RAIRO-Theor. Inf. Appl. 45 (2011) 375–381
DOI: 10.1051/ita/2011111 Available online at:
www.rairo-ita.org

THE CYCLICITY PROBLEM FOR THE IMAGES OF $\mathbb{Q}$-RATIONAL SERIES

Juha Honkala[1]

Abstract. We show that it is decidable whether or not a given $\mathbb{Q}$-rational series in several noncommutative variables has a cyclic image. By definition, a series r has a cyclic image if there is a rational number q such that all nonzero coefficients of r are integer powers of q.

Mathematics Subject Classification. 11B85, 11U05, 68Q45.

1. Introduction

We study $\mathbb{Q}$-rational power series in noncommutative variables and their images. By definition, the image $\mathrm{Im}(r)$ of a series r is the set of its coefficients. We say that the image $\mathrm{Im}(r)$ of r is cyclic if there is a rational number q such that

$$\mathrm{Im}(r) \subseteq \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\}.$$

Hence the image of r is cyclic if and only if the set of nonzero coefficients of r is included in a cyclic subgroup of the multiplicative group of nonzero rationals.

If the image of r is cyclic, then in particular the set of prime factors of r is finite. Recall that a prime p is called a prime factor of r if there is a nonzero coefficient of r such that p divides either its numerator or its denominator. $\mathbb{Q}$-rational series in *one* variable having finitely many prime factors are characterized by a theorem of Polya stating that a $\mathbb{Q}$-rational series r in one variable has finitely many prime factors if and only if r is the sum of a polynomial and of a merge of geometric series (see [1,2,4]).

In this note we prove that it is decidable whether or not a given $\mathbb{Q}$-rational series (in several noncommutative variables) has a cyclic image. Our result is related to the conjecture stating that a noncommutative rational series has only

Keywords and phrases. Rational series, images of rational series, decidability.

[1] Department of Mathematics, University of Turku, 20014 Turku, Finland.
juha.honkala@utu.fi

Article published by EDP Sciences

finitely many prime factors if and only if it is unambiguously rational (see [1], p. 76).

For other decidability results concerning the images of $\mathbb{Q}$-rational series we refer to [1,2]. Below we will use the result of Jacob stating that the finiteness of the image of a rational series is a decidable property (see [3]).

2. Definitions and results

Let X be a finite nonempty set of variables. The set of *formal power series* with noncommutative variables in X and rational coefficients is denoted by $\mathbb{Q}\langle\langle X\rangle\rangle$. If $r \in \mathbb{Q}\langle\langle X\rangle\rangle$, r is a mapping from the free monoid X^* generated by X into $\mathbb{Q}$. The image by r of a word $w \in X^*$ is denoted by (r, w) and r is written as

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

The rational number (r, w) is called the *coefficient* of w in r. A power series $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ is called *proper* if $(r, \varepsilon) = 0$. (Here ε is the empty word).

If $r \in \mathbb{Q}\langle\langle X\rangle\rangle$, the *image* $\mathrm{Im}(r)$ of r is the set of its coefficients. Hence

$$\mathrm{Im}(r) = \{(r, w) \mid w \in X^*\}.$$

We say that $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ has a *cyclic image* if there is a nonzero $q \in \mathbb{Q}$ such that

$$\mathrm{Im}(r) \subseteq \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\}.$$

In other words, r has a cyclic image if and only if there is a cyclic subgroup H of nonzero rationals such that all nonzero coefficients of r belong to H.

Example 2.1. If $w \in X^*$ is a word and $x \in X$ is a letter, then $|w|_x$ stands for the number of occurrences of the letter x in w.

Let $X = \{x, y\}$ be an alphabet with two letters and let

$$r = \sum_{w \in X^*} 2^{|w|_x} 3^{|w|_y} w.$$

Define

$$L_1 = (xy)^*, \;\; L_2 = xy^*, \;\; L_3 = \{x^n y^{n^2} \mid n \geq 0\}, \;\; L_4 = \{w \in X^* \mid |w|_x = |w|_y\}.$$

For $i = 1, 2, 3, 4$, define

$$r_i = \sum_{w \in L_i} (r, w)w.$$

Then r_1 and r_4 have cyclic images while r_2 and r_3 do not.

Next we recall the definitions of $\mathbb{Q}$-recognizable and $\mathbb{Q}$-rational series.

A series $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ is called $\mathbb{Q}$-*recognizable* if there exist an integer $n \geq 1$, a monoid morphism

$$\mu : X^* \to \mathbb{Q}^{n\times n}$$

and two matrices $\lambda \in \mathbb{Q}^{1\times n}$ and $\gamma \in \mathbb{Q}^{n\times 1}$ such that for all $w \in X^*$,

$$(r, w) = \lambda\mu(w)\gamma.$$

Then the triple (λ, μ, γ) is called a *linear representation* of r and n is its *dimension*.

To define the family of $\mathbb{Q}$-rational series we first recall what is meant by a rationally closed subset of $\mathbb{Q}\langle\langle X\rangle\rangle$.

If $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ is a proper series, the *star* r^* of r is defined by

$$r^* = \sum_{n=0}^{\infty} r^n.$$

A subset A of $\mathbb{Q}\langle\langle X\rangle\rangle$ is called *rationally closed* if the following conditions hold:

(i) If $r, s \in A$ and $a \in \mathbb{Q}$, then $r + s \in A$, $rs \in A$ and $ar \in A$.

(ii) If $r \in A$ is a proper series, then $r^* \in A$.

Now, a power series $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ is called $\mathbb{Q}$-*rational* if r belongs to the smallest subset of $\mathbb{Q}\langle\langle X\rangle\rangle$ which contains all polynomials and is rationally closed.

By the theorem of Schützenberger, a power series is $\mathbb{Q}$-recognizable if and only if it is $\mathbb{Q}$-rational (see [1,2,6]).

In the next section we will prove the following result.

Theorem 2.2. *It is decidable whether or not a given $\mathbb{Q}$-rational series has a cyclic image.*

3. Proofs

In this section we will prove Theorem 2.2. We will use Jacob's theorem stating that it is decidable whether or not the image of a given rational series is finite (see [1], Cor. VI.2.7, [3]).

Let $r \in \mathbb{Q}\langle\langle X\rangle\rangle$ be a $\mathbb{Q}$-rational series. First, decide whether or not r has a finite image. If so, the image can be computed effectively and it can be decided whether or not r has a cyclic image. Assume then that the image of r is infinite and compute a coefficient q_1 of r such that $q_1 \neq 0$, $q_1 \neq 1$. (To find such a coefficient we compute initial coefficients of r until we find a coefficient q_1 such that $q_1 \neq 0$, $q_1 \neq 1$. Because we know that the image of r is infinite this computation will succeed). Then there are only finitely many rational numbers q such that $q_1 = q^i$ for some integer i. Hence to prove Theorem 2.2 it suffices to show that it is decidable whether or not

$$\mathrm{Im}(r) \subseteq \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\}$$

holds for a given $\mathbb{Q}$-rational series r and a given rational number q.

In the rest of this section we assume that q is a fixed rational number with $|q| \geq 1$.

We first prove a technical lemma.

If $b_0, b_1, \ldots, b_k$ are rational numbers we say that no partial sum of $b_0 + b_1 + \cdots + b_k$ equals zero if for any $s \geq 1$ and $i_1, \ldots, i_s$ with $0 \leq i_1 < i_2 < \cdots < i_s \leq k$ we have $b_{i_1} + \cdots + b_{i_s} \neq 0$.

Let $a_0 \in \mathbb{Q} - \{0\}$ and $A = \{a_1, \ldots, a_k\} \subseteq \mathbb{Q} - \{0\}$ and define

$$r(a_0, A) = \{ \, |a_0 + a_1 q^{-\alpha_1} + \cdots + a_k q^{-\alpha_k}| \mid \alpha_i \text{ is a nonnegative integer for } i = 1, \ldots, k \text{ and no partial sum of } a_0 + a_1 q^{-\alpha_1} + \cdots + a_k q^{-\alpha_k} \text{ equals zero} \}.$$

Lemma 3.1. *One can effectively compute a positive lower bound for the set* $r(a_0, A)$.

Proof. Without loss of generality we assume that $|q| > 1$. (Recall that we have $|q| \geq 1$. If $|q| = 1$, then the claim is clear because then $r(a_0, A)$ is a finite set). First, compute a positive integer e such that

$$|a_0 + a_1 q^{-\beta_1} + \cdots + a_k q^{-\beta_k}| > \frac{1}{2}|a_0|$$

whenever $\beta_j \geq e$ for $j = 1, \ldots, k$. (In fact, it is enough to choose e such that $|a_i q^{-e}| < \frac{1}{2k}|a_0|$ for all $i = 1, \ldots, k$). Because $r(a_0, A)$ is included in the union of the sets

$$\{|a_0 + a_1 q^{-\beta_1} + \cdots + a_k q^{-\beta_k}| \mid \beta_j \geq e \text{ for } j = 1, \ldots, k\} \tag{3.1}$$

and the sets

$$r(a_0 + a_j q^{-\alpha}, A - \{a_j\}) \tag{3.2}$$

where $1 \leq j \leq k$, $0 \leq \alpha < e$ and $a_0 + a_j q^{-\alpha} \neq 0$, a positive lower bound for $r(a_0, A)$ is obtained by computing positive lower bounds for the sets (3.1) and (3.2). Finally, $\frac{1}{2}|a_0|$ is a lower bound for (3.1) and for sets (3.2) positive lower bounds can be computed inductively. □

For the rest of this section we assume that $r \in \mathbb{Q}\langle\langle X \rangle\rangle$ is a fixed $\mathbb{Q}$-rational series and that (λ, μ, γ) is a linear representation of r having dimension k.

Let $w_0 \in X^*$ be a word of length k. Then there exist words $w_1, \ldots, w_k \in X^*$, each having length less than k, and rational numbers $c_1, \ldots, c_k$ such that

$$(r, ww_0) = c_1(r, ww_1) + \cdots + c_k(r, ww_k)$$

for all $w \in X^*$ (see, *e.g.*, [5], exercise II.3.7).

Lemma 3.2. *Let $w_0 \in X^*$ be a word of length k. Let $w_1, \ldots, w_k$ and $c_1, \ldots, c_k$ be as above. One can compute an integer $K(w_0)$ which has the following property. If*

$$\operatorname{Im}(r) \subseteq \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\} \tag{3.3}$$

and $w \in X^*$, then either

$$(r, ww_0) = 0$$

or there is an integer $i \in \{1, \ldots, k\}$ and an integer β such that

$$(r, ww_0) = q^\beta \cdot (r, ww_i) \tag{3.4}$$

and

$$|\beta| \leq K(w_0). \tag{3.5}$$

Proof. The claim holds if $|q| = 1$. Indeed, in this case the claim holds if we take $K(w_0) = 1$. Assume that $|q| > 1$. (Recall that we have $|q| \geq 1$). By Lemma 3.1 we can compute a positive rational number B_1 such that

$$B_1 \leq x$$

whenever $x \in r(c_i, D)$ for some $i \in \{1, \ldots, k\}$ and $D \subseteq \{c_1, \ldots, c_k\} - \{c_i\}$. (Here we assume that $\{c_i\} \cup D \subseteq \mathbb{Q} - \{0\}$.) Define

$$B_2 = |c_1| + \cdots + |c_k|$$

and compute a nonnegative integer $K(w_0)$ such that

$$B_1 \geq |q|^{-K(w_0)} \quad \text{and} \quad B_2 \leq |q|^{K(w_0)}.$$

Now, suppose (3.3) holds, $w \in X^*$ and $(r, ww_0) \neq 0$. Then there exist an integer t, integers $i_1, \ldots, i_t \in \{1, \ldots, k\}$ and integers $\alpha_1, \ldots, \alpha_t$ such that

$$(r, ww_0) = c_{i_1} \cdot q^{\alpha_1} + \cdots + c_{i_t} \cdot q^{\alpha_t} \tag{3.6}$$

and no partial sum of the right side of (3.6) equals zero. Furthermore,

$$(r, ww_{i_j}) = q^{\alpha_j}$$

for $j = 1, \ldots, t$.

Without loss of generality assume that

$$\alpha_1 = \max\{\alpha_1, \ldots, \alpha_t\}.$$

Then

$$(r, ww_0) = q^{\alpha_1}(c_{i_1} + c_{i_2} q^{\alpha_2 - \alpha_1} + \cdots + c_{i_t} q^{\alpha_t - \alpha_1}),$$

where

$$B_1 \leq |c_{i_1} + c_{i_2} q^{\alpha_2 - \alpha_1} + \cdots + c_{i_t} q^{\alpha_t - \alpha_1}| \leq B_2.$$

Hence

$$|q|^{-K(w_0)} \leq \left| \frac{(r, ww_0)}{(r, ww_{i_1})} \right| \leq |q|^{K(w_0)}.$$

Because by assumption $(r, ww_0) \in \{q^\alpha \mid \alpha \in \mathbb{Z}\}$ and $(r, ww_{i_1}) \in \{q^\alpha \mid \alpha \in \mathbb{Z}\}$, it follows that there is an integer $i \in \{1, \ldots, k\}$ and an integer β such that (3.4) and (3.5) hold. □

Let again $w_0 \in X^*$ be a word of length k. Let $w_1, \ldots, w_k \in X^*$ and $K(w_0)$ be as in Lemma 3.2. Define the series $S(w_0) \in \mathbb{Q}\langle\langle X\rangle\rangle$ by

$$(S(w_0), w) = (r, ww_0) \cdot \prod_{1\le i\le k, |\beta|\le K(w_0)} ((r, ww_0) - q^\beta (r, ww_i))$$

for $w \in X^*$.

Lemma 3.3. *The series $S(w_0)$ is $\mathbb{Q}$-rational.*

Proof. Let $1 \le i \le k$ and let β be an integer such that $|\beta| \le K(w_0)$. Because

$$(r, ww_0) - q^\beta (r, ww_i) = \lambda\mu(ww_0)\gamma - q^\beta \lambda\mu(ww_i)\gamma = \lambda\mu(w)(\mu(w_0)\gamma - q^\beta \mu(w_i)\gamma)$$

for all $w \in X^*$, the series

$$\sum_{w\in X^*} ((r, ww_0) - q^\beta (r, ww_i))w$$

is $\mathbb{Q}$-rational. The claim follows because the Hadamard product of finitely many $\mathbb{Q}$-rational series is $\mathbb{Q}$-rational. □

The following lemma explains the connection between the cyclicity of the image of r and the vanishing of the series $S(w_0)$ for all $w_0 \in X^*$ with $|w_0| = k$.

Lemma 3.4. *We have*

$$\mathrm{Im}(r) \subseteq \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\} \tag{3.7}$$

if and only if

$$(r, w) \in \{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\} \text{ whenever } w \in X^* \text{ and } |w| < k \tag{3.8}$$

and

$$S(w_0) = 0 \text{ whenever } w_0 \in X^* \text{ and } |w_0| = k. \tag{3.9}$$

Proof. Assume first that (3.7) holds. Then trivially (3.8) holds. By Lemma 3.2 and the definition of the series $S(w_0)$ also (3.9) holds.

Conversely, assume that (3.8) and (3.9) hold. Suppose there is a word v such that (r, v) does not belong to $\{q^\alpha \mid \alpha \in \mathbb{Z}\} \cup \{0\}$. Choose v such that its length is as small as possible. By (3.8), the length of v is at least k. Write $v = ww_0$, where $w, w_0 \in X^*$ and $|w_0| = k$. Because $S(w_0) = 0$, there is a word $\overline{w}$ of length less than k and an integer β such that

$$(r, v) = (r, ww_0) = q^\beta \cdot (r, w\overline{w}).$$

Because (r, v) is not an integer power of q, neither is $(r, w\overline{w})$. This contradicts the choice of v because $|w\overline{w}| < |v|$. □

Now the decidability of (3.7) follows because we can decide (3.8) and (3.9). To decide (3.9) we use Lemma 3.3 and the fact that it is decidable whether or not a given rational series equals zero (see [1], Prop. VI.1.1). This concludes the proof of Theorem 2.2.

Acknowledgements. The useful suggestions of two referees are gratefully acknowleged.

References

[1] J. Berstel and C. Reutenauer, *Rational Series and Their Languages*. Springer, Berlin (1988).
[2] J. Berstel and C. Reutenauer, *Noncommutative Rational Series with Applications*. Cambridge University Press, Cambridge (2011).
[3] G. Jacob, La finitude des représentations linéaires des semi-groupes est décidable. *J. Algebra* **52** (1978) 437–459.
[4] G. Polya, Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen. *J. Reine Angew. Math.* **151** (1921) 1–31.
[5] A. Salomaa and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*. Springer, Berlin (1978).
[6] M.-P. Schützenberger, On the definition of a family of automata, *Inf. Control* **4** (1961) 245–270.

Communicated by C. Choffrut.
Received May 31, 2010. Accepted June 27, 2011.