Chapter 1: Semirings and Formal Power Series

Manfred Droste[1] and Werner Kuich[2]

[1] Institut für Informatik, Universität Leipzig, 04009 Leipzig, Germany
droste@informatik.uni-leipzig.de
[2] Institut für Diskrete Mathematik und Geometrie, Technische Universität Wien, 1040 Wien, Austria
kuich@tuwien.ac.at
www.dmg.tuwien.ac.at/kuich

1 Introduction

It is the goal of this chapter to present basic foundations for the theory of weighted automata: semirings and formal power series.

Weighted automata are classical automata in which the transitions carry weights. These weights may model, e.g., the cost involved when executing the transition, the amount of resources or time needed for this, or the probability or reliability of its successful execution. In order to obtain a uniform model of weighted automata for different realizations of weights and their computations, the weight structures are often modeled as semirings. A semiring consists of a set with two operations addition and multiplication satisfying certain natural axioms like associativity, commutativity, and distributivity, just like the natural numbers with their laws for sums and products. The behavior of weighted automata can then be defined as a function associating to each word the total weight of its execution; see Chaps. 3 and 4 of this handbook [12, 38].

Any function from the free monoid Σ^* of all words over a given alphabet Σ into a semiring S is called a formal power series. It is important to notice that

M. Droste, W. Kuich, H. Vogler (eds.), *Handbook of Weighted Automata*, Monographs in Theoretical Computer Science. An EATCS Series,
DOI 10.1007/978-3-642-01492-5_1,

each language over Σ can be viewed as a formal power series over the Boolean semiring $\mathbb{B}$ and Σ^* (by identifying the language with its characteristic series). Therefore, formal power series form a generalization of formal languages, and similarly, weighted automata generalize classical automata. For other semirings (like the natural or real numbers), formal power series can be viewed as weighted, multivalued or quantified languages in which each word is assigned a weight, a number, or some quantity.

In this chapter, we will present the basics of the theory of semirings and formal power series as far as they are used in the forthcoming chapters of this handbook. Now, we give a summary of the contents of this chapter.

First, we consider various particular monoids and semirings. Many semirings (like the natural numbers) carry a natural order. Also, when generalizing the star operation (= Kleene iteration) from languages to formal power series, important questions on the existence of infinite sums arise. This leads to the notions of ordered, complete or continuous monoids and semirings. Besides these, we will consider the related concepts of star semirings and Conway semirings, and also locally finite semirings.

Next, we introduce formal power series, especially locally finite families of power series and cycle-free power series. It is a basic result that the collection of all formal power series over a given semiring and an alphabet can be endowed with addition and Cauchy multiplication yielding again the structure of a semiring, as well as with several further useful operations like the Hadamard product or the Hurwitz (shuffle) product. We prove that, under suitable assumptions, certain equalities involving the Kleene-star of elements are valid. Moreover, various important properties of the underlying semiring transfer to the semiring of formal power series. In particular, this includes properties like being ordered, complete, continuous, or Conway. We also consider morphisms between semirings of formal power series.

As is well known, the set of transitions of a classical finite automaton can be uniformly represented by matrices with entries 0 or 1. A similar representation is also easily possible for the transitions of a weighted automaton: here the matrices have entries from the underlying semiring, namely the weights of the transitions. This yields very compact representations of weighted automata and often very concise algebraic proofs about their behaviors. We prove a theorem on (infinite) matrices central for automata theory: In a complete star semiring, the blocks of the star of a matrix can be represented by applying rational operations to the blocks of the matrix. Moreover, the Kronecker (tensor) product of matrices is considered.

Finally, we consider cycle-free equations. They have a unique solution and can be used to show that two expressions represent the same formal power series. Again, we obtain results on how to compute the blocks of the star of a matrix, but now for arbitrary semirings, by imposing restrictions on the matrix.

In the literature, a number of authors have dealt with the interplay between semirings, formal power series and automata theory. The following books and surveys deal with this topic: Berstel [2], Berstel and Reutenauer [3], Bloom and Ésik [4], Carré [5], Conway [6], Eilenberg [8], Ésik and Kuich [9], Kuich [28], Kuich and Salomaa [29], Sakarovitch [37], Salomaa and Soittola [39], Wechler [40].

Further books on semirings and formal power series are Golan [15] and Hebisch and Weinert [20]. Głazek [13] is a bibliography on semirings and formal power series.

Some ideas and formulations of this presentation originate from Kuich and Salomaa [29] and Ésik and Kuich [11].

2 Monoids and Semirings

In this section, we consider monoids and semirings. The definitions and results on monoids and semirings are mainly due to Bloom and Ésik [4], Eilenberg [8], Goldstern [16], Karner [22, 23], Krob [25, 26], Kuich [27, 28], Kuich and Salomaa [29], Manes and Arbib [31], and Sakarovitch [36]. Our notion of continuous monoids and semirings is a specialization of the continuous algebras as defined, e.g., in Guessarian [17], Goguen, Thatcher, Wagner, and Wright [14], Adámek, Nelson, and Reiterman [1].

A *monoid* consists of a non-empty set M, an associative binary operation $\cdot$ on M and a neutral element 1 such that $m \cdot 1 = 1 \cdot m = m$ for every $m \in M$. A monoid M is called *commutative* if $m_1 \cdot m_2 = m_2 \cdot m_1$ for every $m_1, m_2 \in M$. The binary operation is usually denoted by juxtaposition and often called product.

If the operation and the neutral element of M are understood, then we denote the monoid simply by M. Otherwise, we use the triple notation $\langle M, \cdot, 1\rangle$. A commutative monoid M is often denoted by $\langle M, +, 0\rangle$.

The most important type of a monoid in our considerations is the *free monoid* Σ^* generated by a nonempty set Σ. It has all the (*finite*) *words over* Σ

$$x_1 \dots x_n, \qquad \text{with } x_i \in \Sigma,\ 1 \le i \le n,\ n \ge 0,$$

as its elements, and the product $w_1 \cdot w_2$ is formed by writing the string w_2 immediately after the string w_1. The neutral element of Σ^* (the case $n = 0$), also referred to as the *empty word*, is denoted by ε.

The elements of Σ are called *letters* or *symbols*. The set Σ itself is called an *alphabet*. The *length* of a word $w = x_1 \dots x_n$, $n \ge 0$, in symbols $|w|$, is defined to be n.

A *morphism* h of a monoid M into a monoid M' is a mapping $h : M \to M'$ compatible with the neutral elements and operations in $\langle M, \cdot, 1\rangle$ and $\langle M', \circ, 1'\rangle$, i.e., $h(1) = 1'$ and $h(m_1 \cdot m_2) = h(m_1) \circ h(m_2)$ for all $m_1, m_2 \in M$.

If Σ is an alphabet and $\langle M, \cdot, 1\rangle$ is any monoid, then every mapping $h : \Sigma \to M$ can be uniquely extended to a morphism $h^\sharp : \Sigma^* \to M$ by putting $h^\sharp(\varepsilon) = 1$ and $h^\sharp(x_1 x_2 \dots x_n) = h(x_1) \cdot h(x_2) \cdot \dots \cdot h(x_n)$ for any $x_1, \dots, x_n \in \Sigma$, $n \ge 1$. Usually, $h^\sharp$ is again denoted by h.

Next, we consider monoids with particular properties, like carrying an order or having an infinite sum operation. For our purposes, it suffices to consider commutative monoids. A commutative monoid $\langle M, +, 0\rangle$ is called *idempotent*, if $m + m = m$ for all $m \in M$, and it is called *ordered* if it is equipped with a partial order $\leq$ preserved by the $+$ operation. An ordered monoid M is *positively ordered*, if $m \geq 0$ for each $m \in M$. A commutative monoid $\langle M, +, 0\rangle$ is called *naturally ordered* if the relation $\sqsubseteq$ defined by: $m_1 \sqsubseteq m_2$ if there exists an m such that $m_1 + m = m_2$, is a partial order. Clearly, this is the case, i.e., $\sqsubseteq$ is antisymmetric, iff whenever $m, m', m'' \in M$ with $m + m' + m'' = m$, then $m + m' = m$. Then in particular M is positively ordered. We note that if $\langle M, +, 0\rangle$ is idempotent, then M is naturally ordered and for any $m_1, m_2 \in M$ we have $m_1 + m_2 = \mathsf{sup}\{m_1, m_2\}$ in $\langle M, \sqsubseteq\rangle$. Further, $m_1 \sqsubseteq m_2$ iff $m_1 + m_2 = m_2$. Morphisms of ordered monoids are monoid morphisms which preserve the order.

If I is an index set, an infinitary sum operation $\sum_I : M^I \to M$ associates with every family $(m_i \mid i \in I)$ of elements of M an element $\sum_{i \in I} m_i$ of M. A monoid $\langle M, +, 0\rangle$ is called *complete* if it has infinitary sum operations $\sum_I$ (for any index set I) such that the following conditions are satisfied:

(i) $\sum_{i \in \emptyset} m_i = 0$, $\sum_{i \in \{j\}} m_i = m_j$, $\sum_{i \in \{j,k\}} m_i = m_j + m_k$, for $j \neq k$.
(ii) $\sum_{j \in J}(\sum_{i \in I_j} m_i) = \sum_{i \in I} m_i$, if $\bigcup_{j \in J} I_j = I$ and $I_j \cap I_{j'} = \emptyset$ for $j \neq j'$.

A morphism of complete monoids is a monoid morphism preserving all sums. Note that any complete monoid is commutative.

Recall that a non-empty subset D of a partially ordered set P is called *directed* if each pair of elements of D has an upper bound in D.

A positively ordered commutative monoid $\langle M, +, 0\rangle$ is called a *continuous monoid* if each directed subset of M has a least upper bound and the $+$ operation preserves the least upper bound of directed sets, i.e., when

$$m + \mathsf{sup}\, D = \mathsf{sup}(m + D),$$

for all directed sets $D \subseteq M$ and for all $m \in M$. Here, $m + D$ is the set $\{m + d \mid d \in D\}$.

It is known that a positively ordered commutative monoid M is continuous iff each chain in M has a least upper bound and the $+$ operation preserves least upper bounds of chains, i.e., when $m + \mathsf{sup}\, C = \mathsf{sup}(m + C)$ holds for all non-empty chains C in M. (See Markowsky [32].)

Proposition 2.1. *Any continuous monoid $\langle M, +, 0\rangle$ is a complete monoid equipped with the following sum operation:*

$$\sum_{i \in I} m_i = \mathsf{sup}\Big\{\sum_{i \in F} m_i \mid F \subseteq I,\ F \text{ finite}\Big\},$$

for all index sets I and all families $(m_i \mid i \in I)$ in M.

A function $f : P \to Q$ between partially ordered sets is *continuous* if it preserves the least upper bound of any directed set, i.e., when $f(\mathsf{sup}\, D) = \mathsf{sup}\, f(D)$, for all directed sets $D \subseteq P$ such that $\mathsf{sup}\, D$ exists. It follows that any continuous function preserves the order. A morphism of continuous monoids is defined to be a monoid morphism which is a continuous function. Clearly, any morphism between continuous monoids is a complete monoid morphism.

A *semiring* is a set S together with two binary operations $+$ and $\cdot$ and two constant elements 0 and 1 such that:

(i) $\langle S, +, 0\rangle$ is a commutative monoid,
(ii) $\langle S, \cdot, 1\rangle$ is a monoid,
(iii) the distributivity laws $(a+b)\cdot c = a\cdot c + b\cdot c$ and $c\cdot(a+b) = c\cdot a + c\cdot b$ hold for every a, b, $c \in S$,
(iv) $0 \cdot a = a \cdot 0 = 0$ for every $a \in S$.

A semiring S is called *commutative* if $a \cdot b = b \cdot a$ for every $a, b \in S$. Further, S is called *idempotent* if $\langle S, +, 0\rangle$ is an idempotent monoid. By the distributivity law, this holds iff $1 + 1 = 1$.

If the operations and the constant elements of S are understood, then we denote the semiring simply by S. Otherwise, we use the notation $\langle S, +, \cdot, 0, 1\rangle$. In the sequel, S will denote a semiring.

Intuitively, a semiring is a ring (with unity) without subtraction. A typical example is the semiring of nonnegative integers $\mathbb{N}$. A very important semiring in connection with language theory is the *Boolean* semiring $\mathbb{B} = \{0, 1\}$ where $1 + 1 = 1 \cdot 1 = 1$. Clearly, all rings (with unity), as well as all fields, are semirings, e.g., the integers $\mathbb{Z}$, rationals $\mathbb{Q}$, reals $\mathbb{R}$, complex numbers $\mathbb{C}$, etc.

Let $\mathbb{N}^\infty = \mathbb{N} \cup \{\infty\}$ and $\overline{\mathbb{N}} = \mathbb{N} \cup \{-\infty, \infty\}$. Then $\langle \mathbb{N}^\infty, +, \cdot, 0, 1\rangle$, $\langle \mathbb{N}^\infty, \mathsf{min}, +, \infty, 0\rangle$ and $\langle \overline{\mathbb{N}}, \mathsf{max}, +, -\infty, 0\rangle$, where $+$, $\cdot$, min and max are defined in the obvious fashion (observe that $0\cdot\infty = \infty\cdot 0 = 0$ and $(-\infty)+\infty = -\infty$), are semirings.

Let $\mathbb{R}_+ = \{a \in \mathbb{R} \mid a \geq 0\}$, $\mathbb{R}_+^\infty = \mathbb{R}_+ \cup \{\infty\}$ and $\overline{\mathbb{R}}_+ = \mathbb{R}_+ \cup \{-\infty, \infty\}$. Then $\langle \mathbb{R}_+, +, \cdot, 0, 1\rangle$, $\langle \mathbb{R}_+^\infty, +, \cdot, 0, 1\rangle$ and $\langle \mathbb{R}_+^\infty, \mathsf{min}, +, \infty, 0\rangle$ are semirings. The semirings $\langle \mathbb{N}_+^\infty, \mathsf{min}, +, \infty, 0\rangle$ and $\langle \mathbb{R}_+^\infty, \mathsf{min}, +, \infty, 0\rangle$ are called *tropical semirings* or *min-plus semirings*. Similarly, the semirings $\langle \overline{\mathbb{N}}, \mathsf{max}, +, -\infty, 0\rangle$ and $\langle \overline{\mathbb{R}}_+, \mathsf{max}, +, -\infty, 0\rangle$ are called *max-plus semirings* or *arctic semirings*. A further example is provided by the semiring $\langle [0,1], \mathsf{max}, \cdot, 0, 1\rangle$, called the *Viterbi semiring* in probabilistic parsing.

We note that the tropical and the arctic semirings are very often employed in optimization problems of networks, cf., e.g., Heidergott, Olsder, and van der Woude [21].

Let Σ be a finite alphabet. Then each subset of Σ^* is called a *formal language over* Σ. We define, for formal languages $L_1, L_2 \subseteq \Sigma^*$, the *product* of L_1 and L_2 by

$$L_1 \cdot L_2 = \{w_1 w_2 \mid w_1 \in L_1,\, w_2 \in L_2\}.$$

Then $\langle 2^{\Sigma^*}, \cup, \cdot, \emptyset, \{\varepsilon\}\rangle$ is a semiring, called the *semiring of formal languages over Σ*. Here, 2^U denotes the power set of a set U and $\emptyset$ denotes the empty set.

If U is a set, $2^{U\times U}$ is the set of binary relations over U. Define, for two relations R_1 and R_2, the product $R_1 \cdot R_2 \subseteq U \times U$ by

$$R_1 \cdot R_2 = \{(u_1, u_2) \mid \text{there exists } u \in U \text{ such that } (u_1, u) \in R_1 \text{ and } (u, u_2) \in R_2\}$$

and furthermore, define

$$\Delta = \{(u, u) \mid u \in U\}.$$

Then $\langle 2^{U\times U}, \cup, \cdot, \emptyset, \Delta\rangle$ is a semiring, called the *semiring of binary relations over U*.

Further semirings are the chain of nonnegative reals $\langle \mathbb{R}_+^\infty, \mathsf{max}, \mathsf{min}, 0, \infty\rangle$ and any Boolean algebra, in particular the power set Boolean algebras $\langle 2^U, \cup, \cap, \emptyset, U\rangle$ where U is any set. These examples can be generalized as follows. Recall that a partially ordered set $\langle L, \leq\rangle$ is a *lattice* if for any two elements $a, b \in L$, the least upper bound $a \vee b = \mathsf{sup}\{a, b\}$ and the greatest lower bound $a \wedge b = \mathsf{inf}\{a, b\}$ exist in $\langle L, \leq\rangle$. A lattice $\langle L, \leq\rangle$ is *distributive*, if $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ for all $a, b, c \in L$; and *bounded*, if L contains a smallest element, denoted 0, and a greatest element, denoted 1. Now, let $\langle L, \leq\rangle$ be any bounded distributive lattice. Then $\langle L, \vee, \wedge, 0, 1\rangle$ is a semiring. Since any distributive lattice L also satisfies the dual law $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ for all $a, b, c \in L$, the structure $\langle L, \wedge, \vee, 1, 0\rangle$ is also a semiring. Such semirings are often used for fuzzy automata; see Chap. 12 [35] of this book. Another semiring is the *Łukasiewicz semiring* $\langle [0, 1], \mathsf{max}, \otimes, 0, 1\rangle$ where $a \otimes b = \mathsf{max}\{0, a + b - 1\}$ which occurs in multivalued logic (see Hájek [18]).

Recall that in formal language theory, the Kleene-iteration L^* of a language $L \subseteq \Sigma^*$ is defined by $L^* = \bigcup_{n\geq 0} L^n$. Later on, we wish to extend this star operation to formal power series (i.e., functions) $r : \Sigma^* \to S$ where S is a semiring. For this, it will be useful to know which semirings carry such a star operation like the semiring of formal languages. We will call a *star semiring* any semiring equipped with an additional unary operation *. The following semirings are star semirings:

(i) The Boolean semiring $\langle \mathbb{B}, +, \cdot, ^*, 0, 1\rangle$ with $0^* = 1^* = 1$.
(ii) The semiring $\langle \mathbb{N}^\infty, +, \cdot, ^*, 0, 1\rangle$ with $0^* = 1$ and $a^* = \infty$ for $a \neq 0$.
(iii) The semiring $\langle \mathbb{R}_+^\infty, +, \cdot, ^*, 0, 1\rangle$ with $a^* = 1/(1 - a)$ for $0 \leq a < 1$ and $a^* = \infty$ for $a \geq 1$.
(iv) The tropical semirings $\langle \mathbb{R}_+^\infty, \mathsf{min}, +, ^*, \infty, 0\rangle$ and $\langle \mathbb{N}^\infty, \mathsf{min}, +, ^*, \infty, 0\rangle$ with $a^* = 0$ for all $a \in \mathbb{R}_+^\infty$ resp. all $a \in \mathbb{N}^\infty$.
(v) The arctic semirings $\langle \overline{\mathbb{R}}_+, \mathsf{max}, +, ^*, -\infty, 0\rangle$ and $\langle \overline{\mathbb{N}}, \mathsf{max}, +, ^*, -\infty, 0\rangle$ with $(-\infty)^* = 0^* = 0$ and $a^* = \infty$ for $a > 0$.
(vi) The semiring $\langle 2^{\Sigma^*}, \cup, \cdot, ^*, \emptyset, \{\varepsilon\}\rangle$ of formal languages over a finite alphabet Σ, as noted before, with $L^* = \bigcup_{n\geq 0} L^n$ for all $L \subseteq \Sigma^*$.

(vii) The semiring $\langle 2^{U\times U}, \cup, \cdot, {}^*, \emptyset, \Delta\rangle$ of binary relations over U with $R^* = \bigcup_{n\geq 0} R^n$ for all $R \subseteq U \times U$. The relation R^* is called the *reflexive and transitive closure* of R, i.e., the smallest reflexive and transitive binary relation over S containing R.

(viii) The Łukasiewicz semiring $\langle [0,1], \mathsf{max}, \otimes, {}^*, 0, 1\rangle$ with $a^* = 1$ for all $a \in [0,1]$.

(ix) The idempotent naturally ordered commutative semiring $\langle \{0,1,a,\infty\}, +, \cdot, {}^*, 0, 1\rangle$, with $0 \sqsubseteq 1 \sqsubseteq a \sqsubseteq \infty$, $a \cdot a = a$, $0^* = 1^* = 1$, $a^* = \infty^* = \infty$.

(x) The bounded distributive lattice semiring $\langle L, \vee, \wedge, {}^*, 0, 1\rangle$ with $a^* = 1$ for all $a \in L$.

The semirings (i)–(v) and (viii)–(x) are commutative. The semirings (i), (iv)–(x) are idempotent.

A semiring $\langle S, +, \cdot, 0, 1\rangle$ is called *ordered* if $\langle S, +, 0\rangle$ is an ordered monoid and multiplication with elements $s \geq 0$ preserves the order; it is *positively ordered*, if furthermore, $\langle S, +, 0\rangle$ is positively ordered. When the order on S is the natural order, $\langle S, +, \cdot, 0, 1\rangle$ is automatically a positively ordered semiring.

A semiring $\langle S, +, \cdot, 0, 1\rangle$ is called *complete* if $\langle S, +, 0\rangle$ is a complete monoid and the following distributivity laws are satisfied (see Bloom and Ésik [4], Conway [6], Eilenberg [8], Kuich [28]):

$$\sum_{i\in I}(a \cdot a_i) = a \cdot \Bigl(\sum_{i\in I} a_i\Bigr), \qquad \sum_{i\in I}(a_i \cdot a) = \Bigl(\sum_{i\in I} a_i\Bigr) \cdot a.$$

This means that a semiring S is complete if it is possible to define "infinite sums" (i) that are an extension of the finite sums, (ii) that are associative and commutative and (iii) that satisfy the distributivity laws.

In complete semirings for each element a, we can define the *star* a^* of a by

$$a^* = \sum_{j\geq 0} a^j,$$

where $a^0 = 1$ and $a^{j+1} = a \cdot a^j = a^j \cdot a$ for $j \geq 0$. Hence, with this star operation, each complete semiring is a star semiring called a *complete star semiring*. The semirings (i)–(viii) are complete star semirings. The semiring (ix) is complete, but it violates the above equation for the element a, hence it is not a complete star semiring. The distributive lattice semiring L satisfies $a^* = \bigvee_{j\geq 0} a^j$ for each $a \in L$, but is not necessarily complete. It is a complete semiring iff $(L, \vee, \wedge)$ is a join-continuous complete lattice, i.e., any subset of L has a supremum in L and $a \wedge \bigvee_{i\in I} a_i = \bigvee_{i\in I}(a \wedge a_i)$ for any subset $\{a_i \mid i \in I\}$ of L.

A semiring $\langle S, +, \cdot, 0, 1\rangle$ is called *continuous* if $\langle S, +, 0\rangle$ is a continuous monoid and if multiplication is continuous, i.e.,

$$a \cdot (\mathsf{sup}_{i\in I}\, a_i) = \mathsf{sup}_{i\in I}(a \cdot a_i) \quad \text{and} \quad (\mathsf{sup}_{i\in I}\, a_i) \cdot a = \mathsf{sup}_{i\in I}(a_i \cdot a)$$

for all directed sets $\{a_i \mid i \in I\}$ and $a \in S$ (see Bloom and Ésik [4]). It follows that the distributivity laws hold for infinite sums:

$$a \cdot \left(\sum_{i \in I} a_i\right) = \sum_{i \in I}(a \cdot a_i) \quad \text{and} \quad \left(\sum_{i \in I} a_i\right) \cdot a = \sum_{i \in I}(a_i \cdot a)$$

for all families $(a_i \mid i \in I)$.

Proposition 2.2. *Any continuous semiring is complete.*

All the semirings in (i)–(ix) are continuous.

We now consider two equations that are important in automata theory. Let S be a star semiring. Then for $a, b \in S$:

(i) The *sum star identity* is valid for a and b if $(a+b)^* = (a^*b)^*a^*$.
(ii) The *product star identity* is valid for a and b if $(ab)^* = 1 + a(ba)^*b$.

If the sum star identity (resp. the product star identity) is valid for all $a, b \in S$, then we say that the *sum star identity* (resp. the *product star identity*) is *valid* (in the star semiring S).

A *Conway semiring* is now a star semiring in which the sum star identity and the product star identity are valid (see Conway [6], Bloom and Ésik [4]). All the star semirings in (i)–(x) are Conway semirings. The semiring $\langle \mathbb{Q}_+^\infty, +, \cdot, ^*, 0, 1\rangle$, with $\mathbb{Q}_+^\infty = \mathbb{R}_+^\infty \cap (\mathbb{Q} \cup \{\infty\})$ and operations defined as in (iii), is a Conway semiring (since the sum star identity and product star identity hold in $\mathbb{R}_+^\infty$) but is not complete. Now we have the following proposition.

Proposition 2.3. *Let S be a star semiring. Then S is a Conway semiring iff, for all $a, b \in S$:*

(i) $(a+b)^* = (a^*b)^*a^*$.
(ii) $(ab)^*a = a(ba)^*$.
(iii) $a^* = 1 + aa^* = 1 + a^*a$.

Proof. If S is a Conway semiring, we obtain (iii) from the product star identity with $b = 1$, resp. $a = 1$. Then (ii) follows from the product star identity, distributivity, and (iii). Conversely, for the product star identity compute $(ab)^*$ by using (iii) and then (ii). □

Next we introduce conditions which often simplify the definition or the calculation of the star of elements. A semiring S is *k-closed*, where $k \geq 0$, if for each $a \in S$,

$$1 + a + \cdots + a^k = 1 + a + \cdots + a^k + a^{k+1}.$$

It is called *locally closed*, if for each $a \in S$, there is an integer $k \geq 0$ such that the above equality is valid. (See Carré [5], Mohri [33], Ésik and Kuich [10], Zhao [41], Zimmermann [42].) If $\langle S, +, \cdot, 0, 1\rangle$ is a k-closed semiring, then define the star of $a \in S$ by

$$a^* = 1 + a + \cdots + a^k.$$

An analogous equality defines the star in a locally closed semiring. With this star operation, each k-closed (resp. locally closed) semiring is a star semiring called a *k-closed* (resp. *locally closed*) *star semiring*. The semirings (i), (iv), (viii), and (x) are 0-closed star semirings; the semiring (ix) is a 1-closed semiring, but not a 1-closed star semiring. In [10, 41], the following was shown.

Theorem 2.4. *Any locally closed star semiring is a Conway semiring.*

Next we consider morphisms between semirings. Let S and S' be semirings. Then a mapping $h : S \to S'$ is a *morphism* from S into S' if $h(0) = 0$, $h(1) = 1$, $h(a + b) = h(a) + h(b)$ and $h(a \cdot b) = h(a) \cdot h(b)$ for all $a, b \in S$. That is, a morphism of semirings is a mapping that preserves the semiring operations and constants. A bijective morphism is called an *isomorphism*. For instance, the semirings $\langle \mathbb{R}_+^\infty, \mathsf{min}, +, \infty, 0\rangle$ and $\langle [0, 1], \mathsf{max}, \cdot, 0, 1\rangle$ are isomorphic via the mapping $x \mapsto e^{-x}$, and the semiring $\langle \mathbb{R}_+^\infty, \mathsf{max}, \mathsf{min}, 0, \infty\rangle$ is isomorphic to $\langle [0, 1], \mathsf{max}, \mathsf{min}, 0, 1\rangle$ via the mapping $x \mapsto 1 - e^{-x}$. A morphism h of star semirings is a semiring morphism that preserves additionally the star operation, i.e., $h(a^*) = h(a)^*$ for all $a \in S$. Similarly, a morphism of ordered (resp. complete, continuous) semirings is a semiring morphism that preserves the order (resp. all sums, all suprema of directed subsets). Note that every continuous semiring is an ordered semiring and every continuous semiring morphism is an ordered semiring morphism.

Complete and continuous semirings are typically infinite. For results on weighted automata, sometimes it is assumed that the underlying semiring is finite or "close" to being finite. A large class of such semirings can be obtained by the notion of local finiteness (which stems from group theory where it is well known).

A semiring S is *locally finite* (see Wechler [40], Droste and Gastin [7]) if each finitely generated subsemiring is finite. We note that a semiring $\langle S, +, \cdot, 0, 1\rangle$ is locally finite iff both monoids $\langle S, +, 0\rangle$ and $\langle S, \cdot, 1\rangle$ are locally finite. Indeed, if $\langle S, +, 0\rangle$ and $\langle S, \cdot, 1\rangle$ are locally finite and U is a finite subset of S, then the submonoid V of $\langle S, \cdot, 1\rangle$ generated by U is finite and the submonoid W of $\langle S, +, 0\rangle$ generated by V is also finite. Now, it is easy to check that $W \cdot W \subseteq W$ and we deduce that the subsemiring of $\langle S, +, \cdot, 0, 1\rangle$ generated by U is the finite set W.

For instance, if both sum and product are commutative and idempotent, then the semiring is locally finite. Consequently, any bounded distributive lattice $\langle L, \vee, \wedge, 0, 1\rangle$ is a locally finite semiring. In particular, the chain $\langle [0, 1], \mathsf{max}, \mathsf{min}, 0, 1\rangle$ and any Boolean algebra are locally finite. Further, the Łukasiewicz semiring $\langle [0, 1], \mathsf{max}, \otimes, 0, 1\rangle$ is locally finite, since its additive and multiplicative monoid are commutative and locally finite. Moreover, each positively ordered locally finite semiring is locally closed, and each positively ordered finite semiring is k-closed where k is less than the number of elements of the semiring.

Examples of infinite but locally finite fields are provided by the algebraic closures of the finite fields $\mathbb{Z}/p\mathbb{Z}$ for any prime p.

3 Formal Power Series

In this section, we define and investigate formal power series (for expositions, see Salomaa and Soittola [39], Kuich and Salomaa [29], Berstel and Reutenauer [3], Sakarovitch [37]). Let Σ be an alphabet and S a semiring. Mappings r from Σ^* into S are called *(formal) power series*. The values of r are denoted by (r, w), where $w \in \Sigma^*$, and r itself is written as a formal sum

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

The values (r, w) are also referred to as the *coefficients* of the series. The collection of all power series r as defined above is denoted by $S\langle\langle\Sigma^*\rangle\rangle$.

This terminology reflects the intuitive ideas connected with power series. We call the power series "formal" to indicate that we are not interested in summing up the series but rather, for instance, in various operations defined for series.

Given $r \in S\langle\langle\Sigma^*\rangle\rangle$, the *support* of r is the set

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

A series $r \in S\langle\langle\Sigma^*\rangle\rangle$ where every coefficient equals 0 or 1 is termed the *characteristic series* of its support L, in symbols, $r = \mathrm{char}(L)$ or $r = \mathbb{1}_L$. The subset of $S\langle\langle\Sigma^*\rangle\rangle$ consisting of all series with a finite support is denoted by $S\langle\Sigma^*\rangle$. Series of $S\langle\Sigma^*\rangle$ are referred to as *polynomials*. It will be convenient to use the notations $S\langle\Sigma \cup \{\varepsilon\}\rangle$, $S\langle\Sigma\rangle$ and $S\langle\{\varepsilon\}\rangle$ for the collection of polynomials having their supports in $\Sigma \cup \{\varepsilon\}$, Σ and $\{\varepsilon\}$, respectively.

Examples of polynomials belonging to $S\langle\Sigma^*\rangle$ are 0 and aw, where $a \in S$ and $w \in \Sigma^*$, defined by:

$$(0, w) = 0 \quad \text{for all } w,$$
$$(aw, w) = a \quad \text{and} \quad (aw, w') = 0 \quad \text{for } w \neq w'.$$

Often, $1w$ is denoted by w or $\mathbb{1}_{\{w\}}$.

Next, we introduce several operations on power series. For $r_1, r_2, r \in S\langle\langle\Sigma^*\rangle\rangle$ and $a \in S$, we define the *sum* $r_1 + r_2$, the *(Cauchy) product* $r_1 \cdot r_2$, the *Hadamard product* $r_1 \odot r_2$, and *scalar products* ar, ra, each as a series belonging to $S\langle\langle\Sigma^*\rangle\rangle$, as follows:

- $(r_1 + r_2, w) = (r_1, w) + (r_2, w)$
- $(r_1 \cdot r_2, w) = \sum_{w_1 w_2 = w} (r_1, w_1)(r_2, w_2)$
- $(r_1 \odot r_2, w) = (r_1, w)(r_2, w)$
- $(ar, w) = a(r, w)$
- $(ra, w) = (r, w)a$

for all $w \in \Sigma^*$.

It can be checked that $\langle S\langle\langle\Sigma^*\rangle\rangle, +, \cdot, 0, \varepsilon\rangle$ and $\langle S\langle\Sigma^*\rangle, +, \cdot, 0, \varepsilon\rangle$ are semirings, the semirings of formal power series resp. of polynomials over Σ and S.

We just note that the structure $\langle S\langle\langle \Sigma^*\rangle\rangle, +, \odot, 0, \mathrm{char}(\Sigma^*)\rangle$ is also a semiring (the full Cartesian product of Σ^* copies of the semiring $\langle S, +, \cdot, 0, 1\rangle$).

Clearly, the formal language semiring $\langle 2^{\Sigma^*}, \cup, \cdot, \emptyset, \{\varepsilon\}\rangle$ is isomorphic to $\langle \mathbb{B}\langle\langle \Sigma^*\rangle\rangle, +, \cdot, 0, \varepsilon\rangle$. Essentially, a transition from 2^{Σ^*} to $\mathbb{B}\langle\langle \Sigma^*\rangle\rangle$ and vice versa means a transition from L to $\mathrm{char}(L)$ and from r to $\mathrm{supp}(r)$, respectively. Furthermore, the operation corresponding to the Hadamard product is the intersection of languages. If r_1 and r_2 are the characteristic series of the languages L_1 and L_2, then $r_1 \odot r_2$ is the characteristic series of $L_1 \cap L_2$.

This basic transition between 2^{Σ^*} and $\mathbb{B}\langle\langle \Sigma^*\rangle\rangle$ will be very important in all of the following as it often gives a hint how to generalize classical results from formal language theory into the realm of formal power series (with an arbitrary or suitable semiring S replacing $\mathbb{B}$).

Let $r_i \in S\langle\langle \Sigma^*\rangle\rangle$ $(i \in I)$, where I is an arbitrary index set. Then for $w \in \Sigma^*$ let $I_w = \{i \mid (r_i, w) \neq 0\}$. Assume now that for all $w \in \Sigma^*$, I_w is finite. Then we call the family of power series $\{r_i \mid i \in I\}$ *locally finite*. In this case, we can define the sum $\sum_{i\in I} r_i$ by

$$\left(\sum_{i\in I} r_i, w\right) = \sum_{i\in I_w} (r_i, w)$$

for all $w \in \Sigma^*$. Also, in this case for each $r \in S\langle\langle \Sigma^*\rangle\rangle$, the families $\{r \cdot r_i \mid i \in I\}$ and $\{r_i \cdot r \mid i \in I\}$ are also locally finite, and $r \cdot \sum_{i\in I} r_i = \sum_{i\in I} r \cdot r_i$ and $(\sum_{i\in I} r_i) \cdot r = \sum_{i\in I} r_i \cdot r$. Indeed, let $w \in \Sigma^*$ and put $J = \bigcup_{w=uv} I_v$, a finite set. Then

$$\begin{aligned}\left(r \cdot \sum_{i\in I} r_i, w\right) &= \sum_{w=uv} (r, u)\left(\sum_{i\in J} r_i, v\right) = \sum_{w=uv} \sum_{i\in J} (r, u) \cdot (r_i, v) \\ &= \sum_{i\in J} \sum_{w=uv} (r, u) \cdot (r_i, v) = \sum_{i\in J} (r \cdot r_i, w) = \left(\sum_{i\in I} r \cdot r_i, w\right),\end{aligned}$$

as $(r \cdot r_i, w) \neq 0$ implies $i \in J$. This proves the first equation, and the second one follows similarly.

A power series $r \in S\langle\langle \Sigma^*\rangle\rangle$ is called *proper* or *quasiregular* if $(r, \varepsilon) = 0$. The *star* r^* of a proper power series $r \in S\langle\langle \Sigma^*\rangle\rangle$ is defined by

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

Since r is proper, we infer $(r^n, w) = 0$ for each $n > |w|$. Hence, $\{r^n \mid n \geq 0\}$ is locally finite, $(r^*, w) = \sum_{0\leq n\leq |w|} (r^n, w)$, and the star of a proper power series is well-defined.

We generalize this result to cycle-free power series. A power series $r \in S\langle\langle \Sigma^*\rangle\rangle$ is called *cycle-free of index* $k > 0$ if $(r, \varepsilon)^k = 0$. It is called *cycle-free* if there exists a $k \geq 1$ such that r is cycle-free of index k. Again, we define the *star* of a cycle-free power series $r \in S\langle\langle \Sigma^* \rangle\rangle$ by

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

Since r is cycle-free of some index $k \geq 1$, an easy proof by induction on the length of $w \in \Sigma^*$ yields $(r^n, w) = 0$ for $n \geq k \cdot (|w| + 1)$. Hence, $\{r^n \mid n \geq 0\}$ is locally finite, $(r^*, w) = \sum_{0 \leq n < k(|w|+1)} (r^n, w)$, and the star of a cycle-free power series is well-defined.

Next, we wish to consider identities that are valid for a cycle-free power series r, like, e.g., $rr^* + \varepsilon = r^* r + \varepsilon = r^*$. Using the distributivity laws given above for locally finite families, this follows from:

$$rr^* + \varepsilon = r \cdot \sum_{n \geq 0} r^n + \varepsilon = \sum_{n \geq 0} r^{n+1} + \varepsilon = r^* .$$

Theorem 3.1. *Let r be a cycle-free power series. Then, for each $n \geq 0$,*

$$r^* = r^{n+1} r^* + \sum_{0 \leq j \leq n} r^j = r^* r^{n+1} + \sum_{0 \leq j \leq n} r^j .$$

Proof. We obtain by substitutions

$$r^* = rr^* + \varepsilon = r(rr^* + \varepsilon) + \varepsilon = r^2 r^* + r + \varepsilon = \cdots .$$

The proof of the second equality is analogous. □

Theorem 3.2. *Let $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and assume that rs is cycle-free. Then sr is cycle-free and*

$$(rs)^* r = r(sr)^* .$$

Proof. Since rs is cycle-free, $((rs)^k, \varepsilon) = 0$ for some $k > 0$. Hence,

$$\big((sr)^{k+1}, \varepsilon\big) = (s, \varepsilon)\big((rs)^k, \varepsilon\big)(r, \varepsilon) = 0$$

and sr is cycle-free. It follows that $(rs)^* r = \sum_{n \geq 0} ((rs)^n \cdot r) = \sum_{n \geq 0} r \cdot (sr)^n = r \cdot (sr)^*$. □

The *Hurwitz product* (also called *shuffle product*) is defined as follows. For $w_1, w_2 \in \Sigma^*$ and $x_1, x_2 \in \Sigma$, we define $w_1 \sqcup\!\sqcup\, w_2 \in S\langle\langle \Sigma^* \rangle\rangle$ by

$$w_1 \sqcup\!\sqcup\, \varepsilon = w_1, \qquad \varepsilon \sqcup\!\sqcup\, w_2 = w_2,$$

and

$$w_1 x_1 \sqcup\!\sqcup\, w_2 x_2 = (w_1 x_1 \sqcup\!\sqcup\, w_2) x_2 + (w_1 \sqcup\!\sqcup\, w_2 x_2) x_1 .$$

For $r_1, r_2 \in S\langle\langle \Sigma^* \rangle\rangle$, the Hurwitz product $r_1 \sqcup\!\sqcup\, r_2 \in S\langle\langle \Sigma^* \rangle\rangle$ of r_1 and r_2 is then defined by

$$r_1 \sqcup\!\sqcup\, r_2 = \sum_{w_1, w_2 \in \Sigma^*} (r_1, w_1)(r_2, w_2)(w_1 \sqcup\!\sqcup\, w_2).$$

Observe that

$$(r_1 \sqcup\!\sqcup\, r_2, w) = \sum_{|w_1|+|w_2|=|w|} (r_1, w_1)(r_2, w_2)(w_1 \sqcup\!\sqcup\, w_2, w)$$

is a finite sum for all $w \in \Sigma^*$. Hence, $\{\sum_{w_1 w_2 = w}(r_1, w_1)(r_2, w_2) w_1 \sqcup\!\sqcup\, w_2 \mid w \in \Sigma^*\}$ is locally finite and the Hurwitz product of two power series is well-defined.

In language theory, the shuffle product is customarily defined for languages L and L' by

$$L \sqcup\!\sqcup\, L' = \{w_1 w_1' \ldots w_n w_n' \mid w_1 \ldots w_n \in L,\ w_1' \ldots w_n' \in L',\ n \geq 1\}.$$

If $r_1, r_2 \in \mathbb{B}\langle\langle \Sigma^* \rangle\rangle$, then this definition is "isomorphic" to that given above for formal power series.

When the semiring S is ordered by $\leq$, we may order $S\langle\langle \Sigma^* \rangle\rangle$, and thus $S\langle \Sigma^* \rangle$ by the pointwise order: We define $r \leq r'$ for $r, r' \in S\langle\langle \Sigma^* \rangle\rangle$ iff $(r, w) \leq (r', w)$ for all $w \in \Sigma^*$. Equipped with this order, clearly both $S\langle\langle \Sigma^* \rangle\rangle$ and $S\langle \Sigma^* \rangle$ are ordered semirings.

If $\langle S, +, \cdot, 0, 1\rangle$ is a complete semiring, we can define an infinitary sum operation on $S\langle\langle \Sigma^* \rangle\rangle$ as follows: If $r_i \in S\langle\langle \Sigma^* \rangle\rangle$ for $i \in I$, then $\sum_{i \in I} r_i = \sum_{w \in \Sigma^*} (\sum_{i \in I} (r_i, w)) w$. By arguing elementwise for each word $w \in \Sigma^*$, we obtain the following proposition.

Proposition 3.3. *Let S be a semiring.*

(a) If S is complete, $S\langle\langle \Sigma^* \rangle\rangle$ is also complete.
(b) If S is continuous, $S\langle\langle \Sigma^* \rangle\rangle$ is also continuous.

We just note here that an analogous result holds if S is a Conway semiring, with an appropriate definition of the star operation in $S\langle\langle \Sigma^* \rangle\rangle$; see Chap. 3, Theorem 2.8 [12] of this book.

Proposition 3.3 and the Hurwitz product are now used to prove that each complete star semiring is a Conway semiring (see Kuich [27], Hebisch [19]).

Theorem 3.4. *Each complete star semiring is a Conway semiring.*

Proof. Let S be a complete star semiring and let $a, b \in S$. Let $\bar{a}, \bar{b}$ be letters. Note that to each word $\bar{w} = \bar{c_1}\bar{c_2} \ldots \bar{c_n}$, with $\bar{c_i} \in \{\bar{a}, \bar{b}\}$ for $1 \leq i \leq n$, there corresponds the element $w = c_1 c_2 \ldots c_n \in S$. Let S' be the complete star semiring generated by 1. Then S' is commutative. By Proposition 3.3, $\langle S'\langle\langle \{\bar{a}, \bar{b}\}\rangle\rangle, +, \cdot, 0, \varepsilon\rangle$ is a complete semiring. Also, observe that $\bar{a} \mapsto a$, $\bar{b} \mapsto b$ induces a complete star semiring morphism from the complete star semiring $S'\langle\langle \{\bar{a}, \bar{b}\}^* \rangle\rangle$ to S.

Using induction, the following equalities can be shown for all $n, m \geq 0$:

$$\begin{aligned}\left(\bar{a}+\bar{b}\right)^n &= \sum_{0\leq j\leq n} \bar{a}^j \sqcup\!\sqcup\, \bar{b}^{n-j},\\ \bar{a}^n \sqcup\!\sqcup\, \bar{b}^m &= \sum_{0\leq j\leq n} \left(\bar{a}^j \sqcup\!\sqcup\, \bar{b}^{m-1}\right)\bar{b}\bar{a}^{n-j}\end{aligned}$$

and

$$\bar{a}^* \sqcup\!\sqcup\, \bar{b}^n = \sum_{j\geq 0} \bar{a}^j \sqcup\!\sqcup\, \bar{b}^n = \left(\bar{a}^*\bar{b}\right)^n \bar{a}^*.$$

Hence, we infer the equality

$$\left(\bar{a}+\bar{b}\right)^* = \sum_{n\geq 0}\sum_{j\geq 0} \bar{a}^j \sqcup\!\sqcup\, \bar{b}^n,$$

which implies immediately

$$\left(\bar{a}+\bar{b}\right)^* = (\bar{a}^*\bar{b})^*\bar{a}^*.$$

Applying the complete star semiring morphism defined above, we obtain the sum star identity in S:

$$(a+b)^* = (a^*b)^*a^*.$$

The product star identity is clear by

$$\begin{aligned}(ab)^* &= 1 + \sum_{n\geq 1}(ab)^n = 1 + a\left(\sum_{n\geq 0}(ba)^n\right)b\\ &= 1 + a(ba)^*b. \quad \square\end{aligned}$$

Finally, we show that morphisms between two semirings and also particular morphisms between free monoids induce morphisms between the associated semirings of formal power series.

First, let Σ be an alphabet, S, S' two semirings and $h : S \to S'$ a morphism. We define $\bar{h} : S\langle\langle\Sigma^*\rangle\rangle \to S'\langle\langle\Sigma^*\rangle\rangle$ by $\bar{h}(r) = h \circ r$ for each $r \in S\langle\langle\Sigma^*\rangle\rangle$, i.e., $(\bar{h}(r), w) = h((r, w))$ for each $w \in \Sigma^*$. Often, $\bar{h}$ is again denoted by h. The following is straightforward by elementary calculations.

Proposition 3.5. *Let Σ be an alphabet, S, S' two semirings and $h : S \to S'$ a semiring morphism. Then $h : S\langle\langle\Sigma^*\rangle\rangle \to S'\langle\langle\Sigma^*\rangle\rangle$ is again a semiring morphism. Moreover, if r is cycle-free, so is $h(r)$ and $h(r^*) = (h(r))^*$.*

Second, let S be a semiring, Σ, Σ' two alphabets and $h : \Sigma^* \to \Sigma'^*$ a morphism. We define $h^{-1} : S\langle\langle\Sigma'^*\rangle\rangle \to S\langle\langle\Sigma^*\rangle\rangle$ by $h^{-1}(r') = r' \circ h$ for each $r' \in S\langle\langle\Sigma'^*\rangle\rangle$, that is, $(h^{-1}(r'), v) = (r', h(v))$ for each $v \in \Sigma^*$. We call $h : \Sigma^* \to \Sigma'^*$ *length-preserving*, if $|v| = |h(v)|$ for each $v \in \Sigma^*$; equivalently,

$h(x) \in \Sigma'$ for each $x \in \Sigma$. Further, h is *non-deleting*, if $h(x) \neq \varepsilon$ for each $x \in \Sigma$; equivalently, $|v| \leq |h(v)|$ for each $v \in \Sigma^*$. If h is non-deleting or if S is complete, we define $\bar{h} : S\langle\langle\Sigma^*\rangle\rangle \to S\langle\langle\Sigma'^*\rangle\rangle$ by letting $(\bar{h}(r), w) = \sum_{v \in \Sigma^*, h(v)=w} (r, v)$ for each $r \in S\langle\langle\Sigma^*\rangle\rangle$ and $w \in \Sigma'^*$. Observe that if h is non-deleting, $h^{-1}(w)$ is a finite set for each $w \in \Sigma^*$, and hence $\bar{h}(r)$ is well defined.

Proposition 3.6. *Let S be a semiring, Σ, Σ' two alphabets and $h : \Sigma^* \to \Sigma'^*$ a morphism.*

(i) Let h be length-preserving. Then the mapping $h^{-1} : S\langle\langle\Sigma'^*\rangle\rangle \to S\langle\langle\Sigma^*\rangle\rangle$ is a semiring morphism. Moreover, if $r' \in S\langle\langle\Sigma'^*\rangle\rangle$ is cycle-free, then so is $h^{-1}(r')$, and $h^{-1}(r'^*) = (h^{-1}(r'))^*$.

(ii) Let h be nondeleting, or assume that S is complete. Then $\bar{h} : S\langle\langle\Sigma^*\rangle\rangle \to S\langle\langle\Sigma'^*\rangle\rangle$ is a semiring morphism. Moreover, if h is non-deleting and $r \in S\langle\langle\Sigma^*\rangle\rangle$ is cycle-free, then so is $\bar{h}(r)$, and $\bar{h}(r^*) = (\bar{h}(r))^*$.

Proof. This can be shown again by elementary calculations. For (i), note that if $v \in \Sigma^*$ and $h(v) = w_1 w_2$ with $w_1, w_2 \in \Sigma'^*$, then since h is length-preserving, there are $v_1, v_2 \in \Sigma^*$ with $v = v_1 v_2$ and $h(v_1) = w_1, h(v_2) = w_2$. This implies that h^{-1} preserves the Cauchy product. $\square$

4 Matrices

In this section, we introduce and investigate (possibly infinite) matrices. These are important here since the structure and the behavior of weighted automata can often be compactly described using matrices (see Chaps. 3, 4, and 7 of this book [12, 38, 34]), and hence results from matrix algebra can be used to derive results for weighted automata.

Consider two nonempty index sets I and I' and a set U. A mapping $A : I \times I' \to U$ is called a *matrix*. The values of A are denoted by $A_{i,i'}$, where $i \in I$ and $i' \in I'$. The values $A_{i,i'}$ are also referred to as the *entries* of the matrix A. In particular, $A_{i,i'}$ is called the (i, i')-*entry* of A. The collection of all matrices as defined above is denoted by $U^{I \times I'}$.

If both I and I' are finite, then A is called a *finite matrix*. If I or I' is a singleton, then $A^{I \times I'}$ is denoted by $A^{1 \times I'}$ or $A^{I \times 1}$, and A is called a *row* or *column vector*, respectively. If $A \in U^{I \times 1}$ (resp. $A \in U^{1 \times I'}$), then we often denote the ith entry of A for $i \in I$ (resp. $i \in I'$), by A_i instead of $A_{i,1}$ (resp. $A_{1,i}$). If $I = \{1, \ldots, m\}$ and $I' = \{1, \ldots, n\}$, the set $U^{I \times I'}$ is denoted by $U^{m \times n}$.

As before, we introduce some operations and special matrices inducing a monoid or semiring structure to matrices. Let S be a semiring. For $A, B \in S^{I \times I'}$, we define the *sum* $A + B \in S^{I \times I'}$ by $(A + B)_{i,i'} = A_{i,i'} + B_{i,i'}$ for all $i \in I, i' \in I'$. Furthermore, we introduce the *zero matrix* $0 \in S^{I \times I'}$. All entries of the zero matrix 0 are 0. By these definitions, $\langle S^{I\times I'}, +, 0\rangle$ is a commutative monoid.

Let $A \in S^{I\times I'}$. Consider, for $i \in I$, the set of indices $\{j \mid A_{ij} \neq 0\}$. Then A is called a *row finite matrix* if these sets are finite for all $i \in I$. Similarly, consider, for $i' \in I'$, the set of indices $\{j \mid A_{ji'} \neq 0\}$. Then A is called a *column finite matrix* if these sets are finite for all $i' \in I'$.

If A is row finite or B is column finite, or if S is complete, then for $A \in S^{I_1\times I_2}$ and $B \in S^{I_2\times I_3}$, we define the *product* $AB \in S^{I_1\times I_3}$ by

$$(AB)_{i_1,i_3} = \sum_{i_2\in I_2} A_{i_1,i_2} B_{i_2,i_3} \quad \text{for all } i_1 \in I_1,\ i_3 \in I_3.$$

Furthermore, we introduce the *matrix of unity* $E \in S^{I\times I}$. The diagonal entries $E_{i,i}$ of E are equal to 1, the off-diagonal entries E_{i_1,i_2} $(i_1 \neq i_2)$ of E are equal to 0, for $i, i_1, i_2 \in I$.

It is easily shown that matrix multiplication is associative, the distributivity laws are valid for matrix addition and multiplication, E is a multiplicative unit, and 0 is a multiplicative zero. So, we infer that $\langle S^{I\times I}, +, \cdot, 0, E\rangle$ is a semiring if I is finite or if S is complete. Moreover, the row finite matrices in $S^{I\times I}$ and the column finite matrices in $S^{I\times I}$ form semirings.

If S is complete, infinite sums can be extended to matrices. Consider $S^{I\times I'}$ and define, for $A_j \in S^{I\times I'}$, $j \in J$, where J is an index set, $\sum_{j\in J} A_j$ by its entries:

$$\left(\sum_{j\in J} A_j\right)_{i,i'} = \sum_{j\in J} (A_j)_{i,i'}, \quad \text{for all } i \in I,\ i' \in I'.$$

By this definition, $S^{I\times I}$ is a complete semiring.

If S is ordered, the order on S is extended pointwise to matrices A and B in $S^{I\times I'}$:

$$A \le B \quad \text{if} \quad A_{i,i'} \le B_{i,i'} \text{ for all } i \in I,\ i' \in I'.$$

If S is continuous, then so is $S^{I\times I}$.

Eventually, if S is a locally closed star semiring, then $S^{n\times n}$, $n \ge 1$, is again a locally closed star semiring (see Ésik and Kuich [10], Zhao [41]); and if S is a Conway semiring, then $S^{n\times n}$, $n \ge 1$, is again a Conway semiring (see Conway [6], Bloom and Ésik [4], Ésik and Kuich [9]). Clearly, if S is locally finite, then so is $S^{n\times n}$ for each $n \ge 1$ (cf. [7]).

For the remainder of this chapter, I (resp. Q), possibly provided with indices, denotes an *arbitrary* (resp. *finite*) *index set*. For the rest of this section, we assume that all products of matrices are well-defined.

We now introduce blocks of matrices. Consider a matrix A in $S^{I\times I}$. Assume that we have a decomposition $I = \bigcup_{j\in J} I_j$ where J and all I_j $(j \in J)$ are non-empty index sets such that $I_{j_1} \cap I_{j_2} = \emptyset$ for $j_1 \neq j_2$. The mapping A, restricted to the domain $I_{j_1} \times I_{j_2}$, i.e., $A\restriction_{I_{j_1}\times I_{j_2}} : I_{j_1} \times I_{j_2} \to S$ is, of course, a matrix in $S^{I_{j_1}\times I_{j_2}}$. We denote it by $A(I_{j_1}, I_{j_2})$ and call it the (I_{j_1}, I_{j_2})-*block* of A.

We can compute the blocks of the sum and the product of matrices A and B from the blocks of A and B in the usual way:

$$(A+B)(I_{j_1}, I_{j_2}) = A(I_{j_1}, I_{j_2}) + B(I_{j_1}, I_{j_2}),$$
$$(AB)(I_{j_1}, I_{j_2}) = \sum_{j \in J} A(I_{j_1}, I_j) B(I_j, I_{j_2}).$$

In a similar manner, the matrices of $S^{I \times I'}$ can be partitioned into blocks. This yields the computational rule

$$(A+B)(I_j, I'_{j'}) = A(I_j, I'_{j'}) + B(I_j, I'_{j'}).$$

If we consider matrices $A \in S^{I \times I'}$ and $B \in S^{I' \times I''}$ partitioned into compatible blocks, i.e., I' is partitioned into the same index sets for both matrices, then we obtain the computational rule

$$(AB)(I_j, I''_{j''}) = \sum_{j' \in J'} A(I_j, I'_{j'}) B(I'_{j'}, I''_{j''}).$$

Now let us assume that I and I' are finite, or that S is complete. In the sequel, the following isomorphisms are needed:

(i) The semirings

$$\left(S^{I' \times I'}\right)^{I \times I}, \; S^{(I \times I') \times (I \times I')}, \; S^{(I' \times I) \times (I' \times I)}, \; \left(S^{I \times I}\right)^{I' \times I'}$$

are isomorphic by the correspondences between

$$(A_{i_1,i_2})_{i'_1,i'_2}, \; A_{(i_1,i'_1),(i_2,i'_2)}, \; A_{(i'_1,i_1),(i'_2,i_2)}, \; (A_{i'_1,i'_2})_{i_1,i_2}$$

for all $i_1, i_2 \in I$, $i'_1, i'_2 \in I'$.

(ii) The semirings $S^{I \times I}\langle\langle \Sigma^* \rangle\rangle$ and $(S\langle\langle \Sigma^* \rangle\rangle)^{I \times I}$ are isomorphic by the correspondence between $(A, w)_{i_1,i_2}$ and (A_{i_1,i_2}, w) for all $i_1, i_2 \in I$, $w \in \Sigma^*$.

Moreover, analogous isomorphisms are valid if the semirings of row finite or column finite matrices are considered. Observe that, in case S is complete, these correspondences are isomorphisms of complete semirings, i.e., they respect infinite sums. These isomorphisms are used without further mention. Moreover, the notation A_{i_1,i_2}, where $A \in S^{I_1 \times I_2}\langle\langle \Sigma^* \rangle\rangle$ and $i_1 \in I_1, i_2 \in I_2$, is used: A_{i_1,i_2} is the power series in $S\langle\langle \Sigma^* \rangle\rangle$ such that the coefficient (A_{i_1,i_2}, w) of $w \in \Sigma^*$ is equal to $(A, w)_{i_1,i_2}$. Similarly, the notation (A, w), where $A \in (S\langle\langle \Sigma^* \rangle\rangle)^{I_1 \times I_2}$ and $w \in \Sigma^*$, is used: (A, w) is the matrix in $S^{I_1 \times I_2}$ whose (i_1, i_2)-entry $(A, w)_{i_1,i_2}$ is equal to (A_{i_1,i_2}, w) for each $i_1 \in I_1, i_2 \in I_2$.

For the proof of the next theorem, we need a lemma.

Lemma 4.1. *Let S be a complete star semiring. Then for all $a, b \in S$,*

$$(a+b)^* = (a + ba^*b)^*(1 + ba^*).$$

Proof. Using Theorem 3.4, we have

$$\begin{aligned}(a + ba^*b)^*(1 + ba^*) &= (a^*ba^*b)^*a^*(1 + ba^*)\\ &= \sum_{n\geq 0}(a^*b)^{2n}a^* + \sum_{n\geq 0}(a^*b)^{2n+1}a^*\\ &= (a^*b)^*a^* = (a + b)^*. \quad \square\end{aligned}$$

The next theorem is central for automata theory (see Conway [6], Lehmann [30], Kuich and Salomaa [29], Kuich [28], Bloom and Ésik [4], Kozen [24]). It allows us to compute the blocks of the star of a matrix A by sum, product, and star of the blocks of A.

For notational convenience, we will denote in Theorem 4.2 and in Corollaries 4.3 and 4.4 the matrices $A(I_i, I_j)$ by $A_{i,j}$, for $1 \leq i, j \leq 3$.

Theorem 4.2. *Let S be a complete star semiring. Let $A \in S^{I\times I}$ and $I = I_1 \cup I_2$ with $I_1, I_2 \neq \emptyset$ and $I_1 \cap I_2 = \emptyset$. Then*

$$\begin{aligned}A^*(I_1, I_1) &= (A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1})^*,\\ A^*(I_1, I_2) &= (A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1})^*A_{1,2}A_{2,2}^*,\\ A^*(I_2, I_1) &= (A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2})^*A_{2,1}A_{1,1}^*,\\ A^*(I_2, I_2) &= (A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2})^*.\end{aligned}$$

Proof. Consider the matrices

$$A_1 = \begin{pmatrix} A_{1,1} & 0 \\ 0 & A_{2,2} \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & A_{1,2} \\ A_{2,1} & 0 \end{pmatrix}.$$

The computation of $(A_1 + A_2A_1^*A_2)^*(E + A_2A_1^*)$ and application of Lemma 4.1 prove our theorem. $\square$

Corollary 4.3. *If $A_{2,1} = 0$, then*

$$A^* = \begin{pmatrix} A_{1,1}^* & A_{1,1}^*A_{1,2}A_{2,2}^* \\ 0 & A_{2,2}^* \end{pmatrix}.$$

Corollary 4.4. *Let $I = I_1 \cup I_2 \cup I_3$ be a decomposition into pairwise disjoint nonempty subsets. If $A_{2,1} = 0$, $A_{3,1} = 0$, and $A_{3,2} = 0$, then*

$$A^* = \begin{pmatrix} A_{1,1}^* & A_{1,1}^*A_{1,2}A_{2,2}^* & A_{1,1}^*A_{1,2}A_{2,2}^*A_{2,3}A_{3,3}^* + A_{1,1}^*A_{1,3}A_{3,3}^* \\ 0 & A_{2,2}^* & A_{2,2}^*A_{2,3}A_{3,3}^* \\ 0 & 0 & A_{3,3}^* \end{pmatrix}.$$

Next, we consider an arbitrary partition of the index set I.

Theorem 4.5. *Let S be a complete star semiring, and let $I = \bigcup_{j \in J} I_j$ be a decomposition into pairwise disjoint nonempty subsets. Fix $j_0 \in J$. Assume that the only non-null blocks of the matrix $A \in S^{I \times I}$ are $A(I_j, I_{j_0})$, $A(I_{j_0}, I_j)$ and $A(I_j, I_j)$, for all $j \in J$. Then*

$$A^*(I_{j_0}, I_{j_0}) = \Bigg(A(I_{j_0}, I_{j_0}) + \sum_{j \in J,\, j \neq j_0} A(I_{j_0}, I_j) A(I_j, I_j)^* A(I_j, I_{j_0}) \Bigg)^* .$$

Proof. We partition I into I_{j_0} and $I' = I - I_{j_0}$. Then $A(I', I')$ is a block-diagonal matrix and $(A(I', I')^*)(I_j, I_j) = A(I_j, I_j)^*$ for all $j \in J - \{j_0\}$. By Theorem 4.2, we obtain

$$A^*(I_{j_0}, I_{j_0}) = \big(A(I_{j_0}, I_{j_0}) + A(I_{j_0}, I') A(I', I')^* A(I', I_{j_0}) \big)^* .$$

The computation of the right-hand side of this equality proves our theorem. □

We now introduce the *Kronecker product* (also called *tensor product*) $A \otimes B \in S^{(I_1 \times I_2) \times (I_1' \times I_2')}$ for the matrices $A \in S^{I_1 \times I_1'}$ and $B \in S^{I_2 \times I_2'}$, by defining its entries:

$$(A \otimes B)_{(i_1, i_2), (i_1', i_2')} = A_{i_1, i_1'} B_{i_2, i_2'}, \quad \text{for all } i_1 \in I_1,\ i_1' \in I_1',\ i_2 \in I_2,\ i_2' \in I_2'.$$

Sometimes, the Kronecker product $A \otimes B$ is defined to be in $(S^{I_2 \times I_2'})^{I_1 \times I_1'}$ with

$$\big((A \otimes B)_{i_1, i_1'} \big)_{i_2, i_2'} = A_{i_1, i_1'} B_{i_2, i_2'}, \quad \text{for all } i_1 \in I_1,\ i_1' \in I_1',\ i_2 \in I_2,\ i_2' \in I_2'.$$

Since the semirings $S^{(I_1 \times I_2) \times (I_1 \times I_2)}$ and $(S^{I_2 \times I_2})^{I_1 \times I_1}$ are isomorphic, this will not make any difference in the computations.

Easy proofs show the following computational rules for Kronecker products.

Theorem 4.6. *Let $A, A' \in S^{I_1 \times I_1'}$, $B, B' \in S^{I_2 \times I_2'}$, $C \in S^{I_3 \times I_3'}$. Then:*

(i) $(A + A') \otimes B = A \otimes B + A' \otimes B$.
(ii) $A \otimes (B + B') = A \otimes B + A \otimes B'$.
(iii) $A \otimes 0 = 0$ *and* $0 \otimes B = 0$.
(iv) $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.

Theorem 4.7. *Let $A \in S^{I_1 \times I_2}\langle \{\varepsilon\} \rangle$, $B \in S^{I_2 \times I_3}\langle \{\varepsilon\} \rangle$, $C \in S^{I_4 \times I_5}\langle\langle \Sigma^* \rangle\rangle$ and $D \in S^{I_5 \times I_6}\langle\langle \Sigma^* \rangle\rangle$. Assume that S is complete or that (A, ε) and (C, w) are row finite for all $w \in \Sigma^*$, or that (B, ε) and (D, w) are column finite for all $w \in \Sigma^*$. Furthermore, assume that all entries of (B, ε) commute with those of (C, w) for all $w \in \Sigma^*$. Then*

$$(AB) \otimes (CD) = (A \otimes C)(B \otimes D).$$

Proof. Let $i_j \in I_j$ for $j = 1, 3, 4, 6$. Then we obtain

$$\begin{aligned}
&\big((AB) \otimes (CD)\big)_{(i_1,i_3),(i_4,i_6)} \\
&\quad = (AB)_{i_1,i_3}(CD)_{i_4,i_6} \\
&\quad = \sum_{i_2 \in I_2} \sum_{i_5 \in I_5} A_{i_1,i_2} B_{i_2,i_3} C_{i_4,i_5} D_{i_5,i_6} \\
&\quad = \sum_{i_2 \in I_2} \sum_{i_5 \in I_5} A_{i_1,i_2} C_{i_4,i_5} B_{i_2,i_3} D_{i_5,i_6} \\
&\quad = \sum_{(i_2,i_5) \in I_2 \times I_5} (A \otimes C)_{(i_1,i_4),(i_2,i_5)} (B \otimes D)_{(i_2,i_5),(i_3,i_6)} \\
&\quad = \big((A \otimes C)(B \otimes D)\big)_{(i_1,i_4),(i_3,i_6)}. \qquad \square
\end{aligned}$$

The Kronecker product is useful for investigating the Hadamard product of formal power series, cf., e.g., Chap. 4, Sect. 4.2 [38] of this book.

5 Cycle-Free Linear Equations

Let Σ be an alphabet and S any semiring. Cycle-free linear equations over $S\langle\langle \Sigma^* \rangle\rangle$ are a useful tool for proving identities in $S\langle\langle \Sigma^* \rangle\rangle$. Assume that two expressions are shown to be solutions of such an equation. Then the uniqueness of the solution (shown below) implies that these two expressions represent the same formal power series in $S\langle\langle \Sigma^* \rangle\rangle$.

A *cycle-free linear equation* (*over* $S\langle\langle \Sigma^* \rangle\rangle$) has the form

$$y = ry + s,$$

where $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and r is cycle-free. A *solution* to this equation is given by a power series $\sigma \in S\langle\langle \Sigma^* \rangle\rangle$ such that $\sigma = r\sigma + s$.

Theorem 5.1. *The cycle-free equation* $y = ry + s$ *with* $r, s \in S\langle\langle \Sigma^* \rangle\rangle$, r *cycle-free, has the unique solution* $\sigma = r^* s$.

Proof. By Theorem 3.1, we obtain

$$r\sigma + s = rr^*s + s = (rr^* + \varepsilon)s = r^*s = \sigma.$$

Hence, σ is a solution.

Assume that r is cycle-free of index k, i.e., $(r, \varepsilon)^k = 0$, and that ϱ is a solution. Then by substitution, we obtain for all $n \geq 0$,

$$\varrho = r\varrho + s = \cdots = r^n \varrho + \sum_{0 \leq j < n} r^j s.$$

We now compute the coefficients (ϱ, w) for each $w \in \Sigma^*$:

$$(\varrho, w) = \left(r^{k(|w|+1)}\varrho, w\right) + \sum_{0 \le j < k(|w|+1)} \left(r^j s, w\right) = (r^* s, w) = (\sigma, w).$$

Hence, $\varrho = \sigma$. □

For power series over arbitrary semirings, the sum star identity and the product star identity are valid only for some cycle-free power series.

Theorem 5.2. *Let $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and assume that r, r^*s and $r+s$ are cycle-free. Then the sum star identity is valid for r and s.*

Proof. We show that $(r^*s)^*r^*$ is a solution of the cycle-free equation $y = (r+s)y + \varepsilon$:

Indeed, by Theorem 3.2, we have

$$\begin{aligned}(r+s)(r^*s)^*r^* + \varepsilon &= rr^*(sr^*)^* + (sr^*)(sr^*)^* + \varepsilon \\ &= rr^*(sr^*)^* + (sr^*)^* = r^*(sr^*)^* = (r^*s)^*r^*.\end{aligned}$$

We now apply Theorem 5.1. □

Theorem 5.3. *Let $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and assume that rs is cycle-free. Then the product star identity is valid for r and s.*

Proof. By Theorems 3.2 and 3.1, we obtain

$$\varepsilon + r(sr)^*s = \varepsilon + rs(rs)^* = (rs)^*. \quad \square$$

Corollary 5.4. *Let $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and assume that r is cycle-free and s is proper. Then the sum star identity and the product star identity are valid for r and s.*

Compare the next lemma with Lemma 4.1.

Lemma 5.5. *Let $r, s \in S\langle\langle \Sigma^* \rangle\rangle$ and assume that r, $r+s$ and $r+sr^*s$ are cycle-free. Then*

$$(r+s)^* = (r+sr^*s)^*(\varepsilon + sr^*).$$

Proof. By our assumptions, the power series r^*, $(r+s)^*$ and $(r+sr^*s)^*$ exist. By Theorem 3.1, we have

$$(r+s)^* = r(r+s)^* + s(r+s)^* + \varepsilon.$$

Hence, $(r+s)^*$ is a solution of the equation $y = ry + s(r+s)^* + \varepsilon$. By Theorem 5.1 and the cycle-freeness of r, another representation of this unique solution is $r^*s(r+s)^* + r^*$. Substituting $r^*s(r+s)^* + r^*$ into the third occurrence in the above equality yields

$$(r+s)^* = (r+sr^*s)(r+s)^* + sr^* + \varepsilon.$$

This shows that $(r+s)^*$ is a solution of the equation

$$y = (r + sr^*s)y + sr^* + \varepsilon.$$

By Theorem 5.1 and the cycle-freeness of $r + sr^*s$, another representation for the unique solution of this equation is

$$(r + sr^*s)^*(\varepsilon + sr^*). \quad \square$$

Consider matrices $A \in S^{I_1\times I_2}\langle\langle\Sigma^*\rangle\rangle$ and $B \in S^{I_2\times I_3}\langle\langle\Sigma^*\rangle\rangle$ such that either the matrices $(A,w) \in S^{I_1\times I_2}$ are row finite for all $w \in \Sigma^*$ or the matrices $(B,w) \in S^{I_2\times I_3}$ are column finite for all $w \in \Sigma^*$. Then $AB \in S^{I_1\times I_3}\langle\langle\Sigma^*\rangle\rangle$ is well-defined. Hence, for a matrix $A \in S^{I\times I}\langle\langle\Sigma^*\rangle\rangle$, such that the matrices $(A,w) \in S^{I\times I}$ are row (resp. column) finite for all $w \in \Sigma^*$, all powers $A^n \in S^{I\times I}\langle\langle\Sigma^*\rangle\rangle$ are well-defined. If, furthermore, A is cycle-free then $A^* \in S^{I\times I}\langle\langle\Sigma^*\rangle\rangle$ is well-defined. If (A,w) is row and column finite for all $w \in \Sigma^*$, then so is (A^n,w) for all $n \in \mathbb{N}$ and $w \in \Sigma^*$.

Lemma 4.1 is the main tool for proving the matrix identities of Theorem 4.2. In an analogous manner, Lemma 5.5 is a main tool for proving—under different assumptions—the same matrix identities in the next theorem.

For the rest of the section, let $I = I_1 \cup I_2$ with $I_1, I_2 \neq \emptyset$ and $I_1 \cap I_2 = \emptyset$. The notation is similar to that in Theorem 4.2, but with $A \in S^{I\times I}\langle\langle\Sigma^*\rangle\rangle$ instead of $A \in S^{I\times I}$. For notational convenience, we will denote in Theorems 5.6 and 5.7 and in Corollaries 5.8 and 5.9 the matrices $A(I_i, I_j)$ by $A_{i,j}$, for $1 \leq i,j \leq 3$.

Theorem 5.6. *Assume that $A \in S^{I\times I}\langle\langle\Sigma^*\rangle\rangle$ is cycle-free and (A,w) is row and column finite for all $w \in \Sigma^*$. Furthermore, assume that $A_{1,1}$, $A_{2,2}$, $A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1}$ and $A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2}$ are cycle-free. Then*

$$\begin{aligned}
A^*(I_1,I_1) &= (A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1})^*,\\
A^*(I_1,I_2) &= (A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1})^*A_{1,2}A_{2,2}^*,\\
A^*(I_2,I_1) &= (A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2})^*A_{2,1}A_{1,1}^*,\\
A^*(I_2,I_2) &= (A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2})^*.
\end{aligned}$$

Proof. Consider the matrices

$$A_1 = \begin{pmatrix} A_{1,1} & 0 \\ 0 & A_{2,2} \end{pmatrix} \quad \text{and} \quad A_2 = \begin{pmatrix} 0 & A_{1,2} \\ A_{2,1} & 0 \end{pmatrix}.$$

Since the blocks of the block-diagonal matrix A_1 are cycle-free, the matrix A_1^* exists and equals

$$A_1^* = \begin{pmatrix} A_{1,1}^* & 0 \\ 0 & A_{2,2}^* \end{pmatrix}.$$

This implies that

$$A_1 + A_2A_1^*A_2 = \begin{pmatrix} A_{1,1} + A_{1,2}A_{2,2}^*A_{2,1} & 0 \\ 0 & A_{2,2} + A_{2,1}A_{1,1}^*A_{1,2} \end{pmatrix}.$$

Since the blocks of the block-diagonal matrix $A_1 + A_2 A_1^* A_2$ are cycle-free, the matrix $(A_1 + A_2 A_1^* A_2)^*$ exists and equals

$$(A_1 + A_2 A_1^* A_2)^* = \begin{pmatrix} (A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1})^* & 0 \\ 0 & (A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2})^* \end{pmatrix}.$$

We now apply Lemma 5.5 with $r = A_1$ and $s = A_2$. The computation of

$$(A_1 + A_2 A_1^* A_2)^* (E + A_2 A_1^*)$$

proves the theorem. □

Theorem 5.7. *Consider $A \in S^{I \times I}\langle\langle \Sigma^* \rangle\rangle$ such that (A, w) is row and column finite for all $w \in \Sigma^*$. Furthermore, assume that $A_{1,1}$ and $A_{2,2}$ are cycle-free, and $A_{1,2}$ or $A_{2,1}$ is proper. Then A is cycle-free and*

$$\begin{aligned} A^*(I_1, I_1) &= (A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1})^*, \\ A^*(I_1, I_2) &= (A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1})^* A_{1,2} A_{2,2}^*, \\ A^*(I_2, I_1) &= (A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2})^* A_{2,1} A_{1,1}^*, \\ A^*(I_2, I_2) &= (A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2})^*. \end{aligned}$$

Proof. We only prove the case where $A_{2,1}$ is proper. The proof of the other case is similar. An easy proof by induction on $j \geq 1$ shows that

$$(A, \varepsilon)^j = \begin{pmatrix} (A_{1,1}, \varepsilon)^j & \sum_{j_1 + j_2 = j-1} (A_{1,1}, \varepsilon)^{j_1} (A_{1,2}, \varepsilon)(A_{2,2}, \varepsilon)^{j_2} \\ 0 & (A_{2,2}, \varepsilon)^j \end{pmatrix}.$$

Now let $A_{1,1}$ and $A_{2,2}$ be cycle-free of index k. Then $(A, \varepsilon)^{2k} = 0$ and A is cycle-free. Furthermore $(A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1}, \varepsilon) = (A_{1,1}, \varepsilon)$ and $(A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2}, \varepsilon) = (A_{2,2}, \varepsilon)$. Hence, the assumptions of Theorem 5.6 are satisfied and our theorem is proved. □

Corollary 5.8. *Consider $A \in S^{I \times I}\langle\langle \Sigma^* \rangle\rangle$ such that (A, w) is row and column finite for all $w \in \Sigma^*$. Furthermore, assume that $A_{1,1}$ and $A_{2,2}$ are cycle-free and that $A_{2,1} = 0$. Then A is cycle-free and*

$$A^* = \begin{pmatrix} A_{1,1}^* & A_{1,1}^* A_{1,2} A_{2,2}^* \\ 0 & A_{2,2}^* \end{pmatrix}.$$

Observe that for finite matrices, the row and column finiteness of (A, w) for all $w \in \Sigma^*$ is satisfied and is not needed as assumption in Theorem 5.7. If A is finite and proper, all assumptions of Theorem 5.7 are satisfied.

Corollary 5.9. *Let I be finite and $A \in S^{I \times I}\langle\langle \Sigma^* \rangle\rangle$ be proper. Then*

$$\begin{aligned} A^*(I_1, I_1) &= (A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1})^*, \\ A^*(I_1, I_2) &= (A_{1,1} + A_{1,2} A_{2,2}^* A_{2,1})^* A_{1,2} A_{2,2}^*, \\ A^*(I_2, I_1) &= (A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2})^* A_{2,1} A_{1,1}^*, \\ A^*(I_2, I_2) &= (A_{2,2} + A_{2,1} A_{1,1}^* A_{1,2})^*. \end{aligned}$$

References

1. J. Adámek, E. Nelson, and J. Reiterman. Tree constructions of free continuous algebras. *Journal of Computer and System Sciences*, 24:114–146, 1982.
2. J. Berstel, editor. *Séries formelles en variables non commutatives et applications*. Laboratoire d'Informatique Théorique et Programmation, Ecole Nationale Supérieure de Techniques Avancées, Paris, 1978.
3. J. Berstel and C. Reutenauer. *Les séries rationelles et leurs langages*. Masson, Paris, 1984. English translation: *Rational Series and Their Languages*, volume 12 of *Monographs in Theoretical Computer Science. An EATCS Series*. Springer, Berlin, 1988.
4. S.L. Bloom and Z. Ésik. *Iteration Theories*, *Monographs in Theoretical Computer Science. An EATCS Series*. Springer, Berlin, 1993.
5. G. Carré. *Graphs and Networks*. Clarendon, Oxford, 1979.
6. J.H. Conway. *Regular Algebra and Finite Machines*. Chapman & Hall, London, 1971.
7. M. Droste and P. Gastin. On aperiodic and star-free formal power series in partially commuting variables. *Theory of Computing Systems*, 42:608–631, 2008. Extended abstract in: D. Krob, A.A. Milchalev, and A.V. Milchalev, editors, *Formal Power Series and Algebraic Combinatorics, 12th Int. Conf., Moscow*, pages 158–169. Springer, Berlin, 2000.
8. S. Eilenberg. *Automata, Languages and Machines, volume A*. Academic Press, San Diego, 1974.
9. Z. Ésik and W. Kuich. Modern automata theory. www.dmg.tuwien.ac.at/kuich.
10. Z. Ésik and W. Kuich. Locally closed semirings. *Monatshefte für Mathematik*, 137:21–29, 2002.
11. Z. Ésik and W. Kuich. Equational axioms for a theory of automata. In C. Martin-Vide, V. Mitrana, and G. Paun, editors, *Formal Languages and Applications*, volume 148 of *Studies in Fuzziness and Soft Computing*, pages 183–196. Springer, Berlin, 2004.
12. Z. Ésik and W. Kuich. Finite automata. In M. Droste, W. Kuich, and H. Vogler, editors, *Handbook of Weighted Automata*. Chapter 3. Springer, Berlin, 2009.
13. K. Głazek. *A Guide to the Literature on Semirings and Their Applications in Mathematics and Information Science*. Kluwer Academic, Dordrecht, 2002.
14. J.A. Goguen, J.W. Thatcher, E.G. Wagner, and J.B. Wright. Initial algebra semantics and continuous algebras. *Journal of the Association for Computing Machinery*, 24:68–95, 1977.
15. J. Golan. *Semirings and Their Applications*. Kluwer Academic, Dordrecht, 1999.
16. M. Goldstern. Vervollständigung von Halbringen. Diplomarbeit, Technische Universität Wien, 1985.

17. I. Guessarian. *Algebraic Semantics*, volume 99 of *Lecture Notes in Computer Science*. Springer, Berlin, 1981.
18. P. Hájek. *Metamathematics of Fuzzy Logic*. Kluwer Academic, Dordrecht, 1998.
19. U. Hebisch. The Kleene theorem in countably complete semirings. *Bayreuther Mathematische Schriften*, 31:55–66, 1990.
20. U. Hebisch and H.J. Weinert. *Halbringe—Algebraische Theorie und Anwendungen in der Informatik*. Teubner, Leipzig, 1993. English translation: *Semirings—Algebraic Theory and Applications in Computer Science*. World Scientific, Singapore, 1998.
21. B. Heidergott, G.J. Olsder, and J. van der Woude. *Max Plus at Work*. Princeton University Press, Princeton, 2006.
22. G. Karner. On limits in complete semirings. *Semigroup Forum*, 45:148–165, 1992.
23. G. Karner. Continuous monoids and semirings. *Theoretical Computer Science*, 318:355–372, 2004.
24. D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110:366–390, 1994.
25. D. Krob. Monoides et semi-anneaux complets. *Semigroup Forum*, 36:323–339, 1987.
26. D. Krob. Monoides et semi-anneaux continus. *Semigroup Forum*, 37:59–78, 1988.
27. W. Kuich. The Kleene and the Parikh theorem in complete semirings. In *ICALP'87*, volume 267 of *Lecture Notes in Computer Science*, pages 212–225. Springer, Berlin, 1987.
28. W. Kuich. Semirings and formal power series: Their relevance to formal languages and automata theory. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Languages, volume 1*, Chapter 9, pages 609–677. Springer, Berlin, 1997.
29. W. Kuich and A. Salomaa. *Semirings, Automata, Languages*, volume 5 of *Monographs in Theoretical Computer Science. An EATCS Series*. Springer, Berlin, 1986.
30. D.J. Lehmann. Algebraic structures for transitive closure. *Theoretical Computer Science*, 4:59–76, 1977.
31. E.G. Manes and M.A. Arbib. *Algebraic Approaches to Program Semantics*. Springer, Berlin, 1986.
32. G. Markowsky. Chain-complete posets and directed sets with applications. *Algebra Universalis*, 6:53–68, 1976.
33. M. Mohri. Semiring frameworks and algorithms for shortest-distance problems. *Journal of Automata, Languages and Combinatorics*, 7:321–350, 2002.
34. I. Petre and A. Salomaa. Algebraic systems and pushdown automata. In M. Droste, W. Kuich, and H. Vogler, editors, *Handbook of Weighted Automata*. Chapter 7. Springer, Berlin, 2009.

35. G. Rahonis. Fuzzy languages. In M. Droste, W. Kuich, and H. Vogler, editors, *Handbook of Weighted Automata*. Chapter 12. Springer, Berlin, 2009.
36. J. Sakarovitch. Kleene's theorem revisited. In *Trends, Techniques, and Problems in Theoretical Computer Science, 4th International Meeting of Young Computer Scientists*, volume 281 of *Lecture Notes in Computer Science*, pages 39–50. Springer, Berlin, 1987.
37. J. Sakarovitch. *Éléments de Théorie des Automates*. Vuibert, Paris, 2003.
38. J. Sakarovitch. Rational and recognisable power series. In M. Droste, W. Kuich, and H. Vogler, editors, *Handbook of Weighted Automata*. Chapter 4. Springer, Berlin, 2009.
39. A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Springer, Berlin, 1978.
40. W. Wechler. *The Concept of Fuzziness in Automata and Language Theory*. Akademie Verlag, Berlin, 1978.
41. X. Zhao. Locally closed semirings and iteration semirings. *Monatshefte für Mathematik*, 144:157–167, 2005.
42. U. Zimmermann. *Linear and Combinatorial Optimization in Ordered Algebraic Structures*, volume 10 of *Annals of Discrete Mathematics*. North-Holland, Amsterdam, 1981.