A Robust Class of Linear Recurrence Sequences

Corentin Barloy
École Normale Supérieure de Paris, France

Nathanaël Fijalkow
CNRS, LaBRI, Bordeaux, France
The Alan Turing Institute of data science, London, United Kingdom

Nathan Lhote
University of Warsaw, Poland

Filip Mazowiecki
LaBRI, Université de Bordeaux, France

Abstract

We introduce a subclass of linear recurrence sequences which we call poly-rational sequences because they are denoted by rational expressions closed under sum and product. We show that this class is robust by giving several characterisations: polynomially ambiguous weighted automata, copyless cost-register automata, rational formal series, and linear recurrence sequences whose eigenvalues are roots of rational numbers.

2012 ACM Subject Classification Theory of computation → Models of computation

Keywords and phrases linear recurrence sequences, weighted automata, cost-register automata

Digital Object Identifier 10.4230/LIPIcs.CSL.2020.9


Funding The second author was supported by the CODYS project ANR-18-CE40-0007.

Acknowledgements We thank Théodore Lopez for reporting a maths typo in Lemma 10, S. Akshay for fruitful discussions, and the anonymous reviewers for their useful suggestions.

1 Introduction

The study of sequences of numbers originated in mathematics and has deep connections with many fields. A prominent class of sequences is that of linear recurrence sequences, such as the Fibonacci sequence

$$0, 1, 1, 2, 3, 5, 8, 13, \ldots$$

Despite the simplicity of linear recurrence sequences many problems related to them remain open, and are the object of active research. In theoretical computer science the two main questions are:

- How to finitely represent sequences?
- How to algorithmically analyse properties of sequences?

In this paper we focus on problems related to the first question. The question of representation has led to important insights in the structure of linear recurrence sequences by giving several equivalent characterisations, some of which we briefly review here. We refer to Section 2 and the next sections for technical definitions.
**Linear recurrence sequences.** A sequence of rational numbers \( u = (u_n)_{n \in \mathbb{N}} = (u_0, u_1, u_2, \ldots) \) is a linear recurrence system (LRS) if there exist real numbers \( a_1, \ldots, a_k \) such that for all \( n \geq 0 \)

\[
  u_{n+k} = a_1 u_{n+k-1} + \ldots + a_k u_n.
\]

(1)

In this paper we will consider only sequences of rational numbers, therefore, we additionally assume that \( a_i \) are rational numbers. The smallest \( k \) for which \( u \) satisfies an equation of the form (1) is called the order of \( u \). The Fibonacci sequence \( \langle F_n \rangle_{n \in \mathbb{N}} \) is an LRS of order 2 satisfying the recurrence \( F_{n+2} = F_{n+1} + F_n \).

**Rational expressions.** Studying the closure properties of linear recurrence sequences yields the following result, an instance of the Kleene-Schützenberger theorem [20]: linear recurrence sequences form the smallest class of sequences containing the sequences \( \langle a, 0, 0, \ldots \rangle \) for a rational number \( a \) and closed under sum, Cauchy product, and Kleene star.

**Weighted automata.** The model of weighted automata is a well studied quantitative extension of classical automata. In general a weighted automaton recognises a function \( f : \Sigma^* \rightarrow \mathbb{R} \), hence when considering a unary alphabet this becomes \( f : \{a\}^* \rightarrow \mathbb{R} \), and identifying \( \{a\}^* \) with \( \mathbb{N} \) we can see \( f \) as a sequence of numbers. Whenever we write about sequences recognised by models like weighted automata, we implicitly assume that these are over a unary alphabet.

**Cost-register automata.** Several characterisations of weighted automata have been introduced [6, 12, 3]. We will be interested in the model of cost-register automata (CRA). These are deterministic models with registers whose contents are blindly updated (i.e., without transitions like zero tests). It was shown that considering linear updates yields a model equivalent to weighted automata.

We summarise in one theorem the equivalences above, which is the starting point of our work. Technical definitions are given in the paper.

▶ **Theorem 1** (Folklore, see for instance [5, 20, 7]). The following classes of sequences are effectively equivalent.

- Linear recurrence sequences,
- Sequences recognised by weighted automata,
- Sequences recognised by linear cost-register automata,
- Sequences denoted by rational expressions,
- Sequences whose formal series are rational, i.e. of the form \( \frac{P}{Q} \) where \( P, Q \) are polynomials.

**Algorithmic analysis of linear recurrence sequences**

The questions regarding algorithmic analysis are far from being answered. A very simple and natural problem, the Skolem problem, is still unsolved [21, 18]: given a linear recurrence sequence, does it contain a zero? Recent breakthrough results sharpened our understanding of the Skolem problem [16, 17], but one of the outcomes is that the general problem for the whole class of linear recurrence sequences is beyond our reach at the moment, since it would impact notoriously difficult problems from number theory. We refer the reader to the recent survey about what is known to be decidable for linear recurrence sequences [18].
Our contributions

Since the full class of linear recurrence sequences is too hard to be algorithmically analysed (we only mentioned the Skolem problem but many related problems are also difficult), let us revise our ambitions, go back to the drawing board, and study tractable subclasses.

In this paper we introduce poly-rational sequences which is a strict fragment of linear recurrence sequences. We give several equivalent characterisations of this class following the equivalence results stated in Theorem 1. Our results are summarised in the following theorem.

▶ Theorem 2. The following classes of sequences are effectively equivalent.
- Sequences denoted by poly-rational expressions (Section 2),
- Sequences recognised by polynomially ambiguous weighted automata (Section 3),
- Sequences recognised by copyless cost-register automata (Section 4),
- Sequences whose formal series are of the form $\frac{P}{Q}$ where $P, Q$ are polynomials and the roots of $Q$ are roots of rational numbers (Section 5),
- Linear recurrence sequences whose eigenvalues are roots of rational numbers (Section 5).

We do not discuss the efficiency of reductions proving the equivalences. Our constructions are elementary, and in most cases they yield blow ups in the size of representation.

We note that the Skolem problem and its variants are known to be decidable, and NP-hard, for the subclass of poly-rational sequences. The decidability easily follows from the fact that our class is subsumed by other classes for which such results were obtained (see e.g. [19], for the case where all eigenvalues are roots of algebraic real numbers). The Skolem problem is known to be NP-hard already for the class of LRS whose eigenvalues are roots of unity [1]. This implies that the Skolem problem for the class of poly-rational sequences is also NP-hard, which is the best known lower bound even for the full class of linear recurrence sequences.

Related works

The intractability of the Skolem problem for linear recurrence sequences also impacts the other equivalent models, leading to the study of several restrictions. A classical approach to tame weighted automata is to bound the ambiguity of weighted automata, i.e. bounding the number of accepting runs with a function depending on the length of the word. Many positive results have been obtained in the past years following this approach [11, 10, 8].

Another restriction studied in the model of cost-register automata is the copyless restriction: registers are not allowed to be copied more than once. It was conjectured that the copyless restriction would result in good decidability properties [3], but this has been recently falsified [2].

2 Linear recurrence sequences and rational expressions

We let $u = \langle u_n \rangle_{n \in \mathbb{N}} = \langle u_0, u_1, u_2, \ldots \rangle$ denote a sequence of rational numbers.

Linear recurrence sequences

We will assume that an LRS $u$ is given by the numbers $a_1, \ldots, a_k$ and the values of the first $k$ elements: $u_0, \ldots, u_{k-1}$. The recurrence (1) induces the sequence $u$. We let LRS denote the class of LRS. Given an LRS we define its characteristic polynomial as

$$Q(x) = x^k - a_1 x^{k-1} - \ldots - a_{k-1} x - a_k.$$
The roots of the characteristic polynomial are called the *eigenvalues* of the LRS.

**Formal series**

Formal series are a different representation for sequences. The sequence \((u_n)_{n \in \mathbb{N}}\) induces the formal series \(S(x) = \sum_{n \in \mathbb{N}} u_n x^n\), with the interpretation that the coefficient of \(x^n\) is the value of the \(n\)-th element in the sequence. Note that a polynomial represents a sequence with a finite support.

➤ **Example 3.** A standard example of an LRS is the Fibonacci sequence \(\{F_n\}_{n \in \mathbb{N}}\) defined by the recurrence \(F_{n+2} = F_{n+1} + F_n\) and initial values \(F_0 = 0, F_1 = 1\). Its characteristic polynomial is \(p(x) = x^2 - x - 1\), whose roots are \(\frac{1 + \sqrt{5}}{2}\) and \(\frac{1 - \sqrt{5}}{2}\). The corresponding formal series is \(S(x) = \sum_{n=0}^{\infty} F_n x^n\). Using the definition of \(F\) we obtain \(S(x) = x + xS(x) + x^2S(x)\) and thus \(S(x) = \frac{1}{1-x-x^2}\).

**Rational expressions**

We start by defining three classes of sequences.

- **Fin:** a sequence \(u\) is in **Fin**, or equivalently \(u\) has finite support, if the set \(\{n \in \mathbb{N} : u_n \neq 0\}\) is finite;
- **Arith:** a sequence \(u\) is in **Arith**, or equivalently \(u\) is arithmetic, if \(u_0 = a, u_{n+1} = u_n + b\) for some rational numbers \(a, b\);
- **Geo:** a sequence \(u\) is in **Geo**, or equivalent \(u\) is geometric, if \(u_0 = a, u_{n+1} = \lambda \cdot u_n\), for some rational numbers \(a, \lambda\).

We let **Geo** denote the class of geometric sequences with a fixed parameter \(\lambda\).

We now define some classical operators. Here \(u, v, u^1, \ldots, u^k\) are sequences.

- **Sum:** \(u + v\) is the component wise sum of sequences;
- **Cauchy product:** \(u \cdot v = \{\sum_{p+q=n} u_p \cdot v_q\}_{n \in \mathbb{N}}\); inducing \((u)^n\) defined by \((u)^0 = \langle 1, 0, 0, 0, \ldots \rangle\) and \((u)^{n+1} = (u)^n \cdot u\), in particular \((u)^1 = u\);
- **Kleene star:** \((u)^+ = \sum_{n \in \mathbb{N}} (u)^n\), it is only defined when \(u_0 = 0\);
- **Hadamard product:** \(u \times v\) is the component wise product of sequences;
- **Shift:** \(\langle a, u \rangle = \langle a, u_0, u_1, \ldots \rangle\), defined for any rational number \(a\);
- **Shuffle:** shuffle\((u^1, u^2, \ldots, u^k) = \langle u^1_0, u^2_0, \ldots, u^k_0, u^1_1, u^2_1, \ldots, u^k_1, u^1_2, \ldots \rangle\).

We write \(\text{Rat}[\mathcal{C}, \text{op}_1, \ldots, \text{op}_k]\) for the smallest class of sequences containing \(\mathcal{C}\) and closed under the operators \(\text{op}_1, \ldots, \text{op}_k\). Rational expressions in Theorem 1 are classically defined as follows [20]:

\[
\text{Rat} = \text{Rat}[\text{Fin}, +, *, \cdot].
\]

The class **Rat** contains all classes defined above, and is closed under all mentioned operators, i.e.

\[
\text{Rat} = \text{Rat}[\text{Fin} \cup \text{Arith} \cup \text{Geo}, +, *, \cdot, \times, \text{shift, shuffle}].
\]

We now introduce a class of sequences denoted by a fragment of rational expressions, whose study is the purpose of this article. The class is called poly-rational sequences, because they are denoted by rational expressions using sum and product.

➤ **Definition 4** (Poly-rational sequences).

\[
\text{PolyRat} = \text{Rat}[\text{Arith} \cup \text{Geo}, +, \times, \text{shift, shuffle}].
\]
In other words, \texttt{PolyRat} is the smallest class of sequences containing arithmetic and geometric sequences that is closed under sum, Hadamard product, shift, and shuffle. A trivial observation is that \texttt{Fin} $\subseteq$ \texttt{PolyRat} since using shift one can generate any sequence with finite support. One could try to simplify the definition of \texttt{PolyRat} replacing \texttt{Arith} $\cup$ \texttt{Geo} with \texttt{Fin}. Unfortunately, the operators $+$, $\times$, shift, shuffle are too restricted, and geometric and arithmetic sequences could not be generated. In fact, the class would collapse to \texttt{Fin}.

Since \texttt{Rat} contains \texttt{Arith} and \texttt{Geo} and is closed under Hadamard product, shift, and shuffle, we have \texttt{PolyRat} $\subseteq$ \texttt{Rat}. We will show that the inclusion is indeed strict. As we will see in this paper, the class \texttt{PolyRat} has many equivalent and surprising characterisations.

### 3 Characterisation with polynomially ambiguous weighted automata

We refer to e.g. [7] for an excellent introduction to weighted automata. We consider weighted automata over the rational semiring $(\mathbb{Q}, +, \cdot)$, where $+$ and $\cdot$ are the standard sum and product. For an alphabet $\Sigma$, weighted automata recognise functions assigning rational numbers to finite words, i.e. $f : \Sigma^* \rightarrow \mathbb{Q}$. In this paper we will consider only one-letter alphabets so the set of words is $\{a\}^* = \{\varepsilon, a, a^2, \ldots\}$, which is identified with $\mathbb{N}$. Therefore, weighted automata recognise functions $f : \mathbb{N} \rightarrow \mathbb{Q}$, i.e. weighted automata recognise sequences of rational numbers.

Formally, a weighted automaton is a tuple $A = (Q, M, I, F)$, where $Q$ is a finite set of states, $M$ is a $Q \times Q$ matrix over $\mathbb{Q}$ and $I, F$ are the initial and final vectors, respectively, of dimension $Q$ (for convenience we label the coordinates by elements of $Q$). The sequence recognised by the automaton $A$ is $[[A]]$ defined by $[[A]](n) = I^T M^n F$, where $I^T$ is the transpose of $I$.

We give an equivalent definition of $A$ in terms of accepting runs. We say that a state $q \in Q$ is an initial state if $I(q) \neq 0$ and that it is a final state if $F(q) \neq 0$. If $q$ is initial we say that its initial weight is $I(q)$, and if $q$ is final then its final weight is $F(q)$. For two states $p, q \in Q$ we say that there is a transition from $p$ to $q$ if $M(p, q) \neq 0$. Such a transition is denoted $p \rightarrow q$ and its weights is $M(p, q)$. A run $\rho$ is a sequence of consecutive transitions, and it is accepting if the first state is initial and the last state is final. The value of an accepting run $\rho = q_0 \rightarrow q_1 \rightarrow \cdots \rightarrow q_n$ is

$$|\rho| = I(q_0) \cdot \prod_{i=0}^{n-1} M(q_i, q_{i+1}) \cdot F(q_n).$$

Let $\text{Runs}_A(n)$ denote the set of all accepting runs of length $n$. An alternative and equivalent definition of $[[A]]$ is

$$[[A]](n) = \sum_{\rho \in \text{Runs}_A(n)} |\rho|.$$

\textbf{Example 5}. Consider the automaton $A = (Q, M, I, F)$ represented in Figure 1. We have $[[A]](n) = F_n$, where $(F_n)_{n \in \mathbb{N}}$ is the Fibonacci sequence from Example 3.

The ambiguity of an automaton $A$ is the function $a_A : \mathbb{N} \rightarrow \mathbb{N}$ which associates to $n$ the number of accepting runs $|\text{Runs}_A(n)|$. We consider the following classes:

- $\text{DetWA}$ – the class of deterministic weighted automata, i.e. such that for any $p$, there exists at most one $q$ such that $M(p, q) \neq 0$;
- $k\text{WA}$ for fixed $k \in \mathbb{N}$ – the class of $k$-ambiguous weighted automata, i.e. when $a_A(n) \leq k$ for all $n$;
A Robust Class of Linear Recurrence Sequences

\[ I = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad M = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad F = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \]

Figure 1: A weighted automaton recognising the Fibonacci sequence.

- \( \text{FinWA} = \bigcup_{k \in \mathbb{N}} k \text{WA} \) – the class of finitely ambiguous weighted automata, i.e. when there exists \( k \) such that \( a_A(n) \leq k \) for all \( n \);
- \( \text{PolyWA} \) – class of polynomially ambiguous automata, i.e. when there exists a polynomial \( P : \mathbb{N} \to \mathbb{N} \) such that \( a_A(n) \leq P(n) \) for all \( n \);
- \( \text{WA} \) – the full class of weighted automata.

For example, the automaton in Example 5 is not polynomially ambiguous because the number of accepting runs is exponential. We will see that this is no accident by proving in Section 5 that the Fibonacci sequence is not in \( \text{PolyWA} \).

We present our first characterisation of \( \text{PolyRat} \).

\[ \text{Theorem 6. PolyRat} = \text{PolyWA} \]

Proof of Theorem 6

This subsection is divided into two parts for both inclusions.

\( \text{PolyRat} \subseteq \text{PolyWA} \)

Figure 2 shows how to recognise the arithmetic and the geometric sequences. For each finitely supported sequence a simple weighted automaton can be constructed. It remains to prove that the class \( \text{PolyWA} \) is closed under the operators. The sum and products correspond to union and product of automata, it is readily verified that these standard constructions preserve the polynomial ambiguity. Below we deal with shift and shuffle operators.

Suppose we have a polynomially ambiguous automaton \( A \) for \( u \) and we want to construct a new polynomially ambiguous automaton \( A' \) for \( (a, u) \). We start with the case when \( a = 0 \). Then \( A' \) has the same set of states as \( A \) plus one new state \( q_0 \), which is the only initial state in \( A' \). All transitions from \( A \) are inherited. There are additionally only outgoing transitions from \( q_0 \) to all states that are initial in \( A \); the weight of each transition is the initial weight of the corresponding state in \( A \). It is readily verified that \( A' \) recognises \( (0, u) \) and that \( A' \) is
polynomially ambiguous. For $a \neq 0$ it suffices to add one more state that is both initial and final with initial weight 1 and final weight $a$.

To deal with shuffle we start with the following preliminary construction. Fix some $k > 0$ and a polynomially ambiguous automaton $A$ recognising $u$. We construct $A[k]$ recognising $u' = (u_0, 0, \ldots, 0, u_1, 0, \ldots, 0, u_2, \ldots)$, i.e. elements $u_i$ are separated by $k - 1$ elements with 0.

The idea to construct $A'$ is that the set of states have an additional component $\{0, \ldots, k - 1\}$, and they behave like $A$ every $k$-th step; in the remaining steps they only wait. Formally, the set of states of $A[k]$ is $Q \times \{0, \ldots, k - 1\}$, where $Q$ is the set of states of $A$. The initial (final) states are $(q, 0)$ such that $q$ is initial (final) in $A$ with the same weight. For every transition $p \rightarrow q$ in $A$ there is a transition $(p, 0) \rightarrow (q, 1)$ in $A[k]$ with the same weight. The remaining transitions are $(q, i) \rightarrow (q, (i + 1) \mod k)$ with weight 1, defined for every $i > 0$ and every $q \in Q$. It is readily verified that $A[k]$ recognises $u'$.

Let $A_0, \ldots, A_{k-1}$ be polynomially ambiguous automata recognising $u_0, \ldots, u_{k-1}$. For every $A_i$ let $A_i[k]$ be an automaton as above, additionally shifted $i$ times with 0’s. Then shuffle$(u_0, \ldots, u_{k-1})$ is recognised by the disjoint union of $A_i[k]$.

PolyWA $\subseteq$ PolyRat

The first step is to decompose polynomially ambiguous automata into a union of automata that we will call chained loops. We say that the states $p_0, p_1, \ldots, p_{k-1} \in Q$ form a loop if $M(p_i, p_j) \neq 0$ is equivalent to $j = i + 1 \mod k$ and a path if $M(p_i, p_j) \neq 0$ is equivalent to $j = i + 1$ (in particular $p_{k-1}$ has no successor). A chained loop of size $k$ is an automaton over the set states of $\{q_0, \ldots, q_{k-1}\} \cup P$ such that

- $q_0$ is the unique initial state;
- $q_0, \ldots, q_{k-1}$ form a path;
- each $q_i$ is contained in at most one loop (the states in $P$ are used only as intermediate states in the loops);
- $q_{k-1}$ is the unique final state with $F(q_{k-1}) = 1$.

We define the concatenation of two chained loops $A_1, A_2$: this is the chained loop obtained by constructing the union of the two automata with the initial state being the initial state of $A_1$, the final state being the final state of $A_2$, and rewiring the output of $A_1$ to the initial state of $A_2$, see e.g. Figure 3.

![Figure 3](image-url) Three example chained loops. The initial and final weights are depicted by ingoing and outgoing edges. The chained loop $A_1$ recognises the sequence defined by $f_1(2n) = 2 \cdot 3^n$, $f_1(2n+1) = 0$ whose power series is $\frac{4}{3 \cdot 3^2}$. The chained loop $A_2$ recognises the sequence $f_2(n) = 5^{n+1}$ whose power series is $\frac{1}{5^{n+1}}$. The chained loop $A_3$ is the concatenation of $A_1$ and $A_2$ and it recognises the sequence $f_3(n) = \sum_{i=1}^{n} f_1(i-1) \cdot f_2(n-i)$ whose power series is $\frac{10}{(1-3 \cdot 3^2)(1-5^2)}$. 
Lemma 7. Every polynomially ambiguous weighted automaton is equivalent to a union of chained loops.

Proof. Let $A$ be a polynomially ambiguous weighted automaton. Without loss of generality $A$ is trimmed, i.e., every state occurs in at least one accepting run.

We first note that any state in $A$ is contained in at most one loop. Indeed, a state contained in two loops induces a sequence of words with exponential ambiguity. This implies that a sequence $(q_0, q_1, \ldots, q_k)$ with $q_i \neq q_j$ for $i \neq j$ induces at most one chained loop of which it is the path. There are finitely many such sequences because $k$ is bounded by the number of states of $A$.

We claim that $A$ is equivalent to the union of all chained loops induced by such sequences. Indeed, there is a bijection between the runs of $A$ and the runs of all the chained loops, respecting the values of runs. Consider a run $\rho$ of $A$, where a state $q$ appears multiple times. Then between each occurrence of $q$ this is the same run, because they are loops over $q$ and there can be only one loop containing $q$. So $\rho = uv^k w$, where $v$ is the (only) loop containing $q$. Repeating this for $u$ and $w$, we obtain a unique decomposition of $\rho$ into

$$q_0 \cdot \ell_0^m \cdot q_0 \rightarrow q_1 \cdot \ell_1^m \cdot q_1 \rightarrow \cdots \rightarrow q_k \cdot \ell_k^m \cdot q_k,$$

where $\ell_i$ is a loop over $q_i$ (we can have $m_i = 0$) and $q_i \neq q_j$ for $i \neq j$.

Our aim is to use the decomposition result stated in Lemma 7 to prove the inclusion $\text{PolyWA} \subseteq \text{PolyRat}$. It will be convenient for reasoning to use formal series.

Lemma 8.

- The formal series induced by a chained loop of size 1 with a loop is of the form $\frac{\alpha}{1-\lambda x^\ell}$, where $\alpha = I(q_0)$, $\lambda$ is the product of the weights in the loop and $\ell$ is the length of the loop. If there is no loop this reduces to $\alpha$.
- Let $S_1, S_2$ be the formal series induced by the chained loops $A_1$ and $A_2$, then the formal series induced by the concatenation of $A_1$ and $A_2$ is $x \cdot S_1 \cdot S_2$.
- Let $S_1, S_2$ be the formal series induced by two automata $A_1$ and $A_2$, then the formal series induced by the union of $A_1$ and $A_2$ is $S_1 + S_2$.

Proof. The first and the third item are immediate, we focus on the second. For convenience let us assume that $A_1(-1) = 0$. By definition the concatenation of two chained loops recognises the sequence defined by

$$[A](n) = \sum_{i=0}^{n} [A_1](i-1) \cdot [A_2](n-i)$$

since an accepting run in the concatenation is the concatenation of an accepting run in $A_1$ and an accepting run in $A_2$. The only issue is that the output state of $A_1$ was changed into a transition, and to include this step we write $A_1(i-1)$ instead of $A_1(i)$. Hence the formal series is indeed the Cauchy product of $S_1$ and $S_2$, shifted by one.

We are now half-way through the proof of the inclusion $\text{PolyWA} \subseteq \text{PolyRat}$: thanks to Lemma 7, we can restrict our attention to unions of chained loops, and thanks to Lemma 8, we know what are the formal series induced by the sequences computed by such automata. More specifically, they are obtained from formal series of the form $\frac{\alpha}{1-\lambda x^\ell}$ by taking sums and Cauchy products (with an additional shift).

To prove that $\text{PolyRat}$ contains such sequences it is tempting to attempt showing that the sequences above are in $\text{PolyRat}$ and the closure of $\text{PolyRat}$ under sums and Cauchy
products. Unfortunately, the closure under Cauchy product is not clear (although it will follow from the final result that it indeed holds).

We sidestep this issue by observing that we only need to be able to do Cauchy products of formal series of a special form. Indeed, the formal series described above are of the form $\frac{R}{Q}$ where $P, Q$ are rational polynomials and the roots of $Q$ are roots of rational numbers: this is true of $\frac{1}{1-\lambda x^\ell}$ and is clearly closed under sums and Cauchy products (with the additional shift).

Notice that every chained loop can be obtained as concatenations of chained loops of size 1. Thus Lemma 8 gives a characterisation of formal series corresponding to unions of chained loops: these are sums of products of $\frac{1}{1-\lambda x^\ell}$ and polynomials. We further simplify this characterisation applying the following lemma.

Lemma 9. Consider the formal series $\frac{P}{Q}$ where $P, Q$ are rational polynomials and the roots of $Q$ are roots of rational numbers. Then $\frac{P}{Q}$ can be written as the sum of formal series of the form $\frac{R}{(1-\lambda x^\ell)^k}$ for rational polynomials $R$, rational numbers $\lambda$, and $\ell, k$ natural numbers.

Proof. This is a direct consequence of the fact that $\mathbb{Q}[x]$ is a Euclidean ring. The exact statement following from this is that any product $\prod_{i=1}^n \frac{P_i}{Q_i}$ where the polynomials $P_i$ are mutually prime (meaning, for each $i$, the polynomials $P_i$ and $\prod_{j\neq i} P_j$ are coprime) can be written as a sum of $\frac{P_i}{Q_i}$ for some rational polynomials $Q_i$.

To conclude, we observe that any polynomial whose roots are roots of rational numbers can be written as a product of mutually prime polynomials of the form $(1-\lambda x^\ell)^k$.

By Lemma 8 and Lemma 9 it follows that for every finite union of chained loops its formal series is a sum of $\frac{R}{(1-\lambda x^\ell)^k}$ for rational polynomials $R$, rational numbers $\lambda$, and $\ell, k$ natural numbers. Combining this with Lemma 7 we get that the formal series computed by $\text{PolyWA}$ are of the same form. Thus we have reduced proving the inclusion $\text{PolyWA} \subseteq \text{PolyRat}$ to proving that sequences whose formal series are sums of formal series of the form $\frac{R}{(1-\lambda x^\ell)^k}$ are in $\text{PolyRat}$.

Since $\text{PolyRat}$ is closed under sum, it suffices to consider one such formal series. Moreover, due to the closure under shifts we can assume that the polynomial $R$ is equal to 1; as stated in the lemma below.

Lemma 10. The sequence whose formal series is $\frac{1}{(1-\lambda x^\ell)^k}$ is in $\text{PolyRat}$.

Proof. We know that

$$\frac{1}{(1-\lambda x^\ell)^k} = \sum_{n \in \mathbb{N}} \binom{n+k-1}{k-1} \lambda^n x^\ell n.$$ 

Note that $\binom{n+k-1}{k-1}$ is a polynomial in $n$ of degree at most $k-1$, i.e. $\binom{n+k-1}{k-1} = \sum_{p=0}^{k-1} a_p n^p$.

It follows that

$$\frac{1}{(1-\lambda x^\ell)^k} = \sum_{p=0}^{k-1} a_p \sum_{n \in \mathbb{N}} n^p \lambda^n x^\ell n.$$ 

It is enough to prove that for each $p$ the sequence whose formal series is

$$\sum_{n \in \mathbb{N}} a_p n^p \lambda^n x^\ell n$$

is in $\text{PolyRat}$. Using an arithmetic sequence and Hadamard products we construct $\langle a_p n^p \rangle_{n \in \mathbb{N}}$. Multiplying it using Hadamard product with the geometric sequence $\langle \lambda^n \rangle_{n \in \mathbb{N}}$ yields $\langle a_p n^p \lambda^n \rangle_{n \in \mathbb{N}}$. Shuffling the obtained sequence with $\ell - 1$ null sequences yields the desired sequence.

\[\Box\]
3.1 Application: the ambiguity hierarchy of weighted automata

We show that the natural classes of weighted automata defined by ambiguity can be described using subclasses of rational expressions.

\[ \text{Figure 4} \] The strict ambiguous hierarchy of weighted automata.

\[ \text{Lemma 11.} \]
\[ \text{DetWA} = \bigcup_{\lambda \in \mathbb{Q}} \text{Rat}[\text{Geo}_\lambda, \text{shift}, \text{shuffle}]; \]
\[ \text{FinWA} = \text{Rat}[\text{Geo}, +, \text{shift}, \text{shuffle}]. \]

\textbf{Proof.} We start by proving \( \text{DetWA} = \bigcup_{\lambda \in \mathbb{Q}} \text{Rat}[\text{Geo}_\lambda, \text{shift}, \text{shuffle}] \).

(\( \subseteq \)) Since the automaton is deterministic it has a shape of a lasso, i.e. the states can be partitioned into a path such that the last state on the path is in a loop. Let \( \lambda \) be the value obtained by multiplying all values on the loop, let \( l \) be the length of the loop and let \( m \) be the length of the path. Then it is easy to see that the sequence is obtained by first taking a shuffle of \( l \) sequences in \( \text{Geo}_\lambda \) and then shifting it \( m \) times.

(\( \supseteq \)) We already know that \( \text{Geo}_\lambda \) are definable by deterministic weighted automata from Figure 2. Closure under shift follows from the construction in the proof of \( \text{PolyRat} \subseteq \text{PolyWA} \) because it preserves the property of being deterministic. The shuffle construction preserves this property only up to a certain point. The construction of each automaton \( A_i[k] \) is deterministic but taking their sum does not yield explicitly a deterministic automaton. It suffices to observe that by construction \( A_i[k] \) are all lasso automata with loops of the same length. Moreover, every word is accepted by at most one \( A_i[k] \). To define the final automaton consider \( A_i[k] \) with the longest path. The final automaton will be \( A_i[k] \) with modified transitions and final outputs. Indeed we add the automata one by one, and for every accepting state we readjust the ingoing and outgoing transitions to give the correct value.

Proof of \( \text{FinWA} = \text{Rat}[\text{Geo}, +, \text{shift}, \text{shuffle}] \).

(\( \subseteq \)) By Lemma 7 we know that each automaton in \( \text{FinWA} \) is a union of chained loops. It is easy to see that every such chained loop has to be a lasso otherwise it will contradict the assumption that the automaton is finitely ambiguous. Then the construction follows by doing the construction for every lasso as in the proof of \( \text{DetWA} = \bigcup_{\lambda \in \mathbb{Q}} \text{Rat}[\text{Geo}_\lambda, \text{shift}, \text{shuffle}] \) and using \( + \) to deal with the union.
The linear CRA represented in Figure 5 recognises the Fibonacci sequence.

We give examples witnessing the strict inclusions $\text{DetWA} \subsetneq \text{FinWA} \subsetneq \text{PolyWA} \subsetneq \text{WA}$ and $\text{kWA} \subsetneq (k + 1)\text{WA}$.

Lemma 12.
- $a = \text{shuffle}(2^n)_{n \in \mathbb{N}} \cup (1)^{n \in \mathbb{N}}$ is in $\text{1WA}$ but not in $\text{DetWA}$,
- $u_n$ defined by $u_n = 1^n + 2^n + \cdots + (k + 1)^n$ is in $(k + 1)\text{WA}$ but not in $\text{kWA}$,
- $v$ defined by $v_n = n$ is in $\text{PolyWA}$ but not in $\text{FinWA}$;
- Fibonacci is in $\text{WA}$ but not in $\text{PolyWA}$.

We omit the simple but technical proofs of the first three items. Only the last item will be proved in Section 5, it follows from the fact that $\text{PolyWA} = \text{PolyRat}$ is equal to the class of LRS whose eigenvalues are roots of rational numbers. As mentioned in Example 3 the characteristic polynomial of the Fibonacci sequence is $x^2 - x - 1$, so its eigenvalues are not roots of rationals.

4 Characterisation with copyless cost-register automata

Cost-register automata (CRA) \cite{3} are deterministic automata with write-only registers, where each transition updates the registers using addition and multiplication. Like in Section 3 we will consider only the variant of the model over a one-letter alphabet recognising functions $f : \mathbb{N} \rightarrow \mathbb{Q}$.

Let $\mathcal{X}$ be a set of variables (registers). The set of expressions $\mathcal{Expr}(\mathcal{X})$ is generated by the following grammar
\[
e ::= x \mid r \mid e + e \mid e \cdot e,
\]
where $x \in \mathcal{X}$ and $r \in \mathbb{Q}$. A substitution is a mapping $\nu : \mathcal{X} \rightarrow \mathcal{Expr}(\mathcal{X})$. We let $\mathcal{Subs}(\mathcal{X})$ denote the set of all substitutions. A valuation is a function $\sigma : \mathcal{X} \rightarrow \mathbb{Q}$, it is a special case of substitutions, where expressions are limited to constants. We freely compose these objects: for instance let $\mathcal{X} = \{x\}$, define the valuation $\nu_0(x) = 0$, the substitution $\sigma(x) = x + 1$ and the expression $e = 2x$. Then $\nu_0 \circ \sigma^n \circ e = 2n$. Note that we use the non-standard order for functional composition. We see this computation as the output of a 1-register machine which initialises $x$ with 0, increments its value at each step and outputs its double value.

Formally, a CRA is a tuple $\mathcal{A} = (\mathcal{Q}, \mathcal{X}, \delta, q_0, \nu_0, \mu)$, where $\mathcal{Q}$ is the set of states, $\mathcal{X}$ is the set of registers, $\delta : \mathcal{Q} \rightarrow \mathcal{Q} \times \mathcal{Subs}(\mathcal{X})$ is the transition function, $q_0$ is the initial state, $\nu_0 : \mathcal{X} \rightarrow \mathbb{Q}$ is the initial valuation and $\mu : \mathcal{Q} \rightarrow \mathbb{Q}$ is the final output function. The output of $\mathcal{A}$ on $n$ is defined by the unique run of length $n$: let $q_0 \rightarrow q_1 \rightarrow \cdots \rightarrow q_n$ such that $\delta(q_i) = (q_{i+1}, \sigma_{i+1})$
\[
[\mathcal{A}][n] = \nu_0 \circ \sigma_1 \circ \cdots \circ \sigma_n \circ \mu(q_n).
\]

A CRA is said to be linear if its transitions and output function use only linear expressions, i.e. such that in the grammar $e \cdot e$ is restricted to $e \cdot r$. We let $\text{LCRA}$ denote the class of sequences recognised by linear CRA, which is known to be equivalent to the class $\text{WA}$ \cite{3}. The linear CRA represented in Figure 5 recognises the Fibonacci sequence.

A substitution $\sigma$ is called copyless if each register is used at most once in $\sigma(x)$ for every $x$. It is easy to observe that a composition of copyless substitutions is a copyless substitution.
Figure 5 A linear CRA recognising the Fibonacci sequence. There is only one state and two variables $X = \{x_0, x_1\}$. Since there is only one state the transitions are presented using only the expression that is applied every time.

A CRA is said to be copyless if in each transition, each substitution is copyless. For example in Figure 5 the register $x_1$ is used twice in the substitution so it is not a copyless automaton. We let CCRA denote the class of sequences recognised by copyless cost register automata (CCRA). In [13] it is shown that CCRA is a subclass of linear CRA. We show that this is another class characterising PolyRat.

Theorem 13. PolyRat = CCRA

PolyRat $\subseteq$ CCRA

This inclusion is easy to prove, it requires to perform the classical constructions as in Section 3 and to note that they respect the copyless restriction.

CCRA $\subseteq$ PolyRat

We make use of a simple property in [15]. A substitution is in normal form if there exists an order on the registers $x_1 < \cdots < x_k$ such that the substitutions updating registers respect the order: $\sigma(x_i)$ can use only registers $x_j$ such that $x_j \geq x_i$. A CCRA is in normal form if all substitutions used by it are in normal form, with the same order on the registers. It is known that every CCRA has an equivalent CCRA in normal form [15, Proposition 1]. We will use this fact only to prove Lemma 14, but in the construction we will assume that the CCRA is in normal form.

Consider a CCRA $A$, we prove that the sequence $u$ it recognises is in PolyRat. We assume without loss of generality that $A$ is in normal form. Since $A$ is deterministic it has the shape of a lasso: a tail of length $k$ and a loop of length $\ell$. Let us fix $n \in \mathbb{N}$ and $\ell' \in \{0, \ldots, \ell - 1\}$, the run is

$$q_0 \rightarrow \cdots \rightarrow q_k \rightarrow (p_0 \rightarrow \cdots \rightarrow p_{\ell - 1})^n \rightarrow p_0 \rightarrow \cdots \rightarrow p_{\ell'}.$$  \hspace{1cm} (2)

Let $\delta(q_i) = (q_{i+1 \mod \ell}, \beta_i)$ for $i \in \{0, \ldots, k\}$, with the convention that $q_{k+1} = p_0$, and $\delta(p_i) = (p_{i+1 \mod \ell}, \sigma_i)$ for $i \in \{0, \ldots, \ell - 1\}$. Define

$$u'_0 = u_0 \circ \beta_0 \circ \cdots \circ \beta_k \ ; \quad \sigma = \sigma_0 \circ \cdots \circ \sigma_{\ell - 1} \ ; \quad e = \sigma_0 \circ \cdots \circ \sigma_{\ell' - 1} \circ \mu(p_{\ell'}).$$

Notice that $\sigma$ is a copyless substitution since it is a composition of copyless substitutions. We define the sequence $u[\ell']$ by

$$u_n[\ell'] = u'_0 \circ \sigma^n \circ e.$$
We will prove in Lemma 14 that the sequence \( u[\ell'] \) is in \textbf{PolyRat}. The decomposition of the runs into a lasso implies the following equality:

\[
u = (u_0, u_1, \ldots, u_{k-1}, \text{shuffle}(u[0], \ldots, u[\ell-1])),\]

which implies that \( u \) is in \textbf{PolyRat}, provided the lemma below is true.

\begin{lemma}
For every copyless substitution \( \sigma \) in normal form, for all initial valuation \( \nu \) and for all expression \( e \), the sequence

\[
(\nu \circ \sigma^n \circ e)_{n \in \mathbb{N}}
\]

is in \textbf{PolyRat}.
\end{lemma}

\begin{proof}
We prove that the sequence \( u_x = \nu \circ \sigma^n(x) \) is in \textbf{PolyRat} for every register \( x \), i.e. the lemma holds for \( e = x \). The general case follows since \textbf{PolyRat} is closed under addition and product.

We consider two cases. Suppose \( x \) is not used in \( \sigma(x) \). We prove that for \( n \) big enough the sequence stabilises, i.e. \( \sigma^n(x) = \sigma^{n+1}(x) = c \) for some constant \( c \). We show this by induction on the order \( < \) from the assumed normal form. If \( x \) is the largest element in the order \( < \) then \( \sigma(x) \) is a constant and thus \( \sigma^n(x) = \sigma^{n+1}(x) \). For the induction step suppose \( x \) is not the largest element. If \( \sigma(x) \) is a constant then the claim is trivial. Otherwise let \( x_1, \ldots, x_m \) be registers used in \( \sigma(x) \). Since \( \sigma \) is copyless then \( x_1 \) is not used in \( \sigma(x_i) \) for every \( i \). Hence by the induction assumption for every \( i \) there exists \( n_i \) such that \( \sigma^n(x_i) = \sigma^{n+1}(x_i) \) for all \( n \geq n_i \). It suffices to take \( n = \max_i \{n_i \mid 1 \leq i \leq m\} + 1 \). Since constant sequences are geometric sequences with \( \lambda = 1 \) then \( u_x \) can be defined in \textbf{PolyRat} using shift.

Now suppose that \( x \) is used in \( \sigma(x) \). The expression \( \sigma(x) \) is equivalent to \( \sum_{i=0}^m a_i \cdot x_i \) for some constants \( a_i \), where \( x_0 = x \) and \( x_i \) are pairwise different. Since \( \sigma \) is copyless then for all \( i > 0 \) we know that \( \sigma(x_i) \) does not use \( x_i \). By the previous paragraph there exists \( N \) such that \( \sigma^N(x_i) = \sigma^{N+1}(x_i) = c_i \) for some constants \( c_i \) for all \( i > 0 \). Let \( n \geq N \). Then

\[
\nu \circ \sigma^{n+1}(x) = \nu \circ \sigma^n \circ \sigma(x) = \nu \circ \left( \sum_{i=0}^m a_i \cdot \sigma^n(x_i) \right) = a_0 \cdot (\nu \circ \sigma^n(x)) + \sum_{i=1}^m a_i \cdot c_i.
\]

Let \( a = a_0 \) and \( b = \sum_{i=1}^m a_i \cdot c_i \). We proved that for \( n \geq N \) the sequence \( u_x \) satisfies \( u_x(n+1) = a \cdot u_x(n) + b \). It remains to prove that this sequence is in \textbf{PolyRat}. It is enough to show that \( u_x'(n) = u_x(n + N) \) is in \textbf{PolyRat} since to obtain \( u_x \) it suffices to use shift \( N \) times. There are two cases. If \( a = 1 \) then \( u_x'(n) \) is an arithmetic sequence, which concludes the proof. If \( a \neq 1 \) then

\[
u_x'(n) = a^n \cdot u_x'(0) + \sum_{i=0}^{n-1} a^i \cdot b = a^n \cdot u_x'(0) + b \cdot \frac{a^n - 1}{a - 1}.
\]

This is a sum of a geometric sequence \( a^n \cdot (u_x'(0) + \frac{b}{a-1}) \); and a constant sequence \( \frac{b}{a-1} \), which proves \( u_x' \) is in \textbf{PolyRat}.

\end{proof}

\begin{remark}
One can extract from this proof the equivalence between linear \textbf{CCRA} and \textbf{Rat}[Arith ∪ Geo,+,shift,shuffle].
\end{remark}

It was recently shown that \textbf{CCRA} are strictly less expressive than weighted automata [15]. The proof goes by analysing the Fibonacci sequence. We will get as a corollary of our results a self-contained proof that \textbf{LCRA} and \textbf{CCRA} are different.
Characterisation with linear recurrence sequences and formal series

Our last two characterisations are as follows.

Theorem 16. PolyRat is the class of LRS whose eigenvalues are roots of rational numbers, and equivalently whose formal series are \( \frac{P}{Q} \) with \( P, Q \) rational polynomials and the roots of \( Q \) are roots of rational numbers.

Before proving the theorem, we note that we can now substantiate the claim that the Fibonacci sequence is not in PolyRat (hence not in CCRA and PolyWA), since its eigenvalues are not roots of rational numbers.

We rely on the following classical result about LRS, see e.g. [9].

Lemma 17. Let \( u \) be an LRS and \( Q \) its characteristic polynomial. The formal series induced by \( u \) is \( \frac{P}{Q} \) for some rational polynomial \( P \).

For both inclusions we rely on Theorem 6 stating that PolyRat = PolyWA and the decompositions obtained in the subsequent lemmas.

PolyRat \( \subseteq \) LRS whose eigenvalues are roots of rational numbers

By Lemma 7 and Lemma 8 the formal series of sequences in PolyWA are sums and Cauchy products of formal series of the form \( \frac{R}{1-\lambda x^\ell} \), where \( R \) is a rational polynomial, \( \ell \in \mathbb{N} \) and \( \lambda \in \mathbb{Q} \). The roots of \( 1-\lambda x^\ell \) are roots of \( \frac{1}{\lambda} \), so the roots of the characteristic polynomial are roots of rational numbers.

LRS whose eigenvalues are roots of rational numbers \( \subseteq \) PolyRat

Consider an LRS whose eigenvalues are roots of rational numbers. Thanks to Lemma 17 the formal series it induces is \( \frac{P}{Q} \) with \( P, Q \) rational polynomials and the roots of \( Q \) are roots of rational numbers. By Lemma 9 the formal series can be written as a sum of formal series of the form \( \frac{R}{(1-\lambda x^\ell)^k} \) for rational polynomials \( R \), rational number \( \lambda \), and \( \ell, k \) natural numbers. It follows from Lemma 10 and the closure of PolyRat under sum and shift that such sequences belong to PolyRat.

Conclusion

We introduced a class of linear recurrence sequences and obtained several characterisations. The most surprising equivalence is CCRA = PolyWA. This equality is very particular to our setting: for instance the two classes are incomparable, i.e. neither of the inclusions hold, for tropical semirings [15, 14]. We also conjecture that these classes are incomparable over the rational semiring for general alphabets (of size bigger than 1).

We leave open the precise complexity of the Skolem problem for PolyRat. Recent progress has been made for a subclass of PolyRat [1]: the Skolem problem for LRS whose eigenvalues are roots of unity is NP-complete. Our class is more general since we consider LRS whose eigenvalues are roots of rational numbers, so the NP-hardness also applies. However the algorithm constructed in [1] does not extend to our class.
References


16. Joël Ouaknine and James Worrell. On the Positivity Problem for Simple Linear Recurrence Sequences,. In Automata, Languages, and Programming - 41st International Colloquium,
A Robust Class of Linear Recurrence Sequences


