

# Algebraic characterization of the finite power property

Michal Kunc \*

Department of Mathematics, University of Turku, and  
Turku Centre for Computer Science, FIN-20014 Turku, Finland,  
kunc@math.muni.cz, <http://www.math.muni.cz/~kunc/>

**Abstract.** We give a transparent characterization, by means of a certain syntactic semigroup, of regular languages possessing the finite power property. Then we use this characterization to obtain a short elementary proof for the uniform decidability of the finite power property for rational languages in all monoids defined by a confluent regular system of deletion rules. This result in particular covers the case of free groups solved earlier by d'Alessandro and Sakarovitch by means of an involved reduction to the boundedness problem for distance automata.

## 1 Introduction

A language  $L$  is said to have the finite power property if its iteration  $L^+$  is a union of finitely many powers of  $L$ . The problem to algorithmically determine whether a given regular language possesses the finite power property is one of the most prominent questions in the theory of regular languages. It was formulated by Brzowski during the SWAT conference in 1966, and solved independently by Hashiguchi [4] and Simon [13] more than ten years later. Results on this problem were the starting point of a fruitful and still active research, leading in particular to Hashiguchi's solution of the star-height problem [6]. The approach of Simon initiated the development of the theory of automata with multiplicities over the tropical semiring, which is now a standard method of dealing with problems related to the product operation on regular languages (see [14] for a survey).

On the other hand, the approach of Hashiguchi is combinatorial: he works directly with an automaton for the given language and uses an argument based on the pigeon hole principle. Our solution of the problem can be viewed as uncovering the algebraic background of Hashiguchi's arguments. First steps in this direction were already performed by Kirsten [8]. Here we present a fully algebraic treatment of this technique, and we formulate a simple and easily verifiable algebraic condition on a certain syntactic semigroup, which is equivalent to the finite power property. This approach also allows us to slightly generalize the result to all monoids where length of elements can be well defined and where every two factorizations of any element have a common refinement. These two properties

---

\* Supported by the Academy of Finland under grant 208414.

are sufficient for the two main arguments of the proof: induction on the length of elements and localization of the problem to regular  $\mathcal{J}$ -classes, respectively.

Then we show that deciding the finite power property for rational languages in finitely generated monoids where the word problem is solved by a confluent regular system of deletions, can be uniformly reduced to monoids where the first result can be applied. More precisely, for every rational language in such a monoid we construct a different monoid according to the behaviour of deletions with respect to this language. Note that free groups can be defined by a confluent finite rewriting system consisting of the deletion rules  $aa^{-1} \rightarrow \varepsilon$  and  $a^{-1}a \rightarrow \varepsilon$ , for each of the free generators  $a$ . Therefore, our result generalizes the decidability result for free groups of d'Alessandro and Sakarovitch [3], who follow the usual approach and reduce the problem to testing whether a distance automaton is bounded, which is decidable due to a difficult result of Hashiguchi [5].

Basic concepts employed in this paper are recalled in the following section. For a more comprehensive introduction to semigroup theory, formal languages, rational transductions and rewriting we refer the reader to [7], [11], [1] and [2], respectively.

## 2 Preliminaries

The sets of positive and non-negative integers are denoted by  $\mathbb{N}$  and  $\mathbb{N}_0$ , respectively. For any set  $S$ , the notation  $\wp(S)$  stands for the set of all subsets of  $S$ . As usual, we denote by  $A^+$  the semigroup of all non-empty finite words over a finite alphabet  $A$ , and by  $A^*$  the monoid obtained by adding the empty word  $\varepsilon$  to  $A^+$ . The length of a word  $w \in A^*$  is written as  $|w|$ .

### 2.1 Semigroups and languages

Let  $\mathfrak{M}$  be a monoid with identity element 1. Any subset  $L \subseteq \mathfrak{M}$  is called a *language* in  $\mathfrak{M}$ . The *product* of two languages  $K$  and  $L$  in  $\mathfrak{M}$  is defined as  $KL = \{st \mid s \in K, t \in L\}$ . The subsemigroup of  $\mathfrak{M}$  generated by a language  $L$ , which is equal to  $\bigcup_{n \in \mathbb{N}} L^n$ , is denoted by  $L^+$  and called the *iteration* of  $L$ . The submonoid of  $\mathfrak{M}$  generated by  $L$  is  $L^* = L^+ \cup \{1\}$ . Further, for  $n \in \mathbb{N}$  we write  $L^{\leq n} = L \cup L^2 \cup \dots \cup L^n$ , and we say that a language  $L$  possesses the *finite power property* (FPP) if there exists  $n \in \mathbb{N}$  such that  $L^+ = L^{\leq n}$ .

A language  $L$  in a monoid  $\mathfrak{M}$  is *recognizable* if there exists a homomorphism  $\sigma: \mathfrak{M} \rightarrow \mathfrak{S}$  to a finite semigroup  $\mathfrak{S}$  satisfying  $L = \sigma^{-1}\sigma(L)$ , i.e. such that the membership of elements of  $\mathfrak{M}$  in  $L$  depends only on their  $\sigma$ -images. The *syntactic homomorphism* of  $L$  is the projection homomorphism  $\sigma: \mathfrak{M} \rightarrow \mathfrak{M}/\equiv$ , where the congruence  $\equiv$  of  $\mathfrak{M}$  is defined by the condition

$$v \equiv w \iff (\forall x, y \in \mathfrak{M})(xvy \in L \iff xwy \in L).$$

The factor monoid  $\mathfrak{M}/\equiv$  is called the *syntactic monoid* of  $L$ ; it is the smallest monoid recognizing  $L$ .

A language  $L$  in  $\mathfrak{M}$  is *rational* if it belongs to the smallest family of languages in  $\mathfrak{M}$  containing all finite languages and closed under the *rational operations*: union, product and iteration. Kleene's theorem states that a language in a free monoid  $A^*$  is rational if and only if it is recognizable; such a language is then called *regular*. If the monoid  $\mathfrak{M}$  is generated by a finite set  $A$ , i.e. there is an onto homomorphism  $\gamma: A^* \twoheadrightarrow \mathfrak{M}$ , then a language in  $\mathfrak{M}$  is rational if and only if it is of the form  $\gamma(L)$  for some regular language  $L$  in  $A^*$ .

Let  $\mathfrak{S}$  be an arbitrary semigroup. An *ideal* of  $\mathfrak{S}$  is a non-empty subset  $I \subseteq \mathfrak{S}$  such that for all  $s \in I$  and  $t \in \mathfrak{S}$ , we have  $st \in I$  and  $ts \in I$ . For any ideal  $I$  of  $\mathfrak{S}$ , the *Rees factor semigroup*  $\mathfrak{S}/I$  is defined on the set  $(\mathfrak{S} \setminus I) \cup \{0\}$ , where  $0$  is a new zero element, and elements  $s, t \in \mathfrak{S} \setminus I$  are multiplied according to the formula

$$s \cdot t = \begin{cases} st & \text{if } st \notin I, \\ 0 & \text{if } st \in I. \end{cases}$$

The ideal of  $\mathfrak{S}$  generated by a given element  $s \in \mathfrak{S}$  is equal to  $\mathfrak{S}^1 s \mathfrak{S}^1$ , where  $\mathfrak{S}^1$  denotes the monoid obtained from  $\mathfrak{S}$  by adding a new identity element  $1$ . The quasi-order  $\leq_{\mathcal{J}_{\mathfrak{S}}}$  on  $\mathfrak{S}$  is defined, for any  $s, t \in \mathfrak{S}$ , by the rule

$$s \leq_{\mathcal{J}_{\mathfrak{S}}} t \iff s \in \mathfrak{S}^1 t \mathfrak{S}^1.$$

The Green relation  $\mathcal{J}_{\mathfrak{S}}$  of the semigroup  $\mathfrak{S}$  is the equivalence relation on  $\mathfrak{S}$  associated with the quasi-order  $\leq_{\mathcal{J}_{\mathfrak{S}}}$ , i.e. two elements of  $\mathfrak{S}$  are  $\mathcal{J}$ -equivalent if they generate the same ideal. Consequently, the quasi-order  $\leq_{\mathcal{J}_{\mathfrak{S}}}$  determines a partial order of  $\mathcal{J}$ -classes of  $\mathfrak{S}$ .

A straightforward application of the pigeon hole principle to a  $\mathcal{J}$ -class of a finite semigroup gives the following useful lemma.

**Lemma 1 (Kirsten [8]).** *Let  $J$  be a  $\mathcal{J}$ -class of a finite semigroup  $\mathfrak{S}$ . Let  $n \in \mathbb{N}$  and let  $s_1, \dots, s_n$  be a sequence of elements of  $\mathfrak{S}$  satisfying  $s_1 \cdots s_n \in J$ . Let  $N \subseteq \{1, \dots, n\}$  with  $|N| > |J|$  be such that  $s_i \in J$  for all  $i \in N$ . Then there exist  $k, l \in N$ ,  $k < l$ , such that  $s_k \cdots s_l = s_k$ .*

Recall that an element  $s$  of a semigroup which satisfies  $ss = s$  is called an *idempotent*. A  $\mathcal{J}$ -class  $J$  of a finite semigroup  $\mathfrak{S}$  is *regular* if it contains an idempotent, or equivalently, if there exist elements  $s, t \in J$  such that their product  $st$  belongs to  $J$  too.

Finally, we recall one of the basic constructions of semigroups, which will be used here to encode deletions. Assume we have a semigroup  $\mathfrak{S}$  and an element  $0 \notin \mathfrak{S}$ . Let  $L$  and  $R$  be arbitrary finite sets, and let  $P: R \times L \rightarrow \mathfrak{S} \cup \{0\}$  be any mapping (this mapping can be understood as an  $(R \times L)$ -matrix with entries belonging to  $\mathfrak{S}$  or equal to  $0$ ). The *Rees matrix semigroup*  $\mathcal{M}^0(\mathfrak{S}; L, R; P)$  over  $\mathfrak{S}$  is defined on the set  $(L \times \mathfrak{S} \times R) \cup \{0\}$ , where  $0$  is a new zero element, by the multiplication formula

$$(l, s, r) \cdot (l', s', r') = \begin{cases} (l, s \cdot P(r, l') \cdot s', r') & \text{if } P(r, l') \neq 0, \\ 0 & \text{if } P(r, l') = 0. \end{cases}$$

## 2.2 Rational semigroups

Now we recall the notion of a rational semigroup, which was introduced by Sakarovitch in [12].

A *rational transducer* is a 6-tuple  $(A, B, Q, q_0, Q_f, E)$ , where  $A$  is a finite *input alphabet*,  $B$  is a finite *output alphabet*,  $Q$  is a finite set of *states*,  $q_0 \in Q$  is an *initial state*,  $Q_f \subseteq Q$  is a set of *final states*, and  $E \subseteq Q \times A^* \times B^* \times Q$  is a finite set of oriented edges between states, each of them labelled by a word read from the input and a word sent to the output. The relation *realized* by the transducer consists of all pairs  $(v, w) \in A^* \times B^*$ , where  $v$  and  $w$  are obtained by concatenating input and output words of the edges of some path from the initial state to a final state. A function from  $A^*$  to  $B^*$  is called *rational* if it can be realized by a rational transducer.

A semigroup  $\mathfrak{S}$  is *rational* if there exist a finite set  $A$ , an onto homomorphism  $\alpha: A^+ \twoheadrightarrow \mathfrak{S}$  and a rational function  $\beta: A^+ \rightarrow A^+$  satisfying  $\alpha\beta = \alpha$  and  $\ker(\beta) = \ker(\alpha)$ . This means that  $\mathfrak{S}$  is isomorphic to the semigroup defined on the set  $\beta(A^+)$  by the rule  $u \cdot v = \beta(uv)$ .

An important property of rational monoids is that they satisfy Kleene's theorem:

**Proposition 1 (Sakarovitch [12]).** *In every rational monoid, the family of rational sets is equal to the family of recognizable sets.*

When dealing with rational monoids, we will call rational sets regular as in free monoids. Because rational functions algorithmically preserve regularity, a language  $L$  in a rational monoid is regular if and only if the language  $\beta\alpha^{-1}(L)$  in  $A^*$  is regular. Moreover, rational operations on regular languages in a rational monoid can be performed algorithmically as we can calculate with the corresponding subsets  $\beta\alpha^{-1}(L)$  of  $\beta(A^+)$  using the obvious rules, e.g.  $\beta\alpha^{-1}(K \cdot L) = \beta(\beta\alpha^{-1}(K) \cdot \beta\alpha^{-1}(L))$ .

The class of rational semigroups possesses several useful closure properties with respect to basic semigroup constructions. In our considerations, the following two constructions will be employed.

**Proposition 2 (Sakarovitch [12]).** *The class of rational semigroups is algorithmically closed under taking Rees factors by regular ideals.*

**Proposition 3.** *Let  $\mathfrak{M}$  be a rational monoid with identity element 1. Let  $L$  and  $R$  be finite sets and  $P: R \times L \rightarrow \mathfrak{M} \cup \{0\}$  a mapping such that  $P(\rho, \lambda) = 1$  for certain  $\lambda \in L$  and  $\rho \in R$ . Then the Rees matrix semigroup  $\mathcal{M}^0(\mathfrak{M}; L, R; P)$  over  $\mathfrak{M}$  is rational and can be algorithmically constructed.*

*Proof.* Let  $A$  be a finite set, let  $\alpha: A^+ \twoheadrightarrow \mathfrak{M}$  be an onto homomorphism and  $\beta: A^+ \rightarrow A^+$  a rational function satisfying  $\alpha\beta = \alpha$  and  $\ker(\beta) = \ker(\alpha)$ . Take the word  $u \in A^+$  such that  $\beta\alpha^{-1}(1) = \{u\}$ , and the words  $u_{r,l} \in A^+$ , for  $l \in L$  and  $r \in R$  satisfying  $P(r, l) \neq 0$ , such that  $\beta\alpha^{-1}(P(r, l)) = \{u_{r,l}\}$ . Let

us consider the finite set  $B = (L \times A \times R) \cup \{0\}$  and the auxiliary mapping  $\mu: L \times A^* \times R \rightarrow B^+$  defined for  $l \in L$ ,  $r \in R$ ,  $n \in \mathbb{N}_0$  and  $a_1, \dots, a_n \in A$  as

$$\mu(l, a_1 \cdots a_n, r) = (l, a_1, \rho)(\lambda, a_2, \rho) \cdots (\lambda, a_{n-1}, \rho)(\lambda, a_n, r).$$

Then we define a homomorphism  $\gamma: B^+ \rightarrow \mathcal{M}^0(\mathfrak{M}; L, R; P)$  by the rules  $\gamma((l, a, r)) = (l, \alpha(a), r)$  and  $\gamma(0) = 0$ . This homomorphism is onto because for every  $l \in L$ ,  $s \in \mathfrak{M}$  and  $r \in R$  there exist  $n \in \mathbb{N}$  and  $a_1, \dots, a_n \in A$  such that  $\alpha(a_1 \cdots a_n) = s$ , which immediately gives  $(l, s, r) = \gamma\mu(l, ua_1 \cdots a_n u, r)$ . This suggests us to define a function  $\delta: B^+ \rightarrow B^+$  by setting  $\delta(B^* 0 B^*) = \{0\}$  and

$$\delta((l_1, a_1, r_1) \cdots (l_n, a_n, r_n)) = \mu(l_1, u\beta(a_1 u_{r_1, l_2} a_2 \cdots u_{r_{n-1}, l_n} a_n) u, r_n)$$

if  $P(r_i, l_{i+1}) \neq 0$  for  $i = 1, \dots, n-1$ , and  $\delta((l_1, a_1, r_1) \cdots (l_n, a_n, r_n)) = 0$  otherwise. Then it can be directly verified that  $\gamma\delta = \gamma$  and  $\ker(\delta) = \ker(\gamma)$ .

It remains to show how to construct a rational transducer realizing  $\delta$ . First note that it is enough to deal with words which are not mapped to 0, because  $\delta^{-1}(0)$  is the regular language

$$B^* 0 B^* \cup \bigcup \{ B^*(l, a, r)(l', a', r') B^* \mid l, l' \in L, a, a' \in A, r, r' \in R, P(r, l') = 0 \}.$$

Let  $(A, A, Q, q_0, Q_f, E)$  be a rational transducer realizing  $\beta$ . Because  $\beta$  is a function, we can assume that the input label of each edge is a letter, i.e.  $E \subseteq Q \times A \times A^* \times Q$ . Then the non-zero part of  $\delta$  can be realized by the transducer

$$(B, B, (Q \times R) \cup (L \times Q) \cup \{q_0, q_f\}, q_0, \{q_f\}, F)$$

with one final state  $q_f$ , where

$$\begin{aligned} F = & \{ (q_0, (l, a, r), \mu(l, u\beta(a)u, r), q_f) \mid l \in L, a \in A, r \in R \} \\ & \cup \{ (q_0, (l, a, r), \mu(l, uv, \rho), (q, r)) \mid l \in L, r \in R, (q_0, a, v, q) \in E \} \\ & \cup \{ ((l, p), (l, a, r), \mu(\lambda, vu, r), q_f) \mid l \in L, r \in R, (p, a, v, q) \in E, q \in Q_f \} \\ & \cup \{ ((l, p), (l, a, r), \mu(\lambda, v, \rho), (q, r)) \mid l \in L, r \in R, (p, a, v, q) \in E \} \\ & \cup \{ ((p, r), \varepsilon, \mu(\lambda, v, \rho), (l, q)) \mid l \in L, r \in R, P(r, l) \neq 0, (p, u_{r, l}, v, q) \in \text{tr}(E) \}, \end{aligned}$$

where  $\text{tr}(E)$  denotes the set

$$\{ (q_1, a_1 \cdots a_n, u_1 \cdots u_n, q_{n+1}) \mid n \in \mathbb{N}, (q_1, a_1, u_1, q_2), \dots, (q_n, a_n, u_n, q_{n+1}) \in E \}$$

of all results obtained by moving along a path in  $E$ .  $\square$

### 3 Free monoids

In this section we consider the FPP in a monoid  $\mathfrak{M}$  with identity element 1 and zero element 0, and satisfying the following conditions:

1. There exists a mapping  $\ell: \mathfrak{M} \setminus \{0\} \rightarrow \mathbb{N}_0$  assigning to each non-zero element of  $\mathfrak{M}$  its *length*, and satisfying  $\ell(xy) \geq \ell(x) + \ell(y)$  for all  $x, y \in \mathfrak{M}$  such that  $xy \neq 0$ .
2. For every  $u, v, w, t \in \mathfrak{M}$  satisfying  $uv = wt \neq 0$ , there exists  $x \in \mathfrak{M}$  such that either  $ux = w$  and  $xt = v$  or  $wx = u$  and  $xv = t$ .
3. The languages  $\{0\}$  and  $\{1\}$  in  $\mathfrak{M}$  are recognizable.

*Remark 1.* Any free monoid with the length of a word defined in the usual way and with a zero element added satisfies the above conditions.

**Lemma 2.** *Let  $\mathfrak{M}$  be an arbitrary monoid satisfying condition 2. Let  $m, n \in \mathbb{N}$ ,  $m \leq n$ , and  $w, v_1, \dots, v_m \in \mathfrak{M}$  be such that  $w^n = v_1 \cdots v_m \neq 0$ . Then there exist  $k \in \mathbb{N}_0$ ,  $k < m$ , and elements  $x, y \in \mathfrak{M}$  satisfying  $v_1 \cdots v_k x = w^k$ ,  $y v_{k+2} \cdots v_m = w^{n-k-1}$  and  $v_{k+1} = xwy$ .*

*Proof.* Let  $k \in \mathbb{N}_0$  be the smallest number such that there exists  $y \in \mathfrak{M}$  for which  $w^{k+1}y = v_1 \cdots v_{k+1}$  and  $yv_{k+2} \cdots v_m = w^{n-k-1}$ . Such a number certainly exists since this holds for  $k = m-1$  with  $y = w^{n-m}$ . If  $k = 0$  then it is sufficient to put  $x = 1$ . Otherwise, we apply property 2 of  $\mathfrak{M}$  to the decomposition  $w^k \cdot (wy) = (v_1 \cdots v_k) \cdot v_{k+1}$ . First assume that we have  $w^k x = v_1 \cdots v_k$  and  $xv_{k+1} = wy$  for a certain  $x \in \mathfrak{M}$ . Then we obtain also  $xv_{k+1} \cdots v_m = wyv_{k+2} \cdots v_m = w^{n-k}$ , which contradicts the minimality of  $k$ . Therefore there exists  $x \in \mathfrak{M}$  satisfying  $v_1 \cdots v_k x = w^k$  and  $xwy = v_{k+1}$ , as required.  $\square$

Let  $L \subseteq \ell^{-1}(\mathbb{N})$  be an arbitrary recognizable language in  $\mathfrak{M}$  consisting of elements of non-zero length, and such that  $L^+$  is also recognizable. Let  $\sigma: \mathfrak{M} \rightarrow \mathfrak{S}$  be a homomorphism onto a finite semigroup recognizing the languages  $L$ ,  $L^+$ ,  $\{0\}$  and  $\{1\}$ . Consider the mapping  $\tau: \mathfrak{M} \rightarrow \wp(\mathfrak{S}^3) \cup \{0\}$  defined by the rules  $\tau(0) = 0$  and

$$\tau(w) = \{ (\sigma(x), \sigma(y), \sigma(z)) \mid x, y, z \in \mathfrak{M}, w = xyz \}$$

for  $w \in \mathfrak{M} \setminus \{0\}$ .

**Lemma 3.** *For every monoid  $\mathfrak{M}$  satisfying condition 2, the kernel of  $\tau$  is a congruence of  $\mathfrak{M}$ .*

*Proof.* Let  $v, w \in \mathfrak{M} \setminus \{0\}$ . Since  $\sigma$  recognizes  $\{0\}$ , we have  $vw = 0$  if and only if  $\sigma(vw) = 0$ , which holds exactly when  $\zeta\eta\vartheta\kappa\lambda\mu = 0$  for every  $(\zeta, \eta, \vartheta) \in \tau(v)$  and  $(\kappa, \lambda, \mu) \in \tau(w)$ . And from property 2 it immediately follows that if  $vw \neq 0$ , then the triple  $(\alpha, \beta, \gamma) \in \mathfrak{S}^3$  belongs to  $\tau(vw)$  if and only if there exist  $(\zeta, \eta, \vartheta) \in \tau(v)$  and  $(\kappa, \lambda, \mu) \in \tau(w)$  satisfying at least one of the following conditions:

1.  $\alpha = \zeta\eta\vartheta\kappa$ ,  $\beta = \lambda$  and  $\gamma = \mu$ ;
2.  $\alpha = \zeta$ ,  $\beta = \eta\vartheta\kappa\lambda$  and  $\gamma = \mu$ ;
3.  $\alpha = \zeta$ ,  $\beta = \eta$  and  $\gamma = \vartheta\kappa\lambda\mu$ .

Therefore the kernel of  $\tau$  is a congruence.  $\square$

By Lemma 3 there exists a unique semigroup operation on  $\tau(\mathfrak{M})$  such that  $\tau$  is a homomorphism. Let us denote by  $\mathfrak{T}$  the subsemigroup  $\tau(L^+)$  of  $\tau(\mathfrak{M})$ .

*Remark 2.* Note that if  $\tau(v) = \tau(w)$ , then in particular  $\sigma(v) = \sigma(w)$ . Therefore, the homomorphism  $\tau$  recognizes all languages recognized by  $\sigma$ , and it also means that  $\tau(v) \mathcal{J}_{\mathfrak{T}} \tau(w)$  implies  $\sigma(v) \mathcal{J}_{\mathfrak{S}} \sigma(w)$ . Further observe that the identity element  $\tau(1) \in \tau(\mathfrak{M})$  does not belong to  $\mathfrak{T}$  since  $\tau$  recognizes  $\{1\}$ .

**Theorem 1.** *Let  $\mathfrak{M}$  be an arbitrary monoid satisfying properties 1 through 3. Then for any recognizable language  $L \subseteq \ell^{-1}(\mathbb{N})$  in  $\mathfrak{M}$  such that  $L^+$  is also recognizable, and for  $\sigma$ ,  $\mathfrak{S}$ ,  $\tau$  and  $\mathfrak{T}$  defined above, the following conditions are equivalent:*

1.  $L$  possesses the FPP.
2. For all  $w \in L^+$ , there exists  $n \in \mathbb{N}$  such that  $w^n \in L^{\leq n}$ .
3. Every non-zero regular  $\mathcal{J}$ -class of  $\mathfrak{T}$  contains some element of  $\tau(L)$ .
4. For all  $w \in L^+ \setminus \{0\}$  such that  $\tau(w)$  belongs to a regular  $\mathcal{J}$ -class of  $\mathfrak{T}$ , there exist  $y \in L$  and  $x, z \in L^*$  satisfying  $w = xyz$  and  $\sigma(y) \mathcal{J}_{\mathfrak{S}} \sigma(w)$ .
5.  $L^+ = L^{\leq (j+1)^h}$ , where  $j$  is the maximal size of a  $\mathcal{J}$ -class of  $\mathfrak{S}$  and  $h$  is the length of the longest chain of  $\mathcal{J}$ -classes in  $\mathfrak{T}$ .

*Proof.* 1  $\implies$  2 is trivial.

2  $\implies$  3. Let  $J$  be a non-zero regular  $\mathcal{J}$ -class of  $\mathfrak{T}$ . Then there exists  $w \in L^+ \setminus \{0\}$  such that  $\tau(w)$  is an idempotent belonging to  $J$ . Let  $n \in \mathbb{N}$  be such that  $w^n \in L^{\leq n}$ . Then by Lemma 2 one can find  $k \in \mathbb{N}_0$  and elements  $x, y \in \mathfrak{M}$  and  $u, v \in L^*$  satisfying  $ux = w^k$ ,  $yv = w^{n-k-1}$  and  $xwy \in L$ . Therefore we have

$$\begin{aligned} \tau(u)\tau(xwy)\tau(v) &= \tau(w^n) = \tau(w) \quad \text{and} \\ \tau(xwyv)\tau(w)\tau(uxwy) &= \tau(xw^{n+2}y) = \tau(xwy). \end{aligned}$$

This shows that  $\tau(xwy) \in J$  as required.

3  $\implies$  4. Let  $w \in L^+ \setminus \{0\}$  be such that  $\tau(w)$  belongs to a regular  $\mathcal{J}$ -class of  $\mathfrak{T}$ . Then there exists  $u \in L$  satisfying  $\tau(u) \mathcal{J}_{\mathfrak{T}} \tau(w)$ . Therefore  $\tau(w) = \tau(tuv)$  for certain  $t, v \in L^*$ . By the definition of  $\tau$ , one can find elements  $x, y, z \in \mathfrak{M}$  for which  $w = xyz$ ,  $\sigma(x) = \sigma(t)$ ,  $\sigma(y) = \sigma(u)$  and  $\sigma(z) = \sigma(v)$ . Because  $\sigma$  recognizes both  $L$  and  $L^*$ , this in particular means that  $y \in L$  and  $x, z \in L^*$ . Finally, we have also  $\sigma(y) = \sigma(u) \mathcal{J}_{\mathfrak{S}} \sigma(w)$  due to Remark 2.

4  $\implies$  5. Let us prove that  $L^+ \cap \tau^{-1}(J) \subseteq L^{\leq (j+1)^{h_J}-1}$  for every  $\mathcal{J}$ -class  $J$  of  $\mathfrak{T}$ , where  $h_J$  denotes the length of the longest chain of  $\mathcal{J}$ -classes in  $\mathfrak{T}$  greater or equal to  $J$ . We proceed by induction on  $h_J$ . Let  $w \in L^+ \cap \tau^{-1}(J)$ .

If the class  $J$  is non-regular, consider the longest prefix  $x \in L^* \setminus \tau^{-1}(J)$  of  $w$  such that there exist  $y \in L$  and  $z \in L^*$  satisfying  $w = xyz$ . Then  $\tau(xy) \in J$  and therefore  $\tau(z) \notin J$ , as  $J$  is not regular. Hence, by the induction hypothesis, we obtain

$$w \in L^{\leq 2((j+1)^{h_J-1}-1)+1} \subseteq L^{\leq (j+1)^{h_J}-1}.$$

If  $w = 0$  then  $w = xz$  for some  $x, z \in L^+ \setminus \{0\}$  and we get  $w \in L^{\leq(j+1)^{h_J}-1}$  as in the previous case.

If  $J$  is regular and non-zero, denote the  $\mathcal{J}$ -class of  $\sigma(w)$  in  $\mathfrak{S}$  by  $I$  and consider a decomposition  $w = w_0 v_1 w_1 v_2 \cdots v_n w_n$ , where  $w_0, w_1, \dots, w_n \in L^*$  and  $v_1, v_2, \dots, v_n \in L \cap \sigma^{-1}(I)$ , such that  $\ell(v_1) + \ell(v_2) + \cdots + \ell(v_n)$  is maximal (note that this number is bounded by  $\ell(w)$ ), and among such decompositions the number  $n$  is minimal.

If  $n > |I|$  then Lemma 1 implies that there exist  $k, l \in \{1, \dots, n\}$ ,  $k < l$ , such that  $\sigma(v_k w_k \cdots w_{l-1} v_l) = \sigma(v_k)$ . Because  $\sigma$  recognizes  $L$ , this in particular means that  $v_k w_k \cdots w_{l-1} v_l \in L \cap \sigma^{-1}(I)$ , contradicting the choice of the decomposition of  $w$ . Thus, we have  $n \leq |I|$ .

Assuming  $\tau(w_i) \in J$  for some  $i \in \{0, \dots, n\}$ , by condition 4 we obtain elements  $y \in L$  and  $x, z \in L^*$  satisfying  $w_i = xyz$  and  $\sigma(y) \mathcal{J}_{\mathfrak{S}} \sigma(w_i)$ . Since  $\sigma(w_i) \in I$  can be derived using Remark 2, this means that  $\sigma(y) \in I$ , which contradicts the maximality of the decomposition of  $w$ . Therefore  $\tau(w_i) \notin J$  for all  $i \in \{0, \dots, n\}$ , and so the induction hypothesis gives

$$w \in L^{\leq(|I|+1)((j+1)^{h_J-1}-1)+|I|} \subseteq L^{\leq(j+1)^{h_J}-1}.$$

5  $\implies$  1 is trivial. □

*Remark 3.* Condition 2 was conjectured to be equivalent to the FPP by Linna [10], and later this was proved true for free monoids by Hashiguchi [4].

Let us now present examples demonstrating that both ingredients of the construction of the semigroup  $\mathfrak{T}$  (i.e. the decomposition of words to triples and the restriction to  $\tau(L^+)$ ) are essential.

*Example 1.* Let us consider the language  $L = \{a\} \cup bA^*$  over the alphabet  $A = \{a, b\}$ . This language clearly does not possess the FPP. Since  $L$  satisfies  $L^+ = A^+$ , the syntactic homomorphism  $\sigma$  of  $L$  recognizes all the languages  $L$ ,  $L^+$  and  $\{\varepsilon\}$ . The syntactic monoid of  $L$  has four elements  $\alpha, \beta, \gamma$  and  $\delta$ , which correspond to the languages  $\{\varepsilon\} = \sigma^{-1}(\alpha)$ ,  $\{a\} = \sigma^{-1}(\beta)$ ,  $aA^+ = \sigma^{-1}(\gamma)$  and  $bA^* = \sigma^{-1}(\delta)$ . The only regular  $\mathcal{J}$ -class of  $\sigma(A^+)$  is  $\{\gamma, \delta\}$ , and it contains the element  $\delta \in \sigma(L)$  (note that the same is true also for the subsemigroup  $\sigma(L^+)$ ).

But in the semigroup  $\mathfrak{T} = \tau(L^+)$ , there is really a regular  $\mathcal{J}$ -class which does not contain any element of  $\tau(L)$ , namely the  $\mathcal{J}$ -class of the idempotent

$$\tau(a^6) = \{(\zeta, \eta, \vartheta) \mid \gamma \in \{\zeta, \eta, \vartheta\} \subseteq \{\alpha, \beta, \gamma\}\}.$$

In order to verify this, let us take an arbitrary element of  $\mathfrak{T}$  which is  $\mathcal{J}$ -equivalent to  $\tau(a^6)$ , and assume that it belongs to  $\tau(L)$ . Such an element must be of the form  $\tau(va^6w)$ , where  $v, w \in L^*$ . Because  $\tau$  recognizes  $L$ , we have  $va^6w \in L$ , and therefore  $va^6w \in bA^*$ . Since  $\tau(va^6w) \mathcal{J}_{\mathfrak{T}} \tau(a^6)$ , there exist  $x, y \in L^*$  satisfying  $\tau(xva^6wy) = \tau(a^6)$ . Then  $\tau(xva^6wy)$  contains the triple  $(\sigma(x), \sigma(va^6w), \sigma(y)) = (\sigma(x), \delta, \sigma(y))$ , which cannot belong to  $\tau(a^6)$ , contradicting the previous equality.

*Example 2.* The language  $L = \{ab\} \cup \{ab, ba\}^*ba\{ab, ba\}^*$  over the alphabet  $A = \{a, b\}$  also does not have the FPP. Again, the syntactic homomorphism  $\sigma$  of  $L$  recognizes the languages  $L$ ,  $L^+$  and  $\{\varepsilon\}$ . We are going to verify that every regular  $\mathcal{J}$ -class of  $\tau(A^+)$  containing some element of  $\tau(L^+)$  contains also an element of  $\tau(L)$ . Because

$$\tau(L^+) = \tau(\{ab, ba\}^+) = \tau(L) \cup \tau(ab(ab)^+),$$

it is enough to deal with the  $\mathcal{J}$ -classes of  $\tau(A^+)$  containing  $\tau((ab)^n)$  for  $n \geq 2$ . For  $n \leq 5$ , we have  $\tau^{-1}\tau((ab)^n) = \{(ab)^n\}$ , since the  $\tau$ -image of each of these words is characterized by the presence of some triples formed from the two different elements  $\sigma(ab)$  and  $\sigma(ab(ab)^+)$ . Therefore for  $n \leq 5$ , the element  $\tau((ab)^n)$  forms a non-regular singleton  $\mathcal{J}$ -class of  $\tau(A^+)$ . Further, one can calculate that  $\tau((ab)^6)$  is an idempotent, and  $\tau((ab)^n) = \tau((ab)^6)$  for every  $n \geq 6$ . In this case, one gets  $\tau((ab)^6) \mathcal{J}_{\tau(A^+)} \tau((ba)^7) \in \tau(L)$ .

**Corollary 1.** *The FPP is uniformly decidable for regular languages consisting of elements of non-zero length in rational monoids satisfying conditions 1 and 2.*

*Proof.* First, note that condition 3 holds for every rational monoid, and so Theorem 1 can be applied. By condition 5 of Theorem 1, it is enough to construct a semigroup  $\mathfrak{S}$  recognizing  $L$ ,  $L^+$ ,  $\{0\}$  and  $\{1\}$ , and test whether  $L^+ = L^{\leq m}$ , for  $m = n^{2^{n^3}}$ , where  $n$  is the cardinality of  $\mathfrak{S}$ .  $\square$

Based on the results of Kirsten [8], the author [9] observed that each language recognized by a given finite semigroup  $\mathfrak{S}$  has the FPP if and only if  $\mathfrak{S}$  is a chain of simple semigroups, i.e. for all  $s, t \in \mathfrak{S}$ , either  $st \mathcal{J}_{\mathfrak{S}} s$  or  $st \mathcal{J}_{\mathfrak{S}} t$ . Let us now show how one can derive this fact using Theorem 1 instead of Kirsten's results.

**Corollary 2.** *Let  $\mathfrak{M}$  be a monoid satisfying properties 1 through 3, and let  $\mathfrak{S}$  be a finite semigroup which is a chain of simple semigroups. Then every language  $L \subseteq \ell^{-1}(\mathbb{N})$  in  $\mathfrak{M}$  recognized by some homomorphism  $\rho: \mathfrak{M} \rightarrow \mathfrak{S}$ , and such that  $L^+$  is also recognizable, has the FPP.*

*Proof.* We are going to verify that condition 3 of Theorem 1 holds. Consider  $n \in \mathbb{N}$  and arbitrary elements  $w_1, \dots, w_n \in L$  such that  $\tau(w_1 \cdots w_n)$  is an idempotent, and choose any  $i \in \{1, \dots, n\}$  for which  $\rho(w_i)$  belongs to the smallest of the  $\mathcal{J}$ -classes of  $\mathfrak{S}$  determined by the elements  $\rho(w_1), \dots, \rho(w_n)$ . Because  $\mathfrak{S}$  is a chain of simple semigroups, we have  $\rho(w_i) \mathcal{J}_{\mathfrak{S}} \rho(w_1 \cdots w_n)$ . Let  $m$  be the cardinality of the  $\mathcal{J}$ -class of  $\rho(w_i)$  in  $\mathfrak{S}$ . Applying Lemma 1 to the sequence resulting from concatenating  $2m+1$  copies of the sequence  $\rho(w_1), \dots, \rho(w_n)$ , and to the set  $N = \{i, 2n+i, \dots, 2mn+i\}$  (i.e.  $N$  consists of all odd occurrences of  $\rho(w_i)$ ), we obtain a positive integer  $k$  such that  $\rho(w_i) = \rho(w_i \cdots w_n (w_1 \cdots w_n)^k w_1 \cdots w_i)$ . This shows that  $w_i \cdots w_n (w_1 \cdots w_n)^k w_1 \cdots w_i \in L$ . On the other hand, we have  $\tau(w_1 \cdots w_n) = \tau((w_1 \cdots w_n)^{k+2})$  since  $\tau(w_1 \cdots w_n)$  is an idempotent, and therefore the element  $\tau(w_i \cdots w_n (w_1 \cdots w_n)^k w_1 \cdots w_i) \in \tau(L)$  belongs to the same  $\mathcal{J}$ -class of  $\mathfrak{T}$  as  $\tau(w_1 \cdots w_n)$ . Hence, Theorem 1 implies that  $L$  has the FPP.  $\square$

## 4 Monoids defined by deletions

Let  $\mathfrak{G}$  be a monoid generated by a finite set  $A$  whose word problem can be solved by a confluent regular system of deletion rules  $\mathcal{R} = \{w \rightarrow \varepsilon \mid w \in R\}$ , where  $R \subseteq A^+$  is a regular language. In other words, we have an onto homomorphism  $\gamma: A^* \rightarrow \mathfrak{G}$  such that for every  $v, w \in A^*$ ,

$$\gamma(v) = \gamma(w) \iff \text{norm}(v) = \text{norm}(w),$$

where  $\text{norm}(w)$  denotes the normal form of  $w$  with respect to  $\mathcal{R}$ . We will also use the notation  $\text{norm}(L) = \{\text{norm}(w) \mid w \in L\}$  for a language  $L \subseteq A^*$ .

**Lemma 4.** *The language  $D = \{w \in A^* \mid \text{norm}(w) = \varepsilon\}$  is context-free and algorithmically computable from  $R$ . For every regular language  $L \subseteq A^*$ , the language  $\text{norm}(L)$  is regular and can be algorithmically computed using  $R$  and  $L$ .*

*Proof.* Let  $(A, Q, q_0, Q_f, \delta)$  be a deterministic finite automaton recognizing  $R$ . The language  $D$  can be defined by a context-free grammar with the set of non-terminals  $Q \cup \{S\}$  (where  $S$  is the initial symbol) and the derivation rules  $S \rightarrow q_0$ ,  $q \rightarrow aS\delta(q, a)$  for every  $q \in Q$  and  $a \in A$ ,  $q \rightarrow \varepsilon$  for  $q \in Q_f$ ,  $S \rightarrow SS$  and  $S \rightarrow \varepsilon$ .

Let  $d \notin A$  be a new symbol and consider the context-free substitution  $\varphi$  from  $(A \cup \{d\})^*$  to  $A^*$  defined by the rule  $\varphi(d) = D$  and identical otherwise. Let  $\psi: (A \cup \{d\})^* \rightarrow A^*$  be the homomorphism sending  $d$  to  $\varepsilon$  and leaving other symbols unchanged. Then  $\text{norm}(L) = \psi(\varphi^{-1}(L)) \setminus A^*RA^*$  and since both inverse context-free substitution and homomorphism effectively preserve regularity, the language  $\text{norm}(L)$  is regular and can be algorithmically computed.  $\square$

Let  $\gamma(L) \subseteq \mathfrak{G}$  be a rational language defined by a regular language  $L \subseteq A^*$ ; by Lemma 4 we can assume that  $L \subseteq \text{norm}(A^*)$ . Let the language  $L$  be given by a homomorphism  $\sigma: A^* \rightarrow \mathfrak{S}$  to a finite monoid  $\mathfrak{S}$  recognizing the three languages  $L$ ,  $\text{norm}(A^*)$  and  $\{\varepsilon\}$ .

We are going to use  $\sigma$  to construct a monoid  $\mathfrak{M}$  where deletions of  $\mathcal{R}$  are performed symbolically, and a language  $K$  in this monoid such that  $\gamma(L)$  has the FPP in  $\mathfrak{G}$  if and only if  $K$  has the FPP in  $\mathfrak{M}$ . To achieve this, we need to avoid sequences of elements of  $L$  which are reduced to the empty word using  $\mathcal{R}$ , and calculate only with those which are not completely deleted. The following lemma shows that such a modification does not affect the FPP because all deleted sequences can be produced using only a bounded number of words from  $L$ .

**Lemma 5.** *For given regular languages  $R$  and  $L$ , one can algorithmically calculate a positive integer  $m$  such that*

$$\varepsilon \in \text{norm}(L^+) \implies \varepsilon \in \text{norm}(L^{\leq m})$$

and for all  $x, y, z, u \in A^*$  and  $w \in L^+$  satisfying  $yz \in L$  and  $xu \in L$ , we have

$$\begin{aligned} \text{norm}(zwx) = \varepsilon &\implies \exists \bar{x}, \bar{z} \in A^*, \bar{w} \in L^{\leq m}: y\bar{z}, \bar{x}u \in L \text{ \& } \text{norm}(\bar{z}\bar{w}\bar{x}) = \varepsilon, \\ \text{norm}(zw) = \varepsilon &\implies \exists \bar{z} \in A^*, \bar{w} \in L^{\leq m}: y\bar{z} \in L \text{ \& } \text{norm}(\bar{z}\bar{w}) = \varepsilon, \\ \text{norm}(wx) = \varepsilon &\implies \exists \bar{x} \in A^*, \bar{w} \in L^{\leq m}: \bar{x}u \in L \text{ \& } \text{norm}(\bar{w}\bar{x}) = \varepsilon. \end{aligned}$$

*Proof.* For every  $r, s \in \mathfrak{S}$  we can calculate the context-free language  $L_{r,s} = \sigma^{-1}(r)L^+\sigma^{-1}(s) \cap D$ . For each of these languages we test whether it is non-empty, and if  $L_{r,s} \neq \emptyset$ , we find any word in  $L_{r,s}$ , which belongs to  $\sigma^{-1}(r)L^{m_{r,s}}\sigma^{-1}(s)$  for a certain  $m_{r,s} \in \mathbb{N}$ . We set  $m = \max\{m_{r,s} \mid r, s \in \mathfrak{S}, L_{r,s} \neq \emptyset\}$ . Since  $\sigma$  recognizes both  $L$  and  $\{\varepsilon\}$ , we can easily verify the required properties.  $\square$

Now we construct, for the language  $L$ , a rational monoid to which we are going to apply results of the previous section. Let  $\mathfrak{M}$  be defined on the set  $(\mathfrak{S} \times \text{norm}(A^*) \times \mathfrak{S}) \cup \{1, 0\}$ , where 1 is the identity element and 0 is the zero element, by the rule

$$(p, u, q)(r, v, s) = \begin{cases} (p, uv, s) & \text{if } uv \in \text{norm}(A^*) \text{ \& } \varepsilon \in \text{norm}(\sigma^{-1}(q)L^*\sigma^{-1}(r)), \\ 0 & \text{otherwise,} \end{cases}$$

for every  $p, q, r, s \in \mathfrak{S}$  and  $u, v \in \text{norm}(A^*)$ . Intuitively, the words  $u$  and  $v$  are factors of the resulting concatenation which are not affected by deletions when producing the normal form. And the elements  $q$  and  $r$  represent any suitable words from  $\sigma^{-1}(q)$  and  $\sigma^{-1}(r)$ , which originated as a suffix and a prefix, respectively, of certain words from  $L$ , and which can be deleted using  $\mathcal{R}$  together with several words from  $L$  between them.

We define the length of elements of  $\mathfrak{M}$  as  $\ell((r, v, s)) = |v|$  and  $\ell(1) = 0$ .

**Lemma 6.** *The above defined  $\mathfrak{M}$  is a rational monoid, which can be algorithmically constructed from  $R$  and  $L$  and satisfies conditions 1 and 2.*

*Proof.* Because  $A^* \setminus \text{norm}(A^*) = A^*RA^*$  is an ideal of  $A^*$ , the set  $I = (\mathfrak{S} \times A^*RA^* \times \mathfrak{S}) \cup \{0\}$  is an ideal of the Rees matrix semigroup  $\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)$  over  $A^*$ . Therefore  $\mathfrak{M}$  is a monoid as it is isomorphic to

$$(\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)/I)^1,$$

where  $P$  is defined by the formula

$$P(q, r) = \begin{cases} \varepsilon & \text{if } \varepsilon \in \text{norm}(\sigma^{-1}(q)L^*\sigma^{-1}(r)), \\ 0 & \text{otherwise.} \end{cases}$$

Since the finitely generated free monoid  $A^*$  is rational and  $P$  is computable and satisfies  $P(1, 1) = \varepsilon$ , by Proposition 3 the semigroup  $\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)$  is rational too and can be algorithmically constructed. In order to prove that  $\mathfrak{M}$  is also rational, let us consider the equivalence relation  $\sim_I$  on  $\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)$  defined by the rules

$$\begin{aligned} (p, u, q) \sim_I (r, v, s) &\iff p = r \text{ \& } \sigma(u) = \sigma(v) \text{ \& } q = s, \\ 0 \sim_I (r, v, s) &\iff v \in A^*RA^*. \end{aligned}$$

Because  $\sigma$  recognizes  $\text{norm}(A^*)$ , the relation  $\sim_I$  is easily seen to be a congruence of  $\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)$  of finite index recognizing  $I$ . Hence, the ideal  $I$  is algorithmically regular, and by Proposition 2 the monoid  $\mathfrak{M}$  is rational and can be computed from  $\mathcal{M}^0(A^*; \mathfrak{S}, \mathfrak{S}; P)$ .

One can easily verify that condition 1 is true even in the stronger form with  $\ell(xy) = \ell(x) + \ell(y)$ . Condition 2 trivially holds if one of the elements is the identity element. Otherwise, we have

$$(p, uv, s) = (p, u, q)(r, v, s) = (\bar{p}, \bar{u}, \bar{q})(\bar{r}, \bar{v}, \bar{s}) = (\bar{p}, \bar{u}\bar{v}, \bar{s})$$

for certain  $p, q, r, s, \bar{p}, \bar{q}, \bar{r}, \bar{s} \in \mathfrak{S}$  and  $u, v, \bar{u}, \bar{v} \in \text{norm}(A^*)$ . If  $|u| \leq |\bar{u}|$  then there exists  $x \in \text{norm}(A^*)$  such that  $ux = \bar{u}$  and  $x\bar{v} = v$ , and we immediately obtain  $(p, u, q)(r, x, \bar{q}) = (\bar{p}, \bar{u}, \bar{q})$  and  $(r, x, \bar{q})(\bar{r}, \bar{v}, \bar{s}) = (r, v, s)$  as required. The case  $|u| > |\bar{u}|$  can be treated symmetrically.  $\square$

Let us consider the following language in  $\mathfrak{M}$ :

$$K = \{ (\sigma(x), y, \sigma(z)) \mid x, y, z \in A^*, y \neq \varepsilon, xyz \in L \}$$

**Lemma 7.** *The language  $K$  is regular and a congruence of  $\mathfrak{M}$  of finite index recognizing  $K$  can be algorithmically constructed from  $R$  and  $L$ .*

*Proof.* We prove that  $K$  is recognized by the congruence  $\sim$  of  $\mathfrak{M}$  corresponding to  $\sim_I$ . This congruence has two one-element classes  $\{0\}$  and  $\{1\}$  and on the set  $\mathfrak{S} \times \text{norm}(A^*) \times \mathfrak{S}$  it is defined as

$$(p, u, q) \sim (r, v, s) \iff p = r \ \& \ \sigma(u) = \sigma(v) \ \& \ q = s.$$

Take an element  $(\sigma(x), y, \sigma(z))$  of  $K$ , where  $x, y, z \in A^*$  are such that  $y \neq \varepsilon$  and  $xyz \in L$ , and assume that  $(r, v, s) \sim (\sigma(x), y, \sigma(z))$ . Then  $r = \sigma(x)$ ,  $\sigma(v) = \sigma(y)$  and  $s = \sigma(z)$ , and consequently also  $\sigma(xvz) = \sigma(xyz)$ . Therefore we have  $v \neq \varepsilon$  and  $xvz \in L$  since  $\sigma$  recognizes both  $\{\varepsilon\}$  and  $L$ . Thus, the element  $(r, v, s) = (\sigma(x), v, \sigma(z))$  belongs to  $K$ .  $\square$

**Proposition 4.** *The language  $\gamma(L) \subseteq \mathfrak{S}$  has the FPP if and only if the language  $K \subseteq \mathfrak{M}$  has the FPP.*

*Proof.* Let us first assume that  $\gamma(L)$  possesses the FPP, i.e. that there exists  $k \in \mathbb{N}$  such that  $\text{norm}(L^+) = \text{norm}(L^{\leq k})$ . We are going to prove that  $K^+ \setminus \{0\} = K^{\leq k+2} \setminus \{0\}$ , which is sufficient to verify the FPP for  $K$ . Let  $(r, y, s)$  be an arbitrary non-zero element of  $K^+$ . Then

$$(r, y, s) = (\sigma(x_1), y_1, \sigma(z_1)) \cdots (\sigma(x_l), y_l, \sigma(z_l))$$

for some  $x_i, y_i, z_i \in A^*$  satisfying  $y_i \neq \varepsilon$  and  $x_i y_i z_i \in L$ , for  $i = 1, \dots, l$ . In particular, this implies  $y = y_1 \cdots y_l \in \text{norm}(A^*)$ . It suffices to consider the case of  $l \geq 3$ . By the definition of multiplication in  $\mathfrak{M}$ , we can assume that for every  $i = 1, \dots, l-1$  there exists  $w_i \in L^*$  satisfying  $\text{norm}(z_i w_i x_{i+1}) = \varepsilon$  (note that  $z_i$  and  $x_i$  can be replaced by another elements of  $\sigma^{-1}\sigma(z_i)$  and  $\sigma^{-1}\sigma(x_i)$ , respectively, since  $\sigma$  recognizes  $L$ ). Now we have

$$w_1 x_2 y_2 z_2 w_2 \cdots w_{l-2} x_{l-1} y_{l-1} z_{l-1} w_{l-1} \in L^+,$$

which means that there exists  $u \in L^{\leq k}$  such that

$$\text{norm}(w_1 x_2 y_2 z_2 w_2 \cdots w_{l-2} x_{l-1} y_{l-1} z_{l-1} w_{l-1}) = \text{norm}(u).$$

Because  $y_2 \cdots y_{l-1} \in \text{norm}(A^*)$ , we obtain

$$\text{norm}(z_1 u x_l) = \text{norm}(z_1 w_1 x_2 y_2 z_2 w_2 \cdots w_{l-2} x_{l-1} y_{l-1} z_{l-1} w_{l-1} x_l) = y_2 \cdots y_{l-1}.$$

Let us now consider one sequence of deletions using  $\mathcal{R}$  producing  $y_2 \cdots y_{l-1}$  from  $z_1 u x_l$ , and group together all neighbouring letters which are not deleted. As  $L \subseteq \text{norm}(A^*)$  holds, this regrouping is of the form

$$z_1 = \bar{y}_1 \bar{z}_1, \quad u = v_0 \tilde{x}_1 \tilde{y}_1 \tilde{z}_1 v_1 \cdots v_{n-1} \tilde{x}_n \tilde{y}_n \tilde{z}_n v_n, \quad x_l = \bar{x}_l \bar{y}_l,$$

for certain  $n \in \{0, \dots, k\}$ ,  $\bar{y}_1, \bar{z}_1, \bar{x}_l, \bar{y}_l \in A^*$ ,  $\tilde{x}_i, \tilde{y}_i, \tilde{z}_i \in A^*$ , for  $i = 1, \dots, n$ , and  $v_i \in L^*$ , for  $i = 0, \dots, n$ , which satisfy  $\tilde{y}_i \neq \varepsilon$ ,  $\tilde{x}_i \tilde{y}_i \tilde{z}_i \in L$ , for  $i = 1, \dots, n$ ,

$$\text{norm}(\bar{z}_1 v_0 \tilde{x}_1) = \text{norm}(\tilde{z}_i v_i \tilde{x}_{i+1}) = \text{norm}(\tilde{z}_n v_n \bar{x}_l) = \varepsilon,$$

for  $i = 1, \dots, n-1$ , and  $\bar{y}_1 \tilde{y}_1 \cdots \tilde{y}_n \bar{y}_l = y_2 \cdots y_{l-1}$  (if  $n = 0$  then  $\text{norm}(\bar{z}_1 v_0 \bar{x}_l) = \varepsilon$ ). This immediately gives

$$(r, y, s) = (\sigma(x_1), y_1 \bar{y}_1, \sigma(\bar{z}_1))(\sigma(\tilde{x}_1), \tilde{y}_1, \sigma(\tilde{z}_1)) \cdots (\sigma(\tilde{x}_n), \tilde{y}_n, \sigma(\tilde{z}_n))(\sigma(\bar{x}_l), \bar{y}_l y_l, \sigma(z_l)),$$

where each element in the decomposition belongs to  $K$  (note that  $\sigma(x_1 y_1 \bar{y}_1 \bar{z}_1) = \sigma(x_1 y_1 z_1) \in \sigma(L)$ ), and therefore  $(r, y, s) \in K^{\leq k+2}$ .

In order to prove the converse, let  $K^+ = K^{\leq k}$  for some  $k \in \mathbb{N}$ . We will verify that  $\text{norm}(L^+) = \text{norm}(L^{\leq m(k+1)+k})$ , where  $m$  is the number guaranteed by Lemma 5. Let  $u$  be an arbitrary word from the language  $L^+$ . We have to show  $\text{norm}(u) \in \text{norm}(L^{\leq m(k+1)+k})$ . The first statement of Lemma 5 allows us to assume that  $\text{norm}(u) \neq \varepsilon$ . Because  $L \subseteq \text{norm}(A^*)$ , the word  $u$  can be written in the form

$$u = v_0 x_1 y_1 z_1 v_1 \cdots v_{l-1} x_l y_l z_l v_l,$$

for a certain  $l \in \mathbb{N}$ , where  $x_i, y_i, z_i \in A^*$  satisfy  $y_i \neq \varepsilon$  and  $x_i y_i z_i \in L$ , for  $i = 1, \dots, l$ ,  $v_i \in L^*$ , for  $i = 0, \dots, l$ ,  $\text{norm}(u) = y_1 \cdots y_l$  and

$$\text{norm}(v_0 x_1) = \text{norm}(z_i v_i x_{i+1}) = \text{norm}(z_l v_l) = \varepsilon,$$

for  $i = 1, \dots, l-1$ . This implies that

$$(\sigma(x_1), y_1 \cdots y_l, \sigma(z_l)) = (\sigma(x_1), y_1, \sigma(z_1)) \cdots (\sigma(x_l), y_l, \sigma(z_l)) \in K^l.$$

By the assumption, there exist  $n \in \mathbb{N}$ ,  $n \leq k$ , and  $\tilde{x}_i, \tilde{y}_i, \tilde{z}_i \in A^*$  such that  $\tilde{y}_i \neq \varepsilon$  and  $\tilde{x}_i \tilde{y}_i \tilde{z}_i \in L$ , for  $i = 1, \dots, n$ , which satisfy

$$(\sigma(x_1), \text{norm}(u), \sigma(z_l)) = (\sigma(\tilde{x}_1), \tilde{y}_1, \sigma(\tilde{z}_1)) \cdots (\sigma(\tilde{x}_n), \tilde{y}_n, \sigma(\tilde{z}_n)).$$

According to the definition of the operation of  $\mathfrak{M}$ , words  $\tilde{x}_i$ , for  $i = 2, \dots, n$ , and  $\tilde{z}_i$ , for  $i = 1, \dots, n-1$ , can be chosen so that there exist  $w_i \in L^*$ , for  $i =$

$1, \dots, n-1$ , satisfying  $\text{norm}(\tilde{z}_i w_i \tilde{x}_{i+1}) = \varepsilon$ . By Lemma 5 we can find  $\bar{x}_i, \bar{z}_i \in A^*$ , for  $i = 1, \dots, n$ , and  $\bar{w}_i \in L^{\leq m} \cup \{\varepsilon\}$ , for  $i = 0, \dots, n$ , such that  $\bar{x}_i \tilde{y}_i \bar{z}_i \in L$ , for  $i = 1, \dots, n$ , and

$$\text{norm}(\bar{w}_0 \bar{x}_1) = \text{norm}(\bar{z}_i \bar{w}_i \bar{x}_{i+1}) = \text{norm}(\bar{z}_n \bar{w}_n) = \varepsilon,$$

for  $i = 1, \dots, n-1$  (to get  $\text{norm}(\bar{w}_0 \bar{x}_1) = \varepsilon$ , note that  $x_1 \tilde{y}_1 \tilde{z}_1 \in L$  and  $\text{norm}(v_0 x_1) = \varepsilon$ ). Therefore we have

$$\text{norm}(u) = \tilde{y}_1 \cdots \tilde{y}_n = \text{norm}(\bar{w}_0 \bar{x}_1 \tilde{y}_1 \bar{z}_1 \bar{w}_1 \cdots \bar{w}_{n-1} \bar{x}_n \tilde{y}_n \bar{z}_n \bar{w}_n),$$

and so  $\text{norm}(u)$  belongs to  $\text{norm}(L^{\leq m(k+1)+k})$  as required.  $\square$

**Theorem 2.** *The FPP is uniformly decidable for rational languages in finitely generated monoids whose word problem is solved by a confluent regular system of deletions.*

*Proof.* For given regular languages  $R$  and  $L$ , we can construct by Lemmas 6 and 7 the rational monoid  $\mathfrak{M}$  and the regular language  $K \subseteq \mathfrak{M}$  such that testing whether  $\gamma(L)$  has the FPP in  $\mathfrak{G}$  is equivalent to testing whether  $K$  has the FPP in  $\mathfrak{M}$  (by Proposition 4). Because  $K$  contains only elements of positive length, this can be algorithmically decided using Corollary 1.  $\square$

## References

1. Berstel, J.: *Transductions and Context-Free Languages*. Teubner, Stuttgart (1979).
2. Book, R.V., Otto, F.: *String-Rewriting Systems*. Springer, New York (1993).
3. d'Alessandro, F., Sakarovitch, J.: The finite power property in free groups. *Theoret. Comput. Sci.* **293**(1) (2003) 55–82.
4. Hashiguchi, K.: A decision procedure for the order of regular events. *Theoret. Comput. Sci.* **8**(1) (1979) 69–72.
5. Hashiguchi, K.: Limitedness theorem on finite automata with distance functions. *J. Comput. System Sci.* **24** (1982) 233–244.
6. Hashiguchi, K.: Algorithms for determining relative star height and star height. *Inform. and Comput.* **78**(2) (1988) 124–169.
7. Howie, J.M.: *Fundamentals of Semigroup Theory*. Clarendon Press, Oxford (1995).
8. Kirsten, D.: The finite power problem revisited. *Inform. Process. Lett.* **84**(6) (2002) 291–294.
9. Kunc, M.: Regular solutions of language inequalities and well quasi-orders. *Theoret. Comput. Sci.* **348**(2-3) (2005) 277–293.
10. Linna, M.: Finite power property of regular languages. In: Nivat, M. (ed.): *Automata, Languages and Programming*. North-Holland, Amsterdam (1973) 87–98.
11. Rozenberg, G., Salomaa, A. (eds.): *Handbook of Formal Languages*. Springer, Berlin (1997).
12. Sakarovitch, J.: Easy multiplications. I. The realm of Kleene's theorem. *Inform. and Comput.* **74**(3) (1987) 173–197.
13. Simon, I.: Limited subsets of a free monoid. In: *Proc. 19th Annu. Symp. on Foundations of Computer Science*. IEEE, Piscataway, N.J. (1978) 143–150.
14. Simon, I.: Recognizable sets with multiplicities in the tropical semiring. In: Chytil, M., Janiga, L., Koubek, V. (eds.): *Mathematical Foundations of Computer Science 1988*. Lecture Notes in Comput. Sci., Vol. 324, Springer, Berlin (1988) 107–120.