**Basic Research in Computer Science**



# Rationally Additive Semirings

**Zoltán Ésik**
**Werner Kuich**

**BRICS Report Series** **RS-01-42**

**ISSN 0909-0878** **November 2001**

**See back inner page for a list of recent BRICS Report Series publications.**
**Copies may be obtained by contacting:**

**BRICS**
**Department of Computer Science**
**University of Aarhus**
**Ny Munkegade, building 540**
**DK–8000 Aarhus C**
**Denmark**
**Telephone: +45 8942 3360**
**Telefax: +45 8942 3255**
**Internet: BRICS@brics.dk**

**BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:**

`http://www.brics.dk`
`ftp://ftp.brics.dk`
**This document in subdirectory** `RS/01/42/`

# Rationally Additive Semirings

Zoltán Ésik[1]
(Department of Computer Science, The University of Szeged, Árpád tér 2,
H-6720 Szeged, Hungary.
Email: esik@inf.u-szeged.hu.)

Werner Kuich[2]
( Institut für Algebra und Computermathematik, Technische Universität Wien,
Wiedner Hauptstraße 8–10, A-1040 Wien, Austria.
Email: kuich@tuwien.ac.at.)

**Abstract:** We define rationally additive semirings that are a generalization of ($\omega$)-complete and ($\omega$-)continuous semirings. We prove that every rationally additive semiring is an iteration semiring. Moreover, we characterize the semirings of rational power series with coefficients in $N_\infty$, the semiring of natural numbers equipped with a top element, as the free rationally additive semirings.

**Key Words:** semiring, complete semiring, iteration semiring, fixed point, power series.

**Category:** F.4.3

## 1 Introduction

Rationally additive semirings arise in [Mohri 1998]. Rationally additive semiring possess enough infinite sums to solve any finite system of linear fixed point equations. They are a common generalization of ($\omega$)-complete and ($\omega$-)continuous semirings [see Eilenberg 1974, Kuich 1987, Sakarovitch 1987, Kuich 1997] in which all (countable) sums exist. Two prime examples of rationally additive semirings are the semiring of rational (or regular) sets in $A^*$, where $A$ is any set, and the semiring $N_\infty^{rat}\langle\langle A^*\rangle\rangle$ of rational power series over $A$ with coefficients in $N_\infty$, the semiring of natural numbers with a top element $\infty$.

In our main result, Theorem 10, we prove that every rationally additive semiring is an iteration semiring. This fact extends a result of [Hebisch 1990] by which every complete semiring is a Conway semiring. Iteration semirings appear implicitly in [Conway 1971]. They were explicitly defined in [Bloom, Ésik 1993a, 1993b]. Conway conjectured that a complete axiomatization of the equational theory of rational (regular) languages consists of the Conway semiring equations, defined below, together with the equation $1^* = 1$ and an equation associated with each finite group. Conway's conjecture was confirmed in [Krob 1991], see also [Ésik 1999]. In [Bloom, Ésik 1997], the authors conjectured that the valid equations of

[1] Partially supported by BRICS, Aalborg, Denmark, grant no. T30511 from the National Foundation of Hungary for Scientific Research, grant no. A-4/1999 from the Austrian-Hungarian Bilateral Research and Development Fund, and by a grant from the Austrian-Hungarian Action Foundation.

[2] Partially supported by grant no. A-4/1999 from the Austrian-Hungarian Bilateral Research and Development Fund and by a grant from the Austrian–Hungarian Action Foundations.

rational power series with coefficients in $N_\infty$, the semiring of natural numbers equipped with a top element, can be axiomatized by the iteration semiring equations and the equation $1^* = 1^{**}$. This conjecture is still open. In Theorem 15, we characterize the semirings of rational power series with coefficients in $N_\infty$ as the free rationally additive semirings.

## 2 Conway semirings and iteration semirings

A $^*$-*semiring* is a semiring [see Kuich, Salomaa 1986, Golan 1992] $S = (S, +, \cdot, 0, 1)$ equipped with a star operation $^* : S \to S$. A *Conway semiring* [Bloom, Ésik 1993b] is a $^*$-semiring $S$ which satisfies the *sum-star* and *product-star* equations

$$(x + y)^* = (x^* y)^* x^* \tag{1}$$
$$(xy)^* = 1 + x(yx)^* y. \tag{2}$$

Note that the *fixed point equation*

$$x^* = 1 + xx^* \tag{3}$$

holds in any Conway semiring. (Substitute 1 for $y$ in (2).)

Suppose that $S$ is a $^*$-semiring and $n \geq 0$. We turn the matrix semiring $S^{n\times n}$ into a $^*$-semiring. Let $M \in S^{n\times n}$. When $n = 0$, $M^*$ is the unique $0 \times 0$ matrix, and when $M = [\, a \,]$, then $M^* = [\, a^* \,]$. Suppose now that $n > 1$. Write $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a$ is $(n-1) \times (n-1)$ and $d$ is $1 \times 1$. We define

$$M^* = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{4}$$

where

$$\begin{aligned} \alpha &= (a + bd^* c)^* \\ \beta &= \alpha b d^* \\ \gamma &= \delta c a^* \\ \delta &= (d + ca^* b)^*. \end{aligned}$$

**Theorem 1.** [Conway 1971, Bloom, Ésik 1993] *If $S$ is a Conway semiring, then so is each matrix semiring $S^{n\times n}$. Moreover, the above matrix formula (4) holds for each way of splitting $M$ into four blocks $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $a$ and $d$ are square matrices.*

Suppose that $G$ is a finite group of order $n$ with elements $g_1, \ldots, g_n$. For each $g_i$, let $x_i$ denote a variable associated with $g_i$. We define $M_G = [\, (M_G)_{ij} \,]$, where $(M_G)_{ij}$ is the variable associated with the group element $g_i^{-1} g_j$, i.e., $(M_G)_{ij} = x_k$ where $g_k = g_i^{-1} g_j$. The matrix $M_G^*$ is defined as in (4) above, so that each entry of $M_G^*$ is a term in the variables $x_1, \ldots, x_n$.

The *group-equation associated with* $G$ [see Conway 1971] is the equation

$$e \cdot M_G^* \cdot u = (x_1 + \ldots + x_n)^*,$$

where $e$ is the $1 \times n$ row matrix whose first entry is 1 and whose other entries are 0, and where $u$ is the $n \times 1$ column matrix whose entries are all 1. (Under the Conway semiring equations (1) and (2), the particular order $g_1, \ldots, g_n$ of the group elements is irrelevant.)

An *iteration semiring* [see Bloom, Ésik 1993, Ésik 1999] is a Conway semiring satisfying all group-equations.

**Proposition 2.** [Bloom, Ésik 1993b] *Any Conway semiring $S$ satisfying the* functorial implication

$$AC = CB \Rightarrow A^*C = CB^*,$$

*for all matrices $A \in S^{n\times n}$, $B \in S^{m\times m}$ and $C \in S^{n\times m}$, is an iteration semiring.*

**Notation** For each nonnegative integer $n$, we denote the set $\{1, \ldots, n\}$ by $[n]$. Thus, $[0]$ is another name for the empty set.

For any set $\Sigma$, we denote by $\Sigma^*$ the free monoid of all words over $\Sigma$ including the empty word $\epsilon$. When $S$ is semiring, $S\langle\langle A^*\rangle\rangle$ denotes the semiring of all power series over $A$ with coefficients in $S$. Moreover, we let $S\langle A\rangle$ denote the collection of all finite sums of terms of the form $sa$ with $s \in S$ and $a \in \Sigma$.

## 3 Rationally additive semirings

A *weak rationally additive semiring* is a semiring $S$ equipped with a partial summation $\sum_{i\in I} s_i$ defined on countable families $s_i \in S$, $i \in I$ subject to the following conditions:

- $\mathbf{Ax}_1$. When $s_i \in S$ for $i \in F$ and $F$ is finite, then $\sum_{i\in F} s_i$ is the sum of the $s_i$ as defined in the semiring $S$.
- $\mathbf{Ax}_2$. For each $s \in S$, the geometric sum $\sum_{n=0}^{\infty} s^n$ exists.
- $\mathbf{Ax}_3$. If $\sum_{i\in I} s_i$ exists, then so do $\sum_{i\in I} ss_i$ and $\sum_{i\in I} s_i s$, for each $s \in S$, moreover,

$$s(\sum_{i\in I} s_i) = \sum_{i\in I} ss_i$$
$$(\sum_{i\in I} s_i)s = \sum_{i\in I} s_i s.$$

- $\mathbf{Ax}_4$. Suppose that the countable set $I$ is the disjoint union of the sets $I_j$, $j \in J$. Then for any family $s_i \in S$, $i \in I$, if $r_j = \sum_{i\in I_j} s_i$ exists for each $j \in J$, and if $r = \sum_{j\in J} r_j$ exists, then $\sum_{i\in I} s_i$ also exists and equals $r$.

A *rationally additive semiring* is a weak rationally additive semiring $S$ that satisfies:

– $\mathbf{Ax}_5$. Suppose that the countable set $I$ is the disjoint union of the sets $I_j$, $j \in J$. Then for any family $s_i \in S$, $i \in I$, if $s = \sum_{i\in I} s_i$ exists and $r_j = \sum_{i\in I_j} s_i$ exist, for all $j \in J$, then $\sum_{j\in J} r_j$ exists and equals $s$.

**Proposition 3.** *Suppose that $S$ is a weak rationally additive semiring.*

- *For any countable families $s_i$, $i \in I$ and $r_j$, $j \in J$, if $\sum_{i\in I} s_i = s$ and $\sum_{j\in J} r_j = r$ exist, then so does $\sum_{(i,j)\in I\times J} s_i r_j$. Moreover, $\sum_{(i,j)\in I\times J} s_i r_j = sr$.*
- *For any countable families $s_i \in S$ and $s'_j \in S$ with $i \in I$ and $j \in J$, if there is a bijection $\pi : I \to J$ with $s_i = s'_{i\pi}$, for all $i \in I$, then $\sum_{i\in I} s_i$ exists iff $\sum_{j\in J} s'_j$ does, in which case the two sums are equal.*
- *Any countable sum $\sum_{i\in I} s$ exists. Moreover, $\sum_{i\in I} 0 = 0$, i.e., any countable sum of 0 with itself is 0.*
- *For any countable family $s_i$, $i \in I$, if $\sum_{j\in J} s_j = r$ exists, where $J$ is the set of all $i \in I$ with $s_i \neq 0$, then $\sum_{i\in I} s_i$ exists and equals $r$.*

*Proof.* The first claim follows from $\mathbf{Ax}_3$ and $\mathbf{Ax}_4$. For the second, suppose that $\sum_{i\in I} s_i = s$ exists. Let $J_i = \{i\pi\}$, for each $i \in I$. Thus the sets $J_i$ determine a partition of $J$. Each sum $\sum_{k\in J_i} s'_k = s'_{i\pi} = s_i$ exists, moreover, $\sum_{i\in I} s_i$ exists. Thus, by $\mathbf{Ax}_4$, we have that $\sum_{j\in J} s'_j$ exists and equals $\sum_{i\in I} s_i$. In the same way, it follows that if $\sum_{j\in J} s'_j$ exists then $\sum_{i\in I} s_i$ also exists. For the third claim, assume first that $s = 1$. If $I$ is finite with $n$ elements, then $\sum_{i\in I} s = \sum_{i\in I} 1$ exists by $\mathbf{Ax}_1$, and equals the usual $n$-fold sum of 1 with itself. Assume now that $I$ is infinite. Then $\sum_{i\in I} s = \sum_{i\in I} 1 = \sum_{i=0}^{\infty} 1^i$ exists by $\mathbf{Ax}_2$. Thus for any $s$, we have that $\sum_{i\in I} s = \sum_{i\in I}(s \cdot 1) = s(\sum_{i\in I} 1)$ exists. When $s$ is 0, this sum is also 0. The last claim now follows from $\mathbf{Ax}_4$. □

*Remark.* When $S$ is rationally additive, the converse of the last fact also holds, so that using the same notation, $\sum_{j\in J} s_j$ exists iff $\sum_{i\in I} s_i$ exists.

Suppose that $S$ and $S'$ are (weak) rationally additive semirings. A homomorphism $h : S \to S'$ is a semiring homomorphism that preserves all existing countable sums. Thus, if $\sum_{i\in I} s_i$ exists, where $s_i \in S$ for each $i \in I$, then so does $\sum_{i\in I} s_i h$ and $(\sum_{i\in I} s_i)h = \sum_{i\in I} s_i h$.

*Example 1.* A countably additive (or $\omega$-complete) semiring is a rationally additive semiring $S$ such that $\sum_{i\in I} s_i$ exists for all countable families $s_i \in S$, $i \in I$. For example, the power set semiring of a semiring is countably additive, where summation is defined by set union. An example of a rationally additive semiring which is not countably additive is the semiring of regular sets in $A^*$, where $A$ is any set. In this semiring only those sums (unions) exist that are regular languages. An $\omega$-continuous (or just continuous) semiring is a countably additive semiring which is naturally ordered and such that $\sum_{i\in I} s_i$ is the supremum of the finite sums $\sum_{i\in F} s_i$, for all finite subsets $F \subseteq I$. Since any countably additive semiring is rationally additive, so is any $\omega$-continuous semiring. For more on complete and continuous semirings, the reader is referred to [Eilenberg 1974, Kuich 1987, Sakarovitch 1987, Kuich 1997].

*Example 2.* A prime example of a countably additive semiring is the semiring $N_\infty = \{0, 1, \ldots, \infty\}$ obtained by adding a top element to the natural numbers $N$ equipped with the following summation. For all $n_i \in N_\infty$, $i \in I$, where $I$ is countable, define $\sum_{i\in I} n_i = \infty$ if $n_i = \infty$ for some $i$, or if $n_i > 0$ for infinitely many numbers $i$. Otherwise let $\sum_{i\in I} n_i$ be the ordinary sum. Note that all countable sums exist in $N_\infty$. Moreover, we have $x \cdot \infty = \infty \cdot x = \infty$ for all $x \neq 0$. We call the above countably additive structure on $N_\infty$ the *standard countably additive structure*.

*Remark.* The same semiring $S$ may sometimes be turned into a weak rationally additive semiring in several different ways. Suppose that we have a weak rationally additive structure on $S$ with summation denoted $\sum$. Then there is a smallest weak rationally additive structure on $S$ contained in $\sum$. If we denote the summation operation of this structure by $\sum'$, we have that $\sum'_{i\in I} s_i$ exists iff $I$ is finite, or there is an element $s \in S$ such that for some linear order $i_0, i_1, \ldots$ of the set $I$, we have that $s_{i_n} = s^n$, for all $n \geq 0$, or there is a family $s'_i$, $i \in I$ and an element $s' \in S$ such that either $s_i = s'_i s'$ for all $i$ or $s_i = s' s'_i$ for all $i$, or there exist disjoint sets $I_j$, $j \in J$ with $I = \cup_{j\in J} I_j$ such that $r_j = \sum'_{i\in I_j} s_j$ exists for each $j \in J$ and $\sum'_{j\in J} r_j$ exists. In either case, $\sum'_{i\in I} s_i$, when exists, is defined to be $\sum_{i\in I} s_i$. In the same way, each rationally additive structure on $S$ contains a least rationally additive structure.

*Remark.* There exists a weak rationally additive semiring which is not rationally additive. For one example, take the (standard) countably additive semiring $N_\infty$ defined above. It will be shown below in Corollary 14 that $N_\infty$ has no other rationally additive structure properly included in the standard structure. On the other hand, consider the least weak rationally additive structure contained in it. Let $\sum'$ denote the corresponding summation. Then there is only a countable number of sets $K \subseteq N$ such that $\sum'_{k\in K} k$ exists. Hence this weak additive semiring structure is not the standard countably additive structure.

In any (weak) rationally additive semiring, we define

$$\begin{aligned} {}^* : S &\to S \\ s &\mapsto \sum_{n=0}^{\infty} s^n. \end{aligned}$$

It is clear that morphisms of (weak) rationally additive semirings preserve the $^*$-operation.

**Proposition 4.** *Any weak rationally additive semiring $S$ is a Conway semiring.*

*Proof.* Suppose that $a, b \in S$ and let $\overline{a}$ and $\overline{b}$ denote distinct letters corresponding to $a$ and $b$, respectively. Below we will use regular languages in $(\overline{a} + \overline{b})^*$ as index sets. For any word $\overline{w} \in (\overline{a} + \overline{b})^*$, let $w$ denote the corresponding element in $S$. Since $(a + b)^* = \sum_{n=0}^{\infty} (a + b)^n$ exists, it follows by $\mathbf{Ax}_4$ that $\sum_{\overline{w}\in(\overline{a}+\overline{b})^*} w$ also exists, and $(a + b)^* = \sum_{\overline{w}\in(\overline{a}+\overline{b})^*} w$. Let us partition $(\overline{a} + \overline{b})^*$ into the disjoint union of the sets $L_k = (\overline{a}^* \overline{b})^k \overline{a}^*$, $k \geq 0$. It follows by $\mathbf{Ax}_2$ and $\mathbf{Ax}_3$ that each

sum $\sum_{\overline{w}\in L_k} w$ exists, and $\sum_{\overline{w}\in L_k} w = (a^*b)^k a^*$. Thus, again by $\mathbf{Ax}_2$ and $\mathbf{Ax}_3$, $\sum_{k=0}^{\infty}(a^*b)^k a^* = (a^*b)^* a^*$ exists. Since for each $k$ we have $\sum_{\overline{w}\in L_k} w = (a^*b)^k a^*$, it follows from $\mathbf{Ax}_4$ that $\sum_{\overline{w}\in L} w = (a^*b)^* a^*$. Hence $(a+b)^* = \sum_{\overline{w}\in L} w = (a^*b)^* a^*$.

Also, $\sum_{k=0}^{\infty} a(ba)^k b = a(\sum_{k=0}^{\infty}(ba)^k)b = a(ba)^* b$ exists, hence by $\mathbf{Ax}_4$, $(ab)^* = \sum_{k=0}^{\infty}(ab)^k = 1 + \sum_{k=0}^{\infty} a(ba)^k b = 1 + a(ba)^* b$. □

**Corollary 5.** *The* fixed point equation *(3) holds in any weak rationally additive semiring.*

**Proposition 6.** *Any weak rationally additive semiring $S$ satisfies $1^* = 1^{**}$, $1^*1^* = 1^*$ and $1^* + 1^* = 1^*$.*

*Proof.* Equation $1^* + 1^* = 1^*$ follows from $\mathbf{Ax}_4$. By Proposition 3,

$$1^*1^* = (\sum_{i=0}^{\infty} 1)(\sum_{i=0}^{\infty} 1) = \sum_{i,j=0}^{\infty} 1 = \sum_{k=0}^{\infty} 1 = 1^*,$$

and by $\mathbf{Ax}_3$,

$$1^*1^* = \sum_{i=0}^{\infty}\sum_{j=0}^{\infty} 1.$$

Hence, $(1^*)^n = 1^*$, for all $n \geq 1$. Moreover,

$$1^{**} = 1 + \sum_{n=1}^{\infty}(1^*)^n = 1 + \sum_{n=0}^{\infty} 1^* = 1 + \sum_{n=0}^{\infty}\sum_{m=0}^{\infty} 1 = 1 + 1^* = 1^*,$$

where the last step follows from the fixed point equation. □

*Remark.* In fact, the equations $1^*1^* = 1^*$ and $1^* + 1^* = 1^*$ hold in any Conway semiring satisfying $1^{**} = 1^*$.

Suppose that $S$ is a weak rationally additive semiring. Then, as shown above, $S$ is a Conway semiring. Thus, by Theorem 9, the semirings $S^{n\times n}$, $n \geq 0$ are also Conway semirings. Moreover, for each decomposition of a matrix $A \in S^{n\times n}$ in the form $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a$ and $d$ are square matrices, we have

$$A^* = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{5}$$

where

$$\begin{aligned} \alpha &= (a + bd^*c)^* \\ \beta &= \alpha b d^* \\ \gamma &= \delta c a^* \\ \delta &= (d + ca^*b)^*. \end{aligned}$$

Suppose now that $S$ is rationally additive. We turn $S^{n\times n}$ into a rationally additive semiring. Suppose that $A_i \in S^{n\times n}$, $i \in I$ where $I$ is countable. We say

that $\sum_{i\in I} A_i$ exists if $\sum_{i\in I}(A_i)_{jk}$ exists for all $j,k \in [n]$. Moreover, we define $(\sum_{i\in I} A_i)_{jk} = \sum_{i\in I}(A_i)_{jk}$, for each $j,k \in [n]$. We define the summation on countable families of matrices in $S^{n\times m}$, for $n, m \geq 0$ in the same way.

**Proposition 7.** *Suppose that $S$ is rationally additive. If $A_i \in S^{n\times m}$, $i \in I$ such that $\sum_{i\in I} A_i$ exists, then for any $B \in S^{m\times p}$, $\sum_{i\in I} A_i B$ exists and equals $(\sum_{i\in I} A_i)B$.*

*Proof.* It suffices to prove the proposition for $p = 1$. We argue by induction on $m$. The case that $m = 0$ is trivial. When $m = 1$, the proposition holds by $\mathbf{Ax}_3$. Suppose now that $m > 1$. Then let $m = m_1 + m_2$, where $m_1, m_2 < m$, and let us write $A_i = [\,a_i\ b_i\,]$, $i \in I$, and $B = \begin{bmatrix} x \\ y \end{bmatrix}$, where $a_i$ is $n \times m_1$, etc. Let $a = \sum_{i\in I} a_i$ and $b = \sum_{i\in I} b_i$, so that $A = \sum_{i\in I} A_i = [\,a\ b\,]$. By the induction assumption, both $\sum_{i\in I} a_i x$ and $\sum_{i\in I} b_i y$ exist, moreover, $\sum_{i\in I} a_i x = ax$ and $\sum_{i\in I} b_i y = by$. Since $\mathbf{Ax}_5$ holds in $S$, it follows that $\sum_{i\in I}(a_i x + b_i y)$ exists and equals $ax + by$. Thus, $\sum_{i\in I} A_i B = (\sum_{i\in I} A_i)B$ exists. Note that only a weak form of $\mathbf{Ax}_5$ was used: the case when each set $I_j$ is finite. □

In the same way, we have:

**Proposition 8.** *Suppose that $S$ is rationally additive. If $A_i \in S^{n\times m}$, $i \in I$ such that $\sum_{i\in I} A_i$ exists, then for any $B \in S^{p\times n}$, $\sum_{i\in I} BA_i$ exists and equals $B(\sum_{i\in I} A_i)$.*

**Theorem 9.** *When $S$ is rationally additive, so is $S^{n\times n}$, for any $n \geq 0$. Moreover, for the star operation defined in (5), we have*

$$A^* = \sum_{k=0}^{\infty} A^k.$$

*Proof.* Our claims are clear for $n = 0, 1$. We proceed by induction on $n$. Assume that $n > 1$. It is clear that $\mathbf{Ax}_1$, $\mathbf{Ax}_4$ and $\mathbf{Ax}_5$ hold in $S^{n\times n}$. The fact that $\mathbf{Ax}_3$ holds was shown above.

Suppose now that $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in S^{n\times n}$, where $a, b, c, d$ are submatrices of $A$ such that $a$ and $d$ are square matrices of size smaller than $n$. We want to show that $\sum_{k=0}^{\infty} A^k = A^*$, i.e., that $\sum_{k=0}^{\infty} A^k$ exists and

$$\sum_{k=0}^{\infty} A^k = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$$

where $\alpha$, $\beta$, $\gamma$ and $\delta$ were given as above. We will only show that the submatrix of $\sum_{k=0}^{\infty} A^k$ at the left upper corner exists and equals $\alpha$.

Consider the regular language $L = (\overline{a} + \overline{bd}^*\overline{c})^*$. Then $L$ is the union of the disjoint sets $L_1^k$, $k \geq 0$, where $L_1 = \overline{a} + \overline{bd}^*\overline{c}$. By the induction assumption,

$$a + bd^*c = a + b(\sum_{j=0}^{\infty} d^j)c = a + \sum_{j=0}^{\infty} bd^j c = a + \sum_{\overline{w}\in\overline{bd}^*\overline{c}} w = \sum_{\overline{w}\in L_1} w.$$

Hence, by Proposition 7 and Proposition 8,

$$(a + bd^*c)^2 = (\sum_{\overline{w}\in L_1} w)(\sum_{\overline{w}\in L_1} w) = \sum_{\overline{u},\overline{v}\in L_1} uv = \sum_{\overline{w}\in L_1^2} w,$$

since each word in $L_1^2$ has a unique factorization as a product of two words in $L_1$. In the same way, it follows that

$$(a + bd^*c)^k = \sum_{\overline{w}\in L_1^k} w,$$

for all $k \geq 0$. Thus, by the induction assumption,

$$(a + bd^*c)^* = \sum_{k=0}^{\infty}(a + bd^*c)^k = \sum_{k=0}^{\infty}\sum_{\overline{w}\in L_k} w = \sum_{\overline{w}\in L} w.$$

In particular, $\sum_{\overline{w}\in L} w$ exists. Now let us write $A^k = \begin{bmatrix} a_k & b_k \\ c_k & d_k \end{bmatrix}$, $k \geq 0$. To complete the proof, we need show that $\sum_{k=0}^{\infty} a_k$ exists and equals $\sum_{\overline{w}\in L} w$. But for each $k$, $a_k = \sum_{\overline{w}\in L,\ |\overline{w}|=k} w$. Thus, since $\mathbf{Ax}_5$ holds by the induction assumption, $\sum_{k=0}^{\infty} a_k$ exists and equals $\sum_{\overline{w}\in L} w$. (Again note that only the weak form of $\mathbf{Ax}_5$ when the sets $I_j$ are finite has been used.) □

**Theorem 10.** *Any rationally additive semiring $S$ is an iteration semiring satisfying $1^* = 1^{**}$.*

*Proof.* We have already proved that any rationally additive semiring $S$ is a Conway semiring and satisfies $1^* = 1^{**}$. The fact that the group-equations hold follows from the functorial implication, see Proposition 2, which can be established as follows. Suppose that $A \in S^{n\times n}$, $B \in S^{m\times m}$ and $C \in S^{n\times m}$ with $AC = CB$. Then $A^kC = CB^k$, for all $k \geq 0$. Thus, by Propositions 7 and 8,

$$A^*C = (\sum_{k=0}^{\infty} A^k)C = \sum_{k=0}^{\infty} A^kC = \sum_{k=0}^{\infty} CB^k = C(\sum_{k=0}^{\infty} B^k) = CB^*.$$

□

Assume that $S$ is a rationally additive semiring and $A$ is a set. We turn the power series semiring $S\langle\langle A^*\rangle\rangle$ into a rationally additive semiring. For any countable family $r_i \in S\langle\langle A^*\rangle\rangle$, $i \in I$, we say that $\sum_{i\in I} r_i$ is defined if the sum $\sum_{i\in I}(r_i, u)$ is defined for all $u \in A^*$. Moreover, in this case, we let $(\sum_{i\in I} r_i, u) = \sum_{i\in I}(r_i, u)$.

**Proposition 11.** *Suppose that $S$ is a rationally additive semiring and $A$ is a set. Then $S\langle\langle A^*\rangle\rangle$ is also a rationally additive semiring.*

*Proof.* We only show that $\mathbf{Ax}_2$ and $\mathbf{Ax}_3$ hold in $S\langle\langle A^*\rangle\rangle$. So suppose that $r \in S\langle\langle A^*\rangle\rangle$. We clearly have that

$$\sum_{n=0}^{\infty}(r^n, \epsilon) = \sum_{n=0}^{\infty}(r, \epsilon)^n = (r, \epsilon)^*.$$

Suppose now that $u \neq \epsilon$. Then $(r^n, u) = \sum_{u_1 \ldots u_n = u}(r, u_1) \ldots (r, u_n)$. Thus, by $\mathbf{Ax}_5$, $\sum_{n=0}^{\infty}(r^n, u)$ exists if the sum $\sum_{u_1 \ldots u_n = u,\ n \geq 0}(r, u_1) \ldots (r, u_n)$ does. But this latter sum indeed exists. This can be seen as follows. For each fixed $u_1, \ldots, u_k \neq \epsilon$ with $u_1 \ldots u_k = u$,

$$\sum_{m_0, \ldots, m_k \geq 0}(r, \epsilon)^{m_0}(r, u_1) \ldots (r, u_k)(r, \epsilon)^{m_k} = (r, \epsilon)^*(r, u_1) \ldots (r, u_k)(r, \epsilon)^*$$

exists. Since $\sum_{u_1 \ldots u_n = u}(r, u_1) \ldots (r, u_n)$ is just a finite sum of sums of this form, it follows by $\mathbf{Ax}_4$ that this sum also exists. Again, only a weak form of $\mathbf{Ax}_5$ has been used. □

The following fact is clear.

**Proposition 12.** *Suppose that $S$ is a (weak) rationally additive semiring and $S'$ is a subsemiring of $S$ which is closed under $^*$. Say that $\sum_{i \in I} s_i$ exists in $S'$, where $s_i \in S'$ for all $i \in I$, if $\sum_{i \in I} s_i$ exists in $S$ and belongs to $S'$, and in that case, let the sum in $S'$ be the same as in $S$. Then $S'$ is also a (weak) rationally additive semiring.*

When $S$ is a $^*$-semiring and $B \subseteq S$, the *$B$-rational elements* of $S$ are those contained in the $^*$-semiring generated by $B$. Thus the $B$-rational elements form a $^*$-semiring denoted $Rat_S(B)$, or just $Rat(B)$. Let $S$ be rationally additive and let $A$ be a set. Then, as shown above, $S\langle\langle A^*\rangle\rangle$ is also rationally additive and each $a \in A$ and $s \in S$ can be conveniently identified with a series in $S\langle\langle A^*\rangle\rangle$. We denote $S^{rat}\langle\langle A^*\rangle\rangle = Rat_{S\langle\langle A^*\rangle\rangle}(A \cup S)$.

The countably additive semiring $N_\infty$ was defined above.

**Proposition 13.** *Suppose that $S$ is rationally additive. Then there is a unique morphism $N_\infty \to S$.*

*Proof.* Clearly, any morphism $h : N_\infty \to S$ is forced to map each integer $n$ to the $n$-fold sum of 1 with itself and $\infty$ to $1^*$. The fact that this function is in turn a morphism will follow by Remark 3 once we prove that for any countably infinite family $n_i,\ i \in I$ of nonzero elements of $N_\infty$, the sum $\sum_{i \in I} n_i h$ exists in $S$ and equals $1^*$. But this follows by Proposition 3. □

**Corollary 14.** *There exits no rationally additive semiring structure on $N_\infty$ properly included in the standard structure.*

**Theorem 15.** *For each set $A$, $N_\infty^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is freely generated by $A$ in the class of rationally additive semirings.*

*Proof.* We need to show that if $S$ is a rationally additive semiring and $h$ is a function $A \to S$, then $h$ has a unique extension to a morphism $h^\sharp : N_\infty^{rat}\langle\langle A^*\rangle\rangle \to S$ of rationally additive semirings. Suppose that $r \in N_\infty^{rat}\langle\langle A^*\rangle\rangle$. We are forced to define

$$rh^\sharp = \sum_{(r,u)\neq 0} (r,u)uh, \tag{6}$$

where for any word $u = a_1 \dots a_n \in A^*$ of length $n$, we define $uh = (a_1 h) \cdot \dots \cdot (a_n h)$. Note that the coefficient $(r,u)$ of $uh$ in (6) is taken in $S$. This is meaningful, since to each integer $n$ there corresponds in $S$ the $n$-fold sum of 1 with itself, and to $\infty$ the element $1^*$. See Proposition 13.

In a natural way, we may extend $h$ to a function $N_\infty\langle A\rangle \to S$, and then to a function $(N_\infty\langle A\rangle)^{n\times n} \to S^{n\times n}$, for each $n \geq 0$. For each $n \in N_\infty$ and $a \in A$ we define $(na)h = n(ah)$. For a finite sum $\sum_{i\in F} n_i a_i$, we define $(\sum_{i\in F} n_i a_i)h = \sum_{i\in F} n_i(a_i h)$.

We must show that the sum on the right-hand side of (6) exists. Since $r$ is rational, by (a generalization of) Schützenberger's theorem [see Bloom, Ésik 1993b], there exists $\alpha \in N_\infty^{1\times n}$, $M \in N_\infty\langle A\rangle^{n\times n}$ and $\beta \in N_\infty^{n\times 1}$ with $r = \alpha M^*\beta$. Now, by Theorem 9 and Propositions 7 and 8, we have that $\alpha(Mh)^*\beta = \sum_{k=0}^\infty \alpha(Mh)^k\beta$ exists. But for each $k$,

$$\alpha(Mh)^k\beta = \sum_{|u|=k,\ (r,u)\neq 0} (r,u)uh.$$

Thus, by $\mathbf{Ax}_4$, the right-hand side of (6) exists and equals $\alpha(Mh)^*\beta$.

Note that for any finite set $B \subseteq A$ such that $u \in B^*$ holds for all words $u \in A^*$ with $(r,u) \neq 0$, i.e., such that $supp(r) \subseteq B^*$, we have that $rh^\sharp = \sum_{u\in B^*}(r,u)uh$. We use this fact in our proof that $h^\sharp$ preserves all existing sums. Suppose that $r_i \in N_\infty^{rat}\langle\langle A^*\rangle\rangle$, $i \in I$ such that $\sum_{i\in I} r_i$ exists in $N_\infty^{rat}\langle\langle A^*\rangle\rangle$, so that $\sum_{i\in I} r_i$ is rational. Since $r = \sum_{i\in I} r_i$ is rational, there is a finite set $B \subseteq A$ with $supp(r) \subseteq B^*$. Clearly then, $supp(r_i) \subseteq B^*$ for all $i \in I$. By $\mathbf{Ax}_4$ and $\mathbf{Ax}_5$, the fact that $\sum_{i\in I} r_i h^\sharp$ exists and equals $rh^\sharp$ will follow if we can show that the sum $\sum_{u\in B^*,\ i\in I}(r_i,u)uh$ exists and equals $rh^\sharp$. This in turn will hold if for each fixed $u \in B^*$,

$$\sum_{i\in I}(r_i,u)uh = (\sum_{i\in I}(r_i,u))uh$$

exists and is equal to $(r,u)uh$. But by Proposition 13, the sum $\sum_{i\in I}(r_i,u)$ exists in $S$, and equals $(r,u)$. □

**Corollary 16.** *There is no rationally additive structure on $N_\infty^{rat}\langle\langle A^*\rangle\rangle$ properly contained in the rationally additive structure inherited from the countably additive structure on $N_\infty\langle\langle A^*\rangle\rangle$.*

## References


1. [Bloom, Ésik 1993a] Bloom, S. L., Ésik, Z.: "Matrix and Matricial Iteration Theories"; *J. Computer and System Sciences*, 46, (1993), 381–408.

2. [Bloom, Ésik 1993b] Bloom, S. L., Ésik, Z.,: "Iteration Theories"; Springer-Verlag (1993).
3. [Bloom, Ésik 1997] Bloom, S. L., Ésik, Z.: "The Equational Logic of Fixed Points"; Theoretical Computer Science, 179, (1997), 1–60.
4. [Conway 1971] Conway, J: "Regular Algebra and Finite Machines"; Chapman and Hall (1971).
5. [Eilenberg 1974] Eilenberg, S.: "Automata, Languages and Machines", Vol. A; Academic Press (1974).
6. [Ésik 1999] Ésik, Z.: "Group Axioms for Iteration"; Information and Computation, 148 (1999), 131–180.
7. [Ésik, Kuich 2001] Ésik, Z., Kuich, W.: "Inductive $^*$-Semirings"; to appear.
8. [Golan 1992] Golan, J. S.: "The Theory of Semirings, With Applications in Mathematics and Computer Science"; Longman Scientific (1992).
9. [Hebish 1990] Hebisch, U.: "The Kleene Theorem in Countably Complete Semirings"; Bayreuth. Math. Schr., 31, (1990), 55–66.
10. [Krob 1991] Krob, D.: "Complete Systems of B-Rational Identities"; Theoretical Computer Science, 89, (1991), 207–343.
11. [Kuich 1987] W. Kuich: "The Kleene and the Parikh Theorem in Complete Semirings"; Proc. ICALP 87, LNCS 267, Springer-Verlag (1987), 212–225.
12. [Kuich 1997] Kuich, W.: "Semirings and Formal Power Series", Handbook of Formal Languages, Vol. 1, Springer-Verlag (1997), 609–677.
13. [Kuich, Salomaa 1986] Kuich, W., and Salomaa, A.: Semirings, Automata, Languages; Springer-Verlag (1986).
14. [Mohri 1998] Mohri, M.: "General Algebraic Frameworks for Short-Distance Problems"; Technical Report, AT & T Labs-Research (1998).
15. [Sakarovitch 1987] Sakarovitch, J.: "Kleene's Theorem Revisited"; Trends, Techniques, and Problems in Theoretical Computer Science, LNCS 281, Springer-Verlag (1987), 39–50.

# Recent BRICS Report Series Publications

**RS-01-42** **Zoltán Ésik and Werner Kuich.** ***Rationally Additive Semirings*****. November 2001. 11 pp.**

**RS-01-41** **Ivan B. Damgård and Jesper Buus Nielsen.** ***Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor*****. October 2001. 43 pp.**

**RS-01-40** **Daniel Damian and Olivier Danvy.** ***CPS Transformation of Flow Information, Part II: Administrative Reductions*****. October 2001. 9 pp.**

**RS-01-39** **Olivier Danvy and Mayer Goldberg.** ***There and Back Again*****. October 2001. 14 pp.**

**RS-01-38** **Zoltán Ésik.** ***Free De Morgan Bisemigroups and Bisemilattices*****. October 2001. 13 pp.**

**RS-01-37** **Ronald Cramer and Victor Shoup.** ***Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption*****. October 2001. 34 pp.**

**RS-01-36** **Gerth Stølting Brodal, Rolf Fagerberg, and Riko Jacob.** ***Cache Oblivious Search Trees via Binary Trees of Small Height*****. October 2001.**

**RS-01-35** **Mayer Goldberg.** ***A General Schema for Constructing One-Point Bases in the Lambda Calculus*****. September 2001. 6 pp.**

**RS-01-34** **Flemming Friche Rodler and Rasmus Pagh.** ***Fast Random Access to Wavelet Compressed Volumetric Data Using Hashing*****. August 2001. 31 pp.**

**RS-01-33** **Rasmus Pagh and Flemming Friche Rodler.** ***Lossy Dictionaries*****. August 2001. 14 pp. Short version appears in Meyer auf der Heide, editor,** ***9th Annual European Symposiumon on Algorithms*****, ESA '01 Proceedings, LNCS 2161, 2001, pages 300–311.**

**RS-01-32** **Rasmus Pagh and Flemming Friche Rodler.** ***Cuckoo Hashing*****. August 2001. 21 pp. Short version appears in Meyer auf der Heide, editor,** ***9th Annual European Symposiumon on Algorithms*****, ESA '01 Proceedings, LNCS 2161, 2001, pages 121–133.**