Tropical Semirings

Jean-Eric Pin

LITP/IBP, CNRS-Université Paris 7
2 Place Jussieu, 75251 Paris Cedex 05, FRANCE
`Jean-Eric.Pin@litp.ibp.fr`

1 Introduction

It is a well-known fact that the boolean calculus is one of the mathematical foundations of electronic computers. This explains the important role of the boolean semiring in computer science. The aim of this paper is to present other semirings that occur in theoretical computer science. These semirings were baptized *tropical semirings* by Dominique Perrin in honour of the pioneering work of our brazilian colleague and friend Imre Simon, but are also commonly known as (min, +)-semirings.

The aim of this paper is to present the tropical semirings and to survey a few problems relevant to them. We shall try to give an updated status of the different questions, but detailed solutions of most problems would be too long and technical for this survey. They can be found in the other papers of this volume or in the relevant literature. We tried to keep the paper self-contained as much as possible. Thus, in principle, there are no prerequisite to read this survey, besides a standard mathematical background. However, it was clearly not possible to give within 20 pages a full exposition of the theory of automata. Therefore, suitable references will be given for the readers who would like to elaborate and join the tropical community.

The paper is organized as follows. The main definitions are introduced in Section 2. Two apparently disconnected applications of the tropical semirings are presented: the Burnside type problems in group and semigroup theory, in Section 3 and decidability problems in formal language theory, in Section 4. The connection between the two problems is explained in Section 5. A conclusion section ends the paper.

2 Mathematical objects

This section is a short presentation of the basic concepts used in this paper.

2.1 Semigroups and monoids

A *semigroup* is a set equipped with an associative binary operation, usually denoted multiplicatively [11, 12, 24, 36]. Let S be a semigroup. An element 1 of S is an *identity* if, for all $s \in S$, $1s = s1 = s$. An element 0 of S is a *zero* if, for all $s \in S$, $0s = s0 = 0$. Clearly, a semigroup can have at most one identity, since, if 1 and $1'$ are two identities, then $11' = 1' = 1$. A *monoid* is a semigroup with identity. A semigroup S is commutative if, for every $s, t \in S$, $st = ts$. Given two semigroups S and T, a *semigroup morphism* $\varphi : S \to T$ is a map from S into T such that, for all $x, y \in S$, $\varphi(xy) = \varphi(x)\varphi(y)$. Monoid morphisms are defined analogously, but of course, the condition $\varphi(1) = 1$ is also required.

An *alphabet* is a finite set whose elements are *letters*. A *word* (over the alphabet A) is a finite sequence $u = (a_1, a_2, \ldots, a_n)$ of letters of A. The integer n is the *length* of the word and is denoted $|u|$. In practice, the notation $(a_1, a_2, \ldots, a_n)$ is shortened to $a_1a_2 \cdots a_n$. The empty word, which is the unique word of length 0, is denoted by 1. The (concatenation) *product* of two words $u = a_1a_2 \cdots a_p$ and $v = b_1b_2 \cdots b_q$ is the word $uv = a_1a_2 \cdots a_pb_1b_2 \cdots b_q$. The product is an associative operation on words. The set of all words on the alphabet A is denoted by A^*. Equipped with the product of words, it is a monoid, with the empty word as an identity. It is in fact the free monoid on the set A. This means that A^* satisfies the following universal property: if $\varphi : A \to M$ is a map from A into a monoid M, there exists a unique monoid morphism from A^* into M that extends φ. This morphism, also denoted φ, is simply defined by $\varphi(a_1 \cdots a_n) = \varphi(a_1) \cdots \varphi(a_n)$.

2.2 Semirings

A *semiring* is a set k equipped with two binary operations, denoted additively and multiplicatively, and containing two elements, the *zero* – denoted 0 – and the *unit* – denoted 1 – satisfying the following conditions

1. k is a commutative monoid for the addition, with the zero as identity
2. k is a monoid for the multiplication, with the unit as identity
3. Multiplication is distributive over addition :
   for all $s, t_1, t_2 \in k$, $s(t_1 + t_2) = st_1 + st_2$ and $(t_1 + t_2)s = t_1s + t_2s$
4. The zero is a zero for the second law :
   for all $s \in k$, $0s = s0 = 0$.

A semiring is *commutative* if its multiplication is commutative. Rings are the first examples of semirings that come to mind. In particular, we denote by $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, respectively, the rings of integers, rational and real numbers.

The simplest example of a semiring which is not a ring is the boolean semiring $\mathbb{B} = \{0, 1\}$ defined by $0 + 0 = 0$, $0 + 1 = 1 + 1 = 1 + 0 = 1$, $1.1 = 1$ and $1.0 = 0.0 = 0.1 = 0$. If M is a monoid, then the set $\mathbb{P}(M)$ of subsets of M is a commutative semiring with union as addition and multiplication given by

$$XY = \{xy \mid x \in X \text{ and } y \in Y\}$$

The empty set is the zero of this semiring and the unit is the singleton $\{1\}$. Other examples include the semiring of non negative integers $\mathbb{N} = (\mathbb{N}, +, \times)$ and its completion $\mathcal{N} = (\mathbb{N} \cup \{\infty\}, +, \times)$, where addition and multiplication are extended in the natural way

$$\begin{gathered}
\text{for all } x \in \mathcal{N},\ \ x + \infty = \infty + x = \infty \\
\text{for all } x \in \mathcal{N} \setminus \{0\},\ \ x \times \infty = \infty \times x = \infty \\
\infty \times 0 = 0 \times \infty = 0
\end{gathered}$$

The Min-Plus semiring is $\mathcal{M} = (\mathbb{N} \cup \{\infty\}, \min, +)$. This means that in this semiring the sum is defined as the minimum and the product as the usual addition. Note that ∞ is the zero of this semiring and 0 is its unit. This semiring was introduced by Simon [43] in the context of automata theory (it is also a familiar semiring in Operations Research). Similar semirings were considered in the literature. Mascle [32] introduced the semiring

$$\mathbb{P} = (\mathbb{N} \cup \{-\infty, \infty\}, \max, +)$$

where $-\infty + x = x + (-\infty) = -\infty$ for all x and Leung [25, 26] the semiring

$$\overline{\mathcal{M}} = (\mathbb{N} \cup \{\omega, \infty\}, \min, +)$$

where the minimum is defined with respect to the order

$$0 < 1 < 2 < \cdots < \omega < \infty$$

and addition of the Min-Plus semiring is completed by setting $x + \omega = \omega + x = \max\{x, \omega\}$ for all x. All these semirings are called *tropical semirings*. Other extensions include the tropical integers $\mathcal{Z} = (\mathbb{Z} \cup \{\infty\}, \min, +)$, the tropical rationals $\mathcal{Q} = (\mathbb{Q} \cup \{\infty\}, \min, +)$, the tropical reals $\mathcal{R} = (\mathbb{R} \cup \{\infty\}, \min, +)$. Mascle [31] also suggested to study the Min-Plus semiring of ordinals smaller than a given ordinal α : $\mathcal{M}_\alpha = (\{ordinals < \alpha\}, \min, +)$.

Quotients of $\mathcal{M}$ and $\mathcal{N}$ are also of interest. These quotients are

$$\begin{aligned}
\mathcal{N}_r &= \mathcal{N}/(r = \infty) &\qquad \mathcal{N}'_{r,p} &= \mathcal{N}/(r = r + p) \\
\mathcal{M}_r &= \mathcal{M}/(r = \infty) &\qquad \mathcal{M}'_r &= \mathcal{M}/(r = r + 1)
\end{aligned}$$

where $(r = s)$ denotes the coarsest semiring congruence such that r and s are equivalent.

2.3 Polynomials and Series

This subsection is inspired by the book of Berstel and Reutenauer [2], which is the standard reference on formal power series.

Let A be an alphabet and let k be a semiring. A *formal power series* over k with (non commutative) variables in A is a mapping s from A^* to k. The value of s on a word w is denoted (s, w). The *range* of s is the set of words w such that $(s, w) \neq 0$. A *polynomial* is a power series of finite range. The set of power series over k with variables in A is denoted $k\langle\langle A\rangle\rangle$. It is a semiring with addition defined by

$$(s + t, w) = (s, w) + (t, w)$$

and multiplication defined by

$$(st, w) = \sum_{uv=w} (s, u)(s, v)$$

The set of polynomials, denoted $k\langle A\rangle$, form a subsemiring of $k\langle\langle A\rangle\rangle$. If s is an element of k, one can identify s with the polynomial s defined by

$$(s, w) = \begin{cases} s & \text{if } w = 1 \\ 0 & \text{otherwise} \end{cases}$$

The semiring k can thus be identified to a subsemiring of $k\langle A\rangle$. Similarly, one can identify A^* to a subset of $k\langle A\rangle$ by attaching to each word v the polynomial v defined by

$$(v, w) = \begin{cases} 1 & \text{if } v = w \\ 0 & \text{otherwise} \end{cases}$$

A family of series $(s_i)_{i\in I}$ is *locally finite* if, for each $w \in A^*$, the set

$$I_w = \{i \in I \mid (s_i, w) \neq 0\}$$

is finite. In this case, the sum $s = \sum_{i\in I} s_i$ can be defined by

$$(s, w) = \sum_{i\in I_w} s_i$$

In particular, for every series s, the family of polynomials $\big((s, w)w\big)_{w\in A^*}$ is clearly locally finite and its sum is s. For this reason, a series is usually denoted by the formal sum

$$\sum_{w\in A^*} (s, w)w$$

If $(s, 1) = 0$, that is, if the value of s on the empty word is zero, then the family $(s^n)_{n\geq 0}$ is locally finite, since $(s^n, w) = 0$ for every $n > |w|$. Its sum is denoted s^* and is called the *star* of s. Thus

$$s^* = \sum_{n\geq 0} s^n$$

Note that if k is a ring, $s^* = (1-s)^{-1}$. Actually, the star often plays the role of the inverse, as in the following example. Consider the equation in X

$$X = t + sX \tag{2.1}$$

where s and t are series and $(s,1) = 0$. Then one can show that $X = ts^*$ is the unique solution of 2.1.

The set of *rational series* on k is the smallest subsemiring R of $k\langle\langle A\rangle\rangle$ containing $k\langle A\rangle$ and such that $s \in R$ implies $s^* \in R$. Note that if k is a ring, the rational series form the smallest subring of $k\langle\langle A\rangle\rangle$ containing $k\langle A\rangle$ and closed under inversion (whenever defined). In particular, in the one variable case, this definition coincide with the usual definition of rational series and justifies the terminology.

2.4 Rational sets

Given a monoid M, the semiring $\mathcal{P}(M)$ can be identified with $\mathbb{B}(M)$, the boolean algebra of the monoid M. Thus union will be denoted by $+$ and the empty set by 0. It is also convenient to denote simply by m any singleton $\{m\}$. In particular, 1 will denote the singleton $\{1\}$, which is also the unit of the semiring $\mathcal{P}(M)$.

Given a subset X of M, X^* denotes the submonoid of M generated by X. Note that

$$X^* = \sum_{n \geq 0} X^n$$

where X^n is defined by $X^0 = 1$ and $X^{n+1} = X^n X$. Thus our notation is consistent with the notation s^* used for power series. It is also consistent with the notation A^* used for the free monoid over A. The *rational subsets* of M form the smallest class $\mathcal{R}at(M)$ of subsets of M such that

1. the empty set and every singleton $\{m\}$ belong to $\mathcal{R}at(M)$,
2. if S and T are in $\mathcal{R}at(M)$, then so are ST and $S+T$,
3. if S is in $\mathcal{R}at(M)$, then so is S^*.

In particular, every finite subset and every finitely generated submonoid of M are rational sets.

The case of free monoids is of special interest. Subsets of a free monoid A^* are often called *languages*. According to the general definition, the rational languages form the smallest class of languages containing the finite languages and closed under union, product and star. A key result of the theory, which follows from a theorem of Kleene mentioned in the next section, is that rational languages are also closed under intersection and complement. A similar result holds for the rational subsets of a free group, but doesn't hold for the rational subsets of an arbitrary monoid.

Rational languages can be conveniently represented by *rational expressions*. Rational expressions on the alphabet A are defined recursively by the rules:

1. 0, 1 and a, for each $a \in A$ are rational expressions
2. if e and f are rational expressions, then so are e^*, (ef) and $(e+f)$.

For instance, if $a, b \in A$, $(a+ab)^*ab$ denotes the rational subset of A^* consisting of all elements of the form $a^{n_1}(ba)^{m_1}a^{n_2}(ba)^{m_2}\cdots a^{n_k}(ba)^{m_k}ab$, where $k \geq 0$ and $n_1, m_1, n_2, m_2, \ldots, n_k, m_k \geq 0$. It contains for instance the elements ab (take $k = 0$), $aaaab$ (take $k = 1$, $n_1 = 3$ and $m_1 = 0$) and $ababaaabaab$ (exercise !).

Two rational expressions e and f are *equivalent* ($e \equiv f$) if they denote the same rational language. For instance, if e and f are rational expressions, $e + e \equiv e$, $(e^*)^* \equiv e^*$ and $(e+f) \equiv (f+e)$, but there are much more subtle equivalences, such as $(e^*f)^*e^* \equiv (e+f)^*$. Actually, although there are known algorithms to decide whether two rational expressions are equivalent, there are no finite basis of identities of the type above that would generate all possible equivalences.

Let a^* be the free monoid on the one-letter alphabet $\{a\}$. One can show that for each rational subset R of a^*, there exist two integers i (the index) and p (the period) such that

$$R = F + G(a^p)^*$$

for some $F \subseteq \{1, a, \cdots, a^{i-1}\}$ and $G \subset \{a^i, \cdots a^{i+p-1}\}$. C. Choffrut observed that the rational sets of the form $a^n a^*$ (for $n \geq 0$) form a subsemiring of $\mathcal{R}at(a^*)$ isomorphic to $\mathcal{M}$, since $a^n a^* + a^m a^* = a^{\min\{n,m\}}a^*$ and $(a^n a^*)(a^m a^*) = a^{n+m}a^*$. Thus the tropical semiring embeds naturally into $\mathcal{R}at(a^*)$.

3 Burnside type problems

In 1902, Burnside proposed the following problem:

Is a finitely generated group satisfying an identity of the form $x^n = 1$ necessarily finite?

The answer is yes for $n = 1, 2, 3, 4$ and 6. The case $n \leq 2$ is trivial, the case $n = 3$ was settled by Burnside [7], the case $n = 4$ by Sanov [41] and the case $n = 6$ by M. Hall [14]. Although the original problem finally received a negative answer by Novikov-Adjan in 1968 [34] (see also [3]), several related questions were proposed. At the end of this century, Burnside type problems form a very active but extremely difficult research area, recently promoted by the Fields medal of the russian mathematician E.I. Zelmanov [52, 53, 54]. Burnside type problems can also be stated for semigroups and motivate the following definitions.

A semigroup S is *periodic* (or *torsion*) if, for all $s \in S$, the subsemigroup generated by s is finite. This means that, for every $s \in S$, there exists $n, p > 0$ such that $s^n = s^{n+p}$. A semigroup is *k-generated* if it is generated by a set of k elements. It is *finitely generated* if it is k-generated for some positive integer k.

A semigroup S is *locally finite* if every finitely generated subsemigroup of S is finite. It is *strongly locally finite* if there is an *order function* f such that the order of every k-generated subsemigroup of S is smaller than or equal to $f(k)$.

The general Burnside problem is the following:

Is every periodic semigroup locally finite ?

Morse and Hedlund [33] observed that the existence of an infinite square-free word over a three-letter alphabet [50, 51, 28] shows that the quotient of $A^* \cup \{0\}$ by the relations $x^2 = 0$ is infinite if $|A| \geq 3$. This semigroup satisfies the identity $x^2 = x^3$ and thus the answer is negative for semigroups. Actually, as shown in [6], the monoid presented by $\langle A \mid x^2 = x^3 \text{ for all } x \in A^* \rangle$ is infinite even if $|A| = 2$. Note that, however, the semigroup presented by $\langle A \mid x = x^2 \text{ for all } x \in A^* \rangle$ is always finite.

For groups, a negative answer was given by Golod in 1964 [13] (this follows also from the result of Novikov-Adjan mentioned above). On the positive side, Schur [42] gave a positive answer for groups of matrices over $\mathbb{C}$. Kaplansky [23] extended this result to groups of matrices over an arbitrary field and Procesi [39, 40] to groups of matrices over a commutative ring or even over a PI-ring, i.e. a ring satisfying a polynomial identity. McNaughton and Zalcstein [29] proved a similar result for semigroups of matrices over an arbitrary field. In the same paper, they announced but didn't prove a similar statement for semigroups of matrices over a commutative ring or even over a PI-ring. A complete proof of these results, which do not rely on the group case, was given by Straubing [49] in 1983.

What happens for semigroups of matrices over a commutative semiring ? The general question is still unsolved, but several particular instances of this problem occurred naturally in automata theory. Mandel and Simon [30] proved that every periodic semigroup of matrices over $\mathbb{N}$ or $\mathcal{N}$ is strongly locally finite. Then Simon [43] proved that every periodic semigroup of matrices over $\mathcal{M}$ is locally finite. This result was extended by Mascle [31] to semigroups of matrices over $\mathbb{P}$ and over $\mathcal{R}at(a^*)$.

One of the key results to study locally finite semigroups is Brown's theorem [4, 5].

Theorem 3.1 (Brown) *Let $\varphi : S \to T$ be a semigroup morphism. If T is locally finite and, for every idempotent $e \in T$, $\varphi^{-1}(e)$ is locally finite, then S is locally finite.*

A similar result for strongly locally finite semigroups was given by Straubing [49].

Theorem 3.2 (Straubing) *Let $\varphi : S \to T$ be a semigroup morphism. If T is strongly locally finite with order function f and if, for every idempotent $e \in T$, $\varphi^{-1}(e)$ is strongly locally finite with order function g (not depending on e), then S is strongly locally finite.*

Two other problems on semigroups of matrices over a semiring can also be considered as Burnside type problems:

Finiteness problem: *Given a finite set A of matrices, decide whether the semigroup S generated by A is finite or not.*

Finite section problem: *Given a finite set A of square matrices of size n and $i, j \in \{1, \ldots, n\}$, decide whether the set $\{s_{i,j} \mid s \in S\}$ is finite or not, where S denotes the semigroup generated by A.*

The finiteness problem is decidable for matrices over a field (Jacob [22]), over $\mathbb{N}$ and $\mathcal{N}$ (Mandel and Simon [30]), over $\mathcal{M}$ (Simon [43]), over $\mathbb{P}$ and $\mathcal{R}at(a^*)$ (Mascle[31, 32]). The finite section problem is decidable for matrices over a field (Jacob [22]), over $\mathbb{N}$ and $\mathcal{N}$ (Mandel and Simon [30]), over $\mathcal{M}$ (Hashiguchi [16, 20]). It is still an open problem for matrices over $\mathcal{R}at(a^*)$.

These problems were first considered by Hashiguchi [15, 16] and Simon [43, 44] in connection with decidability problems on rational languages presented in the next section.

4 Problems on rational languages

The *star height* of a rational expression, as defined by Eggan [10], counts the number of nested uses of the star operation. It is defined inductively as follows:

1. The star height of the basic languages is 0. Formally

$$h(0) = 0 \qquad h(1) = 0 \quad \text{and} \quad h(a) = 0 \text{ for every letter } a$$

2. Union and product do not affect star height. If e and f are two rational expressions, then

$$h(e + f) = h(ef) = \max\{h(e), h(f)\}$$

3. Star increases star height. For each rational expression e,

$$h(e^*) = h(e) + 1$$

For instance

$$\Big((a^* + ba^*)^* + (b^*ab^*)^*\Big)^*(b^*a^* + b)^*$$

is a rational expression of star height 3. Now, the *star height* of a recognizable language L is the minimum of the star heights of the rational expressions representing L

$$h(L) = \min\{h(e) \mid \ e \text{ is an rational expression for } L \ \}$$

The difficulty in computing the star height is that a given language can be represented in many different ways by a rational expression !

An explicit example of language of star-height n was given by Dejean and Schützenberger [9]. Given a word $u \in A^*$ and a letter $a \in A$, denote by $|u|_a$ the number of occurrences of a in u. For instance, if $u = abbabba$, $|u|_a = 3$ and $|u|_b = 4$. Let $A = \{a, b\}$ and let

$$L_n = \{u \in A^* \ \Big| \ |u|_a \equiv |u|_b \bmod 2^{n-1}\}$$

Theorem 4.1 (Dejean and Schützenberger) *For each $n \geq 1$, the language L_n is of star height n.*

It is easy to see that the languages of star height 0 are the finite languages, but the effective characterization of the other levels was left open for several years until Hashiguchi first settled the problem for star height 1 [17] and a few years later for the general case [19].

Theorem 4.2 (Hashiguchi) *There is an algorithm to determine the star height of a given rational language.*

Hashiguchi's solution for star height one is now well understood, and deeply relies on the solution of the finite section problem for matrices over $\mathcal{M}$. Hashiguchi's solution for arbitrary star height relies on a complicated induction, which makes the proof very difficult to follow. Let us mention another problem, the solution of which had a great influence on the theory and ultimately led to the solution of the star-height problem.

A language L has the *finite power property* (FPP for short) if there exists an integer k such that

$$X^* = 1 + X + X^2 + \cdots + X^k$$

This means that X^* is actually a polynomial in X and in particular $h(X^*) = h(X)$. For instance, $X = a^* + (a+b)^*b$ has the FPP, since $X^* = A^* = 1 + X + X^2$, but $X = a^*(1+b)$ does not. In 1966, Brzozowski proposed the following problem

FPP problem: *Decide whether a given rational language has FPP.*

A solution was given independently by Simon [43] and Hashiguchi [15]. Simon's proof reduces the problem to the finiteness problem of matrices over $\mathcal{M}$. This reduction will be outlined in section 6.

To conclude this section, let us mention yet another problem on rational languages. Let $\mathcal{R}$ be a set of languages. A language L belongs to the *polynomial closure of* $\mathcal{R}$ if it is a finite union of products of languages of $\mathcal{R}$. For instance, if $\mathcal{R} = \{R_1, R_2\}$ then $R_1 + R_2R_1R_2 + R_2R_2$ belongs to the polynomial closure of $\mathcal{R}$. The following problem was proposed by Hashiguchi [18]

Polynomial closure problem: *Given a finite set $\mathcal{R}$ of rational languages and a rational language R, decide whether R belongs to the polynomial closure of $\mathcal{R}$?*

Note that the FPP problem is a particular instance of this problem. Indeed, the FPP problem amounts to know whether, given a rational language L, L^* belongs to the polynomial closure of the set $\{1, L\}$. It was shown by Hashiguchi [18] that the polynomial closure problem reduces to the finite section problem for matrices over $\mathcal{M}$ and is therefore decidable. See also [37] for a survey.

A little introduction to finite automata and formal languages is in order to explain the connection between the the FPP problem and the Burnside type problems of Section 3.

5 Finite automata and recognizable sets

This section is a brief introduction to the theory of finite automata. A more extensive presentation can be found in [11, 35, 36, 38].

5.1 Finite automata

A *finite (nondeterministic) automaton* is a quintuple $\mathcal{A} = (Q, A, E, I, F)$ where Q is a finite set (the set of *states*), A is an alphabet, E is a subset of $Q \times A \times Q$, called the set of *edges* (also called *transitions*) and I and F

are subsets of Q, called the set of *initial* and *final* states, respectively. Two edges (p, a, q) and (p', a', q') are *consecutive* if $q = p'$. A *path* in $\mathcal{A}$ is a finite sequence of consecutive edges

$$e_0 = (q_0, a_0, q_1), \quad e_1 = (q_1, a_1, q_2), \quad \ldots \quad , \quad e_{n-1} = (q_{n-1}, a_{n-1}, q_n)$$

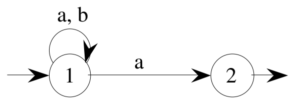
also denoted

$$q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \quad \cdots \quad q_{n-1} \xrightarrow{a_{n-1}} q_n$$

The state q_0 is the *origin* of the path, the state q_n is its *end*, and the word $x = a_0 a_1 \cdots a_{n-1}$ is its *label*. It is convenient to have also, for each state q, an empty path of label 1 from q to q. A path in $\mathcal{A}$ is *successful* if its origin is in I and its end is in F.

The language *recognized* by $\mathcal{A}$ is the set, denoted $|\mathcal{A}|$, of the labels of all successful paths of $\mathcal{A}$. A language X is *recognizable* if there exists a finite automaton $\mathcal{A}$ such that $X = |\mathcal{A}|$. Two automata are said to be *equivalent* if they recognize the same language. Automata are conveniently represented by labeled graphs, as in the example below. Incoming arrows indicate initial states and outgoing arrows indicate final states.

Example. Let $\mathcal{A} = (\{1, 2\}, \{a, b\}, E, \{1\}, \{2\})$ be an automaton, with $E = \{(1, a, 1), (1, b, 1), (1, a, 2)\}$. The path $(1, a, 1)(1, b, 1)(1, a, 2)$ is a successful path of label aba. The path $(1, a, 1)(1, b, 1)(1, a, 1)$ has the same label but is unsuccessful since its end is 1.



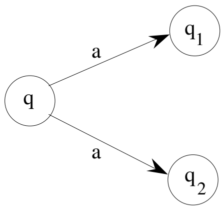
An automaton.

The set of words accepted by $\mathcal{A}$ is $|\mathcal{A}| = A^*a$, the set of all words ending with an a.

Kleene's theorem states the equivalence between automata and rational expressions. Its proof can be found in most books of automata theory [11, 21].

Theorem 5.1 (Kleene) *A language is rational if and only if it is recognizable.*

An automaton is *deterministic* if it has exactly one initial state, usually denoted q_0 and if E contains no pair of edges of the form $(q, a, q_1), (q, a, q_2)$ with $q_1 \neq q_2$.



The forbidden pattern in a deterministic automaton.

In this case, each letter a defines a partial function from Q to Q, which associates with every state q the unique state qa, if it exists, such that $(q, a, qa) \in E$. This can be extended into a right action of A^* on Q by setting, for every $q \in Q$, $a \in A$ and $u \in A^*$:

$$q1 = q$$
$$q(ua) = \begin{cases} (qu)a & \text{if } qu \text{ and } (qu)a \text{ are defined} \\ \text{undefined} & \text{otherwise} \end{cases}$$

Then the language accepted by $\mathcal{A}$ is

$$|\mathcal{A}| = \{u \in A^* \mid q_0 u \in F\}$$

One can show that every finite automaton is equivalent to a deterministic one. This result has an important consequence.

Corollary 5.1 *Recognizable languages are closed under union, intersection and complementation.*

States which cannot be reached from the initial state or from which one cannot access to any final state are clearly useless. This leads to the following definition. A deterministic automaton $\mathcal{A} = (Q, A, E, q_0, F)$ is *trim* if for every state $q \in Q$ there exist two words u and v such that $q_0 u = q$ and $qv \in F$. It is not difficult to see that every deterministic automaton is equivalent to a trim one.

Let $\mathcal{A} = (Q, A, E, q_0, F)$ and $\mathcal{A}' = (Q', A, E', q'_0, F')$ be two deterministic automata. A *covering* from $\mathcal{A}$ onto $\mathcal{A}'$ is a surjective function $\varphi : Q \to Q'$ such that $\varphi(q_0) = q'_0$, $\varphi^{-1}(F') = F$ and, for every $u \in A^*$ and $q \in Q$, $\varphi(qu) = \varphi(q)u$. We denote $\mathcal{A}' \leq \mathcal{A}$ if there exists a covering from $\mathcal{A}$ onto $\mathcal{A}'$. This defines a partial order on deterministic automata. One can show that, amongst the trim deterministic automata recognizing a given recognizable language L, there is a minimal one for this partial order. This automaton is called the *minimal automaton* of L. Again, there are standard algorithms for minimizing a given finite automaton [21].

5.2 Transducers

The modelling power of finite automata can be enriched by adding an output function [1, 11]. Let k be a semiring. The definition of a *k-transducer* (or *automaton with output in k*) is quite similar to that of a finite automaton. It is also a quintuple $\mathcal{A} = (Q, A, E, I, F)$, where Q (resp. I, F) is the set of states (resp. initial and final states) and A is the alphabet. But the set of edges E, instead of being a subset of $Q \times A \times Q$ is a finite subset of $Q \times A \times k \times Q$. An edge $(q, a, x, q') \in Q \times A \times k \times Q$ is graphically represented as follows

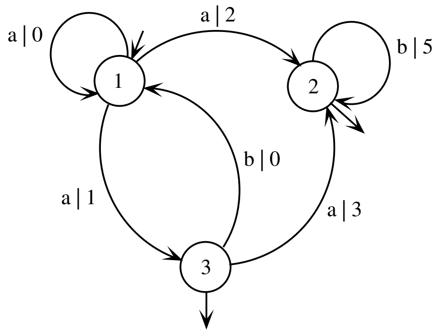
$$q \xrightarrow{a \mid x} q'$$

The *output* of a path

$$q_0 \xrightarrow{a_1 \mid x_1} q_1 \xrightarrow{a_2 \mid x_2} q_2 \ \cdots \ \xrightarrow{a_k \mid x_k} q_k$$

is the product $x_1 x_2 \cdots x_k$. The output $||\mathcal{A}||w$ of a word w is the sum of the outputs of all successful paths of label w. If there is no successful path of label w the output is 0[1]. This defines a function $||\mathcal{A}||$ from A^* into k, called the *output function* of $\mathcal{A}$.

Example. Let $k = \mathcal{M}$ and let $\mathcal{A} = (\{1,2,3\}, \{a,b\}, E, \{1\}, \{2,3\})$, with $E = \{(1,a,0,1), (1,a,2,2), (2,b,5,2), (1,a,1,3), (3,b,0,1), (3,a,3,2)\}$.



An automaton with output.

The label of the path $1 \xrightarrow{a \mid 1} 3 \xrightarrow{b \mid 0} 1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 2} 2 \xrightarrow{b \mid 5} 2$ is 8. There are three successful paths of label aaa :

$$1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 2} 2, \ 1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 1} 3 \text{ and } 1 \xrightarrow{a \mid 0} 1 \xrightarrow{a \mid 1} 3 \xrightarrow{a \mid 3} 2$$

Therefore the output of aaa is $||\mathcal{A}||(aaa) = \min\ \{2, 1, 4\} = 1$.

5.3 Matrix representation

It is convenient to compute the output function by using matrices. Let $\mathcal{A} = (Q, A, E, I, F)$ be a k-transducer. The set $M_Q k$ of $Q \times Q$ matrices over the semiring k form a semiring for the usual addition and multiplication of matrices, defined by

$$\begin{aligned}(m + m')_{p,q} &= m_{p,q} + m'_{p,q} \\ (mm')_{p,q} &= \textstyle\sum_{r \in Q} m_{p,r} m'_{r,q}\end{aligned}$$

[1]This is consistent with the standard convention $\sum_{i \in \emptyset} x_i = 0$

Define a monoid morphism $\mu : A^* \to M_Q k$ by setting, for each $a \in A$,

$$\mu(a)_{p,q} = \sum_{(p,a,x,q) \in E} x$$

where, according to a standard convention, $\sum_{x \in \emptyset} = 0$. Finally, let λ be the row matrix defined by

$$\lambda_q = \begin{cases} 1 & \text{if } q \in I \\ 0 & \text{otherwise} \end{cases}$$

and let ν be the column matrix defined by

$$\nu_q = \begin{cases} 1 & \text{if } q \in F \\ 0 & \text{otherwise} \end{cases}$$

Then the output function is computed by the following fundamental formula

$$||\mathcal{A}||w = \lambda\mu(w)\nu$$

Example. The matrix representation of the transducer of example 5.2 is given by[2]

$$\mu(a) = \begin{pmatrix} 0 & 2 & 1 \\ \infty & \infty & \infty \\ \infty & 3 & \infty \end{pmatrix} \qquad \mu(b) = \begin{pmatrix} \infty & \infty & \infty \\ \infty & 5 & \infty \\ 0 & \infty & \infty \end{pmatrix}$$

Therefore

$$\mu(aaa) = \begin{pmatrix} 0 & 2 & 1 \\ \infty & \infty & \infty \\ \infty & \infty & \infty \end{pmatrix}$$

The vectors λ and ν are given by

$$\lambda = \begin{pmatrix} 0 & \infty & \infty \end{pmatrix} \qquad \nu = \begin{pmatrix} \infty \\ 0 \\ 0 \end{pmatrix}$$

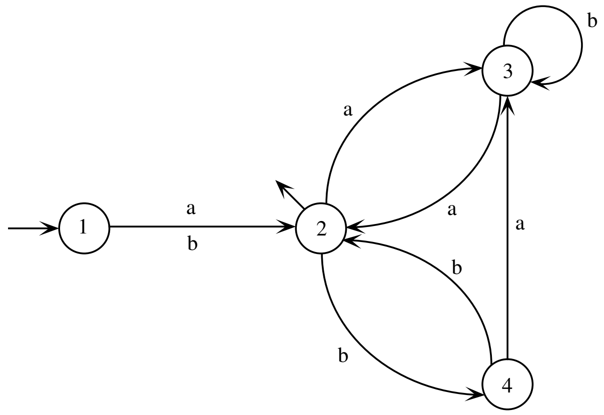
Thus the output of aaa, given by $\lambda\mu(aaa)\nu$, is equal to

$$\begin{pmatrix} 0 & \infty & \infty \end{pmatrix} \begin{pmatrix} 0 & 2 & 1 \\ \infty & \infty & \infty \\ \infty & \infty & \infty \end{pmatrix} \begin{pmatrix} \infty \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 \end{pmatrix} \begin{pmatrix} \infty \\ 0 \\ 0 \end{pmatrix} = 1$$

[2]The slight ambiguity on the role of the symbol 0 may confuse the reader. Here the semiring is the tropical semiring, its zero is ∞ and its unit is 0.

6 Reduction of the FPP problem

In this section, we briefly outline the reduction of the FPP problem to the finiteness problem for semigroup of matrices over $\mathcal{M}$. Since a language L has FPP if and only if $(L \setminus \{1\})^*$ has FPP, one may assume that L does not contain the empty word. Next, by a simple construction, left to the reader, one may assume that L is recognized by an automaton $\mathcal{A} = (Q, A, E, \{1\}, F)$ with a unique initial state 1 and no edge arriving on this initial state, as in the example below:

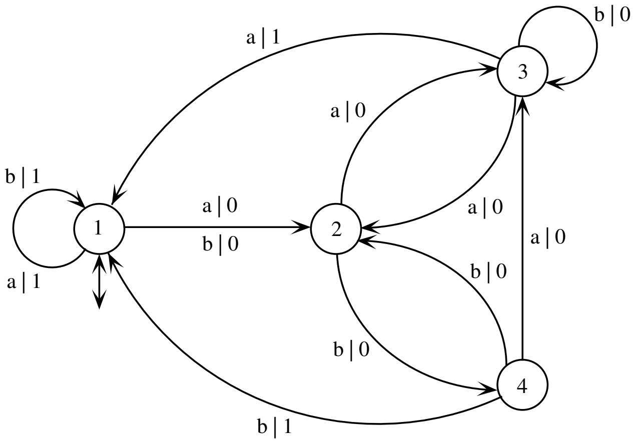


The automaton $\mathcal{A}$.

We claim that an automaton $\mathcal{A}'$ recognizing L^* is obtained by taking 1 as the unique final state and by adding an edge $(s, a, 1)$ for each edge $(s, a, q) \in E$ such that $a \in A$ and $q \in F$. On our example, one would add the edges $(1, a, 1)$, $(1, b, 1)$, $(3, a, 1)$ and $(4, a, 1)$. Let us first verify that every word of L^* is accepted by $\mathcal{A}'$. A word of L^* is a product $u = u_1 \cdots u_k$ of words of L. Since $\mathcal{A}$ does not accept the empty word, each u_i's is the label of some non empty successful path p_i, whose last edge reaches a final state. Replace this last edge (s, a, q), with $q \in F$, by $(s, a, 1)$. One gets a path p'_i from 1 to 1 and the product $p'_1 \cdots p'_k$ is a successful path of label u. Therefore u is accepted by $\mathcal{A}'$.

Conversely, every successful path can be factorized as a product of elementary paths around 1. Necessarily, the last edge of such an elementary path is one of the new edges $(s, a, 1)$ of $\mathcal{A}'$. Thus there is an edge of the form (s, a, q) such that $q \in F$. Therefore the label of the elementary path belongs to L and the label of the full path to L^*. Thus $\mathcal{A}'$ recognizes exactly L^*.

Actually, the previous argument shows that a word belongs to L^k if and only it is the label of a path of $\mathcal{A}'$ containing exactly k new edges. Therefore, one can convert $\mathcal{A}'$ into a $\mathcal{M}$-transducer whose output on a word $u \in L^*$ is the smallest k such that $u \in L^k$. It suffices to have an output 0 on the edges of $\mathcal{A}$ and output 1 on the new edges. This can be interpreted as a cost to pay to go back to the initial state. On our example, one obtains the following transducer



The automaton $\mathcal{B}$.

Now, $||\mathcal{B}||w$ is exactly the least k such that $w \in L^k$ if $w \in L^*$ and ∞ otherwise. Thus L has FPP if and only if the image of the function $||\mathcal{B}||$ is finite. Now, since $||\mathcal{B}||w = \lambda\mu(w)\nu = \mu_{1,1}(w)$, the equivalence of the two first conditions of the following statement has been established.

Theorem 6.1 *Let $\mathcal{A}$ be a finite automaton and L be the language recognized by $\mathcal{A}$. The following conditions are equivalent:*

1. *L has FPP,*
2. *the associated semigroup of matrices has a finite section in* $(1, 1)$*,*
3. *the associated semigroup of matrices is finite.*

The equivalence with the third condition is left as an exercise to the reader. It follows from the fact that all edges with output 1 arrive in state 1.

7 Conclusion

The examples presented in this paper do not exhaust the problems on semigroups or languages connected with tropical semirings and the reader is invited to read the literature on this domain, in particular the recent article of Simon [48]. Roughly speaking, tropical semirings provide an algebraic setting to decide whether a collection of objects is finite or infinite. But, as illustrated on the FPP problem, it is usually a non trivial task to reduce a given problem to a proper algebraic formulation.

References

[1] J. Berstel, 1979, *Transductions and Context-Free Languages*, Teubner, Stuttgart.

[2] J. Berstel and C. Reutenauer, 1984, *Les Séries Rationnelles et leurs Langages*, Masson. English edition, 1988 *Rational Series and Their Languages*, Springer-Verlag, Berlin.

[3] J.L. Britton, the existence of infinite Burnside groups, in *W.W. Boone, F.B. Cannonito, R.C. Lyndon (ed.), Word problems*, North Holland, 67–348.

[4] T. C. Brown (1969), On Van der Waerden's theorem on arithmetic progressions, *Notices Amer. Math. Soc.* **16**, 245.

[5] T. C. Brown (1971), An interesting combinatorial method in the theory of locally finite semigroups, *Pacific J. Math.* **36**, 285–289.

[6] J. A. Brzozowski, K. Čulik II and A. Gabrielian (1971), Classification of noncounting events, *J. Comput. Syst. Sci.* **5**, 41–53.

[7] W. Burnside (1902), On an unsettled question in the theory of discontinuous groups, *Q. J. Pure Appl. Math.* **33**, 230–238.

[8] Chan and Ibarra (1983), On the Finite-Valuedness Problem for Sequential Machines, *Theoretical Comput. Sci.* **23** , 95–101.

[9] F. Dejean and M. P. Schützenberger (1966), On a question of Eggan, *Information and Control* **9**, 23–25.

[10] L. C. Eggan, Transition graphs and the star height of regular events, *Michigan Math. J.* **10**, (1963) 385–397.

[11] S. Eilenberg, *Automata, languages and machines*, Vol. A, Academic Press, New York (1974).

[12] S. Eilenberg, *Automata, languages and machines*, Vol. B, Academic Press, New York (1976).

[13] E.S. Golod (1964), On nil algebras and finitely approximable groups, Izv. Acad. Nauk. SSSR Ser. Matem. **28**, 273–276.

[14] M. Hall Jr. (1957), Solution of the Burnside problem for exponent 6, *Proceedings Nat. Acad. Sci. USA*, **43**, 751–753.

[15] K. Hashiguchi (1979), A Decision Procedure for the Order of Regular Events, *Theoretical Comput. Sci.* **8**, 69–72.

[16] K. Hashiguchi (1982), Limitedness Theorem on Finite Automata with Distance Functions, *J. Comput. System Sci.* **24**, 233–244.

[17] K. Hashiguchi (1982), Regular languages of star height one, *Information and Control* **53** 199–210.

[18] K. Hashiguchi (1983), Representation theorems on regular languages, *J. Comput. System Sci.* **27**, 101–115.

[19] K. Hashiguchi (1988), Algorithms for Determining Relative Star Height and Star Height, *Information and Computation* **78**, 124–169.

[20] K. Hashiguchi (1990), Improved limitedness theorems on finite automata with distance functions *Theoretical Comput. Sci.* **72**, ???–???.

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

[22] G. Jacob (1978), La finitude des représentations linéaires de semi-groupes est decidable, *Journal of Algebra* **52**, 437–459.

[23] I. Kaplansky, 1965, Fields and rings, University of Chicago.

[24] G. Lallement, (1979), *Semigroups and combinatorial applications*, Wiley, New York.

[25] H. Leung (1987), *An algebraic method for solving decision problems in finite automata theory*, PhD thesis, Department of Computer Science, The Pennsylvania State University.

[26] H. Leung (1988), On the topological structure of a finitely generated semigroup of matrices, *Semigroup Forum* **37**, 273–287.

[27] M. Linna (1973), Finite Power Property of Regular Languages, in *Automata, Languages and Programming*, M. Nivat (ed.), North Holland Pu. Co., Amsterdam, 87–98.

[28] M. Lothaire (1983), *Combinatorics on Words*, Encyclopedia of Mathematics and its Applications **17**, Addison Wesley.

[29] R. McNaughton and Y. Zalcstein (1975), The Burnside problem for semigroups, *J. of Algebra* **34**, 292–299.

[30] A. Mandel and I. Simon (1977), On finite semigroups of matrices, *Theoretical Comput. Sci.* **5**, 101–112.

[31] J.P. Mascle, (1985), Quelques résultats de décidabilité sur la finitude des semigroupes de matrices, LITP Report 85–50.

[32] J.P. Mascle, (1986), Torsion Matrix Semigroups and Recognizable Transductions, in *Automata, Languages and Programming, L. Kott ed., Lecture Notes in Computer Science* **226**, 244–253.

[33] M. Morse and G. Hedlund (1944), Unending chess, symbolic dynamics and a problem in semigroups, *Duke Math. J.* **11**, 1–7.

[34] P.S. Novikov and S.I. Adian (1968), On infinite periodic groups, I, II, III, Izv. Acad. Nauk. SSSR Ser. Matem. **32**, 212–244, 251–524, 709–731.

[35] D. Perrin (1990), *Automata*, Chapter 1 in Handbook of Theoretical Computer Science (Van Leeuwen, J. ed.), Vol B: Formal Models and Semantics, Elsevier.

[36] J.-E. Pin (1984), *Variétés de langages formels*, Masson, Paris; English translation: (1986), *Varieties of formal languages*, Plenum, New-York.

[37] J.-E. Pin (1990), Rational and recognizable langages, in *Lectures in applied mathematics and informatics*, Ricciardi (éd.), Manchester University Press, 62–106.

[38] J.-E. Pin (1993), Finite semigroups and recognizable languages : an introduction, in *NATO Advanced Study Institute Semigroups, Formal Languages and Groups*, J. Fountain et V. Gould (éd.), Kluwer academic publishers, to appear.

[39] C. Procesi (1966), The Burnside problem, *J. of Algebra* **4**, 421–425.

[40] C. Procesi (1973), *Rings with polynomial identities*, Marcel Dekker.

[41] I.N. Sanov (1940), Solution of the Burnside problem for exponent 4, *Uch. Zapiski Leningrad State University, Ser. Matem.* **10**, 166–170.

[42] I. Schur (1911), Über Gruppen periodischer Substitutionen, Sitzungsber. Preuss. Akad. Wiss., 619–627.

[43] I. Simon (1978), Limited Subsets of a Free Monoid, in *Proc. 19th Annual Symposium on Foundations of Computer Science*, Piscataway, N.J., Institute of Electrical and Electronics Engineers, 143–150.

[44] I. Simon (1988) Recognizable Sets with Multiplicities in the Tropical Semiring, in *Mathematical Foundations of Computer Science, Chytil, Janiga et Koubek (ed.), Lecture Notes in Computer Science* **324**, Springer Verlag, Berlin, 107–120.

[45] I. Simon (1990), Factorization Forests of Finite Height, *Theoretical Comput. Sci.* **72**, 65–94.

[46] I. Simon (1990), The nondeterministic complexity of a finite automaton, in *Mots - mélanges offerts à M.P. Schützenberger*, M. Lothaire (ed.), Hermes, Paris, 384–400.

[47] I. Simon (1993), The product of rational languages, *Proceedings of ICALP 1993, Lecture Notes in Computer Science* **700**, 430–444.

[48] I. Simon (1994), On semigroups of matrices over the tropical semiring, *Informatique Théorique et Applications* **28**, 277–294.

[49] H. Straubing (1983), The Burnside problem for semigroups of matrices, in *Combinatorics on Words, Progress and Perspectives, L.J. Cummings (ed.)*, Acad. Press, 279–295.

[50] A. Thue (1906), Über unendliche Zeichenreihen, *Norske Vid. Selsk. Skr. I. Math. Nat. Kl.*, Christiana **7**, 1–22.

[51] A. Thue (1912), Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen, *Norske Vid. Selsk. Skr. I. Math. Nat. Kl.*, Christiana **1**, 1–67.

[52] E.I. Zelmanov (1990), The solution of the restricted Burnside problem for groups of odd exponent, Izvestia Akad. Nauk SSSR **54**.

[53] E.I. Zelmanov (1991), The solution of the restricted Burnside problem for 2-groups, Math. Sbornik **182**.

[54] E.I. Zelmanov (1993), On additional laws in the Burnside problem on periodic groups, *International Journal of Algebra and Computation* **3**, 583–600.