

# THE MEMBERSHIP PROBLEM FOR HYPERGEOMETRIC SEQUENCES WITH RATIONAL PARAMETERS

KLARA NOSAN,<sup>1</sup> AMAURY POULY,<sup>1</sup> MAHSA SHIRMOHAMMADI,<sup>1</sup>  
AND JAMES WORRELL<sup>2</sup>

**ABSTRACT.** We investigate the Membership Problem for hypergeometric sequences: given a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  of rational numbers and a target  $t \in \mathbb{Q}$ , **decide whether  $t$  occurs in the sequence.** We show **decidability** of this problem under the assumption that in the defining recurrence  $p(n)u_{n+1} = q(n)u_n$ , **the roots of the polynomials  $p(x)$  and  $q(x)$  are all rational numbers.** Our proof relies on bounds on the density of primes in arithmetic progressions. We also observe a relationship between the decidability of the Membership problem (and variants) and the Rohrlach-Lang conjecture in transcendence theory.

## 1. INTRODUCTION

Recursively defined sequences are natural objects of study in computation, arising in the analysis of algorithms, weighted automata, loop termination, and probabilistic models, among many other areas. In this context, the following decision problem frequently arises: *does a given value appear in a given recurrence sequence?* Perhaps, the most famous example of this type of membership (or reachability) problem is the Skolem Problem, which asks to decide the existence of a zero term in a given linear recurrence sequence (with constant coefficients). For the majority of problems of this kind, their decidability status is wide open and apparently very challenging. For example, the Skolem Problem has been regarded as open since at least the 1970s, with decidability only known for linear recurrences of order at most four [12, 17].

In this paper we are concerned with the membership problem for hypergeometric sequences, which are those satisfying an order-1 recurrence  $p(n)u_{n+1} = q(n)u_n$  with polynomial coefficients  $p(x)$  and  $q(x)$ . In other words, we focus on order-1 polynomially recursive sequences: arguably the simplest class of recurrence sequences which are not linearly recursive. The membership problem here asks, given a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  and target  $t$ , whether there exists  $n$  with  $u_n = t$ .

Decidability of this problem may appear trivial at first glance. Indeed, the sequence  $\langle u_n \rangle_{n=0}^\infty$  either diverges in absolute value or converges to a value in  $\mathbb{R}$ . If the sequence does not converge to  $t$  then it is not difficult to compute a bound  $N$  such that  $u_n \neq t$  for all  $n > N$ . But such a bound can also be computed in case one knows that  $\langle u_n \rangle_{n=0}^\infty$  converges to  $t$  (by straightforward arguments about the monotonicity of the convergence). The difficulty with this analysis is that it depends on being able to distinguish the two cases above, i.e., that it be semi-decidable whether  $\langle u_n \rangle_{n=0}^\infty$  converges to  $t$ . We explore this question in Section 3, observing its connection to the Rohrlach-Lang conjecture in number theory.

In the rest of the paper we approach the decidability of the membership problem from a different angle—specifically, by considering the prime divisors of  $u_n$ . Our strategy is to show that **(except in some degenerate cases) for all sufficiently large  $n$ ,  $u_n$  has a prime divisor  $p$  that is not also a prime divisor of the target  $t$ .** This

<sup>1</sup> UNIVERSITÉ DE PARIS, CNRS, IRIF, F-75013 PARIS, FRANCE

<sup>2</sup> DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF OXFORD, UK

allows us to compute a bound  $N$  such that  $u_n \neq t$  for all  $n > N$ . We obtain this bound using classical results on the distribution of primes in arithmetic progressions. However our proof requires that the polynomial-coefficients  $p(x)$  and  $q(x)$  of the order-1 recurrence that specifies the sequence  $\langle u_n \rangle_{n=0}^\infty$  have rational roots. Of course, in general, these roots will be algebraic numbers. We remark that such rationality assumptions are a feature of work on divisibility properties of hypergeometric sequences (and their associated generating functions, which are hypergeometric series); see, for example, [6].

$\Rightarrow$  the splitting field is  $\mathbb{Q}$  itself

**1.1. Related work.** The paper [1] studies the asymptotic behaviour of sequences of the form  $v_p(u_n)$ , where  $v_p$  is the  $p$ -adic valuation and  $\langle u_n \rangle_{n=0}^\infty$  is a sequence of integers satisfying a recurrence  $u_{n+1} = q(n)u_n$ , i.e., an order-1 polynomial recurrence whose leading coefficient is constant. By contrast, we consider general order-1 recurrences, but consider only divisibility or non-divisibility by a well-chosen set of primes.

The problem of deciding positivity of order-2 polynomially recursive sequences and of deciding the existence of zeros in such sequences is considered in [8, 9, 14, 16]. These works all place syntactic restrictions on the degrees of the polynomial-coefficients involved in the recurrences, and all four give algorithms that are not guaranteed to terminate for all initial values of a given recurrence (essentially due to phenomena similar to that explored in Section 3). A polynomially recursive sequence is said to be a closed form if it is the sum of hypergeometric sequences [15, Definition 8.1.1]. Using the fact that the quotient of two hypergeometric sequences is again hypergeometric, one can easily deduce that the problem of deciding the existence of a zero in a closed-form order-2 polynomially recursive sequence reduces to the membership problem for hypergeometric sequences.

The paper [3] proves a version of the Skolem-Mahler-Lech paper for a subclass of polynomially recursive sequences. Specifically for a sequence  $\langle u_n \rangle_{n=0}^\infty$  satisfying a polynomial recurrence  $u_n = \sum_{k=1}^d p_k(n)u_{n-k}$ , under the assumption that  $p_d$  is a non-zero constant polynomial, it is shown that  $\{n \in \mathbb{N} : u_n = 0\}$  is the union of a finite set and finitely many arithmetic progressions. It remains open whether this conclusion extends to the class of all polynomially recursive sequences. The proof of this result in [3] uses Strassman's Theorem in  $p$ -adic analysis and appears not to give information of how to decide the existence of a zero in a given sequence.

!

## 2. THE MEMBERSHIP PROBLEM

We denote by  $\mathbb{Q}[x]$  the ring of univariate polynomials with rational coefficients, and by  $\mathbb{Q}(x)$  the field of univariate rational functions with rational coefficients.

An infinite sequence  $\langle u_n \rangle_{n=0}^\infty$  of rational numbers is called a *univariate hypergeometric sequence* if it satisfies a recurrence of the form

$$p(n)u_{n+1} - q(n)u_n = 0, \quad (1)$$

where  $p(x), q(x) \in \mathbb{Q}[x]$  are polynomials, and  $p(x)$  has no non-negative integer zeros. By the latter assumption on  $p(x)$ , the recurrence relation (1) uniquely defines an infinite sequence of rational numbers once the initial value  $u_0 \in \mathbb{Q}$  is specified. We say that such an induced sequence is a *hypergeometric sequence with rational parameters* if both  $p(x)$  and  $q(x)$  split completely over  $\mathbb{Q}$ .

Recurrence (1) can be reformulated as follows:

$$u_{n+1} = r(n)u_n,$$

where  $r(x) \in \mathbb{Q}(x)$  is a rational function that, by the assumption above, has no nonnegative integer pole. The rational function  $r(x)$  is called the shift quotient of  $\langle u_n \rangle_{n=0}^\infty$ .

it could have a nonnegative rational zero

Let us introduce the decision problem we seek to investigate. We say that  $t \in \mathbb{Q}$  is a *member* of a sequence  $\langle u_n \rangle_{n=0}^\infty$  if there exists  $n \in \mathbb{N}$  such that  $u_n = t$ ; we further refer to  $n$  as an index of  $t$  in the sequence. The *Membership Problem (MP)* for hypergeometric sequences is the problem of deciding, given a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  (specified by a recurrence of the form (1) with a given initial value  $u_0$ ) and a target  $t \in \mathbb{Q}$ , whether  $t$  is a member of  $\langle u_n \rangle_{n=0}^\infty$ . Our main contribution in this paper is to show that MP is decidable for hypergeometric sequences with rational parameters. Our solution in fact allows to compute the set of all indices of  $t$  in the sequence  $\langle u_n \rangle_{n=0}^\infty$ .

We will assume that in instances of MP, the numerator  $q(x)$  of the shift quotient has no non-negative integer zeros and that the target  $t$  is non-zero. This assumption is without loss of generality for the decidability results as discussed in Appendix A.

**2.1. Limit of Shift Quotients.** Given an instance of MP, consisting of a rational value  $t$  and a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  with rational parameters and initial value  $u_0$ , our general approach to solving MP is to show that there is an effectively computable upper bound  $N$ , depending only on the sequence  $\langle u_n \rangle_{n=0}^\infty$ , such that  $u_n = t$  only if  $n \leq N$ . This reduces the membership test for  $t$  to that of searching within the finite set  $\{u_0, \dots, u_N\}$  and hence entails the decidability of MP and computability of the set of indices of  $t$  in  $\langle u_n \rangle_{n=0}^\infty$ .

*which is a finite set*

To obtain the bound  $N$ , we first note that as  $x \rightarrow \infty$  the shift quotient  $r(x) \in \mathbb{Q}(x)$  converges to some limit in  $\mathbb{Q}$  or diverges to  $\pm\infty$ . In case  $r(x)$  diverges to  $\pm\infty$  or converges to some  $\ell \in \mathbb{Q}$  with  $|\ell| > 1$ , then there exists  $N \in \mathbb{N}$  such that  $|u(n)| = |u_0 \prod_{k=1}^n r(k)| > |t|$  for all  $n \geq N$ . An analogous argument applies when  $r(x)$  converges to some  $\ell$  with  $|\ell| < 1$ .

The challenging case is when the shift quotient  $r(x) \in \mathbb{Q}(x)$  of the sequence converges to  $\pm 1$  as  $x \rightarrow \infty$ . In this case, we establish the existence of the bound  $N$  by providing an infinite sequence  $\langle p_i \rangle_{i=0}^\infty$  of integer primes such that for all sufficiently large  $n$  one prime in the sequence appears in the prime decomposition of  $u_n$  but not  $t$ . We rely on results from analytic number theory on density of primes to construct the sequence  $\langle p_i \rangle_{i=0}^\infty$  of primes. The proof, presented in Section 4, is constructive and allows to compute the bound  $N$ .

### 3. CONNECTION TO THE ROHRLICH-LANG CONJECTURE

In this section, we highlight the link between the Membership Problem for hypergeometric sequences and the Rohrlich(-Lang) conjecture, which concerns algebraic relations among values of the Gamma function at rational points.

Let  $\Gamma$  denote the Gamma function [7]. Using Euler's infinite-product characterisation, it can be shown that certain infinite products of rational functions converge to quotients of values of the Gamma function. In particular, the following is standard, see for example [5].

**Proposition 1.** *Let  $d \geq 1$  and  $\alpha_1, \dots, \alpha_d$  and  $\beta_1, \dots, \beta_d$  be nonzero complex numbers, none of which are negative integers. If  $\alpha_1 + \dots + \alpha_d = \beta_1 + \dots + \beta_d$  then*

$$\prod_{k=0}^{\infty} \frac{(k + \alpha_1) \cdots (k + \alpha_d)}{(k + \beta_1) \cdots (k + \beta_d)} = \frac{\Gamma(\beta_1) \cdots \Gamma(\beta_d)}{\Gamma(\alpha_1) \cdots \Gamma(\alpha_d)}, \quad (2)$$

*otherwise the infinite product diverges.*

We have already observed that the difficult case of the Membership Problem for hypergeometric sequences is when the shift quotient  $r(x)$  converges to 1 as  $x$  tends to infinity. By splitting the numerator and denominator of  $r(x)$  into linear factors,

the Membership Problem in this case is equivalent to deciding whether there exists  $n \in \mathbb{N}$  such that the finite product

$$\prod_{k=0}^n \frac{(k + \alpha_1) \cdots (k + \alpha_d)}{(k + \beta_1) \cdots (k + \beta_d)} \quad (3)$$

is equal to a given value  $t \in \mathbb{Q}$ . The link between this last problem and Proposition 1 arises from the fact that one can compute a bound  $n_0$  such that for all  $n > n_0$  the expression (3) is either strictly increasing or strictly decreasing as a function of  $n$ . As we observe below, this allows us to reduce the Membership Problem to a question about infinite products:

**Proposition 2.** *The Membership Problem for hypergeometric sequences with real parameters reduces to deciding, given  $d \geq 1$  and  $\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d \in \mathbb{R} \setminus \mathbb{Z}_{<0}$ , whether*

$$\Gamma(\beta_1) \cdots \Gamma(\beta_d) = \Gamma(\alpha_1) \cdots \Gamma(\alpha_d). \quad (4)$$

*Proof sketch.* We treat the case that the product (3) is eventually strictly increasing. The case that it is eventually strictly decreasing follows *mutatis mutandis*.

Write  $\omega$  for the limit (2) of the finite product (3) as  $n$  tends to  $\infty$ . By the assumption that (3) is eventually strictly increasing, we can compute  $n_0$  such that  $u_n < \omega$  for all  $n > n_0$ . If  $\omega \leq t$  then we have  $u_n \neq t$  for all  $n > n_0$ , and it remains to check by exhaustive search whether  $t \in \{u_0, \dots, u_{n_0}\}$ . On the other hand, if  $\omega > t$ , then we can find  $n_1 \geq n_0$  such that  $u_n > t$  for all  $n > n_1$ . Again, this leaves only a finite number of cases to check.

We thus need only decide whether or not  $\omega \leq t$ . But it is recursively enumerable whether  $\omega < t$  and whether  $\omega > t$ , simply by computing  $\omega$  to sufficient precision. Thus the Membership Problem for real parameters reduces to deciding whether  $\omega = t$ . Now note that  $\Gamma(t+1) = t\Gamma(t)$ , hence

$$\omega = t \Leftrightarrow \frac{\Gamma(\beta_1) \cdots \Gamma(\beta_d) \Gamma(t)}{\Gamma(\alpha_1) \cdots \Gamma(\alpha_d) \Gamma(t+1)} = 1.$$

But the equation above is an instance of (4) with two extra parameters,  $\alpha_{d+1} := t+1$  and  $\beta_{d+1} := t$ . This completes the reduction.  $\square$

Unfortunately, deciding whether (4) holds appears to be a difficult problem, and we take a different approach to solving the Membership Problem in the rest of this paper. Nevertheless (4) is still of interest for closely related problems, such as the *Positivity Problem* which asks, given a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  and target  $t$ , whether  $u_n \geq t$  holds for all  $n \in \mathbb{N}$ . In fact we have:

**Proposition 3.** *The Positivity Problem for hypergeometric sequences with real parameters is interreducible with the problem of deciding, given  $d \geq 1$  and  $\alpha_1, \dots, \alpha_d, \beta_1, \dots, \beta_d \in \mathbb{R} \setminus \mathbb{Z}_{<0}$ , whether (4) holds.*

Examining (4) in more detail, we note that the values of the Gamma function at rational points may be transcendental. Moreover, we are not aware of any lower bound on the difference between the two terms of (4) in case they are different, thus ruling out a numerical algorithm to decide equality. The following example from [5] illustrates a case where a quotient is an integer but in which none of the values of  $\Gamma$  involved are known to be algebraic:

$$\frac{\Gamma(\frac{1}{14})\Gamma(\frac{9}{14})\Gamma(\frac{11}{14})}{\Gamma(\frac{3}{14})\Gamma(\frac{5}{14})\Gamma(\frac{13}{14})} = 2.$$

A different approach is to study the algebraic relations among the values of the Gamma function. D. Rohrlich considered the question of giving a complete list of

all *multiplicative relations* among the values of the Gamma function *at rational points*. Recall that  $\Gamma$  satisfies the following three standard relations:

$$\begin{aligned} \Gamma(x+1) &= x\Gamma(x) && \text{(Translation),} \\ \Gamma(x)\Gamma(1-x) &= \frac{\pi}{\sin(\pi x)} && \text{(Reflection),} \\ \prod_{k=0}^{n-1} \Gamma\left(x + \frac{k}{n}\right) &= (2\pi)^{\frac{n-1}{2}} n^{\frac{1}{2}-nx} \Gamma(nx) && \text{(Multiplication)} \end{aligned} \quad (5)$$

for all  $x \in \mathbb{C}$  except at poles.

**Conjecture 4** (Rohrlich). *Any multiplicative relation of the form*

$$\pi^{b/2} \prod_{a \in \mathbb{Q}} \Gamma(a)^{m_a} \in \overline{\mathbb{Q}}$$

*with  $b$  and  $m_a$  in  $\mathbb{Z}$  is a consequence of the standard relations (5).*

This conjecture was formalised by Lang in terms of “universal distribution” [11]. This conjecture remains wide open and is part of the larger work on the transcendence of periods [18]. The closest result to our problem is a theorem by Koblitz and Ogus [10] giving a sufficient condition under which a quotient of values of Gamma is algebraic. A stronger conjecture, known as the Rohrlich-Lang conjecture deals more generally with polynomial relations. See [2, Section 24.6] for more details on these conjectures.

Note that Rohrlich’s conjecture is only concerned with rational parameters and, as far as we are aware, there is no analog of this conjecture for algebraic parameters. We now observe that if Rohrlich’s conjecture is true, then the Membership and Positivity Problems become decidable for rational parameters.

**Theorem 5.** *The Membership and Positivity Problems for hypergeometric sequences with rational parameters are decidable if Rohrlich’s conjecture is true.*

*Proof sketch.* By Propositions 2 and 3, the Membership and Positivity Problems both reduce to the question of deciding equations of the form (4), in which the parameters  $\alpha_i$  and  $\beta_i$  are rational. Assuming Rohrlich’s conjecture, the latter problem is recursively enumerable: if equality holds, then the equation has a finite derivation using the standard relations (5). On the other hand, the problem is also straightforwardly co-recursively enumerable: if Equation (4) does not hold, then by computing the left and right-hand sides to sufficient precision we will eventually conclude that the two terms are not equal.  $\square$

#### 4. THE MAIN RESULT

*The ring  $\mathbb{Z}_{(p)}$ .* Let  $p$  be a prime. We denote by  $v_p : \mathbb{Q} \rightarrow \mathbb{Z} \cup \{\infty\}$  the  $p$ -adic valuation on  $\mathbb{Q}$ . Recall that for a non-zero rational number  $x$ , the valuation  $v_p(x)$  is the unique integer such that  $x$  can be written in the form  $x = p^{v_p(x)} \frac{a}{b}$  with  $p \nmid ab$ . Following the standard convention, define  $v_p(0) := \infty$ .

We denote by  $\mathbb{Z}_{(p)}$  the ring  $\{x \in \mathbb{Q} : v_p(x) \geq 0\}$ . Alternatively, we have  $\mathbb{Z}_{(p)} = \{\frac{a}{b} : a, b \in \mathbb{Z}, p \nmid b\}$ . This is a local ring, whose unique maximal ideal is the principal ideal  $p\mathbb{Z}_{(p)}$ . The quotient  $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$  is isomorphic to the finite field  $\mathbb{F}_p$ . Specifically, we consider the quotient map  $\text{rem}_p : \mathbb{Z}_{(p)} \rightarrow \mathbb{F}_p$ , given by

$$\text{rem}_p\left(\frac{a}{b}\right) := ab^{-1} \bmod p.$$

Henceforth, when we say that  $\frac{a}{b} \in \mathbb{Z}_{(p)}$  has  $p$  as a prime divisor we refer to divisibility in  $\mathbb{Z}_{(p)}$ .

**4.1. Overview of the proof.** In the section we give a high-level overview of our main result.

As discussed in Section 2.1, to prove decidability of MP it remains to handle those instances in which the shift quotient  $r(x) \in \mathbb{Q}(x)$  converges to  $\pm 1$  as  $x \rightarrow \infty$ . In such instances,  $r(x)$  is necessarily the quotient of two polynomials of equal degree. Throughout this section, we fix such an instance of MP, consisting of a rational value  $t$  and a hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  with rational parameters and rational initial value  $u_0$ .

We aim at computing a bound  $N$  such that all indices of  $t$  in  $\langle u_n \rangle_{n=0}^\infty$  are at most  $N$ . Our strategy is to find  $N$  such that for all  $n > N$  there exists a prime  $p$  that is a prime divisor of  $u_n$  but not of  $t$ . To explain this idea in more detail, rewrite the shift quotient  $r(x)$  as

$$\frac{(x - \alpha_1) \cdots (x - \alpha_d)}{(x - \beta_1) \cdots (x - \beta_d)},$$

where the  $\alpha_i$  and the  $\beta_i$  are in  $\mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$ . We denote by  $A$  the multiset  $\{\alpha_1, \dots, \alpha_d\}$  consisting of all the (possibly repeated) roots of the numerator and by  $B$  the multiset  $\{\beta_1, \dots, \beta_d\}$  of the roots of the denominator. Denote by  $\text{Supp}(C)$  the underlying set of a multiset  $C$ . For each element  $x \in \text{Supp}(C)$  we write  $m_C(x)$  for its multiplicity in  $C$ . We write  $A \uplus B$  for the multiset with underlying set  $\text{Supp}(A) \cup \text{Supp}(B)$  where the multiplicity of each of its elements  $x$  is  $m_A(x) + m_B(x)$ .

Given a prime  $p$ , we have that

$$v_p(u_n) = v_p(u_0) + v_p\left(\prod_{k=1}^n r(k)\right)$$

for all  $n \in \mathbb{N}$ . In particular, if  $v_p(t) = v_p(u_0) = 0$  and

$$v_p\left(\prod_{k=1}^n r(k)\right) \neq 0,$$

then  $u_n \neq t$ . Furthermore the term  $v_p\left(\prod_{k=1}^n r(k)\right)$  can be expanded as

$$S_p(n) := \sum_{k=1}^n \left( \sum_{\alpha \in A} v_p(k - \alpha) - \sum_{\beta \in B} v_p(k - \beta) \right). \quad (6)$$

Thus, for all  $n \in \mathbb{N}$  and all primes  $p$  not dividing  $u_0$  or  $t$ , if  $S_p(n) \neq 0$  then  $u_n \neq t$ .

*The preorder  $\preceq_r$ .* Given an integer prime  $p$ , we define a preorder  $\preceq_p$  on  $\mathbb{Z}_{(p)}$  by writing  $\frac{a}{b} \preceq_p \frac{a'}{b'}$  if and only if  $\text{rem}_p(\frac{a}{b}) \leq \text{rem}_p(\frac{a'}{b'})$ , where  $\leq$  is the usual order on  $\{0, \dots, p-1\}$ .

Denote by  $b$  the least common denominator of all fractions in  $A \uplus B$ . For every prime  $p$  in the arithmetic progression  $b\mathbb{N} + 1$ , all elements of  $A \uplus B$  are in  $\mathbb{Z}_{(p)}$ . In Proposition 8 we show that for all sufficiently large primes  $p \in b\mathbb{N} + 1$  the orders  $\preceq_p$  restricted to  $A \uplus B$  are identical. We denote this common preorder by  $\preceq_r$ , where  $r$  is the shift quotient of our fixed sequence.

*Unbalanced intervals.* Given an integer prime  $p$ , let  $\frac{a}{b} \in \mathbb{Z}_{(p)}$  be such that  $\gcd(a, b) = 1$ . Note that  $v_p(b) = 0$ , and for all  $k \in \{1, \dots, p-1\}$  such that  $0 < |kb - a| < p^2$  we have

$$v_p\left(k - \frac{a}{b}\right) = \begin{cases} 1 & \text{if } \text{rem}_p(\frac{a}{b}) = \text{rem}_p(k), \\ 0 & \text{otherwise.} \end{cases} \quad (7)$$

Recall that  $A \uplus B \subseteq \mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$ , and assume that all its elements are given in a reduced form (i.e.,  $\gcd(a, b) = 1$  for all  $\frac{a}{b} \in A \uplus B$ ). Let  $p$  be a prime such

that all elements of  $A \uplus B$  are in  $\mathbb{Z}_{(p)}$ . Let  $n \in \{1, \dots, p-1\}$  be such that for all  $k \in \{1, \dots, n\}$ , for all  $\frac{a}{b} \in A \uplus B$ , the inequalities  $0 < |kb - a| < p^2$  hold. In this case, by Equation (7), the  $p$ -adic valuations in Equation (6) all take value 0 or 1. This means that  $S_p(n)$  is non-zero if and only if

$$|\{\alpha \in A : \alpha \preceq_p n\}| \neq |\{\beta \in B : \beta \preceq_p n\}|. \quad (8)$$

We say that  $n \in \mathbb{N}$  is  $p$ -unbalanced if  $S_p(n) \neq 0$ . We extend this notion to sub-intervals of  $\mathbb{N}$  by saying that an interval  $I \subseteq \mathbb{N}$  is  $p$ -unbalanced if all  $n \in I$  are  $p$ -unbalanced. By Equation (8), the maximal  $p$ -unbalanced sub-intervals of  $\{1, \dots, p-1\}$  will have endpoints that are equal or adjacent to the images  $\text{rem}_p(\frac{a}{b})$  of  $\frac{a}{b} \in A \uplus B$ ; see Example 1.

Let  $\gamma$  and  $\gamma'$  be distinct elements of  $A \uplus B$  such that  $\gamma \prec_r \gamma'$ . We denote by  $(\gamma, \gamma')$  the family of sub-intervals  $\{n \in \mathbb{N} : \text{rem}_p(\gamma) \leq n < \text{rem}_p(\gamma')\}$  of  $\mathbb{N}$  indexed by primes  $p \in b\mathbb{N} + 1$  whose respective orders agree with  $\prec_r$  (i.e., indexed by sufficiently large primes in  $b\mathbb{N} + 1$ ).

We show that for such a family of sub-intervals, indexed by primes  $p$ , either every interval is  $p$ -unbalanced or none of the intervals is  $p$ -unbalanced. In the former case we say that the family of intervals is  $r$ -unbalanced, where  $r$  is the shift quotient.

*Expanding families and contiguous intervals.* Assume that there exist  $\gamma, \gamma' \in A \uplus B$  such that  $\gamma - \gamma' \notin \mathbb{Z}$  and  $\gamma \prec_r \gamma'$ . In Proposition 9 we prove that the distance  $\text{rem}_p(\gamma') - \text{rem}_p(\gamma)$  between the respective residues of  $\gamma$  and  $\gamma'$  modulo a prime  $p$  is a strictly increasing function of  $p$ , for sufficiently large  $p$  belonging to the arithmetic progression  $b\mathbb{N} + 1$ . In this case we say that the family of intervals  $(\gamma, \gamma')$  is  $r$ -expanding.

The identification of expanding families of unbalanced intervals is a crucial element in our proof. We further show that:

**Proposition 6.** *Given  $r(x) \in \mathbb{Q}(x)$  converging to  $\pm 1$  as  $x \rightarrow \infty$ , either*

- (1) *there exists an  $r$ -expanding  $r$ -unbalanced family of intervals, or*
- (2) *otherwise, every hypergeometric sequence  $\langle u_n \rangle_{n=0}^\infty$  with shift quotient  $r(x)$  is a rational function of  $n$ .*

For the case when  $\langle u_n \rangle_{n=0}^\infty$  is a rational function of  $n$ , we can rewrite it as  $u_n = \frac{f(n)}{g(n)}$  with  $f, g \in \mathbb{Q}[x]$ . In order to test membership of  $t$ , it suffices to check whether the polynomial  $f(x) - tg(x)$  has an integer root. Henceforth, we assume without loss of generality that there exists an  $r$ -expanding  $r$ -unbalanced family of intervals for our fixed instance of MP.

Pick  $\gamma, \gamma' \in A \uplus B$  such that  $(\gamma, \gamma')$  is an  $r$ -expanding  $r$ -unbalanced family of intervals. Let  $p, q \in b\mathbb{N} + 1$  be primes sufficiently large that their respective orders agree with  $\prec_r$ . In Proposition 10 we show that if  $p < q < p(1 + \frac{1}{b}) + C$  with  $C$  a constant depending only on  $r$ , the respective intervals between  $\gamma$  and  $\gamma'$  for primes  $p$  and  $q$  are *contiguous*. That is, we show that  $\text{rem}_q(\gamma) \leq \text{rem}_p(\gamma')$  where  $\leq$  is the usual order on  $\mathbb{Z}$ . By previous arguments, for all  $n$  with  $\text{rem}_p(\gamma) \leq n < \text{rem}_q(\gamma')$  either  $v_p(u_n) = 0$  or  $v_q(u_n) = 0$ .

From the instance of MP we now construct an  $r$ -expanding  $r$ -unbalanced family of intervals that covers  $\{n \in \mathbb{N} : n > N\}$  for some effectively computable finite bound  $N$ . This will conclude our conceptually simple proof for decidability of MP.

*An infinite sequence of primes with contiguous unbalanced intervals.* We use effective bounds on the density of primes in arithmetic progressions to construct a sequence  $\langle p_i \rangle_{i=0}^\infty$  of primes with contiguous  $r$ -unbalanced intervals. Intuitively speaking, given a prime  $p_i \in b\mathbb{N} + 1$ , we would need  $p_{i+1} < p_i(1 + \frac{1}{b}) + C$  with  $C$  a fixed constant

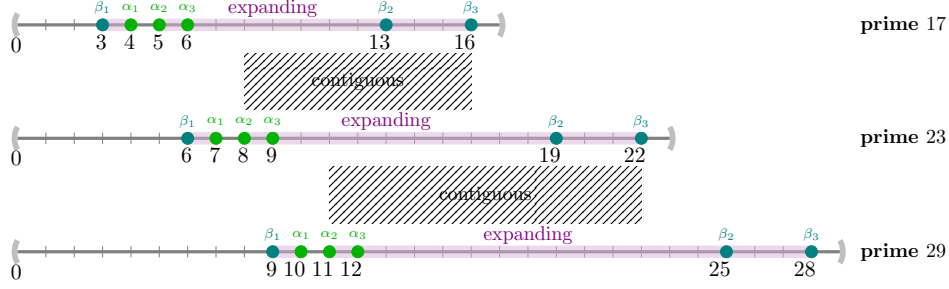


FIGURE 1. Consider the sequence  $\langle w_n \rangle_{n=0}^\infty$  given in Example 1. Observe that  $\beta_1 \preceq_p \alpha_1 \preceq_p \alpha_2 \preceq_p \alpha_3 \preceq_p \beta_2 \preceq_p \beta_3$  for all primes  $p \in \{17, 23, 29\}$ . The two families of intervals  $(\beta_1, \alpha_1)$  and  $(\alpha_2, \beta_3)$  are  $s$ -unbalanced, where only the latter is  $s$ -expanding. In particular, the distance between residues of  $\alpha_2$  and  $\beta_3$  modulo 23 is greater than their respective distance modulo 17. The same holds for their distance modulo 29 compared to their distance modulo 23. The  $s$ -expanding  $s$ -unbalanced intervals for 17, 23 and 29 are contiguous, which in turn ensures that for all  $n \in \{5, \dots, 27\}$  either 17 or 23 or 29 divides  $w_n$ . See Example 1 for a more detailed discussion.

depending on  $r$ . We prove that if  $p_i$  is large enough there always exists another prime  $p_{i+1} \in b\mathbb{N} + 1$  where  $p_{i+1} < p_i(1 + \frac{1}{b}) + C$ . See Proposition 12 for more details.

**Example 1.** Consider the sequence  $\langle w_n \rangle_{n=0}^\infty$  defined by  $w_0 = 1$  and the shift quotient

$$s(x) := \frac{(x + \frac{9}{2})(x + \frac{7}{2})(x + \frac{5}{2})}{(x + \frac{11}{2})(x + 4)(x + 1)}.$$

The rational function  $s(x)$  converges to 1 from above as  $x \rightarrow \infty$ . This implies that the sequence  $\langle w_n \rangle_{n=0}^\infty$  is monotonically increasing to its limit value, that is

$$\prod_{k=0}^{\infty} \frac{(k + \frac{9}{2})(k + \frac{7}{2})(k + \frac{5}{2})}{(k + \frac{11}{2})(k + 4)(k + 1)} = \frac{\Gamma(\frac{11}{2})\Gamma(4)\Gamma(1)}{\Gamma(\frac{9}{2})\Gamma(\frac{7}{2})\Gamma(\frac{5}{2})} = \frac{3 \cdot 2^5}{5\pi}.$$

We give two arguments that  $\frac{13}{6}$  does not lie in the sequence. First, using the fact  $\langle w_n \rangle_{n=0}^\infty$  is strictly increasing, it suffices to observe that  $w_6 > \frac{13}{6}$  and that none of  $w_0, \dots, w_5$  equals  $\frac{13}{6}$ . Such an argument is possible because  $w_n$  does not converge to  $\frac{13}{6}$ . Next, we prove the non-membership of  $\frac{13}{6}$  in the sequence using our approach based on prime divisors of the  $w_n$ . To this end, let

$$\begin{aligned} \alpha_1 &:= \frac{-9}{2} & \alpha_2 &:= \frac{-7}{2} & \alpha_3 &:= \frac{-5}{2} \\ \beta_1 &:= \frac{-11}{2} & \beta_2 &:= -4 & \beta_3 &:= -1 \end{aligned}$$

Considering that  $v_{13}(\frac{13}{6}) = 1$ , in our approach, we use larger primes to rule out the membership of  $\frac{13}{6}$ . For the prime 17, as depicted in Figure 1, we have that

$$\beta_1 \preceq_{17} \alpha_1 \preceq_{17} \alpha_2 \preceq_{17} \alpha_3 \preceq_{17} \beta_2 \preceq_{17} \beta_3.$$

The maximal 17-unbalanced intervals in our example are  $\{3\}$  and  $\{5, 6, \dots, 15\}$ . This implies that, for  $n \in \{1, \dots, 16\}$ ,  $S_{17}(n)$  is non-zero if and only if  $n$  belongs to  $\{3\} \cup \{5, \dots, 15\}$ .

As it turns out 17 is sufficiently large so that, for all primes  $p \geq 17$ , the respective order  $\prec_p$  agrees with  $\prec_s$ . Consequently, the families of intervals  $(\beta_1, \alpha_1)$  and  $(\alpha_2, \beta_3)$



are  $s$ -unbalanced. Furthermore, the family  $\overline{(\alpha_2, \beta_3)}$  is  $s$ -expanding, whereas  $\overline{(\beta_1, \alpha_1)}$  is not. As shown in Figure 1, the intervals between  $\alpha_2$  and  $\beta_3$  are contiguous for primes in  $\{17, 23, 29\}$ . This, in turn, ensures that for all  $n \in \{5, \dots, 27\}$  either 17, 23, or 29 divides  $w_n$ .

By the main theorem in [13], for all primes  $p \geq 8$ , there exists another prime less than  $p(1 + \frac{1}{2})$ . This, in combination with the above, guarantees that for all  $n \geq 5$ , there exists a prime  $p$  other than 13 appearing in the factorisation of  $w_n$ . This reduces the membership test of  $\frac{13}{6}$  to the finite set  $\{w_1, \dots, w_4\}$ .

**4.2. Technical Lemmas.** Recall that the elements in  $A \subseteq \mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$  are the roots of the numerator, and the elements in  $B \subseteq \mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$  are the roots of the denominator of the shift quotient  $r(x)$  of the fixed sequence  $\langle u_n \rangle_{n=0}^\infty$ .

Let  $b > 0$  be the least common denominator of the fractions in  $A \uplus B$ . Then every element  $\gamma \in A \uplus B$  admits a unique representation in the form  $\gamma = c - \frac{a}{b}$  under the conditions  $c \in \mathbb{Z}$  and  $a \in \{1, \dots, b\}$ . We call this the *canonical representation*. Associated with this, define a nonnegative integer

$$N_\gamma := \begin{cases} \max\left(c, \lceil \frac{bc}{b-a} \rceil\right) & \text{if } c \geq 1, \\ \max\left(-c, \lceil \frac{-bc}{a} \rceil\right) & \text{if } c \leq 0. \end{cases}$$

Note that  $N_\gamma$  is well-defined, i.e., there is no division by zero. Indeed, if  $c \geq 1$ , by the convention that  $\gamma \notin \mathbb{Z}_{\geq 0}$ , the value  $b - a$  is non-zero, whereas  $a \neq 0$  ensures well definedness in the second case.

**Proposition 7.** *Let  $\gamma = c - \frac{a}{b}$  be a canonical representation. Then for all primes  $p > N_\gamma$  such that  $p \in b\mathbb{N} + 1$  we have  $\text{rem}_p(\gamma) = c + \frac{(p-1)a}{b}$ .*

*Proof.* The assumption that  $p \in b\mathbb{N} + 1$  implies that  $\text{rem}_p(-\frac{1}{b}) = \frac{p-1}{b}$ . Thus, by the homomorphism property of  $\text{rem}_p$ , it only remains to verify that  $c + \frac{(p-1)a}{b} \in \{0, \dots, p-1\}$ . To this end, there are two cases, following the definition of  $N_\gamma$ .

The first case is that  $c \geq 1$ . Here we clearly have  $c + \frac{(p-1)a}{b} \geq 0$ . Furthermore, by the assumption  $p > N_\gamma$ , we have  $p-1 \geq \frac{bc}{b-a}$ . Recall also that  $a \neq b$  due to the assumption that  $\gamma \notin \mathbb{Z}_{\geq 0}$ . Thus, multiplying the previous inequality by  $b-a > 0$ , we have  $(b-a)(p-1) \geq bc$ . Dividing by  $b$  and rearranging terms, we conclude that  $c + \frac{(p-1)a}{b} \leq p-1$ .

The second case is that  $c \leq 0$ . Here, since  $a \leq b$ , it is clear that  $c + \frac{(p-1)a}{b} \leq p-1$ . Furthermore, by the assumption  $p > N_\gamma$ , we have  $p-1 \geq \frac{-bc}{a}$ . Multiplying the latter inequality by  $\frac{a}{b}$  and rearranging terms, we get  $c + \frac{(p-1)a}{b} \geq 0$ .  $\square$

Next we use Proposition 7 to show that, given distinct  $\gamma$  and  $\gamma'$  in  $A \uplus B$ , for all large enough primes  $p$  in the arithmetic progression  $b\mathbb{N} + 1$ , their order respective to  $\prec_p$  is fixed.

**Proposition 8.** *Let  $\gamma = c - \frac{a}{b}$  and  $\gamma' = c' - \frac{a'}{b}$  be canonical representations. For all primes  $p > b(N_\gamma + N_{\gamma'}) + 1$  such that  $p \in b\mathbb{N} + 1$  we have:*

$$\gamma \prec_p \gamma' \text{ if and only if } ((a < a') \text{ or } (a = a' \text{ and } c < c')).$$

*Proof.* For the first direction, assume that  $\gamma \prec_p \gamma'$ . Following Proposition 7, since  $p > N_\gamma + N_{\gamma'}$  and  $p \in b\mathbb{N} + 1$ , we can rewrite the assumption as  $c + \frac{(p-1)a}{b} < c' + \frac{(p-1)a'}{b}$ . We can rearrange the inequality to obtain

$$cb - c'b + a' - a < p(a' - a).$$

Towards a contradiction, assume that  $a > a'$ . In this case, the above yields  $\frac{c-c'}{a'-a}b + 1 > p$ . Since  $N_\gamma \geq |c|$  and  $N_{\gamma'} \geq |c'|$ , by the assumption that  $p >$

$b(N_\gamma + N_{\gamma'}) + 1$  we have that  $p > (c - c')b + 1 > \frac{c-c'}{a'-a}b + 1$ , a contradiction. Again, towards a contradiction, assume that  $a = a'$  but  $c \geq c'$ . Since  $b > 0$  we can multiply the inequality by  $b$  to get  $cb \geq c'b$ , a contradiction. The claim follows.

To show the other direction of the equivalence, we need to look at two cases depending on  $a$  and  $a'$ . First assume that  $a < a'$ . By  $p > b(N_\gamma + N_{\gamma'}) + 1$  we can write

$$p > (c - c')b + 1 \geq \frac{c - c'}{a' - a}b + 1 = \frac{cb - c'b + a' - a}{a' - a}.$$

Since  $a' - a > 0$ , we can multiply the above inequality by  $(a' - a)$  to obtain  $p(a' - a) > cb - c'b + a' - a$ . By rearranging the terms, we get  $(p - 1)a + cb < (p - 1)a' + c'b$ . As  $p > N_\gamma + N_{\gamma'}$  and  $p \in b\mathbb{N} + 1$  by Proposition 7, it follows that  $\gamma \prec_p \gamma'$ .

For the second case, assume  $a = a'$  and  $c < c'$ . Since  $b > 0$ , we can write  $cb < c'b$ . It follows that  $(p - 1)a + cb < (p - 1)a + c'b$ . Again, since  $p > N_\gamma + N_{\gamma'}$  and  $p \in b\mathbb{N} + 1$  by Proposition 7, it follows that  $\gamma \prec_p \gamma'$ .  $\square$

Associated to the shift quotient  $r(x)$  of the sequence  $\langle u_n \rangle_{n=0}^\infty$ , define the nonnegative integer

$$N_r := b \sum_{\gamma \in A \uplus B} N_\gamma + 1. \quad (9)$$

From Proposition 8 it follows that for all primes  $p > N_r$  in the arithmetic progression  $b\mathbb{N} + 1$

- $\text{rem}_p(\gamma), \text{rem}_p(\gamma')$  are distinct for all distinct  $\gamma, \gamma' \in A \uplus B$ ,
- the orders  $\preceq_p$  on  $A \uplus B$  are identical.

We henceforth denote by  $\preceq_r$  the common order on  $A \uplus B$  for all primes  $p > N_r$  in the arithmetic progression  $b\mathbb{N} + 1$ . Let  $\gamma, \gamma' \in A \uplus B$  be such that  $\gamma - \gamma' \notin \mathbb{Z}$ . In the following proposition we show that for larger and larger primes  $p \in b\mathbb{N} + 1$  whose orders agree with  $\preceq_r$ , the distance between  $\text{rem}_p(\gamma)$  and  $\text{rem}_p(\gamma')$  gets larger and larger:

**Proposition 9.** *Let  $p, q \in b\mathbb{N} + 1$  be primes with  $q > p > N_r$ . Let  $\gamma, \gamma' \in A \uplus B$  be such that  $\gamma - \gamma' \notin \mathbb{Z}$  and  $\gamma \prec_r \gamma'$ . Then*

$$\text{rem}_p(\gamma') - \text{rem}_p(\gamma) < \text{rem}_q(\gamma') - \text{rem}_q(\gamma)$$

where  $<$  is the total order on  $\mathbb{Z}$ .

*Proof.* Since  $p < q$  and  $b > 0$ , we can write  $\frac{p-1}{b} < \frac{q-1}{b}$ . Given the canonical representations  $\gamma = c - \frac{a}{b}$  and  $\gamma' = c' - \frac{a'}{b}$ , note that since  $\gamma - \gamma' \notin \mathbb{Z}$ , we have  $a \neq a'$ . Now since  $\gamma \prec_r \gamma'$ , by Proposition 8 we have  $a < a'$ . We can thus multiply the above inequality by  $(a' - a)$  to obtain

$$\frac{p-1}{b}(a' - a) < \frac{q-1}{b}(a' - a).$$

Now by adding  $(c' - c)$  on both sides of the above inequality we get

$$c' + \frac{p-1}{b}a' - \left(c + \frac{p-1}{b}a\right) < c' + \frac{q-1}{b}a' - \left(c + \frac{q-1}{b}a\right).$$

By the assumption that  $p, q \in b\mathbb{N} + 1$  with  $p, q > N_r$ , we can use Proposition 7 to conclude that

$$\text{rem}_p(\gamma') - \text{rem}_p(\gamma) < \text{rem}_q(\gamma') - \text{rem}_q(\gamma).$$

$\square$

Let  $\gamma, \gamma' \in A \uplus B$  be such that  $\overline{(\gamma, \gamma')}$  is an  $r$ -expanding  $r$ -unbalanced family of intervals. For a prime  $p \in b\mathbb{N} + 1$  with  $p > N_r$ , we obtain a condition on larger primes  $q \in b\mathbb{N} + 1$  that ensures the intervals  $\{n \in \mathbb{N} : \text{rem}_p(\gamma) \leq n < \text{rem}_p(\gamma')\}$  and  $\{n \in \mathbb{N} : \text{rem}_q(\gamma) \leq n < \text{rem}_q(\gamma')\}$  are contiguous.

**Proposition 10.** *Let  $p, q \in b\mathbb{N} + 1$  be primes with  $q > p > N_r$ . Let  $\gamma, \gamma' \in A + B$  such that  $\gamma - \gamma' \notin \mathbb{Z}$  and  $\gamma \prec_r \gamma'$ . We have  $\text{rem}_q(\gamma) < \text{rem}_p(\gamma')$  if*

$$q < p + \frac{p-1}{b} + C$$

for some effective constant  $C$  depending on  $\gamma$  and  $\gamma'$ .

*Proof.* Given the canonical representations  $\gamma = c - \frac{a}{b}$  and  $\gamma' = c' - \frac{a'}{b}$ , write  $C := \frac{c'-c}{a}b$ . Then the initial assumption can be rewritten as

$$q < p + \frac{p-1}{b} + \frac{c'-c}{a}b.$$

We can further rewrite the above inequality as

$$q-1 < (p-1)\left(1 + \frac{1}{b}\right) + \frac{c'-c}{a}b.$$

Note that since  $\gamma - \gamma' \notin \mathbb{Z}$ , we have  $a \neq a'$ . Now by Proposition 8, from  $\gamma \prec_r \gamma'$  it follows that  $a < a'$ . By further recalling that  $a < a' \leq b$ , we have  $\frac{a'}{a} = \left(1 + \frac{a'-a}{a}\right) \geq \left(1 + \frac{1}{b}\right)$ . Then from the above it follows that

$$q-1 < (p-1)\frac{a'}{a} + \frac{c'-c}{a}b.$$

Since  $\frac{a}{b} > 0$ , we can multiply the inequality by  $\frac{a}{b}$  to obtain

$$\frac{(q-1)a}{b} + c < \frac{(p-1)a'}{b} + c'.$$

By the assumption that  $p, q \in b\mathbb{N} + 1$  with  $p, q > N_r$ , we can now use Proposition 7 to conclude that  $\text{rem}_q(\gamma) < \text{rem}_p(\gamma')$ .  $\square$

**4.3. The Main Theorem.** In order to prove our main theorem, we first need a preliminary result on the number of primes in an interval in an arithmetic progression. To this end, we rely on effective bounds on the density of primes in an arithmetic progression.

Given coprime numbers  $a, n \in \mathbb{N}$  with  $a < n$ , write  $\pi_{n,a}(x)$  for the number of primes less than  $x$  that are congruent to  $a$  modulo  $n$ . The following estimates on  $\pi_{n,a}(x)$  can be found in [4, Theorem 1.3].

**Theorem 11.** *Given  $n \geq 3$  and  $a \in \mathbb{N}$  coprime to  $n$ , there exist explicit positive constants  $c$  and  $x_0$  depending on  $n$  such that*

$$\left| \pi_{n,a}(x) - \frac{Li(x)}{\varphi(n)} \right| < c \frac{x}{(\log x)^2} \text{ for all } x > x_0.$$

Note that in the above theorem  $Li(x)$  denotes the *offset logarithmic integral function*, which is defined as

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Asymptotically, the above function behaves as the prime number counting function  $\pi(x)$ , that is, as  $O\left(\frac{x}{\log x}\right)$ .

**Proposition 12.** *Let  $b \in \mathbb{N}$  and  $C \in \mathbb{Z}$ . There exist an effectively computable bound  $M \in \mathbb{N}$  such that for all primes  $p \in b\mathbb{N} + 1$  greater than  $M$ , there exists a prime  $q \in b\mathbb{N} + 1$  with  $p < q < p + \frac{p-1}{b} + C$ .*

*Proof.* Let  $x \in b\mathbb{N} + 1$ , and denote by  $y = x(1 + \frac{1}{b})$ . We would like to show that there exists a bound  $M \in \mathbb{N}$  such that  $\pi_{b,1}(y) - \pi_{b,1}(x) > 0$  for all  $x > M$ . Using Theorem 11 to estimate  $\pi_{b,1}(y)$  and  $\pi_{b,1}(x)$ , it suffices to show that:

$$\frac{Li(y)}{\varphi(b)} - c \frac{y}{(\log y)^2} > \frac{Li(x)}{\varphi(b)} + c' \frac{x}{(\log x)^2}$$

The above then simplifies to:

$$\frac{Li(y) - Li(x)}{\varphi(b)} > 2c \frac{y}{(\log y)^2} \quad (10)$$

Now write  $y = x(1 + \epsilon)$  with  $\epsilon = \frac{1}{b}$ , and observe that

$$Li(y) - Li(x) = \int_x^y \frac{dt}{\log t} = \frac{y}{\log y} - \frac{x}{\log x} \sim \frac{\epsilon x}{\log x}$$

where  $\sim$  denotes asymptotic equivalence. As for the right hand side of (10), note that

$$\frac{y}{(\log y)^2} \sim \frac{x}{(\log x)^2}.$$

It remains to note that  $\frac{x}{\log x} \gg \frac{x}{(\log x)^2}$ .  $\square$

The above proposition ensures that we can construct an infinite sequence of primes  $\langle p_i \rangle_{i=0}^\infty$  in  $b\mathbb{N} + 1$  such that for all  $p_i$  its successor  $p_{i+1}$  is between  $p_i$  and  $p_i + \frac{p_i-1}{b}$ . Proposition 10 then implies that if we choose  $p_0 > \max(M, N_r)$ , for every  $\gamma, \gamma' \in A \uplus B$  such that  $(\gamma, \gamma')$  is an  $r$ -expanding  $r$ -unbalanced family of intervals, for all  $i$ , the intervals  $\{n \in \mathbb{N} : \text{rem}_{p_i}(\gamma) \leq n < \text{rem}_{p_i}(\gamma')\}$  and  $\{n \in \mathbb{N} : \text{rem}_{p_{i+1}}(\gamma) \leq n < \text{rem}_{p_{i+1}}(\gamma')\}$  are contiguous.

The sequence  $\langle p_i \rangle_{i=0}^\infty$  is the last part of our construction, allowing us to prove our main result:

**Theorem 13.** *The membership problem for hypergeometric sequences with rational parameters is decidable.*

*Proof.* As discussed in Section 2.1, the only case of MP that is not trivially decidable is when the shift quotient  $r(x) \in \mathbb{Q}(x)$  of the sequence  $\langle u_n \rangle_{n=0}^\infty$  converges to  $\pm 1$  as  $x \rightarrow \infty$ . Given such an instance of MP, we write  $r(x)$  as

$$\frac{(x - \alpha_1) \cdots (x - \alpha_d)}{(x - \beta_1) \cdots (x - \beta_d)}.$$

We denote by  $A$  the multiset  $\{\alpha_1, \dots, \alpha_d\}$  consisting of all the (possibly repeated) roots of the numerator and by  $B$  the multiset  $\{\beta_1, \dots, \beta_d\}$  of the roots of the denominator. As discussed in Section 2, all elements in  $A \uplus B$  are in  $\mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$ .

We now show that there exists a bound  $N \in \mathbb{N}$  such that for all  $n > N$ , there exists a prime  $p$  appearing in the factorisation of  $u_n$  but not in the factorisation of  $u_0$  or that of  $t$ . This implies that it suffices to check whether  $u_n = t$  for all  $n \in \{1, \dots, N\}$  to decide MP. In particular, we show that for all  $n > N$ , we can find a prime  $p$  with  $v_p(t) = v_p(u_0) = 0$  such that  $S_p(n)$ , as defined in Equation (6), is non-zero.

Write  $u_0 = \frac{v}{v'}$  and  $t = \frac{w}{w'}$ . Now define

$$N' = \max(|v|, |v'|, |w|, |w'|, N_r)$$

where  $N_r$  is defined as in Equation (9). Note that none of the primes  $p > N'$  divide the target  $t$  nor the initial value  $u_0$ .

Following Proposition 6, we can assume without loss of generality that there exists an  $r$ -expanding  $r$ -unbalanced family of intervals  $(\gamma, \gamma')$  for some  $\gamma, \gamma' \in A \uplus B$ . Let  $M$  be the bound computed in Proposition 12. Let  $p_0 \in b\mathbb{N} + 1$  be a prime with  $p_0 > \max(M, N')$ . Observe that for all  $n$  in

$$\{k \in \mathbb{N} : \text{rem}_{p_0}(\gamma) \leq k < \text{rem}_{p_0}(\gamma')\},$$

the sum  $S_{p_0}(n)$  defined in Equation (6) is indeed non-zero.

Following Proposition 12, we can construct an infinite sequence of primes  $\langle p_i \rangle_{i=0}^{\infty}$  with initial element  $p_0$  such that for every prime  $p_i$  in the sequence, its successor  $p_{i+1}$  is between  $p_i$  and  $p_i + \frac{p_i-1}{b}$  in the arithmetic progression  $b\mathbb{N} + 1$ . By Proposition 10, for all  $i$ , the intervals  $\{k \in \mathbb{N} : \text{rem}_{p_i}(\gamma) \leq k < \text{rem}_{p_i}(\gamma')\}$  and  $\{k \in \mathbb{N} : \text{rem}_{p_{i+1}}(\gamma) \leq k < \text{rem}_{p_{i+1}}(\gamma')\}$  are contiguous. Therefore we can cover all  $n > \text{rem}_{p_0}(\gamma)$ , which concludes our proof.  $\square$

## 5. DISCUSSION

Our main result shows decidability of the Membership Problem for hypergeometric sequences, where the coefficient polynomials have rational roots. In extending our results to the general case, that is when the coefficient polynomials have algebraic roots, it appears that the difficulty is when the splitting fields of the coefficient polynomials are identical. Otherwise, there exists a prime  $p$  such that one of polynomials splits over  $\mathbb{Q}_p$  but the other does not. Such a prime can be used to deduce an upper bound on the largest index of the target value.

## REFERENCES

- [1] T. Amdeberhan, L. Medina, and V. Moll. Asymptotic valuations of sequences satisfying first order recurrences. *Proceedings of the American Mathematical Society*, 137:885–890, 10 2007.
- [2] Y. André. *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, volume 17 of *Panoramas et Synthèses*. Société Mathématique de France, 2004.
- [3] J. Bell, S. Burris, and K. Yeats. **On the set of zero coefficients of a function satisfying a linear differential equation**. *Mathematical Proceedings of the Cambridge Philosophical Society*, 153:235–247, 05 2011.
- [4] M. A. Bennett, G. Martin, K. O’Byrant, and A. Rechnitzer. Explicit bounds for primes in arithmetic progressions. *Illinois Journal of Mathematics*, 62(1-4):427 – 532, 2018.
- [5] M. Chamberland and A. Straub. On gamma quotients and infinite products. *Advances in Applied Mathematics*, 51(5):546–562, 2013.
- [6] E. Delaygue, T. Rivoal, and J. Roques. On dwork’s p-adic formal congruences theorem and hypergeometric mirror maps. *Memoirs of the American Mathematical Society*, 246, 09 2013.
- [7] M. Kauers and P. Paule. *The Concrete Tetrahedron - Symbolic Sums, Recurrence Equations, Generating Functions, Asymptotic Estimates*. Texts & Monographs in Symbolic Computation. Springer, 2011.
- [8] M. Kauers and V. Pillwein. When can we detect that a p-finite sequence is positive? In Wolfram Koepf, editor, *Symbolic and Algebraic Computation, International Symposium, ISSAC, Proceedings*, pages 195–201. ACM, 2010.
- [9] G. Kenison, O. Klurman, E. Lefauchaux, F. Luca, P. Moree, J. Ouaknine, M. A. Whiteland, and J. Worrell. On positivity and minimality for second-order holonomic sequences. In *46th International Symposium on Mathematical Foundations of Computer Science, MFCS*, volume 202 of *LIPIcs*, pages 67:1–67:15. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
- [10] N. Koblitz and A. Ogus. Algebraicity of some products of values of the f function, appendix of valeurs de fonctions l et périodes d’intégrales. *Proceedings of Symposia in Pure Mathematics*, 33:part 2, 313–346, 1979.
- [11] S. Lang. Relations de distributions et exemples classiques. *Séminaire Delange-Pisot-Poitou. Théorie des nombres*, 19(2), 1977-1978.
- [12] M. Mignotte, T. N. Shorey, and R. Tijdeman. The distance between terms of an algebraic recurrence sequence. *Journal für die reine und angewandte Mathematik*, 349, 1984.
- [13] J. Nagura. On the interval containing at least one prime number. *Proceedings of the Japan Academy*, 28(4):177–181, 1952.
- [14] E. Neumann, J. Ouaknine, and J. Worrell. Decision problems for second-order holonomic recurrences. In *48th International Colloquium on Automata, Languages, and Programming, ICALP*, volume 198 of *LIPIcs*, pages 99:1–99:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021.
- [15] M. Petkovsek, H. Wilf, and D. Zeilberger. *A = B*. A K Peters, 1997.
- [16] V. Pillwein and M. Schussler. An efficient procedure deciding positivity for a class of holonomic functions. *ACM Commun. Comput. Algebra*, 49(3):90–93, 2015.

- [17] N. K. Vereshchagin. The problem of appearance of a zero in a linear recurrence sequence (in Russian). *Mat. Zametki*, 38(2), 1985.
- [18] M. Waldschmidt. Transcendence of periods: the state of the art. *Pure and Applied Mathematics Quarterly*, 2(2):435–463, 2006.

#### APPENDIX A. MEMBERSHIP OF ZERO AND ASSUMPTION ON $q(x)$

In our MP instances, we will assume that the numerator  $q(x)$  of the shift quotient has no non-negative integer zeros and  $t \neq 0$ . This assumption on  $q(x)$  is without loss of generality as otherwise, the sequence  $\langle u_n \rangle_{n=0}^{\infty}$  will be ultimately always zero. Indeed, if  $q(x)$  has non-negative integer zeros,  $u_n = 0$  for all  $n \geq m$  where  $m$  is the smallest non-negative integer root of  $q(x)$ . Consequently, the search domain for indices of  $t$  in MP will be limited to the finite set  $\{u_0, \dots, u_m\}$ . This assumption on  $q(x)$  will exclude the membership of zero in the sequence  $\langle u_n \rangle_{n=0}^{\infty}$ , and will allow us to further assume that  $t \neq 0$ .

#### APPENDIX B. PROOF OF PROPOSITION 6

Recall we can write the shift quotient  $r(x)$  as

$$\frac{(x - \alpha_1) \cdots (x - \alpha_d)}{(x - \beta_1) \cdots (x - \beta_d)}$$

where the  $\alpha_i$  and the  $\beta_i$  are in  $\mathbb{Q} \setminus \mathbb{Z}_{\geq 0}$ . We denote by  $A$  the multiset  $\{\alpha_1, \dots, \alpha_d\}$  consisting of all the (possibly repeated) roots of the numerator and by  $B$  the multiset  $\{\beta_1, \dots, \beta_d\}$  of the roots of the denominator.

Our proof relies on the following observation: if there exists a bijective function  $f : A \rightarrow B$  such that for all  $\alpha \in A$  we have  $\alpha - f(\alpha) \in \mathbb{Z}$ , then Item 2 holds. Otherwise, Item 1 holds.

Towards Item 2, assume that there exists a bijective function  $f : A \rightarrow B$  such that for all  $\alpha \in A$  we have  $\alpha - f(\alpha) \in \mathbb{Z}$ . Given an enumeration  $\alpha_1, \dots, \alpha_d$  on  $A$ , enumerate the elements of  $B$  so that  $f(\alpha_i) = \beta_i$ . Then given a pair  $\alpha_i, \beta_i$ , write  $\ell_i = |\alpha_i - \beta_i| \in \mathbb{N}$ .

Recall that given an instance of MP with a target value  $t \in \mathbb{Q}$  and initial value  $u_0 \in \mathbb{Q}$ , the problem asks to decide whether there exists  $n \in \mathbb{N}$  such that

$$u_0 \prod_{k=1}^n r(k) = t. \tag{11}$$

Observe that we can expand a part of the above product in the following way:

$$\begin{aligned} \prod_{k=1}^n r(k) &= \prod_{k=1}^n \frac{(k - \alpha_1) \cdots (k - \alpha_d)}{(k - \beta_1) \cdots (k - \beta_d)} \\ &= \prod_{k=1}^n \frac{(k - \alpha_1)}{(k - \beta_1)} \cdots \prod_{k=1}^n \frac{(k - \alpha_d)}{(k - \beta_d)} \end{aligned}$$

Now if we look at the product  $\prod_{k=1}^n \frac{(k - \alpha_i)}{(k - \beta_i)}$ . If  $\beta_i > \alpha_i$ , observe that we can write

$$\frac{k - \alpha_i}{k - \beta_i} = \frac{k + (\beta_i - \alpha_i) - \beta_i}{k - \beta_i} = \frac{k + \ell_i - \beta_i}{k - \beta_i}.$$

We can thus write:

$$\begin{aligned}
& \prod_{k=1}^n \frac{(k - \alpha_i)}{(k - \beta_i)} \\
&= \prod_{k=1}^n \frac{(k + \ell_i - \beta_i)}{(k - \beta_i)} \\
&= \frac{(1 + \ell_i - \beta_i)}{(1 - \beta_i)} \cdots \frac{((\ell_i + 1) + \ell_i - \beta_i)}{((\ell_i + 1) - \beta_i)} \cdots \frac{(n + \ell_i - \beta_i)}{(n - \beta_i)} \\
&= \frac{(1 + \ell_i - \beta_i)}{(1 - \beta_i)} \cdots \frac{((\ell_i + 1) + \ell_i - \beta_i)}{(\ell_i + 1 - \beta_i)} \cdots \frac{(n + \ell_i - \beta_i)}{(n - \beta_i)}
\end{aligned}$$

Note how in the last line above, we were able to simplify at least two terms. Observe that we will be able to do so for all but  $\ell_i$  terms in the numerator and all but  $\ell_i$  terms in the denominator. That is, we transform:

$$\prod_{k=1}^n \frac{(k - \alpha_i)}{(k - \beta_i)} = \frac{(n + 1 - \beta_i) \cdots (n + \ell_i - \beta_i)}{(1 - \beta_i) \cdots (\ell_i - \beta_i)} = \frac{f_i(n)}{g_i(n)}$$

for  $n > \ell_i$ .

Similarly, observe that if  $\alpha_i > \beta_i$ , we can write

$$\frac{k - \alpha_i}{k - \beta_i} = \frac{k - \alpha_i}{k + (\alpha_i - \beta_i) - \alpha_i} = \frac{k - \alpha_i}{k + \ell_i - \alpha_i}$$

By repeating the above computation, we obtain:

$$\prod_{k=1}^n \frac{(k - \alpha_i)}{(k - \beta_i)} = \frac{(1 - \alpha_i) \cdots (d_i - \alpha_i)}{(n + 1 - \alpha_i) \cdots (n + \ell_k - \alpha_i)} = \frac{f_i(n)}{g_i(n)}$$

for  $n > \ell_i$ .

By applying the above transformation to all pairs  $\alpha_i, \beta_i$  with their respective distance  $\ell_i$ , we can rewrite  $\prod_{k=1}^n r(k)$  as:

$$\prod_{k=1}^n r(k) = \frac{f_1(n)}{g_1(n)} \cdots \frac{f_d(n)}{g_d(n)} = \frac{\hat{f}(n)}{\hat{g}(n)}$$

The above is well-defined for all  $n > \max(\ell_1, \dots, \ell_d)$ , and implies that the product  $\prod_{k=1}^n r(k)$  can be decomposed as a product of a constant number of rational functions in  $n$ .

To show Item 1, assume that there is no bijective function  $f : A \rightarrow B$  such that for all  $\alpha \in A$  we have  $\alpha - f(\alpha) \in \mathbb{Z}$ . Let  $\gamma_1, \dots, \gamma_{2d}$  be a fixed permutation of the elements of  $A \uplus B$ , such that  $\gamma_j \preceq_r \gamma_k$  for all  $1 \leq j < k \leq 2d$ .

We claim that there exists an index  $j$  such that  $(\gamma_j, \gamma_{j+1})$  is an  $r$ -expanding  $r$ -unbalanced family of intervals. That is,  $j$  such that

- $\gamma_j - \gamma_{j+1} \notin \mathbb{Z}$ , and
- the number of  $\alpha_i$  in the block  $\gamma_1 \preceq_r \dots \preceq_r \gamma_j$  is not equal to the number of  $\beta_i$  in the block  $\gamma_1 \preceq_r \dots \preceq_r \gamma_{j+1}$ .

Indeed, if there is no such  $j$ , then we can take each block of the  $\alpha_i$  and  $\beta_i$  with integer distances and construct a bijection mapping from the set of  $\alpha_i$ 's to the set of  $\beta_i$ 's appearing in the block alone. Putting together the mappings given by the block bijections gives us a bijection  $f : A \rightarrow B$  such that  $\alpha_i - f(\alpha_i) \in \mathbb{Z}$  for all  $i$ , which would lead to a contradiction.