are several equivalent ways to specify a hypergeometric datum. One is to specify two tuples A and B for which the identity

$$\prod_{j=1}^{r} \frac{x - e^{2\pi i\alpha_j}}{x - e^{2\pi i\beta_j}} = \frac{\prod_{a\in A} \Phi_a(x)}{\prod_{b\in B} \Phi_b(x)}$$

holds in $\mathbb{C}(x)$, where $\Phi_n(x)$ denotes the n-th cyclotomic polynomial.

Definition 2.10. The *zigzag function* $Z_{\alpha,\beta} : [0, 1] \to \mathbb{Z}$ associated to a hypergeometric datum (α, β) is defined by

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

Notation 2.11. We denote by $M^{\alpha,\beta}$ the putative (see Remark 2.17) hypergeometric family over $\mathbb{P}^1$ associated to the hypergeometric datum (α, β). Its expected properties are as follows:

- It is a pure motive of degree r with base field $\mathbb{Q}(t)$ and coefficient field $\mathbb{Q}$.
- Its Hodge realization is the one constructed by Fedorov in [Fed18]. This means that as per [Fed18, Theorem 2], its minimal motivic weight is

$$\begin{aligned} w &= \max\{Z_{\alpha,\beta}(x) : x \in [0, 1]\} - \min\{Z_{\alpha,\beta}(x) : x \in [0, 1]\} - 1 \\ &= \max\{Z_{\alpha,\beta}(x) : x \in \alpha\} - \min\{Z_{\alpha,\beta}(x) : x \in \beta\} - 1 \end{aligned} \tag{2.12}$$

and a similar recipe (see [CG11, Conjecture 1.4] or [Fed18, Theorem 1]) computes the Hodge numbers. Note that rw is even [Wat15, §1.2].

- Its ℓ-adic étale realization is Katz's perverse sheaf [Kat90, Chapter 8].
- For $z \in \mathbb{Q} \setminus \{0, 1, \infty\}$, let $M_z^{\alpha,\beta}$ denote the specialization of $M^{\alpha,\beta}$ at $t = z$. Then the primes of bad reduction for $M_z^{\alpha,\beta}$ are those primes p at which z and $z-1$ are not both p-adic units (called *tame* primes) and those primes p at which the α_i and β_i are not all integral (called *wild* primes). By the compatibility with Katz, the L-function associated to $M_z^{\alpha,\beta}$ is given by the Beukers–Cohen–Mellit trace formula [BCM15].

Remark 2.13. In order to avoid some case subdivisions in what follows, we assume hereafter that $0 \notin \alpha$. This is relatively harmless because of the isomorphism

$$M_z^{\alpha,\beta} \cong M_{1/z}^{\beta,\alpha}. \tag{2.14}$$

Example 2.15. As per [Ono98], $M^{(1/2,1/2),(0,0)}$ is the motive $H^1(E, \mathbb{Q})$, where

$$E : y^2 = -x(x-1)(x-t). \tag{2.16}$$

For other (putative) examples, see [BK12] and [Nas17].

Remark 2.17. We use the qualifier "putative" in Notation 2.11 for two reasons. One is to avoid any precision about motives; while [BCM15] describes a specific variety whose ℓ-adic cohomology includes Katz's perverse sheaf, lifting this containment to the motivic level would require a deeper dive into motivic categories (including a choice of which such category to consider).

The other, more serious issue is that there is no existing reference that provides this missing precision on hypergeometric motives. The reader seeking to remedy this should start with [And04] for a user's guide to motives.

2B1. *Trace formulas.* We are particularly interested in computing

$$\det(1 - T \operatorname{Frob} | M_z^{\alpha,\beta}), \tag{2.18}$$

where Frob is the Frobenius automorphism at a prime p of good reduction for $M_z^{\alpha,\beta}$. (For concreteness, we may replace $M_z^{\alpha,\beta}$ with an étale realization.) We ignore primes of bad reduction both because they are small enough to be handled individually and because a somewhat different recipe is required (see [Wat15, § 11] for a partial description, noting that our z is Watkins's $1/t$).

Definition 2.19. Let $\{x\} := x - \lfloor x \rfloor$ be the fractional part of x. For $q = p^f$, define

$$\Gamma_q^*(x) := \prod_{v=0}^{f-1} \Gamma_p(\{p^v x\}), \tag{2.20}$$

and then define a p-adic analogue of the Pochhammer symbol by setting

$$(x)_m^* := \frac{\Gamma_q^*\left(x + \frac{m}{1-q}\right)}{\Gamma_q^*(x)}. \tag{2.21}$$

Let $[z]$ be the multiplicative representative in $\mathbb{Z}_p$ of the residue class of z (the unique $(p-1)$-st root of 1 congruent to z modulo p). As in [Wat15, § 2], write

$$H_q\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right) := \frac{1}{1-q}\sum_{m=0}^{q-2}(-p)^{\eta_m(\alpha)-\eta_m(\beta)} q^{D+\xi_m(\beta)}\left(\prod_{j=1}^{r}\frac{(\alpha_j)_m^*}{(\beta_j)_m^*}\right)[z]^m, \tag{2.22}$$

using the notation

$$\eta_m(x_1,\dots,x_r) := \sum_{j=1}^{r}\sum_{v=0}^{f-1}\left\{p^v\left(x_j + \frac{m}{1-q}\right)\right\} - \{p^v x_j\}, \tag{2.23}$$

$$\xi_m(\beta) := \#\{j : \beta_j = 0\} - \#\left\{j : \beta_j + \frac{m}{1-q} = 0\right\}, \tag{2.24}$$

$$D := \frac{w+1-\#\{j:\beta_j=0\}}{2}. \tag{2.25}$$

By adapting [BCM15, Theorem 1.3] using the Gross–Koblitz formula as in [Wat15, §2] (and twisting by q^D to minimize the weight), we deduce the following.

Theorem 2.26. *We have*

$$H_{p^f}\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right) = \mathrm{Tr}(\mathrm{Frob}^f \,|M_z^{\alpha,\beta}) \in \mathbb{Z}.$$

From [Wat15, §11], we also have a precise formula for the functional equation which is associated to $\det(1 - T\,\mathrm{Frob}\,|M_z^{\alpha,\beta})$.

Theorem 2.27. *We have*

$$\det(1 - q^{-w}T^{-1}\,\mathrm{Frob}\,|M_z^{\alpha,\beta}) = \pm q^{-rw/2}T^{-r}\det(1 - T\,\mathrm{Frob}\,|M_z^{\alpha,\beta}), \tag{2.28}$$

where $\pm$ denotes $+1$ if w is even, and otherwise is given by

$$\begin{cases} (\Delta|p), & \Delta = z(z-1)\prod_{a\in A}\mathrm{Disc}(\Phi_a(x)) \quad \text{for } r \equiv 0 \pmod 2,\\ -(\Delta|p), & \Delta = (1-z)\prod_{b\in B}\mathrm{Disc}(\Phi_b(x)) \quad \text{for } r \equiv 1 \pmod 2.\end{cases}$$

Here A, B, Φ_a, Φ_b are as in Remark 2.9 and $(\Delta|p)$ is the Kronecker symbol.

Using these two results, we recover $\det(1-T\,\mathrm{Frob}\,|M_z^{\alpha,\beta})$ from the values $H_{p^f}\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right)$ for $f = 1,\dots,\lfloor\frac{r}{2}\rfloor$.

2B2. *Complexity considerations.* Computing $H_{p^f}\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right)$ via (2.22) requires $O(fp^f)$ arithmetic operations,[1] due to the number of terms in the sum and product [Wat15, §2.1.4]. As these operations are in $\mathbb{Z}_p$,

[1] The factor of f comes from computing Γ_p. We do not incur a factor of f from computing Γ_q^* because the latter is invariant under $x \mapsto \{px\}$, so we only need $O(q/f)$ evaluations of Γ_q^*.

we must also pay attention to p-adic working precision; since $H_{p^f}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right)$ is the sum of r algebraic integers of complex norm $p^{wf/2}$, it is uniquely determined by its reduction modulo p^e for $e > \frac{1}{2}wf + \log_p(2r)$.

For the use case of computing L-series, a different analysis applies.

Theorem 2.29. *Fix a hypergeometric datum (α, β). Given $H_p\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right)$ for all primes $p \le X$, one can compute the first X coefficients of the Dirichlet L-series associated to $M_z^{\alpha,\beta}$ in at most $O(X^{3/2})$ arithmetic operations.*

Proof. The first X coefficients of the Dirichlet series are determined by the coefficients indexed by prime powers up to X, and hence by the values $H_q\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right)$ for all prime powers $q \le X$. The number of such q which are not prime is

$$O(X^{1/2}/\log X),$$

for $q = p^f$; evaluating (2.22) takes $O(fp^f) = O(X \log X)$ arithmetic operations. □

3. Accumulating remainder trees

The use of a *remainder tree* to expedite modular reduction has its origins in the fast Fourier transform (FFT). An early description was given by Borodin and Moenck [BM74]; for a modern treatment with more historical references, see [Ber08].

Accumulating remainder trees were introduced in [CGH14] in order to compute $(p-1)! \pmod{p^2}$ for many primes p. We use the variant described in [HS14, §4].

Definition 3.1. Suppose $\mathcal{P}$ is a sequence $p_1, \dots, p_{b-1}$ of pairwise coprime integers with $p_i \le X$, and $A_0, \dots, A_{b-2}$ is a sequence of 2×2 integer matrices. We may use an accumulating remainder tree to compute

$$C_n := A_0 \cdots A_{n-1} \bmod p_n \tag{3.2}$$

for $1 \le n < b$ as follows. For notational convenience we assume $b = 2^\ell$, set $A_{b-1} = 0$ and $p_0 = 1$. Then as in [HS14, §4], write

$$\begin{aligned} m_{i,j} &:= p_{j2^{\ell-i}} p_{j2^{\ell-i}+1} \cdots p_{(j+1)2^{\ell-i}-1}, \\ A_{i,j} &:= A_{j2^{\ell-i}} A_{j2^{\ell-i}+1} \cdots A_{(j+1)2^{\ell-i}-1}, \\ C_{i,j} &:= A_{i,0} \cdots A_{i,j-1} \bmod m_{i,j}. \end{aligned} \tag{3.3}$$

This leads us to Algorithm 1.

Theorem 3.4 [HS14, Theorem 4.1]. *Let B be an upper bound on the bit size of $\prod_{j=0}^{b-1} p_j$ and H an upper bound on the bit size of any p_i or A_i. The running time of Algorithm 1 is*

$$O((B + bH)\log(B + bH)\log(b))$$

(*using* [HVDH19] *for the runtime of integer multiplication*) *and its space complexity is*

$$O((B + bH)\log(b)).$$

Algorithm 1: Accumulating Remainder Tree

Input: $A_0, \dots, A_{b-1}$, $p_0, \dots, p_{b-1}$ as in Definition 3.1
Output: $\{C_i\}$

```
def RemTree({A_i}, {p_i}):
    for j := 0 to b − 1 do
        m_{ℓ,j} := p_j and A_{ℓ,j} := A_j
    for i := ℓ − 1 to 0 do
        for j := 0 to 2^i − 1 do
            m_{i,j} := m_{i+1,2j} m_{i+1,2j+1} and A_{i,j} := A_{i+1,2j} A_{i+1,2j+1}
    C_{0,0} := id
    for i := 1 to ℓ do
        for j := 0 to 2^i − 1 do
            if j even then
                C_{i,j} := C_{i−1,⌊j/2⌋} mod m_{i,j}
            else
                C_{i,j} := C_{i−1,⌊j/2⌋} A_{i,j−1} mod m_{i,j}
    return {C_{ℓ,j}}_{j=1,...,b−1}
```

3A. ***Accumulating remainder tree with spacing.*** In most applications (including this one), there is not a one-to-one correspondence between the moduli p_i and the multiplicands A_i. Rather, we will be given

- a list of matrices $A_0, \dots, A_{b-1}$,
- a list of primes $p_1, \dots, p_c$, and
- a list of distinct cut points $b_1, \dots, b_c$,

with the aim of computing $C_n := A_0 \cdots A_{b_n-1} \bmod p_n$ for $1 \le n < c$. This reduces to Algorithm 1 by suitably grouping terms; see Algorithm 2. (One may also handle repeated cut points, as long as the cut points up to X occur at most $O(X)$ times.)

Remark 3.5. In practice, we split our products to work around discontinuities of (2.22) (see Section 5B). One gains some savings (particularly in space complexity) by splitting a bit further, replacing remainder trees with *remainder forests* [HS14, Theorem 4.2]; we omit the details here.

4. Nuts and bolts

We record two technical lemmas used in the description of our algorithm. For the rest of the paper, we make the simplifying assumption $q = p$ in Theorem 2.26.

Lemma 4.1. *Set $I_b := [0,1] \cap \frac{1}{b}\mathbb{Z}$. Suppose $\gamma \in I_b$ and p is a prime not dividing b. Let $m = \lfloor \gamma(p-1) \rfloor$. Then there exist $\delta \in I_b$ and $\epsilon \in \{1,2\}$ so that*

$$m + \epsilon \equiv \delta \pmod{p}.$$

Moreover, δ and ϵ only depend on b, γ, and $p \pmod{b}$.

Algorithm 2: Accumulating Remainder Tree with Spacing

Input: $A_0, \dots, A_{b-1}, p_1, \dots, p_c, b_1, \dots, b_c$ as in Section 3A
Output: $C_1, \dots, C_{c-1}$

```
def RemTreeWithSpacing({A_i}, {p_i}, {b_i}):
    ℓ := ⌈log_2(b)⌉
    for j := b to 2^ℓ − 1 do
        A_j := 0
    for j := 0 to 2^ℓ − 1 do
        p'_j := 1
    for i := 1 to c do
        p'_{b_i} := p_i
    C'_i := RemTree({A_i}, {p'_i})
    return {C'_{b_i}}_{i=0,...,c−1}
```

Proof. Write $\gamma = \frac{a}{b}$ and define an integer $r \in \{0, \dots, b-1\}$ by the condition that

$$a(p-1) = mb + r.$$

We then set

$$\begin{cases} \epsilon := 1, \ \delta := \frac{1}{b}(b - a - r) & \text{if } a + r < b, \\ \epsilon := 2, \ \delta := \frac{1}{b}(2b - a - r) & \text{otherwise.} \end{cases}$$

Note that

$$b(\delta - \epsilon) = -(a + r) = mb - ap$$

so $m + \epsilon \equiv \delta \pmod{p}$. The fact that $\delta \in I_b$ follows from the bounds $0 \le a, r \le b$. □

Lemma 4.2. *Suppose* $0 \le m < p-1$ *and either* $\eta_m(\alpha) - \eta_m(\beta) \ne \eta_{m+1}(\alpha) - \eta_{m+1}(\beta)$ *or* $\xi_m(\beta) \ne \xi_{m+1}(\beta)$. *Then* $\lfloor \gamma(p-1) \rfloor \in \{m, m+1\}$ *for some* $\gamma \in \alpha \cup \beta$.

Proof. Since $q = p$, we have

$$\eta_m(\alpha) - \eta_m(\beta) = \sum_{j=1}^{r} \left(\left\{ \alpha_j - \frac{m}{p-1} \right\} - \{\alpha_j\} \right) - \sum_{j=1}^{r} \left(\left\{ \beta_j - \frac{m}{p-1} \right\} - \{\beta_j\} \right). \tag{4.3}$$

For $x, y \in [0, 1)$ we have

$$\{x - y\} = \begin{cases} x - y, & (x \ge y), \\ x - y + 1, & (x < y). \end{cases} \tag{4.4}$$

Consequently, the only way for $\eta_m(\alpha) - \eta_m(\beta)$ to change values when m goes to $m+1$ is for there to exist $\gamma \in \alpha \cup \beta$ such that

$$\gamma - \frac{m}{p-1} \ge 0, \qquad \gamma - \frac{m+1}{p-1} < 0.$$

This occurs precisely when $m = \lfloor \gamma(p-1) \rfloor$. Meanwhile, by (2.24), $\xi_m(\beta) = \xi_{m+1}(\beta)$ unless $\beta_j = m/(p-1)$ or $\beta_j = (m+1)/(p-1) = 0$ for some j. □

5. Computing trace functions of hypergeometric motives

Throughout this section, fix α, β and z. We now describe how to compute the trace $H_p\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right)$ modulo p in average polynomial time using (2.22), which we duplicate here modulo p for ease of reference:

$$H_p\left(\begin{matrix}\alpha\\ \beta\end{matrix}\middle| z\right) \equiv \sum_{m=0}^{p-2} (-p)^{\eta_m(\alpha)-\eta_m(\beta)} p^{D+\xi_m(\beta)} \left(\prod_{j=1}^{r} \frac{(\alpha_j)_m^*}{(\beta_j)_m^*}\right) z^m \pmod p. \tag{5.1}$$

5A. ***Overview of the algorithm.*** In order to apply Algorithm 2, we would like to identify 2×2 integer matrices $B(m)$, such that we may extract $H_p\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right) \pmod p$ from $B(0)B(1)\cdots B(p-2)$. In practice, we will consider shorter subproducts and choose $B(m)$ based on the residue of p modulo a fixed integer (independent of m and p); we will then apply Algorithm 2 once for each subproduct and residue class.

As a first approximation, let us instead model the sum $\sum_{m=0}^{p-2} P_m$ where

$$P_m := z^m \prod_{j=1}^{r} \frac{(\alpha_j)_m^*}{(\beta_j)_m^*} \in \mathbb{Z}_p^\times. \tag{5.2}$$

If we can find $f(m), g(m) \in \mathbb{Z}[m]$ so that

$$P_{m+1} \equiv \frac{f(m)}{g(m)} P_m \pmod p, \tag{5.3}$$

we can then set

$$B(m) := \begin{pmatrix} g(m) & 0 \\ g(m) & f(m)\end{pmatrix} = g(m) \begin{pmatrix} 1 & 0 \\ 1 & f(m)/g(m)\end{pmatrix} \tag{5.4}$$

and $\widetilde{B} = B(0)\cdots B(p-2) \pmod p$, so that

$$\widetilde{B} \equiv g(0)\cdots g(p-2) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{p-2} P_m & P_{p-1}\end{pmatrix} \pmod p$$

and so $\sum_{m=0}^{p-2} P_m \equiv \widetilde{B}_{21}/\widetilde{B}_{11} \pmod p$. That is, $\widetilde{B}_{11}$ tracks a common denominator, $\widetilde{B}_{22}$ tracks the product P_m, and $\widetilde{B}_{12}$ computes the sum of the P_m.

There are two problems with the approach described above. First, to correctly simulate (5.1) we must sum not P_m but

$$P'_m := (-p)^{\eta_m(\alpha)-\eta_m(\beta)} p^{D+\xi_m(\beta)} P_m, \tag{5.5}$$

which we cannot directly handle by modifying $B(m)_{21}$ because the extra factor depends on both p and m. Second, while we can find polynomials f and g satisfying (5.3) for most values of m using (2.21) and the functional equation (2.4), there will be a few values of m where $f(m)$ or $g(m)$ is a multiple of p. We cannot filter these values out during the remainder tree because p is not fixed.

The solution to both of these issues is to break up the range $[0, p-2]$ into intervals on which (5.3) holds and the values $\eta_m(\alpha)-\eta_m(\beta)$ and $\xi_m(\beta)$ are constant. The breaks between these intervals occur when $m = \lfloor \gamma(p-1)\rfloor$, where $\gamma \in \alpha \cup \beta$. We thus use a separate accumulating remainder tree for each

interval, yielding for each p a fixed number of subproducts with isolated missing terms in between; we then compute separately for each p to bridge the gaps.

A third issue is that while we can vary the endpoint in an accumulating remainder tree as a function of p (as described in Section 3), it is more difficult to change the start point. Our solution is to use Lemma 4.1 to find a rational number δ so that adding δ to each α_j and β_j has the effect of shifting the start point to 0.

5B. ***Construction of the matrix product.*** We now construct the matrix product described above. We begin with the division of the interval $[0, p-1]$ and the division of primes into residue classes. We assume that $q = p$ is good and not 2.

Definition 5.6. Given a hypergeometric motive $M_z^{\alpha,\beta}$, let $0 = \gamma_0 < \cdots < \gamma_s = 1$ be the distinct elements in $\alpha \cup \beta \cup \{0, 1\}$. Let b be the least common denominator of $\alpha \cup \beta$ and fix $c \in (\mathbb{Z}/b\mathbb{Z})^\times$. Let p be a prime congruent to c modulo b and not dividing the denominator of z. Write m_i for $\lfloor \gamma_i(p-1) \rfloor$.

We next exhibit polynomials that we use to compute Pochhammer symbols and their partial sums on the interval (γ_i, γ_{i+1}).

Definition 5.7. Fix an interval (γ_i, γ_{i+1}), choose δ_i and ϵ_i associated to γ_i as in Lemma 4.1, and let

$$\iota(x, y) := \begin{cases} 1, & x \le y, \\ 0, & x > y. \end{cases} \tag{5.8}$$

Define polynomials $f_{i,c}(k), g_{i,c}(k) \in \mathbb{Z}[k]$ as follows: set

$$\begin{aligned} F_{i,c}(k) &:= z \prod_{j=1}^{r} (\alpha_j + \delta_i + \iota(\alpha_j, \gamma_i) + k - \epsilon_i), \\ G_{i,c}(k) &:= \prod_{j=1}^{r} (\beta_j + \delta_i + \iota(\beta_j, \gamma_i) + k - \epsilon_i), \end{aligned} \tag{5.9}$$

let $d_{i,c}$ be the least common multiple of the denominators of $F_{i,c}$ and $G_{i,c}$, and set $f_{i,c}(k) := d_{i,c} F_{i,c}(k)$ and $g_{i,c}(k) := d_{i,c} G_{i,c}(k)$.

Lemma 5.10. *Define P_m as in (5.2), and suppose $m_i < m < m_{i+1}$. Then*

$$P_{m+1} \equiv \frac{f_{i,c}(k)}{g_{i,c}(k)} P_m \pmod{p},$$

where $1 \le k < m_{i+1} - m_i$ and $m = m_i + k$.

Proof. We first focus on a single Pochhammer symbol $(\alpha_j)_m^*$. First note that, for $m_i < m \le m_{i+1}$, by (4.4) we have

$$\left\{ \alpha_j + \frac{m}{1-p} \right\} = \alpha_j + \frac{m}{1-p} + \begin{cases} 0 & m \le \lfloor \alpha_j(p-1) \rfloor \\ 1 & m > \lfloor \alpha_j(p-1) \rfloor \end{cases} = \alpha_j + \frac{m}{1-p} + \iota(\alpha_j, \gamma_i). \tag{5.11}$$

Combining (5.11) with Lipschitz continuity (2.3) and the functional equation for Γ_p (2.4) and Lemma 4.1, for $m_i < m < m_{i+1}$ we obtain

$$\begin{aligned}\Gamma_p\left(\left\{\alpha_j + \frac{m+1}{1-p}\right\}\right) &\equiv \Gamma_p(\alpha_j + m + 1 + \iota(\alpha_j, \gamma_i)) \\ &= -(\alpha_j + m + \iota(\alpha_j, \gamma_i))\Gamma_p(\alpha_j + m + \iota(\alpha_j, \gamma_i)) \\ &\equiv -(\alpha_j + \delta_i + \iota(\alpha_j, \gamma_i) + k - \epsilon_i)\Gamma_p\left(\left\{\alpha_j + \frac{m}{1-p}\right\}\right) \pmod p.\end{aligned} \tag{5.12}$$

Taking the product over all the Pochhammer symbols, the minus sign cancels out, and we obtain (5.9), as desired. □

We next account for the power of p in the product, and assemble a matrix product that computes the sum between two breaks.

Definition 5.13. Let $\xi(\beta) = \#\{j : \beta_j = 0\}$ and

$$\sigma_i := \begin{cases} 1, & Z_{\alpha,\beta}(\gamma_i) + \xi(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_i) \equiv 0 \pmod 2, \\ -1, & Z_{\alpha,\beta}(\gamma_i) + \xi(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_i) \equiv 1 \pmod 2, \\ 0, & \text{otherwise.} \end{cases} \tag{5.14}$$

By Lemma 4.2, σ_i gives the value of $(-p)^{\eta_m(\alpha)-\eta_m(\beta)} p^{\xi_m(\beta)+D} \bmod p$ for all m with $m_i < m < m_{i+1}$. Now set

$$A_{i,c}(k) := \begin{pmatrix} g_{i,c}(k) & 0 \\ \sigma_i g_{i,c}(k) & f_{i,c}(k) \end{pmatrix}. \tag{5.15}$$

Since $A_{i,c}(k)$ depends only on c and not p, we can use an accumulating remainder tree for each c to compute

$$S_i(p) := A_{i,c}(1)A_{i,c}(2)\cdots A_{i,c}(m_{i+1} - m_i - 1) \pmod p. \tag{5.16}$$

Lemma 5.17. *For P'_m as defined in (5.5),*

$$S_i(p)_{11}^{-1} S_i(p) \equiv \begin{pmatrix} 1 & 0 \\ \sum_{m=m_i+1}^{m_{i+1}-1} P'_m/P_{m_i+1} & P_{m_{i+1}}/P_{m_i+1} \end{pmatrix} \pmod p. \tag{5.18}$$

Proof. By Lemma 5.10, for $k = 1, \ldots, m_{i+1} - m_i - 1$,

$$\frac{(A_{i,c}(1)\cdots A_{i,c}(k))_{22}}{(A_{i,c}(1)\cdots A_{i,c}(k))_{11}} \equiv \frac{P_{m_i+k+1}}{P_{m_i+1}} \pmod p$$

and hence

$$\frac{(A_{i,c}(1)\cdots A_{i,c}(k))_{21}}{(A_{i,c}(1)\cdots A_{i,c}(k))_{11}} \equiv \sigma_i \sum_{l=1}^{k} \frac{P_{m_i+l}}{P_{m_i+1}} \pmod p.$$

Taking $k = m_{i+1} - m_i - 1$, and then applying Lemma 4.2 to replace σ_i with P'_m/P_m, yields the desired result. □

It remains to deal with the breaks. Since the number of breaks is independent of p, we have the luxury of computing matrices $T_i(p)$ separately for each p that move the Pochhammer symbols and partial sums past the break γ_i.

Definition 5.19. With ω defined as in (2.4), let

$$h_i(\gamma, p) := \begin{cases} \omega(\gamma + m_i + 1) & \text{if } \gamma(p-1) < m_i, \\ \omega(\gamma + m_i) & \text{if } \gamma(p-1) \geq m_i + 1, \\ \omega(\gamma + m_i + 1)\omega(\gamma + m_i) & \text{otherwise,} \end{cases} \tag{5.20}$$

$$\tau_i := \begin{cases} 0 & \gamma_i = 0, \\ 1 & Z_{\alpha,\beta}(\gamma_{i-1}) + \xi_{m_i}(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_{i-1}) \equiv 0 \pmod 2, \\ -1 & Z_{\alpha,\beta}(\gamma_{i-1}) + \xi_{m_i}(\beta) + D = 0 \text{ and } Z_{\alpha,\beta}(\gamma_{i-1}) \equiv 1 \pmod 2, \\ 0 & \text{otherwise,} \end{cases} \tag{5.21}$$

and then set

$$T_i(p) := \begin{pmatrix} 1 & 0 \\ \tau_i & z \prod_{j=1}^{r} \frac{h_i(\alpha_j, p)}{h_i(\beta_j, p)} \end{pmatrix}, \tag{5.22}$$

$$S(p) := \prod_{i=0}^{s-1} T_i(p) S_i(p). \tag{5.23}$$

Note that modulo p, $T_i(p)$ is congruent to a matrix that depends on p only via c.

Lemma 5.24. *For suitable choices of scalars, we have*

$$\prod_{j=0}^{i-1} T_j(p) S_j(p) \equiv (\text{scalar}) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{m_i-1} P'_m & P_{m_i} \end{pmatrix} \pmod p,$$

$$\left(\prod_{j=0}^{i-1} T_j(p) S_j(p) \right) T_i(p) \equiv (\text{scalar}) \begin{pmatrix} 1 & 0 \\ \sum_{m=0}^{m_i} P'_m & P_{m_i+1} \end{pmatrix} \pmod p.$$

Proof. This follows by induction on i using Lemma 5.17. □

Summing up, we obtain the following:

Proposition 5.25. *For $p \equiv c \pmod b$ not dividing the denominator of z,*

$$H_p\left(\begin{matrix} \alpha \\ \beta \end{matrix} \middle| z \right) \equiv S(p)_{21} / S(p)_{11} \pmod p.$$

Proof. This follows from (5.1) and the case $i = s$ of Lemma 5.24. □

5C. ***Algorithm and runtime.*** We summarize with Algorithm 3.

Theorem 5.26. *For fixed α, β, Algorithm 3 is correct and runs in time*

$$O(X \log(X)^3).$$

Algorithm 3: Trace mod p

Input: $\alpha, \beta \in \big(\mathbb{Q} \cap [0,1)\big)^r$, $z \in \mathbb{Q}$ and a bound X

Output: $H_p\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix} \middle| z\right) \pmod p$ for all good $p \le X$

```
def Traces(α, β, z, X):
    if 0 ∈ α then
        α, β, z := β, α, 1/z
    gamma := Sorted( Set( α ∪ β ∪ {0, 1}))
    for good primes p ≤ X do
        result[p] := IdentityMatrix(2)
    for start, end consecutive elements of gamma do
        b := Denominator(start)
        for c ∈ (ℤ/bℤ)^× do
            δ, ϵ := RationalShift(start, c)                    // Using Lemma 4.1
            mats := Matrices(z, start, δ, ϵ)                   // As in (5.15)
            cut := (p ↦ ⌊end · (p − 1)⌋ − ⌊start · (p − 1)⌋)
            primes := {good primes p ≡ c (mod b), p ≤ X}
            {C_i} := RemTreeWithSpacing(mats, primes, cut)
            for i := 0, ..., #primes − 1 do
                p := primes[i]
                result[p] := result[p] · FixBreak(z, start, p)  // As in (5.22)
                result[p] := result[p] · C_i
    for good primes p ≤ X do
        result[p] := result[p]_21 / result[p]_11 (mod p)
    return result
```

Proof. Correctness is immediate from Proposition 5.25. The runtime is dominated by the calls to Algorithm 2; these calls take place inside a loop over consecutive elements of $\alpha \cup \beta \cup \{0,1\}$ and a second loop over residue classes modulo a divisor of b. These two loops together have length $O(rb)$; combining with the runtime estimate from Theorem 3.4 (taking $B = b = O(X)$, $H = O(\log X)$) yields the desired result. □

5D. ***Implementation notes.*** We have implemented Algorithm 3 in SageMath, using a variant of Algorithm 2 implemented in C by Drew Sutherland (see Remark 3.5). Our implementation is available at https://github.com/edgarcosta/amortizedHGM, and vastly outperforms SageMath and Magma while giving matching answers; see Table 1 for sample timings.

5E. ***An example.*** Let $\alpha = \left(\frac14, \frac12, \frac12, \frac34\right)$, $\beta = \left(\frac13, \frac13, \frac23, \frac23\right)$ and $z = \frac15$. We plot the zigzag function in Figure 1. Using (2.12), we see that $M^{\alpha,\beta}$ has weight 1 and the intervals contributing to the computation

X	Algorithm 3	Sage	Magma	X	Algorithm 3
2^{10}	0.07s	0.39s	0.11s	2^{18}	1.81s
2^{11}	0.05s	0.68s	0.35s	2^{19}	4.59s
2^{12}	0.06s	2.12s	1.29s	2^{20}	10.71s
2^{13}	0.08s	7.39s	4.83s	2^{21}	24.53s
2^{14}	0.12s	26.0s	18.24s	2^{22}	58.0s
2^{15}	0.18s	92.27s	68.35s	2^{23}	135s
2^{16}	0.34s	343s	280s	2^{24}	322s
2^{17}	0.80s	1328s	1190s	2^{25}	857s

Table 1. Comparison of Algorithm 3 against SageMath and Magma for $\alpha = \left(\frac{1}{4}, \frac{1}{2}, \frac{1}{2}, \frac{3}{4}\right)$, $\beta = \left(\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}\right)$ and $z = \frac{1}{5}$. Note the observable difference between linear and quadratic complexity.

of $H_p\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\middle| z\right)$ are $(\gamma_2, \gamma_3) = \left(\frac{1}{3}, \frac{1}{2}\right)$ and $(\gamma_4, \gamma_5) = \left(\frac{2}{3}, \frac{3}{4}\right)$. For the remainder of the example we will focus on the congruence class $p \equiv 7 \pmod{12}$. Applying Lemma 4.1 to $\gamma_2 = \frac{1}{3}$ (resp. $\gamma_4 = \frac{2}{3}$), we obtain $\delta_2 = \frac{2}{3}$ and $\epsilon_2 = 1$ (resp. $\delta_4 = \frac{1}{3}$ and $\epsilon_4 = 1$). By (5.9) and (5.14),

$$f_{2,7}(k) = 5184k^4 + 8640k^3 + 4428k^2 + 852k + 55,$$
$$g_{2,7}(k) = 25920k^4 + 69120k^3 + 63360k^2 + 23040k + 2880,$$
$$f_{4,7}(k) = 5184k^4 + 12096k^3 + 9612k^2 + 2820k + 175,$$
$$g_{4,7}(k) = 25920k^4 + 86400k^3 + 106560k^2 + 57600k + 11520,$$

and $\sigma_2 = \sigma_4 = -1$. Taking $p = 67$, we obtain $(m_2, m_3) = (22, 33)$ and $(m_4, m_5) = (44, 49)$. Using an accumulating remainder tree (or simple multiplication), we get

$$S_2(67) = \begin{pmatrix} 65 & 0 \\ 34 & 5 \end{pmatrix}, \qquad S_4(67) = \begin{pmatrix} 54 & 0 \\ 25 & 41 \end{pmatrix}.$$

However, we can't ignore the other intervals: they may not contribute to the sum, but they do track the Pochhammer symbols. Similar computations show

$$S_0(67) = \begin{pmatrix} 38 & 0 \\ 0 & 62 \end{pmatrix}, \quad S_1(67) = \begin{pmatrix} 50 & 0 \\ 0 & 47 \end{pmatrix}, \quad S_3(67) = \begin{pmatrix} 1 & 0 \\ 0 & 16 \end{pmatrix}, \quad S_5(67) = \begin{pmatrix} 1 & 0 \\ 0 & 38 \end{pmatrix}.$$

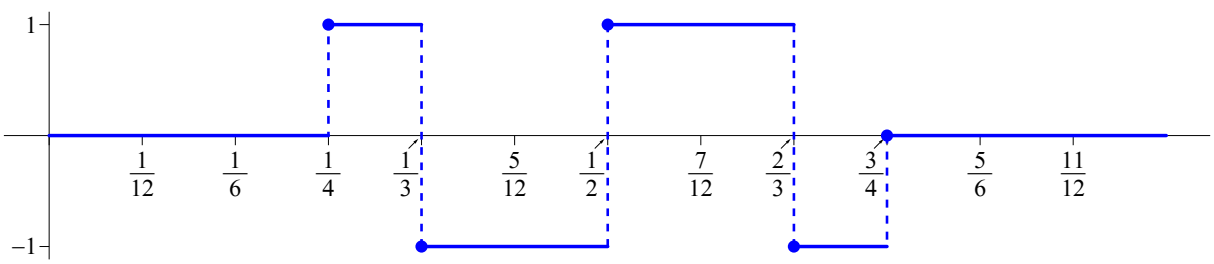


Figure 1. $Z_{\alpha,\beta}(x)$ for $\alpha = \left(\frac{1}{4}, \frac{1}{2}, \frac{1}{2}, \frac{3}{4}\right)$, $\beta = \left(\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, \frac{2}{3}\right)$.

It remains to handle the break points. Using Definition 5.19 we get

$$T_0(67) = \begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \qquad T_1(67) = \begin{pmatrix} 1 & 0 \\ 0 & 31 \end{pmatrix}, \qquad T_2(67) = \begin{pmatrix} 1 & 0 \\ -1 & 12 \end{pmatrix},$$
$$T_3(67) = \begin{pmatrix} 1 & 0 \\ -1 & 40 \end{pmatrix}, \qquad T_4(67) = \begin{pmatrix} 1 & 0 \\ -1 & 40 \end{pmatrix}, \qquad T_5(67) = \begin{pmatrix} 1 & 0 \\ -1 & 31 \end{pmatrix}.$$

Putting them all together, we get

$$S(67) = T_0(67)S_0(67)\cdots T_5(67)S_5(67) = \begin{pmatrix} 21 & 0 \\ 33 & 21 \end{pmatrix}$$

yielding $H_{67}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix} \middle| \frac{1}{5}\right) \equiv \frac{33}{21} \equiv 59 \pmod{67}$.

6. Future goals and challenges

We would like to be able to compute $H_{p^f}\left(\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix} \middle| z\right) \pmod{p^e}$ in average polynomial time for general e and f, but we currently only implement this for $e = f = 1$. We highlight the key points at which new ideas would be needed to achieve this goal.

6A. ***The case e > 1.*** Allowing $e > 1$ creates two related issues where our computation exploits extra structure of the trace formula mod p: the replacement of $[z]$ with z, and the use of the functional equation in (5.12) to compare two values of Γ_p at arguments that differ by $\frac{1}{1-p}$.

Such issues can usually be resolved using the "generic prime" technique of [Har15, §4.4]: make the average polynomial time computation carrying suitable nilpotent variables, then make a separate specialization for each p.

6B. ***The case f > 1.*** Allowing $f > 1$ creates more serious issues because of the change in the definition of $\Gamma_q^*(x)$, which interferes with our division of the summation into a fixed number of ranges. To see this in more detail, fix $v \in \{0, \dots, f-1\}$. For each $\gamma \in \alpha \cup \beta$, a break occurs when the value of $\left\{p^v\left(\gamma - \frac{m}{q-1}\right)\right\}$ changes when m goes to $m+1$; there are p^v such breaks.

It is unclear whether one can rearrange the formula (2.22) to remedy this issue. It may help to implement the method of Frobenius structures suggested in [Ked19], which scales linearly in p rather than q. We may then argue as in Theorem 2.29 to compute the first X coefficients of an L-series in average polynomial time.

References

[And04] Yves André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, Panoramas et Synthèses, no. 17, Société Mathématique de France, Paris, 2004. MR 2115000

[BCM15] Frits Beukers, Henri Cohen, and Anton Mellit, *Finite hypergeometric functions*, Pure Appl. Math. Q. **11** (2015), no. 4, 559–589. MR 3613122

[Ber08] Daniel J. Bernstein, *Fast multiplication and its applications*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Pub., no. 44, Cambridge Univ. Press, 2008, pp. 325–384. MR 2467550

[BK12] Rupam Barman and Gautam Kalita, *Hypergeometric functions and a family of algebraic curves*, Ramanujan J. **28** (2012), no. 2, 175–185. MR 2925173

[BM74] A. Borodin and R. Moenck, *Fast modular transforms*, J. Comput. System Sci. **8** (1974), 366–386. MR 371144

[Boy80] Maurizio Boyarsky, *p-adic gamma functions and Dwork cohomology*, Trans. Amer. Math. Soc. **257** (1980), no. 2, 359–369. MR 552263

[CG11] Alessio Corti and Vasily Golyshev, *Hypergeometric equations and weighted projective spaces*, Sci. China Math. **54** (2011), no. 8, 1577–1590. MR 2824960

[CGH14] Edgar Costa, Robert Gerbicz, and David Harvey, *A search for Wilson primes*, Math. Comp. **83** (2014), no. 290, 3071–3091. MR 3246824

[CHK19] Edgar Costa, David Harvey, and Kiran S. Kedlaya, *Zeta functions of nondegenerate hypersurfaces in toric varieties via controlled reduction in p-adic cohomology*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium (Berkeley, CA), Open Book Ser., no. 2, Math. Sci. Publ., 2019, pp. 221–238. MR 3952014

[Coh15] Henri Cohen, *Computing L-functions: a survey*, J. Théor. Nombres Bordeaux **27**:3 (2015), 699–726. MR 3429316

[DKS+18] Charles F. Doran, Tyler L. Kelly, Adriana Salerno, Steven Sperber, John Voight, and Ursula Whitcher, *Zeta functions of alternate mirror Calabi–Yau families*, Israel J. Math. **228** (2018), no. 2, 665–705. MR 3874856

[Fed18] Roman Fedorov, *Variations of Hodge structures for hypergeometric differential operators and parabolic Higgs bundles*, Int. Math. Res. Not. **2018** (2018), no. 18, 5583–5608. MR 3862114

[FKS16] Francesc Fité, Kiran S. Kedlaya, and Andrew V. Sutherland, *Sato–Tate groups of some weight 3 motives*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 57–101. MR 3502939

[GK79] Benedict H. Gross and Neal Koblitz, *Gauss sums and the p-adic Γ-function*, Ann. of Math. (2) **109** (1979), no. 3, 569–581. MR 534763

[GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, resultants and multidimensional determinants*, Birkhäuser, Boston, 2008, Reprint of the 1994 edition. MR 2394437

[Gre87] John Greene, *Hypergeometric functions over finite fields*, Trans. Amer. Math. Soc. **301** (1987), no. 1, 77–101. MR 879564

[Har14] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803. MR 3152945

[Har15] David Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. (3) **111** (2015), no. 6, 1379–1401. MR 3447797

[HMS16] David Harvey, Maike Massierer, and Andrew V. Sutherland, *Computing L-series of geometrically hyperelliptic curves of genus three*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 220–234. MR 3540957

[HS14] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time*, LMS J. Comput. Math. **17** (2014), no. suppl. A, 257–273. MR 3240808

[HS16] David Harvey and Andrew V. Sutherland, *Computing Hasse–Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang–Trotter and Sato–Tate conjectures, Contemp. Math., no. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 127–147. MR 3502941

[HVDH19] David Harvey and Joris Van Der Hoeven, *Integer multiplication in time O(n log n)*, preprint, 2019.

[Kat90] Nicholas M. Katz, *Exponential sums and differential equations*, Annals of Mathematics Studies, no. 124, Princeton University Press, 1990. MR 1081536

[Ked19] Kiran S. Kedlaya, *Frobenius structures on hypergeometric equations*, preprint, 2019. arXiv 1912.13073v1

[KT99] Nicholas M. Katz and John Tate, *Bernard Dwork (1923–1998)*, Notices Amer. Math. Soc. **46** (1999), no. 3, 338–343. MR 1669973

[LMFDB] The LMFDB collaboration, *The L-functions and modular forms database*.

[Magma] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system, I: the user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[McC13] Dermot McCarthy, *The trace of Frobenius of elliptic curves and the p-adic gamma function*, Pacific J. Math. **261** (2013), no. 1, 219–236. MR 3037565

[Nas17] Bartosz Naskrecki, *On a certain hypergeometric motive of weight 2 and rank 3*, preprint, 2017. arXiv 1702.07738v2

[Ono98] Ken Ono, *Values of Gaussian hypergeometric series*, Trans. Amer. Math. Soc. **350** (1998), no. 3, 1205–1223. MR 1407498

[PAR19] PARI group, *PARI/GP*, 2019, version 2.11.2.

[Rob00] Alain M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, no. 198, Springer, 2000. MR 1760253

[RV07] Fernando Rodriguez Villegas, *Experimental number theory*, Oxford Graduate Texts in Mathematics, no. 13, Oxford University Press, 2007. MR 2317419

[SageMath] The Sage Development Team, *SageMath, the Sage Mathematics Software System*.

[Wat15] Mark Watkins, *Hypergeometric motives over $\mathbb{Q}$ and their L-functions*, preprint, 2015.

Received 28 Feb 2020. Revised 4 Aug 2020.

EDGAR COSTA: edgarc@mit.edu
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States

KIRAN S. KEDLAYA: kedlaya@ucsd.edu
Department of Mathematics, University of California, San Diego, La Jolla, CA, United States

DAVID ROE: roed.math@gmail.com
Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA, United States

VOLUME EDITORS

Stephen D. Galbraith
Mathematics Department
University of Auckland
New Zealand
https://orcid.org/0000-0001-7114-8377

The cover image is based on an illustration from the article "Supersingular curves with small noninteger endomorphisms", by Jonathan Love and Dan Boneh (see p. 9).

Electronic copies can be obtained free of charge from http://msp.org/obs/4 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-07-1 (print), 978-1-935107-08-8 (electronic)

First published 2020.

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 4

Fourteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational and algorithmic number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the fourteenth ANTS meeting, which took place 29 June to 4 July 2020 via video conference, the plans for holding it at the University of Auckland, New Zealand, having been disrupted by the COVID-19 pandemic. The volume contains revised and edited versions of 24 refereed papers and one invited paper presented at the conference.

TABLE OF CONTENTS