Hypergeometric L-functions in average polynomial time, II

Edgar Costa (MIT)

July 16, 2024, Simons Collaboration Annual Meeting

Algorithmic Number Theory Symposium XVI (ANTS)

Slides available at `edgarcosta.org`

with Kiran Kedlaya and David Roe.

Hypergeometric datum

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 **balanced**: the multiplicity of any reduced fraction depends only on its denominator. For example

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

Hypergeometric datum

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 **balanced**: 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:

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

where $F_p[t] = 1 - a_p t + \cdots \in \mathbb{Z}[t]$ of degree at most r.

Hypergeometric families in the wild

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

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

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

$$\mathrm{H}^2(X_\lambda, \mathbb{Q}) = Pic(X_\lambda) \oplus T_\lambda \quad (22 = 19 + 3)$$

$$T_\lambda \simeq M_{\lambda^4}^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{4}, \tfrac{1}{2}, \tfrac{3}{4}),\ \beta = (1,1,1)$$

This generalizes to the Dwork pencil for Calabi–Yau threefolds

$$x^5 + y^5 + z^5 + w^5 + v^5 - 5\lambda xyzwv = 0 \subset \mathbb{P}^4$$

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

$$\mathrm{H}^2(X_\lambda, \mathbb{Q}) = Pic(X_\lambda) \oplus T_\lambda \quad (22 = 19 + 3)$$

$$T_\lambda \simeq M_{\lambda^4}^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{4}, \tfrac{1}{2}, \tfrac{3}{4}),\ \beta = (1,1,1)$$

  This generalizes to the Dwork pencil for Calabi–Yau threefolds

$$x^5 + y^5 + z^5 + w^5 + v^5 - 5\lambda xyzwv = 0 \subset \mathbb{P}^4$$

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

$$\mathrm{H}^2(X_\lambda, \mathbb{Q}) = Pic(X_\lambda) \oplus T_\lambda \quad (22 = 16 + 4)$$

$$T_\lambda \simeq M_{2^{10}3^6\lambda^{12}}^{\alpha,\beta} \text{ where } \alpha = (\tfrac{1}{12}, \tfrac{1}{6}, \tfrac{5}{12}, \tfrac{7}{12}, \tfrac{5}{6}, \tfrac{11}{12}),\ \beta = (0,0,0,\tfrac{1}{3}, \tfrac{1}{2}, \tfrac{2}{3})$$

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.

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).

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 $v_p(z-1) \neq 0$.

These are the primes supporting the conductor N.

L-functions of hypergeometric motives

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

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 $v_p(z-1) \neq 0$.

These are the primes supporting the conductor N.
Completing the L-function gives

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

We expect Λ to satisfy the functional equation

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

L-functions of hypergeometric motives

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 $v_p(z-1) \neq 0$.

These are the primes supporting the conductor N.

Completing the L-function gives

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

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

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

The Good, the Tame and the Wild

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

The Good, the Tame and the Wild

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

We do not yet have formulas for F_p at the wild primes.

There is a recipe for F_p at the tame primes.

The Good, the Tame and the Wild

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

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, i.e., 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

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

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 (C–Kedlaya–Roe )

We exhibit an algorithm to compute $a_p \pmod{p}$ for all primes $p \leq X$.
For fixed α, β, z, the complexity is $O(X)$ modulo log factors.

Hypergeometric L-functions in average polynomial time, II

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

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 (C–Kedlaya–Roe)

We exhibit an algorithm to compute $a_p \cancel{\pmod p}$ for all primes $p \le X$.
For fixed α, β, z, the complexity is $O(X)$ modulo log factors.

This enables the computation of L-functions with motivic weight > 1!

Amortization over primes

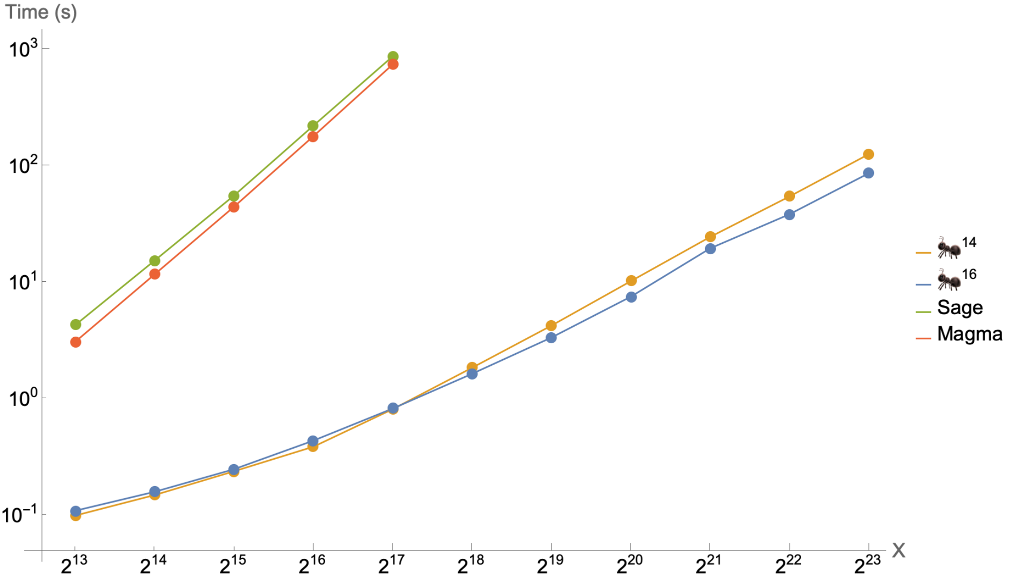
$$a_p = H_p \left(\begin{matrix} \alpha \\ \beta \end{matrix} \middle| z \right) := \frac{1}{1-p} \sum_{m=0}^{p-2} \pm p^{\xi(m)} \left(\prod_{j=1}^{r} \frac{(\alpha_j)^*_m}{(\beta_j)^*_m} \right) [z]^m,$$

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

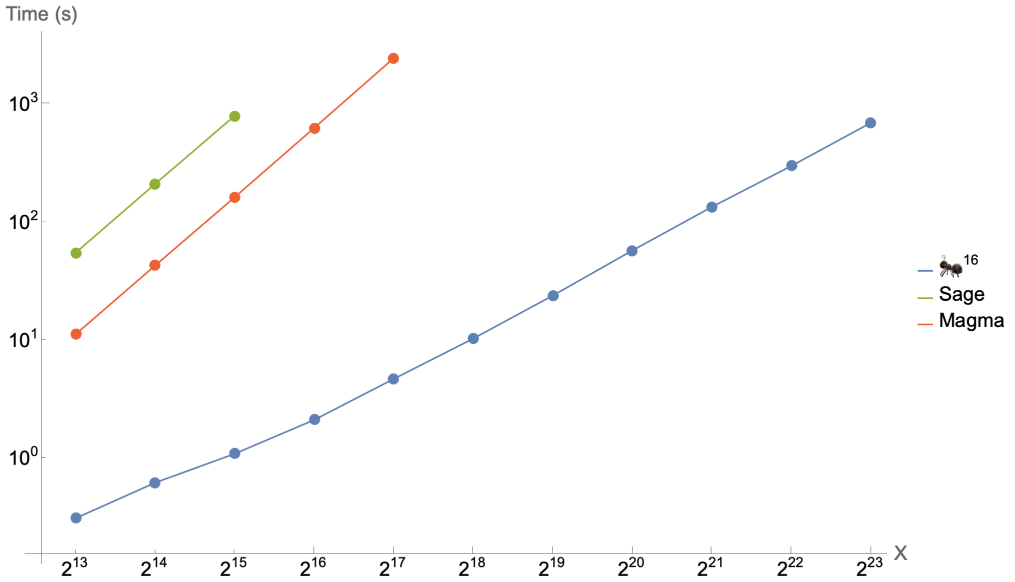
The implementations in `Magma` and `Sage` compute a_p one p at a time. Since the sum is over $O(p)$ terms, computing all prime Dirichlet coefficients up to X requires $O(X^2)$ (modulo log factors) arithmetic operations.

The shape of the formula makes it feasible to amortize this complexity over p, and thus requiring $O(X)$ (modulo log factors) arithmetic operations.

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



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



Amortization $\pmod p$ vs $\pmod{p^e}$

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

where $[z]$ is the multiplicative lift of $z \bmod p$, and

$$(\gamma)^*_m := \Gamma_p\left(\left\{\gamma + \frac{m}{1-p}\right\}\right)/\Gamma_p(\{\gamma\}) \quad \text{with } \{x\} := x - \lfloor x \rfloor$$

is the p-adic variant of the Pochhammer symbol.

Recall $\Gamma_p(x+1)/\Gamma_p(x) = \begin{cases} -x & x \in \mathbb{Z}_p^\times \\ -1 & x \in p\mathbb{Z}_p \end{cases}$ and observe $\frac{m}{1-p} = m \pmod p$.

Amortization $\pmod p$ vs $\pmod{p^e}$

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

where $[z]$ is the multiplicative lift of $z \bmod p$, and

$$(\gamma)_m^* := \Gamma_p\left(\left\{\gamma + \frac{m}{1-p}\right\}\right)/\Gamma_p(\{\gamma\}) \quad \text{with } \{x\} := x - \lfloor x \rfloor$$

is the p-adic variant of the Pochhammer symbol.

Recall $\Gamma_p(x+1)/\Gamma_p(x) = \begin{cases} -x & x \in \mathbb{Z}_p^\times \\ -1 & x \in p\mathbb{Z}_p \end{cases}$ and observe $\frac{m}{1-p} = m \pmod p$.

Ignoring the "discontinuities" that Γ_p and $\{\bullet\}$ introduce, computing $a_p \pmod p$ in spirit boils down to computing something like $\sum_{k=0}^{p-1} k! \bmod p$.

Amortization $\pmod{p}$ vs $\pmod{p^e}$

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

where $[z]$ is the multiplicative lift of $z \bmod p$, and

$$(\gamma)^*_m := \Gamma_p\left(\left\{\gamma + \frac{m}{1-p}\right\}\right)/\Gamma_p(\{\gamma\}) \quad \text{with } \{x\} := x - \lfloor x \rfloor$$

is the p-adic variant of the Pochhammer symbol.

Recall $\Gamma_p(x+1)/\Gamma_p(x) = \begin{cases} -x & x \in \mathbb{Z}_p^\times \\ -1 & x \in p\mathbb{Z}_p \end{cases}$ and observe $\frac{m}{1-p} = m \pmod{p}$.

Ignoring the "discontinuities" that Γ_p and $\{\bullet\}$ introduce, computing $a_p \pmod{p}$ in spirit boils down to computing something like $\sum_{k=0}^{p-1} k! \bmod p$.

One cannot ignore these issues, and that is the problem we solved in [14].

Remainder trees

The key is to reduce the problem to subproblems of the following form: given a square matrix $M(x)$ over $\mathbb{Z}[x]$, compute

$$M(0)\cdots M(\kappa(p)-1) \pmod p$$

for all primes p in some arithmetic progression.

Example

If $M(m) = \begin{pmatrix} g(m) & 0 \\ g(m) & f(m) \end{pmatrix}$, then $1 + \sum_{k=0}^{N-1} \prod_{m=0}^{k} \frac{f(m)}{g(m)} = \frac{S_{2,1}}{S_{1,1}}$ where $S = \prod_{m=0}^{N} M(m)$.

We use a very similar matrix in [14] to compute $a_p \pmod p$.

Remainder trees

The key is to reduce the problem to subproblems of the following form: given a square matrix $M(x)$ over $\mathbb{Z}[x]$, compute

$$M(0)\cdots M(\kappa(p)-1) \pmod{p}$$

for all primes p in some arithmetic progression.

Example

If $M(m) = \begin{pmatrix} g(m) & 0 \\ g(m) & f(m) \end{pmatrix}$, then $1 + \sum_{k=0}^{N-1} \prod_{m=0}^{k} \frac{f(m)}{g(m)} = \frac{S_{2,1}}{S_{1,1}}$ where $S = \prod_{m=0}^{N} M(m)$.

We use a very similar matrix in [14] to compute $a_p \pmod{p}$.

This paradigm excludes the possibility of computing expressions involving p.

Generic prime (Harvey)

One can sometimes circumvent this issue by having $M(x, P) \in \mathbb{Z}[x, P]/(P^e)$, where P is specialized to p at the end.

Amortization $\pmod p$ vs $\pmod{p^e}$

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

where $[z]$ is the multiplicative lift of $z \bmod p$, and

$$(\gamma)^*_m := \Gamma_p\left(\left\{\gamma + \frac{m}{1-p}\right\}\right)/\Gamma_p(\{\gamma\}) \quad \text{with } \{x\} := x - \lfloor x \rfloor$$

is the p-adic variant of the Pochhammer symbol.

To compute $a_p \pmod{p^e}$ we need to handle increments by $\frac{1}{1-p} = 1 + p + p^2 + \cdots$.

Amortization $\pmod p$ vs $\pmod{p^e}$

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

where $[z]$ is the multiplicative lift of $z \bmod p$, and

$$(\gamma)_m^* := \Gamma_p\left(\left\{\gamma + \frac{m}{1-p}\right\}\right) / \Gamma_p(\{\gamma\}) \quad \text{with } \{x\} := x - \lfloor x \rfloor$$

is the p-adic variant of the Pochhammer symbol.

To compute $a_p \pmod{p^e}$ we need to handle increments by $\frac{1}{1-p} = 1 + p + p^2 + \cdots$.


generic
prime ?

Decoupling 1 and $p/(1-p)$ increments

Idea

Decouple the effect of shifting the argument of Γ_p by a 1 and $p/(1-p) \in p\mathbb{Z}_p$.

$$\frac{\Gamma_p(\gamma + k + k\frac{p}{1-p})}{\Gamma_p(\gamma)} = \frac{\Gamma_p(\gamma + k\frac{p}{1-p})}{\Gamma_p(\gamma)} \cdot \frac{\Gamma_p(\gamma + k + k\frac{p}{1-p})}{\Gamma_p(\gamma + k\frac{p}{1-p})}$$

Decoupling 1 and $p/(1-p)$ increments

Idea

Decouple the effect of shifting the argument of Γ_p by a 1 and $p/(1-p) \in p\mathbb{Z}_p$.

$$\frac{\Gamma_p(\gamma + k + k\frac{p}{1-p})}{\Gamma_p(\gamma)} = \frac{\Gamma_p(\gamma + k\frac{p}{1-p})}{\Gamma_p(\gamma)} \cdot \frac{\Gamma_p(\gamma + k + k\frac{p}{1-p})}{\Gamma_p(\gamma + k\frac{p}{1-p})}$$

Lemma

One can compute $c_i(p)$ for all $p < X$ in $O(X)$ (modulo log factors) such that

$$\frac{\Gamma_p(\gamma + k\frac{p}{1-p})}{\Gamma_p(\gamma)} = \sum_{i=0}^{e-1} c_i(p)\left(k\frac{p}{1-p}\right)^i \pmod{p^e} \quad \forall_k.$$

Lemma

There exists $f \in \mathbb{Z}[y]/(y^e)$ such that $\frac{\Gamma_p(\gamma+k+y)}{\Gamma_p(\gamma+y)} = \prod_{j=1}^{k} f(y+j) \bmod p^e$ for k small.

We end up working in $\mathbb{Z}[y]/(y^e)$ where y will be replaced at the end by $\frac{p}{1-p}$.

Remainder trees redux (extremely oversimplified)

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

We set a product

$$M(1)\cdots M(k) = \begin{pmatrix}\Delta & 0\\ \Sigma & \Pi\end{pmatrix},$$

a block matrix of $e \times e$ matrices such that

- Δ is a scalar matrix
- $\Delta^{-1}\Sigma$ "records" $\sum_{m=0}^{k-1} \pmod{p^e}$
- $\Delta^{-1}\Pi$ "records" $p^{\xi(k)}\left(\prod_{j=1}^{r}\frac{(\alpha_j)^*_k}{(\beta_j)^*_k}\right)[z]^k$.

Slightly more precisely,

$$(c_0 \cdots c_{e-1}) \cdot \Delta^{-1}\Sigma \cdot (1\, p/(1-p) \cdots (p/(1-p))^{e-1})^T = \sum_{m=0}^{k-1} \pmod{p^e}$$