



On the representability of sequences as constant terms

Alin Bostan, Armin Straub, Sergey Yurkevich

► To cite this version:

Alin Bostan, Armin Straub, Sergey Yurkevich. On the representability of sequences as constant terms. Journal of Number Theory, 2023, 253, pp.235-256. 10.1016/j.jnt.2023.06.015 . hal-03907115v2

HAL Id: hal-03907115

<https://hal.science/hal-03907115v2>

Submitted on 22 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

On the representability of sequences as constant terms

Alin Bostan¹, Armin Straub², and Sergey Yurkevich^{1,3}

¹*Inria, Univ. Paris-Saclay, France*

alin.bostan@inria.fr

²*University of South Alabama, USA*

straub@southalabama.edu

³*University of Vienna, Austria*

sergey.yurkevich@univie.ac.at

Abstract

A constant term sequence is a sequence of rational numbers whose n -th term is the constant term of $P^n(\mathbf{x})Q(\mathbf{x})$, where $P(\mathbf{x})$ and $Q(\mathbf{x})$ are multivariate Laurent polynomials. While the generating functions of such sequences are invariably diagonals of multivariate rational functions, and hence special period functions, it is a famous open question, raised by Don Zagier, to classify those diagonals which are constant terms. In this paper, we provide such a classification in the case of sequences satisfying linear recurrences with constant coefficients. We further consider the case of hypergeometric sequences and, for a simple illustrative family of hypergeometric sequences, classify those that are constant terms.

Keywords: Integer sequences, C-finite sequences, hypergeometric sequences, constant term sequences, P-recursive sequences, Laurent polynomials, Gauss congruences, diagonals of rational functions.

1 Introduction

Recognizing and interpreting integrality of sequences defined by recursions is at the same time an extensively studied and a hardly understood topic in number theory. Even for the case of sequences $A(n)$ defined by linear recurrences with polynomial coefficients, the so-called *P-recursive* sequences,

$$p_r(n)A(n+r) = p_{r-1}(n)A(n+r-1) + \cdots + p_0(n)A(n), \quad p_i(n) \in \mathbb{Z}[n],$$

neither a criterion nor even an algorithm is known for classifying/deciding integrality. An attempt for such a classification is the famous and widely open conjecture by Christol [Chr90, Conjecture 4, p. 55]. Roughly speaking, it states that a P-recursive sequence $(A(n))_{n \geq 0}$ with (at most) geometric growth is integral if and only if $(A(n))_{n \geq 0}$ is the coefficient sequence of the diagonal of a rational function $R(\mathbf{x}) \in \mathbb{Z}(x_1, \dots, x_d) \cap \mathbb{Z}[[x_1, \dots, x_d]]$ for some $d \geq 1$. Recall that the diagonal of a multivariate power series

$$R(\mathbf{x}) = \sum_{n_1, n_2, \dots, n_d \geq 0} c(n_1, n_2, \dots, n_d) x_1^{n_1} x_2^{n_2} \cdots x_d^{n_d} \quad (1)$$

is the univariate power series $\text{Diag}(R)$ whose coefficient sequence is given by $A(n) = c(n, n, \dots, n)$. For a precise statement of Christol's conjecture see Conjecture 6.3 below.

Often integrality of sequences can be explained by the underlying combinatorial nature. For example, the Catalan numbers $C(n)$ satisfying

$$(n+2)C(n+1) = 2(2n+1)C(n), \quad C(0) = 1,$$

are clearly integers because they count triangulations of convex polygons with $n+2$ vertices. On the other hand, for many other integral and P-recursive sequences, combinatorial interpretations are not *a priori* known; this is the case, for instance, for the Apéry numbers $A(n)$ (associated with the irrationality proof of $\zeta(3)$) defined by

$$(n+1)^3 A(n+1) = (2n+1)(17n^2 + 17n + 5)A(n) - n^3 A(n-1), \\ A(0) = 1, A(1) = 5.$$

In both examples above, integrality can be seen from the explicit formulas

$$C(n) = \binom{2n}{n} - \binom{2n}{n+1} \quad \text{and} \quad A(n) = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2.$$

Putting Christol's conjecture in practice gives a different justification for the integrality of these two examples. It namely holds that

$$\sum_{n \geq 0} C(n)t^n = \text{Diag} \left(\frac{1-y}{1-x(y+1)^2} \right) \quad \text{and} \\ \sum_{n \geq 0} A(n)t^n = \text{Diag} \left(\frac{1}{1-(xy+x+y)(zw+z+w)} \right),$$

and the integrality of $C(n)$ and $A(n)$ follows from that of the coefficients in the Taylor expansions of the corresponding multivariate rational functions.

In the context of the current text, however, we would like to emphasize a slightly different viewpoint, which does not only justify integrality of the two examples, but also implies some interesting arithmetic properties. Writing $\text{ct}[P(\mathbf{x})]$ for the constant term of a Laurent polynomial $P(\mathbf{x}) \in \mathbb{Q}[x_1^{\pm 1}, \dots, x_d^{\pm 1}]$, one can prove that [Str14, Rem. 1.4]

$$\begin{aligned} C(n) &= \text{ct} \left[(x^{-1} + 2 + x)^n (1 - x) \right] \quad \text{and} \\ A(n) &= \text{ct} \left[\left(\frac{(x+y)(z+1)(x+y+z)(y+x+1)}{xyz} \right)^n \right]. \end{aligned}$$

Similar identities as in the examples of the Catalan and Apéry numbers can be deduced for many other integral P-recursive sequences. This motivates the following definition and the subsequent natural question.

Definition 1.1. A sequence $A(n)$ is a *constant term* if it can be represented as

$$A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})], \quad (2)$$

where $P, Q \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$ are Laurent polynomials in $\mathbf{x} = (x_1, \dots, x_d)$.

Using the geometric series it is easy to see that generating functions of constant term sequences can be expressed as diagonals of rational functions. The converse is, however, not true in general. This leads to the following question which was raised by Zagier [Zag18, p. 769, Question 2] and Gorodetsky [Gor21] in the case $Q = 1$ (see Proposition 5.1 below for an indication why this case is of particular arithmetic significance).

Question 1. *Which P-recursive sequences are constant terms?*

To our knowledge, Question 1 is widely open. In fact, the initial motivation for the present text was the goal of answering the following very particular sub-question asked by the second author in [Str22, Question 5.1]:

Question 2. *Is the Fibonacci sequence $(F(n))_{n \geq 0}$ a constant term sequence?*

Recall that the Fibonacci sequence $(F(n))_{n \geq 0}$ is the coefficient sequence in the Taylor expansion of the univariate rational function $x/(1 - x - x^2)$, or equivalently the P-recursive sequence $(F(n))_{n \geq 0}$ defined by $F(n+2) = F(n+1) + F(n)$ and $F(0) = 0, F(1) = 1$.

Already in [Str22] the second author noted that a representation of the Fibonacci numbers as constant terms with $Q = 1$ is impossible since

$(F(n))_{n \geq 0}$ does not satisfy the so-called *Gauss congruences* (see (9)). Exploiting the fact that for any prime p , the value $F(p) \pmod{p}$ depends on $p \pmod{5}$, we can show (see Example 3.2) that the answer to Question 2 is negative. The reason for this is that, as we will prove, for any constant term sequence $A(n)$, the sequence $A(p) \pmod{p}$ must be constant for large enough primes p . Note that this is not a sufficient criterion, since already the Lucas numbers $L(n)$ (defined by the same recursion as the Fibonacci numbers, but with different initial terms $L(0) = 2, L(1) = 1$, see (8)) do satisfy the Gauss congruences but are not constant terms (see Example 4.2).

In the present text, we are able to answer Question 1 in the case of diagonals of rational functions $F(x) \in \mathbb{Q}(x)$ in a single variable. Such sequences are precisely the (rational) *C-finite sequences* (also known as *C-recursive sequences*), and are characterized by the fact that they satisfy a linear recursion with constant rational coefficients. More explicitly, we define a sequence $A(n)$ of rational numbers to be C-finite if there exists a polynomial $P(x) \in \mathbb{Q}[x]$ such that for every $n \geq 0$ we have

$$P(N)A(n) = 0, \quad (3)$$

where N denotes the shift operator $N^\ell(A(n)) := A(n + \ell)$ for all $\ell \geq 0$. Equivalently, there exist integers $r > 0$ and $n_0 \geq 0$, and complex numbers c_0, \dots, c_{r-1} with $c_0 \neq 0$ such that

$$A(n + r) = c_{r-1}A(n + r - 1) + \dots + c_0A(n) \quad \text{for all } n \geq n_0. \quad (4)$$

We recall that associated to the recursion (4), the *characteristic roots* are usually defined as the roots of

$$\chi(\lambda) := \lambda^r - c_{r-1}\lambda^{r-1} - \dots - c_0.$$

For our purpose, however, it is useful to define the characteristic roots of a C-finite sequence $A(n)$ as the roots of $P(x)$, where $P(x)$ is chosen with minimal degree such that (3) holds. Note that the only difference between considering roots of χ and P is that 0 can be a root of the latter. Equivalently, 0 is defined to be a characteristic root of $A(n)$ of multiplicity m_0 if the minimal n_0 in (4) (chosen so that r is minimal) equals m_0 . With these definitions we obtain the following:

Proposition 1.2. *Let $A(n)$ be a C-finite sequence. $A(n)$ is a constant term if and only if it has a single characteristic root λ and $\lambda \in \mathbb{Q}$.*

This proposition immediately answers Question 2 but also shows that, for example, the sequence $A(n) = 2^n + 1$ is not a constant term sequence

either (in both of these cases, there are two different characteristic roots). Evidently, however, it is the sum of two constant terms: we see that the class of constant term sequences is not a ring. Therefore, to fix this issue, it is natural to consider the class of sequences given as \mathbb{Q} -linear combinations of constant terms:

Question 3. *Which P-recursive sequences are finite \mathbb{Q} -linear combinations of constant terms?*

Again in the case of C-finite sequences, we can answer this question completely with the main result of the present work:

Theorem 1.3. *Let $A(n)$ be a C-finite sequence. Then $A(n)$ is an r -term \mathbb{Q} -linear combination of constant terms if and only if it has at most r distinct characteristic roots, all of which are rational.*

Having completed the classification of C-finite sequences that can be written as (sums of) constant terms, there are two most natural directions for further work. On the one hand, it is reasonable to go from diagonals in one variable to diagonals in two variables. By the combination of results due to Pólya [P622] and Furstenberg [Fur67] this is known to be exactly the class of algebraic generating functions. One is then lead to the following question which we leave for future work:

Question 4. *Which sequences $A(n)$ with algebraic generating function are constant terms?*

Another reasonable direction is to try to classify those hypergeometric sequences which are constant terms. Recall that a P-recursive sequence $A(n)$ is called *hypergeometric* if it satisfies a recursion of order one, i.e. $\alpha(n)A(n+1) = \beta(n)A(n)$ for some polynomials $\alpha(n), \beta(n) \in \mathbb{Q}[n]$. In this sense, this class of sequences is arguably the simplest (and best understood) among P-recursive ones. Still, Christol's conjecture remains open even in this very special case. In fact, it is still an open question whether the generating function of the sequence

$$A(n) = \frac{\left(\frac{1}{9}\right)_n \left(\frac{4}{9}\right)_n \left(\frac{5}{9}\right)_n}{n!^2 \left(\frac{1}{3}\right)_n}$$

can be represented as the diagonal of a rational function. Here and later, $(x)_n := x(x+1) \cdots (x+n-1)$ denotes the rising factorial. We can use the same methods as in the C-finite case to prove that $A(n)$ is not a constant

term sequence (see Lemma 6.6). By classifying when the family (21) of hypergeometric sequences is a constant term, we are further able to conclude that not all hypergeometric diagonals are constant terms. The following question, however, remains open in general:

Question 5. *Which hypergeometric sequences are constant terms?*

The organization of the paper is as follows: In Section 2, we review properties of C-finite sequences that will be important for our purposes. In particular, we state Theorem 2.2 which is due to Minton [Min14] and which is a crucial ingredient of our approach. In Section 3, we derive certain congruences that are satisfied by any constant term sequence; these are already enough to answer Question 2. By combining these congruences with Minton's Theorem, we prove in Section 4 our main Theorem 1.3, thus answering Question 1 and Question 3 in the case of C-finite sequences. In the short Section 5 we prove a statement which is pleasingly similar to Minton's theorem and which allows to classify the constant terms with $Q = 1$ among all constant terms. Finally, in Section 6, we turn our attention to hypergeometric sequences and discuss Question 5.

Throughout the article, p denotes a prime number, \mathbb{F}_p the finite field with p elements and \mathbb{Z}_p the ring of p -adic integers.

2 Trace sequences

Let $A(n)$ be a C-finite sequence. Denote by $\lambda_1, \lambda_2, \dots, \lambda_d \in \overline{\mathbb{Q}}$ the characteristic roots, and let m_j be the multiplicity of the root λ_j . Recall that $\lambda_0 = 0$ is defined to be a characteristic root of $A(n)$ of multiplicity m_0 if the minimal n_0 in (4) equals m_0 . $A(n)$ can be written as a linear combination

$$A(n) = A_0(n) + \sum_{j=1}^d \sum_{r=0}^{m_j-1} c_{j,r} n^r \lambda_j^n \quad (5)$$

for certain coefficients $c_{j,r} \in \overline{\mathbb{Q}}$ (more precisely, $c_{j,r} \in \mathbb{Q}(\lambda_1, \dots, \lambda_d)$) and $A_0(n)$ a sequence of finite support $\{0, 1, \dots, m_0-1\}$. We refer to [EvdPSW03] or [KP11, Chapter 4] for introductions to C-finite sequences. Note that allowing 0 as a characteristic root is equivalent to not restricting the numerator of the rational generating function of $A(n)$ to have degree less than the degree of its denominator. In the following, we will refer to

$$A^{\text{sep}}(n) = A_0(0) + \sum_{j=1}^d c_{j,0} \lambda_j^n \quad (6)$$

as the *separable part* of $A(n)$. We note that, if $A(n) \in \mathbb{Q}$, then $A^{\text{sep}}(n) \in \mathbb{Q}$.

A sequence $A(n)$ is said to be a *trace sequence* if it is a \mathbb{Q} -linear combination of traces $\text{Tr}(\theta^n) = \theta_1^n + \cdots + \theta_r^n$ of algebraic numbers θ with Galois conjugates $\theta_1 = \theta, \theta_2, \dots, \theta_r$ (with the understanding that $\text{Tr}(0^n)$ is 1 for $n = 0$ and 0 otherwise). Equivalently, a trace sequence is a C-finite sequence for which the multiplicity of each characteristic root is $m_j = 1$ and for which $c_{i,0} = c_{j,0}$ in (5) whenever λ_i and λ_j have the same minimal polynomial. We further note as in [BHS18] that the condition to be a trace sequence is equivalent to the property that the generating function $F(x)$ is $F(0)$ plus a \mathbb{Q} -linear combination of functions of the form $xu'(x)/u(x)$, where $u \in \mathbb{Q}[x]$ is irreducible and $u(0) = 1$.

Example 2.1. For the Fibonacci numbers $F(n)$, the representation (5) takes the form

$$F(n) = \frac{\varphi_+^n - \varphi_-^n}{\sqrt{5}}, \quad \varphi_{\pm} = \frac{1 \pm \sqrt{5}}{2}. \quad (7)$$

Because the coefficients of φ_+^n and φ_-^n differ in sign, the Fibonacci numbers $F(n)$ are not a trace sequence. On the other hand, the Lucas numbers

$$L(n) = \varphi_+^n + \varphi_-^n = \text{tr}[M^n], \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad (8)$$

which satisfy the same recurrence as the Fibonacci numbers, are a trace sequence. In particular, it follows from Theorem 2.2 that the Lucas numbers $L(n)$ satisfy the Gauss congruences (9).

Minton [Min14] classified those C-finite sequences that satisfy the Gauss congruences (9) (see [BHS18] for another proof of Minton's result).

Theorem 2.2 (Minton, 2014). *Let $A(n)$ be C-finite. Then the following are equivalent:*

- (a) *For all large enough primes p and for all $r \geq 1$, $A(n)$ satisfies the Gauss congruences*

$$A(p^r n) \equiv A(p^{r-1} n) \pmod{p^r}. \quad (9)$$

- (b) *For all large enough primes p , $A(n)$ satisfies the congruences*

$$A(pn) \equiv A(n) \pmod{p}. \quad (10)$$

- (c) *$A(n)$ is a trace sequence.*

We conclude from Minton's Theorem 2.2 the following result, which we employ in the proof of our main result (Theorem 1.3). To see the importance of Lemma 2.3, we note that, as we will show later (in Corollary 3.4), the sequences $A(n)$ which are linear combinations of constant terms satisfy the congruences $A(p^r n) \equiv A(pn) \pmod{p}$ for all $r \geq 1$ and large enough primes p .

Lemma 2.3. *Let $A(n)$ be C-finite. If $A(n)$ satisfies the congruences*

$$A(p^r n) \equiv A(pn) \pmod{p} \quad (11)$$

for all $r \geq 1$ and for all large enough primes p , then the separable part $A^{\text{sep}}(n)$ is a trace sequence.

Proof. It follows from comparing (5) with (6) that for n large enough

$$A(n) = A^{\text{sep}}(n) + n\tilde{A}(n),$$

where $A^{\text{sep}}(n)$ and $\tilde{A}(n)$ are rational and satisfy the minimal recurrence for $A(n)$. In particular, each of these sequences is in \mathbb{Z}_p for large enough p , since denominators can only arise from the coefficients of the recurrence and the initial conditions. It follows that

$$A^{\text{sep}}(pn) \equiv A(pn) \pmod{p}$$

for all large enough p . Consequently, the congruences (11) are also satisfied by the C-finite sequence $A^{\text{sep}}(n)$. That is, for all $r \geq 1$ and large enough p

$$A^{\text{sep}}(p^r n) \equiv A^{\text{sep}}(pn) \pmod{p}. \quad (12)$$

On the other hand, let us consider the C-finite sequence $A^{\text{sep}}(n)$ in \mathbb{F}_p . To avoid confusion, we denote this reduced sequence by $a_p^{\text{sep}}(n)$. Since the characteristic polynomial of $A^{\text{sep}}(n)$ over \mathbb{Q} is separable, it is also separable for all large enough primes p (this can be seen by looking at the discriminant which, if nonzero over \mathbb{Q} , can only vanish modulo finitely many primes). Consequently, we have a version of (6) with coefficients and roots in $\overline{\mathbb{F}}_p$. Namely,

$$a_p^{\text{sep}}(n) = \sum_{j=1}^d d_j \mu_j^n, \quad d_j, \mu_j \in \overline{\mathbb{F}}_p.$$

Denoting with $\varphi_p : \overline{\mathbb{F}}_p \rightarrow \overline{\mathbb{F}}_p$ the Frobenius automorphism defined by $\varphi_p(z) = z^p$, we therefore have

$$a_p^{\text{sep}}(p^s n) = \sum_{j=1}^d d_j \mu_j^{p^s n} = \sum_{j=1}^d d_j (\varphi_p^s(\mu_j))^n$$

for each $s \in \mathbb{Z}_{>0}$. Note that φ_p acts as a permutation on the roots μ_j . Writing m for the order of this permutation, we have $\varphi_p^m(\mu_j) = \mu_j$ and thus

$$a_p^{\text{sep}}(p^m n) = a_p^{\text{sep}}(n).$$

Consequently, the corresponding sequence $A^{\text{sep}}(n)$ satisfies

$$A^{\text{sep}}(p^m n) \equiv A^{\text{sep}}(n) \pmod{p}.$$

Combined with the congruences (12), this implies that

$$A^{\text{sep}}(pn) \equiv A^{\text{sep}}(n) \pmod{p}$$

for all large enough p . Theorem 2.2 therefore implies that $A^{\text{sep}}(n)$ is a trace sequence. \square

3 Congruences for constant terms

In this section we will show that if $A(n)$ is a constant term sequence then it must satisfy certain congruences for large enough primes p . As a consequence, this allows us to conclude that the Fibonacci numbers are not a constant term sequence, thus answering Question 2 from the introduction.

For a Laurent polynomial $P \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$, let $\deg(P)$ denote the maximal degree with which any variable or its inverse appears in P .

Lemma 3.1. *Let $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ with $P, Q \in \mathbb{Z}_p[\mathbf{x}^{\pm 1}]$. Then*

$$A(p^r n + k) \equiv A(k) \text{ct}[P(\mathbf{x})^{p^{r-1}n}] \pmod{p^r}$$

for all integers $n, k \geq 0$ and $r \geq 1$, provided that $p > \deg(P^k Q)$.

Proof. Recall that (see, for instance, [RY15, Proposition 1.9]), for any Laurent polynomial $F \in \mathbb{Z}_p[\mathbf{x}^{\pm 1}]$,

$$F(\mathbf{x})^{p^r} \equiv F(\mathbf{x}^p)^{p^{r-1}} \pmod{p^r}. \quad (13)$$

As in [Str22], it follows from (13) that

$$\begin{aligned} A(p^r n + k) &= \text{ct}[P(\mathbf{x})^{p^r n} P(\mathbf{x})^k Q(\mathbf{x})] \\ &\equiv \text{ct}[P(\mathbf{x}^p)^{p^{r-1}n} P(\mathbf{x})^k Q(\mathbf{x})] \pmod{p^r} \\ &= \text{ct}[P(\mathbf{x})^{p^{r-1}n} \Lambda_p[P(\mathbf{x})^k Q(\mathbf{x})]], \end{aligned}$$

where Λ_p denotes the Cartier operator

$$\Lambda_p \left[\sum_{\mathbf{k} \in \mathbb{Z}^d} a_{\mathbf{k}} \mathbf{x}^{\mathbf{k}} \right] = \sum_{\mathbf{k} \in \mathbb{Z}^d} a_{p\mathbf{k}} \mathbf{x}^{\mathbf{k}}.$$

If $p > \deg(P^k Q)$, then

$$\Lambda_p[P(\mathbf{x})^k Q(\mathbf{x})] = \text{ct}[P(\mathbf{x})^k Q(\mathbf{x})] = A(k)$$

and the claim follows. \square

Example 3.2. For the Fibonacci numbers $F(n)$, it is a well-known consequence of (7) that, modulo any prime p , we have the congruences

$$F(p) \equiv \begin{cases} 1, & \text{if } p \equiv 1, 4 \pmod{5}, \\ -1, & \text{if } p \equiv 2, 3 \pmod{5}, \end{cases} \pmod{p}.$$

Since this is incompatible with Lemma 3.1 (setting $r = n = 1$ and $k = 0$ implies that $A(p) \equiv A(0) \cdot c \pmod{p}$ for some $c \in \mathbb{Q}$ that is independent of p), we see that $F(n)$ is not a constant term sequence.

On the other hand, by Theorem 2.2, the Lucas numbers $L(n)$ (from (8)) satisfy the congruences $L(p^r n) \equiv L(pn) \pmod{p}$ for $r \geq 1$ and p large enough. As such, Lemma 3.1 is not sufficient to conclude that $L(n)$ is not a constant term sequence. However, we will be able to conclude in Example 4.2 the stronger result that both the Fibonacci numbers and the Lucas numbers cannot be expressed as a \mathbb{Q} -linear combination of constant terms.

Corollary 3.3. *Let $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ with $P, Q \in \mathbb{Z}_p[\mathbf{x}^{\pm 1}]$. Then*

$$A(p^s n + k) \equiv A(p^r n + k) \pmod{p^r}$$

for all integers $n, k \geq 0$ and $s \geq r \geq 1$, provided that $p > \deg(P^k Q)$.

Proof. It follows from Lemma 3.1 and (13) that

$$\begin{aligned} A(p^s n + k) &\equiv A(k) \text{ct}[P(\mathbf{x})^{p^{s-1}n}] \pmod{p^s} \\ &\equiv A(k) \text{ct}[P(\mathbf{x}^{p^{s-r}})^{p^{r-1}n}] \pmod{p^r} \\ &= A(k) \text{ct}[P(\mathbf{x})^{p^{r-1}n}], \end{aligned}$$

as claimed. \square

The simple but useful special case $r = 1$ and $k = 0$ of the corollary above takes the following form. Here, p is large enough if $p > \deg(Q)$ and $P, Q \in \mathbb{Z}_p[\mathbf{x}^{\pm 1}]$.

Corollary 3.4. *Let $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ with $P, Q \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$. If p is large enough, then, for all integers $n \geq 0$ and $r \geq 1$,*

$$A(p^r n) \equiv A(pn) \pmod{p}.$$

4 C-finite sequences that are constant terms

In this section, we prove our main result, Theorem 1.3 stated in the introduction, thus classify those C-finite sequences that are constant terms or linear combinations of such. We start by proving the following weaker version, since it illustrates well our approach and the usefulness of the congruences proved in Section 3. We then extend the argument to prove Theorem 1.3 in full generality.

Proposition 4.1. *Let $A(n)$ be a C-finite sequence. $A(n)$ is a \mathbb{Q} -linear combination of constant terms if and only if all characteristic roots are rational.*

Proof. For one direction, note that

$$\text{ct}[(x + \lambda)^n (\lambda/x)^r] = \binom{n}{r} \lambda^n = \frac{n(n-1) \cdots (n-r+1)}{r!} \lambda^n. \quad (14)$$

Varying r , the right-hand side forms a basis for the span of the sequences $(n^r \lambda^n)_{n \geq 0}$. A sequence $A_0(n)$ of finite support can be represented as

$$A_0(n) = \text{ct}[x^n (A(0) + A(1)x^{-1} + \cdots + A(N)x^{-N})],$$

where N is the largest integer for which $A_0(N)$ is non-zero. It therefore follows with (5) that, if all characteristic roots λ are rational, then $A(n)$ can be represented as a linear combination of constant terms.

On the other hand, suppose that $A(n)$ is a linear combination of constant terms. Note that this implies that any shift $A(n+k)$, where $k \in \mathbb{Z}_{\geq 0}$, is a linear combination of constant terms as well. These shifts generate the space V_A of rational solutions of the minimal constant-coefficient recursion satisfied by $A(n)$. Thus, any sequence in V_A is a linear combination of constant terms. Assume, for contradiction, that there is a characteristic root λ that is not rational. Then among the sequences in V_A there is always

a sequence $B(n)$ of the form (6) (that is, $B(n)$ equals its separable part) which is not a trace sequence.

For instance, if $\lambda_1, \dots, \lambda_d$ are the roots of the minimal polynomial of λ , then the space V_λ of rational sequences of the form $b(n) = c_1\lambda_1^n + \dots + c_d\lambda_d^n$, with $c_1, \dots, c_d \in \mathbb{Q}$, is a d -dimensional subspace of V_A . Clearly, each sequence in V_λ is of the form (6). Note that $\lambda_1^n + \dots + \lambda_d^n$ and its multiples are the only trace sequences in V_λ . Since $d \geq 2$, we can therefore choose a sequence $B(n)$ in V_λ that is not a trace sequence.

It follows from Corollary 3.4 that $B(n)$ satisfies the congruences

$$B(p^r n) \equiv B(pn) \pmod{p}$$

for all $r \geq 1$ and all large enough primes p . Lemma 2.3 therefore implies that $B^{\text{sep}}(n) = B(n)$ is a trace sequence. This is a contradiction, and we conclude that all characteristic roots must be rational. \square

Example 4.2. Recall from (7) that the Fibonacci numbers $F(n)$ are C-finite with characteristic roots $(1 \pm \sqrt{5})/2$. Since these are not rational, it follows from Proposition 4.1 that $F(n)$ cannot be expressed as a linear combination of constant terms.

The same argument applied to (8) shows that the Lucas numbers $L(n)$ cannot be expressed as a linear combination of constant terms as well. Alternatively, this can also be concluded from the relationship

$$2L(n+1) - L(n) = 5F(n)$$

combined with the fact that Fibonacci numbers are not a sum of constant terms.

We next prove the case $r = 1$ of Theorem 1.3, that is Proposition 1.2, stating that a C-finite sequence $A(n)$ is a single constant term if and only if it has a single characteristic root λ and $\lambda \in \mathbb{Q}$.

Proof of Proposition 1.2. It follows from (5) and (14) that if $A(n)$ is a C-finite sequence with the single characteristic root $\lambda \in \mathbb{Q}$ (possibly repeated or possibly 0), then $A(n)$ is a constant term, namely $A(n) = \text{ct}[(x+\lambda)^n Q(x^{-1})]$ for a suitable polynomial $Q(x)$.

On the other hand, suppose that $A(n) = \text{ct}[P(x)^n Q(x)]$ is a single constant term. Since $A(n)$ is a C-finite sequence, it has a representation of the form (5) or, equivalently,

$$A(n) = A_0(n) + \sum_{j=1}^d \lambda_j^n p_j(n) \tag{15}$$

for pairwise distinct $\lambda_j \in \overline{\mathbb{Q}}^\times$ and nonzero $p_j(n) \in \overline{\mathbb{Q}}[n]$. As before, $A_0(n)$ is a sequence with finite support, corresponding to the characteristic root 0. It follows from Proposition 4.1 that all characteristic roots λ_j are rational, and this further implies that $p_j(n) \in \mathbb{Q}[n]$.

Let $c_0 = \text{ct}[P(\mathbf{x})] \in \mathbb{Q}$. From Lemma 3.1 (with $r = 1$ and $n = 1$) it follows that

$$A(p+n) \equiv A(n) \cdot c_0 \pmod{p}$$

for all $n \geq 0$ and all large enough primes p (namely, $p > \deg(P^n Q)$ and large enough so that $c_0 \in \mathbb{Z}_p$). Combining this congruence with (15) and applying Fermat's little theorem to reduce λ_j^{p+n} and $p_j(p+n)$ modulo p to λ_j^{n+1} and $p_j(n)$ respectively, we find that

$$\sum_{j=1}^d \lambda_j^{n+1} p_j(n) \equiv c_0 \left[A_0(n) + \sum_{j=1}^d \lambda_j^n p_j(n) \right] \pmod{p} \quad (16)$$

for all large enough p (in particular, so that p is larger than any denominator occuring in the $p_j(n)$ and so that $A_0(p+n) = 0$). Note that both sides of (16) are independent of p . Since they agree modulo any large enough p , it follows that they must be equal (for each fixed value of n). Accordingly, we have the identity

$$\sum_{j=1}^d \lambda_j^{n+1} p_j(n) = c_0 \left[A_0(n) + \sum_{j=1}^d \lambda_j^n p_j(n) \right] \quad \text{for all } n \geq 0. \quad (17)$$

Note that both sides of (17) are C-finite sequences so that, because the representation (15) is unique, we must have, in particular, $c_0 A_0(n) = 0$. If $c_0 = 0$ then it follows by comparison with the left-hand side of (17) that $d = 0$ so that $A(n) = A_0(n)$ with the single characteristic root $\lambda = 0$. In the other case, that is if $c_0 \neq 0$, we have $A_0(n) = 0$, so 0 is not a characteristic root. Further comparing both sides of (17), we find that $\lambda_j = c_0$ for all j . Since the λ_j are distinct, we conclude that $d = 1$ so that $A(n) = \lambda_1^n p_1(n)$ with the single characteristic root $\lambda_1 \in \mathbb{Q}^\times$. \square

We now extend Proposition 1.2 to the case of r -term \mathbb{Q} -linear combinations of constant terms, thus proving our main result Theorem 1.3. We recall that its statement is that a C-finite $A(n)$ sequence is an r -term \mathbb{Q} -linear combination of constant terms if and only if it has at most r characteristic roots, all of which are rational.

Proof of Theorem 1.3. The case $r = 1$ is proved by Proposition 1.2. With the same argument as in (14) it follows that any C-finite sequence with r characteristic roots, all of which are rational, can be represented as a linear combination of r constant terms.

Therefore, suppose that $r > 1$ and that

$$A(n) = \text{ct}[P_1(\mathbf{x})^n Q_1(\mathbf{x})] + \cdots + \text{ct}[P_r(\mathbf{x})^n Q_r(\mathbf{x})]$$

is an r -term \mathbb{Q} -linear combination of constant terms with $P_j, Q_j \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$. We need to show that $A(n)$ has at most r characteristic roots, all of which are rational. As in the proof of Proposition 1.2, we find that all characteristic roots of $A(n)$ are rational and that $A(n)$ can be represented in the form (15) with $p_j(n) \in \mathbb{Q}[n]$.

Let $c_j = \text{ct}[P_j(\mathbf{x})] \in \mathbb{Q}$. It follows from Lemma 3.1 that

$$A(p+n) \equiv c_1 \text{ct}[P_1(\mathbf{x})^n Q_1(\mathbf{x})] + \cdots + c_r \text{ct}[P_r(\mathbf{x})^n Q_r(\mathbf{x})] \pmod{p}$$

for all $n \geq 0$ and all large enough primes p . On the other hand, for large p , by Fermat's little theorem,

$$A(p+n) \equiv \sum_{j=1}^d \lambda_j^{n+1} p_j(n) \pmod{p}.$$

Note that the right-hand sides of the last two congruences are independent of p . Since the congruences hold modulo all large enough primes, we conclude that

$$\sum_{j=1}^d \lambda_j^{n+1} p_j(n) = c_1 \text{ct}[P_1(\mathbf{x})^n Q_1(\mathbf{x})] + \cdots + c_r \text{ct}[P_r(\mathbf{x})^n Q_r(\mathbf{x})].$$

Note that the sequence

$$B(n) := \sum_{j=1}^d \lambda_j^{n+1} p_j(n) - c_1 A(n) = \sum_{j=1}^d (\lambda_j - c_1) \lambda_j^n p_j(n) - c_1 A_0(n)$$

is C-finite and is an $(r-1)$ -term \mathbb{Q} -linear combination of constant terms. By induction, we may conclude that $B(n)$ has at most $r-1$ characteristic roots, all of which are rational. By comparison with (15), we see that $A(n)$ has at most one more characteristic root than $B(n)$. Thus $A(n)$ has at most r characteristic roots, which is what we had to show. \square

Theorem 1.3 classifies those rational recursive sequences with constant coefficients which can be represented as a linear combination of r constant terms. In particular, a rational C-finite sequence $A(n)$ is a linear combination of constant terms if and only if all of its characteristic roots are rational. It is natural to wonder whether we can restrict to integer sequences and conclude that all characteristic roots must be integral. This can be achieved by using the following proposition¹, that we could not locate in the vast literature on C-finite sequences.

Proposition 4.3. *Let $A(n)$ be a C-finite sequence with characteristic roots $\lambda_1, \dots, \lambda_d \in \mathbb{Q}$. If $A(n)$ is an integer sequence, then $\lambda_1, \dots, \lambda_d \in \mathbb{Z}$.*

Proof. By assumption, $A(n)$ is equal to $\sum_{i=1}^d p_i(n)\lambda_i^n$, where the λ_i 's are mutually distinct rational numbers and the $p_i(x)$'s are polynomials in $\mathbb{Q}[x]$. We will prove that if for some $N \in \mathbb{Z} \setminus \{0\}$ we have that $A(n) \in \frac{1}{N}\mathbb{Z}$ for all n , then all the λ_i 's are integers.

Let us start with the observation that this is true if $d = 1$; indeed, if $\lambda_1 = a/b$ with coprime integers a, b , and $p_1(n) = q(n)/c$ with $q(x) \in \mathbb{Z}[x]$ and $c \in \mathbb{Z}$, then the assumption “ $A(n) = p_1(n)\lambda_1^n \in \frac{1}{N}\mathbb{Z}$ for all n ” implies that b^n divides $Nq(n)$ for all n , hence $b = 1$.

Let us now treat the general case. Denote by V the $d \times d$ Vandermonde matrix attached with the λ_i 's, that is $V = (\lambda_i^{j-1})_{1 \leq i, j \leq d}$. Since the λ_i 's are mutually distinct, V is in $\text{GL}_d(\mathbb{Q})$. Therefore, the equality

$$[p_1(n)\lambda_1^n, \dots, p_d(n)\lambda_d^n] \cdot V = [A(n), \dots, A(n+d-1)]$$

implies that each term $p_i(n)\lambda_i^n$ is equal to $1/\det(V)$ times a linear combination of the integers $A(n), \dots, A(n+d-1)$ with fixed rational coefficients. In other terms, each $p_i(n)\lambda_i^n$ is in $\frac{1}{N_i}\mathbb{Z}$ for some $N_i \in \mathbb{Z} \setminus \{0\}$ independent of n . By the case $d = 1$, this implies that all the λ_i 's are integers. \square

We conclude this section with the following immediate consequence of Proposition 1.2, Theorem 1.3 and Proposition 4.3:

Corollary 4.4. *Let $A(n) \in \mathbb{Z}$ be a C-finite sequence. $A(n)$ is a constant term if and only if it has a single characteristic root λ and $\lambda \in \mathbb{Z}$. More generally, $A(n)$ is an r -term \mathbb{Q} -linear combination of constant terms if and only if it has at most r distinct characteristic roots, all of which are integral.*

¹The proof of Prop. 4.3 was communicated to us by Carlo Sanna (Politecnico di Torino).

5 An analog of Minton's theorem

In this section, we record the following result which, though having a much simpler proof, is pleasingly similar to Theorem 2.2 due to Minton [Min14]. Moreover, this result gives a classification of constant term sequences of the form $A(n) = \text{ct}[P(\mathbf{x})^n]$ among all constant term sequences $\text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$.

Proposition 5.1. *Suppose $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ with $P, Q \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$. Then the following are equivalent:*

- (a) *For all large enough primes p and for all $r \geq 1$, $A(n)$ satisfies the Gauss congruences (9).*
- (b) *For all large enough primes p , $A(n)$ satisfies the congruences (10).*
- (c) $A(n) = A(0) \text{ct}[P(\mathbf{x})^n]$.

Proof. We conclude from Lemma 3.1 with $r = 1$ and $k = 0$ that

$$A(pn) \equiv A(0) \text{ct}[P(\mathbf{x})^n] \pmod{p}$$

for large enough p (namely, if $p > \deg(Q)$). If $A(n)$ satisfies the congruences (10), we find that, for large enough p ,

$$A(n) \equiv A(0) \text{ct}[P(\mathbf{x})^n] \pmod{p}.$$

In that case, since this congruence holds modulo infinitely many p , we conclude the equality $A(n) = A(0) \text{ct}[P(\mathbf{x})^n]$. Thus the third condition follows from the second.

To complete the proof, we need to show that the third condition implies the first. This follows from Lemma 3.1 with $k = 0$ and $Q = 1$. \square

Remark 5.2. Note that Proposition 5.1 does not imply that if $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ satisfies the Gauss congruences (9) for large enough primes, then Q must be constant. For instance, for any $P(x) \in \mathbb{Z}[x^{\pm 1}]$, the constant terms $\text{ct}[P(x^2)^n(1+x)] = \text{ct}[P(x^2)^n] = \text{ct}[P(x)^n]$ satisfy the Gauss congruences for all primes p , even though the first constant term has a non-constant Q . Proposition 5.1 rather shows that if (a) or (b) are fulfilled, then Q can be replaced by $\text{ct}[Q]$.

6 Hypergeometric constant terms

Exiting the class of C-finite sequences, we find it natural to ask (Question 5 in the introduction): Which hypergeometric sequences² $A(n)$ are constant term sequences?

The reason for the specialization to hypergeometric sequences is three-fold. First, it can be argued that it is the easiest P-recursive case. Second, similar to constant terms, hypergeometric sequences are not stable under addition. Finally, as we will see below in Lemma 6.1, the congruences proven in Section 3 behave nicely with the hypergeometric assumption.

It follows from Lemma 3.1 (specialized to $n = 1$ and $r = 1$) that if $A(n) = \text{ct}[P(\mathbf{x})^n Q(\mathbf{x})]$ with $P, Q \in \mathbb{Q}[\mathbf{x}^{\pm 1}]$, then

$$A(p+k) \equiv A(k) \text{ct}[P(\mathbf{x})] \pmod{p}$$

for all integers $k \geq 0$, provided that $p > \deg(P^k Q)$ and $P, Q \in \mathbb{Z}_p[\mathbf{x}^{\pm 1}]$. In other words, if $A(n)$ is a constant term, then there exists a constant $c \in \mathbb{Q}$ such that, for each $k \in \mathbb{Z}_{\geq 0}$, the congruences

$$A(p+k) \equiv A(k) \cdot c \pmod{p} \tag{18}$$

hold for all large enough p . We shall now show that, for hypergeometric sequences, the congruences (18) follow from the base case $k = 0$.

Lemma 6.1. *Let $A(n)$ be a hypergeometric sequence. Suppose that there exists a constant $c \in \mathbb{Q}$ such that*

$$A(p) \equiv c \pmod{p} \tag{19}$$

for all large enough p . Then, for each $k \in \mathbb{Z}_{\geq 0}$, the congruence (18) holds for sufficiently large p .

Proof. Since $A(n)$ is hypergeometric, we have $A(n+1) = \rho(n)A(n)$ for a rational function $\rho(n) = \beta(n)/\alpha(n)$ with $\alpha(n), \beta(n) \in \mathbb{Z}[n]$. Fix $k \in \mathbb{Z}_{\geq 0}$ and suppose that the congruence (18) holds for all large enough p . By applying the hypergeometric recurrence twice, we obtain

$$A(p+k+1) = \rho(p+k)A(p+k) \equiv \rho(k)cA(k) = cA(k+1) \pmod{p},$$

²Recall that a sequence $A(n)$ is hypergeometric if it satisfies a first-order recurrence $\alpha(n)A(n+1) = \beta(n)A(n)$ for some polynomials $\alpha(n), \beta(n) \in \mathbb{Q}[n]$. For our purposes we will assume $\alpha(n) \neq 0$ for all $n \geq 0$.

which is (18) with $k + 1$ in place of k . Here we used that $\rho(p + k) \equiv \rho(k) \pmod{p}$, which holds true provided that $\alpha(k) \not\equiv 0 \pmod{p}$. The latter is true for all sufficiently large p since, by assumption, $\alpha(k) \neq 0$. The claim therefore follows by induction on k . \square

Remark 6.2. Note that Lemma 6.1 does not hold for non-hypergeometric sequences in general. For instance, it does not hold for the Lucas numbers $L(n)$ as defined in (8). These form a trace sequence so that, by Minton's Theorem 2.2, the Gauss congruences (9) are satisfied. In the case $n = 1$, these imply the congruences (19). However, the Lucas numbers do not satisfy the congruences (18) for $k > 0$.

Lemma 3.1 gives a necessary condition for $A(n)$ to be a constant term sequence. It is natural to wonder whether, or to which degree, this condition is sufficient: Is an integer hypergeometric sequence $A(n)$ that satisfies the congruences (19) a constant term? Natural sources of potential counterexamples to this question are families of integer sequences that are quotients of binomial coefficients but cannot be written as products of those, for example $A(n) = \binom{8n}{4n} \binom{4n}{n} \binom{2n}{n}^{-1}$ (see [Bob09, Thm. 1.2]).

We recall that the corresponding question for diagonals (1) (namely, to classify which hypergeometric sequences $A(n)$ are coefficients of diagonals) also remains open. The following conjecture due to Christol [Chr90, Conjecture 4, p. 55] attempts such a classification. In its statement, we call a sequence $(A(n))_{n \geq 0}$ *almost integral* if there exists a positive integer K such that $K^{n+1}A(n) \in \mathbb{Z}$ for all integers $n \geq 0$. An almost integral sequence with (at most) geometric growth is called *globally bounded*.

Conjecture 6.3 ([Chr90]). *Let $(A(n))_{n \geq 0}$ be sequence of rational numbers. The generating function $\sum_{n \geq 0} A(n)t^n$ is the diagonal of a rational function if and only if $(A(n))_{n \geq 0}$ is P-recursive and globally bounded.*

Any hypergeometric sequence is P-recursive since it satisfies, by definition, a recurrence with polynomial coefficients of order one. Moreover, thanks to a result of Christol [Chr87], [Chr90] it is easy to check when a hypergeometric sequence is integral (in the case when $\alpha(n)$ and $\beta(n)$ in the definition split in $\mathbb{Q}[n]$). This makes hypergeometric sequences a natural source of potential counterexamples to Conjecture 6.3. We refer to [BBC⁺13], [AKM20] and [BY22] for recent progress in this area. Here, we only mention that even for

$$A(n) = \frac{\left(\frac{1}{9}\right)_n \left(\frac{4}{9}\right)_n \left(\frac{5}{9}\right)_n}{n!^2 \left(\frac{1}{3}\right)_n} \quad (20)$$

the conjecture is open. In other words, it is an open question whether the sequence (20) is the diagonal of a rational function. On the other hand, we will show in this section that (20) is not a constant term. Before doing so, we first prove the following result answering Question 5 for a special family of hypergeometric sequences.

Lemma 6.4. *Let $m \geq 2$ be an integer and consider the sequence*

$$A_m(n) = \frac{\left(\frac{1}{m}\right)_n \left(1 - \frac{1}{m}\right)_n}{n!^2}. \quad (21)$$

- (a) $A_m(n)$ is a diagonal for all $m \geq 2$.
- (b) $A_m(n)$ is a constant term if and only if $m \in \{2, 3, 4, 6\}$.

Note that the classification in Lemma 6.4 suggests that constant term sequences are special among diagonals and often have significant additional arithmetic properties. Indeed, the cases $m \in \{2, 3, 4, 6\}$ (see [A002894](#), [A006480](#), [A000897](#) and [A113424](#) in the on-line encyclopedia of integer sequences [ST22]) correspond precisely to those special hypergeometric functions underlying Ramanujan's theories of elliptic functions ($m = 2$ being the classical case and $m = 3, 4, 6$ corresponding the alternative bases). We refer to [BBG95] for more information.

Example 6.5. The hypergeometric sequence

$$B(n) = 5^{3n} \frac{\left(\frac{1}{5}\right)_n \left(\frac{4}{5}\right)_n}{n!^2} = 1, 20, 1350, 115500, 10972500, \dots \quad (22)$$

is an integer sequence and grows at most exponentially. As suggested by Christol's Conjecture 6.3 and stated in Lemma 6.4, the sequence $B(n)$ is a diagonal. However, $B(n)$ is not a constant term. The proof of Lemma 6.4 in this case proceeds by showing that we have the congruences

$$B(p) \equiv \begin{cases} 20, & \text{if } p \equiv \pm 1 \pmod{5}, \\ 30, & \text{otherwise,} \end{cases} \pmod{p},$$

which contradict Lemma 6.1.

Proof of Lemma 6.4. Part (a) follows from the fact that the generating function of $A_m(n)$ is the Hadamard (term-wise) product of $(1 - x)^{-1/m}$ and $(1 - x)^{1/m-1}$. The latter are algebraic functions and hence diagonals by a result of Furstenberg [Fur67]. Since diagonals are closed under Hadamard products [Chr88], it follows that $A_m(n)$ is a diagonal.

That $A_m(n)$ is a constant term if $m \in \{2, 3, 4, 6\}$ follows from the following alternative representations as products of binomial coefficients:

$$\begin{aligned} 2^{4n} A_2(n) &= \frac{(2n)!^2}{n!^4} = \binom{2n}{n}^2, \\ 3^{3n} A_3(n) &= \frac{(3n)!}{n!^3} = \binom{3n}{2n} \binom{2n}{n}, \\ 4^{3n} A_4(n) &= \frac{(4n)!}{(2n)!n!^2} = \binom{4n}{2n} \binom{2n}{n}, \\ 2^{4n} 3^{3n} A_6(n) &= \frac{(6n)!}{(3n)!(2n)!n!} = \binom{6n}{3n} \binom{3n}{n}. \end{aligned}$$

In the remainder, we will show that $A_m(n)$ is not a constant term if $m \notin \{2, 3, 4, 6\}$. If m is coprime to p (as it is for large enough p) then the right-hand side of

$$m^p \left(\frac{1}{m}\right)_p = 1 \cdot (m+1)(2m+1) \cdots ((p-1)m+1)$$

is a product of all the residues modulo p . In particular, exactly one factor is of the form ap where $a \in \{1, 2, \dots, m-1\}$ is characterized by $ap \equiv 1 \pmod{m}$. By Wilson's theorem, we therefore have

$$m^p \left(\frac{1}{m}\right)_p \equiv -ap \pmod{p^2}$$

or, equivalently,

$$\frac{m^p \left(\frac{1}{m}\right)_p}{p!} \equiv a \pmod{p}.$$

Similarly,

$$m^p \left(1 - \frac{1}{m}\right)_p = (m-1)(2m-1) \cdots (pm-1)$$

and, again, the right-hand side features a product of all residues modulo p . Exactly one factor is of the form bp where $b \in \{1, 2, \dots, m-1\}$ is characterized by $bp \equiv -1 \pmod{m}$. It follows that $b = m - a$. Combined, we conclude that

$$m^{2p} A_m(p) = \frac{m^{2p} \left(\frac{1}{m}\right)_p \left(1 - \frac{1}{m}\right)_p}{p!^2} \equiv a(m-a) \pmod{p}. \quad (23)$$

Since $a \in \{1, 2, \dots, m-1\}$ is characterized by $a \equiv 1/p \pmod{m}$ it, in particular, depends only on the residue class of p modulo m . As p ranges through all primes, it follows from Dirichlet's theorem on primes in arithmetic progressions, that each value $a \in \{1, 2, \dots, m-1\}$ with a coprime to

m appears infinitely many times. There are $\phi(m)$ many such values of a , where ϕ is Euler's totient function. Consequently, the quantity $a(m-a)$ on the right-hand side of (23) takes $\phi(m)/2$ many different values as p ranges through all primes $p > m$.

On the other hand, if $A_m(n)$ is a constant term sequence, then by (19) there exists a constant $c \in \mathbb{Q}$ such that $m^{2p}A_m(p) \equiv c \pmod{p}$ for all large enough primes. If (23) holds for infinitely many p , we necessarily have $c = a(m-a)$, which is only possible if $\phi(m)/2 = 1$.

Thus, if $\phi(m) > 2$ then $m^{2p}A_m(p)$ cannot satisfy the congruences (19) for all large enough primes and, hence, the sequences $m^{2n}A_m(n)$ and $A_m(n)$ cannot be constant terms. Since $\phi(m) > 2$ for all integers $m \geq 2$ except for $m \in \{2, 3, 4, 6\}$, the claim follows. \square

For hypergeometric sequences, we therefore have the following inclusions $\{\text{constant terms}\} \subsetneq \{\text{diagonals}\} \subseteq \{\text{P-recursive \& globally bounded seq's}\}$.

We note that these inclusions are also true for C-finite as well as for P-recursive sequences. An example for the strictness of the first inclusion in the realm of hypergeometric sequences is given by the sequence (22) and in the class of C-finite sequences by the Fibonacci numbers. The second inclusion is a consequence of a result due to Lipshitz [Lip88] and it is strict if and only if Christol's Conjecture 6.3 (restricted to hypergeometric sequences) is false. A potential candidate of a globally bounded hypergeometric sequence that is not a diagonal is sequence (20). We now show that this sequence is not a constant term.

Lemma 6.6. *The hypergeometric sequence $A(n)$ defined in (20) is not a constant term sequence.*

Proof. Proceeding as in the proof of Lemma 6.4, we find

$$m^p \left(\frac{r}{m}\right)_p = r(m+r) \cdots ((p-1)m+r),$$

where the right-hand side is a product over all residues modulo p . Exactly one factor is of the form ap where $a \in \{1, 2, \dots, m-1\}$ is characterized by $ap \equiv r \pmod{m}$. In that case,

$$\frac{m^p \left(\frac{r}{m}\right)_p}{p!} \equiv a \pmod{p}.$$

If $p \equiv 1 \pmod{9}$, we therefore find

$$\frac{9^p \left(\frac{1}{9}\right)_p}{p!} \equiv \frac{3^p \left(\frac{1}{3}\right)_p}{p!} \equiv 1, \quad \frac{9^p \left(\frac{4}{9}\right)_p}{p!} \equiv 4, \quad \frac{9^p \left(\frac{5}{9}\right)_p}{p!} \equiv 5 \pmod{p},$$

which combine to

$$3^{5p}A(p) = 3^{5p} \frac{\left(\frac{1}{9}\right)_p \left(\frac{4}{9}\right)_p \left(\frac{5}{9}\right)_p}{p!^2 \left(\frac{1}{3}\right)_p} \equiv \frac{1 \cdot 4 \cdot 5}{1} = 20 \pmod{p}.$$

On the other hand, if $p \equiv -1 \pmod{9}$, then

$$\frac{9^p \left(\frac{1}{9}\right)_p}{p!} \equiv 8, \quad \frac{3^p \left(\frac{1}{3}\right)_p}{p!} \equiv 2, \quad \frac{9^p \left(\frac{4}{9}\right)_p}{p!} \equiv 5, \quad \frac{9^p \left(\frac{5}{9}\right)_p}{p!} \equiv 4 \pmod{p},$$

which combine to

$$3^{5p}A(p) = 3^{5p} \frac{\left(\frac{1}{9}\right)_p \left(\frac{4}{9}\right)_p \left(\frac{5}{9}\right)_p}{p!^2 \left(\frac{1}{3}\right)_p} \equiv \frac{8 \cdot 4 \cdot 5}{2} = 80 \pmod{p}.$$

As in the proof of Lemma 6.4 we conclude that $3^{5n}A(n)$ and, hence, $A(n)$ cannot be a constant term. \square

Acknowledgments. Our warm thanks go to the [PolSys team](#) of the Sorbonne University for providing a very nice atmosphere for the three authors to collaborate. We are grateful to [Carlo Sanna](#) who provided the elegant and elementary proof of Proposition 4.3 and permitted us to include it in our article. The first and third authors were supported by ANR-19-CE40-0018 [De Rerum Natura](#) and the [WTZ collaboration/Amadeus project](#) FR-09/2021 (46411YJ). The second author gratefully acknowledges support through a Collaboration Grant (#514645) awarded by the Simons Foundation. The third author is funded by DOC scholarship P-26101 of the [ÖAW](#).

References

- [AKM20] Y. Abdelaziz, C. Koutschan, and J.-M. Maillard. On Christol’s conjecture. *Journal of Physics A: Mathematical and Theoretical*, 53(20):205201, 2020.
- [BBC⁺13] A. Bostan, S. Boukraa, G. Christol, S. Hassani, and J.-M. Maillard. Ising n -fold integrals as diagonals of rational functions and integrality of series expansions. *Journal of Physics A: Mathematical and Theoretical*, 46(18):185202, May 2013.

- [BBG95] B. C. Berndt, S. Bhargava, and F. G. Garvan. Ramanujan’s Theories of Elliptic Functions to Alternative Bases. *Transactions of the American Mathematical Society*, 347(11):4163, November 1995.
- [BHS18] F. Beukers, M. Houben, and A. Straub. Gauss congruences for rational functions in several variables. *Acta Arithmetica*, 184:341–362, 2018.
- [Bob09] J. W. Bober. Factorial ratios, hypergeometric series, and a family of step functions. *Journal of the London Mathematical Society. Second Series*, 79(2):422–444, 2009.
- [BY22] A. Bostan and S. Yurkevich. On a class of hypergeometric diagonals. *Proceedings of the American Mathematical Society*, 150(3):1071–1087, 2022.
- [Chr87] G. Christol. Fonctions hypergéométriques bornées. *Groupe de travail d’analyse ultramétrique*, 14:1–16, 1986-1987. Talk no. 8.
- [Chr88] G. Christol. Diagonales de fractions rationnelles. In *Séminaire de Théorie des Nombres, Paris, 1986–87*, volume 7 of *Progr. Math.*, pages 65–90. Birkhäuser Boston, Boston, MA, 1988.
- [Chr90] G. Christol. Globally bounded solutions of differential equations. In K. Nagasaka and E. Fouvry, editors, *Analytic Number Theory*, number 1434 in *Lecture Notes in Mathematics*, pages 45–64. Springer Berlin Heidelberg, January 1990.
- [EvdPSW03] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward. *Recurrence Sequences*, volume 104 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.
- [Fur67] H. Furstenberg. Algebraic functions over finite fields. *Journal of Algebra*, 7(2):271–277, October 1967.
- [Gor21] O. Gorodetsky. New representations for all sporadic Apéry-like sequences, with applications to congruences. *Experimental Mathematics*, 2021.
- [KP11] M. Kauers and P. Paule. *The Concrete Tetrahedron*. Springer-Verlag, 2011.

- [Lip88] L. Lipshitz. The diagonal of a D -finite power series is D -finite. *Journal of Algebra*, 113(2):373–378, 1988.
- [Min14] G. T. Minton. Linear recurrence sequences satisfying congruence conditions. *Proceedings of the American Mathematical Society*, 142(7):2337–2352, April 2014.
- [Pó22] G. Pólya. Sur les séries entières, dont la somme est une fonction algébrique. *L’Enseignement Mathématique*, 22:38–47, 1921/1922.
- [RY15] E. Rowland and R. Yassawi. Automatic congruences for diagonals of rational functions. *Journal de Théorie des Nombres de Bordeaux*, 27(1):245–288, 2015.
- [ST22] N. J. A. Sloane and The OEIS Foundation Inc. The On-Line Encyclopedia of Integer Sequences, 2022. Published electronically at <http://oeis.org>.
- [Str14] A. Straub. Multivariate Apéry numbers and supercongruences of rational functions. *Algebra & Number Theory*, 8(8):1985–2007, 2014.
- [Str22] A. Straub. On congruence schemes for constant terms and their applications. *Research in Number Theory*, 8(3), May 2022.
- [Zag18] D. B. Zagier. The arithmetic and topology of differential equations. In V. Mehrmann and M. Skutella, editors, *Proceedings of the European Congress of Mathematics, Berlin, 18-22 July, 2016*, pages 717–776. European Mathematical Society, 2018.