Theoretical Computer Science 998 (2024) 114540

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Rational power series in several noncommuting variables and the Skolem–Mahler–Lech theorem ☆

Juha Honkala

Department of Mathematics and Statistics, University of Turku, FI-20014 Turku, Finland

ARTICLE INFO

Keywords:
Formal power series
Skolem–Mahler–Lech theorem
Slender language
Single loop language

ABSTRACT

We generalize the Skolem–Mahler–Lech theorem for rational power series in several noncommuting variables having a slender support. This generalization gives a connection between the Skolem–Mahler–Lech theorem and the characterization of slender regular languages proved independently by Păun and Salomaa and by Shallit.

1. Introduction

Let K be a field of characteristic zero and let $(a_n)_{n\geq 0}$ be a K-rational sequence. The Skolem–Mahler–Lech theorem states that the set

$$\{n \in \mathbb{N} \mid a_n = 0\}$$

is the union of a finite set and of a finite number of arithmetic progressions (see [1,3]). Skolem [14] proved this result for integer sequences. Mahler [8] extended the result for algebraic number fields, and Lech [7] to all fields of characteristic zero. The original proofs by Skolem, Mahler and Lech use p-adic analysis. Hansel [4] gave a proof which uses some p-adic ideas, but does not use p-adic analysis. For a presentation of Hansel's proof, see also [1].

The Skolem–Mahler–Lech theorem implies that the support of a rational series in one variable with coefficients in a field of characteristic zero is a regular language. It is well known that this does not hold for rational series in two or more variables.

The purpose of this note is to argue that the assumption that the series is in one variable can be replaced by the assumption that the series has only a limited number of terms of each degree, a property which holds trivially for series in one variable.

Following Păun and Salomaa [9] we call a language L slender if there is a positive integer k such that for every positive integer n, L contains at most k words of length n. A language L is called a single loop language if there exist words u, v, w such that $L = uv^*w = \{uv^n w \mid n \geq 0\}$. Clearly, a single loop language is slender. Păun and Salomaa [9] and Shallit [13] have independently proved that if a regular language is slender, then it is a finite union of single loop languages.

We will show that if a rational series in any number of variables having coefficients in a field of characteristic zero has a slender support, then the support is a finite union of single loop languages. In particular, the support is a regular language.

Our extension of the Skolem–Mahler–Lech theorem brings out a link between the Skolem–Mahler–Lech theorem and the characterization of slender regular languages. In fact, the characterization is a special case of the extension.

☆ This article belongs to Section C: Theory of natural computing, Edited by Lila Kari.

E-mail address: juha.honkala@utu.fi.

https://doi.org/10.1016/j.tcs.2024.114540
Received 11 December 2023; Received in revised form 12 March 2024; Accepted 27 March 2024

Available online 2 April 2024

We assume that the reader is familiar with the basics of rational series (see [1,2,6,12]). We use standard terminology and notation concerning words and languages (see [11]).

2. Definitions and results

The *free monoid* generated by a finite nonempty set X is denoted by X^*. The identity element of X^* is the *empty word* ε. The *length* of a word w is $|w|$. If w is a word, then $w[i]$ is the ith letter of w for $i = 1, \ldots, |w|$. The last letter of a nonempty word w is $\mathrm{last}(w)$. A nonempty word w is *primitive* if w is not a power of a shorter word. If u, v, w are words such that $uv = w$, we denote $v = u^{-1}w$ and $u = wv^{-1}$.

A language L is *slender* if there is a positive integer k such that for every positive integer n, L contains at most k words of length n. A language L is called *a single loop language* if there exist words u, v, w such that

$$L = uv^*w = \{uv^nw \mid n \geq 0\}$$

(see [9]). Single loop languages are slender.

Let d be a positive integer. A set A of nonnegative integers is called *d-syndetic* if

$$A \cap \{n, n+1, \ldots, n+d-1\} \neq \emptyset$$

for all nonnegative integers n. In this note we require this condition for all n. In the literature, usually finitely many exceptional values are allowed.

Next we recall some notions concerning formal power series. Let K be a commutative semiring and let X be a finite nonempty set of variables. The set of *formal power series with noncommuting variables* in X and coefficients in K is denoted by $K\langle\langle X\rangle\rangle$. If $r \in K\langle\langle X\rangle\rangle$, r is a mapping from X^* to K. The image of a word $w \in X^*$ by r is denoted (r, w) and r is written as

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

Here (r, w) is called the *coefficient* of w in r.

If $r \in K\langle\langle X\rangle\rangle$, the *support* of r is the set

$$\mathrm{supp}(r) = \{w \in X^* \mid (r, w) \neq 0\}.$$

A formal series with a finite support is called a *polynomial*. The subset of $K\langle\langle X\rangle\rangle$ consisting of polynomials is denoted by $K\langle X\rangle$.

A series $r \in K\langle\langle X\rangle\rangle$ is called *proper* if the coefficient of the empty word ε vanishes. If $r \in K\langle\langle X\rangle\rangle$ is proper, the series r^* is defined by

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

Next we recall the definitions of recognizable and rational series.

Let p, q be positive integers. Then $K^{p\times q}$ is the set of $p \times q$ matrices with entries in K.

A series $r \in K\langle\langle X\rangle\rangle$ is called *recognizable* if there is an integer $d \geq 1$, a monoid morphism $\mu : X^* \to K^{d\times d}$ and two matrices $\alpha \in K^{1\times d}$ and $\beta \in K^{d\times 1}$ such that

$$(r, w) = \alpha\mu(w)\beta$$

for all $w \in X^*$.

A subsemiring of $K\langle\langle X\rangle\rangle$ is called *rationally closed* if it contains r^* whenever it contains a proper series r. The family of *K-rational series* is the smallest rationally closed subsemiring of $K\langle\langle X\rangle\rangle$ which contains all polynomials.

It is well known that a series is rational if and only if it is recognizable (see [1,2,6,12]).

We now state the Skolem–Mahler–Lech theorem.

Theorem 1 *(Skolem, Mahler, Lech). Let K be a field of characteristic 0 and let z be a letter. Assume that $r = \sum r_n z^n \in K\langle\langle z\rangle\rangle$ is K-rational. Then the set*

$$\{n \in \mathbb{N} \mid r_n = 0\}$$

is the union of a finite set and of a finite number of arithmetic progressions.

In the next section we will prove the following extension of the Skolem–Mahler–Lech theorem.

Theorem 2. *Let K be a field of characteristic 0 and let X be a finite nonempty set. Let $r \in K\langle\langle X\rangle\rangle$ be a K-rational series. Assume that* $\mathrm{supp}(r)$ *is slender. Then* $\mathrm{supp}(r)$ *is a finite union of single loop languages.*

If X is a one-element set, Theorem 2 is equivalent with the Skolem–Mahler–Lech theorem. For every X, Theorem 2 implies that if the support of a K-rational series r is slender, then $\mathrm{supp}(r)$ is a regular language.

If L is a slender regular language, then the characteristic series of L is K-rational and has a slender support. Hence Theorem 2 implies that L is a finite union of single loop languages.

3. Proof of Theorem 2

Let K be a field of characteristic 0 and let X be a finite nonempty set.

We will use the following iteration theorem for rational series.

Theorem 3. *Let $s \in K\langle\langle X \rangle\rangle$ be K-rational. There exists an integer k such that every word y in $\mathrm{supp}(s)$, $|y| \geq k$, can be written as $y = uvw$ such that $|v| \leq k$ and the set*

$$uv^*w \cap \mathrm{supp}(s)$$

is infinite.

Theorem 3 is a consequence of a stronger iteration theorem due to Jacob [5] (see also [1,10]).

For the remaining part of this section, fix a K-rational series $r \in K\langle\langle X \rangle\rangle$ and let $L = \mathrm{supp}(r)$.

Corollary 4. *There is a positive integer k such that if $y \in L$ and $|y| \geq k$, then there are words $u, v, w \in X^*$ satisfying the following conditions:*
(i) $|v| \leq k$,
(ii) $y \in uv^*w$,
(iii) $uv^*w \cap L$ is infinite,
(iv) v is primitive,
(v) either $u = \varepsilon$ or $\mathrm{last}(u) \neq \mathrm{last}(v)$,
(vi) v is not a prefix of w.

Proof. By Theorem 3 there exists a positive integer k such that if $y \in L$ and $|y| \geq k$, there exist $u, v, w \in X^*$ satisfying (i), (ii) and (iii).

It is easy to modify the words u, v, w so that they satisfy also (iv), (v) and (vi). Indeed, if v is not primitive, replace v by its primitive root. If $u \neq \varepsilon$ and $\mathrm{last}(u) = \mathrm{last}(v)$, replace u, v and w by $u\,\mathrm{last}(u)^{-1}$, $\mathrm{last}(u)v\,\mathrm{last}(v)^{-1}$ and $\mathrm{last}(v)w$, respectively. Repeat this step until (v) holds. Finally, if v is a prefix of w, replace w by $v^{-1}w$ as many times as needed. □

Let k be as in Corollary 4. Let

$$T = \{(u, v, w) \in X^* \times X^* \times X^* \mid \text{(i), (iv), (v) and (vi) of Corollary 4 hold}\}$$

and

$$T_\infty = \{(u, v, w) \in T \mid uv^*w \cap L \text{ is infinite }\}.$$

The following result is an immediate consequence of Corollary 4.

Corollary 5. *Let k be as in Corollary 4. Denote $X^{<k} = \{z \in X^* \mid |z| < k\}$. Then*

$$L = \bigcup_{(u,v,w) \in T_\infty} (L \cap uv^*w) \cup (L \cap X^{<k}).$$

To conclude the proof of Theorem 2 we show that T_∞ is a finite set and that for every $(u, v, w) \in T_\infty$, the set $L \cap uv^*w$ is a finite union of single loop languages. The finiteness of T_∞ requires three lemmas while the second claim follows easily by the Skolem–Mahler–Lech theorem.

Lemma 6. *Let $(u_i, v_i, w_i) \in T$ for $i = 1, 2$. If*

$$u_1v_1^*w_1 \cap u_2v_2^*w_2 \tag{1}$$

is infinite, then $(u_1, v_1, w_1) = (u_2, v_2, w_2)$.

Proof. Assume that (1) is infinite. We show first that $|u_1| = |u_2|$. Assume on the contrary that, say, $|u_1| < |u_2|$. If n is a large integer, then

$$\begin{aligned}\text{last}(u_2) &= (u_2 v_2^n)[|u_2|] = (u_1 v_1^n)[|u_2|] = (u_1 v_1^n)[|u_2| + |v_1||v_2|] \\ &= (u_2 v_2^n)[|u_2| + |v_1||v_2|] = \text{last}(v_2),\end{aligned}$$

which contradicts the assumption that $(u_2, v_2, w_2) \in T$. Hence $|u_1| = |u_2|$, which implies that $u_1 = u_2$. It follows that

$$v_1^* w_1 \cap v_2^* w_2$$

is infinite. This implies that

$$v_1^{|v_2|} = v_2^{|v_1|}.$$

Since v_1 and v_2 are primitive, we have $v_1 = v_2$. Finally, since v_1 is not a prefix of w_1 and v_2 is not a prefix of w_2, we get $w_1 = w_2$. □

Since r is K-rational, there is an integer $d \geq 1$, a monoid morphism $\mu : X^* \to K^{d\times d}$ and two matrices $\alpha \in K^{1\times d}$, $\beta \in K^{d\times 1}$ such that

$$(r, y) = \alpha \mu(y) \beta$$

for all $y \in X^*$.

Recall that a set of nonnegative integers is called *eventually periodic* if it is a finite union of arithmetic progressions.

Lemma 7. *Let $(u, v, w) \in T_\infty$ and let d be as above. Then the set*

$$\{n \mid uv^n w \in L\} \tag{2}$$

is d-syndetic and eventually periodic. Consequently, the set

$$L \cap uv^* w \tag{3}$$

is a finite union of single loop languages.

Proof. Define the sequence $(a_n)_{n\geq 0}$ by

$$a_n = (r, uv^n w)$$

for $n \geq 0$. Let $\alpha_1 = \alpha\mu(u)$ and $\beta_1 = \mu(w)\beta$. Then for $n \geq 0$,

$$a_n = \alpha_1 \mu(v)^n \beta_1.$$

Hence there exist $c_1, \ldots, c_d \in K$ such that

$$a_{n+d} = c_1 a_{n+d-1} + \cdots + c_d a_n$$

for all $n \geq 0$. Now, if there were a nonnegative integer m such that $a_m = \cdots = a_{m+d-1} = 0$, the sequence (a_n) would be eventually zero. This is not possible since $(u, v, w) \in T_\infty$. Hence (2) is d-syndetic. The Skolem–Mahler–Lech theorem implies that the complement of the set (2) and, hence, the set (2) is eventually periodic. This implies that (3) is a finite union of single loop languages. □

In what follows we need the fact that all of the sets (2) considered in Lemma 7 are syndetic with the same constant d. This fact is not an immediate consequence of the eventual periodicity of the sets.

Lemma 8. *Assume that $L = \text{supp}(r)$ is slender. Then T_∞ is a finite set.*

Proof. Assume on the contrary that T_∞ is an infinite set.

Let s be an arbitrary integer. Denote $q = dks + 1$. Here d is the constant from Lemma 7 and k is the constant from Corollary 4. Since T_∞ is infinite, T_∞ contains q distinct elements (u_i, v_i, w_i), $1 \leq i \leq q$. By Lemma 6, the set

$$u_i v_i^* w_i \cap u_j v_j^* w_j$$

is finite if $1 \leq i < j \leq q$. Let

$$m = \max\{|y| \mid y \in u_i v_i^* w_i \cap u_j v_j^* w_j \text{ for some } 1 \leq i < j \leq q\}.$$

Now, denote

$$\ell_1 = m + 1 + \sum_{i=1}^{q} |u_i w_i|$$

and

$$\ell_2 = \ell_1 + dk.$$

Fix $i \in \{1, \ldots, q\}$. Since $|u_i w_i| < \ell_1$, there is a nonnegative integer n such that

$$\ell_1 \le |u_i v_i^n w_i| < \ell_1 + |v_i|.$$

By Lemma 7 there is an integer $n_i \in \{n, n+1, \ldots, n+d-1\}$ such that

$$u_i v_i^{n_i} w_i \in L.$$

Here

$$\begin{aligned}\ell_1 \le |u_i v_i^{n_i} w_i| &= |u_i v_i^n w_i| + (n_i - n)|v_i| < \ell_1 + |v_i| + (n_i - n)|v_i| \\ &\le \ell_1 + d|v_i| \le \ell_1 + dk = \ell_2.\end{aligned}$$

Now, let

$$K = \{y \in L \mid \ell_1 \le |y| < \ell_2\}.$$

We have seen that every loop $u_i v_i^* w_i$, $1 \le i \le q$, gives at least one word of K. Since $\ell_1 > m$, no two loops give the same word. Hence K contains at least q words. Since $q = dks + 1$ and $\ell_2 - \ell_1 = dk$, it follows that K contains more than s words having the same length. This contradicts the assumption that L is slender, since s was an arbitrary positive integer. □

Now Theorem 2 follows by Corollary 5, Lemma 7 and Lemma 8.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] J. Berstel, C. Reutenauer, Noncommutative Rational Series with Applications, Cambridge University Press, 2011.
[2] M. Droste, W. Kuich, H. Vogler (Eds.), Handbook of Weighted Automata, Springer, 2009.
[3] G. Everest, A. van der Poorten, I. Shparlinski, T. Ward, Recurrence Sequences, American Mathematical Society, 2003.
[4] G. Hansel, Une démonstration simple du théorème de Skolem–Mahler–Lech, Theor. Comput. Sci. 43 (1986) 91–98.
[5] G. Jacob, Un théorème de factorisation des produits d'endomorphismes de k^n, J. Algebra 63 (1980) 389–412.
[6] W. Kuich, A. Salomaa, Semirings, Automata, Languages, Springer, 1986.
[7] C. Lech, A note on recurring series, Ark. Mat. 2 (1953) 417–421.
[8] K. Mahler, Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen, Proc. Akad. Wet. Amst. 38 (1935) 51–60.
[9] G. Păun, A. Salomaa, Thin and slender languages, Discrete Appl. Math. 61 (1995) 257–270.
[10] C. Reutenauer, An Ogden-like iteration lemma for rational power series, Acta Inform. 13 (1980) 189–197.
[11] G. Rozenberg, A. Salomaa (Eds.), Handbook of Formal Languages, vols. 1-3, Springer, 1997.
[12] A. Salomaa, M. Soittola, Automata-Theoretic Aspects of Formal Power Series, Springer, 1978.
[13] J. Shallit, Numeration systems, linear recurrences, and regular sets, Inf. Comput. 113 (1994) 331–347.
[14] T. Skolem, Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen, in: Comptes Rendus du Congrés des Mathèmaticiens Scandinaves, Stockholm, 1934, 1935, pp. 163–188.