Electronic Colloquium on Computational Complexity - Reports Series 1997 - available via:
ECCC
TR97-055
FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

A Decision Method for the Rational Sequence Problem

B. Litow [§]

September 22, 1997

Running Title: Rational Sequence Problem Decidability

Abstract

We give an algorithm to decide whether or not a linear recurrence of finite order with rational coefficients and initial values produces 0. We also show that this problem is PSPACE hard, and that m-variate versions are not computable for very small values of m.

AMS Keywords: 03D35, 05A15,05A16

1 Introduction

A linear recurrence of finite order with constant rational coefficients and initial values is one of the most basic elements of combinatorics. Linear recurrences also turn up in many areas of engineering. It is natural to ask about the distribution of values produced by a linear recurrence. For example, it is a classical result that the magnitude of the n-th term is bounded by α^n, for some $\alpha > 0$, and that α can be computed from the recurrence data. However, even more slightly exacting questions seem to be very hard. In particular, one can ask whether or not a recurrence ever produces 0. This is the *rational sequence problem* and it is posed as an open problem in [13]. We will present an algorithm for the rational sequence problem. We also discuss extensions of the problem which are not computable.

Issues related to computability of expressions involving algebraic numbers are briefly discussed in an appendix. We will not go into much more detail about these issues, except to say that all the explicit questions about algebraic numbers raised in this paper can be formulated as sentences in the first order theory of real number arithmetic. Collins [4] was the first to give a decision method for this theory, and a subsequent refinement was introduced in [1].

2 Rational sequences and series

The rational sequence problem will be cast in terms of rational series. $\mathbb{N}$ is the semiring of non-negative integers. $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}$ are the complex, real and rational fields, respectively.

[§]Dept. of Computer Science, University of Central Florida, Orlando, FL 32816-2362, bruce@cs.jcu.edu.au

$\mathbb{K}[[x]]$ is the set of formal power series in x with coefficients in a field $\mathbb{K}$, and $\mathbb{K}[x]$ is the subset of polynomials. $[x^n]f$ is the coefficient of x^n in f. We will write $f(a)$ to indicate the value of $f \in \mathbb{K}[[x]]$ at $x = a \in \mathbb{K}$. Let $p, q \in \mathbb{K}[x]$, such that $q(0) = 1$. If $f \in \mathbb{K}[[x]]$ can be formally identified (term-by-term) with the expansion of

$$p \cdot (1 + (1 - q) + (1 - q)^2 + \cdots)$$

then f is said to be a $\mathbb{K}$-*rational series*. We will write $f = p/q$ for this. We will drop explicit mention of the field when it is $\mathbb{Q}$. The concepts of formal series and rational series can be greatly generalized [13, 9]. It is classical that $\mathbb{K}$-rational series are precisely the generating series of sequences produced by linear recurrences of finite order whose coefficients and initial values are in $\mathbb{K}$. A full treatment for $\mathbb{Q}$ is given in [7]. Determining whether or not such a linear recurrence generates 0 as a term is called the $\mathbb{K}$-*rational sequence problem* ($\mathbb{K}$-RSP). It is clear that $\mathbb{K}$-RSP is equivalent to determining for a given $\mathbb{K}$-rational series f whether or not there exists $n \in \mathbb{N}$ such that $[x^n]f = 0$. The computability status of $\mathbb{K}$-RSP has been open until now. The main result of this paper settles this status for the field $\mathbb{Q}$.

Theorem 1 *RSP is computable.*

We also prove two negative results.

Theorem 2 *RSP is PSPACE hard.*

Theorem 3 *If m is the smallest number of variables such that the m-variate Diophantine decision problem (Hilbert's 10th problem) is non-computable, then RSP for rational series in m commuting variables is non-computable.*

It is interesting to note that Berstel and Mignotte were able to prove [3]

Theorem 4 *It is computable to determine for a rational series f whether or not infinitely many of its coefficients are* 0.

We mention that this result is closely connected to the Skolem-Mahler-Lech theorem.

Theorem 5 (Skolem-Mahler-Lech) *Let $\mathbb{K}$ be any field of characteristic* 0 *and let $f \in \mathbb{K}[[x]]$. Define $I_f(0) = \{n \mid [x^n]f = 0\}$. If f is $\mathbb{K}$-rational, then $I_f(0)$ can be expressed as the union of a finite number of arithmetic progressions.*

It is clear that $I_f(0)$ can be replaced in the theorem by $I_f(a)$, where $a \in \mathbb{K}$, since if f is $\mathbb{K}$-rational, then so is $f - \frac{a}{1-x}$.

The assumption that $\mathbb{K}$ has characteristic 0 is essential. A counterexample to the assertion of the theorem in non-zero characteristic is given in [5]. Finally, we point out that a refinement of Thm. 5 has been given by [8]. We use the usual term *semilinear set* for a subset of $\mathbb{N}$ that can be expressed a finite union of arithmetic progressions. Note that the

collection of semilinear sets is closed under the Boolean operations.

We recall the definition of the *Hadamard product* $h = f \circ g$ of formal series f and g. h is defined by $[x^n]h = [x^n]f \cdot [x^n]g$. Note that the Hadamard product is commutative, provided the coefficient domain is commutative. Note also that $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n$ is the Hadamard product identity. It is clear that RSP is equivalent to determining for rational f whether or not there is a series g such that $f \circ g = \sum_{n=0}^{\infty} x^n$. In this situation, f and g are said to be *Hadamard inverses* of one another. It is easy to check that

$$\frac{1}{(1-x)^2} \circ \frac{\ln(1-x)}{x} = \frac{1}{1-x}$$

which shows that a rational series can have a transcendental series as its Hadamard inverse. Benzaghou has characterized those rational series having rational Hadamard inverses [2].

In the case of rational series in $\mathbb{C}[[x]]$ it is possible to make a modest extension of Thm. 5.

Theorem 6 *If f is a $\mathbb{C}$-rational series, then for any $\rho \geq 0$, the set $\{n \mid |[x^n]f| = \rho\}$ is semilinear.*

Proof : For any series $f \in \mathbb{C}[[x]]$, define $\bar{f} = \sum_{n=0}^{\infty} \overline{[x^n]f} x^n$, where $\bar{a}$ is the complex conjugate of $a \in \mathbb{C}$. It is clear that if f is rational, then $\bar{f}$ is rational. It is known that the Hadamard product of $\mathbb{K}$-rational series is again $\mathbb{K}$-rational. See Thm. 4.4 [13]. Hence, if f is $\mathbb{C}$-rational, then $f \circ \bar{f}$ is also $\mathbb{C}$-rational. The theorem now follows from Thm. 5 by noting that

$$\{n \mid |[x^n]f| = \rho\} = \{n \mid [x^n](f \circ \bar{f}) = \rho^2\}$$

□

If $A \subseteq \mathbb{N}$, then define f_A to be the series $f_A = \sum_{n \in A} x^n$. If g is any series, then g *combed by* A is the series h given by

$$h = \sum_{n \in A} [x^n]g \cdot x^n$$

This is equivalent to

$$h = g \circ f_A \tag{1}$$

The following result is a special case of Thm.4.4 in [13].

Lemma 1 *Given rational series f and g, polynomials p and q can be computed such that $f \circ g = p/q$.*

Corollary 1 *If A is a given semilinear set, and g is a given rational series, then g combed by A is a computable rational series.*

Proof : It is clear that f_A is a rational series for any semilinear set A. The result now follows from Eq. 1 and Lem. 1. □

3 Technical results

We collect four technical lemmas that form the basis for the decision method. Throughout, 'root of unity' will mean complex root of unity.

Lemma 2 *Given roots of unity $\omega_1, \ldots, \omega_s$, and $g_1, \ldots, g_s \in \mathbb{C}[x]$, define A to be the set of $n \in \mathbb{N}$ such that*

$$S(n) = \sum_{i=1}^{s} g_i(n)\omega_i^n = 0$$

then A is a computable semilinear set.

Proof : It is evident that over all $n \in \mathbb{N}$, there are only finitely many distinct s-tuples $(\omega_1^n, \ldots, \omega_s^n)$. For each such s-tuple, $(a_1, \ldots, a_s)$ it is also evident that the set of n for which $(\omega_1^n, \ldots, \omega_s^n) = (a_1, \ldots, a_s)$ is a semilinear set. Call these semilinear sets *level sets.*

Fix $d \in \mathbb{N}$ and consider the sum

$$S_{d,n} = \sum_{i=1}^{s} [x^d] g_i \omega_i^n$$

Now, $S_{d,n}$ is a computable constant $c_d \in \mathbb{C}$ for n in a level set. Thus, for n in a level set

$$S(n) = \sum_{d=0}^{D} c_d \cdot n^d$$

where D is the maximum degree of any g_i. Over each level set $S \in \mathbb{C}[x]$ is computable, so if $S \neq 0$, then an upper bound on the modulus of any of its zeros is computable. This implies that either there is a computable upper bound on n in a level set such that $S(n)$ can vanish, or $S(n) = 0$ over the level set. If there is an upper bound, then we can exhaustively test whether or not $S(n) = 0$ for each n in the level set up to this bound. Since there are only finitely many level sets, A is a union of level sets and finite sets, hence A is semilinear and computable. □

A square matrix M is said to be *irreducible* iff when all non-zero entries are replaced by 1, the result is the adjacency matrix of a strongly connected graph.

Lemma 3 *If f is a given rational series, then f can be expressed as $f = p/q$, such that the zeros of q of smallest modulus ρ are exactly $\rho, \rho\omega, \rho\omega^2, \ldots, \rho\omega^{k-1}$, for some non-negative integer k, where ω is a primitive k-th root of unity. The polynomials p and q are computable.*

Proof : We will show that from a given rational series $f = p/q$ we can compute a row vector u, a column vector v, and an irreducible square matrix M, such that all of their entries are in $\mathbb{Q}$, all entries of M are non-negative and

$$f = u \cdot (U - xM)^{-1} \cdot v$$

where U is the identity matrix of the same size as M. It is clear from this that we can write $f = p/q$ where $q = \mathrm{Det}(U - xM)$. Note that the reciprocals of the zeros of q are

the eigenvalues of M. The Perron-Frobenius theorem asserts that the largest modulus eigenvalues of M are exactly $1/\rho, \omega/\rho, \ldots, \omega^{k-1}/\rho$, for some $\rho > 0$, positive integer k, and where ω is a primitive k-th root of unity [12].

It is classical that if $f = p/q$ is a rational series, then we have

$$f = u \cdot (U_h - xM)^{-1} \cdot v$$

where u is a $1 \times h$ rational matrix, v is a $h \times 1$ rational matrix, M is a $h \times h$ rational matrix, and U_h is the $h \times h$ identity matrix. We actually have

- $u = (0, 0, \ldots, 0, 1)$
- v is the transpose of $([x^{h-1}]p, \ldots, [x^0]p)$
- M has 0 entries except for
  - Column h is the transpose of
    $$(-[x^h]q, -[x^{h-1}]q, \ldots, -[x^1]q)$$
  - For $2 \leq i \leq h$, $M_{i,i-1} = 1$

Observe that M is irreducible because $M_{1,h}, M_{2,1}, \ldots, M_{h,h-1}$ are all non-zero. If M is non-negative, then we are done. Hence, we will assume that M is not non-negative. This implies that at least one entry in column h must be negative.

Define H to be the $2h \times h$ matrix (recall that U_h is the $h \times h$ identity matrix)

$$H = \begin{pmatrix} +U_h \\ -U_h \end{pmatrix}$$

We are going to define a nonnegative $2h \times 2h$ matrix $\hat{M}$ which is a solution to

$$H \cdot M = \hat{M} \cdot H \tag{2}$$

$\hat{M}$ will be defined entry by entry.

1. For $2 \leq i \leq h$, $\hat{M}_{i,i-1} = 1$ and $\hat{M}_{h+i,h+i-1} = 1$.
2. For $1 \leq i \leq h$, if $M_{i,h} \geq 0$, then $\hat{M}_{i,h} = M_{i,h}$ and $\hat{M}_{h+i,2h} = M_{i,h}$.
3. For $1 \leq i \leq h$, if $M_{i,h} < 0$, then $\hat{M}_{i,2h} = -M_{i,h}$ and $\hat{M}_{h+i,h} = -M_{i,h}$.
4. All other entries of $\hat{M}$ are 0.

We check that $\hat{M}$ is a nonnegative matrix which satisfies Eq. 2. It is clear that $\hat{M}$ is nonnegative. Next, we verify that Eq. 2 holds. Note that both $H \cdot M$ and $\hat{M} \cdot H$ are $2h \times h$ matrices. Throughout all the following cases we use item 4 implicitly which means that each row/column product involves a single multiplication.

First observe that if $2 \leq i \leq h$, then

$$(H \cdot M)_{i,i-1} = H_{i,i} \cdot M_{i,i-1} = M_{i,i-1} = 1$$

and

$$(\hat{M} \cdot H)_{i,i-1} = \hat{M}_{i,i-1} \cdot H_{i-1,i-1} = \hat{M}_{i,i-1} = 1 \text{ using item 1}$$

Also,

$$(H \cdot M)_{i+h,i+h-1} = H_{i+h,i+h} \cdot M_{i+h,i+h-1} = -M_{i+h,i+h-1} = -1$$

and

$$(\hat{M} \cdot H)_{i+h,i+h-1} = \hat{M}_{i+h,i+h-1} \cdot H_{i+h-1,i+h-1} = -M_{i+h,i+h-1} = -1 \text{ using item 1}$$

Assume that $1 \leq i \leq h$. If $M_{i,h} \geq 0$, then

$$(H \cdot M)_{i,h} = H_{i,i} \cdot M_{i,h} = M_{i,h}$$

and

$$(\hat{M} \cdot H)_{i,h} = \hat{M}_{i,h} \cdot H_{h,h} = \hat{M}_{i,h} = M_{i,h} \text{ using item 2}$$

Next,

$$(H \cdot M)_{i+h,h} = H_{i+h,i} \cdot M_{i,h} = -M_{i,h}$$

and

$$(\hat{M} \cdot H)_{i+h,h} = \hat{M}_{i+h,2h} \cdot H_{2h,2h} = -\hat{M}_{i+h,2h} = -M_{i,h} \text{ using item 2}$$

If $M_{i,h} < 0$, then

$$(H \cdot M)_{i,h} = H_{i,i} \cdot M_{i,h} = M_{i,h}$$

and

$$(\hat{M} \cdot H)_{i,h} = \hat{M}_{i,2h} \cdot H_{2h,h} = -\hat{M}_{i,2h} = M_{i,h} \text{ using item 3}$$

Next,

$$(H \cdot M)_{i+h,h} = H_{i+h,i} \cdot M_{i,h} = -M_{i,h}$$

and

$$(\hat{M} \cdot H)_{i+h,h} = \hat{M}_{i+h,h} \cdot H_{h,h} = \hat{M}_{i+h,h} = -M_{i,h} \text{ using item 3}$$

Finally, assume that $j \notin \{i-1, h\}$ and $j < h$.

$$(H \cdot M)_{i,j} = H_{i,i} \cdot M_{i,j} = 0$$

and noting that $\hat{M}_{i,j} = \hat{M}_{i,h+j} = 0$ by items 1 and 4,

$$(\hat{M} \cdot H)_{i,j} = \hat{M}_{i,j} \cdot H_{j,j} + \hat{M}_{i,j+h} \cdot H_{j+h,j} = 0$$

Now we check that $\hat{M}$ is irreducible. Let G be the digraph of $\hat{M}$. We again point out that $M_{1,h} \neq 0$. If $M_{1,h} > 0$, then G has the edges

$$(2,1), \ldots, (h, h-1), (h+2, h+1), \ldots, (2h, 2h-1), (1,h), (h+1, 2h)$$

and since at least one $M_{i,h} < 0$, there are also edges $(i, 2h)$ and $(h+i, h)$, by item 3. It is clear from these edges that G is strongly connected. If $M_{1,h} < 0$, then G has the edges

$$(2,1), \ldots, (h, h-1), (h+2, h+1), \ldots, (2h, 2h-1), (1,2h), (h+1, h)$$

with the last two edges coming from item 3, and again G is strongly connected.

We can now finish the proof. Define the $2h \times 1$ vector v' by $v' = H \cdot v$. Define u' to be the $1 \times 2h$ vector whose first h components match those of u and whose last h are all 0. It is clear that $u' \cdot H = u$. We have

$$u' \cdot \hat{M}^n \cdot v' = u' \cdot \hat{M}^n \cdot H \cdot v = u' \cdot H \cdot M^n \cdot v = u \cdot M^n \cdot v$$

This is equivalent to

$$u' \cdot (U_{2h} - x\hat{M})^{-1} \cdot v' = u \cdot (U_h - xM)^{-1} \cdot v$$

□

Lemma 4 *Let f be a given rational series, with $f = p/q$ according to Lem. 3. Let α be the reciprocal of the smallest modulus of any zero of q. There is a constant $c > 0$ and an infinite arithmetic progression A such that if $n \in A$, then*

$$|[x^n]f| > c\alpha^n$$

Proof : Following the exposition in [7] (p. 22-23), and the fact that the smallest modulus zeros of q are exactly ω^i/α, for $i = 0, 1, \ldots, k-1$, for some positive integer k, where ω is a primitive k-th root of unity, we get

$$[x^n]f = \alpha^n \sum_{i=0}^{k-1} c_i \cdot \omega^{in} + O(1/\beta_1^n)$$

where $\beta_1, \ldots, \beta_r$ are the other zeros of q arranged in non-decreasing modulus, and $c_i \neq 0$ for $0 \leq i \leq k-1$. In fact,

$$c_i = \gamma \prod_{j=1}^{r} (\omega^i/\alpha - \beta_j)^{m_j}$$

where γ is a non-zero constant and m_j is the multiplicity of β_j. Define $g \in \mathbb{C}[x]$ by

$$g = \sum_{i=0}^{k-1} c_i x^i$$

Now, g has at most $k-1$ distinct zeros, but since $\omega^0, \omega^1, \ldots, \omega^{k-1}$ are all distinct, $\sum_{i=0}^{k-1} c_i \omega^{in}$ cannot be zero for all n. The lemma now follows from Lem. 2. □

A set $\theta_1, \ldots, \theta_r$ is said to be *linearly independent* over $\mathbb{Q}$ (LIQ) iff $b_0, b_1, \ldots, b_r \in \mathbb{Q}$ and $b_0 + \sum_{i=1}^{r} b_i\theta_i = 0$ imply that $b_0 = b_1 = \cdots = b_r = 0$. Define $\mathbf{e}(z)$ by

$$\mathbf{e}(z) = \exp(2\pi\sqrt{-1} \cdot z)$$

Lemma 5 *Let $\theta_1, \ldots, \theta_s$ be real numbers at least one of which is irrational. Let $g_i \in \mathbb{C}$, such that $g_i \neq 0$, for $1 \leq i \leq s$. Then, for any infinite arithmetic progression A, there exists $c > 0$ such that for infinitely many $n \in A$*

$$|\sum_{i=1}^{s} g_i \mathbf{e}(n\theta_i)| > c$$

Proof : Since $\mathbf{e}(z+k) = \mathbf{e}(z)$ for any integer k, we can assume that $0 \leq \theta_1, \ldots, \theta_s < 1$. In fact, for any x such that $0 \leq x < 1$, and any integer k, when we write kx we will mean the fractional part only. By re-indexing if necessary, let $\{\theta_1, \ldots, \theta_r\}$ be a maximal subset of $\{\theta_1, \ldots, \theta_s\}$ which is LIQ. There must be a non-empty LIQ subset since at least θ_1 is irrational, so $r \geq 1$. If $r < s$, then for $r+1 \leq j \leq s$

$$\theta_j = b_{j,0} + \sum_{i=1}^{r} b_{j,i}\theta_i \tag{3}$$

where $b_{j,0}, b_{j,1}, \ldots, b_{j,r} \in \mathbb{Q}$.

Let A be an arbitrary infinite arithmetic progression $A = \{h + gn \mid n \in \mathbb{N}\}$. It is easy to reduce the restriction $n \in A$ to $n \in \mathbb{N}$. Notice that if $m \in A$, then

$$\sum_{i=1}^{s} g_i \mathbf{e}(m\theta_i) = \sum_{i=1}^{s} g_i \cdot \mathbf{e}(h\theta_i) \cdot \mathbf{e}(gn\theta_i)$$

where $m = h + gn$, and $n \in \mathbb{N}$. Since the factors $\mathbf{e}(h\theta_i)$ are non-zero constants, we will ignore them. Therefore, it suffices to establish the result for an expression

$$\sum_{i=1}^{s} g_i \mathbf{e}(nd\theta_i)$$

where g divides d.

Let d be the least positive integer such that g divides d and $db_{j,i}$ is an integer for $r+1 \leq j \leq s$ and $1 \leq i \leq r$. Note that $\{d\theta_1, \ldots, d\theta_r\}$ is a maximal LIQ subset of $\{d\theta_1, \ldots, d\theta_s\}$. The Weyl-von Neumann Theorem asserts that for any $0 \leq \eta_1, \ldots, \eta_r < 1$ and any $\epsilon > 0$, there exists $n \in \mathbb{N}$, such that for $1 \leq i \leq r$,

$$|nd\theta_i - \eta_i| < \epsilon \tag{4}$$

Let $\eta_i = i\theta$. We will choose θ shortly. Let $z = \mathbf{e}(\theta)$. Using the fact that if $0 \leq \epsilon < 1$, and x is real, then $|\mathbf{e}(x+\epsilon)| = \mathbf{e}(x) + O(\epsilon)$, and Eq. 3, and Eq. 4 we have

$$\sum_{i=1}^{s} g_i \mathbf{e}(nd\theta_i) = \sum_{i=1}^{r} g_i z^i + \sum_{j=r+1}^{s} g_j \mathbf{e}(db_{j,0}) z^{\sum_{i=1}^{r} db_{j,i}} + O(\epsilon) \tag{5}$$

Note that the big-O notation indicates a dependence only on the number of terms and the g_i, and not on n. We remark that $\mathbf{e}(db_{j,0}) = 1$. Every power of z in Eq. 5 is an integer, so we can write

$$\sum_{i=1}^{s} g_i \mathbf{e}(nd\theta_i) = z^k B + O(\epsilon)$$

such that k is an integer, and $B \in \mathbb{C}[z]$.

B is not identically zero since each $g_i \neq 0$, hence it has only finitely many zeros. Choose $z = \mathbf{e}(\theta)$ not to be one of these zeros, then $|z^k B(z)| = |B(z)| = c' > 0$. Thus, we can choose $c = c'/2$, say, and ϵ such that $c' + O(\epsilon) > c'/2 = c$. □

4 The decision method

The following expression for the n-th coefficient of a rational series $f = p/q$ is well known. A full derivation is given in [7]. Let $\alpha_1, \ldots, \alpha_s$ be the reciprocals of the distinct zeros of q.

$$[x^n]f = \sum_{i=1}^{s} g_i(n)\alpha_i^n \tag{6}$$

Each $g_i \in \mathbb{C}[x]$ has degree less than the degree of q. The g_i can be computed from p and q.

We next prove Thm. 1 by giving the steps of a decision method, and verifying their computability.

Proof : We are given a rational series $f = p/q$.

Step 1 Compute the reciprocals of $\alpha_1, \ldots, \alpha_s$ of the distinct zeros of q, and polynomials $g_1, \ldots, g_s \in \mathbb{C}[x]$, such that Eq. 6 holds.

Step 2 Arrange the α_i in sets $T_1, \ldots, T_\ell$ such that all elements of T_j have the same modulus, and if $j < j'$, then the modulus of elements in T_j is larger than the modulus of elements in $T_{j'}$. Let ρ_j be the modulus of the elements in T_j. We define $\theta_i \in \mathbb{R}$ by $0 \leq \theta_i < 1$ and

$$\alpha_i = |\alpha_i|\mathbf{e}(\theta_i)$$

The set of θ_i associated with the elements in T_j will be called the *arguments* of T_j. Define $S_j(n)$ as

$$S_j(n) = \sum_{\alpha_i \in T_j} g_i(n) \cdot \mathbf{e}(n\theta_i)$$

If all of the arguments of T_j are rational, then we will say that T_j is rational, otherwise we will say that T_j is irrational. By the techniques in the proof of Lem. 2, if T_j is rational, then we can decide whether or not $S_j(n) = 0$ for infinitely many n. If $S_j(n) = 0$ for infinitely many n, then we will say that T_j is null, otherwise we will say that it is is non-null.

Step 3

- If all T_j are rational, then go to Step 6.
- If T_1 is irrational, then let $A = \mathbb{N}$. If $T_1, \ldots, T_{j-1}$ are rational, and T_j is irrational, then define $A = \bigcap_{i=1}^{j-1} A_i$, where $A_i = \{n \mid S_i(n) = 0\}$. Note that A is always a computable semilinear set. If A is finite, then go to Step 5.

Step 4 Let h be f combed by A. We know by Cor. 1 that h is a rational series computable from f. Notice that if $[x^n]h \neq 0$, then $n \in A$, and if $n \in A$, then

$$[x^n]h = \sum_{i=j}^{s} g_i(n)\alpha_i^n \tag{7}$$

Let $h = p'/q'$, according to Lem. 3. Let $\alpha'_1, \ldots, \alpha'_{s'}$ be the reciprocals of the distinct zeros of q', ordered according to the scheme used for $\alpha_1, \ldots, \alpha_s$. Eq. 6 for h becomes

$$[x^n]h = |\alpha'_1|^n \cdot \sum_{i=1}^{m} g'_i(n)\omega^{in} + o(|\alpha'_1|^n \tag{8}$$

where ω is a primitive m-th root of unity. Lem. 4 implies that $|\alpha'_1| = \rho_1$.

By Lem. 2,

$$\sum_{i=1}^{m} g'_i(n)\omega^{in}$$

vanishes on a semilinear set B. If B were infinite, then for $n \in B$

$$|[x^n]f| = o(|\alpha'_1|^n = o(\rho_1^n)$$

However, this would contradict Lem. 5, since over any infinite arithmetic progression $B' \subseteq B$, there exists some $c > 0$ and infinitely many $n \in B'$ such that

$$|S_1(n)| > c|\rho_1|^n$$

Thus, we conclude that B must be finite. By Lem. 2, we can compute $N \in \mathbb{N}$ such that $n > N$ implies that $|\rho_1^n \sum_{i=1}^{m} g'_i(n)\omega^{in}|$ dominates the $o(|\alpha'_1|^n)$ term in Eq. 8. Now, $[x^n]f = 0$ can be tested explicitly for $n = 0, 1, \ldots, N$.

Step 5 If A is finite, then by Lem. 2, we can compute an N as in Step 4, and test $[x^n]f = 0$ explicitly for $n = 0, \ldots, N$.

Step 6 The computability of RSP is clear, based on Lem. 2. □

5 Negative results

We first prove Thm. 2.

Proof : The problem of deciding whether or not a finite automaton F with binary input alphabet A accepts A^* is PSPACE-complete [6]. The generating series of F is just $f = \sum_{n=0}^{\infty} c_n \cdot x^n$, such that c_n is the sum over all words of length n of the number of their accepting computations by F. The computation of f from F as a ratio of polynomials from by solving a linear system is in PTIME in the size of F. Now, F accepts A^* iff f has an Hadamard inverse. Thus, whether or not F accepts A^* is PTIME reducible to RSP. □

RSP can be generalized to multivariate series. A formal series f in k non-commuting variables is a mapping $f : A^* \to \mathbb{Q}$, where A is a k-ary alphabet. A formal polynomial is a series which is non-zero only on a finite subset of A^*. A series f is said to be rational iff there are polynomials p and q such that $q(\lambda) = 0$ and

$$f = p \cdot (1 + q + q^2 + \cdots)$$

Here, 1 is the series such that $1(\lambda) = 1$, and otherwise $1(w) = 0$. Given a rational f, determining whether or not $f(w) = 0$ for some $w \in A^*$ is the non-commuting bivariate

version of RSP. A proof that this version of RSP is non-computable via reduction from Hilbert's 10th Problem is given in [9].

It is also possible to say something about the multivariate versions of RSP in the commuting case. A series $f \in \mathbb{Q}[[x_1, \ldots, x_r]]$ is said to be rational if there are polynomials $p, q \in \mathbb{Q}[x_1, \ldots, x_r]$, such that $q(0, 0, \ldots, 0) = 1$ and $f = p/q$. We next prove Thm. 3.

Proof : We adapt the proof for the non-commuting case to the commuting case. If all the coefficients of $p \in \mathbb{Q}[x - 1, \ldots, x_r]$ are integers, then p is called a *Diophantine polynomial*. Hilbert's 10th Problem was to produce an algorithm which would decide whether or not there exist non-negative integers $m_1, \ldots, m_r$ such that $p(m_1, \ldots, m_r) = 0$. A set of non-negative integers $\{m_1, \ldots, m_r\}$ such that $p(m_1, \ldots, m_r) = 0$ is said to be a *Diophantine solution* for p. It is known that there is a positive integer N such that no algorithm for Hilbert's 10th Problem exists for r-variate Diophantine polynomials with $r \geq N$. See [9].

We reduce the N-variate version of Hilbert's 10th Problem to the commutative, N-variate RSP. Given any N-variate Diophantine polynomial p, we will construct a rational series f such that

$$[x_1^{n_1} \cdots x_N^{n_N}] f = p(n_1, \ldots, n_N) \tag{9}$$

It is clear from eq. 9 that p has a Diophantine solution iff f does not have an Hadamard inverse.

A Diophantine polynomial p can be obtained through a finite number of additions and multiplications, starting with the polynomials $1, -1$, and $x_1, \ldots, x_N$. The rational series $\prod_{i=1}^{N} \frac{1}{1-x_i}$ and the polynomial 1 satisfy Eq. 9. The same is true for the rational series $-\prod_{i=1}^{N} \frac{1}{1-x_i}$ and the polynomial -1. For $1 \leq j \leq N$, the rational series $\frac{x_j}{1-x_j} \cdot \prod_{i=1}^{N} \frac{1}{1-x_i}$ and the polynomial x_j also satisfy Eq. 9.

Let us write $f \sim p$ to indicate that Eq. 9 holds between a rational series f and a Diophantine polynomial p. It is clear that if $f_1 \sim p_1$ and $f_2 \sim p_2$, then $f_1 + f_2 \sim p_1 + p_2$ and $f_1 \circ f_2 \sim p_1 \cdot p_2$ (ordinary polynomial product). Since $f_1 \circ f_2$ is again rational by Thm.4.4 of [13], we have shown how to construct a rational series f such that $f \sim p$ for any given Diophantine polynomial. □

We conjecture that RSP is non-computable in the bivariate, commuting case.

Appendix

We make some remarks about the notion 'given' that has been used throughout this paper. By a given rational series $f = p/q$, we mean that the polynomials p and q are known explicitly as sequences of rational numbers. Let q have the distinct zeros $\alpha_1, \ldots, \alpha_s$, with multiplicities $m_1, \ldots, m_s$, respectively. It is well known for any $k \in \mathbb{N}$ that a list $((\tilde{\alpha}_1, m_1), (\tilde{\alpha}_s.m_s))$ can be computed such that $|\alpha_i - \tilde{\alpha}_i| < 1/2^k$. $\tilde{\alpha}_i$ is a pair of rationals a_i, b_i representing the complex number $a_i + \sqrt{-1} \cdot b_i$. See [10, 11]. It is also well known that whether or not $\alpha_i/|\alpha_i|$ is a root of unity can be computed. If $\alpha_i/|\alpha_i|$ is a root of unity, then its argument can be computed.

References

[1] M. Ben-Or, D. Kozen, and J. Reif. The complexity of elementary algebra and geometry. *JCSS*, 32:251–264, 1986.

[2] B. Benzaghou. Algèbres de Hadamard. *Bull. Soc. Math. France*, 98:209–252, 1970.

[3] J. Berstel and M. Mignotte. Deux propriétés décidables des suites récurrents linéaires. *Bull. Soc. Math. France*, 104:175–184, 1976.

[4] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata theory and formal languages*, pages 134–183. springer, 1975.

[5] S. Eilenberg. *Automata,Languages and Machines.* Academic Press, 1974.

[6] Michael R. Garey and David S. Johnson. *Computers and Intractability.* W.H.Freeman and Company, New York, 1979.

[7] M. Hall. *Combinatorial Theory.* Wiley Interscience, 1967.

[8] G. Hansel. A simple proof of the Skolem-Mahler-Lech theorem. In *ICALP85*, pages 244–249, 1985.

[9] W. Kuich and A. Salomaa. *Semirings,Automata,Languages.* Springer-Verlag, 1986.

[10] M. Mignotte. *Mathematics for Computer Algebra.* Springer, 1992.

[11] B. Mishra. *Algorithmic Algebra.* Springer, 1993.

[12] M. Rosenblatt. *Random Processes.* Oxford Univ. Press, 1962.

[13] A. Salomaa and S. Soittola. *Automata Theoretic Aspects of Formal Power Series.* Springer-Verlag, 1978.