Publ. I.R.M.A. Strasbourg, 1988, 358/S-18
Actes 18^{e} Séminaire Lotharingien, p. 5-51

SEMIRINGS, AUTOMATA AND COMBINATORIAL APPLICATIONS

VON

WERNER KUICH

ABSTRACT. This paper introduces into the basics of linear algebra in semirings and automata theory. These are then applied to combinatorial problems.

The topics from semirings and automata considered in this paper should interest mathematicians who are specialized in combinatorics. They include the basic definitions of semirings and formal power series, convergence and linear equations, matrices, automata, rational power series, algebraic systems, algebraic power series and pushdown automata. The presentation of these topics is along the lines of Sections 1,2,3,4,7,8 and 10 of Kuich,Salomaa [15]. There the results are fully referenced. The Hadamard product of matrices and Construction 5 seem to be new. The Hurwitz product of matrices and Construction 6 are due to Küster [16].

An interested reader is referred to the books on the classical theory of automata and languages:Bucher,Maurer [2],Ginsburg [7],Harrison [10], Hopcroft,Ullman [11],Hotz,Estenfeld [12],Salomaa [19],[20]; and on books on the theory of automata and languages based on formal power series:Berstel,Reutenauer [1],Conway [4],Eilenberg [5],Kuich,Salomaa [15],Salomaa,Soittola [21] and Wechler [23].

There are some books and papers that apply the theory of automata and languages to combinatorics:Chomsky,Schützenberger [3],Eilenberg [5], Goldman [8],Goulden,Jackson [9],Kuich [14] and Straubing [22].

Our applications include the following topics:Rational sequences and rational sequences with finitely many distinct coefficients are characterized; normal form automata for the generation of rational sequences are defined; a new proof for the Cayley-Hamilton Theorem in commutative rings is given; Constructions on automata are defined that lead directly to operations on generating functions; these constructions are applied in a number of examples to rational and algebraic sequences.

1. SEMIRINGS AND POWER SERIES.

In this section we define the basic notions: semirings and formal power series.

By a semiring we mean a set A together with two binary operations + and · and two constant elements 0 and 1 such that

(i) $\langle A,+,0\rangle$ is a commutative monoid,

(ii) $\langle A,\cdot,1\rangle$ is a monoid,

(iii) the distribution laws $a\cdot(b+c) = a\cdot b + a\cdot c$ and $(a+b)\cdot c = a\cdot c + b\cdot c$ hold for every a,b,c,

(iv) $0\cdot a = a\cdot 0 = 0$ for every a.

A semiring is called commutative iff $a\cdot b = b\cdot a$ for every a and b.

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

The two most important semirings are the Boolean semiring $\mathbb{B}$ and the semiring $\mathbb{N}$. Here $\mathbb{B}$ consists of two different elements 0, 1 and is defined by 1+1 = 1. The semiring $\mathbb{N}$ consists of the nonnegative integers with the usual operations.

The following notational conventions will hold throughout the paper: A denotes a semiring, Σ denotes an alphabet and Σ^* denotes the words over Σ including the empty word ε. All items may be indexed.

Mappings r of Σ^* into A 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. We say also that r is a series with (noncommuting) variables in Σ. The collection of all power series r as defined above is denoted by $A\langle\langle\Sigma^*\rangle\rangle$.

Given $r \in A\langle\langle\Sigma^*\rangle\rangle$, where A is a semiring, the subset of Σ^* defined by

$$\{w \mid (r,w) \neq 0\}$$

is termed the support of r and denoted by supp(r). The subset of $A\langle\langle\Sigma^*\rangle\rangle$ consisting of all series with a finite support is denoted

by $A\langle\Sigma^*\rangle$. Series of $A\langle\Sigma^*\rangle$ are referred to as polynomials. It will be convenient to use the notations $A\langle\Sigma\cup\varepsilon\rangle$, $A\langle\Sigma\rangle$ and $A\langle\varepsilon\rangle$ for the collections of polynomials having their supports in $\Sigma\cup\varepsilon$, Σ and ε, respectively.

Observe that we have written ε instead of $\{\varepsilon\}$. We do not usually make any notational distinction between an element and the singleton consisting of that element.

Examples of polynomials belonging to $A\langle\Sigma^*\rangle$ are the power series 0 and w, $w \in \Sigma^*$, defined by $(0,w') = 0$ and $(w,w') = \delta_{w,w'}$ for all $w' \in \Sigma^*$, respectively. Here $\delta_{w,w'}$ denotes the Kronecker symbol: $\delta_{w,w'} = 1$ if $w = w'$ and $\delta_{w,w'} = 0$ if $w \neq w'$. (We will use in the sequel the Kronecker symbol for arbitrary sets.)

For $r_1, r_2 \in A\langle\langle\Sigma^*\rangle\rangle$ we define the sum r_1+r_2 and the product $r_1 \cdot r_2$ by $(r_1+r_2,w) = (r_1,w)+(r_2,w)$ and $(r_1 \cdot r_2,w) = \sum_{w_1w_2=w} (r_1,w_1)(r_2,w_2)$, for all $w \in \Sigma^*$. Clearly, $\langle A\langle\langle\Sigma^*\rangle\rangle,+,\cdot,0,\varepsilon\rangle$ and $\langle A\langle\Sigma^*\rangle,+,\cdot,0,\varepsilon\rangle$ are semirings again.

Subsets of Σ^* are called formal languages over Σ. We now connect the theories of formal languages and formal power series. For $L \subseteq \Sigma^*$, we define the characteristic series of L, $\mathrm{char}(L) \in A\langle\langle\Sigma^*\rangle\rangle$ by $(\mathrm{char}(L),w) = 1$ if $w \in L$ and $(\mathrm{char}(L),w) = 0$ if $w \notin L$.

When we consider formal power series in $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$, then $r \in \mathbb{B}\langle\langle\Sigma^*\rangle\rangle$ corresponds to $L \subseteq \Sigma^*$ iff $r = \mathrm{char}(L)$ (or, equivalently, $L = \mathrm{supp}(r)$). Hence, the semirings $\langle\mathbb{B}\langle\langle\Sigma^*\rangle\rangle,+,\cdot,0,\varepsilon\rangle$ and $\langle\mathcal{P}(\Sigma^*),\cup,\cdot,\emptyset,\{\varepsilon\}\rangle$ are isomorphic. Here $\mathcal{P}$ denotes the power set, $\emptyset$ denotes the empty set and $\cdot$ is the usual product of formal languages.

The Hadamard product of two power series r_1 and r_2 belonging to $A\langle\langle\Sigma_1^*\rangle\rangle$ and $A\langle\langle\Sigma_2^*\rangle\rangle$ is defined by

$$r_1 \odot r_2 = \sum_{w \in (\Sigma_1 \cap \Sigma_2)^*} (r_1,w)(r_2,w)w.$$

In language theory, the operation corresponding to the Hadamard product is the intersection of languages. If r_1 and r_2 correspond to the languages L_1 and L_2 in the isomorphism referred to above then $r_1 \odot r_2$ corresponds to $L_1 \cap L_2$.

Another operation for languages is the Hurwitz (shuffle) product $\sqcup\!\sqcup$. In language theory, it is customarily defined for languages L and L',

by $L \sqcup L' = \{w_1 w_1' \ldots w_n w_n' \mid n \geq 1, w_1 \ldots w_n \in L, w_1' \ldots w_n' \in L'\}$. (Here w_i and w_i' are words, for $i=1,\ldots,n$.) We prefer an inductive definition. For $w_1, w_2 \in \Sigma^*$ and $x_1, x_2 \in \Sigma$, we define

$$w_1 \sqcup \varepsilon = w_1, \quad \varepsilon \sqcup w_2 = w_2,$$

and

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

Hence, $\sqcup$ maps two words over Σ into a power series in $A\langle\langle\Sigma^*\rangle\rangle$. We now define the Hurwitz product of the power series r_1 and r_2 in $A\langle\langle\Sigma^*\rangle\rangle$ by

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

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

Observe that $\langle A\langle\langle\Sigma^*\rangle\rangle, +, \odot, 0, \mathrm{char}(\Sigma^*)\rangle$ and $\langle A\langle\langle\Sigma^*\rangle\rangle, +, \sqcup, 0, \varepsilon\rangle$ are semirings.

The <u>partial derivative</u> $r_z \in A\langle\langle\Sigma^*\rangle\rangle$ of a formal power series $r \in A\langle\langle\Sigma^*\rangle\rangle$ with respect to a symbol $z \in \Sigma$ is defined by

$$(r_z, w) = \sum_{w = w_1 w_2} (r, w_1 z w_2).$$

2. CONVERGENCE AND EQUATIONS.

We now give an axiomatic definition for the notion of convergence of a special type. The notion is particularly suitable for handling equations arising in automata theory. It also gives rise to some important identities needed later on.

A mapping $\alpha:\mathbb{N}\to A$ is called a sequence in A. By $A^{\mathbb{N}}$ we denote the set of all such sequences. If $\alpha\in A^{\mathbb{N}}$ then we use the notation $\alpha=(\alpha(n))$.

We denote by o and η the sequences defined by $o(n)=0$ and $\eta(n)=1$, for all $n\geq 0$, respectively. For $\alpha\in A^{\mathbb{N}}$, $c\in A$, we define $c\alpha$ and αc in $A^{\mathbb{N}}$ by $(c\alpha)(n)=c\alpha(n)$ and $(\alpha c)(n)=\alpha(n)c$, for all $n\geq 0$, respectively. For $\alpha_1,\alpha_2\in A^{\mathbb{N}}$, we define $\alpha_1+\alpha_2$ and $\alpha_1\cdot\alpha_2$ in $A^{\mathbb{N}}$ by $(\alpha_1+\alpha_2)(n)=\alpha_1(n)+\alpha_2(n)$ and $(\alpha_1\cdot\alpha_2)(n)=\alpha_1(n)\alpha_2(n)$, for all $n\geq 0$, respectively.

Observe that $\langle A^{\mathbb{N}},+,\cdot,o,\eta\rangle$ is a semiring. We need one further operation before giving the basic definitions of convergence.

Consider $\alpha\in A^{\mathbb{N}}$ and $a\in A$. Then $\alpha_a\in A^{\mathbb{N}}$ denotes the sequence defined by

$$\alpha_a(0)=a,\quad \alpha_a(n+1)=\alpha(n),\ \text{for all } n\geq 0.$$

Each set $D\subseteq A^{\mathbb{N}}$ satisfying the following conditions (D1)-(D3) is called a set of convergent sequences in A.

(D1) $\eta\in D$.

(D2) (i) If $\alpha_1,\alpha_2\in D$ then $\alpha_1+\alpha_2\in D$.

(ii) If $\alpha\in D$ and $c\in A$ then $c\alpha,\alpha c\in D$.

(D3) If $\alpha\in D$ and $a\in A$ then $\alpha_a\in D$.

Let D be a set of convergent sequences in A. A mapping $\lim:D\to A$ satisfying the following conditions (lim 1)-(lim 3) is called a limit function (on D).

(lim 1) $\lim\eta=1$.

(lim 2) (i) If $\alpha_1,\alpha_2\in D$ then $\lim(\alpha_1+\alpha_2)=\lim\alpha_1+\lim\alpha_2$.

(ii) If $\alpha\in D$ and $c\in A$ then $\lim c\alpha=c\lim\alpha$ and $\lim\alpha c=(\lim\alpha)c$.

(lim 3) If $\alpha\in D$ and $a\in A$ then $\lim\alpha_a=\lim\alpha$.

Observe that, for all $c\in A$, the sequence $c\eta=\eta c$ is convergent independently of D and converges to c.

In what follows we often use the terms "convergence in A" and "limit in A" without explicitly specifying D and lim. Sets of convergent sequences will be considered only in the case that a limit function is defined. We also use the notation $\lim_{n\to\alpha} \alpha(n)$ for $\lim \alpha$.

A notion of convergence definable for every A, referred to as discrete convergence, will now be discussed. This notion of convergence is the classical one considered in connection with semirings and will also be the most important one needed in the sequel.

The set of convergent sequences D_d is the set of ultimately constant sequences. Here, a sequence α is ultimately constant iff there exists an $n_\alpha \geq 0$ such that for all $k \geq 0$

$$\alpha(n_\alpha+k)=\alpha(n_\alpha).$$

The value of the limit function $\lim_d$ on D_d for such an ultimately constant sequence is $\alpha(n_\alpha)$.

Each set of convergent sequences D has to contain D_d, i.e., D_d is the smallest set of sequences for which (D1)-(D3) holds. Furthermore, if lim is a limit function on D, then $\lim \alpha = \lim_d \alpha$ for all $\alpha \in D_d$.

Hence, the discrete convergence is the only notion of convergence if the set of convergent sequences is given by D_d. It is a notion of convergence in all semirings.

The following two examples show that our notion of limit is compatible with the customary ones.

Example 2.1. A sequence $\alpha \in \mathbb{R}^{\mathbb{N}}$ is called a Cauchy sequence iff for all $\varepsilon > 0$, there exists an $n_\varepsilon \geq 0$ such that $|\alpha(n_1)-\alpha(n_2)| < \varepsilon$ holds for all $n_1, n_2 \geq n_\varepsilon$.

One possible choice for the set D of convergent sequences in $\mathbb{R}$ is the set of Cauchy sequences with the usual convergence in $\mathbb{R}$. This notion of convergence in $\mathbb{R}$ is called the Cauchy convergence. □

Example 2.2. A sequence $\alpha \in \mathbb{R}^{\mathbb{N}}$ is called an Euler sequence iff the sequence $\left(\sum_{j=0}^{n} \binom{n}{j} \alpha(j)/2^n \right)$ is a Cauchy sequence.

One possible choice for the set D of convergent sequences in $\mathbb{R}$ is the set of Euler sequences with the following notion of convergence:

$\lim_E \alpha = \lim_{n\to\infty} \sum_{j=0}^{n} \binom{n}{j} \alpha(j)/2^n$, where the limit on the right side denotes the Cauchy convergence.

This notion of convergence in $\mathbb{R}$ is called the Euler convergence. It can be shown that, for all $a\in\mathbb{R}$, with $-3<a<1$ $\lim_E \sum_{j=0}^{n} a^j = 1/(1-a)$ and $\lim_{n\to\infty E} a^n = 0$.

Let $a=-1$. Then $1,-1,1,-1,\ldots$ converges to 0 and $1,0,1,0,\ldots$ converges to $\frac{1}{2}$. □

In the next example a somewhat unusual notion of convergence will be considered. The notion is connected with the important concept of a quasi-inverse discussed below.

Example 2.3. Consider the set D of sequences in $\mathbb{R}$, generated by (D2) and (D3) from the sequences (a^n), where a is in $\mathbb{R}$.

Then it is easily seen that D forms a set of convergent sequences and, furthermore, $\alpha\in D$ iff there exist $n_\alpha \geq 0$ and $\ell \geq 1$ such that, for all $k\geq 0$

$$\alpha(n_\alpha+k) = \sum_{j=1}^{\ell} c_j a_j^k + b, \quad c_j, a_j, b\in\mathbb{R},$$

$a_i \neq a_j$ for $i\neq j$ and $a_j \neq 1$, where $1\leq i, j\leq \ell$.

It is easy to see, either directly or using the Vandermonde determinant, that

$\sum_{j=1}^{\ell} c_j a_j^k + b = 0$ for all $k\geq 0$ implies $c_j = 0$, $1\leq j\leq \ell$, and $b=0$.

Hence, if we define $\lim: D\to\mathbb{R}$ by $\lim \alpha = b$ for $\alpha(n_\alpha+k) = \sum_{j=1}^{\ell} c_j a_j^k + b$, then lim is a welldefined mapping and it is easily seen that lim is a limit function in $\mathbb{R}$.

We note that $\lim_{n\to\infty} \sum_{j=0}^{n} a^j = \lim_{n\to\infty}(1-a^{n+1})/(1-a) =$

$1/(1-a) - a \lim_{n\to\infty} a^n/(1-a) = 1/(1-a)$ for $a\neq 1$. □

The powers a^i, $i\geq 0$, of an element a in a semiring A are defined in

the natural way, whereby $a^0=1$.

If $(\sum_{j=1}^{n} a^j)\in D$ then we write

$$\lim_{n\to\infty} \sum_{j=1}^{n} a^j=a^+$$

and call it the quasi-inverse of a (with respect to the given notion of convergence). If $(\sum_{j=0}^{n} a^j)\in D$ then we write

$$\lim_{n\to\infty} \sum_{j=0}^{n} a^j=a^*$$

and call it the star of a (with respect to the given notion of convergence).

(For n=0 the range of j is empty in the sum defining a^+. In this case we consider the sum to be equal to 0.)

The next theorem shows the close interconnection between a^+ and a^*.

Theorem 2.1. Let $a\in A$. Then a^* exists iff a^+ exists, and $1+a^+=a^*$, $aa^*=a^*a=a^+$.

Proof. Let a^+ exist. Then $1+a^+=\lim\, \eta+\lim(\sum_{j=1}^{n} a^j)=\lim(\eta+(\sum_{j=1}^{n} a^j))=$ $\lim_{n\to\infty} \sum_{j=0}^{n} a^j=a^*$. Hence a^* exists.

Let a^* exist. Then $aa^*=a \lim_{n\to\infty} \sum_{j=0}^{n} a^j=\lim_{n\to\infty} \sum_{j=1}^{n+1} a^j=\lim_{n\to\infty} \sum_{j=1}^{n} a^j=a^+$. Hence a^+ exists. Obviously $aa^*=a^*a$. □

Corollary 2.2. If a^* exists then

$$a^*=\sum_{j=0}^{n} a^j+a^{n+1}a^*, \text{ and}$$

$$a^*=\sum_{j=0}^{n} a^j+a^*a^{n+1}, \text{ for all } n\geq 0.$$ □

We now consider equations of the form

$$y=ay+b,\ a,b\in A, \qquad (1)$$

where y is a variable. An element $s\in A$ is called a solution of (1) iff $s=as+b$.

Theorem 2.3. If a^* exists then $s=a^*b$ is a solution of (1).

Proof. By Corollary 2.2, we have $a^*=aa^*+1$. Multiplying by b gives $a^*b=aa^*b+b$, which shows that this a^*b is a solution of (1). □

The next theorem gives a sufficient condition for the uniqueness of the solution.

Theorem 2.4. If a^* exists and $\lim_{n\to\infty} a^n=0$ then $s=a^*b$ is the unique solution of (1).

Proof. By Theorem 2.3, s is a solution of (1). Assume $t\in A$ is a solution of (1). Then

$$t=at+b=a^2t+ab+b=\ldots=a^{n+1}t+\sum_{j=0}^{n} a^jb$$

holds for all $n\geq 0$.

Since $\lim_{n\to\infty} a^n=0$, we have

$$a \lim_{n\to\infty} a^n=\lim_{n\to\infty} a^{n+1}=0.$$

Furthermore, $a^{n+1}t+\sum_{j=0}^{n} a^jb=t$ implies $(a^{n+1})t+(\sum_{j=0}^{n} a^j)b=nt$. Hence, by (lim 1)-(lim 3),

$$(\lim_{n\to\infty} a^{n+1})t+(\lim_{n\to\infty} \sum_{j=0}^{n} a^j)b=a^*b=t. \qquad \square$$

example{} endexample

Example 2.4. Let $y=ay+1$, $-3<a<1$. We work with the Euler convergence. Then $\lim_{n\to\infty} a^n=0$ and $a^*=1/(1-a)$. Hence, the unique solution of $y=ay+1$ is $1/(1-a)$. $\square$

We now continue Example 2.3. Recall that, for $a\neq 1$, $\lim_{n\to\infty} a^n=0$, a^* exists and $a^*=1/(1-a)$. This implies that the equation $y=ay+1$, $a\neq 1$, has the unique solution $s=1/(1-a)$.

We now turn to the discussion of some important identities. The letter a, with or without subscripts, stands for an element of A.

Theorem 2.5. $(a_1a_2)^*$ exists iff $(a_2a_1)^*$ exists. Whenever $(a_1a_2)^*$ exists then $(a_1a_2)^*a_1=a_1(a_2a_1)^*$.

Proof. To prove the first sentence, it suffices to show that the existence of $(a_1a_2)^*$ implies the existence of $(a_2a_1)^*$. Assume that $(a_1a_2)^*$ exists. Then

$$(\sum_{j=0}^{n-1}(a_1a_2)^j)\in D \text{ and } n+(a_2\sum_{j=0}^{n-1}(a_1a_2)^ja_1)=(\sum_{j=0}^{n}(a_2a_1)^j)\in D$$

The second sentence of the theorem follows because

$$(a_1a_2)^*a_1=\lim_{n\to\infty}\sum_{j=0}^{n}(a_1a_2)^ja_1=\lim_{n\to\infty}a_1\sum_{j=0}^{n}(a_2a_1)^j=a_1(a_2a_1)^*. \qquad \square$$

Theorem 2.6. Assume the existence of $(a_1+a_2)^*$, a_1^* and $(a_2a_1^*)^*$ and, furthermore, that

$$\lim_{n\to\infty}(a_1+a_2)^n=0.$$

Then

$$(a_1+a_2)^*=a_1^*(a_2a_1^*)^*=(a_1^*a_2)^*a_1^*.$$

Proof. We first show that $a_1^*(a_2a_1^*)^*$ is a solution of the equation $y=(a_1+a_2)y+1$:

$$(a_1+a_2)a_1^*(a_2a_1^*)^*+1=a_1^+(a_2a_1^*)^*+a_2a_1^*(a_2a_1^*)^*+1=a_1^+(a_2a_1^*)^*+(a_2a_1^*)^*=a_1^*(a_2a_1^*)^*.$$

By our assumption and Theorem 2.4, the solution obtained is unique. Our theorem now follows by Theorem 2.5.

We again continue Example 2.3. Assume that $a_1\neq1$, $a_2\neq1$, $a_1+a_2\neq1$. Then

$$a_1^*=1/(1-a_1),$$

$$(a_1^*a_2)^*a_1^*=(1/(1-a_2/(1-a_1)))/(1-a_1)=1/(1-(a_1+a_2))=(a_1+a_2)^*. \qquad \square$$

Theorem 2.7. Assume the existence of $(a_1+a_2)^*$, a_1^* and $(a_1+a_2a_1^*a_2)^*$ and, furthermore, that

$$\lim_{n\to\infty}a_1^n=\lim_{n\to\infty}(a_1+a_2a_1^*a_2)^n=0.$$

Then

$$(a_1+a_2)^*=(a_1+a_2a_1^*a_2)^*(1+a_2a_1^*).$$

Proof. By Corollary 2.2, we have

$$(a_1+a_2)^*=a_1(a_1+a_2)^*+a_2(a_1+a_2)^*+1.$$

Hence, by our assumption and Theorem 2.4, the unique solution of the equation

$$y=a_1y+a_2(a_1+a_2)^*+1$$

equals $(a_1+a_2)^*$. By Theorem 2.3 and our assumption, another representation of the unique solution is $a_1^*a_2(a_1+a_2)^*+a_1^*$. Substituting $a_1^*a_2(a_1+a_2)^*+a_1^*$ for the third occurrence of $(a_1+a_2)^*$ in the first equality of the proof yields

$$(a_1+a_2)^*=(a_1+a_2a_1^*a_2)(a_1+a_2)^*+a_2a_1^*+1.$$

This shows that $(a_1+a_2)^*$ is a solution of the equation

$$y=(a_1+a_2a_1^*a_2)y+a_2a_1^*+1.$$

By Theorem 2.4 and our assumption $\lim_{n\to\infty}(a_1+a_2a_1^*a_2)^n=0$, the solution is unique. By Theorem 2.3 and the existence of $(a_1+a_2a_1^*a_2)^*$, another representation for the unique solution is

$$(a_1+a_2a_1^*a_2)^*(1+a_2a_1^*).$$ □

We now show how a notion of convergence in A can be transferred to $A\langle\langle\Sigma^*\rangle\rangle$. The main idea is that a sequence of power series determines, for each w in Σ^*, a sequence of coefficients of w. The limits of the latter sequences determine the coefficients in the limit of our sequence of power series.

Observe first that $A^{\mathbb{N}}\langle\langle\Sigma^*\rangle\rangle$ and $(A\langle\langle\Sigma^*\rangle\rangle)^{\mathbb{N}}$ are isomorphic. Assume now that a convergence in A is given by D and lim. Then a convergence in $A\langle\langle\Sigma^*\rangle\rangle$ is given by $D\langle\langle\Sigma^*\rangle\rangle$ and lim', where

$$\lim'\ \alpha = \sum_{w\in\Sigma^*}\lim(\alpha,w)w,\quad \alpha\in D\langle\langle\Sigma^*\rangle\rangle.$$

The concept of a quasiregular power series will be very important in the sequel. A power series r of $A\langle\langle\Sigma^*\rangle\rangle$ is termed <u>quasiregular</u> iff $(r,\varepsilon)=0$. Our next theorem shows that the star of a quasiregular power series always exists. Moreover, the star does not depend on the used notion of convergence.

<u>Theorem 2.8.</u> If $r\in A\langle\langle\Sigma^*\rangle\rangle$ is quasiregular then $\lim_{n\to\infty} r^n=0$ and r^* exists.

<u>Proof.</u> We consider first $\lim_{n\to\infty} r^n$ and r^* with respect to the discrete convergence in A. Since $(r,\varepsilon)=0$, by induction on $|w|$ we infer the

$$(r^n,w)=0 \text{ for all } n>|w|,\ w\in\Sigma^*.$$

This implies

$$\lim_{n\to\infty} r^n=0.$$

Furthermore, we have

$$\sum_{j=0}^{|w|+k}(r^j,w)=\sum_{j=0}^{|w|}(r^j,w) \text{ for all } k\geq 0,\ w\in\Sigma^*.$$

Hence,

$$(r^*,w)=(\lim_{n\to\infty}\sum_{j=0}^{n} r^j,w)=(\sum_{j=0}^{|w|} r^j,w)$$

for all $w\in\Sigma^*$, and r^* exists with respect to the discrete convergence. By the observations made above, these equalities remain valid for an

arbitrary convergence. □

Corollary 2.9. If $r \in A\langle\langle \Sigma^* \rangle\rangle$ is quasiregular then

$$r^* = \sum_{w \in \Sigma^*} \left(\sum_{j=0}^{|w|} r^j, w \right) w. \qquad \square$$

We now introduce the notion of a strong convergence. This notion is particularly suitable for handling power series. In view of Theorem 2.4, the existence of the star of r and the convergence of r^n to 0 are of great importance for a power series r. Strong convergence in A and the convergence of $(r,\varepsilon)^n$ to 0 guarantee these two important properties for a power series r.

A convergence in A is called strong iff the condition

$\left(\sum_{j=0}^{n} a^j \alpha(n-j) \right) \in D$ is satisfied for each $\alpha \in D$ and each $a \in A$ such that $(a^n) \in D$ and $\lim_{n \to \infty} a^n = 0$.

Theorem 2.10. Assume that a strong convergence has been defined in A. Furthermore, assume that $(a^n) \in D$ and $\lim_{n \to \infty} a^n = 0$. Then a^* exists and, whenever $\alpha \in D$, then

$$\lim_{n \to \infty} \sum_{j=0}^{n} a^j \alpha(n-j) = a^* \lim \alpha.$$

Proof. Since η is a convergent sequence, the sequence

$\left(\sum_{j=0}^{n} a^j \eta(n-j) \right) = \left(\sum_{j=0}^{n} a^j \right)$ is again convergent by the definition of a strong convergence in A. This shows the existence of a^*.

Assume now that α is a convergent sequence and denote

$$\lim_{n \to \infty} \sum_{j=0}^{n} a^j \alpha(n-j) = b.$$

By (D2), (lim 2) and (D3), (lim 3) the equality

$$\sum_{j=0}^{n} a^j \alpha(n-j) = \alpha(n) + a \sum_{j=0}^{n-1} a^j \alpha(n-1-j)$$

implies that

$$b = \lim \alpha + ab.$$

Hence, by Theorem 2.4, b is the unique solution $a^* \lim \alpha$ of the equation $y = ay + \lim \alpha$. □

Theorem 2.10 shows that a convergence in A being strong means that

$$\lim_{n\to\infty} a^n=0$$

implies

$$\lim_{n\to\infty} \sum_{j=0}^{n} a^j\alpha(n-j)=a^*\lim_{n\to\infty} \alpha(n),$$

provided $\lim_{n\to\infty} \alpha(n)$ exists.

Our next example shows that a notion of strong convergence is definable for every semiring A. It is, of course, the discrete convergence.

Example 2.5. Consider the discrete convergence in A.

For notational convenience we denote D_d and $\lim_d$ by D and lim, respectively. Consider an a in A such that $(a^n)\in D$ and $\lim_{n\to\infty} a^n=0$. By the definition of D and lim this means the existence of an $n_0\geq 1$ such that, for all $k\geq 0$,

$$a^{n_0+k}=0. \tag{2}$$

Hence, we have that

$$a^*=\sum_{j=0}^{n_0-1} a^j. \tag{3}$$

Furthermore, consider a sequence α in D. This means the existence of an $n_\alpha\geq 0$ such that, for all $k\geq 0$,

$$\alpha(n_\alpha)=\alpha(n_\alpha+k)$$

and

$$\lim_{n\to\infty} \alpha(n)=\alpha(n_\alpha).$$

We have to show that the sequence

$$\beta(n)=\sum_{j=0}^{n} a^j\alpha(n-j)$$

is a convergent sequence. Define $n_\beta=n_0+n_\alpha-1$.

Then, for all $k\geq 0$, we have that

$$\beta(n_\beta+k)=\sum_{j=0}^{n_0+n_\alpha+k-1} a^j\alpha(n_0+n_\alpha+k-j-1)=$$

$$=\sum_{j=0}^{n_0-1} a^j\alpha(n_0+n_\alpha+k-j-1)=\sum_{j=0}^{n_0-1} a^j\alpha(n_\alpha)=a^*\alpha(n_\alpha).$$

Indeed, the first equality follows by the definition of β and n_β, the second equality by (2), the third equality by the observation that $n_0+n_\alpha+k-j-1 \geq n_\alpha+k$ for $0 \leq j \leq n_0-1$, and the last equality by (3). Hence, β is a convergent sequence.

By the definition of lim, we infer that

$$\lim_{n\to\infty} \beta(n) = a^* \alpha(n_\alpha) = a^* \lim_{n\to\infty} \alpha(n). \qquad \square$$

For the next theorem we assume strong convergence in A. It is stated without proof.

Theorem 2.11. Assume that r is a power series in $A\langle\langle \Sigma^* \rangle\rangle$ such that $\lim_{n\to\infty} (r,\varepsilon)^n = 0$. Then $\lim_{n\to\infty} r^n = 0$, r^* exists and, furthermore,

$$(r^*,w) = \sum_{\substack{uv=w \\ u\neq\varepsilon}} (r^*,\varepsilon)(r,u)(r^*,v)$$

holds for all $w \in \Sigma^+$. $\square$

The following two examples show that the Cauchy convergence and the Euler convergence are strong.

Example 2.6. We consider the Cauchy convergence introduced in Example 2.1.

The Theorem of Mertens states that, if $\sum_{n=0}^{\infty} a_n$ is absolutely convergent and $\sum_{n=0}^{\infty} b_n$ is convergent then $\sum_{n=0}^{\infty} \sum_{j=0}^{n} a_j b_{n-j} = \sum_{n=0}^{\infty} a_n \sum_{m=0}^{\infty} b_m$.

Consider an $a \in \mathbb{R}$ with $|a|<1$. Then (a^n) converges to 0 and, furthermore, $(\sum_{j=0}^{\infty} a^j)$ converges absolutely to $a^*=1/(1-a)$. Let α be a convergent sequence and define

$$\beta(0)=\alpha(0), \quad \beta(j)=\alpha(j)-\alpha(j-1) \text{ for } j \geq 1.$$

Then $\sum_{j=0}^{n} \beta(j) = \alpha(n)$ and $(\sum_{j=0}^{n} \beta(j))$ is a convergent sequence with

$$\lim_{n\to\infty} \sum_{j=0}^{n} \beta(j) = \lim_{n\to\infty} \alpha(n).$$

Hence, by the Theorem of Mertens, the sequence

$$\left(\sum_{k=0}^{n}\sum_{j=0}^{k} a^j\,\beta(k-j)\right)$$

is a convergent sequence with limit

$$a^* \lim_{n\to\infty} \alpha(n).$$

Furthermore,

$$\sum_{k=0}^{n}\sum_{j=0}^{k} a^j\,\beta(k-j) =$$

$$\sum_{k=1}^{n}\sum_{j=0}^{k-1} a^j(\alpha(k-j)-\alpha(k-j-1)) + \sum_{k=0}^{n} a^k\,\alpha(0) =$$

$$\sum_{k=1}^{n}\sum_{j=0}^{k-1} a^j\,\alpha(k-j) - \sum_{k=0}^{n-1}\sum_{j=0}^{k} a^j\,\alpha(k-j) + \sum_{k=1}^{n} a^k\,\alpha(0) + \alpha(0) =$$

$$\sum_{k=1}^{n}\sum_{j=0}^{k} a^j\,\alpha(k-j) - \sum_{k=0}^{n-1}\sum_{j=0}^{k} a^j\,\alpha(k-j) + \alpha(0) = \sum_{j=0}^{n} a^j\,\alpha(n-j).$$

Here the first equality follows by the definition of β, the second equality by changing in the second term of the right side the index k to $k+1$, the third equality by adding the first and third term of its left side and the last equality simply by addition.

Hence, we have that

$$\lim_{n\to\infty}\sum_{j=0}^{n} a^j\,\alpha(n-j) = \lim_{n\to\infty}\sum_{k=0}^{n}\sum_{j=0}^{k} a^j\,\beta(k-j) = a^* \lim_{n\to\infty}\alpha(n).$$

If $a \in \mathbb{R}$ with $|a|>1$ or $a = -1$, then (a^n) is not a convergent sequence. If $a=1$, then (a^n) converges, but $\lim_{n\to\infty} a^n=1\neq 0$. This implies that the Cauchy convergence is strong. □

Example 2.7. We consider the Euler convergence introduced in Example 2.2. Using a theorem similar to the Theorem of Mertens, we may conclude as above that the Euler convergence is strong. □

Example 2.8. We consider the convergence introduced in Example 2.3. Let $a \in \mathbb{R}$ with $a\neq 1$ and define the sequence $\alpha(n)=a^n$, $n\geq 0$. Then α is a convergent sequence. Since

$$\sum_{j=0}^{n} a^j \alpha(n-j) = (n+1)a^n$$

and $((n+1)a^n)$ is not a convergent sequence, we conclude that the considered convergence is not a strong convergence. □

Theorem 2.11 shows that, in case of a strong convergence, the coefficient of ε has a great influence on the convergence behavior of a power series. The definition of a cycle-free power series is now clear: a power series r is called cycle-free (with respect to the given notion of strong convergence) iff $\lim_{n\to\infty}(r,\varepsilon)^n=0$.

Theorem 2.12. For each cycle-free power series r, $\lim_{n\to\infty} r^n=0$ and r^* exists.

Proof. By Theorem 2.11. □

Example 2.9. Consider $\mathbb{R}\langle\langle\Sigma^*\rangle\rangle$. Then we know three strong convergences in $\mathbb{R}$ and, hence, three types of cycle-freeness of power series.

A power series r is cycle-free with respect to the discrete convergence iff $(r,\varepsilon)=0$, i.e., if r is quasiregular. A power series r is cycle-free with respect to the Cauchy convergence iff $|(r,\varepsilon)|<1$. And a power series r is cycle-free with respect to the Euler convergence iff $-3<(r,\varepsilon)<1$. □

By Example 2.9, the question arises whether a power series cycle-free with respect to different notions of strong convergence may have different stars. The next theorem shows that this is not the case.

Theorem 2.13. Assume that a power series r is cycle-free, possibly with respect to different notions of strong convergence. Then r^* is independent of the notion of strong convergence.

Proof. By Theorem 2.12, $\lim_{n\to\infty} r^n=0$ and $\lim_{n\to\infty} \sum_{j=0}^{n} r^j=r^*$ exist with respect to any of the notions of strong convergence considered. Since the equation $y=ry+\varepsilon$, ε and r in $A\langle\langle\Sigma^*\rangle\rangle$, has, by Theorem 2.4, the unique solution r^*, the star of r is independent of the convergence used. □

This means that it depends on the notion of the strong convergence considered, whether a power series r is cycle-free or not. But if r is cycle-free then r^* is uniquely determined.

We transfer the term cycle-free to equations. An equation

$$y=ry+s,\quad r,s\in A\langle\langle\Sigma^*\rangle\rangle, \tag{4}$$

is termed cycle-free iff r is cycle-free.

Theorem 2.14. Every cycle-free equation (4) has the unique solution r^*s.

Proof. Since r is cycle-free. Theorem 2.12 implies that $\lim_{n\to\infty} r^n=0$ and, furthermore, the existence of r^*.

By Theorem 2.4, (4) has the unique solution r^*s. □

Consider a power series r in $A\langle\langle\Sigma^*\rangle\rangle$. The power series $r_0=(r,\varepsilon)\varepsilon$ is called the ε-part and $r_1=\sum_{w\in\Sigma^+}(r,w)w$ is called the quasiregular part of r.

Theorem 2.15. For each cycle-free power series r,

$$r^*=r_0^*(r_1r_0^*)^*=(r_0^*r_1)^*r_0^*.$$

Proof. Since $r=r_0+r_1$ is cycle-free, $(r_0+r_1)^*$ exists and $\lim_{n\to\infty}(r_0+r_1)^n=0$. Since we use a strong convergence, $\lim_{n\to\infty} r_0^n=0$ implies the existence of r_0^*. Since $r_1r_0^*$ is quasiregular, $r_1r_0^*$ is cycle-free and $(r_1r_0^*)^*$ exists.

Hence, Theorem 2.6 implies our theorem. □

Theorem 2.15 is extremely useful for the computation of the star of a power series.

Example 2.9. Consider the power series $r=a\varepsilon+bx$ in $\mathbb{R}\langle\langle x^*\rangle\rangle$ with $-3<a<1$. We work with the Euler convergence. Then r is cycle-free and

$$r^*=(a^*bx)^*a^*.$$

Hence,

$$r^*=\left(\frac{b}{1-a}\,x\right)^*\frac{1}{1-a}=\sum_{j=0}^{\infty}\frac{b^j}{(1-a)^{j+1}}\,x^j.$$

Furthermore, r^* is the unique solution of the equation

$$y=(a\varepsilon+bx)y+\varepsilon.$$

□

3. MATRICES AND AUTOMATA.

We now introduce matrices and vectors with entries in a semiring and indexed by countable index sets. Automata are then defined in terms of matrices.

Consider two nonempty countable index sets I and I'. Mappings M of IxI' into A are called matrices. The values of M are denoted by $M_{i,i'}$ where $i\in I$ and $i'\in I'$. The values $M_{i,i'}$ are also referred to as the entries of the matrix. In particular, $M_{i,i'}$ is called the (i,i')-entry of M. The collection of all matrices M as defined above is denoted by $A^{IxI'}$.

If I or I' is a singleton, M is called a row or column vector, respectively. If I is finite and equals $\{1,\ldots,n\}$ or I' is finite and equals $\{1,\ldots,m\}$ then $A^{IxI'}$ is also denoted by $A^{nxI'}$ or A^{Ixm}, respectively. If both, I and I' are finite, then M is called a finite matrix.

For each $i\in I$, consider the set of indices $R(i)=\{i' \mid M_{i,i'}\neq 0\}$. Then M is called a row finite matrix iff R(i) is finite for all $i\in I$. Similarly, consider the set $C(i')=\{i \mid M_{i,i'}\neq 0\}$ for $i'\in I'$. Then M is called a column finite matrix iff C(i') is finite for all $i'\in I'$.

The collection of all matrices that are both row and column finite as defined above is denoted by $A_J^{IxI'}$.

Unless stated otherwise, the letter I (resp. Q), possibly provided with indices, will denote in the sequel a countable (resp. finite) nonempty index set.

We introduce some operations and special matrices inducing a monoid or semiring structure to matrices. For $M_1,M_2\in A^{IxI'}$ we define the sum $M_1+M_2\in A^{IxI'}$ by

$(M_1+M_2)_{i,i'}=(M_1)_{i,i'}+(M_2)_{i,i'}$ for all $i\in I$, $i'\in I'$.

Furthermore, we introduce the zero matrix $0\in A^{IxI'}$. All the entries of 0 are 0. By the definition of the sum and the zero matrix, $\langle A^{IxI'},+,0\rangle$ and $\langle A_J^{IxI'},+,0\rangle$ are commutative monoids.

For $M_1\in A^{I_1xI_2}$ and $M_2\in A^{I_2xI_3}$, where M_1 is row finite or M_2 is column finite, we define the product $M_1M_2\in A^{I_1xI_3}$ by

$(M_1M_2)_{i_1,i_3} = \sum_{i_2 \in I_2} (M_1)_{i_1,i_2} (M_2)_{i_2,i_3}$ for all $i_1 \in I_1$, $i_3 \in I_3$.

If M_1 is row (resp. M_2 is column) finite then the range of the variable i_2 in the sum is, in fact, $R(i_1)$ (resp. $C(i_3)$). Hence, in both cases, the range of the variable i_2 is finite and M_1M_2 is welldefined. Furthermore, we introduce the <u>matrix of unity</u> $E \in A^{I \times I}$, where $E_{i_1,i_2} = \delta_{i_1,i_2}$ for all $i_1,i_2 \in I$. Clearly, $\langle A_J^{I \times I}, +, \cdot, 0, E \rangle$ is a semiring.

In the sequel we will need some isomorphisms between semirings of matrices. The semirings $(A^{Q \times Q})_J^{I \times I}$, $A_J^{(I \times Q) \times (I \times Q)}$, $A_J^{(Q \times I) \times (Q \times I)}$ and $(A_J^{I \times I})^{Q \times Q}$ are isomorphic by the correspondence

$$((M_1)_{i_1,i_2})_{q_1,q_2} = (M_2)_{(i_1,q_1),(i_2,q_2)} = (M_3)_{(q_1,i_1),(q_2,i_2)} =$$
$$((M_4)_{q_1,q_2})_{i_1,i_2}, \quad i_1,i_2 \in I, \ q_1,q_2 \in Q.$$

Moreover, there are certain isomorphisms between the semirings $A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$ (that are formal power series whose coefficients are matrices) and $(A \langle\langle \Sigma^* \rangle\rangle)_J^{I \times I}$ (that are matrices whose entries are formal power series): There exists a subsemiring of $A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$ isomorphic to $(A \langle\langle \Sigma^* \rangle\rangle)_J^{I \times I}$ and there exists a subset of $(A \langle\langle \Sigma^* \rangle\rangle)^{I \times I}$ that is a semiring isomorphic to $A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$. Both isomorphisms are due to the correspondence $(M_1,w)_{i_1,i_2} = ((M_2)_{i_1,i_2},w)$, $i_1,i_2 \in I$, $w \in \Sigma^*$. Hence, for $M \in A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$ we may use the notation (M_{i_1,i_2},w) and for $M \in (A \langle\langle \Sigma^* \rangle\rangle)_J^{I \times I}$ we may use the notation $(M,w)_{i_1,i_2}$.

All limits (especially the star) are taken in $A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$ and all definitions valid for (ordinary) formal power series are valid also for matrices in $(A \langle\langle \Sigma^* \rangle\rangle)_J^{I \times I}$. E.g., $M_2 \in (A \langle\langle \Sigma^* \rangle\rangle)_J^{I \times I}$ is cycle-free iff $\lim_{n \to \infty} (M_1,\varepsilon)^n = 0$ for the corresponding matrix $M_1 \in A_J^{I \times I} \langle\langle \Sigma^* \rangle\rangle$, i.e. iff there exists a $k \geq 1$ such that $(M_1,\varepsilon)^k = 0$.

We now introduce blocks of matrices.

Assume the existence of nonempty countable index sets J, J' and I_j, $I'_{j'}$ for $j \in J$, $j' \in J'$ such that $I = \bigcup_{j \in J} I_j$, $I' = \bigcup_{j' \in J'} I'_{j'}$ and $I_{j_1} \cap I_{j_2} = \emptyset$, $I'_{j'_1} \cap I'_{j'_2} = \emptyset$ for $j_1 \neq j_2$, $j'_1 \neq j'_2$. Consider a matrix M in $A^{I \times I'}$.

Then the restricted mapping

$$M:I_j \times I'_j, \to A$$

is a matrix in $A^{I_j \times I'_j,}$ and is called the $(I_j, I'_j,)$-block of M. Consider now the matrices $M_1, M_2 \in A^{I \times I'}$ with blocks $M_t(I_j, I'_j,)$, $t=1,2$. Then the blocks of the sum of the matrices M_1 and M_2 can be expressed by the blocks of M_1 and M_2 in the usual way:

$$(M_1+M_2)(I_j, I'_j,) = M_1(I_j, I'_j,) + M_2(I_j, I'_j,).$$

Moreover, if M_1 is a matrix in the semiring $A_J^{I \times I}$ and M_2 is a matrix in $A_J^{I \times I'}$ then

$$(M_1 M_2)(I_{j_1}, I'_j,) = \sum_{j \in J} M_1(I_{j_1}, I_j) M_2(I_j, I'_j,).$$

In general, limits of sequences in $(A\langle\langle\Sigma^*\rangle\rangle)_J^{I \times I}$ are taken (isomorphically) in $A_J^{I \times I}\langle\langle\Sigma^*\rangle\rangle$ and the convergence in $A_J^{I \times I}$ is the discrete one.

In the next four theorems, we assume that I is partitioned into I_1 and I_2 and that M is a matrix in $A_J^{I \times I}\langle\langle\Sigma^*\rangle\rangle$. For notational convenience, we will denote $M(I_{j_1}, I_{j_2})$ by M_{j_1,j_2} for $1 \leq j_1, j_2 \leq 2$.

Theorem 3.1. Assume that M is cycle-free and, furthermore, that $M_{1,1}, M_{2,2}, M_{1,1}+M_{1,2}M_{2,2}^* M_{2,1}$ and $M_{2,2}+M_{2,1}M_{1,1}^* M_{1,2}$ are cycle-free.

Then

$$M^*(I_1, I_1) = (M_{1,1}+M_{1,2}M_{2,2}^* M_{2,1})^*,$$
$$M^*(I_1, I_2) = (M_{1,1}+M_{1,2}M_{2,2}^* M_{2,1})^* M_{1,2}M_{2,2}^*,$$
$$M^*(I_2, I_1) = (M_{2,2}+M_{2,1}M_{1,1}^* M_{1,2})^* M_{2,1}M_{1,1}^*,$$
$$M^*(I_2, I_2) = (M_{2,2}+M_{2,1}M_{1,1}^* M_{1,2})^*.$$

Proof. Consider the matrices

$$M_1 = \begin{pmatrix} M_{1,1} & 0 \\ 0 & M_{2,2} \end{pmatrix} \quad \text{and} \quad M_2 = \begin{pmatrix} 0 & M_{1,2} \\ M_{2,1} & 0 \end{pmatrix}.$$

The matrix M_1 is cycle-free. Hence, M_1^* exists and equals

$$\begin{pmatrix} M_{1,1}^* & O \\ O & M_{2,2}^* \end{pmatrix}.$$

This implies that

$$M_1+M_2M_1^*M_2 = \begin{pmatrix} M_{1,1}+M_{1,2}M_{2,2}^*M_{2,1} & O \\ O & M_{2,2}+M_{2,1}M_{1,1}^*M_{1,2} \end{pmatrix}.$$

Hence, by our assumptions we infer that $M_1+M_2M_1^*M_2$ is cycle-free. We are now in the position to apply Theorem 2.7 with $a_1=M_1$ and $a_2=M_2$. The computation of

$$(M_1+M_2M_1^*M_2)^*(E+M_2M_1^*)$$

proves the theorem. □

Theorem 3.2. Assume that $M_{1,1}$ and $M_{2,2}$ are cycle-free, and $M_{1,2}$ or $M_{2,1}$ is quasiregular.

Then M is cycle-free and

$M^*(I_1,I_1)=(M_{1,1}+M_{1,2}M_{2,2}^*M_{2,1})^*$,

$M^*(I_1,I_2)=(M_{1,1}+M_{1,2}M_{2,2}^*M_{2,1})^*M_{1,2}M_{2,2}^*$,

$M^*(I_2,I_1)=(M_{2,2}+M_{2,1}M_{1,1}^*M_{1,2})^*M_{2,1}M_{1,1}^*$,

$M^*(I_2,I_2)=(M_{2,2}+M_{2,1}M_{1,1}^*M_{1,2})^*$.

Proof. We only prove the case that $M_{2,1}$ is quasiregular. The proof of the other case is similar.

We claim that, for $k\geq 1$,

$$(M,\varepsilon)^k = \begin{pmatrix} (M_{1,1},\varepsilon)^k & \sum_{k_1+k_2=k-1} (M_{1,1},\varepsilon)^{k_1}(M_{1,2},\varepsilon)(M_{2,2},\varepsilon)^{k_2} \\ O & (M_{2,2},\varepsilon)^k \end{pmatrix}.$$

The proof is by induction on k.

Since $(M_{2,1},\varepsilon)=O$, the claim holds true for k=1.

If $k>1$,

$(M,\varepsilon)^k=(M,\varepsilon)(M,\varepsilon)^{k-1}=$

$$\begin{pmatrix} (M_{1,1},\varepsilon) & (M_{1,2},\varepsilon) \\ 0 & (M_{2,2},\varepsilon) \end{pmatrix} \begin{pmatrix} (M_{1,1},\varepsilon)^{k-1} & \sum_{k_1+k_2=k-1} (M_{1,1},\varepsilon)^{k_1}(M_{1,2},\varepsilon)(M_{2,2},\varepsilon)^{k_2} \\ 0 & (M_{2,2},\varepsilon)^{k-1} \end{pmatrix} =$$

$$\begin{pmatrix} (M_{1,1},\varepsilon)^{k} & \sum_{k_1+k_2=k-2} (M_{1,1},\varepsilon)^{k_1+1}(M_{1,2},\varepsilon)(M_{2,2},\varepsilon)^{k_2} + (M_{1,2},\varepsilon)(M_{2,2},\varepsilon)^{k-1} \\ 0 & (M_{2,2},\varepsilon)^{k} \end{pmatrix}.$$

Clearly, the last matrix obtained equals the right side of our claim.

Denote

$$M_1 = \begin{pmatrix} (M_{1,1},\varepsilon) & 0 \\ 0 & 0 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 0 & (M_{1,2},\varepsilon) \\ 0 & 0 \end{pmatrix},$$

$$M_3 = \begin{pmatrix} 0 & 0 \\ 0 & (M_{2,2},\varepsilon) \end{pmatrix}.$$

Since the discrete convergence in A_J^{IxI} is strong, we obtain

$$\lim_{n\to\infty} \sum_{k_1+k_2=n-1} M_1^{k_1} M_2 M_3^{k_2} = M_1^* M_2 \lim_{n\to\infty} M_2^{n-1} = 0.$$

This implies that M is cycle-free. Furthermore, $(M_{1,1}+M_{1,2}M_{2,2}^*M_{2,1},\varepsilon)=(M_{1,1},\varepsilon)$ and $(M_{2,2}+M_{2,1}M_{1,1}^*M_{1,2},\varepsilon)=(M_{2,2},\varepsilon)$. Hence, the conditions of Theorem 3.1 are satisfied and our theorem is proved. □

Theorem 3.3. Assume that $M_{1,1}$ and $M_{2,2}$ are cycle-free. Furthermore, assume that $M_{2,1}=0$. Then M is cycle-free and

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

Proof. By Theorem 3.2. □

Theorem 3.4. Assume that $M_{1,1}$ and $M_{2,2}$ are cycle-free. Furthermore, assume that $M_{1,2}=0$. Then M is cycle-free and

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

Proof. By Theorem 3.2. □

We now consider linear systems of the form

$$Y=MY+P,\ M\in A_J^{I\times I}\langle\langle\Sigma^*\rangle\rangle,\ P\in A_J^{I\times I'}\langle\langle\Sigma^*\rangle\rangle, \qquad (5)$$

where Y is a variable. A matrix $S\in A^{I\times I'}\langle\langle\Sigma^*\rangle\rangle$ is called a solution of (5) iff S=MS+P. The linear system (5) is called cycle-free iff M is cycle-free.

Theorem 3.5. Every cycle-free linear system (5) has the unique solution M^*P. □

As we will see below there is a close connection between linear systems and automata.

We need four operations on matrices which are used later on for automatatheoretic constructions: Kronecker product, Kronecker sum, Hadamard product and Hurwitz product.

(i) The Kronecker product of $M_1\in A^{I_1\times I_1'}$ and $M_2\in A^{I_2\times I_2'}$, denoted by $M_1\otimes M_2$, is the matrix in $A^{(I_1\times I_2)\times(I_1'\times I_2')}$ defined by

$$(M_1\otimes M_2)_{(i_1,i_2),(i_1',i_2')}=(M_1)_{i_1,i_1'}(M_2)_{i_2,i_2'}.$$

(ii) The Kronecker sum of $M_1\in A^{I_1\times I_1}$ and $M_2\in A^{I_2\times I_2}$, denoted by $M_1\oplus M_2$, is the matrix defined by

$$M_1\oplus M_2=M_1\otimes E_2+E_1\otimes M_2.$$

Here E_t is the matrix of unity in $A^{I_t\times I_t}$, t=1,2.

The Kronecker product and the Kronecker sum are easily extended to more structured semirings by isomorphism.

(iii) The Hadamard product of $M_1 \in A^{I_1 x I_1'}_{<<\Sigma_1^*>>}$ and $M_2 \in A^{I_2 x I_2'}_{<<\Sigma_2^*>>}$, denoted by $M_1 \odot M_2$, is the matrix defined by

$$M_1 \odot M_2 = \sum_{w \in (\Sigma_1 \cap \Sigma_2)^*} (M_1, w) \otimes (M_2, w) w.$$

(iv) The Hurwitz product of $M_1 \in A^{I_1 x I_1'}_{<<\Sigma^*>>}$ and $M_2 \in A^{I_2 x I_2'}_{<<\Sigma^*>>}$, denoted by $M_1 \sqcup\!\sqcup M_2$, is the matrix defined by

$$M_1 \sqcup\!\sqcup M_2 = \sum_{w_1 \in \Sigma^*} \sum_{w_2 \in \Sigma^*} (M_1, w_1) \otimes (M_2, w_2) w_1 \sqcup\!\sqcup w_2.$$

The next three theorems state the usual properties of the Kronecker product.

Theorem 3.6. Assume that, for $t=1,2$, $M_t, M_t' \in A^{I_t x I_t'}$. Then

$$(M_1 + M_1') \otimes M_2 = M_1 \otimes M_2 + M_1' \otimes M_2, \quad M_1 \otimes (M_2 + M_2') = M_1 \otimes M_2 + M_1 \otimes M_2',$$
$$M_1 \otimes O = O \text{ and } O \otimes M_2 = O.$$ □

Theorem 3.7. Assume that $M_t \in A^{I_t x I_t'}$, $t=1,2,3$. Then

$$M_1 \otimes (M_2 \otimes M_3) = (M_1 \otimes M_2) \otimes M_3.$$ □

Theorem 3.8. Let A be a commutative semiring. Assume that

$$M_1 \in A_J^{I_1 x I_2}, \quad M_2 \in A_J^{I_2 x I_3}, \quad M_3 \in A_J^{I_4 x I_5}{}_{<<\Sigma^*>>} \text{ and}$$
$$M_4 \in A_J^{I_5 x I_6}{}_{<<\Sigma^*>>}.$$

Then

$$(M_1 M_2) \otimes (M_3 M_4) = (M_1 \otimes M_3)(M_2 \otimes M_4).$$ □

The next two theorems give properties of the Hadamard product.

Theorem 3.9. Let A be a commutative semiring. Assume that

$$M_1 \in A_J^{I_1 x I_2}{}_{<\Sigma>}, \quad M_2 \in A_J^{I_2 x I_3}{}_{<<\Sigma^*>>}, \quad M_3 \in A_J^{I_4 x I_5}{}_{<\Sigma>} \text{ and}$$
$$M_4 \in A_J^{I_5 x I_6}{}_{<<\Sigma^*>>}.$$

Then

$$(M_1 M_2) \odot (M_3 M_4) = (M_1 \odot M_3)(M_2 \odot M_4).$$

Proof. $(M_1M_2)\odot(M_3M_4)=$

$$\sum_{x\in\Sigma}\sum_{w\in\Sigma^*}((M_1,x)(M_2,w)\otimes(M_3,x)(M_4,w))xw=$$

$$\sum_{x\in\Sigma}\sum_{w\in\Sigma^*}((M_1,x)\otimes(M_3,x))((M_2,w)\otimes(M_4,w))xw=(M_1\odot M_3)(M_2\odot M_4).$$

Here the second equality follows by Theorem 3.8. □

Theorem 3.10. Let A be a commutative semiring. Assume that

$$M_t\in A_J^{I_t\times I_t}\langle\langle\Sigma\rangle\rangle,\ t=1,2.$$

Then

$$(M_1\odot M_2)^*=M_1^*\odot M_2^*.$$

Proof. We show that $M_1^*\odot M_2^*$ is the solution of

$$Y=(M_1\odot M_2)Y+E_1\odot E_2$$

by

$$(M_1\odot M_2)(M_1^*\odot M_2^*)+E_1\odot E_2=(M_1M_1^*)\odot(M_2M_2^*)+E_1\odot E_2=M_1^+\odot M_2^+ +E_1\odot E_2=M_1^*\odot M_2^*.$$

Here the first equality follows by Theorem 3.9. Theorem 2.15 now proves Theorem 3.10. □

The next theorem, dealing with Kronecker sum and Hurwitz product, is proven in a similar manner.

Theorem 3.11. Let A be a commutative semiring. Assume that

$$M_t\in A_J^{I_t\times I_t}\langle\langle\Sigma\rangle\rangle,\ t=1,2.$$

Then

$$(M_1\oplus M_2)^*=M_1^*\sqcup\sqcup M_2^*.$$ □

We now introduce automata.

An A<<Σ^*>>-automaton

$$\mathcal{A}=(I,M,S,P)$$

is given by

(i) a countable set I of states,

(ii) a matrix $M\in(A\langle\langle\Sigma^*\rangle\rangle)_J^{I\times I}$ called the transition matrix,

(iii) $S\in(A\langle\langle\varepsilon\rangle\rangle)_J^{1\times I}$ called the initial state vector,

(iv) $P\in(A\langle\langle\varepsilon\rangle\rangle)_J^{I\times 1}$ called the final state vector.

If $M_{i,j}=r\neq 0$, $i,j\in I$, then we say that the edge (i,j) with the label r is in $\mathcal{A}$. A path c from i to j in $\mathcal{A}$ is a finite sequence of edges $(j_0,j_1),(j_1,j_2),\ldots,(j_{k-1},j_k)$, $i=j_0$, $j=j_k$, $k>0$. it is written $c:i\to j$. The integer k is called the length of the path and is denoted by $|c|$. If r_t is the label of (j_{t-1},j_t), $1\leq t\leq k$, then the label $\|c\|$ of the path c is defined be $\|c\|=r_1r_2\ldots r_k$.

For each state $i\in I$ we introduce the null path λ_i from i to i with $|\lambda_i|=0$ and $\|\lambda_i\|=\varepsilon$.

Assume that $c:i_1\to i_2$ and $d:i_2\to i_3$ are paths. Then the composition $cd:i_1\to i_3$ is defined by concatenation. We have $|cd|=|c|+|d|$ and $\|cd\|=\|c\|\,\|d\|$.

When it exists, the behavior $\|\mathcal{A}\|\in A\langle\langle\Sigma^*\rangle\rangle$ of an $A\langle\langle\Sigma^*\rangle\rangle$-automaton $\mathcal{A}=(I,M,S,P)$ is defined by

$$\|\mathcal{A}\| = SM^*P,$$

i.e., by the sum of the labels of all paths multiplied by the appropriate components of S and P:

$$\|\mathcal{A}\| = \sum_{i_1,i_2\in I} S_{i_1}\Big(\sum_{c:i_1\to i_2}\|c\|\Big)P_{i_2}.$$

An $A\langle\langle\Sigma^*\rangle\rangle$-automaton $\mathcal{A}=(I,M,S,P)$ is called cycle-free iff M is cycle-free.

Theorem 3.12. Let $\mathcal{A}=(I,M,S,P)$ be a cycle-free $A\langle\langle\Sigma^*\rangle\rangle$-automaton. Then

$$\|\mathcal{A}\| = SM^*P$$

is welldefined. □

Theorem 3.13. Let $\mathcal{A}=(I,M,S,P)$ be a cycle-free $A\langle\langle\Sigma^*\rangle\rangle$-automaton and consider the cycle-free linear system $Y=MY+P$.

Let T be its unique solution. Then

$$\|\mathcal{A}\| = ST.$$ □

If the entries of the transition matrix of an $A\langle\langle\Sigma^*\rangle\rangle$-automaton $\mathcal{A}$ are in $A\langle\Sigma\rangle$ or $A\langle\Sigma\cup\varepsilon\rangle$ then $\mathcal{A}$ is called $A\langle\Sigma\rangle$- or $A\langle\Sigma\cup\varepsilon\rangle$-automaton, respectively. If the set of states of an $A\langle\langle\Sigma^*\rangle\rangle$-automaton $\mathcal{A}$ is finite then $\mathcal{A}$ is called $A\langle\langle\Sigma^*\rangle\rangle$-finite-automaton.

Given $A\langle\Sigma\rangle$-automata $\mathcal{A}_j=(I_j,M_j,S_j,P_j)$, $j=1,2$, $I_1\cap I_2=\emptyset$, we construct

$A\langle\langle\Sigma\rangle\rangle$-automata $k\theta_1$, $k\in A$, $\theta_1+\theta_2$, $\theta_1\theta_2$, θ_1^+, $\theta_1\odot\theta_2$, $\theta_1 \sqcup \theta_2$ and $(\theta_1)_z$, $z\in\Sigma$. Their behavior will be as expected: $k\|\theta_1\|$, $\|\theta_1\|+\|\theta_2\|$, $\|\theta_1\|\cdot\|\theta_2\|$, $\|\theta_1\|^+$, $\|\theta_1\|\odot\|\theta_2\|$, $\|\theta_1\| \sqcup \|\theta_2\|$ and $\|\theta_1\|_z$. These automata-theoretic constructions will have combinatorial applications in the field of generating functions.

Construction 1. $k\theta_1=(I_1,M_1,kS_1,P_1)$. Clearly, we have

$$\|k\theta_1\| = k\|\theta_1\|. \qquad \square$$

Construction 2. $\theta_1+\theta_2=(I_1 \cup I_2,M,S,P)$, where

$$S=(S_1\ S_2),\quad M=\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix},\quad P=\begin{pmatrix} P_1 \\ P_2 \end{pmatrix}.$$

We have $\|\theta_1+\theta_2\| = SM^*P = S_1M_1^*P_1+S_2M_2^*P_2 = \|\theta_1\|+\|\theta_2\|$. $\square$

Construction 3. $\theta_1\theta_2=(I_1 \cup I_2,M,S,P)$, where

$$S=(S_1\ 0),\quad M=\begin{pmatrix} M_1 & P_1S_2M_2 \\ 0 & M_2 \end{pmatrix},\quad P=\begin{pmatrix} P_1S_2P_2 \\ P_2 \end{pmatrix}.$$

Theorem 3.3 yields

$$M^* = \begin{pmatrix} M_1^* & M_1^*P_1S_2M_2^+ \\ 0 & M_2^* \end{pmatrix}.$$

Hence, $\|\theta_1\theta_2\| = S_1M_1^*P_1S_2P_2+S_1M_1^*P_1S_2M_2^+P_2 = \|\theta_1\|\,\|\theta_2\|$. $\square$

Construction 4. Assume $\|\theta_1\|$ to be quasiregular, i.e., $(\|\theta_1\|,\varepsilon)=(S_1P_1,\varepsilon)=0$. That means $S_1P_1=0$ and $\|\theta_1\|=S_1M_1^+P_1$.

$\theta_1^+ = (I_1,M_1+P_1S_1M_1,S_1,P_1)$.

Theorem 2.6 yields

$$(M_1+P_1S_1M_1)^* = M_1^*(P_1S_1M_1^+)^*.$$

Hence,

$\|\theta_1^+\| = S_1(M_1+P_1S_1M_1)^*P_1 = S_1M_1^*(P_1S_1M_1^+)^*P_1 = S_1M_1^+P_1(S_1M_1^+P_1)^* = \|\theta_1\|^+$. $\square$

Construction 5. Let A be commutative. Then $\theta_1\odot\theta_2=(I_1\times I_2,M_1\odot M_2,S_1\odot S_2,P_1\odot P_2)$. We obtain, by Theorems 3.9 and

3.10,

$$\|\vartheta_1 \odot \vartheta_2\| = (S_1 \odot S_2)(M_1 \odot M_2)^*(P_1 \odot P_2) = (S_1 \odot S_2)(M_1^* \odot M_2^*)(P_1 \odot P_2) = \|\vartheta_1\| \odot \|\vartheta_2\| . \quad \square$$

Construction 6. Let A be commutative. Then

$$\vartheta_1 \sqcup \vartheta_2 = (I_1 \times I_2, M_1 \oplus M_2, S_1 \otimes S_2, P_1 \otimes P_2) .$$

We obtain, by Theorems 3.8 and 3.11,

$$\|\vartheta_1 \sqcup \vartheta_2\| = (S_1 \otimes S_2)(M_1 \oplus M_2)^*(P_1 \otimes P_2) = (S_1 \otimes S_2)(M_1^* \sqcup M_2^*)(P_1 \otimes P_2) =$$

$$\sum_{w_1 \in \Sigma^*} \sum_{w_2 \in \Sigma^*} ((S_1, \varepsilon) \otimes (S_2, \varepsilon))((M_1^*, w_1) \otimes (M_2^*, w_2))((P_1, \varepsilon) \otimes (P_2, \varepsilon)) w_1 \sqcup w_2 =$$

$$\sum_{w_1 \in \Sigma^*} \sum_{w_2 \in \Sigma^*} (((S_1, \varepsilon)(M_1^*, w_1)(P_1, \varepsilon))((S_2, \varepsilon)(M_2^*, w_2)(P_2, \varepsilon)) w_1 \sqcup w_2 =$$

$$\sum_{w_1 \in \Sigma^*} \sum_{w_2 \in \Sigma^*} (\|\vartheta_1\|, w_1)(\|\vartheta_2\|, w_2) w_1 \sqcup w_2 = \|\vartheta_1\| \sqcup \|\vartheta_2\| . \quad \square$$

Construction 7. $(\vartheta_1)_z = (I_1 \cup \bar{I}_1, M, S, P)$, where $\bar{I}_1$ is a copy of I_1,

$$S = (S_1 \ \ 0), \quad M = \begin{pmatrix} M_1 & (M_1, z) M_1 \\ 0 & M_1 \end{pmatrix}, \quad P = \begin{pmatrix} (M_1, z) P_1 \\ P_1 \end{pmatrix} .$$

Hence,

$$\|(\vartheta_1)_z\| = S_1 M_1^* (M_1, z) P_1 + S_1 M_1^* (M_1, z) M_1^+ P_1 = S_1 M_1^* (M_1, z) M_1^* P_1$$

and

$$(\|(\vartheta_1)_z\|, w) = \sum_{w_1 w_2 = w} (S_1, \varepsilon)(M_1^*, w_1)(M_1, z)(M_1^*, w_2)(P_1, \varepsilon) =$$

$$\sum_{w_1 w_2 = w} (\|\vartheta_1\|, w_1 z w_2) = (\|\vartheta_1\|_z, w) . \quad \square$$

A power series $r \in A\langle\langle \Sigma^* \rangle\rangle$ is termed A-rational (over Σ) iff r can be obtained from elements of $A\langle \Sigma^* \rangle$ by finitely many applications of the operation of sum, product and quasi-inverse (applied to quasiregular power series). The family of A-rational power series over Σ is denoted by $A^{rat}\langle\langle \Sigma^* \rangle\rangle$.

A subsemiring of $A\langle\langle \Sigma^* \rangle\rangle$ is rationally closed iff it contains the quasi-inverse of every quasiregular element.

The next theorem is the famous Kleene-Schützenberger Theorem.

Theorem 3.14. $A^{rat}\langle\langle \Sigma^* \rangle\rangle$ coincides with the family of behaviors of $A\langle \Sigma \rangle$-finite-automata.

Proof. Constructions 2,3 and 4 prove that the family of behaviors of $A<\Sigma>$-finite-automata is a rationally closed semiring containing $A<\Sigma^*>$. (Clearly, $a\varepsilon$, $a\in A$, and $x\in\Sigma$ are behaviors of $A<\Sigma>$-finite-automata.) The converse is proven by induction on the number of states of $A<\Sigma>$-finite-automata by help of Theorem 3.2. □

We now introduce $A<<\Sigma^*>>$-pushdown-automata. Γ denotes an alphabet (of pushdown symbols).

A matrix $M\in((A<<\Sigma^*>>)^{Q\times Q})_J^{\Gamma^*\times\Gamma^*}$ is termed a pushdown transition matrix iff for all $\pi_1,\pi_2\in\Gamma^*$,

$$M_{\pi_1,\pi_2} = \begin{cases} M_{p,\pi_3} & \text{if there exist } p\in\Gamma,\ \pi_4\in\Gamma^* \text{ with } \pi_1=p\pi_4 \\ & \text{and } \pi_2=\pi_3\pi_4; \\ 0 & \text{otherwise.} \end{cases}$$

An $A<<\Sigma^*>>$-pushdown-automaton

$$\mathcal{P}=(Q,\Gamma,M,S,p_0,P)$$

is given by

(i) a finite set Q of states,

(ii) an alphabet Γ of pushdown symbols,

(iii) a pushdown transition matrix M,

(iv) $S\in(A<\varepsilon>)^{1\times Q}$ called the initial state vector,

(v) $p_0\in\Gamma$ called the initial pushdown symbol,

(vi) $P\in(A<\varepsilon>)^{Q\times 1}$ called the final state vector.

The behavior $\|\mathcal{P}\|\in A<<\Sigma^*>>$ of an $A<<\Sigma^*>>$-pushdown-automaton $\mathcal{P}=(Q,\Gamma,M,S,p_0,P)$ is defined by

$$\|\mathcal{P}\| = S(M^*)_{p_0,\varepsilon}P$$

provided M^* exists. An $A<<\Sigma^*>>$-pushdown-automaton $\mathcal{P}=(Q,\Gamma,M,S,p_0,P)$ is called cycle-free iff M is cycle-free. In this case, the behavior of $\mathcal{P}$ is welldefined.

Theorem 3.15. For every cycle-free $A<<\Sigma^*>>$-pushdown-automaton $\mathcal{P}$ there exists a cycle-free $A<<\Sigma^*>>$-automaton $\mathcal{A}$ such that $\|\mathcal{A}\|=\|\mathcal{P}\|$.

Proof. Consider a cycle-free $A<<\Sigma^*>>$-pushdown-automaton

$$\mathcal{P} = (Q,\Gamma,M,S,p_0,P)$$

with the behavior $\|\mathcal{P}\| = S(M^*)_{p_0,\varepsilon}P$.

Let $M' \in (A\langle\langle\Sigma^*\rangle\rangle)_J^{(\Gamma^* \times Q)\times(\Gamma^* \times Q)}$ be the isomorphic copy of M, i.e.,

$$M'_{(\pi_1,q_1),(\pi_2,q_2)} = (M_{\pi_1,\pi_2})_{q_1,q_2}.$$

Define, furthermore, $S' \in (A\langle\varepsilon\rangle)^{1\times(\Gamma^* \times Q)}$ and $P' \in (A\langle\varepsilon\rangle)^{(\Gamma^* \times Q)\times 1}$ by

$S'_{(p_0,q)} = S_q$, $S_{(\pi,q)} = 0$, $\pi \neq p_0$, $P'_{(\varepsilon,q)} = P_q$, $P'_{(\pi,q)} = 0$, $\pi \neq \varepsilon$.

Consider now the $A\langle\langle\Sigma^*\rangle\rangle$-automaton

$$\mathcal{A} = (\Gamma^* \times Q, M', S', P').$$

Then $\|\mathcal{A}\| = S'M'^*P' =$

$$\sum_{(\pi_1,q_1),(\pi_2,q_2)\in\Gamma^* \times Q} S'_{(\pi_1,q_1)} (M'^*)_{(\pi_1,q_1),(\pi_2,q_2)} P'_{(\pi_2,q_2)} =$$

$$\sum_{q_1,q_2\in Q} S'_{(p_0,q_1)} (M'^*)_{(p_0,q_1),(\varepsilon,q_2)} P'_{(\varepsilon,q_2)} =$$

$$\sum_{q_1,q_2\in Q} S'_{q_1} ((M^*)_{p_0,\varepsilon})_{q_1,q_2} P_{q_2} = S(M^*)_{p_0,\varepsilon}P = \|\mathcal{P}\|. \qquad \square$$

Hence, all definitions introduced for $A\langle\langle\Sigma^*\rangle\rangle$-automata hold also for $A\langle\langle\Sigma^*\rangle\rangle$-pushdown-automata.

4. ALGEBRAIC SYSTEMS.

In this section we show the connection between pushdown automata and algebraic systems.

To simplify our presentation, we assume for the rest of this paper that A is a commutative semiring.

An $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system (briefly algebraic system) with variables in $Y = \{y_1,\ldots,y_n\}$, $Y\cap\Sigma = \emptyset$, is a system of equations

$$y_i = p_i,\ 1\leq i\leq n,$$

where each p_i is a polynomial in $A\langle(\Sigma\cup Y)^*\rangle$. Intuitively, a solution of such an algebraic system is given by n power series $\sigma_1,\ldots,\sigma_n$ in $A\langle\langle\Sigma^*\rangle\rangle$ satisfying the algebraic system in the sense that if each variable y_i is replaced by the series σ_i then valid equations result.

More formally, consider

$$\sigma = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} \in (A\langle\langle(\Sigma\cup Y)^*\rangle\rangle)^{nx1}.$$

Then we can define a morphism

$$\sigma : (\Sigma\cup Y)^* \to A\langle\langle(\Sigma\cup Y)^*\rangle\rangle$$

by $\sigma(y_i) = \sigma_i$, $1\leq i\leq n$, and $\sigma(x) = x$, $x\in\Sigma$.

Extend σ to a mapping

$$\sigma : A\langle(\Sigma\cup Y)^*\rangle \to A\langle\langle(\Sigma\cup Y)^*\rangle\rangle$$

by the definition

$$\sigma(p) = \sum_{\gamma\in(\Sigma\cup Y)^*} (p,\gamma)\sigma(\gamma),$$

where p is in $A\langle(\Sigma\cup Y)^*\rangle$. Then this extended mapping σ is a semiring morphism.

A solution to the algebraic system $y_i = p_i$, $1\leq i\leq n$, is given by a column vector $\sigma\in(A\langle\langle\Sigma^*\rangle\rangle)^{nx1}$ such that $\sigma_i = \sigma(p_i)$, $1\leq i\leq n$.

The approximation sequence

$$\sigma^0,\sigma^1,\ldots,\sigma^j,\ldots,\sigma^j \in (A\langle\Sigma^*\rangle)^{nx1}$$

associated to an algebraic system $y_i = p_i$, $1 \leq i \leq n$, is defined as follows:

$$\sigma^0 = 0, \quad \sigma_i^{j+1} = \sigma^j(p_i), \quad j \geq 0, \quad 1 \leq i \leq n.$$

If the approximation sequence converges, i.e., $\lim_{j \to \infty} \sigma^j = \sigma$, then σ is referred to as the strong solution.

The next theorems are wellknown.

Theorem 4.1. The strong solution (when it exists) is a solution. □

Theorem 4.2. Every $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$-algebraic system has a strong solution. □

Every context-free grammar with the terminal alphabet Σ and every semiring A give rise to an $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system. Conversely, every $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system gives rise to a context-free grammar. More explicitly, this interrelation is defined as follows.

Consider the context-free grammar $G = (Y, \Sigma, R, y_1)$. Then define the $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system $y_i = p_i$, $1 \leq i \leq n$, by

$$(p_i, \gamma) = 1 \text{ if } y_i \to \gamma \in R,$$

and

$$(p_i, \gamma) = 0 \text{ otherwise,}$$

where γ is in $(\Sigma \cup Y)^*$. Conversely, given an $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system $y_i = p_i$, $1 \leq i \leq n$, define the context-free grammar $G = (Y, \Sigma, R, y_1)$ by

$$y_i \to \gamma \in R \text{ iff } (p_i, \gamma) \neq 0,$$

where γ is in $(\Sigma \cup Y)^*$.

Whenever we speak of a context-free grammar corresponding to an algebraic system, or vice versa, then we mean the correspondence in the sense of the above definition. The next theorem shows the connection between $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$-algebraic systems and context-free grammars.

Theorem 4.3. Assume that $G = (Y,\Sigma,R,y_1)$ is a context-free grammar and $y_i = p_i$, $1 \leq i \leq n$, is the corresponding $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$-algebraic system with the strong solution σ. Then

$$L(G) = \mathrm{supp}(\sigma_1)$$

or, equivalently,

$$\sigma_1 = \mathrm{char}(L(G)).$$ □

An $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system $y_i = p_i$, $1 \leq i \leq n$, is termed strict iff $\mathrm{supp}(p_i) \subseteq \varepsilon \cup \Sigma(\Sigma \cup Y)^*$.

Theorem 4.4. Strong solutions exist for all strict algebraic systems. Moreover, the strong solution is the unique solution of a strict algebraic system. □

The collection of all power series in $A\langle\langle\Sigma^*\rangle\rangle$ that are the first component of the unique solution of a strict algebraic system is denoted by $A^{alg}\langle\langle\Sigma^*\rangle\rangle$. The next theorem is an easy consequence of Theorem 4.3.

Theorem 4.5. A formal language $L \subseteq \Sigma^*$ is context-free iff $\mathrm{char}(L)$ is in $\mathbb{B}^{alg}\langle\langle\Sigma^*\rangle\rangle$. □

We now show the connection of the power series in $A^{alg}\langle\langle\Sigma^*\rangle\rangle$ and the power series that are behaviors of cycle-free $A\langle\Sigma \cup \varepsilon\rangle$-pushdown-automata.

Theorem 4.6. Assume that $y_i = p_i$, where $\mathrm{supp}(p_i) \subseteq \Sigma(\Sigma \cup Y)^*$, $1 \leq i \leq n$, is an $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system with the strong solution σ. Then there exists an $A\langle\Sigma\rangle$-pushdown-automaton $\mathcal{P}$ such that $\|\mathcal{P}\| = \sigma_1$. □

It is easy to show that, whenever a formal power series r is accepted by a cycle-free $A<\Sigma\cup\varepsilon>$-pushdown-automaton then so is $a\varepsilon+r$, $a\in A$. Hence, each series in $A^{alg}\langle\langle\Sigma^*\rangle\rangle$ is accepted by a cycle-free $A<\Sigma\cup\varepsilon>$-pushdown-automaton. The reverse transition will now be established.

Theorem 4.7. Assume that $\mathcal{P}$ is a cycle-free $A<\Sigma\cup\varepsilon>$-pushdown-automaton. Then there exists an $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system with the unique solution σ such that $\sigma_1 = \|\mathcal{P}\|$.

Proof. Assume that $\mathcal{P} = (Q,\Gamma,M,S,p_0,P)$ is a cycle-free $A<\Sigma\cup\varepsilon>$-pushdown-automaton with the behavior $\|\mathcal{P}\| = S(M^*)_{p_0,\varepsilon}P$.

We now construct an $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system with the alphabet of variables

$$Y=\{y^p_{q_1,q_2} \mid p\in\Gamma, q_1,q_2\in Q\}.$$

By definition, the matrices $Y_p\in(A<Y>)^{Q\times Q}$, $p\in\Gamma$, have the (q_1,q_2)-entry $y^p_{q_1,q_2}$, $q_1,q_2\in Q$. Using these matrices we define

$$Y_\varepsilon = E, \quad Y_{p\pi} = Y_p Y_\pi.$$

Our algebraic system is now given in the following matrix notation

$$Y_p = \sum_{\pi\in\Gamma^*} M_{p,\pi} Y_\pi, \quad p\in\Gamma.$$

Its unique solution is given by $(M^*)_{p,\varepsilon}$, $p\in\Gamma$. Here it is understood that $(M^*)_{p,\varepsilon}$ is substituted for Y_p, $p\in\Gamma$.

We now add an equation $y_0 = S\sum_{\pi\in\Gamma^*} M_{p_0,\pi} Y_\pi P$. Then $\|\mathcal{P}\|$ equals the component in the unique solution of the augmented $A\langle\langle\Sigma^*\rangle\rangle$-algebraic system corresponding to y_0. □

Theorem 4.8. A formal power series is in $A^{alg}\langle\langle\Sigma^*\rangle\rangle$ iff it is accepted by a cycle-free $A<\Sigma\cup\varepsilon>$-pushdown-automaton. □

5. COMBINATORIAL APPLICATIONS.

Our combinatorial applications concern mainly rational and algebraic sequences and their generating functions. Here a sequence $\alpha \in A^{\mathbb{N}}$ is termed A-rational (A-algebraic, respectively) iff $\sum_{n=0}^{\infty} \alpha(n) z^n$ is a power series in $A^{rat}\langle\langle z^* \rangle\rangle$ ($A^{alg}\langle\langle z^* \rangle\rangle$, respectively).

Goulden, Jackson [9] and Flajolet [6] have presented the theory to solve combinatorial enumeration problems via the symbolic operator method by the use of generating functions. That means that they translate combinatorial constructions into operators on counting generating functions. These operations on generating functions will be defined in this section by the help of automata.

Recall that A is assumed to be a commutative semiring. We first consider A-rational sequences.

Lemma 5.1. Let $q=a_1 z+\ldots+a_k z^k$ and $p=b_0 \varepsilon+\ldots+b_{k-1} z^{k-1}$ be polynomials and consider the A-rational power series $r=q^* p$. Then

(i) for all $0 \leq n \leq k-1$, $(r,z^n)=a_1(r,z^{n-1})+\ldots+a_n(r,\varepsilon)+b_n$;

(ii) for all $n \geq k$, $(r,z^n)=a_1(r,z^{n-1})+\ldots+a_k(r,z^{n-k})$.

Proof. Observe that, by Corollary 2.2,
$r=qq^*p+p=qr+p=a_1 zr+\ldots+a_k z^k r+p$. □

Theorem 5.2. Let $q=a_1 z+\ldots+a_k z^k$, r_1 and r_2 be polynomials and consider the A-rational power series $r=q^* r_1+r_2$.

Then, for some $n_0 \geq k$ and all $n \geq n_0$,

$(r,z^n)=a_1(r,z^{n-1})+\ldots+a_k(r,z^{n-k})$.

Proof. Lemma 5.1 implies that, for all sufficiently large n,

$$(r,z^n)=(q^* r_1,z^n)=a_1(q^* r_1,z^{n-1})+\ldots+a_k(q^* r_1,z^{n-k})=$$
$$a_1(r,z^{n-1})+\ldots+a_k(r,z^{n-k}).$$ □

The following theorem is a slight generalization of Klarner [13], Theorem 3 and Eilenberg [5], Theorem VIII.4.2. A sequence $\alpha \in A^{\mathbb{N}}$ is termed ultimately periodic iff there exist integers $t \geq 0$ and $s \geq 1$ such that $\alpha(n+s)=\alpha(n)$ for all $n \geq t$.

Theorem 5.3. The following statements concerning a sequence $\alpha \in A^{\mathbb{N}}$ are equivalent:

(i) α is ultimately periodic;

(ii) there exist $s \geq 1$ and $r_1, r_2 \in A\langle z^* \rangle$ such that $\sum_{n=0}^{\infty} \alpha(n) z^n = (z^s)^* r_1 + r_2$;

(iii) for some $n_0 \geq k$ and all $n \geq n_0$, $\alpha(n) = a_1\alpha(n-1) + \ldots + a_k\alpha(n-k)$ and $\{\alpha(n) \mid n \geq 0\}$ is finite.

Proof.

(i)$\Rightarrow$(ii): Since α is ultimately periodic there exist $t \geq 0$ and $s \geq 1$ such that $\alpha(n+s) = \alpha(n)$ for all $n \geq t$. Consider the two polynomials $r_1 = \alpha(t) z^t + \ldots + \alpha(t+s-1) z^{t+s-1}$, $r_2 = \alpha(0)\varepsilon + \ldots + \alpha(t-1) z^{t-1}$ and let

$r = (z^s)^* r_1 + r_2$.

We claim that, for all $n \geq 0$,

$$(r, z^n) = \alpha(n).$$

Let $0 \leq n \leq t-1$. Then $(r, z^n) = (r_2, z^n) = \alpha(n)$.

Let $n \geq t$. There are unique $m_1, m_2 \geq 0$ such that $n - t = s \cdot m_1 + m_2$, $0 \leq m_2 \leq s-1$. Hence, $n = s \cdot m_1 + m_2 + t$.

This implies

$(r, z^n) = ((z^s)^* r_1, z^n) = ((z^s)^*, (z^s)^{m_1})(r_1, z^{m_2+t}) = (r_1, z^{m_2+t}) =$

$\alpha(t+m_2) = \alpha(sm_1 + m_2 + t) = \alpha(n)$.

(ii)$\Rightarrow$(iii): Theorem 5.2 implies that, for some $n_0 \geq s$ and all $n \geq n_0$

$$\alpha(n) = \alpha(n-s).$$

Now we obtain

$\{\alpha(n) \mid n \geq 0\} = \{\alpha(n) \mid 0 \leq n \leq n_0 - 1\}$.

(iii)$\Rightarrow$(i): Assume that $\{\alpha(n) \mid n \geq 0\}$ contains exactly $\ell \geq 1$ elements of A. Consider the k-tuples

$\beta_i = (\alpha(n_0 + (i-1)k), \ldots, \alpha(n_0 + ik - 1))$, $i \geq 0$.

Since there exist at most ℓ^k distinct such k-tuples, there exist $j_1 \geq 0$, $j_2 > 0$, $j_1 + j_2 \leq \ell^k$, such that $\beta_{j_1} = \beta_{j_1+j_2}$.

Hence,

$\alpha(n_0 + (j_1 - 1)k) = \alpha(n_0 + (j_1 + j_2 - 1)k), \ldots, \alpha(n_0 + j_1 k - 1) = \alpha(n_0 + (j_1 + j_2)k - 1)$.

The recurrence equation of (iii) and these equalities yield

$$\alpha(n+j_2k)=\alpha(n)$$

for all $n\geq n_0+(j_1-1)k$. □

The next theorem shows that all A-rational power series are of the form of Lemma 1, i.e., $r=q^*p$, in case A is a commutative ring (with unity). (See Eilenberg [5], Theorem VIII.3.1 and Kuich,Salomaa [15], Theorem 8.16).

Theorem 5.4. Let A be a commutative ring. Then r is a power series in $A^{rat}\langle\langle z^*\rangle\rangle$ iff there exist polynomials $p,q\in A\langle z^*\rangle$, where q is quasiregular, such that

$$r=q^*p.$$

Proof. We have to show that $q_1^*p_1+q_2^*p_2$, $q_1^*p_1q_2^*p_2$, $(q^*p)^+$, q_1,q_2,q,p quasiregular, are of the form indicated by our theorem. We prove only the last case (by Theorem 2.6):

$$(q+p)^*p=(q^*p)^*q^*p=(q^*p)^+.$$

Theorem 5.5. Let A be a commutative ring. The following statements concerning a sequence $\alpha\in A^{\mathbb{N}}$ are equivalent:

(i) α is A-rational;

(ii) there exist polynomials $p,q\in A\langle z^*\rangle$, where q is quasiregular, such that, for all $n\geq 0$,
$$\alpha(n)=(q^*p,z^n);$$

(iii) for some $n_0\geq k$ and all $n\geq n_0$,
$$\alpha(n)=a_1\alpha(n-1)+\ldots+a_k\alpha(n-k).$$

Proof. We have only to prove that (iii) implies (ii). The remaining implications are proved by Theorems 5.2 and 5.4.

Assume now (iii) and define the polynomial $q=a_1z+\ldots+a_kz^k$. An easy computation shows that $(\varepsilon-q)\sum_{n=0}^{\infty}\alpha(n)z^n=p$ is a polynomial.

Since A is a ring, we obtain the equality $q^*(\varepsilon-q)=\varepsilon$. Hence,

$$\sum_{n=0}^{\infty}\alpha(n)z^n=q^*p.$$ □

Theorem 5.6. Let A be a commutative ring. The following statements concerning a sequence $\alpha \in A^{\mathbb{N}}$ are equivalent:

(i) α is A-rational and $\{\alpha(n) \mid n \geq 0\}$ is finite;

(ii) there exist $s \geq 1$ and $p \in A\langle z^* \rangle$ such that
$$\sum_{n=0}^{\infty} \alpha(n) z^n = (z^s)^* p;$$

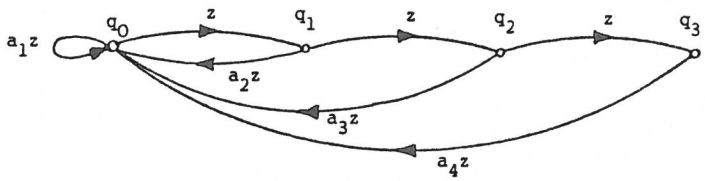
(iii) for some $n_0 \geq k$ and all $n \geq n_0$,
$\alpha(n) = a_1\alpha(n-1) + \ldots + a_k\alpha(n-k)$ and $\{\alpha(n) \mid n \geq 0\}$ is finite;

(iv) α is ultimately periodic.

Proof. Theorem 5.6 is implied by Theorems 5.3 and 5.5 and the following identity.

Let r_1, r_2 and q be polynomials in $A\langle z^* \rangle$ and q be quasiregular. Since A is a ring, we obtain the identity
$$q^* r_1 + r_2 = q^* r_1 + q^*(\varepsilon - q) r_2 = q^*(r_1 + r_2 - q r_2).$$ □

By definition, the $A\langle z \rangle$-finite-automaton
$\mathcal{A}(a_1, \ldots, a_k; b_0, \ldots, b_{k-1}) = (Q, M, S, P)$ is given by $Q = \{q_0, \ldots, q_{k-1}\}$;
$S = (\varepsilon, 0, \ldots, 0)$; $M_{q_i, q_0} = a_{i+1} z$, $M_{q_i, q_{i+1}} = z$, $0 \leq i \leq k-1$; $M_{q_i, q_j} = 0$ otherwise;
$P_{q_i} = b_i$, $0 \leq i \leq k-1$. The next figure shows $\mathcal{A}(a_1, a_2, a_3, a_4; b_0, b_1, b_2, b_3)$.



Theorem 5.7. $\| \mathcal{A}(a_1, \ldots, a_k; b_0, \ldots, b_{k-1}) \| =$
$$(a_1 z + \ldots + a_k z^k)^* (b_0 \varepsilon + \ldots + b_{k-1} z^{k-1}).$$

Proof. By Theorem 3.2 we obtain for the q_0-row of M^*
$$(a_1 z + \ldots + a_k z^k)^* (\varepsilon, z, \ldots, z^{k-1}).$$

Hence, SM^*P equals the expression described in the theorem. □

In case A is a commutative ring, the $A\langle z \rangle$-finite-automaton $\mathcal{A}(a_1, \ldots, a_k; b_0, \ldots, b_{k-1})$ constitutes a "normal form automaton" for

the generation of the A-rational sequence α, where

$$\sum_{n=0}^{\infty} \alpha(n) z^n = (a_1 z + \ldots a_k z^k)^* (b_0 \varepsilon + \ldots + b_{k-1} z^{k-1}) = \| \mathcal{A}(a_1, \ldots, a_k; b_0, \ldots, b_{k-1}) \| .$$

A sequence $\alpha \in A^{\mathbb{N}}$ is <u>generated</u> by an $A\langle z\rangle$-automaton $\mathcal{A}$ iff, for all $n \geq 0$, $\alpha(n) = (\| \mathcal{A} \|, z^n)$. If A is a commutative ring, each A-rational sequence is generated by some normal form automaton $\mathcal{A}(a_1, \ldots, a_k; b_0, \ldots, b_{k-1})$.

A power series $q^* r \in A^{rat}\langle\langle z^* \rangle\rangle$, $q, r \in A\langle z\rangle$, q quasiregular, is the <u>generating function</u> of an A-rational sequence α iff, for all $n \geq 0$, $\alpha(n) = (q^* r, z^n)$.

Our next goal is to show the Cayley-Hamilton Theorem in commutative rings. Clearly, this yields an easy method for the computation of the generating function from a generating $A\langle z\rangle$-finite-automaton.

An analysis of the results and proofs in Nrs.33-35 of von Mangoldt, Knopp [17] shows that these are valid also in commutative rings. We assume the reader to be familiar with the definitions of a determinant det(M) of a matrix M.

Let now M be a kxk-matrix, $k \geq 2$, and consider the (k-1)x(k-1)-matrix M^{ij} that originates from M by cancelling the i-th row and the j-th column of M. By definition, the (i,j)-<u>minor</u> $\mu_{i,j}$ is given by

$$\mu_{i,j} = (-1)^{i+j} \det(M^{ij}) .$$

By Nr.35(6) of von Mangoldt,Knopp [17] we have the identities

$$\sum_{s=1}^{n} M_{i,s}\, \mu_{j,s} = \sum_{s=1}^{n} M_{s,i}\, \mu_{s,j} = \delta_{i,j} \det(M), \quad 1 \leq i,j \leq k.$$

Let now $M \in (A\langle z\rangle)^{kxk}$. Define $P_j \in (A\langle \varepsilon\rangle)^{kx1}$ and $S \in (A^{rat}\langle\langle z^* \rangle\rangle)^{kx1}$ by $(P_j)_s = \delta_{j,s}$ and

$$S = MS + P_j .$$

By Theorem 3.5 we obtain that

$$S_i = (M^*)_{i,j}, \quad 1 \leq i \leq k.$$

Since A is a (commutative) ring, we have

$$(E-M)S = P_j ,$$

i.e.,

$$\sum_{t=1}^{k} (\delta_{s,t} - M_{s,t}) S_t = \delta_{s,j}, \quad 1 \leq s \leq k.$$

Multiply the s-th equality by the (s,i)-minor $\mu_{s,i}$ of E-M,

$$\sum_{t=1}^{k} (\delta_{s,t}-M_{s,t})\mu_{s,i}\, S_t=\delta_{s,j}\,\mu_{s,i},\quad 1\leq s\leq k,$$

and add these k equalities

$$\sum_{s=1}^{k}\sum_{t=1}^{k} (\delta_{s,t}-M_{s,t})\mu_{s,i}S_t=\sum_{s=1}^{k}\delta_{s,j}\,\mu_{s,i}=\mu_{j,i}.$$

This yields

$$\sum_{t=1}^{k}\sum_{s=1}^{k} (E-M)_{s,t}\,\mu_{s,i}\,S_t=\sum_{t=1}^{k}\delta_{t,i}\ \det(E-M)S_t=\det(E-M)S_i=\mu_{j,i}.$$

Since ε-det(E-M) is quasiregular, we obtain

$$(M^*)_{i,j}=(\varepsilon\text{-det}(E-M))^*\mu_{j,i},\quad 1\leq i,j\leq k.$$

Clearly, the degrees of ε-det(E-M) and $\mu_{j,i}$, respectively, are at most k and k-1, respectively. Hence, Lemma 5.1 proves the following Cayley-Hamilton Theorem in commutative rings.

Theorem 5.8. Let A be a commutative ring. Consider a matrix $M\in(A\langle z\rangle)^{k\times k}$ and compute $\varepsilon\text{-det}(E-M)=a_1z+\ldots+a_kz^k$. Then, for all $n\geq k$, $1\leq i,j\leq k$,

$$((M,z)^n)_{i,j}=a_1((M,z)^{n-1})_{i,j}+\ldots+a_k((M,z)^{n-k})_{i,j}.$$

Proof. $(M^*)_{i,j}=\sum_{n=0}^{\infty}((M,z)^n)_{i,j}z^n=(a_1z+\ldots+a_kz^k)^*\mu_{j,i}$. Now apply Lemma 5.1 (ii). □

Flajolet [6], Part I, Figure 2, has given a table of the translation of operations on sequences into operators on generating functions. We do the same for operators on A<z>-automata. If in the following table the A<z>-automata $\mathcal{A}$ and $\mathcal{B}$ generate the sequences (a_n) and (b_n), then the A<z>-automaton in the second column generates the sequence (s_n) in the first column.

Sequence	A<z>-automaton
ka_n	$k\mathcal{A}$
a_n+b_n	$\mathcal{A}+\mathcal{B}$
$\sum_{k=0}^{n} a_kb_{n-k}$	$\mathcal{A}\mathcal{B}$
$a_n+\sum_{k=1}^{n} a_ks_{n-k}$	$\mathcal{A}^+$
a_nb_n	$\mathcal{A}\odot\mathcal{B}$
$\sum_{k=0}^{n}\binom{n}{k}a_kb_{n-k}$	$\mathcal{A}\sqcup\mathcal{B}$
$(n+1)a_{n+1}$	$\mathcal{A}_z$

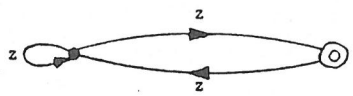
If $\mathcal{A}$ and $\mathcal{B}$ are A<z>-finite-automata then the automata in the second column are again A<z>-finite-automata and the (s_n) are A-rational sequences. If $\mathcal{A}$ and $\mathcal{B}$ are A<z>-pushdown-automata (in cases $\odot$ and $\sqcup\!\sqcup$, $\mathcal{B}$ has to be an A<z>-finite-automaton), then the automata in the second column are again A<z>-pushdown-automata and the (s_n) are A-algebraic sequences. (The constructions 1-7 have to be performed carefully on the blocks to yield again A<z>-pushdown-automata.)

Examples will show the usefulness of the constructions. The basic commutative ring is $\mathbb{Z}$.

Example 5.1. The Fibonacci numbers F_n, $n\geq 0$, are defined by $F_0=0$, $F_1=1$ and $F_n=F_{n-1}+F_{n-2}$, $n\geq 2$. They are generated by

$$\sum_{n=0}^{\infty} F_n z^n = (z+z^2)^* z.$$

This shows that the sequence of the Fibonacci numbers is $\mathbb{N}$-rational. The normal form automaton for the sequence (F_n) is $\mathcal{A}(1,1;0,1)=(\{q_0,q_1\},M,S,P)$, which is drawn in the next figure.



(i) Let (C_n) be the sequence $(F_n)\cdot(F_n)$, i.e., the Cauchy product of the sequence of Fibonacci numbers with itself. Then $\mathcal{A}(1,1;0,1)\cdot\mathcal{A}(1,1;0,1)=(\{q_0,q_1,q_2,q_3\},M_1,S_1,P_1)$ generates (C_n):

$$M_1=\begin{pmatrix} z & z & 0 & 0 \\ z & 0 & z & z \\ 0 & 0 & z & z \\ 0 & 0 & z & 0 \end{pmatrix}, \quad P_1=\begin{pmatrix} 0 \\ 0 \\ 0 \\ \varepsilon \end{pmatrix}, \quad S_1=(\varepsilon,0,0,0).$$

We obtain $\det(E-M_1)=\varepsilon-2z-z^2+2z^3+z^4$ and $\mu_{4,1}=z^2$. Hence, (C_n) is generated by $(2z+z^2-2z^3-z^4)^* z^2$:
$C_0=C_1=0$, $C_2=1$, $C_3=2$, $C_4=5$, $C_5=10$, $C_6=20$, $C_7=38,\ldots$.

(ii) Let (H_n) be the sequence $(F_n)\odot(F_n)$, i.e., the Hadamard product of the sequence of Fibonacci numbers with itself. Then $\mathcal{A}(1,1;0,1)\odot\mathcal{A}(1,1;0,1)=(\{q_0,q_1,q_2,q_3\},M_2,S_2,P_2)$ generates (H_n):

$$M_2=\begin{pmatrix} z & z & z & z \\ z & 0 & z & 0 \\ z & z & 0 & 0 \\ z & 0 & 0 & 0 \end{pmatrix}, \quad P_2=\begin{pmatrix} 0 \\ 0 \\ 0 \\ \varepsilon \end{pmatrix}, \quad S_2=(\varepsilon,0,0,0).$$

We obtain $\det(E-M_2)=\varepsilon-z-4z^2-z^3+z^4$ and $\mu_{4,1}=z-z^3$. Hence, (H_n) is generated by $(z+4z^2+z^3-z^4)^*(z-z^3)$:
$H_0=0$, $H_1=1$, $H_2=1$, $H_3=4$, $H_4=9$, $H_5=25$, $H_6=64$, $H_7=169,\ldots$.

(iii) Let (T_n) be the sequence $(F_n)\sqcup\!\sqcup(F_n)$, i.e., the Hurwitz product of the sequence of Fibonacci numbers with itself. Then $\mathcal{A}(1,1;0,1)\sqcup\!\sqcup\mathcal{A}(1,1;0,1)=(\{q_0,q_1,q_2,q_3\},M_3,S_3,P_3)$ generates (T_n):

$$M_3=\begin{pmatrix} 2z & z & z & 0\\ z & z & 0 & z\\ z & 0 & z & z\\ 0 & z & z & 0\end{pmatrix},\quad P_3=\begin{pmatrix}0\\0\\0\\ \varepsilon\end{pmatrix},\quad S_3=(\varepsilon,0,0,0).$$

Since M_3 is blockstochastic (see Kuich,Salomaa [15],Exercise 4.5), the A<z>-finite-automaton $(\{q_0,q_1,q_3\},M_3',S_3',P_3')$ generates (T_n):

$$M_3'=\begin{pmatrix} 2z & 2z & 0\\ z & z & z\\ 0 & 2z & 0\end{pmatrix},\quad P_3'=\begin{pmatrix}0\\0\\ \varepsilon\end{pmatrix},\quad S_3'=(\varepsilon,0,0).$$

We obtain $\det(E-M_3')=\varepsilon-3z-2z^2+4z^3$ and $\mu_{3,1}=2z^2$. Hence, (T_n) is generated by $(3z+2z^2-4z^3)^*2z^2$:
$T_0=T_1=0$, $T_2=2$, $T_3=6$, $T_4=22$, $T_5=70$, $T_6=230$, $T_7=742,\ldots$. □

Example 5.2. We want to prove the identity
$\binom{n}{0}F_0+\binom{n}{1}F_1+\ldots+\binom{n}{n}F_n=F_{2n}$.

(i) The value on the left side of the identity is the n-th element of the sequence $(F_n)\sqcup\!\sqcup(1)$. This sequence is generated by the A<z>-finite-automaton

$$(\{q_0,q_1\},\begin{pmatrix}2z & z\\ z & z\end{pmatrix},(\varepsilon,0),\begin{pmatrix}0\\ \varepsilon\end{pmatrix}).$$

(ii) The sequence $(F_n)\odot((1^n+(-1)^n)/2)$, $F_0,0,F_2,0,F_4,0,\ldots,F_{2n},0,\ldots$, is generated by

$$(\{q_0,q_1,q_2,q_3\},M,S,P),$$

where

$$M=\begin{pmatrix}z & z\\ z & 0\end{pmatrix}\odot\begin{pmatrix}0 & z\\ z & 0\end{pmatrix}=\begin{pmatrix}0 & z & 0 & z\\ z & 0 & z & 0\\ 0 & z & 0 & 0\\ z & 0 & 0 & 0\end{pmatrix},\quad P=\begin{pmatrix}0\\0\\ \varepsilon\\0\end{pmatrix},\quad S=(\varepsilon,0,0,0).$$

Consider the automaton

$$(\{q_0,q_1,q_2,q_3\},M^2,S,P).$$

This automaton is equivalent to

$$(\{q_0,q_2\}, \begin{pmatrix} 2z^2 & z^2 \\ z^2 & z^2 \end{pmatrix}, (\varepsilon,0), \begin{pmatrix} 0 \\ \varepsilon \end{pmatrix}).$$

Substituting z for z^2 yields an A<z>-finite-automaton generating (F_{2n}). Inspection shows that this automaton and the automaton of (i) are isomorphic. □

Example 5.3. Consider the $\mathbb{N}$<z>-automata $\mathcal{P}_1=(\mathbb{N},M,S,P)$ and $\mathcal{P}_2=(\mathbb{N},M \oplus (z),S,P)$, where $S=(\varepsilon,0,0,\ldots)$,

$$P = \begin{pmatrix} \varepsilon \\ 0 \\ 0 \\ \cdot \\ \cdot \end{pmatrix} \quad \text{and} \quad M = \begin{pmatrix} 0 & z & 0 & 0 & \cdot & \cdot & \cdot \\ z & 0 & z & 0 & \cdot & \cdot & \cdot \\ 0 & z & 0 & z & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

The automata $\mathcal{P}_1$ and $\mathcal{P}_2$ are "almost" pushdown automata. (Add an extra state and an edge labeled by z from state 0 to this extra state.)

By the construction in the proof of Theorem 4.7, we obtain
$\|\mathcal{P}_1\|=z^2\|\mathcal{P}_1\|^2+\varepsilon$, $\|\mathcal{P}_2\|=z^2\|\mathcal{P}_2\|^2+z\|\mathcal{P}_2\|+\varepsilon$,

$(\|\mathcal{P}_1\|,z^{2n}) = \frac{(2n)!}{n!(n+1)!}$ and $(\|\mathcal{P}_2\|,z^n) = \binom{n,3}{n}-\binom{n,3}{n-2}$, where $\binom{n,3}{k}$ is a triomial coeffizient (see Kuich [14],Prodinger [18]).

Observe that $\mathcal{P}_2=\mathcal{P}_1 \sqcup\!\sqcup \mathcal{Q}$, where $\mathcal{Q}=(\{q\},(z),(\varepsilon),(\varepsilon))$.

Hence,

$$\sum_{k=0}^{n} \binom{n}{k} (\|\mathcal{P}_1\|,z^k) = \binom{n,3}{n}-\binom{n,3}{n-2},$$

i.e.,

$$\sum_{k=0}^{[n/2]} \binom{n}{2k} C_k = \binom{n,3}{n}-\binom{n,3}{n-2},$$

where $C_k = \frac{(2k)!}{k!(k+1)!}$ is a Catalan number. □

Example 5.4. Given a language $L \subseteq \Sigma^*$, define the language

$D(L)=\{w \in \Sigma^* \mid$ there exist $v_1 \in L$ and $v_2 \in \Sigma^*$ such that $w \in v_1 \sqcup\!\sqcup v_2\}$.

The words of Σ^*-D(L) are called totally clean by Zeilberger [24]. Zeilberger [24] computes the weight enumerator of Σ^*-D(L) in case L is finite. We will extend this to the case of a regular language L: D(L) is then again a regular language and enumerating functions are easily computed. (Of course this is valid for Σ^*-D(L), too.)

Let $\mathcal{A}'=(Q',M',q_0',P')$ be an $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$-finite-automaton whose behavior is $\mathrm{char}(L)$. Let $M'' \in (\mathbb{B}\langle\langle\Sigma^*\rangle\rangle)^{Q\times Q}$ be the diagonal matrix defined by $M''_{q_1,q_2} = \delta_{q_1,q_2}\cdot\mathrm{char}(\Sigma)$ and let $\mathcal{A}''=(Q',M'+M'',q_0',P')$. Then $D(L)=\mathrm{supp}\|\mathcal{A}''\|$.

Finally, let $\mathcal{A}=(Q,M,q_0,P)$ be a deterministic $\mathbb{B}\langle\langle\Sigma^*\rangle\rangle$-finite-automaton with $\|\mathcal{A}\| = \mathrm{char}(D(L))$ (easily constructed from $\mathcal{A}''$).

Consider now $\mathcal{A}$ to be an $\mathbb{N}\langle\langle\Sigma^*\rangle\rangle$-finite-automaton. Again we obtain $\|\mathcal{A}\| = \mathrm{char}(D(L))$, but now $\|\mathcal{A}\| \in \mathbb{N}\langle\langle\Sigma^*\rangle\rangle$. Since $\|\mathcal{A}\| = (M^*P)_{q_0}$, the weight enumerator of $D(L)$ and the structure generating function of $D(L)$ are easily computed (see Kuich [14]).

We take the example from Zeilberger [24]. Let $\Sigma=\{x_1,x_2,x_3\}$ and $L=\{x_1x_2x_3\}$. Then

$$M = \begin{pmatrix} x_2+x_3 & x_1 & 0 & 0 \\ 0 & x_1+x_3 & x_2 & 0 \\ 0 & 0 & x_1+x_2 & x_3 \\ 0 & 0 & 0 & x_1+x_2+x_3 \end{pmatrix} \quad \text{and} \quad P = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \varepsilon \end{pmatrix},$$

where q_0 corresponds to the first row and column. We obtain

$$\|\mathcal{A}\| = (x_2+x_3)^*x_1(x_1+x_3)^*x_2(x_1+x_2)^*x_3(x_1+x_2+x_3)^*.$$

Hence, the weight enumerator of $D(L)$ is given by

$$x_1x_2x_3(1-x_2-x_3)^{-1}(1-x_1-x_3)^{-1}(1-x_1-x_2)^{-1}(1-x_1-x_2-x_3)^{-1}.$$

The structure generating function of $D(L)$ is given by

$$z^3(1-3z)(1-2z)^{-3}.$$

Similar computations can be done with clean words (see Zeilberger [24], "second standard"): construct a deterministic finite automaton $\mathcal{A}$ for $\mathrm{char}(\Sigma^*L\Sigma^*)$. □

REFERENCES.

[1] Berstel, J. and Reutenauer, C., Les series rationnelles et leur langages, Masson, 1984.

[2] Bucher, W. and Maurer, H., Theoretische Grundlagen der Programmiersprachen, Bibliographisches Institut, 1984.

[3] Chomsky, N. and Schützenberger, M.P., The algebraic theory of context-free languages, in Computer Programming and Formal Systems (P.Braffort and D.Hirschberg, Eds.), North Holland, 1963, 118-161.

[4] Conway, J.H., Regular Algebra and Finite Machines, Chapman and Hall, 1971.

[5] Eilenberg, S., Automata, Languages and Machines, Vol.A., Academic Press, 1974.

[6] Flajolet, P., Mathematical methods in the analysis of algorithms and data structures, Lecture Notes for "A Graduate Course on Computation Theory", Udine, 1984.

[7] Ginsburg, S., Algebraic and Automata-Theoretic Properties of Formal Languages, North Holland, 1975.

[8] Goldman, J.R., Formal languages and enumeration, Journal of Comb.Theory, Serie A 24(1978), 318-338.

[9] Goulden, I. and Jackson, M., Combinatorial Enumeration, John Wiley, 1983.

[10] Harrison, S.A., Introduction to Formal Language Theory, Addison-Wesley, 1978.

[11] Hopcroft, J.E. and Ullman, J.D., Introduction to Automata Theory, Languages and Computation, Addison-Wesley, 1979.

[12] Hotz, W. and Estenfeld, K., Formale Sprachen, Bibliographisches Institut, 1981.

[13] Klarner, D.A., A ring of sequences generated by rational functions, Am.Math.Monthly 74(1967), 813-816.

[14] Kuich, W., On the entropy of context-free languages, Inf.Control 16(1970), 173-200.

[15] Kuich, W. and Salomaa, A., Semirings, Automata, Languages, Springer, 1986.

[16] Küster, G., Das Hadamardprodukt abstrakter Familien von Potenzreihen, Dissertation Technische Universität Wien, 1986.

[17] v.Mangoldt, H. and Knopp, K., Einführung in die höhere Mathematik, I.Band, Hirzel, 1979(16.Auflage).

[18] Prodinger, H., Einige Bemerkungen zu einer Arbeit von W.Knödel über das mittlere Verhalten von on-line-Packungsalgorithmen, EIK 21(1985), 3-7.

[19] Salomaa, A., Formal Languages, Springer, 1973.

[20] Salomaa, A., Computation and Automata, Addison-Wesley, 1985.

[21] Salomaa, A. and Soittola, M., Automata-Theoretic Aspects of Formal Power Series, Springer, 1978.

[22] Straubing, H., Applications of the theory of automata in enumeration, Discrete Math.64(1987), 269-279.

[23] Wechler, W., The Concept of Fuzziness in Automata and Language Theory, Akademie-Verlag, 1978.

[24] Zeilberger, D., Enumerating totally clean words, Discrete Math. 64(1987), 313-315.

Werner Kuich

Institut für Algebra u.Diskrete Mathematik
Abt.Theoretische Informatik
Technische Universität Wien

A-1040 Wien, Wiedner Hauptstr.8-10

Österreich