Algorithms for Algebraic and Arithmetic Attributes of Hypergeometric Functions

Xavier Caruso
CNRS; IMB, Université de Bordeaux
Talence, France
xavier@caruso.ovh

Florian Fürnsinn
University of Vienna, Faculty of Mathematics
Vienna, Austria
florian.fuernsinn@univie.ac.at

Abstract

We discuss algorithms for arithmetic properties of hypergeometric functions. Most notably, we are able to compute the p-adic valuation of a hypergeometric function on any disk of radius smaller than the p-adic radius of convergence. This we use, building on work of Christol, to determine the set of prime numbers modulo which it can be reduced. Moreover, we describe an algorithm to find an annihilating polynomial of the reduction of a hypergeometric function modulo p.

CCS Concepts

• **Computing methodologies → Symbolic and algebraic manipulation**.

Keywords

Algorithms, Hypergeometric Series, Algebraicity, Tropical algebra, Newton polygons

ACM Reference Format:

Xavier Caruso and Florian Fürnsinn. 2026. Algorithms for Algebraic and Arithmetic Attributes of Hypergeometric Functions. In *Proceedings of ACM Conference (ISSAC'26)*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 Introduction

A *hypergeometric function* with *top parameters* $\boldsymbol{\alpha} \coloneqq (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$ and *bottom parameters* $\boldsymbol{\beta} \coloneqq (\beta_1, \ldots, \beta_m) \in \mathbb{C}^m$ is defined as the power series

$$\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) \coloneqq \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \cdots (\alpha_n)_k}{(\beta_1)_k \cdots (\beta_m)_k} \cdot x^k \in \mathbb{C}[[x]],$$

where $(\gamma)_k \coloneqq \gamma(\gamma+1)\cdots(\gamma+k-1)$ denotes the *rising factorial* or *Pochhammer symbol*.

The second named author was funded by a DOC Fellowship (27150) of the Austrian Academy of Sciences at the University of Vienna. Further he thanks the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF grant 10.55776/I6130) for financial support.
The authors thank Austria's Agency for Education and Internationalisation (OeAD) and Campus France for providing funding for research stays via WTZ collaboration project/Amadeus project FR02/2024.

ISSAC'26, Oldenburg, Germany

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

We restrict ourselves to rational parameters for our investigation; in particular our hypergeometric functions are elements of $\mathbb{Q}[[x]]$. To simplify the exposition, we will also suppose that none of the α_i, β_j are nonpositive integers. We mention nevertheless that all our algorithms extend without this hypothesis, assuming only that the hypergeometric function $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ is well-defined.

Usually in the literature, hypergeometric functions are normalized differently. The hypergeometric function ${}_nF_m(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ is defined as $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}'; x)$, with $\boldsymbol{\beta}' = (\beta_1, \ldots, \beta_m, 1)$, *i.e.*, it includes an additional parameter 1 at the bottom. Conversely, $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) = {}_{n+1}F_m(\boldsymbol{\alpha}', \boldsymbol{\beta}; x)$ with $\boldsymbol{\alpha}' = (\alpha_1, \ldots, \alpha_n, 1)$. The classical notation is convenient to derive the differential equation

$$\big(x(\vartheta+\alpha_1)\cdots(\vartheta+\alpha_n) - \vartheta(\vartheta-\beta_1)\cdots(\vartheta-\beta_m)\big) \cdot {}_nF_m(\boldsymbol{\alpha}, \boldsymbol{\beta}; x) = 0,$$

where $\vartheta = x\frac{\mathrm{d}}{\mathrm{d}x}$. It shows that hypergeometric functions are *D-finite*, *i.e.*, they satisfy a nonzero linear differential equation with polynomial coefficients. However, for our arguments and algorithms, it proves more convenient not to insist on the additional parameter 1.

Hypergeometric functions play an important role in combinatorics and physics, for example the generating functions of many well-known sequences, such as the Catalan numbers, are of this shape. At the same time, hypergeometric functions serve as test examples for conjectures on algebraic and D-finite series. For example, Christol's conjectured in [12, 13] that *globally bounded* D-finite series (*i.e.,* D-finite series with positive radius of convergence, that can be reduced modulo almost all primes) can be written as diagonals of multivariate algebraic power series and then gave the first evidences by studying the class of hypergeometric functions. As of 2026, Christol's conjecture is still unsolved, even in the hypergeometric case, despite recent progress [5, 3, 4, 1, 6].

On a different note, we recall that a power series $f(x) \in K[[x]]$ is called *algebraic*, if there exists a nonzero polynomial $P[x, y] \in K[x, y]$, such that $P(x, f(x)) = 0$. Although D-finite power series $f(x) \in \mathbb{Q}[[x]]$ are usually not algebraic, it is frequently the case that their reductions modulo the primes are (see [10, Subsection 2.1] for many examples). For example, if Christol's conjecture on diagonals proves to be true, Furstenberg's theorem [17] would imply that the reduction of any globally bounded D-finite series is algebraic. In the article [10], written jointly with Vargas-Montoya, we went further in this direction and proposed a conjecture predicting what the Galois groups of D-finite functions modulo the primes could be.

Hypergeometric series form a class of examples for which algebraicity properties are well studied and understood: while there is only a small set of parameters $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ leading to algebraic series over $\mathbb{Q}$ [22, 20, 21, 15, 12, 2, 18, 16], it is known that reductions modulo p, when they exist, are always algebraic [12, 11, 24, 23] and certain Galois groups were computed in [10, Subsection 3.3].

Our contributions. The aim of the present article is to develop algorithmic tools for hypergeometric series, focusing particularly on reductions modulo primes and their algebraicity properties.

To start with, we describe an algorithm to determine the set of prime numbers, for which a given hypergeometric function can be reduced (Subsection 3.1). Our algorithm heavily relies on routines to compute the p-adic valuation of hypergeometric functions, which themselves find their roots in Christol's article [12], while similar approaches were also studied in [14, Prop. 24]. We develop those routines in Subsection 2.2 and extend them to the computation of Newton polygons (Subsection 2.3) and evaluation of hypergeometric functions at p-adic arguments (Subsection 2.4).

Then, building on the work of Christol, Vargas-Montoya and the authors [12, 11, 24, 23, 10], we design an algorithm to compute an annihilating polynomial of any hypergeometric series modulo p (Subsection 3.3). We underline that our approach gives in addition a new proof of algebraicity without any assumption on the parameters $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, nor on the prime p (aforementioned references often exclude certain cases for simplicity). In the same spirit, we mention that, while most of the questions considered in this paper simplify when the prime number p is chosen large enough with respect to the absolute value of the parameters and their common denominator, we especially take care to treat small primes as well. We believe that it is important for applications, given that large primes usually lead to huge outputs, *e.g.* huge annihilating polynomials, from which it looks more difficult to extract relevant information.

All the algorithms discussed in this article have been implemented in SageMath [9, 8] and can be tested online at the URL: https://xavier.caruso.ovh/notebook/hypergeometric-functions/

2 Valuations (the p-adic picture)

In this section, we fix a prime number p together with two tuples of parameters $\boldsymbol{\alpha} \coloneqq (\alpha_1, \dots, \alpha_n) \in \mathbb{Q}^n$ and $\boldsymbol{\beta} \coloneqq (\beta_1, \dots, \beta_m) \in \mathbb{Q}^m$. The aim of this section is to study the behavior of the p-adic valuation, denoted val_p, of the coefficients of associated hypergeometric series $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$.

To start with, we observe that, if γ is a rational number with $\mathrm{val}_p(\gamma) < 0$, one has $\mathrm{val}_p((\gamma)_k) = k \cdot \mathrm{val}_p(\gamma)$. Hence the valuations of the coefficients of $\mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ are directly related to the valuations of the coefficients of $\mathcal{H}(\boldsymbol{\alpha}', \boldsymbol{\beta}'; x)$ where the new parameters $\boldsymbol{\alpha}'$ and $\boldsymbol{\beta}'$ are obtained from $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ by removing the α_i and β_j with negative p-adic valuation. For this reason, we will always assume in what follows that $\mathrm{val}_p(\alpha_i)$ and $\mathrm{val}_p(\beta_j)$ are all nonnegative. We set $h(x) \coloneqq \mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ and we write h_k for the coefficient of $h(x)$ in x^k.

2.1 Zigzag functions

We fix a positive integer $r > 0$. Let $w_r : \mathbb{N} \to \mathbb{N}$ be the sequence defined by $w_r(0) = 0$ and the recurrence relation

$$\begin{aligned} w_r(k+1) = w_r(k) &+ \left|\{1 \le i \le n : k + \alpha_i \equiv 0 \bmod p^r\}\right| \\ &- \left|\{1 \le j \le m : k + \beta_j \equiv 0 \bmod p^r\}\right|. \end{aligned}$$

We follow Kedlaya's terminology, see for example [19], and call w_r a *zigzag function.* We start by noticing that

$$\forall k \ge 0, \quad w_r(k + p^r) = w_r(k) + (n - m). \tag{1}$$

Besides, the function w_r does not vary often. More precisely, we define the set $\Gamma \coloneqq \{1, \alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m\}$ and denote by s its cardinality. Let also

$$0 = \xi_{r,0} \le \xi_{r,1} \le \cdots \le \xi_{r,s-1} < p^r$$

be the reductions modulo p^r of $1 - \gamma$, for $\gamma \in \Gamma$, sorted in ascending order. We prolong the sequence $(\xi_{r,i})_i$ by repeating the same values translated by p^r, $2p^r$, *etc.* Formally, we set $\xi_{r,i+s} = \xi_{r,i} + p^r$ for $i \ge 0$. Then, on each interval $I_{r,i} \coloneqq [\xi_{r,i}, \xi_{r,i+1})$, the sequence w_r is constant.

We note that, the reductions modulo p^r of a rational number x with denominator coprime with p, can be read off on its p-adic expansion. More precisely, if

$$x = x_0 + x_1 p + x_2 p^2 + \cdots \in \mathbb{Z}_p$$

we have $x \bmod p^r = x_0 + x_1 p + \cdots + x_{r-1} p^{r-1}$. If we assume moreover that x is not a nonnegative integer, its p-adic expansion is not finite, which implies that $x \bmod p^r$ goes to infinity when r grows. More precisely, using that the sequence (x_i) is ultimately periodic (since x is a rational number), we find that $x \bmod p^r$ grows at least linearly in p^r. As a consequence, we derive that $\xi_{r,1} \ge c p^r$ for some constant c depending only on $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$.

Lemma 2.1. *For $k \ge 0$, we have $\mathrm{val}_p(h_k) = \sum_{r=1}^{\infty} w_r(k)$.*

The proof of the lemma follows the standard argument used to prove Legendre's formula giving the p-adic valuation of a factorial (see also [12, Equation (6)]).

Noticing that w_r vanishes on the interval $[0, \xi_{r,1})$, we derive from the estimation $\xi_{r,1} \ge c p^r$ that the the sum of Theorem 2.1 is finite for any given k; more precisely it contains at most $\log_p(k) + O(1)$ terms.

Proposition 2.2. *We have $\lim_{k\to\infty} \frac{\mathrm{val}_p(h_k)}{k} = \frac{n-m}{p-1}$.*

Proof. For $k < p^r$, we have $-m \le w_r(k) \le n$. Using Equation (1), this implies that there exists some constant M, such that

$$\left| w_r(k) - k \cdot \tfrac{n-m}{p^r} \right| \le M$$

for arbitrary k. Summing over r and using a geometric sum and the triangle inequality, we then find

$$\left| \mathrm{val}_p(h_k) - k \cdot \tfrac{n-m}{p-1} + k \cdot \tfrac{n-m}{p^s(p-1)} \right| \le Ms,$$

where $s = \log_p(k) + O(1)$ is the number of summands involved in the sum of Theorem 2.1. The term $k \cdot \frac{n-m}{p^s(p-1)}$ then remains bounded when k grows, proving that

$$\left| \mathrm{val}_p(h_k) - k \cdot \tfrac{n-m}{p-1} \right| \le M \log_p(k) + O(1).$$

The proposition follows. □

2.2 Drifted valuations

The valuation of the hypergeometric series $h(x)$ is defined as the minimum of $\mathrm{val}_p(h_k)$ when k varies. More generally, we define its *ν-drifted valuation* by

$$\mathrm{val}_{p,\nu}(h(x)) \coloneqq \min_{k \ge 0} \mathrm{val}_p(h_k) + \nu k.$$

Working with drifted valuations is important to handle smoothly the reduction to parameters whose denominators are not divisible by p, and will be also crucial when we will study Newton polygons in Subsection 2.3.

2.2.1 Recurrence over the tropical semiring. It follows from Theorem 2.2 that $\mathrm{val}_{p,\nu}(h(x)) = -\infty$ when $\nu < \nu_0 := \frac{m-n}{p-1}$. From now on, we will then assume that $\nu \geq \nu_0$. For $r \in \mathbb{N}$ we introduce the drifted partial sums

$$\sigma_r : \mathbb{N} \to \mathbb{Q}, \quad k \mapsto \nu k + \textstyle\sum_{s=1}^{r} w_s(k).$$

It directly follows from Theorem 2.1 that

$$\forall k \geq 0, \quad \mathrm{val}_p(h_k) + \nu k = \lim_{r\to\infty} \sigma_r(k).$$

Besides, the sequence σ_r satisfies the periodicity condition

$$\forall k \geq 0, \quad \sigma_r(k + p^r) = \sigma_r(k) + (\nu - \nu_0)p^r + \nu_0. \tag{2}$$

We recall that we have defined in Subsection 2.1 the numbers $\xi_{r,i}$ and the intervals $I_{r,i} = [\xi_{r,i}, \xi_{r,i+1})$, in such a way that the function w_r is constant on each $I_{r,i}$. We let $\mu_{r,i}$ denote the minimum of σ_r on this interval (with the convention that $\mu_{r,i} = +\infty$ if $I_{r,i}$ is empty). We are going the prove that the $\mu_{r,i}$ are subject to recurrence relations which allows to compute them recursively. First of all, with respect to the variable i, we have the relation

$$\mu_{r,i+s} = \mu_{r,i} + (\nu - \nu_0)p^r + \nu_0 \tag{3}$$

which follows directly from Equation (2). Hence the knowledge of the first s terms of the sequence $(\mu_{r,i})_{i\geq 0}$ is enough to reconstruct the whole sequence.

We now move to the variable r. We first note that the $\mu_{1,i}$ are easily computed since σ_1 is affine on all intervals $I_{1,i}$. The key observation to go from $r-1$ to r is that each $\xi_{r,i}$, being the reduction modulo p^r of one of the $1-\gamma$ for $\gamma \in \Gamma$, also appears in the sequence $(\xi_{r-1,j})_j$. In other words, there exists an index $j_{r,i}$ such that $\xi_{r,i} = \xi_{r-1,j_{r,i}}$. Setting $J_{r,i} = \mathbb{Z} \cap [j_{r,i}, j_{r,i+1})$, we deduce that $I_{r,i}$ is the disjoint union of the $I_{r-1,j}$ for j varying in $J_{r,i}$ and then

$$\mu_{r,i} = w_r(\xi_{r,i}) + \min_{j\in J_{r,i}} \mu_{r-1,j}. \tag{4}$$

It is convenient to reformulate what precedes in the language of tropical algebra. We let $\mathcal{T}$ denote the tropical semiring $\mathbb{Q} \sqcup \{+\infty\}$ equipped with the operations $\oplus = \min$ and $\odot = +$. We set $\boldsymbol{\mu}_r = (\mu_{r,0}, \ldots, \mu_{r,s-1})$ and view it as a row vector over $\mathcal{T}$. Then Equation (4) translates to a relation of the form

$$\boldsymbol{\mu}_r = \boldsymbol{\mu}_{r-1} \odot T_r \tag{5}$$

where T_r is a square matrix over $\mathcal{T}$ of size s, which is explicit in terms of the functions w_r.

2.2.2 Halting criterion. Equation (5) gives an efficient recursive method to compute the $\mu_{r,i}$. Besides, remembering that $\xi_{r,1}$ goes to infinity when r grows, we find that $\mathrm{val}_{p,\nu}(h(x)) = \lim_{r\to\infty} \mu_{r,0}$.

It then only remains to find a criterion to detect when the limit is attained.

Let d denote a common denominator of the elements of Γ, and let e be the multiplicative order of p modulo d.

Lemma 2.3. *If r fulfills the three following requirements*

- $r > e + \log_p \max\{1, |1-\gamma_1|, \ldots, |1-\gamma_{s-1}|\}$,
- $p^r(\nu - \nu_0) + \nu_0 \geq me$
- $\mu_{r,i} \geq \mu_{r,0} + me$ *for all* $i \in \{1, \ldots, s-1\}$,

then $\mu_{r',0} = \mu_{r,0}$ *for all* $r' \geq r$.

The proof of Theorem 2.3 uses the following result.

Lemma 2.4. *Let $x \in \mathbb{Z}_{(p)}$ and let $x = \sum_{r\geq 0} x_r p^r$ be its p-adic expansion, with $x_r \in \{0, 1, \ldots, p-1\}$ for all r. Let e be the multiplicative order of p modulo the denominator of x. Then $x_{r+e} = x_r$ for all $r > e + \max(0, \log_p |x|)$.*

Proof. Set $d := p^e - 1$. It follows from the definition of e that dx is an integer. Therefore we can write $x = a + \frac{b}{d}$ with $a, b \in \mathbb{Z}$ and $0 \leq b < d$. If $b_0, \ldots, b_{e-1}$ are the digits in base p of b, the p-adic expansion of $\frac{b}{d}$ is $\sum_{i=0}^{\infty} b_{i \bmod e} \cdot p^i$. Hence, it is periodic (from the start) of period e.

We first assume that $a \geq 0$. Then its p-adic expansion is finite and has $1 + \lfloor \log_p a \rfloor$ digits. Moreover, while performing the addition $a + \frac{b}{d}$, the last carry can move at most by e digits given that $b_0, \ldots, b_{e-1}$ cannot be all equal to $p-1$. The lemma follows in this case.

The case $a = -1$ is similar by writing down the subtraction.

Finally, if $a < -1$, we replace x by $-1-x$. This has the effect of replacing every digit x_r of x by $p-1-x_r$, which does not change the periodicity properties. So, we are back to the case $a \geq 0$. ◻

Proof of Lemma 2.3. Given Equation (3), the second and third requirements together imply that $\mu_{r,i} \geq \mu_{r,0} + me$ for all $i \geq 1$. Therefore, using Equation (4), we find $\mu_{r+1,0} = \mu_{r,0}$ (since $0 \in J_{r+1,0}$) and $\mu_{r+1,i} \geq \mu_{r,0} + m(e-1)$ for all $i \geq 1$ (since $w_{r+1}(\xi_{r+1}, i) \geq -m$ for all i). Repeating the same argument, we obtain by induction on r' that, $\mu_{r',0} = \mu_{r,0}$ and

$$\forall i \geq 1, \quad \mu_{r',i} \geq \mu_{r,i} + m(e + r - r').$$

for $r' \in \{r+1, \ldots, r+e\}$. In order to continue the induction beyond $r+e$, we observe that the first assumption and Theorem 2.4 ensure that the values $1-\gamma \bmod p^r$, for $\gamma \in \Gamma$, are sorted in the same way as $1-\gamma \bmod p^{r+e}$. Thus, the values $\xi_{i,r}$ and $\xi_{i,r+e}$ correspond to the same parameter for all i. We deduce that $\xi_{r+e,i} \geq \xi_{r,i} + p^r$ for $i < s$. Applying Equation (4) with $r+1, \ldots, r+e$ as before, we find

$$\begin{aligned}\mu_{r+e,i} &\geq \mu_{r,i} + (\nu - \nu_0)p^r + \nu_0 - me \\ &\geq \mu_{r,0} + me = \mu_{r+e,0} + me.\end{aligned}$$

Therefore, the requirements of the lemma are also fulfilled with r replaced by $r+e$, and the induction can go on. ◻

When $\nu > \nu_0$, it follows from Theorem 2.2 that the $\mu_{r,i}$ with $i > 0$ grow at least linearly in p^r. The condition of Theorem 2.3 will then be rapidly fulfilled.

On the contrary, when $\nu = \nu_0$, we rely on the following lemma.

Lemma 2.5. *We assume $\nu = \nu_0$ and let r_0 be the smallest integer greater than $e + \log_p \max\{1, |1-\gamma_1|, \ldots, |1-\gamma_{s-1}|\}$. Then the sequence $(T_r)_{r\geq r_0}$ is periodic of period e.*

Proof. Let $r \geq r_0$. We have seen in the proof of Theorem 2.3 that $\xi_{r,i}$ and $\xi_{r+e,i}$ correspond to the same (top or bottom) parameter for all i. It follows that $w_{r+e}(\xi_{r+e,i}) = w_r(\xi_{r,i})$ and $J_{r+e,i} = J_{r,i}$ for all i. Therefore $T_{r+e} = T_r$ by Equation (4). ◻

We set $T := T_{r_0+1} \odot T_{r_0+2} \odot \cdots \odot T_{r_0+e} \in M_s(\mathcal{T})$. Then $\boldsymbol{\mu}_{r_0+\ell e} = \boldsymbol{\mu}_{r_0} \odot T^{\odot \ell}$ for all $\ell \geq 0$. Noticing in addition that the sequence $(\mu_{r,0})_{r\geq 0}$ is nonincreasing, we find that $\mathrm{val}_{p,\nu}(h(x))$ is the first coordinate of $\boldsymbol{\mu}_{r_0} T^+$ where

$$T^+ := T + T^{\odot 2} + T^{\odot 3} + \cdots \tag{6}$$

is the so-called *weak transitive closure* of T (see [7, §1.6.2]). The latter can be efficiently computed using the Floyd–Warshall algorithm (see [7, Algorithm 1.6.21]), which then completes our algorithm.

We underline nonetheless that the sum of Equation (6) may diverge. This is however not an issue; indeed, this case is detected by the Floyd–Warshall algorithm and it corresponds to the situation where $\mathrm{val}_{p,\nu}(h(x)) = -\infty$. Hence, we can conclude in all cases.

Remark 2.6. We can adapt the previous algorithm so that it computes in addition the smallest integer k such that $\mathrm{val}_p(h_k)+\nu k = \mathrm{val}_{p,\nu}(h(x))$. For doing this, we compute the integers

$$k_{r,i} \coloneqq \min\left\{k \in I_{r,i} : \sigma_r(h_k) = \mu_{r,i}\right\}$$

at the same time as the $\mu_{r,i}$ while running the algorithm. We recover k at the end of the computation using $k = \lim_{r\to\infty} k_{r,0}$.

2.2.3 An example. We consider the parameters $\boldsymbol{\alpha} = \left(\frac{1}{3}, \frac{4}{3}\right)$ and $\boldsymbol{\beta} = \left(\frac{2}{3}, 1\right)$, set $h(x) = \mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ and want to compute $v_{p,0}(h(x))$.

We start with $p = 7$. We then have $\nu_0 = 0$ and we take $\nu = 0$ as well. Given that $p \equiv 1 \pmod 3$, we find that the reductions of the $1-\alpha_i$ and $1-\beta_j$ modulo p^r are

$$\xi_{r,0} = 0, \quad \xi_{r,1} = \tfrac{p^r-1}{3}, \quad \xi_{r,2} = \tfrac{p^r+2}{3}, \quad \xi_{r,3} = \tfrac{2p^r+1}{3}$$

corresponding to the parameters 1, $\frac{4}{3}$, $\frac{1}{3}$ and $\frac{2}{3}$ respectively. The zigzag function w_r is p^r-periodic and

- it takes the value 0 on the interval $[0, \xi_{r,1})$,
- it takes the value 1 on the interval $[\xi_{r,1}, \xi_{r,2})$,
- it takes the value 2 on the interval $[\xi_{r,2}, \xi_{r,3})$,
- it takes the value 1 on the interval $[\xi_{r,3}, p^r)$.

From this, we infer the $J_{r,i}$ (see Figure 1) and the matrices $T_r \in M_4(\mathcal{T})$; they are independent of r and given by:

$$T_r = \begin{pmatrix} 0 & +\infty & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & +\infty & 2 & 1 \\ 0 & +\infty & 2 & 1 \end{pmatrix}.$$

The Floyd–Warshall algorithm gives $T^+ = T_r$. We finally compute $\boldsymbol{\mu}_1 = (0, 1, 2, 1)$ and conclude that $\mathrm{val}_{p,0}(h(x))$ is the first coordinate of the vector $\boldsymbol{\mu}_1 \odot T^+ = (0, 2, 2, 1)$, *i.e.* $\mathrm{val}_{p,0}(h(x)) = 0$.

We now take $p = 11$ and continue with $\nu = 0$. In this case, the "ξ-ordering" depends on the parity of r. Precisely, if r is even,

$$\xi_{r,0} = 0, \quad \xi_{r,1} = \tfrac{p^r-1}{3}, \quad \xi_{r,2} = \tfrac{p^r+2}{3}, \quad \xi_{r,3} = \tfrac{2p^r+1}{3}$$

corresponding to the parameters 1, $\frac{4}{3}$, $\frac{1}{3}$ and $\frac{2}{3}$ respectively as before. However, if r is odd, we have

$$\xi_{r,0} = 0, \quad \xi_{r,1} = \tfrac{p^r+1}{3}, \quad \xi_{r,2} = \tfrac{2p^r-1}{3}, \quad \xi_{r,3} = \tfrac{2p^r+2}{3}$$

corresponding to the parameters 1, $\frac{2}{3}$, $\frac{4}{3}$, $\frac{1}{3}$ in this order. Therefore, the matrix T_r also depends on the parity of r; a calculation gives

$$T_{2r'} = \begin{pmatrix} 0 & +\infty & 2 & 1 \\ 0 & +\infty & 2 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & +\infty & 2 & 1 \end{pmatrix} \quad ; \quad T_{2r'+1} = \begin{pmatrix} 0 & -1 & +\infty & 1 \\ 0 & -1 & 0 & 1 \\ 0 & -1 & +\infty & 1 \\ 0 & -1 & +\infty & 1 \end{pmatrix}.$$

Hence

$$T = T_{2r'} \odot T_{2r'+1} = \begin{pmatrix} 0 & -1 & +\infty & 1 \\ 0 & -1 & +\infty & 1 \\ 0 & -1 & 1 & 1 \\ 0 & -1 & +\infty & 1 \end{pmatrix}.$$

In this case, the sum of Equation (6) defining T^+ does not converge (this is due to the coefficient -1 on the diagonal) and so, we conclude that $\mathrm{val}_{p,0}(h(x)) = -\infty$.

In § 3.1 we will see that all primes essentially follow the pattern displayed for either $p = 7$ or $p = 11$.

2.2.4 Complexity. Our algorithm manipulates rational numbers whose size can significantly grow during the execution. For this reason, we will estimate its complexity by counting bit operations.

In what follows, we use the standard soft-O notation $O^\sim(-)$ to hide logarithmic factors. We also assume that FFT-based algorithms are used to perform multiplications on integers; an operation on two integers of B bits then requires at most $O^\sim(B)$ bit operations.

Proposition 2.7. *Let r_0 be defined as in Theorem 2.5 and let D be a common denominator of ν and ν_0. Then, the algorithm described in §§2.2.1–2.2.2 performs at most*

- *Case $\nu = \nu_0$:* $O^\sim\big((n+m)^2 r_0 \log p + (n+m)^3 \log(r_0 p)\big)$
- *Case $\nu > \nu_0$:* $O^\sim\big((n+m)^2(r_0 \log p + \log D)\big(r_0 \log p - \log\min(1, \nu-\nu_0)\big)\big)$

bit operations.

Proof. For simplicity, we set $w = n + m$.

We first observe that, throughout the algorithm, the computer only manipulates rational numbers in $\frac{1}{D}\mathbb{Z}$. Besides, the finite entries of the matrix T_r are all in $O\big(w + (\nu - \nu_0)p^r\big)$.

To start with, we assume that $\nu = \nu_0$. In this case, D is a divisor of $p-1$, so $D \leq p$. We need to compute $\boldsymbol{\mu}_r$ until $r = r_0 + e = O(r_0)$. For a fixed r, computing $\boldsymbol{\mu}_r$ from $\boldsymbol{\mu}_{r-1}$ requires $O(s^2) \subset O(w^2)$ operations on rational numbers of order of magnitude $O(wr)$. This can be done within $O^\sim(w^2 \log(rp))$ bit operations. In total, computing all the requires μ_r then costs $O^\sim(w^2 r_0 \log p)$ bit operations. Finally, applying the Floyd–Warshall requires $O(s^3)$ additional operations on rational numbers in $O(wr_0)$; this costs at most $O^\sim(w^3 \log(r_0 p))$ bit operations.

We now move to the case where $\nu > \nu_0$. Let R be the first integer for which the requirements of Theorem 2.3 are fulfilled. It follows from the proof of Theorem 2.3 that $\xi_{r,1} \geq p^{r-r_0}$ for all r. Following the proof of Proposition 2.2, we deduce that

$$\mu_{r,1} \geq (\nu - \nu_0)p^{r-r_0} - wr + O(p^{r_0})$$

which in turn implies that $p^R = O^\sim\Big(\frac{wp^{r_0}}{\nu-\nu_0} + p^{2r_0}\Big)$.

Hence the finite entries of the matrices T_r with $r \leq R$ are all in $O^\sim(wp^{r_0} + p^{2r_0})$. As in the first part of the proof, we deduce that the computations of $\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_R$ requires at most

$$O^\sim\big(w^2 R(r_0 \log p + \log D)\big)$$

bit operations. We conclude the proof by noticing that

$$R = O\big(\log w + r_0 \log p - \log\min(1, \nu-\nu_0)\big). \qquad \square$$

2.3 Newton polygons

The *Newton polygon* $\mathrm{NP}(h)$ of the series $h(x)$ is, by definition, the topological closure of the convex hull in $\mathbb{R}^2$ of the points of coordinates (k, v) with $v \geq \mathrm{val}_p(h_k)$. The Newton polygon is closely

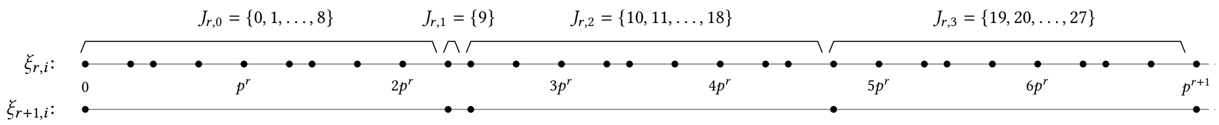


Figure 1: The sets $J_{r,i}$ for $\boldsymbol{\alpha} = \left(\frac{1}{3}, \frac{4}{3}\right)$, $\boldsymbol{\beta} = \left(\frac{2}{3}, 1\right)$ and $p = 7$

related to the drifted valuations; indeed, for $\nu \geq \nu_0$, we have

$$\mathrm{val}_{p,\nu}(h(x)) = \min_{(a,b)\in \mathrm{NP}(h)} a\nu + b.$$

To model these relations, we introduce two new tropical semirings:

(1) the set $\mathcal{F}$ of concave functions $f : [\nu_0, +\infty) \to \mathbb{R} \sqcup \{+\infty\}$; we endow $\mathcal{F}$ with the pointwise operations $\oplus = \min$ and $\odot = +$
(2) the set $\mathcal{N}$ of closed convex subsets $N \subset \mathbb{R}^2$ which are stable under the translations by $(0, 1)$ and $(1, \nu_0)$, endowed with

$$N_1 \oplus N_2 = \text{convex hull of } N_1 \cup N_2,$$
$$N_1 \odot N_2 = N_1 + N_2 \text{ (Minkowski sum)}.$$

We have a map $\varepsilon : \mathcal{N} \to \mathcal{F}$ that takes N to the function

$$\varepsilon(N) : \nu \mapsto \min_{(a,b)\in N} a\nu + b.$$

One checks that ε is a morphism of semirings. Moreover, the theorem of Hahn–Banach implies that it is an isomorphism, its inverse being given by the map that takes $f \in \mathcal{F}$ to the subset of $\mathbb{R}^2$ consisting of pairs (a, b) such that $f(\nu) \leq a\nu + b$. A decisive advantage of $\mathcal{N}$ (over $\mathcal{F}$) is that it provides concrete algorithmic perspectives, given that handling operations in $\mathcal{N}$ is effectively doable (at least when the convex sets are described by finite amounts of data).

2.3.1 Recurrence over $\mathcal{N}$. We are now in position to design a uniform version (with respect to ν) of the algorithm of Subsection 2.2; roughly speaking, it simply consists in replacing $\mathcal{T}$ by $\mathcal{N}$ everywhere. Precisely, we define the $\mu_{r,i} \in \mathcal{N}$ by the relations

$$\mu_{1,i} = \textstyle\bigoplus_{\xi\in I_{1,i}} \varepsilon^{-1}\big(\nu \mapsto \xi\nu + w_1(\xi)\big),$$
$$\mu_{r,i} = \varepsilon^{-1}\big(\nu \mapsto w_r(\xi_{r,i})\big) \odot \Big(\textstyle\bigoplus_{j\in J_{r,i}} \mu_{r-1,j}\Big).$$

We notice in addition that ε^{-1} of the affine function $\nu \mapsto a\nu + b$ is simply the convex subset of $\mathbb{R}^2$ with one vertex at (a, b) and two rays in the directions $(0, 1)$ and $(1, \nu_0)$. In particular, multiplying by $\varepsilon^{-1}(\nu \mapsto w_r(\xi_{r,i}))$ is nothing but translating the convex set by the vector $(0, w_r(\xi_{r,i}))$.

As in Subsection 2.2, the $\mu_{r,i}$ are subject to a recurrence relation with respect to i, which reads

$$\mu_{r,i+s} = \mu_{r,i} \odot \varepsilon^{-1}\big(\nu \mapsto (\nu - \nu_0)p^r + \nu_0\big)$$

(compare with Equation (3)). This allows to only retain the s first terms of the sequences $(\mu_{r,i})_{i\geq 0}$: setting $\boldsymbol{\mu}_r = (\mu_{r,0}, \ldots, \mu_{r,s-1})$, we have a relation of the form $\boldsymbol{\mu}_r = \boldsymbol{\mu}_{r-1} \odot T_r$ where T_r is now a square matrix of size s with entries in $\mathcal{N}$.

Finally, the Newton polygon of $h(x)$ is obtained as the first coordinate of

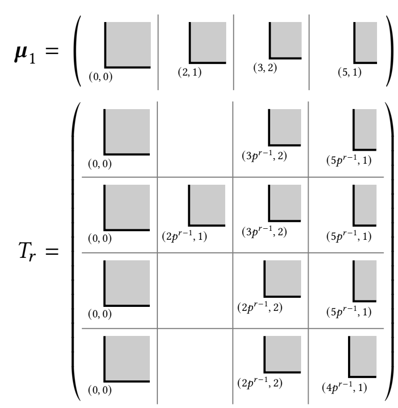
$$\textstyle\bigoplus_{\ell\geq 1} \boldsymbol{\mu}_1 \odot T_2 \odot \cdots \odot T_\ell. \tag{7}$$

When $\mathrm{val}_{p,\mu_0}(h(x))$ is finite, it follows from what we did in Subsection 2.2 and [7, Proposition 1.6.15] that the above infinite sum can be truncated to $\ell \leq r_0 + s$ (with the notation introduced at the end of Subsection 2.2) without changing the final result. We then get a complete algorithm to compute $\mathrm{NP}(h)$.

On the contrary, when $\mathrm{val}_{p,\mu_0}(h(x)) = -\infty$, the sum of Equation (7) converges but it cannot be reduced to a finite sum: each additional term provides more and more accurate approximations of $\mathrm{NP}(h)$. This is perfectly in line with the fact that $\mathrm{NP}(h)$ has an infinite number of slopes in this case. An option to nevertheless obtain a meaningful result is to shrink a bit the domain of definition of the functions and replace ν_0 by another bound $\nu_1 > \nu_0$. Doing this, the sum of Equation (7) again reduces to a finite sum, and we can decide when the computation can be stopped using the condition of Theorem 2.3; indeed, inequalities of functions correspond to inclusions of Newton polygons and so, they can easily be checked.

2.3.2 An example. We continue the example of Subsection 2.2.3. We start with $p = 7$. In this case, finding the Newton polygon is easy. Indeed, we already know that $\mathrm{val}_{p,0}(h(x)) = 0$. Besides, we derive from Proposition 2.2 that $\mathrm{val}_p(h_k) = o(k)$. This readily implies $\mathrm{NP}(h) = \mathbb{R}^+ \times \mathbb{R}^+$.

Let us nonetheless apply our algorithm and show that it outputs the same result. In our case, the vector $\boldsymbol{\mu}_1$ and the matrix $T_r \in M_4(\mathcal{N})$ are the following ones:



We recall that the Newton polygon we are looking for is the limit of the first coordinate of Equation (7) when r goes to infinity. In our case, we observe that all the entries of $\boldsymbol{\mu}_1$ and T_r are subsets of $\mathbb{R}^+ \times \mathbb{R}^+$. Therefore, for all $r \geq 2$, the four coordinates of $\boldsymbol{\mu}_1 \odot T_2 \odot \cdots \odot T_r$ are also subsets of $\mathbb{R}^+ \times \mathbb{R}^+$. We conclude that $\mathrm{NP}(h) = \mathbb{R}^+ \times \mathbb{R}^+$ as expected.

When $p = 11$, on the contrary, we are in the situation where $\mathrm{val}_{p,0}(h(x)) = -\infty$, meaning that the limit of Equation (7) is not reached at finite level. In this case, the matrices T_r are those shown on Figure 2 and we can see that the entries of the second column of T_r are not subsets of $\mathbb{R}^+ \times \mathbb{R}^+$ when r is odd. What happens more precisely is that each summand in Equation (7) corresponding to an odd number $\ell = 2r' - 1$ introduces a new vertex $V_{r'}$ with

y-coordinate equal to $-r'$. This vertex then propagates to the first coordinate and eventually contributes to the Newton polygon.

As explained in the description of the algorithm, we can avoid this by slightly degrading the precision and adding a ray in the direction $(0, v_1)$ (with $v_1 > 0$ fixed) to all entries of $\boldsymbol{\mu}_1$ and T_r. This will absorb the vertices $V_{r'}$ for r' large enough.

Remark 2.8. Carrying out all computations, one finds that the vertices of $\mathrm{NP}(h)$ are the points $\left(4\frac{p^{2r'}-1}{p^2-1}, -r'\right)$ with $r' \in \mathbb{N}$. In this particular example, they then exhibit very strong regularity patterns. One may wonder whether this is a general phenomenon and, if it is, if we can use it to compute $\mathrm{NP}(h)$ and/or to accelerate the computation of $\mathrm{val}_{p,\nu}(h(x))$ when $\nu > \nu_0$.

2.4 Application to p-adic evaluation

Proposition 2.2 ensures that, if $\mathrm{val}_p(x) > \nu_0$, then $\mathrm{val}_p(h_k x^k)$ goes to infinity when k grows, and so the hypergeometric series $\sum_k h_k x^k$ converges for the p-adic topology. Hence, it defines a function $h : B_{\nu_0} \to \mathbb{Q}_p$ where $\mathbb{Q}_p$ is the field of p-adic numbers and B_{ν_0} is its open disc centered at 0 of radius $p^{-\nu_0}$. In what follows, we briefly outline an algorithm to compute $h(a)$ at precision $O(p^N)$ for given $a \in B_{\nu_0}$ and $N \in \mathbb{Z}$.

Lemma 2.9. *Let ν be a real number the interval $(\nu_0, \mathrm{val}_p(a))$. Then $\mathrm{val}_k(h_k a^k) \geq N$ for all $k \geq K := \frac{N - \mathrm{val}_{p,\nu}(h(x))}{\mathrm{val}_p(a) - \nu}$.*

Proof. The lemma follows from the inequality

$$\mathrm{val}_p(h_k a^k) \geq \mathrm{val}_{p,\nu}(h(x)) + k \cdot (\mathrm{val}_p(a) - \nu)$$

which is a direct consequence of the definition of $\mathrm{val}_{p,\nu}(h(x))$. □

To compute $h(a)$, we then proceed as follows:
(1) we choose a rational number $\nu \in (\nu_0, \mathrm{val}_p(a))$,
(2) we compute $\mathrm{val}_{p,\nu}(h(x))$ using the algorithm of §2.2,
(3) we compute the bound K of Lemma 2.9,
(4) we output $\sum_{k<K} h_k a^k + O(p^N)$.

Although the previous algorithm works for any value of ν, bad choices could lead to huge truncation bounds and so, dramatic performances. Nonetheless, we know from the proof of Proposition 2.2 that the order of magnitude of $\nu_0 k - \mathrm{val}_p(h_k)$ is about $\log_p(k)$. Using this approximation and solving the corresponding optimization problem, one finds the following heuristic for the choice of ν:

$$\nu = \nu_0 + \frac{\mathrm{val}_p(a) - \nu_0}{N} \in (\nu_0, \mathrm{val}_p(a)).$$

In practice, this choice leads to K close to $\frac{N}{\mathrm{val}_p(a) - \nu_0}$, which is basically the best we can hope for.

3 Reduction modulo primes

We fix a prime number p and we let $\mathbb{Z}_{(p)}$ denote the subring of $\mathbb{Q}$ consisting of rational numbers x such that $\mathrm{val}_p(x) \geq 0$, *i.e.* rational numbers $\frac{a}{b}$ with $\gcd(b, p) = 1$. Any element of $\mathbb{Z}_{(p)}$ can be reduced modulo p, yielding a result in $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$.

It may happen for some parameters $\boldsymbol{\alpha}, \boldsymbol{\beta}$ that *all* the coefficients $(h_k)_{k\geq 0}$ of $h(x) = \mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x)$ lie in $\mathbb{Z}_{(p)}$ or, equivalently, that $\mathrm{val}_{p,0}(h(x)) \geq 0$. In this case, we say that $h(x)$ has *good reduction* modulo p and we write $h(x) \bmod p$ for the image of $h(x)$ in $\mathbb{F}_p[[x]]$.

3.1 Good reduction primes

We fix two tuples to parameters $\boldsymbol{\alpha} \in \mathbb{Q}^n$ and $\boldsymbol{\beta} \in \mathbb{Q}^m$ and set

$$h(x) = \textstyle\sum_{k\geq 0} h_k x^k := \mathcal{H}(\boldsymbol{\alpha}, \boldsymbol{\beta}; x).$$

Checking if $h(x)$ has good reduction at p can be done using the algorithm of Subsection 2.2: we compute $\mathrm{val}_{p,0}(h(x))$ and look whether it is negative or not. However, describing explicitly the set $\mathcal{P}_h$ of all primes p at which $h(x)$ has good reduction looks more challenging. The aim of this subsection is to answer this question.

Let d be the smallest common divisors of the parameters in $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$. Since d has of course only finitely many prime divisors, it is easy to treat them separately. Hence, in what follows, we shall always assume that p does not divide d.

When $m > n$, we deduce from Theorem 2.2 that $\mathrm{val}_p(h_k)$ goes to $-\infty$ when k grows. Hence $h(x)$ cannot have good reduction in this case. From now on, we then assume that $m \leq n$.

If x is a real number, we denote by $\{x\}$ its decimal part, that is, by definition, the unique real number in $[0, 1)$ such that $x - \{x\} \in \mathbb{Z}$. We will need the following result, which is a slight reformulation of [12, Lemma 4].

Lemma 3.1 (Christol). *Let $\gamma = \frac{a}{d} \in \mathbb{Q}$. Let $q > |a-d|$ be an integer which is coprime with d and let Δ be the unique integer in $\{1, \ldots, d-1\}$ such that $\Delta q \equiv 1 \pmod{d}$.*
Then the reduction of $1-\gamma$ modulo q is $(1-\gamma) + q \cdot \{\gamma\Delta\}$.

Writing $\mathrm{den}(x, y)$ for the smallest common denominator of x and y, we set

$$B(\boldsymbol{\alpha}, \boldsymbol{\beta}) := \max_{\gamma, \gamma' \in \Gamma} \mathrm{den}(\gamma, \gamma') \cdot |\gamma - \gamma'|$$

where we recall that $\Gamma = \{1, \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m\}$. Theorem 3.1 implies that, for $p > B(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and $r \geq 1$, the ordering of the $1-\gamma \bmod p^r$, for $\gamma \in \Gamma$ only depends on the congruence of p modulo a common denominator d of the α_i and β_j.

Case $m = n$. Here, in virtue of what we did previously, the vector $\boldsymbol{\mu}_1$ and the matrices T_r of Subsection 2.2 only depend on $p \bmod d$ provided that $p > B(\boldsymbol{\alpha}, \boldsymbol{\beta})$. This is then also the case for $\mathrm{val}_{p,0}(h(x))$ and, consequently, for the fact that $h(x)$ has or has not good reduction modulo p. In other words, $\mathcal{P}_h$ is the union of exceptional primes up to the bound $B(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and then, it consists of primes in arithmetic progressions of ratio d.

These observations also readily give an algorithm to compute $\mathcal{P}_h$: we check whether $h(x)$ has good or bad reduction for all primes $p \leq B(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and for one representative of each invertible class modulo d. We mention nonetheless that checking congruence classes can be done more efficiently by using the criterion of [10, Theorem 3.1.3].

Case $m < n$. In this case, the matrix $\boldsymbol{\mu}_1$ is again independent from p as soon as $p > B(\boldsymbol{\alpha}, \boldsymbol{\beta})$. However, the matrices T_r are not. Following their construction, we nonetheless realize that they can be written as

$$T_r = U_r + \frac{p^{r-1}-1}{p-1} \cdot V_r$$

where U_r and V_r are independent from p for $p > B(\boldsymbol{\alpha}, \boldsymbol{\beta})$. Besides $U_r \geq -m$ (in the sense that all its entries are at least $-m$) and $V_r \geq 0$. In particular T_2 does not depend on p as well and so neither does $\boldsymbol{\mu}_2 = \boldsymbol{\mu}_1 \odot T_2$. Define $\tilde{\boldsymbol{\mu}}_r := \boldsymbol{\mu}_r \oplus (0, \ldots, 0)$. By induction on r, we prove that $\boldsymbol{\mu}_r \geq -mr$ for all r, which in turns implies

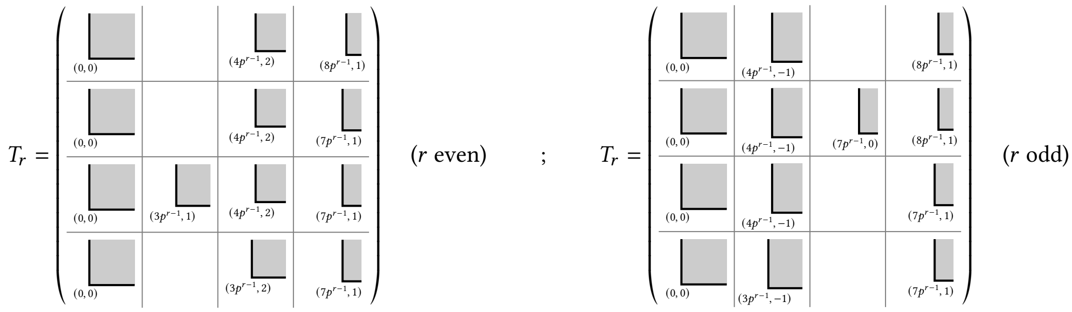


Figure 2: The matrices T_r for the hypergeometric series $\mathcal{H}\left(\left(\frac{1}{3}, \frac{4}{3}\right), \left(\frac{2}{3}\right); x\right)$ and $p = 11$

that $\tilde{\boldsymbol{\mu}}_r = \tilde{\boldsymbol{\mu}}_{r-1} \odot U_r$ if $p^{r-1}-1 > mr(p-1)$. We conclude that $\tilde{\boldsymbol{\mu}}_r$ only depends on $r \bmod d$ provided that $p > B(\boldsymbol{\alpha}, \boldsymbol{\beta})$ as before and $p^{r-1}-1 > mr(p-1)$ for all $r \geq 3$. The latter condition is fulfilled as soon as $p \geq 2m$; indeed from $p \geq 2m$, we derive $p^i \geq 2m$ for all i and then

$$\frac{p^{r-1}-1}{p-1} = 1 + p + \cdots + p^{r-2} \geq 1 + 2m(r-2) > mr \quad (r \geq 3).$$

We now recall that the first coordinate of $\boldsymbol{\mu}_r$ tends to $\mathrm{val}_{p,0}(h(x))$ when r goes to infinity. Therefore, the limit of the first coordinate of $\tilde{\boldsymbol{\mu}}_r$ is $\mathrm{val}_{p,0}(h(x)) \oplus 0 = \min\left(\mathrm{val}_{p,0}(h(x)), 0\right)$. The fact that $h(x)$ has good reduction at p can then be read off on the $\tilde{\boldsymbol{\mu}}_r$, and thus only depend on the congruence class of p modulo d provided that $p > \max(B(\boldsymbol{\alpha}, \boldsymbol{\beta}), 2m)$.

As a consequence, one can compute the set $\mathcal{P}_f$ by proceeding as in the case $m = n$, except that the bound $B(\boldsymbol{\alpha}, \boldsymbol{\beta})$ needs now to be replaced by $\max(B(\boldsymbol{\alpha}, \boldsymbol{\beta}), 2m)$.

3.2 Section operators

From now on, we fix a prime number p of good reduction for $h(x)$ and aim at studying the algebraic properties of $h(x) \bmod p$.

We let n' (resp. m') be the number of top (resp. bottom) parameters which are in $\mathbb{Z}_{(p)}$ and let v' (resp. w') be the sum of the valuations of the top (resp. bottom) parameters which are not in $\mathbb{Z}_{(p)}$. Following what we did in Subsection 2.2, we define $v_0 \coloneqq w' - v' + \frac{m'-n'}{p-1}$.

From Proposition 2.2, we derive that $\lim_{k\to\infty} \mathrm{val}_p(h_k)/k = -v_0$. Hence, our good reduction assumption ensures that $v_0 \leq 0$. We also set $\nu \coloneqq (1-p)v_0 = (p-1)(w'-v') + (m'-n') \in \mathbb{N}$.

Key tools for studying $h(x) \bmod p$ are the section operators that we introduce now.

Definition 3.2. Let r be a nonnegative integer. The map

$$\begin{array}{rccl} \Lambda_r : & \mathbb{Z}_{(p)}[[x]] & \to & \mathbb{Z}_{(p)}[[x]] \\ & \sum_{k=0}^{\infty} a_k x^k & \mapsto & \sum_{k=0}^{\infty} a_{kp+r} x^k \end{array}$$

is called the r-th *section operator.*

We are going to prove that the r-th section of a hypergeometric series is closely related to a scalar multiple of another hypergeometric series. Before proceeding, we need the two following definitions.

Definition 3.3. For $a, b \in \mathbb{Q}$, we say that a is *multiplicatively congruent* to b modulo p and we write $a \equiv_\times b \pmod{p}$ if $a = b = 0$, or $b \neq 0$ and $\frac{a}{b} \in 1 + p\mathbb{Z}_{(p)}$.

Similarly, if $f(x) = \sum_k a_k x^k$ and $g(x) = \sum_k b_k x^k$ are two series with coefficients in $\mathbb{Q}$, we write $f \equiv_\times g \pmod{p}$ if $a_k \equiv_\times b_k \pmod{p}$ for all k.

Definition 3.4 (Dwork map). We define the map $\mathfrak{D}_p : \mathbb{Q} \to \mathbb{Q}$ by:

- when $\gamma \in \mathbb{Z}_{(p)}$, $\mathfrak{D}_p(\gamma)$ is the unique element of $\mathbb{Z}_{(p)}$ such that $p\mathfrak{D}_p(\gamma) - \gamma \in \{0, \ldots, p-1\}$,
- when $\gamma \notin \mathbb{Z}_{(p)}$, $\mathfrak{D}_p(\gamma) \coloneqq \gamma$.

Proposition 3.5. *For $r \geq 0$, we have*

$$\Lambda_r(h(x)) \equiv_\times h_r \cdot \mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}+r), \mathfrak{D}_p(\boldsymbol{\beta}+r); (-p)^\nu x\right) \pmod{p}.$$

Proof. A direct computation gives

$$h_r \cdot \mathcal{H}\left(\boldsymbol{\alpha}+r, \boldsymbol{\beta}+r; x\right) = \textstyle\sum_{k\geq 0} h_{k+r} x^k.$$

Therefore, we can assume without loss of generality that $r = 0$. Let $\gamma \in \mathbb{Z}_{(p)}$. Among $\gamma, \gamma+1, \ldots, \gamma+p-1$, one finds all congruence classes modulo p. Besides, the unique $\gamma + a$ (for $0 \leq a < p$) which lies in $p\mathbb{Z}_{(p)}$ is $p\mathfrak{D}_p(\gamma)$ by definition of the Dwork map. Thus we get the multiplicative congruence

$$(\gamma)_p = \gamma(\gamma+1) \cdots (\gamma+p-1) \equiv_\times (p-1)! \cdot p\mathfrak{D}_p(\gamma) \pmod{p}.$$

Hence $(\gamma)_p \equiv_\times -p\mathfrak{D}_p(\gamma) \pmod{p}$ using Wilson's theorem. Repeating the argument k times and using $\mathfrak{D}_p(\gamma+p) = \mathfrak{D}_p(\gamma) + 1$, we end up with

$$(\gamma)_{pk} \equiv_\times (-p)^k \cdot (\mathfrak{D}_p(\gamma))_k \pmod{p}.$$

If now $\gamma \notin \mathbb{Z}_{(p)}$, we find instead, using Fermat's theorem,

$$\begin{aligned} (\gamma)_{pk} &\equiv_\times \gamma^{pk} \equiv_\times p^{k(p-1)\mathrm{val}_p(\gamma)} \cdot \gamma^k \\ &\equiv_\times (-p)^{k(p-1)\mathrm{val}_p(\gamma)} \cdot (\mathfrak{D}_p(\gamma))_k \pmod{p}. \end{aligned}$$

For the last congruence, we used $(-1)^{p-1} \equiv 1 \pmod{p}$.

Putting now all together, we obtain

$$h_{pk} \equiv_\times (-p)^{k\nu} \cdot \frac{(\mathfrak{D}_p(\alpha_1))_k \cdots (\mathfrak{D}_p(\alpha_n))_k}{(\mathfrak{D}_p(\beta_1))_k \cdots (\mathfrak{D}_p(\beta_m))_k} \pmod{p}$$

which gives the desired multiplicative congruence. □

Remark 3.6. Theorem 3.5 yields an algorithm with complexity $O\big((m+n)p\log N\big)$ for computing the multiplicative congruence class modulo p of h_N. Indeed, if $N = pN_1 + r_0$ is the Euclidean division of N by p, we have $h_N \equiv_\times h_{r_0} h^{(1)}_{N_1} \pmod{p}$ where

$$h^{(1)}(x) = \textstyle\sum_{k\geq 0} h^{(1)}_k x^k \coloneqq \mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}+r), \mathfrak{D}_p(\boldsymbol{\beta}+r); (-p)^\nu x\right).$$

Repeating this argument again and again, we finally end up with a multiplicative congruence of the form

$$h_N \equiv_\times h_{r_0} h_{r_1}^{(1)} h_{r_2}^{(2)} \cdots h_{r_\ell}^{(\ell)} \pmod p$$

where ℓ is the number of digits of N in base p, hence $\ell \in O(\log N)$. Since moreover $r_i < p$ for all i, each term $h_{r_i}^{(i)}$ can be computed for a cost of $O\big((m+n)p\big)$ multiplications and divisions.

Theorem 3.5 can be rephrased by means of classical congruences as follows.

Corollary 3.7. *Let r be a nonnegative integer. Set*

$$g(x) = \textstyle\sum_{k\geq 0} g_k x^k := \mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}+r), \mathfrak{D}_p(\boldsymbol{\beta}+r); x\right).$$

Then $\mathrm{val}_p(h_r) + \mathrm{val}_\nu(g(x)) \geq 0$ and

- *if $\mathrm{val}_p(h_r) + \mathrm{val}_\nu(g(x)) > 0$, then $\Lambda_r(h(x)) \equiv 0 \pmod p$,*
- *if $\mathrm{val}_p(h_r) + \mathrm{val}_\nu(g(x)) = 0$, then*

$$\begin{aligned}&\Lambda_r(h(x))\\ &\equiv h_{r+ps} x^s \cdot \mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}+r)+s, \mathfrak{D}_p(\boldsymbol{\beta}+r)+s; (-p)^\nu x\right) \pmod p\end{aligned}$$

where s is the smallest integer such that $\mathrm{val}_p(g_s) + \nu s = \mathrm{val}_\nu(g(x))$.

We emphasize that Corollary 3.7 is effective in the sense that $\mathrm{val}_\nu(g(x))$ and s can both be computed using the algorithm of Subsection 2.2 (see also Theorem 2.6).

3.3 Algebraicity modulo p

Writing $h(x) \equiv \sum_{r=0}^{p-1} x^r \cdot \Lambda_r(h(x))^p \pmod p$, we derive from Theorem 3.7 that $h(x) \bmod p$ can be written as a linear combination over $\mathbb{F}_p[x]$ of p-th powers of other hypergeometric series. We call this identity the *Dwork relation* associated to $h(x)$. Our aim in this subsection is to derive from Dwork relations an algebraic relation involving uniquely $h(x) \bmod p$.

When $\nu_0 < 0$, the series $h(x) \bmod p$ is a polynomial, and algebraicity is clear. From now on, we then assume that $\nu_0 = 0$; hence $\nu = 0$ as well.

The main ingredient of our proof is the fact that iterating Dwork relations, we only encounter a finite number of auxiliary hypergeometric series. To establish this, we define X as the smallest subset of $\mathbb{Q}^n \times \mathbb{Q}^m$ containing $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ and stable by the operations

$$(\boldsymbol{\alpha}', \boldsymbol{\beta}') \mapsto \left(\mathfrak{D}_p(\boldsymbol{\alpha}'+r), \mathfrak{D}_p(\boldsymbol{\beta}'+r)\right) \quad (0 \leq r < p).$$

Using that $\mathfrak{D}_p(\gamma) = \frac{\gamma}{p} + O(1)$ for $\gamma \in \mathbb{Z}_{(p)}$, we deduce that X is finite (see also [10, Lemma 3.2.1 (2)]). Let $(\boldsymbol{\alpha}', \boldsymbol{\beta}') \in X$ and write

$$g(x) = \textstyle\sum_{k\geq 0} g_k x^k := \mathcal{H}\left(\boldsymbol{\alpha}', \boldsymbol{\beta}'; x\right).$$

If $\mathrm{val}_{p,0}(g(x)) > -\infty$, we let t denote the smallest integer for which $\mathrm{val}_p(g_t) = \mathrm{val}_{p,0}(g(x))$ and consider the new parameters $(\boldsymbol{\alpha}'+t, \boldsymbol{\beta}'+t)$. We let Y denote the set of all parameters obtained this way by letting $(\boldsymbol{\alpha}', \boldsymbol{\beta}')$ vary in X. Clearly, Y is finite as well.

Proposition 3.8. *For any nonnegative integer e, there exists a relation of the form*

$$h(x) \equiv P(x) + \sum_{\boldsymbol{\gamma}\in Y} Q_{\boldsymbol{\gamma}}(x) \cdot \mathcal{H}\left(\boldsymbol{\gamma}; x\right)^{p^e} \pmod p$$

where $P(x)$ and $Q_{\boldsymbol{\gamma}}(x)$ are polynomials in $\mathbb{F}_p[x]$.

Proof. Let $\boldsymbol{\gamma} \in Y$. Then $\boldsymbol{\gamma} = (\boldsymbol{\alpha}'+s, \boldsymbol{\beta}'+s)$ for some $(\boldsymbol{\alpha}', \boldsymbol{\beta}') \in X$ and $s \in \mathbb{N}$. The Dwork relation makes $\mathcal{H}\left(\boldsymbol{\gamma}; x\right) \bmod p$ appear as a $\mathbb{F}_p[x]$-linear combination of the series

$$\mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}'+s+r) + s_r, \mathfrak{D}_p(\boldsymbol{\beta}'+s+r) + s_r; x\right)^p \bmod p \quad (0 \leq r < p)$$

for some $s_r \in \mathbb{N}$. We observe that, if $s+r = ap + b$ is the Euclidean division of $s+r$ by p, we have $\mathfrak{D}_p(\gamma+s+r) = \mathfrak{D}_p(\gamma+b) + a$ for all $\gamma \in \mathbb{Z}_{(p)}$. Moreover, when $\gamma \notin \mathbb{Z}_{(p)}$, shifting γ by any integer does not change the hypergeometric series modulo p. Therefore, $\mathcal{H}\left(\boldsymbol{\gamma}; x\right) \bmod p$ is also in the $\mathbb{F}_p[x]$-linear span of the

$$\mathcal{H}\left(\mathfrak{D}_p(\boldsymbol{\alpha}'+b) + t_b, \mathfrak{D}_p(\boldsymbol{\beta}'+b) + t_b; x\right)^p \bmod p \quad (0 \leq b < p)$$

for some $t_b \in \mathbb{N}$. Moreover, for each fixed $b \in \{0, \ldots, p{-}1\}$, the pair $(\boldsymbol{\alpha}'', \boldsymbol{\beta}'') := (\mathfrak{D}_p(\boldsymbol{\alpha}'+b), \mathfrak{D}_p(\boldsymbol{\beta}'+b))$ is by definition in X. Let $g(x) = \sum_k g_k x^k$ be the associated hypergeometric series and let t be the smallest integer such that $\mathrm{val}_p(g_t) = \mathrm{val}_{p,0}(g(x))$ which $\mathcal{H}\left(\boldsymbol{\alpha}''+t, \boldsymbol{\beta}''+t; x\right)$ has good reduction modulo p. Thus $t_b \geq t$ and there exists $c_b \in \mathbb{F}_p$, $C_b(x) \in \mathbb{F}_p[x]$ such that

$$\begin{aligned}&\mathcal{H}\left(\boldsymbol{\alpha}''+t_b, \boldsymbol{\beta}''+t_b; x\right)\\ &\qquad\equiv C_b(x) + c_b x^{t_b - t} \mathcal{H}\left(\boldsymbol{\alpha}''+t, \boldsymbol{\beta}''+t; x\right) \pmod p.\end{aligned}$$

It follows that $\mathcal{H}\left(\boldsymbol{\gamma}; x\right) \bmod p$ is in the $\mathbb{F}_p[x]$-linear span of 1 and the hypergeometric series $\mathcal{H}\left(\boldsymbol{\gamma}'; x\right)^p \bmod p$ for $\boldsymbol{\gamma}'$ varying in Y.

The proposition follows by induction on e. □

Theorem 3.9. *The series $h(x) \bmod p$ is algebraic over $\mathbb{F}_p(x)$.*

Proof. Set $N := \mathrm{Card}(Y){+}1$. Raising the relation of Theorem 3.8 to the power p^{N-e}, we obtain

$$h(x)^{p^{N-e}} \equiv \textstyle\sum_{\boldsymbol{\gamma}\in Y^\bullet} Q_{\boldsymbol{\gamma}}(x)^{p^{N-e}} \cdot \mathcal{H}\left(\boldsymbol{\gamma}; x\right)^{p^N} \pmod p$$

where we have set $Y^\bullet = Y \sqcup \{\bullet\}$ and $Q_\bullet(x) = P(x)$, $\mathcal{H}\left(\bullet; x\right) = 1$. These equalities give a linear system, yielding a single matrix relation of the form

$$\left(h(x)^{p^e}\right)_{0\leq e\leq N} \equiv \left(\mathcal{H}\left(\boldsymbol{\gamma}; x\right)^{p^N}\right)_{\boldsymbol{\gamma}\in Y^\bullet} \cdot M(x) \pmod p$$

where $M(x)$ is a matrix over $\mathbb{F}_p[x]$ with rows indexed by $Y^\bullet$ and columns indexed by $\{0, \ldots, N\}$. Hence $M(x)$ has more columns than rows, and so it has a nontrivial vector $(v_0(x), \ldots, v_N(x))$ in its right kernel. Thus $v_0(x)h(x) + v_1(x)h(x)^p + \cdots + v_N(x)h(x)^{p^N} = 0$, proving algebraicity. □

Again, we underline that the proofs of Theorem 3.8 and Theorem 3.9 readily yield an algorithm for computing an annihilating polynomial of $h(x) \bmod p$. Its complexity is polynomial when we count operations in $\mathbb{F}_p[x]$ but the size of the polynomials can grow very rapidly, due to frequent raisings to the p-th power. We believe nonetheless that this blow up is intrinsic to the problem in the sense that a general hypergeometric series $h(x) \bmod p$ has only huge annihilating polynomials with coefficients having degree growing exponentially fast with respect to p.

References

[1] Y. Abdelaziz, C. Koutschan, and J.-M. Maillard. 2020. On Christol's conjecture. *Journal of Physics A: Mathematical and Theoretical*, 53, 20, 205201. doi:10.1088/1751-8121/ab82dc.

[2] F. Beukers and G. Heckman. 1989. Monodromy for the hypergeometric function ${}_nF_{n-1}$. *Inventiones Mathematicae*, 95, 2, 325–354. doi:10.1007/BF01393900.

[3] A. Bostan, S. Boukraa, G. Christol, S. Hassani, and J.-M. Maillard. 2013. Ising n-fold integrals as diagonals of rational functions and integrality of series expansions. *Journal of Physics A: Mathematical and Theoretical*, 46, 18, 185202. doi:10.1088/1751-8113/46/18/185202.

[4] A. Bostan, S. Boukraa, J.-M. Maillard, and J.-A. Weil. 2015. Diagonals of rational functions and selected differential Galois groups. *Journal of Physics A: Mathematical and Theoretical*, 48, 50, 504001. doi:10.1088/1751-8113/48/50/504001.

[5] A. Bostan, S. Boukraa, G. Christol, S. Hassani, and J.-M. Maillard. 2012. Ising n-fold integrals as diagonals of rational functions and integrality of series expansions: integrality versus modularity. eprint: arXiv:1211.6031 (math-ph).

[6] A. Bostan and S. Yurkevich. 2022. On a class of hypergeometric diagonals. *Proceedings of the American Mathematical Society*, 150, 3, 1071–1087. doi:10.1090/proc/15693.

[7] P. Butkovič. 2010. *Max-Linear Systems: Theory and Algorithms. Springer Monographs in Mathematics.* Springer London, London. doi:10.1007/978-1-84996-299-5.

[8] X. Caruso and F. Fürnsinn. 2026. Algebraic and arithmetic attributes of hypergeometric functions in SageMath. eprint: arXiv:2602.04531 (cs.SC).

[9] X. Caruso and F. Fürnsinn. 2025. Algebraic and modular properties of hypergeometric functions. https://github.com/sagemath/sage/pull/41113.

[10] X. Caruso, F. Fürnsinn, and D. Vargas-Montoya. 2025. Galois groups of reductions modulo p of D-finite series. eprint: arXiv:2504.09429 (math).

[11] G. Christol. 1986. Fonctions et éléments algébriques. *Pacific Journal of Mathematics*, 125, 1, 1–37. doi:10.2140/pjm.1986.125.1.

[12] G. Christol. 1986. Fonctions hypergéométriques bornées. *Groupe de travail d'analyse ultramétrique*. exp. no 8 14, 1–16. http://www.numdam.org/item/GAU_1986-1987__14__A4_0.pdf.

[13] G. Christol. 1990. Globally bounded solutions of differential equations. *Analytic Number Theory*. Vol. 1434. K. Nagasaka and E. Fouvry, (Eds.) Springer Berlin Heidelberg, Berlin, Heidelberg, 45–64. doi:10.1007/BFb0097124.

[14] E. Delaygue, T. Rivoal, and J. Roques. 2017. On Dwork's p-adic formal congruences theorem and hypergeometric mirror maps. *Memoirs of the American Mathematical Society*, 246, 1163. doi:10.1090/memo/1163.

[15] A. Errera. 1913. Zahlentheoretische lösung einer functionentheoretischen frage. *Rendiconti del Circolo Matematico di Palermo*, 35, 1, 107–144. doi:10.1007/BF03015595.

[16] F. Fürnsinn and S. Yurkevich. 2024. Algebraicity of hypergeometric functions with arbitrary parameters. *Bulletin of the London Mathematical Society*, blms.13103. doi:10.1112/blms.13103.

[17] H. Furstenberg. 1967. Algebraic functions over finite fields. *Journal of Algebra*, 7, 2, 271–277. doi:10.1016/0021-8693(67)90061-0.

[18] N. M. Katz. 1990. *Exponential Sums and Differential Equations.* Number 124 in *Annals of Mathematics Studies.* Princeton Univ. Press, Princeton, N.J. 430 pp.

[19] K. S. Kedlaya. 2022. Frobenius structures on hypergeometric equations. *Arithmetic, geometry, cryptography, and coding theory, AGC2T. 18th international conference, Centre International de Rencontres Mathématiques, Marseille, France, May 31 – June 4, 2021.* Providence, RI: American Mathematical Society (AMS), 133–158. doi:10.1090/conm/779/15673.

[20] E. Landau. 1904. Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1904, 127, 92–102. doi:10.1515/crll.1904.127.92.

[21] E. Landau. 1911. *Über Einen Zahlentheoretischen Satz Und Seine Anwendung Auf Die Hypergeometrische Reihe.* Heidelberg University Library. doi:10.11588/HEIDOK.00012365.

[22] H. Schwarz. 1873. Ueber diejenigen fälle, in welchen die gaussische hypergeometrische reihe eine algebraische function ihres vierten elementes darstellt. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1873, 75, 292–335. doi:10.1515/crll.1873.75.292.

[23] D. Vargas-Montoya. 2024. Algebraicity modulo p of generalized hypergeometric series ${}_nF_{n-1}$. *Journal of Number Theory*, 259, 273–321. doi:10.1016/j.jnt.2024.01.004.

[24] D. Vargas-Montoya. 2021. Algébricité modulo p, séries hypergéométriques et structures de frobenius fortes. *Bulletin de la Société mathématique de France.* doi:10.24033/bsmf.2834.