On Some Decidability Questions Concerning Supports of Rational Series

Peter Kostolányi[1]

Department of Computer Science, Comenius University in Bratislava,
Mlynská dolina, 842 48 Bratislava, Slovakia

Abstract

A well-known construction of a weighted automaton over the integers, assigning zero to precisely the nonempty words from the equality set of a given Post's correspondence problem instance, is extended to the case of weights taken from an arbitrary integral domain that is not locally finite. Undecidability of problems for rational series such as universality or rationality of support thus generalises to such domains as well. In spite of being fairly simple, these findings imply that the support rationality problem can be undecidable over rings of positive characteristic, answering an open question of D. Kirsten and K. Quaas. In addition, a more general undecidability result for rational series over other than locally finite integral domains is proved, which subsumes, e.g., the undecidability of support rationality or context-freeness.

Keywords: Rational series, Weighted automaton, Decidability, Post's correspondence problem, Support

1. Introduction

An instance of the *Post's correspondence problem* (PCP) is given by a pair of homomorphisms f, g between two free monoids. The *equality set* of such an instance consists of all w such that $f(w) = g(w)$, and the task is to decide whether it contains a nonempty word. The Post's correspondence problem is famous for being undecidable [10].

It is a classical observation that for each PCP instance with equality set E, there exists a rational series over $\mathbb{Z}$ whose support consists precisely of words *not* in E and of the empty word ε: if a PCP instance is given by homomorphisms f, g, then one can construct a weighted automaton $\mathcal{A}_{f,g}$ over $\mathbb{Z}$, which assigns zero to precisely the nonempty words w such that $f(w) = g(w)$. This fact was independently discovered several times. For instance, it has been proved by S. Eilenberg [7, Theorem VI.12.1]; his construction is also reproduced in [16, 17]. Another reference is given by [2, Exercise 3.4.2]. It also appears implicitly in works dealing with decidability of problems for matrix semigroups – see, e.g., [9, Section 6.1]. As a consequence of this observation, it follows that the support universality problem for rational series over $\mathbb{Z}$, in which one asks whether or not the coefficients of a series realised by an automaton are all nonzero, is undecidable.

Another result discovered several times is that of undecidability of support rationality for rational series over $\mathbb{Z}$ – in other words, it is impossible to decide whether a given weighted automaton over $\mathbb{Z}$ realises a series whose support is a rational language. This undecidability result has already been mentioned in Exercise II.12.1 of the book by A. Salomaa and M. Soittola [19]. Later, a proof via modification of the above-mentioned reduction from PCP has been given by D. Kirsten and K. Quaas [14]; their proof technique appears to be the most universal when it comes to possible generalisations. Finally, B. Steinberg has noted in a MathOverflow answer [20] that the result follows *directly* by constructability of $\mathcal{A}_{f,g}$ and a result of A. Salomaa [18], according to which it is undecidable whether a given PCP instance has a rational equality set; this is probably the simplest known proof.

To sum up, algorithmic constructability of $\mathcal{A}_{f,g}$ is sufficient to deduce undecidability both of the support universality problem and of the support rationality problem for rational series over $\mathbb{Z}$.

Email address: `kostolanyi@fmph.uniba.sk` (Peter Kostolányi)

[1]The author was partially supported by the grant VEGA 1/0601/20.

D. Kirsten and K. Quaas [14] have also opened the question of decidability of the support rationality problem for semirings other than $\mathbb{Z}$. Undecidability of this problem over $\mathbb{Z}$ clearly implies its undecidability over all semirings containing $\mathbb{Z}$, and in particular over all rings of characteristic zero. On the other hand, the problem is trivial over the so-called *SR-semirings* – *i.e.*, semirings S such that *all* rational series over S have rational supports; an algebraic characterisation of such semirings was given by D. Kirsten [12, 13]. The following two problems have been left open in [14]:

1. Is there a semiring not containing $\mathbb{Z}$ that is not an SR-semiring?
2. If so, is there a semiring not containing $\mathbb{Z}$, over which the support rationality problem is undecidable?

An answer to the former question was actually already known at the time [2, Exercise 3.4.1], and was also given later by G. Chapuy and I. Klimann [3]: the field $\mathbb{F}_p(x)$ is not an SR-semiring for any finite field $\mathbb{F}_p$ with prime p. The latter question of [14] has been left untouched.

In this note, we first emphasise that the abovementioned property implies a characterisation of integral domains that are at the same time SR-semirings – this happens if and only if the integral domain in question is locally finite. We also notice that this property is further equivalent to all rational series having context-free supports.

Next, we show that weighted automata assigning zero to precisely the nonempty words from the equality set of a PCP instance can as well be constructed over all integral domains that are not locally finite. A very simple property of such integral domains is sufficient to establish this result.

Using the same reasoning as over the integers, this implies that problems such as support rationality or support universality are decidable over an integral domain R if and only if R is locally finite. In particular, the support rationality problem is undecidable for other than locally finite integral domains of positive characteristic, providing an affirmative answer to the second open question from [14].

Some other closely related decision problems are shown to be undecidable over other than locally finite integral domains as well.

Finally, we prove a relatively general undecidability result for rational series over other than locally finite integral domains R, providing sufficient conditions for a class of languages $\mathscr{L}$ under which it is undecidable whether the support of a rational series over R belongs to $\mathscr{L}$. We show that when $\mathscr{L}$ contains all rational languages and is closed under left quotients by words, then nontriviality of this decision problem always implies its undecidability. In particular, it follows that the context-freeness of support is undecidable.

2. Preliminaries

Alphabets are always nonempty and finite in what follows. The empty word over any alphabet is denoted by ε. Given an alphabet Σ, $w \in \Sigma^*$, and $c \in \Sigma$, we denote by $|w|$ the length of the word w and by $|w|_c$ the number of occurrences of c in w. If moreover $L \subseteq \Sigma^*$, we denote by $w^{-1}L$ the left quotient $w^{-1}L = \{x \in \Sigma^* \mid wx \in L\}$ of L by w.

We denote by $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$, respectively, the sets of all *nonnegative* integers, integers, and rational numbers. For each $n \in \mathbb{N}$, we write $[n] = \{1, \ldots, n\}$.

A *semiring* is an algebra $(S, +, \cdot, 0, 1)$, where $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid, multiplication distributes over addition both from left and from right, and $a \cdot 0 = 0 \cdot a = 0$ holds for all $a \in S$. A *ring* is a semiring $(R, +, \cdot, 0, 1)$ such that R forms an abelian group with addition; it is said to be commutative if $\cdot$ is. An *integral domain* is a nontrivial commutative ring in which $a = 0$ or $b = 0$ whenever $a \cdot b = 0$. A *field* is an integral domain $(\mathbb{F}, +, \cdot, 0, 1)$ such that $\mathbb{F} \setminus \{0\}$ forms an abelian group with multiplication.

The reader may consult any standard text on abstract algebra, such as [6, 11], for the necessary background. In what follows, we just briefly review some basic algebraic concepts used in this article.

The subsemiring of a semiring S generated by a set $X \subseteq S$ is the smallest subsemiring of S containing X. Similarly, the subring of a ring R generated by $X \subseteq R$ is the smallest subring of R containing X, and the subfield of a field $\mathbb{F}$ generated by $X \subseteq \mathbb{F}$ is the smallest subfield of $\mathbb{F}$ containing X. A semiring, a ring, or a field, resp., is said to be *finitely generated* if it is generated by a finite set, and *locally finite* if its finitely generated subsemirings, subrings, or subfields, resp., are all finite. A field is locally finite if and only if it is locally finite as a ring (or as a semiring).

An element a of a semiring is said to be of *infinite multiplicative order* if $a^n = a^m$ for $n, m \in \mathbb{N}$ always implies $n = m$.

The *characteristic* of a ring R is, in case it exists, the *smallest* positive integer n such that $\sum_{k=1}^{n} 1 = 0$ holds in R; if there is no such n, then the characteristic of R is said to be zero. A positive characteristic *of an integral domain* is always a prime, as any ring with composite characteristic $n = pq$ for $p, q \in [n] \setminus \{1, n\}$ satisfies

$$\left(\sum_{k=1}^{p} 1\right) \cdot \left(\sum_{k=1}^{q} 1\right) = \sum_{k=1}^{n} 1 = 0,$$

the factors on the left-hand side being nonzero.

The *prime subfield* of a field $(\mathbb{F}, +, \cdot, 0, 1)$ is the subfield of $\mathbb{F}$ generated by 1. The prime subfield of every field of characteristic zero equals $\mathbb{Q}$ (up to isomorphism), while the prime subfield of a field of positive characteristic p is always (up to isomorphism) the finite field $\mathbb{F}_p$ of order p.

A field $\mathbb{K}$ is said to be an *extension* of a field $\mathbb{F}$ if $\mathbb{F}$ is a subfield of $\mathbb{K}$. Given some extension $\mathbb{K}$ of a field $\mathbb{F}$ and $X \subseteq \mathbb{K}$, we denote by $\mathbb{F}[X]$ the subring of $\mathbb{K}$ generated by X over $\mathbb{F}$, *i.e.*, the subring of $\mathbb{K}$ generated by $\mathbb{F} \cup X$. Similarly, $\mathbb{F}(X)$ denotes the subfield of $\mathbb{K}$ generated by X over $\mathbb{F}$, *i.e.*, the subfield of $\mathbb{K}$ generated by $\mathbb{F} \cup X$. If X is a finite set $X = \{\alpha_1, \ldots, \alpha_n\}$, we also write $\mathbb{F}[\alpha_1, \ldots, \alpha_n]$ for $\mathbb{F}[X]$ and $\mathbb{F}(\alpha_1, \ldots, \alpha_n)$ for $\mathbb{F}(X)$. The ring $\mathbb{F}[X]$ defined above is actually always an integral domain and $\mathbb{F}(X)$ is its field of fractions.

An extension $\mathbb{K}$ of a field $\mathbb{F}$ is *finite* if $\mathbb{K}$ is finite-dimensional as a vector space over $\mathbb{F}$.

Given an extension $\mathbb{K}$ of a field $\mathbb{F}$, an element $\alpha \in \mathbb{K}$ is *algebraic* over $\mathbb{F}$ if it is a root of some nonzero univariate polynomial over $\mathbb{F}$, and *transcendental* over $\mathbb{F}$ otherwise. An extension $\mathbb{K}$ of $\mathbb{F}$ is said to be *algebraic* if all elements of $\mathbb{K}$ are algebraic over $\mathbb{F}$, and *transcendental* otherwise. Every finite extension is algebraic; if X is a finite set of elements algebraic over $\mathbb{F}$, then $\mathbb{F}(X)$ is a finite extension of the field $\mathbb{F}$.

If α is a transcendental element over $\mathbb{F}$, then the ring $\mathbb{F}[\alpha]$ is isomorphic to the *univariate polynomial ring* $\mathbb{F}[x]$ over $\mathbb{F}$ and $\mathbb{F}(\alpha)$ is isomorphic to the *field of rational fractions* $\mathbb{F}(x)$ over $\mathbb{F}$, *i.e.*, to the fraction field of the integral domain $\mathbb{F}[x]$.

Let $\mathbb{K}$ be an extension of $\mathbb{F}$ and $X \subseteq \mathbb{K}$. Then X is said to be *algebraically dependent* over $\mathbb{F}$ if there exists $n \in \mathbb{N} \setminus \{0\}$ and a nonzero n-variate polynomial p over $\mathbb{F}$ such that $p(\alpha_1, \ldots, \alpha_n) = 0$ for some pairwise distinct $\alpha_1, \ldots, \alpha_n \in X$. When this is not the case, X is said to be *algebraically independent* over $\mathbb{F}$. Observe that if $X = \{\alpha_1, \ldots, \alpha_n\}$ is algebraically independent over $\mathbb{F}$, then α_n is necessarily transcendental over $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-1})$.[2]

For an extension field $\mathbb{K}$ of $\mathbb{F}$, a *transcendence basis* of $\mathbb{K}$ over $\mathbb{F}$ is a maximal subset B of $\mathbb{K}$ that is algebraically independent over $\mathbb{F}$. Any two transcendence bases of $\mathbb{K}$ over $\mathbb{F}$ have the same cardinality – this is known as the *transcendence degree* of $\mathbb{K}$ over $\mathbb{F}$. If B is a transcendence basis of $\mathbb{K}$ over $\mathbb{F}$, then $\mathbb{K}$ is an algebraic extension of $\mathbb{F}(B)$. In particular, every field $\mathbb{K}$ is an algebraic extension of a field obtained by extending the prime subfield $\mathbb{P}$ of $\mathbb{K}$ by a transcendence basis of $\mathbb{K}$ over $\mathbb{P}$.

If $\mathbb{F}$ is a field generated by a set X and $\mathbb{P}$ is the prime subfield of $\mathbb{F}$, then clearly $\mathbb{F} = \mathbb{P}(X)$. Moreover, it is easy to see that a transcendence basis of $\mathbb{F}$ over $\mathbb{P}$ can always be chosen as a subset of the generating set X. In particular, it follows that if $\mathbb{F}$ is finitely generated, it can be expressed as $\mathbb{F} = \mathbb{P}(\alpha_1, \ldots, \alpha_n)(\alpha'_1, \ldots, \alpha'_t)$, where $\mathbb{P}$ is the prime subfield of $\mathbb{F}$, $n, t \in \mathbb{N}$, the elements $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ form a transcendence basis of $\mathbb{F}$ over $\mathbb{P}$, and $\alpha'_1, \ldots, \alpha'_t \in \mathbb{F}$ are algebraic over $\mathbb{P}(\alpha_1, \ldots, \alpha_n)$.

We now recall the basic facts about noncommutative formal power series and weighted automata; see [2, 4, 5, 16, 17, 19] for a comprehensive treatment. A *formal power series* over a semiring S and alphabet Σ is a mapping $r\colon \Sigma^* \to S$. The value of r upon $w \in \Sigma^*$ is denoted by (r, w) instead of $r(w)$ and called the *coefficient* of r at w. The series r itself is written as

$$r = \sum_{w \in \Sigma^*} (r, w)\, w.$$

The set of all series over S and Σ is denoted by $S\langle\langle \Sigma^* \rangle\rangle$.

Elements of S and words over Σ are naturally identified with power series having at most one nonzero coefficient (*i.e.*, monomials). Given $r, s \in S\langle\langle \Sigma^* \rangle\rangle$, the *sum* $r + s$, *Cauchy product* $r \cdot s$, and *Hadamard product* $r \odot s$ are defined by

$$\begin{aligned}(r + s, w) &= (r, w) + (s, w),\\ (r \cdot s, w) &= \sum_{\substack{u,v \in \Sigma^* \\ uv = w}} (r, u) \cdot (s, v),\\ (r \odot s, w) &= (r, w) \cdot (s, w)\end{aligned}$$

[2]This follows by noting that any root of a univariate polynomial over $\mathbb{F}(\alpha_1, \ldots, \alpha_{n-1})$ is at the same time a root of a univariate polynomial over $\mathbb{F}[\alpha_1, \ldots, \alpha_{n-1}]$.

for all $w \in \Sigma^*$. The *support* of $r \in S\langle\langle\Sigma^*\rangle\rangle$ is the language $\mathrm{supp}(r) = \{w \in \Sigma^* \mid (r, w) \neq 0\}$. The *characteristic series* of a language $L \subseteq \Sigma^*$ over S is the series $\mathbf{1}_L \in S\langle\langle\Sigma^*\rangle\rangle$ such that $(\mathbf{1}_L, w) = 1$ for all $w \in L$ and $(\mathbf{1}_L, w) = 0$ for all $w \in \Sigma^* \setminus L$.

A family of series $(r_i \mid i \in I)$ from $S\langle\langle\Sigma^*\rangle\rangle$ is *locally finite* if $I(w) = \{i \in I \mid (r_i, w) \neq 0\}$ is finite for all $w \in \Sigma^*$. The sum $\sum_{i\in I} r_i$ over such family is defined pointwise: for all $w \in \Sigma^*$,

$$\left(\sum_{i\in I} r_i, w\right) = \sum_{i\in I(w)} (r_i, w).$$

A *weighted* (*finite*) *automaton* over a semiring S and alphabet Σ is a quadruple $\mathcal{A} = (Q, \sigma, \iota, \tau)$, where Q is a finite set of states, $\sigma\colon Q \times \Sigma \times Q \to S$ a transition weighting function, $\iota\colon Q \to S$ an initial weighting function, and $\tau\colon Q \to S$ a terminal weighting function.

A *run* of the automaton $\mathcal{A}$ is a (finite) word $\gamma = q_0c_1q_1c_2q_2 \ldots q_{n-1}c_nq_n \in (Q\Sigma)^*Q$ with $q_0, \ldots, q_n \in Q$ and $c_1, \ldots, c_n \in \Sigma$ such that $\sigma(q_{k-1}, c_k, q_k) \neq 0$ holds for $k = 1, \ldots, n$; we also say that γ is a *run from* q_0 *to* q_n. The *label* of γ is the word $\lambda(\gamma) = c_1 \ldots c_n$ and the *value* of γ is the semiring element $\sigma(\gamma) = \sigma(q_0, c_1, q_1)\cdot\sigma(q_1, c_2, q_2)\cdot\ldots\cdot\sigma(q_{n-1}, c_n, q_n)$.

The set of all runs of $\mathcal{A}$ from $p \in Q$ to $q \in Q$ is denoted by $\mathcal{R}_{p,q}(\mathcal{A})$. The *behaviour* of $\mathcal{A}$ is a series

$$\|\mathcal{A}\| = \sum_{p,q\in Q} \sum_{\gamma\in\mathcal{R}_{p,q}(\mathcal{A})} (\iota(p)\sigma(\gamma)\tau(q))\ \lambda(\gamma),$$

where the inner sum is obviously over a locally finite family of series. We also say that the series $\|\mathcal{A}\|$ is *realised* by $\mathcal{A}$. A series $r \in S\langle\langle\Sigma^*\rangle\rangle$ is *rational* over S if it is realised by a weighted automaton over S.

Every weighted automaton over S and Σ admits an equivalent with terminal weights in $\{0, 1\}$.

Given a weighted automaton $\mathcal{A} = (Q, \sigma, \iota, \tau)$ and $q \in Q$, we denote by $\|\mathcal{A}\|_q$ the series $\|\mathcal{A}_q\|$ realised by the automaton $\mathcal{A}_q = (Q, \sigma, \iota, \tau_q)$, where $\tau_q(q) = 1$ and $\tau_q(p) = 0$ for all $p \in Q \setminus \{q\}$.

It is well known that the class of rational series over a semiring S is closed under sum and Cauchy product; when S is commutative, it is also closed under Hadamard product.

The class of rational series over S is also known to be closed under inverse homomorphisms of free monoids [19, Theorem II.4.3]. More precisely, let Σ, Γ be alphabets, $h\colon \Sigma^* \to \Gamma^*$ a homomorphism, and $r \in S\langle\langle\Gamma^*\rangle\rangle$ a rational series over S. The series $h^{-1}(r) \in S\langle\langle\Sigma^*\rangle\rangle$, defined by

$$h^{-1}(r) = \sum_{w\in\Sigma^*} (r, h(w))\, w,$$

is then rational over S as well. This property can be easily proved via linear representations [19].[3]

All closure properties mentioned above are effective, *i.e.*, they correspond to algorithmically realisable constructions on weighted automata.

An instance of the *Post's correspondence problem* (PCP) over a binary alphabet is a triple (Σ, f, g), where Σ is an alphabet and $f, g\colon \Sigma^* \to \{0, 1\}^*$ are homomorphisms. The task is to decide whether there exists a word $w \in \Sigma^+$ such that $f(w) = g(w)$, *i.e.*, whether the equality set

$$E(f, g) = \{w \in \Sigma^* \mid f(w) = g(w)\}$$

of (Σ, f, g) contains a nonempty word. It is well known that this problem is undecidable [10].

3. Basic Observations

The reductions of the PCP to problems about supports of rational series are often based on an interpretation of words over $\{0, 1\}$ as binary representations of numbers. In what follows, we use the same idea over general integral domains. However, the difference is that $2 = 1 + 1$ might no longer be a convenient base for a numeral system with digits taken from $\{0, 1\}$, as the resulting representation might not be unambiguous over integral domains of positive characteristic. This motivates the following definition.

Definition 3.1. Let R be an integral domain and $\alpha \in R$. We say that α is a *binary numeral base* over R if the mapping $\psi_\alpha\colon \{0, 1\}^* \to R$, given for all $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \{0, 1\}$ by

$$\psi_\alpha(a_1 \ldots a_n) = \alpha^n + \sum_{k=1}^{n} a_k\alpha^{n-k},$$

is injective.

[3] As such, it is actually more a property of *recognisable* series. Nevertheless, the rational and recognisable series over free monoids are well known to coincide.

We now proceed to the fundamental observation on existence of binary numeral bases, which we later use to obtain our main results.

Proposition 3.2. *Let R be an integral domain. Then R contains a binary numeral base if and only if R is not locally finite.*

Proof. For all $\alpha \in R$, the mapping ψ_α sends binary words to elements of the subring $\langle\alpha\rangle$ of R, generated by α. If R is locally finite, then $\langle\alpha\rangle$ is finite, so that ψ_α cannot be injective. Thus R contains no binary numeral base in this case.

Suppose that R is not locally finite. When R is of characteristic zero, it contains an isomorphic copy of $\mathbb{Z}$, and 2 clearly is a binary numeral base over R. More generally, if a rational number q different from 0 and ± 1 is in R, then it is a binary numeral base.[4] Indeed, if an element $\alpha \in R$ is *not* a binary numeral base over R, then

$$\psi_\alpha(a_1 \dots a_n) = \psi_\alpha(b_1 \dots b_n)$$

for some $n \in \mathbb{N}$ and $a_1, \dots, a_n, b_1, \dots, b_n \in \{0, 1\}$ such that $a_k \neq b_k$ for some $k \in [n]$.[5] This implies that α is a root of a nonzero polynomial

$$p(x) = \sum_{k=1}^{n} (a_k - b_k) x^{n-k}$$

with coefficients in $\{-1, 0, 1\}$. Thus α cannot be a rational number other than 0 or ± 1 by the rational root theorem. It also follows that α cannot be transcendental over $\mathbb{Q}$, so that if R contains such element, it is necessarily a binary numeral base as well.

Let us finally suppose that R is not locally finite and of characteristic $p > 0$, which is surely a prime. The fraction field $\mathbb{F}$ of R then has the finite field $\mathbb{F}_p$ as its prime subfield, and $\mathbb{F}_p$ is necessarily contained in R. If all elements of R were algebraic over $\mathbb{F}_p$, then $\mathbb{F}$ would be locally finite, as any finitely generated subfield of $\mathbb{F}$ would be a finite extension of $\mathbb{F}_p$, which is itself finite. As a consequence, R would be locally finite as well, which would contradict our assumption. The integral domain R thus contains at least one element α transcendental over $\mathbb{F}_p$. This in particular implies that α is not a root of a polynomial with coefficients in $\{-1, 0, 1\}$. Thus, by the same reasoning as in the case of characteristic zero, α is a binary numeral base. □

Note that the proof of the preceding theorem tells us much about how the binary numeral bases over R might look like.

If R is of characteristic zero, then every rational number in R except 0 and ± 1 is a binary numeral base. In addition, R might or might not contain elements transcendental over $\mathbb{Q}$ – these are binary numeral bases as well. The remaining elements of R might or might not be binary numeral bases.

If R is not locally finite and is of positive characteristic p, then R necessarily contains an element transcendental over $\mathbb{F}_p$, and every such element is a binary numeral base. On the contrary, elements of R algebraic over $\mathbb{F}_p$ cannot be binary numeral bases.

For later reference, let us record one particularly simple property of binary numeral bases.

Proposition 3.3. *Let R be an integral domain and $\alpha \in R$ a binary numeral base over R. Then α is of infinite multiplicative order.*

Proof. Assume for contradiction that $\alpha^n = \alpha^m$ for some nonnegative integers $n \neq m$. Then $\psi_\alpha(0^n) = \psi_\alpha(0^m)$, contradicting the assumption of α being a binary numeral base. □

We now proceed to the characterisation of integral domains over which all rational series have rational or context-free supports. The result for rationality is already known in its essence [2, Exercise 3.4.1] – see also [3] – and the one for context-freeness is a trivial extension of the same observation.

Nevertheless, we still include a proof of the proposition below, in which we make use of a slightly more straightforward approach compared to [2, 3]. While [2, 3] describe a counterexample over a unary alphabet that works in the case of positive characteristic only, we give a counterexample that can be used regardless of the characteristic, at the price of not being over a unary alphabet anymore.[6]

[4] Similar results are known in literature; see, e.g., [8]. In what follows, we give a self-contained proof of this fact.

[5] The length of both words can clearly be assumed to be the same without loss of generality.

[6] G. Chapuy and I. Klimann [3] have proved that *univariate* rational series over fields of characteristic zero always have rational supports.

Proposition 3.4. *Let R be an integral domain. Then the following are equivalent:*

(*i*) *The support of every rational series over R is rational.*

(*ii*) *The support of every rational series over R is context-free.*

(*iii*) *The integral domain R is locally finite.*

Proof. It is well known that all rational series over locally finite semirings have rational supports [13]. It thus remains to show that in case the integral domain R is not locally finite, there is a rational series over R whose support is not context-free.

Let us suppose that R is not locally finite. By Proposition 3.2, there is a binary numeral base $\alpha \in R$ over R. Let $\Sigma = \{a, b, c\}$. The series $r_{a,b}, r_{a,c}, r_{b,c} \in R\langle\langle\Sigma^*\rangle\rangle$, given for all $w \in \Sigma^*$ by

$$(r_{a,b}, w) = \alpha^{|w|_a} - \alpha^{|w|_b},$$
$$(r_{a,c}, w) = \alpha^{|w|_a} - \alpha^{|w|_c},$$
$$(r_{b,c}, w) = \alpha^{|w|_b} - \alpha^{|w|_c},$$

are then clearly rational over R. The series

$$r = r_{a,b} \odot r_{a,c} \odot r_{b,c},$$

satisfying

$$(r, w) = (\alpha^{|w|_a} - \alpha^{|w|_b})(\alpha^{|w|_a} - \alpha^{|w|_c})(\alpha^{|w|_b} - \alpha^{|w|_c})$$

for all $w \in \Sigma^*$, is thus rational as well. As α is of infinite multiplicative order by Proposition 3.3 and as R is an integral domain, it follows that (r, w) is zero if and only if at least one of the equalities $|w|_a = |w|_b$, $|w|_a = |w|_c$, or $|w|_b = |w|_c$ holds. In other words,

$$\text{supp}(r) = \{w \in \Sigma^* \mid |w|_a \neq |w|_b \neq |w|_c \neq |w|_a\},$$

which can easily be seen to be not context-free. □

4. The Main Results

We are now prepared to generalise the standard undecidability results for rational series over $\mathbb{Z}$ to rational series over other than locally finite integral domains. The main tool that we use to establish these results is a construction of a weighted automaton assigning zero to precisely the nonempty words from the equality set of a given PCP instance. This is described in Theorem 4.2 below and mimics the one over the integers [14], while using the observations of the previous section. The following proposition captures the gist of this construction.

Proposition 4.1. *Let R be an integral domain, $\alpha \in R$, and $\Gamma = \{0, 1\}$. The series $\Psi_\alpha \in R\langle\langle\Gamma^*\rangle\rangle$, defined for all $x \in \Gamma^*$ by*

$$(\Psi_\alpha, x) = \psi_\alpha(x),$$

is rational over R.

Proof. The series Ψ_α is realised by the weighted automaton $\mathcal{A}_\alpha$ in Fig. 1.

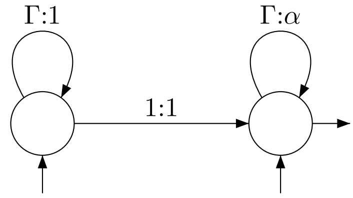

Figure 1: The automaton $\mathcal{A}_\alpha$. The notation $\Gamma{:}\beta$ with $\beta \in R$ is used as a shorthand for two transitions labelled by $0{:}\beta$ and $1{:}\beta$. Nonzero initial and final weights are always 1 and they are omitted in the diagram.

Indeed, given $x = a_1 \ldots a_n$ with $a_1, \ldots, a_n \in \Gamma$, the run of $\mathcal{A}_\alpha$ that reads the entire x in the right state is of value α^n. For each $k \in [n]$ with $a_k = 1$, the run of $\mathcal{A}_\alpha$ that reads $a_1 \ldots a_{k-1}$ using the loop at the left state, then moves to the right state upon a_k, and finally reads the rest of the word, is of value α^{n-k}. As these are the only runs whose values contribute to $(\|\mathcal{A}_\alpha\|, x)$, we obtain

$$(\|\mathcal{A}_\alpha\|, x) = \alpha^n + \sum_{k=1}^{n} a_k \alpha^{n-k} = \psi_\alpha(x),$$

since the nonzero initial and terminal weights are all equal to 1. □

Theorem 4.2. *Let R be an integral domain that is not locally finite. Given an instance (Σ, f, g) of the PCP, it is possible to algorithmically construct a weighted automaton $\mathcal{A}_{f,g}(R)$ over R and Σ such that*

$$\text{supp}\left(\|\mathcal{A}_{f,g}(R)\|\right) = \Sigma^* \setminus (E(f, g) \setminus \{\varepsilon\}).$$

Proof. By Proposition 3.2, there exists $\alpha \in R$ that is a binary numeral base over R. Using the closure properties of rational series and Proposition 4.1, it follows that one can algorithmically construct a weighted automaton realising the series

$$r = f^{-1}(\Psi_\alpha) - g^{-1}(\Psi_\alpha) + 1$$

that satisfies $(r, \varepsilon) = 1$ and

$$(r, w) = \psi_\alpha(f(w)) - \psi_\alpha(g(w))$$

for all $w \in \Sigma^+$. By injectivity of ψ_α for a binary numeral base α, it follows that $(r, w) = 0$ if and only if w is a nonempty word such that $f(w) = g(w)$. The weighted automaton over R and Σ constructed for r can thus be taken for $\mathcal{A}_{f,g}(R)$. □

The possibility to algorithmically construct the automaton $\mathcal{A}_{f,g}(R)$ from the above theorem allows us to directly generalise several standard undecidability results for rational series over the integers [16, 17, 14] to rational series over an arbitrary integral domain R that is not locally finite.

Corollary 4.3. *Let R be an integral domain that is not locally finite. For a rational series r over R and some alphabet Σ, given by a weighted automaton, it is impossible to decide:*

(i) *Whether* $\mathrm{supp}(r) = \Sigma^*$.

(ii) *Whether there exists $w \in \Sigma^*$ such that $(r, w) = \beta$ for some fixed $\beta \in R$.*[7]

(iii) *Whether* $\mathrm{supp}(r)$ *is cofinite in* Σ^*.

(iv) *Whether* $\mathrm{supp}(r)$ *is rational.*

Moreover, all these problems are decidable over locally finite integral domains.

Proof. Consider an arbitrary Post's correspondence problem instance (Σ, f, g) and the corresponding weighted automaton $\mathcal{A}_{f,g}(R)$ over R and Σ that can be algorithmically constructed by Theorem 4.2. The instance (Σ, f, g) has a solution if and only if $E(f, g)$ contains a nonempty word, which happens if and only if $E(f, g)$ is infinite. Thus, by the property of $\mathcal{A}_{f,g}(R)$ described in Theorem 4.2, existence of a solution for (Σ, f, g) is further equivalent to universality and cofiniteness of $\mathrm{supp}(\|\mathcal{A}_{f,g}(R)\|)$ in Σ^*.

The problems *(i)* and *(iii)* are thus undecidable. Moreover, the problem *(ii)* can clearly be reduced to *(i)* by constructing an automaton for the series

$$r - \beta \cdot \mathbf{1}_{\Sigma^*}.$$

The problem *(ii)* is thus undecidable as well. Finally, rationality of $E(f, g)$ is known to be undecidable [18], while it is clearly equivalent to rationality of $\mathrm{supp}(\|\mathcal{A}_{f,g}(R)\|)$ – undecidability of *(iv)* is established as well.

On the other hand, it is well known that weighted automata over locally finite semirings – and thus also over locally finite integral domains – are determinisable using a generalised subset construction [15]. The first three problems can clearly be decided using the automaton resulting from this construction. Rationality of $\mathrm{supp}(r)$ is trivial over locally finite integral domains by Proposition 3.4 (and in fact for all locally finite semirings as well [13]). □

Note that using some suitable encoding, it is possible to reduce the undecidable problems from the above corollary to their counterparts, in which Σ is a fixed two-letter alphabet.[8] All four problems thus remain undecidable over binary alphabets.

The undecidability of *(iv)* for other than locally finite integral domains of positive characteristic affirmatively answers an open question of D. Kirsten and K. Quaas [14], who have asked whether there exists a semiring not containing $\mathbb{Z}$, for which the support rationality problem is undecidable.

Given undecidability of support rationality for rational series over other than locally finite integral domains, it is natural to ask whether it is possible to decide membership of the support of a given rational series to some other language classes. Similar methods as we have used for support rationality can sometimes be used to establish undecidability of such problems. For instance, A. Salomaa [18] has also proved that it is undecidable whether the equality set of a given PCP instance is context-free, implying undecidability for the membership of supports to the class of complements of context-free languages.

However, undecidability results for membership of PCP equality sets to language classes tend to be quite technical.[9] For this reason, we now better adopt a different approach to study decidability

[7] A slight modification of this problem, in which β is a part of the input, has been considered as the so-called $\exists$-*exact problem* for tropical automata by S. Almagor, U. Boker, and O. Kupferman [1]. The $\exists$-exact problem for weighted automata over other than locally finite integral domains is thus undecidable as well.

[8] For problems *(i)*, *(iii)*, and *(iv)*, this involves making sure that nonzero values are always assigned to invalid codewords; for problem *(ii)*, some value other than β has to be assigned to such words.

[9] For instance, already the proof of A. Salomaa [18] for context-free languages is much more involved than an obvious easy proof for the rational languages.

questions related to supports, generalising the one of D. Kirsten and K. Quaas [14].

In what follows, we prove a relatively general undecidability result, providing sufficient conditions under which it is impossible to decide whether the support of a rational series over an integral domain belongs to a language class $\mathscr{L}$. The following lemma is needed for the proof of this result.

Lemma 4.4. *Let $\mathbb{F}, \mathbb{K}$ be fields such that $\mathbb{K}$ is a finite extension of $\mathbb{F}$. Let $(\beta_1, \ldots, \beta_m)$ with $m \in \mathbb{N} \setminus \{0\}$ be a basis of $\mathbb{K}$ as a vector space over $\mathbb{F}$. Every rational series r over $\mathbb{K}$ then satisfies*

$$r = \sum_{k=1}^{m} \beta_k r_k$$

for some rational series $r_1, \ldots, r_m$ over $\mathbb{F}$.

Proof. Let $\mathcal{A} = (Q, \sigma, \iota, \tau)$ be a weighted automaton over $\mathbb{K}$ and alphabet Σ such that $\|\mathcal{A}\| = r$. Without loss of generality, let us assume that $\tau(q) \in \{0, 1\}$ for all $q \in Q$.

We now describe a construction of a weighted automaton $\mathcal{B} = (Q \times [m], \sigma', \iota', \tau')$ over $\mathbb{F}$, in which the definition of τ' is left unspecified. For every $q \in Q$, let $a_{q,1}, \ldots, a_{q,m}$ be the unique elements of $\mathbb{F}$ such that

$$\iota(q) = a_{q,1}\beta_1 + \ldots + a_{q,m}\beta_m,$$

and set

$$\iota'(q, \ell) = a_{q,\ell}$$

for $\ell = 1, \ldots, m$. Similarly, for each $p, q \in Q$, $c \in \Sigma$, and $k \in [m]$, let $b_{(p,c,q),k,1}, \ldots, b_{(p,c,q),k,m}$ be the unique elements of $\mathbb{F}$ such that

$$\sigma(p, c, q)\beta_k = b_{(p,c,q),k,1}\beta_1 + \ldots + b_{(p,c,q),k,m}\beta_m.$$

For all $(p, c, q) \in Q \times \Sigma \times Q$ and $k, \ell = 1, \ldots, m$, set

$$\sigma'\left((p, k), c, (q, \ell)\right) = b_{(p,c,q),k,\ell}.$$

We prove by induction on $|w|$ that for all $w \in \Sigma^*$,

$$(\|\mathcal{A}\|_q, w) = \sum_{\ell=1}^{m} \left(\|\mathcal{B}\|_{(q,\ell)}, w\right) \beta_\ell \qquad (1)$$

holds for every $q \in Q$. For $w = \varepsilon$, one has

$$(\|\mathcal{A}\|_q, \varepsilon) = \iota(q) = \sum_{\ell=1}^{m} a_{q,\ell}\beta_\ell = \sum_{\ell=1}^{m} \iota'(q, \ell)\beta_\ell = \sum_{\ell=1}^{m} \left(\|\mathcal{B}\|_{(q,\ell)}, \varepsilon\right) \beta_\ell.$$

For $x \in \Sigma^*$ and $c \in \Sigma$, the induction hypothesis gives us

$$\begin{aligned}
(\|\mathcal{A}\|_q, xc) &= \sum_{p \in Q} \sigma(p, c, q)\,(\|\mathcal{A}\|_p, x) = \\
&= \sum_{p \in Q} \sigma(p, c, q) \sum_{k=1}^{m} \left(\|\mathcal{B}\|_{(p,k)}, x\right) \beta_k = \\
&= \sum_{(p,k) \in Q \times [m]} \left(\|\mathcal{B}\|_{(p,k)}, x\right) \sigma(p, c, q)\beta_k = \\
&= \sum_{(p,k) \in Q \times [m]} \left(\|\mathcal{B}\|_{(p,k)}, x\right) \sum_{\ell=1}^{m} b_{(p,c,q),k,\ell}\beta_\ell = \\
&= \sum_{\ell=1}^{m} \beta_\ell \sum_{\overline{p} \in Q \times [m]} \sigma'\left(\overline{p}, c, (q, \ell)\right) (\|\mathcal{B}\|_{\overline{p}}, x) = \\
&= \sum_{\ell=1}^{m} \left(\|\mathcal{B}\|_{(q,\ell)}, xc\right) \beta_\ell,
\end{aligned}$$

finishing the proof of (1).

Finally, observe that (1) implies

$$\|\mathcal{A}\|_q = \sum_{k=1}^{m} \beta_k \|\mathcal{B}\|_{(q,k)}$$

for all $q \in Q$. Thus

$$\begin{aligned}
r = \|\mathcal{A}\| &= \sum_{\substack{q \in Q \\ \tau(q)=1}} \|\mathcal{A}\|_q = \\
&= \sum_{\substack{q \in Q \\ \tau(q)=1}} \sum_{k=1}^{m} \beta_k \|\mathcal{B}\|_{(q,k)} = \\
&= \sum_{k=1}^{m} \beta_k \sum_{\substack{q \in Q \\ \tau(q)=1}} \|\mathcal{B}\|_{(q,k)},
\end{aligned}$$

so that it suffices to set

$$r_k = \sum_{\substack{q \in Q \\ \tau(q)=1}} \|\mathcal{B}\|_{(q,k)}$$

for $k = 1, \ldots, m$. As $r_1, \ldots, r_m$ are clearly rational over $\mathbb{F}$, the lemma is proved. □

To prove Theorem 4.5 below, we need to recall the following property [19, Theorem III.2.2]: if R is an integral domain with fraction field $\mathbb{F}$ and r is a rational series over $\mathbb{F}$, then there exists a rational series s over R such that $\operatorname{supp}(s) = \operatorname{supp}(r)$. Indeed, let $\mathcal{A}$ be a weighted automaton over $\mathbb{F}$ such that $\|\mathcal{A}\| = r$. Write the weights of $\mathcal{A}$ as fractions of elements of R, and let M be the product of denominators of all these fractions. Then it is easy to see that

$$s = \sum_{w \in \Sigma^*} \left(M^{|w|+2}(r, w)\right)\, w$$

is a rational series over R satisfying $\operatorname{supp}(s) = \operatorname{supp}(r)$, and that a weighted automaton over R realising s can be algorithmically constructed from $\mathcal{A}$.

Theorem 4.5. *Let R be an integral domain that is not locally finite and $\mathscr{L}$ a class of languages such that the following three conditions hold:*

(i) *All rational languages are in $\mathscr{L}$.*

(ii) *The class $\mathscr{L}$ is closed under left quotients by words.*

(iii) *There exists a rational series r over R and some alphabet Γ such that* $\operatorname{supp}(r) \notin \mathscr{L}$.

Then it is impossible to decide whether the support of a rational series over R, given by a weighted automaton, is in $\mathscr{L}$.

Proof. Let $\mathbb{F}$ be the fraction field of R and $\mathbb{P}$ its prime subfield. Consider the series r from (iii), and let $\mathcal{A}$ be a weighted automaton over R such that $\|\mathcal{A}\| = r$. Then r is in particular rational over the subfield of $\mathbb{F}$ finitely generated by the weights of $\mathcal{A}$. This subfield can then be written as $\mathbb{P}(\alpha_1, \ldots, \alpha_n)(\alpha'_1, \ldots, \alpha'_t)$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ for $n \in \mathbb{N}$ form its transcendence basis over $\mathbb{P}$,[10] and where $\alpha'_1, \ldots, \alpha'_t$ for $t \in \mathbb{N}$ are algebraic over $\mathbb{P}(\alpha_1, \ldots, \alpha_n)$. Thus $\mathbb{P}(\alpha_1, \ldots, \alpha_n)(\alpha'_1, \ldots, \alpha'_t)$ is a finite extension of $\mathbb{P}(\alpha_1, \ldots, \alpha_n)$.

Let $(\beta_1, \ldots, \beta_m)$ with $m \in \mathbb{N} \setminus \{0\}$ and $\beta_1 = 1$ be a basis of $\mathbb{P}(\alpha_1, \ldots, \alpha_n)(\alpha'_1, \ldots, \alpha'_t)$ as a vector space over $\mathbb{P}(\alpha_1, \ldots, \alpha_n)$. By Lemma 4.4, there are rational series $r_1, \ldots, r_m$ over $\mathbb{P}(\alpha_1, \ldots, \alpha_n)$ such that

$$r = \sum_{k=1}^{m} \beta_k r_k.$$

Two cases can now be distinguished. When $n = 0$, the series r is rational over a finite algebraic extension of $\mathbb{P}$. As the support of r is not rational by (i), it follows by Proposition 3.4 that $\mathbb{P} = \mathbb{Q}$, so that R is of characteristic zero. The series $r_1, \ldots, r_m$ are thus rational over $\mathbb{Q}$. Now, apply the construction similar to the one from above the statement of this theorem: let M be the product of denominators of fractions appearing as weights in automata for $r_1, \ldots, r_m$; then

$$s = \sum_{w \in \Gamma^*} \left(M^{|w|+2}(r, w)\right)\, w$$

is a rational series over $\mathbb{F}$ with the same support as r, while it can be written as

$$s = \sum_{k=1}^{m} \beta_k s_k$$

for some series $s_1, \ldots, s_k$ rational over $\mathbb{Z}$.

When $n > 0$, write

$$\mathbb{P}(\alpha_1, \ldots, \alpha_n) = \mathbb{P}(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$$

and the same reasoning as above gives us existence of a rational series s' over $\mathbb{F}$ with the same support as r such that

$$s' = \sum_{k=1}^{m} \beta_k s'_k$$

for $s'_1, \ldots, s'_k$ rational over $\mathbb{P}(\alpha_1, \ldots, \alpha_{n-1})[\alpha_n]$.

Let us now consider an arbitrary PCP instance (Σ, f, g). If $n = 0$ – *i.e.*, R is necessarily of characteristic zero – it follows that 2 is a binary numeral base over R. As already observed in the proof of Theorem 4.2, the series

$$r_{f,g} = f^{-1}(\Psi_2) - g^{-1}(\Psi_2) + 1$$

satisfies $(r, w) = 0$ if and only if w is a nonempty word such that $f(w) = g(w)$. Moreover, for

$$C = \max\{|f(c)|, |g(c)| \mid c \in \Sigma\},$$

it is easy to see that

$$|(r_{f,g}, w)| \le 2^{C|w|+1}$$

for all $w \in \Sigma^*$. Let $\# \notin \Sigma \cup \Gamma$. The series

$$s_{f,g} = r_{f,g} \# \mathbf{1}_{\Gamma^*} + \left(\sum_{w \in \Sigma^*} 2^{C|w|+2}\, w\right) \# s$$

[10] In particular, α_k is transcendental over $\mathbb{P}(\alpha_1, \ldots, \alpha_{k-1})$ for $k = 1, \ldots, n$.

then satisfies $(s_{f,g}, x) = 0$ if and only if either $x \notin \Sigma^*\#\Gamma^*$, or $x = u\#v$, where $u \in \Sigma^+$ is a nonempty word such that $f(u) = g(u)$ and $v \in \Gamma^*$ is such that $(s, v) = (r, v) = 0$.

For $n > 0$, use the transcendental binary numeral base α_n and

$$r'_{f,g} = f^{-1}(\Psi_{\alpha_n}) - g^{-1}(\Psi_{\alpha_n}) + 1$$

instead. For C as above, we observe that $(r'_{f,g}, w)$ is a polynomial from $\mathbb{P}[\alpha_n] \subseteq \mathbb{P}(\alpha_1, \ldots, \alpha_{n-1})[\alpha_n]$ of degree at most $C|w|$ for all $w \in \Sigma^*$. It thus follows that for $\# \notin \Sigma \cup \Gamma$, the series

$$s'_{f,g} = r'_{f,g}\#\mathbf{1}_{\Gamma^*} + \left(\sum_{w \in \Sigma^*} \alpha_n^{C|w|+1}\, w\right)\#s'$$

again satisfies $(s'_{f,g}, x) = 0$ if and only if either $x \notin \Sigma^*\#\Gamma^*$, or $x = u\#v$, where $u \in \Sigma^+$ is a nonempty word such that $f(u) = g(u)$ and $v \in \Gamma^*$ is such that $(s', v) = (r, v) = 0$.

The series $s_{f,g}$ and $s'_{f,g}$ defined above are clearly rational over $\mathbb{F}$ and realised by automata algorithmically constructible from (Σ, f, g). By what has been said in the discussion preceding the statement of this theorem, in both cases it is possible to algorithmically construct a weighted automaton $\mathcal{B}$ over R such that $\mathrm{supp}(\|\mathcal{B}\|) = \mathrm{supp}(s_{f,g})$ or $\mathrm{supp}(\|\mathcal{B}\|) = \mathrm{supp}(s'_{f,g})$, respectively.

When (Σ, f, g) has no solution, the support of $\|\mathcal{B}\|$ equals $\Sigma^*\#\Gamma^*$ – this language is rational, and thus in $\mathscr{L}$ by (*i*). On the other hand, when (Σ, f, g) has a solution given by $w \in \Sigma^+$ such that $f(w) = g(w)$, then clearly

$$(w\#)^{-1}\,\mathrm{supp}(\|\mathcal{B}\|) = \mathrm{supp}(r) \notin \mathscr{L},$$

so that

$$\mathrm{supp}(\|\mathcal{B}\|) \notin \mathscr{L}$$

by our assumption (*ii*). As a result, PCP can be reduced to the problem of deciding whether the support of a rational series over R is in $\mathscr{L}$, implying that the latter problem is undecidable. □

As a consequence, we can now establish undecidability of support context-freeness for rational series over other than locally finite integral domains; it is easy to see that undecidability of support rationality, already established in Corollary 4.3, follows by Theorem 4.5 in the same way.

Corollary 4.6. *Let R be an integral domain that is not locally finite. Then it is impossible to decide, for a rational series r over R given by a weighted automaton, whether* $\mathrm{supp}(r)$ *is context-free.*

Proof. All rational languages are context-free and the class of all context-free languages is closed under left quotient by words. Moreover, we have seen in Proposition 3.4 that there is a rational series over R whose support is not context-free. The undecidability of support context-freeness for rational series over R thus follows by Theorem 4.5. □

Similarly as for Corollary 4.3, it is easy to see that the undecidability result of Corollary 4.6 actually already holds over a two-letter alphabet.

References

[1] S. Almagor, U. Boker, and O. Kupferman. What's decidable about weighted automata? *Information and Computation*, 282, 2022. Article 104651.

[2] J. Berstel and C. Reutenauer. *Noncommutative Rational Series with Applications*. Cambridge University Press, 2011.

[3] G. Chapuy and I. Klimann. On the supports of recognizable series over a field and a single letter alphabet. *Information Processing Letters*, 111(23–24):1096–1098, 2011.

[4] M. Droste, W. Kuich, and H. Vogler, editors. *Handbook of Weighted Automata*. Springer, 2009.

[5] M. Droste and D. Kuske. Weighted automata. In J.-É. Pin, editor, *Handbook of Automata Theory, Vol. 1*, chapter 4, pages 113–150. European Mathematical Society, 2021.

[6] D. S. Dummit and R. M. Foote. *Abstract Algebra*. John Wiley & Sons, 3rd edition, 2004.

[7] S. Eilenberg. *Automata, Languages, and Machines, Vol. A*. Academic Press, 1974.

[8] C. Frougny and J. Sakarovitch. Number representation and finite automata. In V. Berthé and M. Rigo, editors, *Combinatorics, Automata and Number Theory*, chapter 2, pages 49–122. Cambridge University Press, 2010.

[9] V. Halava. Decidable and undecidable problems in matrix theory. Technical report, Turku Centre for Computer Science, 1997. Available at `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.5792\&rep=rep1\&type=pdf`.

[10] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 1979.

[11] T. W. Hungerford. *Algebra*. Springer, New York, 1974.

[12] D. Kirsten. An algebraic characterization of semirings for which the support of every recognizable series is recognizable. In *Mathematical Foundations of Computer Science, MFCS 2009*, pages 489–500, 2009.

[13] D. Kirsten. An algebraic characterization of semirings for which the support of every recognizable series is recognizable. *Theoretical Computer Science*, 534:45–52, 2014.

[14] D. Kirsten and K. Quaas. Recognizability of the support of recognizable series over the semiring of the integers is undecidable. *Information Processing Letters*, 111(10):500–502, 2011.

[15] S. Lombardy and J. Sakarovitch. Sequential? *Theoretical Computer Science*, 356:224–244, 2006.

[16] J. Sakarovitch. *Elements of Automata Theory*. Cambridge University Press, 2009.

[17] J. Sakarovitch. Rational and recognisable power series. In M. Droste, W. Kuich, and H. Vogler, editors, *Handbook of Weighted Automata*, chapter 4, pages 105–174. Springer, 2009.

[18] A. Salomaa. Equality sets for homomorphisms of free monoids. *Acta Cybernetica*, 4(1):127–139, 1978.

[19] A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Springer, 1978.

[20] B. Steinberg. Is it decidable whether the support of a rational $\mathbb{Z}$-series is a regular language? MathOverflow. URL: `https://mathoverflow.net/q/139729` (version: 2013-08-27).