On Power Series over a Graded Monoid

Zoltán Ésik[1] and Werner Kuich[2(✉)]

[1] University of Szeged, Szeged, Hungary
[2] Technische Universität Wien, Vienna, Austria
werner.kuich@tuwien.ac.at

Abstract. We consider power series over a graded monoid M of finite type. We show first that, under certain conditions, the equivalence problem of power series over M with coefficients in the semiring $\mathbb{N}$ of nonnegative integers can be reduced to the equivalence problem of power series over $\{x\}^*$ with coefficients in $\mathbb{N}$. This result is then applied to rational and recognizable power series over M with coefficients in $\mathbb{N}$, and to rational power series over Σ^* with coefficients in the semiring $\mathbb{Q}_+$ of nonnegative rational numbers, where Σ is an alphabet.

1 Power Series over a Graded Monoid and a Decidability Result

In [4], Sakarovitch considers power series over a graded monoid. Let $\langle M, \cdot, 1\rangle$ be a monoid and let $|\ | : M \to \mathbb{N}$ be a mapping, called *length*, such that

(i) $|m| > 0$ for all $m \in M$, $m \neq 1$;
(ii) $|m \cdot n| = |m| + |n|$ for all $m, n \in M$.

Then $\langle M, \cdot, 1\rangle$ is called *graded monoid*. The definition implies that $|1| = 0$. If a graded monoid M is finitely generated, we call M a graded monoid of *finite type*. In Section 2 of [4], Sakarovitch proves the following results:

Proposition 1 (Sakarovitch [4])**.** *In a graded monoid of finite type, the number of elements whose length is less than an arbitrary given integer $n > 0$ is finite.*

A monoid is called *finitely decomposable* if, for all $m \in M$, the set of pairs (m_1, m_2) such that $m_1 m_2 = m$ is finite.

Corollary 1 (Sakarovitch [4])**.** *In a graded monoid of finite type, every element is finitely decomposable.*

Let S be a semiring and M be a graded monoid of finite type. Then any mapping from M into S is a *(formal) power series* (*over M with coefficients in S*). The set of all these power series is denoted by $S\langle\langle M\rangle\rangle$. If r is a power series

Partially supported by grant no. K 108448 from the National Foundation of Hungary for Scientific Research.
Partially supported by Austrian Science Fund (FWF): grant no. I1661-N25.

C.S. Calude et al. (Eds.): Gruska Festschrift, LNCS 8808, pp. 49–55, 2014.
DOI: 10.1007/978-3-319-13350-8_4

then the image of an element $m \in M$ under r is denoted by (r, m) which is called *coefficient* of m and the power series is written as

$$r = \sum_{m \in M} (r, m)m \,.$$

Power series where almost all coefficients are 0 are called *polynomials*. The set of all polynomials is denoted by $S\langle M \rangle$.

For all $r_1, r_2 \in S\langle\langle M \rangle\rangle$, we consider the following operations:

(i) the (pointwise) addition of r_1 and r_2, denoted by $r_1 + r_2$ and defined by

$$(r_1 + r_2, m) = (r_1, m) + (r_2, m) \text{ for all } m \in M;$$

(ii) the (Cauchy) product of r_1 and r_2, denoted by $r_1 \cdot r_2$ and defined by

$$(r_1 \cdot r_2, m) = \sum_{m_1 m_2 = m} (r_1, m_1)(r_2, m_2) \text{ for all } m \in M;$$

(iii) the (pointwise) Hadamard product of r_1 and r_2, denoted by $r_1 \odot r_2$ and defined by

$$(r_1 \odot r_2, m) = (r_1, m)(r_2, m) \text{ for all } m \in M;$$

Moreover, we consider the scalar multiplications of $s \in S$ and $r \in S\langle\langle M \rangle\rangle$ denoted by $s \cdot r$ and $r \cdot s$ and defined by

$$(s \cdot r, m) = s \cdot (r, m) \text{ and } (r \cdot s, m) = (r, m) \cdot s \text{ for all } m \in M, \text{ respectively.}$$

The power series 0 and 1 are defined by

$$\begin{aligned} &(0, m) = 0 \text{ for all } m \in M \text{ and} \\ &(1, 1) = 1, \quad (1, m') = 0 \text{ for all } m' \in M,\ m' \neq m, \text{ respectively.} \end{aligned}$$

Proposition 2 (Sakarovitch [4])**.** *Let M be a graded monoid of finite type and S a semiring. Then $\langle S\langle\langle M \rangle\rangle, +, \cdot, 0, 1\rangle$ and $\langle S\langle M \rangle, +, \cdot, 0, 1\rangle$ are semirings.*

In the sequel, $\langle M, \cdot, 1\rangle$ will always denote a graded monoid of finite type and S will denote a semiring.

A power series $r \in S\langle\langle M \rangle\rangle$ is called *cycle-free* if there exists an $n \geq 1$ such that $(r, 1)^n = 0$; it is called *proper* if $(r, 1) = 0$. Let $r \in S\langle\langle M \rangle\rangle$. Then the *proper part* of r is the power series $\sum_{m \in M,\ m \neq 1} (r, m)m$ and the *constant term* of r is the power series $(r, 1)1$, also written $(r, 1)$. If $r \in S\langle\langle M \rangle\rangle$ is cycle-free then $\{n \mid (r^n, m) \neq 0\}$ is locally finite, i. e., is a finite set for all $m \in M$. Hence, the infinite sum

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

is defined; it is called the *star of* r.

Proposition 3 (Sakarovitch [4]). *Let $r \in S\langle\langle M\rangle\rangle$ be a cycle-free power series with constant term r_0 and proper part r_1. Then*

$$r^* = (r_0^* r_1)^* r_0^* = r_0^*(r_1 r_0^*)^* .$$

Defining $\varphi : \mathbb{N}\langle\langle M\rangle\rangle \to \mathbb{N}\langle\langle \{x\}^*\rangle\rangle$, x a symbol, by

$$\varphi(r) = \sum_{m \in M} (r, m) x^{|m|} ,$$

it is easily shown that φ is a semiring morphism. The mapping φ is also compatible with the star operation applied to a cycle-free power series r, i. e.,

$$\varphi(r^*) = \varphi(r)^* \text{ if } r \in \mathbb{N}\langle\langle M\rangle\rangle \text{ is cycle-free.}$$

A power series $r \in S\langle\langle M\rangle\rangle$ is termed *rational* (over S and M) if r can be obtained from polynomials of $S\langle M\rangle$ by finitely many applications of the *rational operations* $+, \cdot, ^*$, where * is applied only to *proper* power series. The family of rational power series (over S and M) is denoted by $S^{\mathrm{rat}}\langle\langle M\rangle\rangle$. By Proposition 3, we get an equivalent definition of rational power series if we replace *proper* by *cycle-free*. The formula telling how a given rational power series r is obtained from these polynomials by rational operations is referred to as a *rational expression for r*.

Theorem 1. *Let M be a graded monoid of finite type and assume that $|\ | : M \to \mathbb{N}$ is recursive. Then φ, as a mapping $\mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle \to \mathbb{N}^{\mathrm{rat}}\langle\langle \{x\}^*\rangle\rangle$, is recursive.*

Proof. We prove the theorem by induction on the structure of a rational power series $r \in \mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle$. We show that from a rational expression for $r \in \mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle$ we can compute a rational expression for $\varphi(r)$ since φ is a semiring morphism preserving *.

(i) For $r = n$, $n \in \mathbb{N}$, $\varphi(r) = n\varepsilon$. For $r = a$, $a \in M$, $\varphi(a) = x^{|a|}$. Since φ is a semiring morphism, $\varphi(p) \in \mathbb{N}\langle \{x\}^*\rangle$ for $p \in \mathbb{N}\langle M\rangle$.

(ii) Since φ is a semiring morphism, we obtain $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$.

(iii) Since φ is a semiring morphism, we obtain, for a proper power series in $\mathbb{N}\langle\langle M\rangle\rangle$,

$$\varphi(r^*) = \sum_{n \geq 0} \varphi(r^n) = \sum_{n \geq 0} \varphi(r)^n = \varphi(r)^* .$$

□

We call a power series $r \in S\langle\langle M\rangle\rangle$ *unambiguous* if, for all $m \in M$, $(r, m) \in \{0, 1\}$.

In the proof of our next theorem we use the following equality:

$$(\varphi(r), x^k) = \sum_{|m| = k} (r, m), \quad r \in \mathbb{N}\langle\langle M\rangle\rangle,\ k \geq 0 .$$

This next theorem is a generalization of Theorems 16.21 and 16.22 of Kuich, Salomaa [3].

Theorem 2. *Let M be a graded monoid of finite type and assume that $|\ |: M \to \mathbb{N}$ is recursive. Then*

(i) for $r_1, r_2 \in \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$ with $(r_1, m) \geq (r_2, m)$ for all $m \in M$ the problem whether or not $r_1 = r_2$ is decidable;
(ii) if $\mathfrak{R} \subseteq \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$ such that, for $s_1 \in \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$ and $s_2 \in \mathfrak{R}$, $s_1 \odot s_2$ is in $\mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$, then for two unambiguous power series $r_1 \in \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$ and $r_2 \in \mathfrak{R}$ the problem whether or not $r_1 = r_2$ is decidable.

Proof. By Theorem 1 the mapping $\varphi : \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle \to \mathbb{N}^{\mathrm{rat}}\langle\langle \{x\}^* \rangle\rangle$ is recursive. By Corollary 8.18 of Kuich, Salomaa [3] the equivalence problem for power series in $\mathbb{N}^{\mathrm{rat}}\langle\langle \{x\}^* \rangle\rangle$ is decidable. Hence, for two given rational power series r_1 and r_2 in $\mathbb{N}^{\mathrm{rat}}\langle\langle \{x\}^* \rangle\rangle$ we can decide, whether or not $\varphi(r_1) = \varphi(r_2)$.

(i) If $\varphi(r_1) = \varphi(r_2)$ then, for all $k \geq 0$, $\sum_{|m|=k}(r_1, m) = \sum_{|m|=k}(r_2, m)$. Hence, $(r_1, m) \geq (r_2, m)$ for all $m \in M$ implies $(r_1, m) = (r_2, m)$. If $\varphi(r_1) \neq \varphi(r_2)$ then, for some $k \geq 0$, $\sum_{|m|=k}(r_1, m) \neq \sum_{|m|=k}(r_2, m)$. Hence, for some $m' \in M$ of length k we obtain $(r_1, m') \neq (r_2, m')$.

(ii) Since (r_1, m) and (r_2, m) are in $\{0, 1\}$ for all $m \in M$, we obtain $(r_1 \odot r_2, m) \leq (r_1, m)$ and $(r_1 \odot r_2, m) \leq (r_2, m)$ for all $m \in M$. By (i) it is decidable whether or not $r_1 \odot r_2 = r_1$ and $r_1 \odot r_2 = r_2$. Clearly, $r_1 = r_2$ iff $r_1 \odot r_2 = r_1$ and $r_1 \odot r_2 = r_2$. Hence, $r_1 = r_2$ is decidable. □

2 Decidability Problems for Unambiguous Power Series

In the sequel, Σ, $1 \notin \Sigma$, denotes a finite generating set of M and S denotes a semiring. We write Σ^* for the set of all finite products of elements of Σ. Hence, we obtain $\Sigma^* = M$. By $S\langle \Sigma \cup \{1\} \rangle$ and $S\langle \{1\} \rangle$ we denote the set of polynomials of the form $p = (p, 1)1 + \sum_{x \in \Sigma}(p, x)x$ and $p = (p, 1)1$, respectively.

A *finite (weighted) automaton* (over Σ and S)

$$\mathfrak{A} = (Q, R, A, P)$$

is given by

(i) a finite nonempty set Q of *states*,
(ii) a *transition matrix* $A \in (S\langle \Sigma \cup \{1\} \rangle)^{Q \times Q}$,
(iii) an *initial state vector* $R \in (S\langle \{1\} \rangle)^{1 \times Q}$,
(iv) an *final state vector* $P \in (S\langle \{1\} \rangle)^{Q \times 1}$.

The finite automaton $\mathfrak{A}$ is *cycle-free* (resp. *proper*) if the isomorphic copy of A in $S^{Q \times Q}\langle \Sigma \cup \{1\} \rangle$ is cycle-free (resp. proper).

The behavior $||\mathfrak{A}||$ of a cycle-free finite automaton $\mathfrak{A}$ is defined by

$$||\mathfrak{A}|| = \sum_{q_1, q_2 \in Q} R_{q_1} (A^*)_{q_1, q_2} P_{q_2} = RA^*P\,.$$

(See Sakarovitch [4], Section 3 and Gruska [1], Chapter 3.)

By Proposition 3.14 of Sakarovitch [4], for each *cycle-free* finite automaton there exists a *proper* finite automaton with the same behavior.

By Theorem 3.10 of Sakarovitch [4], we obtain

$$S^{\mathrm{rat}}\langle\langle M\rangle\rangle = \{||\mathfrak{A}|| \mid \mathfrak{A} \text{ is a proper finite automaton over } \Sigma \text{ and } S\}\,.$$

Let $\mu : M \to S^{Q\times Q}$, Q a finite index set, be a morphism, and let $\lambda \in S^{1\times Q}$, $\nu \in S^{Q\times 1}$. Then (λ, μ, ν) is called *S-representation of M of dimension Q*. A power series $r \in S\langle\langle M\rangle\rangle$ is called *S-recognizable* if there exists a finite set Q and an S-representation of M of dimension Q (λ, μ, ν) such that

$$r = \sum_{m\in M} (\lambda\mu(m)\nu)m\,.$$

We say then that the S-representation (λ, μ, ν) *recognizes* r. The set of all S-recognizable formal power series is denoted by $S^{\mathrm{rec}}\langle\langle M\rangle\rangle$.

Theorem 3 (Sakarovitch [4], Theorem 4.38**).** *Suppose that S is a commutative semiring. Let $r \in S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ and $u \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$. Then $r \odot u \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$. Moreover, if r is recognized by an S-representation and u is given by a rational expression then a rational expression for $r \odot u$ can be effectively constructed.*

Proof. The first sentence of our theorem is implied by Theorem 4.38 of Sakarovitch [4]. For the proof of the second sentence, we first show that the constructions of Theorems 4.13 and 4.35, and of Proposition 4.33 of Sakarovitch [4] are effective. We use the notation of Sakarovitch [4] as far as possible.

Theorem 4.13: If r and u in $S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ are recognized by the S-representations (λ, μ, ν) and (η, κ, ξ), respectively, then $r \odot u$ is recognized by the S-representation $(\lambda \otimes \eta, \mu \otimes \kappa, \nu \otimes \xi)$, where $\otimes$ denotes the Kronecker product. Clearly, the construction is effective.

Theorem 4.35: Let M and N be graded monoids and $\theta : M \to N$ be a continuous monoid morphism, i. e., $m\theta$ is unequal to the unit of N for all $m \in M$.

(i) From a rational expression for $r \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$ a rational expression for $r\underline{\theta} \in S^{\mathrm{rat}}\langle\langle N\rangle\rangle$ can effectively be constructed.
(ii) If θ is surjective, then from a rational expression for $u \in S^{\mathrm{rat}}\langle\langle N\rangle\rangle$ a rational expression for some $r \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$ such that $r\underline{\theta} = u$ can effectively be constructed.

Proposition 4.33: Let $\theta : M \to N$ be a monoid morphism and $u \in S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ be recognized by the S-representation (λ, μ, ν). Then $u\underline{\theta^{-1}} \in S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ is recognized by the S-representation $(\lambda, \theta\mu, \nu)$. Clearly, the construction of the latter S-representation is effective.

We now prove the second sentence of our theorem. Since M is finitely generated there exists a finite alphabet Σ' and a surjective continuous morphism $\theta : \Sigma'^* \to M$. Here Σ' has the same cardinality as the generating set Σ of M. Assuming $\Sigma = \{m_1, \ldots, m_k\}$ and $\Sigma' = \{x_1, \ldots, x_k\}$ we construct effectively $\theta(x_j) = m_j$, $1 \le j \le k$. By Theorem 4.35(ii) there exists a power series

$u' \in S^{\mathrm{rat}}\langle\langle(\Sigma')^*\rangle\rangle$ such that $u'\underline{\theta} = u$ and a rational expression for $u'\underline{\theta}$ can effectively be constructed by the given rational expression for u.

By Lemma 4.37 of Sakarovitch [4],

$$r \odot u = (r\underline{\theta^{-1}} \odot u')\underline{\theta}\,.$$

Proposition 4.33 ensures that $r\underline{\theta^{-1}} \in S^{\mathrm{rec}}\langle\langle\Sigma'^*\rangle\rangle = S^{\mathrm{rat}}\langle\langle\Sigma'^*\rangle\rangle$. It is wellknown that a rational expression for $r\underline{\theta^{-1}}$ can effectively be constructed from an S-representation that recognizes $r\underline{\theta^{-1}}$. Hence, a rational expression for $r\underline{\theta^{-1}}$ can effectively be constructed. Since $r\underline{\theta^{-1}} \odot u' \in S^{\mathrm{rec}}\langle\langle\Sigma'^*\rangle\rangle = S^{\mathrm{rat}}\langle\langle\Sigma'^*\rangle\rangle$ by Theorem 4.13 a rational expression for $r\underline{\theta^{-1}} \odot u'$ can effectively be constructed. Finally, by Theorem 4.35(i) the construction of a rational expression for $(r\underline{\theta^{-1}} \odot u')\underline{\theta} = r \odot u$ is effective. □

A monoid M is called *rationally enumerable* if $\mathrm{char}(M) \in \mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle$. Here char denotes the characterisic series.

Theorem 4 (Sakarovitch [4], Corollary 4.39)**.** *Suppose that S is a commutative semiring. If M is rationally enumerable then $S^{\mathrm{rec}}\langle\langle M\rangle\rangle \subseteq S^{\mathrm{rat}}\langle\langle M\rangle\rangle$. If an S-representation recognizing $r \in S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ is given then a rational expression for r can effectively be constructed.*

Proof. We use the proof of Corollary 4.39 of Sakarovitch [4]. Since $r \in S^{\mathrm{rec}}\langle\langle M\rangle\rangle$ and, by hypothesis, $\mathrm{char}(M) \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$, we obtain $r \odot \mathrm{char}(M) = r \in S^{\mathrm{rat}}\langle\langle M\rangle\rangle$ and, by Theorem 3, a rational expression for r can be effectively constructed from a given S-representation recognizing r. □

Corollary 2. *Let M be a graded monoid of finite type that is rationally enumerable and assume that $|\ | : M \to \mathbb{N}$ is recursive. Then φ, as a function $\mathbb{N}^{\mathrm{rec}}\langle\langle M\rangle\rangle \to \mathbb{N}^{\mathrm{rat}}\langle\langle\{x\}^*\rangle\rangle$, is recursive.*

Theorem 5. *Let M be a rationally enumerable graded monoid of finite type such that $|\ | : M \to \mathbb{N}$ is recursive. Then for two unambiguous power series $r \in \mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle$ and $s \in \mathbb{N}^{\mathrm{rec}}\langle\langle M\rangle\rangle$ the problem whether or not $r = s$ is decidable.*

Proof. By Theorem 1 and Corollary 2, $\varphi : \mathbb{N}^{\mathrm{rat}}\langle\langle M\rangle\rangle \to \mathbb{N}^{\mathrm{rat}}\langle\langle\{x\}^*\rangle\rangle$ and $\varphi : \mathbb{N}^{\mathrm{rec}}\langle\langle M\rangle\rangle \to \mathbb{N}^{\mathrm{rat}}\langle\langle\{x\}^*\rangle\rangle$, respectively, are recursive. Now the application of Corollary 8.18 of Kuich, Salomaa [3] and of Theorems 3 and 2 (ii) proves our theorem. □

Harju, Karhumäki [2] proved the famous result that the equivalence problem for deterministic finite multitape automata is decidable. The next corollary states a weak version of this result.

Corollary 3. *Let $\Sigma_1, \ldots, \Sigma_n$ be alphabets. Then for a deterministic finite automaton $\mathfrak{A}$ over $\Sigma = \{(a_1, \varepsilon, \ldots, \varepsilon) \mid a_1 \in \Sigma_1\} \cup \cdots \cup \{(\varepsilon, \varepsilon, \ldots, a_n) \mid a_n \in \Sigma_n\}$ and $\mathbb{N}$, and an unambiguous power series $r \in \mathbb{N}^{\mathrm{rec}}\langle\langle\Sigma_1^* \times \cdots \times \Sigma_n^*\rangle\rangle$ the problem, whether or not $||\mathfrak{A}|| = r$ is decidable.*

An inspection of the proof of Theorem 2 shows that $\mathfrak{R} \subseteq \mathbb{N}^{\mathrm{rat}}\langle\langle M \rangle\rangle$ can be replaced by $\mathfrak{R} \subseteq S^{\mathrm{rat}}\langle\langle M \rangle\rangle$ if the semiring S is ordered and satisfies the following condition: For all $a_1, a_2, b_1, b_2 \in S$,

$$a_1 + a_2 = b_1 + b_2,\ a_1 \geq b_1,\ a_2 \geq b_2 \text{ imply } a_1 = b_1,\ a_2 = b_2.$$

A nontrivial complete ordered semiring does not satisfy this condition; the semirings $\mathbb{Q}_+$ and $\mathbb{R}_+$ do satisfy this condition.

Theorem 6. *Let Σ be an alphabet and $r \in \mathbb{Q}_+^{\mathrm{rat}}\langle\langle \Sigma^* \rangle\rangle$ such that $(r, w) \leq 1$ for all $w \in \Sigma^*$. Then it is decidable whether or not r is unambiguous.*

Proof. Since $(r, w) \leq 1$ for all $w \in \Sigma^*$ we have $r \odot r \leq r$. Since $\mathbb{Q}_+^{\mathrm{rat}}\langle\langle \Sigma^* \rangle\rangle$ is closed under Hadamard product, by Corollary 8.18 of Kuich, Salomaa [3] and by Theorem 2 (i) it is decidable whether or not $r \odot r = r$. The theorem is proved by the observation that $r \odot r = r$ iff $(r, w) \in \{0, 1\}$ for all $w \in \Sigma^*$. □

References

1. Gruska, J.: Foundations of Computing. Thomson Learning (1997)
2. Harju, T., Karhumäki, J.: The equivalence problem of multitape finite automata. Theoretical Computer Science **78**, 347–355 (1991)
3. Kuich, W., Salomaa, A.: Semirings, Automata, Languages. EATCS Monographs on Theoretical Computer Science, Vol. 5. Springer (1986)
4. Sakarovitch, J.: Rational and recognisable power series. In: Droste, M., Kuich, W., Vogler, H. (eds.) Handbook of Weighted Automata, ch. 4. Springer (2009)