BRICS

Basic Research in Computer Science

BRICS RS-00-27 Ésik & Kuich: Inductive -Semirings

Inductive *-Semirings

Zoltán Ésik
Werner Kuich

BRICS Report Series **RS-00-27**

ISSN 0909-0878 **October 2000**

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/00/27/`

Inductive *-Semirings*

Z. Ésik†
Dept. of Computer Science
University of Szeged
Árpád tér 2
H-6720 Szeged
Hungary
email: esik@inf.u-szeged.hu

W. Kuich‡
Institut für Algebra und
Computermathematik
Technische Universität Wien
Wiedner Hauptstraße 8–10
A-1040 Wien
Austria
email: kuich@tu-wien.ac.at

October 2000

Abstract

One of the most well-known induction principles in computer science is the fixed point induction rule, or least pre-fixed point rule. Inductive *-semirings are partially ordered semirings equipped with a star operation satisfying the fixed point equation and the fixed point induction rule for linear terms. Inductive *-semirings are extensions of continuous semirings and the Kleene algebras of Conway and Kozen.

We develop, in a systematic way, the rudiments of the theory of inductive *-semirings in relation to automata, languages and power series. In particular, we prove that if S is an inductive *-semiring, then so is the semiring of matrices $S^{n\times n}$, for any integer $n \geq 0$, and that if S is an inductive *-semiring, then so is any semiring of power series $S\langle\langle A^*\rangle\rangle$. As shown by Kozen, the dual of an inductive *-semiring may not be inductive. In contrast, we show that the dual of an iteration semiring is an iteration semiring. Kuich proved a general Kleene theorem for continuous semirings, and Bloom and Ésik proved a Kleene theorem for all Conway semirings. Since any inductive *-semiring is a Conway semiring and an iteration semiring, as we show, there results a Kleene theorem

*The results of this paper were presented at the 3rd International Colloquium on Words, Languages and Combinatorics, Kyoto, March 2000.

†Partially supported by grant no. T22423 from the National Foundation of Hungary for Scientific Research and the Austrian-Hungarian Bilateral Research and Development Fund, no. A-4/1999. The work reported in the paper was partially carried out during the first author's visit at BRICS.

‡Partially supported by the Austrian-Hungarian Bilateral Research and Development Fund, no. A-4/1999.

applicable to all inductive *-semirings. We also describe the structure of the initial inductive *-semiring and conjecture that any free inductive *-semiring may be given as a semiring of rational power series with coefficients in the initial inductive *-semiring. We relate this conjecture to recent axiomatization results on the equational theory of the regular sets.

1 Introduction

One of the most well-known induction principles used in computer science and in particular in semantics is the fixed point induction rule, see de Bakker and Scott [9] and Park [21]. Inductive *-semirings are semirings equipped with a partial order satisfying the fixed point equation and the fixed point induction rule for linear terms. Inductive *-semirings extend the notion of continuous semirings used by Goldstern [13], Sakarovitch [22] and Kuich [19] and the Kleene algebras of Conway [7] and Kozen [16, 17]. Also, every Blikle net [2] and quantale [15] is an inductive *-semiring. Continuous semirings cannot be defined within first-order logic. In contrast, inductive semrings are defined by implications and thus form a quasi-variety.

We provide, in a systematic way, the rudiments of a theory of inductive *-semirings related to automata, languages and power series. In particular, we prove that if S is an inductive *-semiring, then so is $S^{n\times n}$, for any integer $n \geq 0$. Also, we prove that if S is an inductive *-semiring, then so is any semiring of power series $S\langle\langle A^*\rangle\rangle$. Moreover, we prove that any inductive *-semiring is a Conway semiring and an iteration semiring. As shown by Kozen [17], the dual of an inductive *-semiring is not not always an inductive *-semiring. In contrast, we prove that the dual of an iteration semiring is an iteration semiring.

Kuich [19] proved a general Kleene theorem for continuous semirings. Bloom and Ésik [4, 6] define Conway semirings and prove a general Kleene theorem for all Conway semirings. Since any inductive *-semiring is a Conway semiring and an iteration semiring, there results a Kleene theorem applicable to all inductive *-semirings. We present a variation of this result which also applies to all Conway semirings and thus to all inductive *-semirings. Our proof follows standard arguments, see, e.g., Conway [7], but we recall the main constructions in order to make the paper selfcontained.

We also describe the structure of the initial inductive *-semiring and conjecture that any free inductive *-semiring may be characterized as a semiring of rational power series with coefficients in the initial inductive *-semiring. We relate this conjecture to recent axiomatization results on the equational theory of the regular sets and rational power series, see [18, 16, 5, 10, 11].

In a companion paper, we plan to study semirings equipped with a partial order satsifying the fixed point equation and the fixed point induction rule for

all algebraic terms.
Some notation. For each integer $n \geq 0$, we denote the set $\{1, \ldots, n\}$ by $[n]$. Thus, $[0]$ is the empty set. If A is a set, we let A^* denote the set of all words over A including the empty word ϵ. For each word $w \in A^*$, $|w|$ denotes the length of w.

2 Inductive *-semirings and Conway semirings

In this section we define our main concept, inductive *-semirings, and establish some elementary properties of inductive *-semirings. We then prove that every inductive *-semiring is a Conway semiring.
Recall that a *semiring* is an algebra $S = (S, +, \cdot, 0, 1)$ equipped with binary operations $+$ (sum or addition) and $\cdot$ (product or multiplication) and constants 0 and 1 such that $(S, +, 0)$ is a commutative monoid, $(S, \cdot, 1)$ is a monoid and multiplication distributes over all finite sums, including the empty sum. Thus,

$$\begin{aligned} (a+b)c &= ac + bc \\ c(a+b) &= ca + cb \\ a \cdot 0 &= 0 \\ 0 \cdot a &= 0 \end{aligned}$$

hold for all $a, b, c \in S$. An *ordered semiring*[1] is a semiring S equipped with a partial order $\leq$ such that the operations are monotonic. A morphism of semirings is a function that preserves the operations and constants. A morphism of ordered semirings also preserves the partial order.
A **-semiring* is a semiring S equipped with a star operation $^* : S \to S$. Morphisms of *-semirings preserve the star operation.

Definition 2.1 *An* inductive *-semiring *is a *-semiring which is also an ordered semiring and satisfies the* fixed point inequation

$$aa^* + 1 \quad \leq \quad a^* \tag{1}$$

and the fixed point induction rule

$$ax + b \leq x \quad \Rightarrow \quad a^*b \leq x. \tag{2}$$

A morphism of inductive *-semirings is an order preserving *-semiring morphism.

Proposition 2.2 *The* fixed point equation

$$aa^* + 1 \quad = \quad a^* \tag{3}$$

holds in any inductive *-semiring. Moreover, the star operation is monotonic.

[1]This notion of ordered semiring is more special than the one defined in [12].

Proof. Since the semiring operations are monotonic, (1) implies

$$a(aa^* + 1) + 1 \quad \leq \quad aa^* + 1.$$

Thus, $a^* \leq aa^* + 1$ by the fixed point induction rule. By (1) this proves (3). As for the second claim, suppose that $a \leq b$ in an inductive *-semiring. Then $ab^* + 1 \leq bb^* + 1 = b^*$, so that $a^* \leq b^*$ by the fixed point induction rule. $\square$

The main examples of inductive *-semirings can be derived from the continuous semirings defined below. Recall that a *directed set* in a partially ordered set P is a nonempty set $D \subseteq P$ such that any two elements of D have an upper bound in D. We call P a *complete partially ordered set*, or *cpo*[2], for short, if P has a least element and least upper bounds $\sup D$ of all directed sets $D \subseteq P$. When P is a cpo, so is P^n, for any $n \geq 0$. The order on P^n is the pointwise order. Suppose that P and Q are cpo's. A function $f : P \to Q$ is called *continuous* if f preserves the sup of any directed set, i.e.,

$$f(\sup D) \quad = \quad \sup f(D),$$

for all directed sets $D \subseteq P$. It follows that any continuous function is monotonic.

Definition 2.3 *A* continuous semiring *is an ordered semiring S which is a cpo with least element* 0 *and such that the sum and product operations are continuous. A morphism of continuous semirings is a continuous semiring morphism.*

In a continuous semiring S, we may define the sum of any family of elements of S. Given $a_i \in S$, $i \in I$, we define

$$\sum_{i \in I} a_i \quad = \quad \sup_{F \subseteq I,\ F \text{ finite}} \sum_{i \in F} a_i. \tag{4}$$

It follows that any continuous semiring morphism preserves all sums.

Definition 2.4 *Suppose that S is both a *-semiring and a continuous semiring. We call S a* continuous *-semiring *if the star operation on S is given by*

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

for all $a \in S$. A morphism of continuous *-semirings is a *-semiring morphism which is continuous.

[2] Cpo's are called dcpo's in [8].

It follows that the star operation is also continuous. Note that if S and S' are continuous *-semirings, then any continuous semiring morphism $S \to S'$ automatically preserves the star operation.
By the well-known fixed-point theorem for continuous functions, [8] Theorem 4.5, we have:

Proposition 2.5 *Any continuous *-semiring is an inductive *-semiring.*

Some examples of continuous *-semirings are:

1. The semiring $\mathbf{P}_M$ of all subsets of a multiplicative monoid M, equipped with the union and complex product operations and the partial order given by set inclusion.

2. For any set A, the semiring $\mathbf{L}_A$ of all languages in A^*.

3. For any set A, the semiring $\mathbf{Rel}_A$ of all binary relations over A.

4. The semiring $\mathbf{N}_\infty$ obtained by adding a top element to $\mathbf{N}$, the ordered semiring of natural numbers $\{0, 1, 2, \dots\}$ equipped with the usual sum and product operations.

5. Any finite ordered semiring, in particular the semiring $\mathbf{k} = \{0, 1, \dots, k-1\}$, for each integer $k > 1$. In this semiring, the sum and product operations and the partial order are the usual ones except that $x + y$ is $k - 1$ if the usual sum is $> k - 1$, and similarly for xy. When $k = 2$, this semiring is also known as the *Boolean semiring* $\mathbf{B}$.

6. Every Blikle net [2] or quantale [15].

Inductive *-semirings other than continuous *-semirings include the semirings $\mathbf{R}_A$ and $\mathbf{CF}_A$ of regular and context free languages in A^*, and the Kleene algebras of Kozen [16] that we will call Kozen semirings below. For the existence of inductive *-semirings that cannot be embedded in any continuous *-semiring see below.

Example 2.6 *We give a generalization of an example of Kozen [17]. Suppose that $(M, +, 0, \leq)$ is a commutative monoid equipped with a partial order $\leq$ such that 0 is the least element of M and such that M is a cpo, i.e., all directed sets have a supremum. Moreover, suppose that $+$ is continuous. Let F_M denote the set of all strict additive and monotonic functions $f : M \to M$, i.e., such that*

$$\begin{aligned} f(a+b) &= f(a) + f(b) \\ f(0) &= 0 \\ a \leq b &\Rightarrow f(a) \leq f(b), \end{aligned}$$

for all $a, b \in A$. When $f, g \in F_M$, define

$$\begin{aligned}(f+g)(a) &= f(a)+g(a)\\ (f\circ g)(a) &= f(g(a))\end{aligned}$$

for all $a \in A$. Moreover, let $0(a) = 0$, $1(a) = a$, all $a \in A$. Equipped with these operations and constants, and the pointwise partial order, F_M is an ordered semiring. By the Knaster-Tarski fixed point theorem [8], for each $f \in F_M$ and $a \in A$, the monotonic function $x \mapsto f(x)+a$, $x \in M$ has a least pre-fixed point that we denote by $f^*(a)$. In fact, $f^*(a)$ is the "limit" of the sequence

$$\begin{aligned}f^0(a) &= a\\ f^{\alpha+1} &= f(f^\alpha(a))+a\\ f^\alpha(a) &= \sup_{\beta<\alpha} f^\beta(a), \quad \alpha > 0 \ \textit{ is a limit ordinal.}\end{aligned}$$

Using this, and the continuity of $+$, it follows easily that f^* is a strict additive function. Since f^* is also monotonic, there results a well-defined star operation on F_M. In fact, F_M is an inductive *-semiring.

Suppose that S is a *-semiring which is an ordered semiring. Below we will say that the *weak fixed point induction rule* holds in S if

$$ax + b = x \quad \Rightarrow \quad a^*b \leq x,$$

for all a, b and x in S.

Proposition 2.7 *The following equations hold in an inductive semiring:*

$$\begin{aligned}a^*a+1 &= a^* &(5)\\ (ab)^* &= 1+a(ba)^*b &(6)\\ (ab)^*a &= a(ba)^* &(7)\\ (a+b)^* &= (a^*b)^*a^*. &(8)\end{aligned}$$

Proof. To prove (5), note that

$$\begin{aligned}a(a^*a+1)+1 &= (aa^*+1)a+1\\ &= a^*a+1,\end{aligned}$$

so that

$$a^* \leq a^*a+1, \tag{9}$$

by the weak fixed point induction rule. But for all b,

$$\begin{aligned} aba(ba)^* + a &= a(ba(ba)^* + 1) \\ &= a(ba)^*. \end{aligned}$$

Thus,

$$(ab)^*a \leq a(ba)^*, \tag{10}$$

again by the weak fixed point induction rule. Taking $b = 1$ in (10), we have

$$a^*a \leq aa^*. \tag{11}$$

By (9) and (11),

$$a^* \leq a^*a + 1 \leq aa^* + 1 = a^*.$$

Next we prove (6). Since

$$\begin{aligned} ab(a(ba)^*b + 1) + 1 &= a(ba(ba)^* + 1)b + 1 \\ &= a(ba)^*b + 1, \end{aligned}$$

we have

$$(ab)^* \leq a(ba)^*b + 1, \tag{12}$$

by the weak fixed point induction rule. But by (10) and (3),

$$\begin{aligned} a(ba)^*b + 1 &\leq ab(ab)^* + 1 \\ &= (ab)^*, \end{aligned}$$

which together with (12) yields (6).
We now prove (7).

$$\begin{aligned} (ab)^*a &= (a(ba)^*b + 1)a \\ &= a((ba)^*ba + 1) \\ &= a(ba)^*, \end{aligned}$$

by (6) and (5).
To prove (8), note that by (3), (6) and (7),

$$\begin{aligned} (a+b)(a^*b)^*a^* + 1 &= a(a^*b)^*a^* + b(a^*b)^*a^* + 1 \\ &= aa^*(ba^*)^* + (ba^*)^* \\ &= (aa^* + 1)(ba^*)^* \\ &= a^*(ba^*)^* \\ &= (a^*b)^*a^*. \end{aligned}$$

Thus,

$$(a+b)^* \quad \leq \quad (a^*b)^*a^*. \tag{13}$$

For the reverse inequation, assume that

$$(a+b)x+1 \quad = \quad x \tag{14}$$

for some x. Then,

$$ax+bx+1 \quad = \quad x,$$

so that

$$a^*(bx+1) = a^*bx+a^* \quad \leq \quad x,$$

by the weak fixed point induction rule. Now, by the fixed point induction rule,

$$(a^*b)^*a^* \quad \leq \quad x.$$

Thus, taking $x = (a+b)^*$ in (14), we have

$$(a^*b)^*a^* \quad \leq \quad (a+b)^*. \tag{15}$$

Equation (8) now follows from (13) and (15). □

The *- semirings satisfying (6) and (8) have a distinguishing name.

Definition 2.8 [4, 6, 12] *A* Conway semiring *is a *-semiring satisfying the* sum star equation *(8) and the* product star equation *(6). A morphism of Conway semirings is a *-semiring morphism.*

Note that the fixed point equation and all of the equations appearing in Proposition 2.7 hold in any Conway semiring. By the fixed point equation, also $0^* = 1$ in any Conway semiring.
Only the weak fixed point induction rule was used in Proposition 2.7 to prove (6). This observation gives rise to the following definition.

Definition 2.9 *A* weak inductive *-semiring *is an ordered semiring which is also a *-semiring and satisfies the fixed point equation (3), the sum star equation (8) and the weak fixed point induction rule. A morphism of weak inductive *-semirings is an ordered semiring morphism which preserves the star operation.*

Clearly, every inductive *-semiring is a weak inductive *-semiring.

Corollary 2.10 *Any weak inductive *-semiring is a Conway semiring. Any inductive *-semiring is a Conway semiring with a monotonic star operation.*

Proposition 2.11 *The inequations*

$$\begin{aligned} 0 &\leq a \\ a &\leq a+b \\ \sum_{i=0}^{n} a_i &\leq a^*, \quad n \geq 0 \end{aligned}$$

hold in any weak inductive *-semiring S.

Proof. Since

$$1 \cdot a + 0 \;=\; a,$$

we have $0 = 1^* \cdot 0 \leq a$. Since the sum operation is monotonic, also

$$\begin{aligned} a &= a+0 \\ &\leq a+b, \end{aligned}$$

for all $a, b \in S$. Since by repeated applications of the fixed point equation,

$$a^* \;=\; a^{n+1}a^* + \sum_{i=0}^{n} a^i,$$

we have $\sum_{i=0}^{n} a^i \leq a^*$, for all $n \geq 0$. □

Remark 2.12 Inductive *-semirings are ordered algebraic structures in the usual universal algebraic sense, see [3, 23]. In fact, since inductive *-semirings are defined by (in)equations and implications, they form a *quasi-variety*. Hence, the class of inductive *-semirings is closed under the constructions of direct products, substructures, direct and inverse limits, etc. (When S and S' are inductive *-semirings, we say that S is a substructure of S' if $S \subseteq S'$ and the operations and the partial order on S are the restrictions of the corresponding operations and the partial order on S'.) Similar closure properties are enjoyed by weak inductive *-semirings.

3 Sum-ordered semirings

In any semiring S, we may define a relation $\preceq$ by $a \preceq b$ iff there is some c with $a + c = b$. This relation is a preorder preserved by the semiring operations.

Definition 3.1 *An ordered semiring S is called* sum-ordered *[20] if the partial order $\leq$ given on S coincides with the above relation $\preceq$, i.e., when*

$$a \leq b \quad \Leftrightarrow \quad \exists c \; a + c = b,$$

for all $a, b \in S$.

Note that $0 \leq a$ and hence $a \leq a+b$ hold for all a, b in a sum-ordered semiring S, so that 0 is the least element of S. Each of the continuous semirings $\mathbf{P}_M$, $\mathbf{L}_A$, $\mathbf{R}_A$, $\mathbf{Rel}_A$, $\mathbf{N}_\infty$ and $\mathbf{k}$ is sum-ordered.

Proposition 3.2 *Suppose that S, partially ordered by the relation $\leq$, is an ordered semiring. Then S, equipped with the relation $\preceq$, is a sum-ordered semiring iff 0 is least. Moreover, in this case, $\preceq$ is included in $\leq$.*

Proof. We only need to show that when 0 is least in S, then $\preceq$ is antisymmetric. But suppose that $a \preceq b$ and $b \preceq a$. Then there exists some c with $a + c = b$. Thus, since $0 \leq c$ and the sum operation is monotonic, we have $a \leq a + c = b$. In the same way, $b \leq a$. But $\leq$ is antisymmetric, so that $a = b$. □

Thus, by Proposition 2.11, if S is a (weak) inductive *-semiring, then S, equipped with the relation $\preceq$ is a sum-ordered semiring.

Proposition 3.3 *Suppose that S and S' are ordered semirings and h is a semiring morphism $S \to S'$. If S is sum-ordered and 0 is the least element of S', then h is an ordered semiring morphism.*

Proof. If $a \leq b$ in S, then there is some c with $a + c = b$. Thus, $h(a) + h(c) = h(b)$, so that $h(a) \preceq h(b)$ in S'. But since 0 is the least element of S', we have $h(a) \leq h(b)$. □

Proposition 3.4 *Suppose that S is a *-semiring which is a sum-ordered semiring. Then S is an inductive *-semiring iff S satisfies the fixed point (in)equation and the weak fixed point induction rule. Thus, S is an inductive *-semiring iff S is a weak inductive *-semiring.*

Proof. We only need to show that if S satisfies the weak fixed point induction rule, then S also satisfies the fixed point induction rule. So suppose that $ax + b \leq x$, for some $a, b, x \in S$. Then, since S is sum-ordered, there exists $c \in S$ with $ax + (b + c) = x$. Hence, $a^*b + a^*c = a^*(b + c) \leq x$, so that $a^*b \leq x$. $\square$

We end this section by presenting an inductive *-semiring S which, equipped with the sum-order, is not inductive. Let N denote the natural numbers. Suppose that $M = N \cup \{a, b, c\}$ is equipped with the the usual $+$ operation on N, and

$$x + y \quad = \quad \begin{cases} a & \text{if } x \in N \text{ and } y = a, \text{ or } x = a \text{ and } y \in N \\ b & \text{if } x \in N \text{ and } y = b, \text{ or } x = b \text{ and } y \in N \\ c & \text{otherwise.} \end{cases}$$

Let $\leq$ be the usual partial order on N, and let $n \leq a \leq b \leq c$, all $n \in N$, and of course $a \leq a$, $b \leq b$ and $c \leq c$. Let S denote the semiring of all strict additive and monotonic functions on M as defined in Example 2.6. As shown above, S, equipped with the pointwise partial order can be turned into an inductive *-semiring. But the same semiring S, equipped with the sum-order, has no appropriate star operation. Indeed, when f is the function $f(n) = n + 1$ and $f(x) = x$ for $x \notin N$, then, with respect to the sum-order, there is no least x with $f(x) = x$.

Problem 3.1 Does there exist a weak inductive *-semiring with a nonmonotonic star operation? Does there exist a weak inductive *-semiring with a monotonic star operation which is not an inductive *-semiring?

4 Idempotent inductive *-semirings

A semiring S is called *idempotent* if $1 + 1 = 1$ holds in S. It then follows that $a + a = a$, for all $a \in S$.

Proposition 4.1 *Suppose that S is an idempotent ordered semiring. The following conditions are equivalent.*

1. *0 is the least element of S, i.e., $0 \leq a$ holds for all a in S.*
2. *For all $a, b \in S$, $a \leq a + b$.*
3. *For all $a, b \in S$, $a \leq b$ iff $a + b = b$.*
4. *S is sum-ordered.*

Proof. It is clear that the first condition implies the second and that the last condition implies the first. In fact, the first two conditions are equivalent in any ordered semiring. Suppose that the second condition holds. If $a \leq b$ then $a + b \leq b + b = b \leq a + b$, so that $a + b = b$. Conversely, if $a + b = b$, then $a \leq b$, since $a \leq a + b$. Thus the second condition implies the third. Finally, if the third condition holds then $a \leq b$ iff there is some c with $a + c = b$. It follows that S is sum-ordered. □

Corollary 4.2 *Suppose that S and S' are ordered semirings such that S is idempotent and 0 is least in both S and S'. Then any semiring morphism $S \to S'$ is an ordered semiring morphism.*

Corollary 4.3 *An ordered idempotent semiring S equipped with a star operation is an inductive *-semiring iff S satisfies the fixed point (in)equation and the weak fixed point induction rule. Hence S is an inductive semiring iff S is a weak inductive *-semiring.*

Proposition 4.4 *Any idempotent inductive *-semiring S satisfies the equation*

$$1^* \quad = \quad 1.$$

Proof. Since $1 + 1 = 1$, $1^* \leq 1$. On the other hand, $1 \leq 1^* + 1 = 1^*$. □

5 Matrices

If S is a Conway semiring, then for each $n \geq 0$, the semiring $S^{n \times n}$ of all $n \times n$ matrices over S may be turned into a Conway semiring. In fact, our definition of the star operation on $S^{n \times n}$ applies to any *-semiring.

Definition 5.1 *Suppose that S is a *-semiring. We define the star M^* of an $n \times n$ matrix M in $S^{n \times n}$ by induction on n.*

- *If $n = 0$, M^* is the unique 0×0 matrix.*
- *If $n = 1$, $M = [a]$, for some $a \in S$. We define $M^* = [a^*]$.*
- *If $n > 1$, write*

$$M \quad = \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where a is $(n-1)\times(n-1)$ and d is 1×1. We define

$$M^* \quad = \quad \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \tag{16}$$

where

$$\alpha \quad = \quad (a+bd^*c)^* \tag{17}$$
$$\beta \quad = \quad \alpha bd^* \tag{18}$$
$$\gamma \quad = \quad \delta ca^* \tag{19}$$
$$\delta \quad = \quad (d+ca^*b)^*. \tag{20}$$

The following result is implicit in [7].

THEOREM 5.2 [7] *If S is a Conway semiring, then so is $S^{n\times n}$, for any $n\geq 0$. Moreover, for each matrix $M\in S^{n\times n}$, and for each way of writing M as*

$$M \quad = \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where a and d are square matrices, it holds that

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

where α,β,γ and δ are given as above.

In fact, the collection of all $n\times m$ matrices, for $n,m\geq 0$ form a *Conway theory* [6]. (In [4, 6], Theorem 5.2 is derived from a general result that holds for all Conway theories.) We now give a characterization of Conway semirings.

THEOREM 5.3 *The following conditions are equivalent for a *-semiring S.*

1. *S is a Conway semiring.*
2. *$S^{2\times 2}$ satisfies the fixed point equation.*
3. *For each $n\geq 0$, $S^{n\times n}$ satisfies the fixed point equation.*

Proof. It is clear that the last condition implies the second. Moreover, by the previous theorem, the first condition implies (the second and) the third. Thus, we are left to show that the second condition implies the first. So suppose that the fixed point equation holds in $S^{2\times 2}$, i.e.,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}^* + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad = \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^*$$

for all $a, b, c, d \in S$. Thus, using the definition of the star operation,

$$a(a+bd^*c)^* + b(d+ca^*b)^*ca^* + 1 = (a+bd^*c)^* \quad (21)$$

$$a(a+bd^*c)^*bd^* + b(d+ca^*b)^* = (a+bd^*c)^*bd^*. \quad (22)$$

Letting $b = 0$ (and $c = d = 0$, say) in (21) we obtain $aa^* + 1 = a^*$, so that the fixed point equation holds in S. In particular, $0^* = 1$. Thus, letting $a = d = 0$, (21) gives $b(cb)^*c + 1 = (bc)^*$. Also, letting $a = 0$ and $b = 1$, (22) gives $(d+c)^* = (d^*c)^*d^*$. Hence, both the product star and sum star equations hold in S proving that S is a Conway semiring. □

The above argument actually gives the following results:

COROLLARY 5.4 *A *-semiring S is a Conway semiring iff for some $n > 1$, $S^{n\times n}$ satisfies the fixed point equation.*

COROLLARY 5.5 *A *-semiring S is a Conway semiring iff the fixed point equation holds in $S^{2\times 2}$ for all lower or upper triangular matrices.*

When S is a partially ordered semiring, then, equipped with the pointwise order, so is $S^{n\times n}$, for any integer $n \geq 0$.

THEOREM 5.6 *Suppose that S is an inductive *-semiring. Then for each $n \geq 0$, $S^{n\times n}$ is also an inductive *-semiring.*

Proof. We have already proved that any inductive semiring is a Conway semiring. Hence, the fixed point equation holds in $S^{n\times n}$, for all $n \geq 0$. As for the fixed point induction rule, we prove by induction on n that if $a \in S^{n\times n}$, $b, \xi \in S^{n\times m}$ with $a\xi + b \leq \xi$, then $a^*b \leq \xi$. Our argument is essentially the same as the proof of Theorem 4 in Chapter 3 of Conway [7]. The case $n = 0$ is trivial and the case $n = 1$ holds by assumption. Supposing $n > 1$, write

$$a = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$$

$$b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

$$\xi = \begin{bmatrix} \xi_1 \\ \xi_2 \end{bmatrix}$$

where a_1 is $(n-1)\times(n-1)$, b_1 and ξ_1 are $(n-1)\times m$, etc. Since $a\xi + b \leq b$, we have

$$a_1\xi_1 + a_2\xi_2 + b_1 \leq \xi_1$$

$$a_3\xi_1 + a_4\xi_2 + b_2 \leq \xi_2.$$

By the induction assumption,

$$a_1^*(a_2\xi_2 + b_1) \quad \leq \quad \xi_1,$$

so that

$$a_3a_1^*a_2\xi_2 + a_3a_1^*b_1 \quad \leq \quad a_3\xi_1$$

and

$$(a_4 + a_3a_1^*a_2)\xi_2 + (a_3a_1^*b_1 + b_2) \quad \leq \quad \xi_2.$$

Thus,

$$(a_4 + a_3a_1^*a_2)^*(a_3a_1^*b_1 + b_2) \quad \leq \quad \xi_2, \tag{23}$$

since the fixed point induction rule holds in S. In the same way,

$$(a_1 + a_2a_4^*a_3)^*(a_2a_4^*b_2 + b_1) \quad \leq \quad \xi_1. \tag{24}$$

But

$$a^* \quad = \quad \begin{bmatrix} (a_1 + a_2a_4^*a_3)^* & (a_1 + a_2a_4^*a_3)^*a_2a_4^* \\ (a_4 + a_3a_1^*a_2)^*a_3a_1^* & (a_4 + a_3a_1^*a_2)^* \end{bmatrix}$$

so that (23) and (24) amount to $a^*b \leq \xi$. □

REMARK 5.7 Theorem 5.6 may be viewed as an instance of the well-known rule found independently by Bekić [1] and de Bakker and Scott [9] to compute "simultaneous least pre-fixed points" of continuous functions.

PROBLEM 5.1 Suppose that S is a weak inductive *-semiring. Are the matrix semirings $S^{n\times n}$ weak inductive semirings?

6 Iteration semirings

Iteration semirings were originally defined in [4]. Here we recall the definition given in [10].

Suppose that G is a finite group of order n, say $G = \{g_1, \ldots, g_n\}$. For each g_i, let a_{g_i} be a variable associated with g_i. The $n \times n$ matrix M_G is defined by

$$(M_G)_{i,j} \quad = \quad a_{g_i^{-1}g_j}, \quad i, j \in [n].$$

Thus, each row of M_G is a permutation of the first row, and similarly for columns. In particular, for each $i \in [n]$, let π_{g_i} denote the $n \times n$ permutation matrix corresponding to the permutation of G induced by left multiplication with g_i. Thus, for any $r, s \in [n]$, $(\pi_{g_i})_{r,s} = 1$ iff $g_s = g_ig_r$.

LEMMA 6.1 [18]

$$\pi_{g_i} M_G \pi_{g_i}^{-1} \quad = \quad M_G,$$

for all $i \in [n]$.

Let α_n denote the $1 \times n$ matrix whose first component is 1 and whose other components are 0, and let δ_n denote the $n \times 1$ matrix whose components are all 1.

DEFINITION 6.2 Conway [7] *The* group-equation associated with G *is*

$$\alpha_n M_G^* \delta_n \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*.$$

We will use the group-equations only in Conway semirings. In such semirings, it is irrelevant in what order the elements of the group G are listed. This follows from the following fact.

LEMMA 6.3 *The* permutation equation *holds in all Conway semirings S:*

$$(\pi M \pi^{-1})^* \quad = \quad \pi M^* \pi^{-1},$$

for all $\pi, M \in S^{n \times n}$ such that π is a permutation matrix with inverse π^{-1}.

Proof. Since $S^{n \times n}$ is a Conway semiring, by the product star and dual fixed point equations we have

$$\begin{aligned}
(\pi M \pi^{-1})^* &= \pi (M \pi^{-1} \pi)^* M \pi^{-1} + 1 \\
&= \pi M^* M \pi^{-1} + 1 \\
&= \pi (M^* M + 1) \pi^{-1} \\
&= \pi M^* \pi^{-1}.
\end{aligned}$$

See also [7, 4]. □

DEFINITION 6.4 [4, 6] *An* iteration semiring *is a Conway semiring satisfying the group-equations for all finite groups. A morphism of iteration semirings is a *-semiring morphism.*

THEOREM 6.5 *Any inductive *-semiring is an iteration semiring.*

Proof. Suppose that S is an inductive *-semiring. By Corollary 2.10, S is a Conway semiring. Thus we only need to establish the group-equations. So let $G = \{g_1, \ldots, g_n\}$ denote a group of order n, and let $a_{g_1}, \ldots, a_{g_n}$ be some elements of S associated with the group elements. Define $a = a_{g_1} + \ldots + a_{g_n}$. Since each row of M_G is a permutation of the a_{g_i}, we have that

$$M_G \delta_n \;=\; \delta_n a, \tag{25}$$

i.e., each row of M_G sums up to a. Thus,

$$\begin{aligned} M_G(\delta_n a^*) + \delta_n &= \delta_n(aa^* + 1) \\ &= \delta_n aa^* \\ &= \delta_n a^*, \end{aligned}$$

so that $M_G^* \delta_n \leq \delta_n a^*$ and

$$\alpha_n M_G^* \delta_n \;\leq\; a^*$$

by the weak fixed point induction rule. As for the reverse inequality, note that each row of M_G^* is a permutation of the first row. This follows since for each $i \in [n]$, $M_G = \pi_{g_i} M_G \pi_{g_i}^{-1}$, by Lemma 6.1. Thus, $M_G^* = \pi_{g_i} M_G^* \pi_{g_i}^{-1}$, by the permutation equation. Thus,

$$M_G^* \delta_n \;=\; \delta_n \alpha_n M_G^* \delta_n. \tag{26}$$

Thus, by (25) and (26),

$$\begin{aligned} a(\alpha_n M_G^* \delta_n) + 1 &= \alpha_n \delta_n a \alpha_n M_G^* \delta_n + \alpha_n \delta_n \\ &= \alpha_n M_G \delta_n \alpha_n M_G^* \delta_n + \alpha_n \delta_n \\ &= \alpha_n M_G M_G^* \delta_n + \alpha_n \delta_n \\ &= \alpha_n (M_G M_G^* + 1) \delta_n \\ &= \alpha_n M_G^* \delta_n. \end{aligned}$$

The weak fixed point induction rule gives

$$a^* \;\leq\; \alpha_n M_G^* \delta_n.$$

□

Remark 6.6 It is shown in [18, 10] that whenever S is an iteration semiring, then so is $S^{n \times n}$, for each $n \geq 0$. In fact, the *algebraic theory of matrices* over an iteration semiring is an *iteration theory*, see [10].

7 Duality

The opposite or *dual* S^{op} of a *-semiring S is equipped with the same operations and constants as S except for multiplication, which is the reverse of the multiplication in S. When S is ordered, so is S^{op} equipped with the same partial order. Note that $(S^{\mathrm{op}})^{\mathrm{op}} = S$.

Proposition 7.1 *A *-semiring S is a Conway semiring iff S^{op} is a Conway semiring.*

Proof. Suppose that S is a Conway semiring. It is clear that the product star equation (6) holds in S^{op}. As for the sum star equation, note that in S,

$$\begin{aligned}(a+b)^* &= (a^*b)^*a^* \\ &= a^*(ba^*)^*,\end{aligned}$$

by the product star equation. It follows that the sum star equation holds in S^{op}. □

When M is an $n \times m$ matrix over a semiring S, define M^{op} to be the $m \times n$ matrix with $M^{\mathrm{op}}_{ij} = M_{ji}$, for all $i \in [m]$ and $j \in [n]$. Note that when S is a *-semiring, then both $S^{n\times n}$ and $(S^{\mathrm{op}})^{n\times n}$ are *-semirings, for any $n \geq 0$.

Theorem 7.2 *Suppose that S is a Conway semiring. Then the Conway semirings $(S^{n\times n})^{\mathrm{op}}$ and $(S^{\mathrm{op}})^{n\times n}$ are isomorphic.*

Proof. It is clear that the map $M \mapsto M^{\mathrm{op}}$ preserves the sum operation and the constants 0 and 1. To complete the proof that this map is the required isomorphism, we need to show that

$$(MN)^{\mathrm{op}} = N^{\mathrm{op}} \circ M^{\mathrm{op}} \tag{27}$$

$$(M^*)^{\mathrm{op}} = (M^{\mathrm{op}})^{\otimes} \tag{28}$$

hold for all $M, N \in S^{n\times n}$, where $\circ$ and $^{\otimes}$ denote the product and star operations in $(S^{\mathrm{op}})^{n\times n}$. We leave the verification of (27) to the reader. The proof of (28) is by induction on n. The cases $n = 0, 1$ are clear. When $n > 1$, let us partition M into four block matrices

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

as above. Then

$$M^{\mathrm{op}} = \begin{bmatrix} a^{\mathrm{op}} & c^{\mathrm{op}} \\ b^{\mathrm{op}} & d^{\mathrm{op}} \end{bmatrix}$$

Recall that

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

where $\alpha, \beta, \gamma, \delta$ are defined as in (17) – (20). Let

$$(M^{\mathrm{op}})^{\otimes} \quad = \quad \begin{bmatrix} \alpha' & \gamma' \\ \beta' & \delta' \end{bmatrix}$$

We need to prove that $\alpha^{\mathrm{op}} = \alpha'$, $\beta^{\mathrm{op}} = \beta'$, etc. But, by using the induction assumption,

$$\begin{aligned}
\alpha^{\mathrm{op}} &= ((a + bd^*c)^*)^{\mathrm{op}} \\
&= ((a + bd^*c)^{\mathrm{op}})^{\otimes} \\
&= (a^{\mathrm{op}} + c^{\mathrm{op}} \circ (d^*)^{\mathrm{op}} \circ b^{\mathrm{op}})^{\otimes} \\
&= (a^{\mathrm{op}} + c^{\mathrm{op}} \circ (d^{\mathrm{op}})^{\otimes} \circ b^{\mathrm{op}})^{\otimes} \\
&= \alpha'.
\end{aligned}$$

Also, using the Conway semiring equation

$$\begin{aligned}
u^*z(x + yu^*z)^* &= u^*z(x^*yu^*z)^*x^* \\
&= (u^*zx^*y)^*u^*zx^* \\
&= (u + zx^*y)^*zx^*,
\end{aligned}$$

it follows that

$$\begin{aligned}
\beta^{\mathrm{op}} &= (\alpha bd^*)^{\mathrm{op}} \\
&= (d^*)^{\mathrm{op}} \circ b^{\mathrm{op}} \circ \alpha^{\mathrm{op}} \\
&= (d^{\otimes})^{\mathrm{op}} \circ b^{\mathrm{op}} \circ \alpha' \\
&= (d^{\otimes})^{\mathrm{op}} \circ b^{\mathrm{op}} \circ (a^{\mathrm{op}} + c^{\mathrm{op}} \circ (d^{\mathrm{op}})^{\otimes} \circ b^{\mathrm{op}})^{\otimes} \\
&= (d + b^{\mathrm{op}} \circ (a^{\mathrm{op}})^{\otimes} \circ c^{\mathrm{op}})^{\otimes} \circ b^{\mathrm{op}} \circ (a^{\mathrm{op}})^{\otimes} \\
&= \beta'.
\end{aligned}$$

The proofs of the other equations are similar. Note that the Conway identities (8) and (6) were needed only in the proof of (33). $\square$

The dual t^{op} of a *-semiring term t is defined by induction on the structure of t.

- If t is a variable or one of the constants $0, 1$, then $t^{\mathrm{op}} = t$.
- If $t = t_1 + t_2$ then $t^{\mathrm{op}} = t_1^{\mathrm{op}} + t_2^{\mathrm{op}}$.

- If $t = t_1 t_2$ then $t^{\mathrm{op}} = t_2^{\mathrm{op}} t_1^{\mathrm{op}}$.
- If $t = t_1^*$ then $t^{\mathrm{op}} = (t_1^{\mathrm{op}})^*$.

Thus, $(t^{\mathrm{op}})^{\mathrm{op}} = t$. The dual of an equation $t_1 = t_2$ is the equation $t_1^{\mathrm{op}} = t_2^{\mathrm{op}}$, and the dual of an implication $t_1 = s_1 \wedge \ldots \wedge t_n = s_n \Rightarrow t = s$ is $t_1^{\mathrm{op}} = s_1^{\mathrm{op}} \wedge \ldots \wedge t_n^{\mathrm{op}} = s_n^{\mathrm{op}} \Rightarrow t^{\mathrm{op}} = s^{\mathrm{op}}$. The dual of an inequation $t \le s$ or implication $t_1 \le s_1 \wedge \ldots \wedge t_n \le s_n \Rightarrow t \le s$ is defined in the same way. Note that the dual fixed point equation (5) is indeed the dual of the fixed point equation (3), and the *dual fixed point induction rule*

$$xa + b \le x \quad \Rightarrow \quad ba^* \le x \tag{29}$$

is the dual of (2). Moreover, the product star equation is *self dual* in that its dual is equivalent to the product star equation. The dual of the sum star equation is the equation $(a+b)^* = a^*(ba^*)^*$ mentioned above.

Proposition 7.3 *The dual of an (in)equation or implication holds in a *-semiring S iff it holds S^{op}.*

Corollary 7.4 *An equation (or implication) holds in all Conway semirings iff so does its dual.*

Below we will consider term matrices. The sum and product operations on term matrices are defined in the usual way. The star of a term matrix is defined by the matrix formula (16). When M is an $n \times p$ term matrix, we define M^{op} to be the $p \times n$ matrix such that $(M^{\mathrm{op}})_{ij} = (M_{ji})^{\mathrm{op}}$, for all $i \in [p]$ and $j \in [n]$. If M and M' are $n \times p$ term matrices and S is a *-semiring, we say that the equation $M = M'$ holds in S if each equation $M_{ij} = M'_{ij}$ does, for any $i \in [n]$, $j \in [p]$. The dual of the equation $M = M'$ is the equation $M^{\mathrm{op}} = M'^{\mathrm{op}}$.
Clearly, any *-semiring satisfies the equations

$$\begin{aligned} (M+N)^{\mathrm{op}} &= M^{\mathrm{op}} + N^{\mathrm{op}} && (30)\\ (MN)^{\mathrm{op}} &= N^{\mathrm{op}} M^{\mathrm{op}} && (31)\\ (M^{\mathrm{op}})^{\mathrm{op}} &= M && (32) \end{aligned}$$

for any term matrices M, N of appropriate size.
By Theorem 7.2, we also have

Corollary 7.5 *Any Conway semiring satisfies the equations*

$$(M^*)^{\mathrm{op}} = (M^{\mathrm{op}})^*, \tag{33}$$

for any term matrices M, N of appropriate size.

Recall that the group-equation associated with a finite group $G = \{g_1, \ldots, g_n\}$ of order n is the equation

$$\alpha_n \cdot M_G^* \cdot \delta_n \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*,$$

where $(M_G)_{ij} = a_{g_i^{-1} g_j}$, for all $i, j \in [n]$, α_n is the n-dimensional row vector whose first component is 1 and whose other components are 0, and δ_n is the n-dimensional column vector whose components are all 1. Below, without loss of generality we will assume that g_1 is the unit of G.

Lemma 7.6 *In Conway semirings, the group-equation associated with a finite group G is equivalent to the equation*

$$\delta_n^{\mathrm{op}} \cdot M_G^* \cdot \alpha_n^{\mathrm{op}} \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*.$$

Proof. Note that the meaning of this equation is that the sum of the entries of the first column of M_G^* is $(a_{g_1} + \ldots + a_{g_n})^*$.
By Lemma 6.1 and the permutation equation, the equation

$$\pi_{g_i} \cdot M_G^* \cdot \pi_{g_i}^{\mathrm{op}} \quad = \quad M_G^*$$

holds in all Conway semirings for each $i \in [n]$. Thus, if we let $t_{g_1}, \ldots, t_{g_n}$ denote the terms in the first row of M_G^*, then under the Conway semiring equations, for each $i \in [n]$ the ith row is $t_{g_i^{-1} g_1}, \ldots, t_{g_i^{-1} g_n}$. Hence, under the Conway semiring equations, there is a bijective correspondence between the entries of the first row and the entries of the first column of M_G^*. □

The matrix $N_G = M_G(a_{g_1^{-1}}, \ldots, a_{g_n^{-1}})$ is obtained form M_G by substituting $a_{g_i^{-1}}$ for a_{g_i}, for all $i \in [n]$.

Corollary 7.7 *In Conway semirings, the equation associated with a finite group G of order n is equivalent to the equation*

$$\delta_n^{\mathrm{op}} \cdot N_G^* \cdot \alpha_n^{\mathrm{op}} \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*.$$

Note that for each $i, j \in [n]$, the (i, j)th entry of N_G is $a_{g_j^{-1} g_i}$. Thus,

Lemma 7.8 *The matrices M_G^{op} and N_G are equal.*

Thus, by Corollary 7.5, we have

Lemma 7.9 *The equation*

$$(M_G^*)^{\mathrm{op}} \quad = \quad N_G^*$$

holds in all Conway semirings.

Proposition 7.10 *If the group-equation associated with a finite group G of order n holds in a Conway semiring S, then so does its dual.*

Proof. Using the above notation, the dual of the equation associated with G is

$$\delta_n^{\mathrm{op}} \cdot (M_G^*)^{\mathrm{op}} \cdot \alpha_n^{\mathrm{op}} \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*.$$

By Lemma 7.9, this equation holds in S iff the equation

$$\delta_n^{\mathrm{op}} \cdot N_G^* \cdot \alpha_n^{\mathrm{op}} \quad = \quad (a_{g_1} + \ldots + a_{g_n})^*$$

holds. But by Corollary 7.7, in Conway semirings this equation is equivalent to the group-equation associated with G. $\square$

Corollary 7.11 *Any iteration semiring satisfies the dual of any group-equation. A *-semiring is an iteration semiring iff its dual is an iteration semiring.*

Corollary 7.12 *An equation holds in all iteration semirings iff so does its dual.*

We have seen that the dual of a Conway or iteration semiring is also a Conway or iteration semiring. As pointed out by Kozen, the corresponding fact does not hold for inductive *-semirings.

Proposition 7.13 Kozen [17] *There exists an idempotent inductive *-semiring S such that S^{op} is not an inductive *-semiring.*

In fact, as shown by Kozen, when A is an infinite set and M is $P(A)$, the power set of A equipped with the union operation and the subset order, then the dual of the inductive *-semiring F_M constructed in Example 2.6 is not an inductive *-semiring. Such a semiring cannot be embedded in any continuous *-semiring.

Definition 7.14 *A* symmetric inductive *-semiring *is an inductive *-semiring which satisfies the dual fixed point induction rule (29). A morphism of symmetric inductive *-semirings is an inductive *-semiring morphism.*

Proposition 7.15 *An inductive *-semiring S is a symmetric inductive *-semiring iff S^{op} is also an inductive *-semiring.*

Proof. By Proposition 2.7, the dual of the fixed point equation (5) holds in any inductive *-semiring. $\square$

PROPOSITION 7.16 *Any continuous *-semiring is a symmetric inductive *-semiring.*

Proof. Is S is a continuous *-semiring, then so is S^{op}. $\square$

PROPOSITION 7.17 *If S is a symmetric inductive semiring, then so is $S^{n\times n}$, for each $n \geq 0$.*

Proof. By Theorem 5.6, both $S^{n\times n}$ and $(S^{\mathrm{op}})^{n\times n}$ are inductive *-semirings. But by Theorem 7.2, $(S^{\mathrm{op}})^{n\times n}$ is isomorphic to $(S^{n\times n})^{\mathrm{op}}$. $\square$

We end this section with a definition.

DEFINITION 7.18 *A* Kozen semiring *is an idempotent symmetric inductive *-semiring. A morphism of Kozen semirings is an inductive semiring morphism.*

Kozen semirings are called Kleene algebras in [16].
Examples of Kozen semirings are the semirings $\mathbb{P}_M$, $\mathbb{L}_A$, $\mathbb{R}_A$, $\mathbb{CF}_A$, $\mathbb{R}\lessdot_A$ and the Boolean semiring $\mathbb{B}$. In fact, any idempotent continuous *-semiring is a Kozen semiring.

8 Power series

Suppose that S is a semiring and A is a set. Recall that a formal power series over A with coefficients in S is a function

$$r : A^* \quad\rightarrow\quad S,$$

usually denoted

$$r \quad=\quad \sum_{u\in A^*} (r,u)u,$$

where (r, u) is just $r(u)$, the value of function r on the word u. Here, A^* denotes the free monoid of all words over A including the empty word ϵ. Equipped with the operations of pointwise sum and Cauchy product, power series form a semiring $S\langle\langle A^*\rangle\rangle$. The neutral elements are the series 0 whose coefficients are all zero, and the series 1 such that the coefficient of the empty word ϵ is 1 and the other coefficients are 0. (In a similar fashion, every element of S can be identified with a power series.) When S is partially ordered, we may turn $S\langle\langle A^*\rangle\rangle$ into a partially ordered semiring by the pointwise order.

Definition 8.1 *Suppose that S is a *-semiring. For each $s \in S\langle\langle A^*\rangle\rangle$, we define*

$$\begin{aligned}(s^*, \epsilon) &= (s, \epsilon)^* \\ (s^*, u) &= (s, \epsilon)^* \sum_{vw=u,\ v\neq\epsilon} (s, v)(s^*, w),\end{aligned}$$

for all $u \in A^*, u \neq \epsilon$.

This defines a star operation on $S\langle\langle A^*\rangle\rangle$.

Remark 8.2 It is easy to see by induction on the length of the word u that

$$(s^*, u) = \sum_{u_1\ldots u_n=u,\ u_i\neq\epsilon} (s,\epsilon)^*(s,u_1)(s,\epsilon)^* \ldots (s,u_n)(s,\epsilon)^*.$$

It then follows that

$$(s, u^*) = (\sum_{wv=u,\ v\neq\epsilon} (s^*, w)(s, v))(s, \epsilon)^*,$$

for all $u \neq \epsilon$.

Theorem 8.3 [4, 6] *If S is a Conway semiring, or an iteration semiring, then so is $S\langle\langle A^*\rangle\rangle$.*

Theorem 8.4 *If S is an inductive *-semiring, then so is $S\langle\langle A^*\rangle\rangle$.*

Proof. First we show that the fixed point equation holds, i.e.,

$$(ss^* + 1, u) = (s^*, u),$$

for all $s \in S\langle\langle A^*\rangle\rangle$ and $u \in A^*$. When $u = \epsilon$, we have

$$\begin{aligned}(ss^* + 1, \epsilon) &= (s, \epsilon)(s^*, \epsilon) + 1 \\ &= (s, \epsilon)(s, \epsilon)^* + 1 \\ &= (s, \epsilon)^* \\ &= (s^*, \epsilon),\end{aligned}$$

since the fixed point equation holds in S. Suppose now that $u \neq \epsilon$. Then, again using the fixed point equation in S,

$$\begin{aligned}(ss^*+1,u) &= (s,\epsilon)(s^*,u) + \sum_{vw=u,\ v\neq\epsilon} (s,v)(s^*,w)\\ &= (s,\epsilon)[(s,\epsilon)^* \sum_{vw=u,\ v\neq\epsilon} (s,v)(s^*,w)] + \sum_{vw=u,\ v\neq\epsilon} (s,v)(s^*,w)\\ &= ((s,\epsilon)(s,\epsilon)^*+1) \sum_{vw=u,\ v\neq\epsilon} (s,v)(s^*,w)\\ &= (s,\epsilon)^* \sum_{vw=u,\ v\neq\epsilon} (s,v)(s^*,w)\\ &= (s^*,u).\end{aligned}$$

We now prove that the fixed point induction rule holds in $S\langle\langle A^*\rangle\rangle$. So suppose that $r, s, \xi \in S\langle\langle A^*\rangle\rangle$ such that

$$r\xi + s \quad \leq \quad \xi. \tag{34}$$

We must prove that $r^*s \leq \xi$, i.e., that $(r^*s,u) \leq (\xi,u)$, for all words $u \in A^*$. When $u = \epsilon$, (34) gives

$$(r,\epsilon)(\xi,\epsilon) + (s,\epsilon) \quad \leq \quad (\xi,\epsilon).$$

Since the fixed point induction rule holds in S, we have $(r^*s,\epsilon) = (r,\epsilon)^*(s,\epsilon) \leq (\xi,\epsilon)$. Assume that $u \neq \epsilon$. Then by (34),

$$(r,\epsilon)(\xi,u) + \sum_{vw=u,\ v\neq\epsilon} (r,v)(\xi,w) + (s,u) \quad \leq \quad (\xi,u). \tag{35}$$

By induction,

$$(r^*s,w) \quad \leq \quad (\xi,w), \tag{36}$$

for all w with $|w| < |u|$. By (35) and (36),

$$(r,\epsilon)(\xi,u) + \sum_{vw=u,\ v\neq\epsilon} (r,v)(r^*s,w) + (s,u) \quad \leq \quad (\xi,u),$$

so that

$$(r,\epsilon)^*(\sum_{vw=u,\ v\neq\epsilon} (r,v)(r^*s,w) + (s,u)) \quad \leq \quad (\xi,u),$$

by the fixed point induction rule. Thus, by Lemma 8.5 below, $(r^*s,u) \leq (\xi,u)$. $\square$

LEMMA 8.5 *For all $u \in A^*$,*

$$(r,\epsilon)^*(\sum_{vw=u,\ v\neq\epsilon}(r,v)(r^*s,w)+(s,u)) \quad = \quad (r^*s,u).$$

Proof. Let us denote by $\mathrm{suf}(u)$ the set of all suffixes of u, i.e., the set of all $z \in A^*$ such that $z'z = u$ for some uniquely defined z'. Below we will denote z' by u/z. Then,

$$\begin{aligned}
&(r,\epsilon)^*(\sum_{vw=u,\ v\neq\epsilon}(r,v)(r^*s,w)+(s,u))\\
&= (r,\epsilon)^*(\sum_{vwz=u,\ v\neq\epsilon}(r,v)(r^*,w)(s,z)+(s,u))\\
&= \sum_{z\in\mathrm{suf}(u),z\neq u}(r,\epsilon)^*(\sum_{vw=u/z,\ v\neq\epsilon}(r,v)(r^*,w)(s,z))+(r,\epsilon)^*(s,u)\\
&= \sum_{z\in\mathrm{suf}(u),z\neq u}(r^*,u/z)(s,z)+(r^*,\epsilon)(s,u)\\
&= \sum_{z\in\mathrm{suf}(u)}(r^*,u/z)(s,z)\\
&= \sum_{vz=u}(r^*,v)(s,z)\\
&= (r^*s,u).
\end{aligned}$$

□

REMARK 8.6 A certain converse of Theorem 8.4 holds also. Suppose that S is an inductive *-semiring. Then $S\langle\langle A^*\rangle\rangle$ is an ordered semiring. We have proved that each linear function $\xi \mapsto r\xi + s$ over $S\langle\langle A^*\rangle\rangle$ has a least pre-fixed point solution, viz. s^*r. Thus, if $S\langle\langle A^*\rangle\rangle$ is turned into an inductive *-semiring, by any definition of srtar, then that star operation is the same as the one given in Definition 8.1.

PROBLEM 8.1 Does Theorem 8.4 hold for weak inductive *-semirings?

We now consider power series with coefficients in the dual semiring.

PROPOSITION 8.7 *Suppose that S is a *-semiring and A is a set. Then the *-semirings $(S\langle\langle A^*\rangle\rangle)^{\mathrm{op}}$ and $S^{\mathrm{op}}\langle\langle A^*\rangle\rangle$ are isomorphic.*

Proof. For each $s \in S\langle\langle A^*\rangle\rangle$, define the power series s^{op} by

$$(s^{\mathrm{op}}, u) \;=\; (s, u^{\mathrm{op}}), \quad u \in A^*,$$

where u^{op} is the word u written in the reverse order. The reader will have no difficulty to check that the function $s \mapsto s^{\mathrm{op}}$ is a semiring isomorphism $(S\langle\langle A^*\rangle\rangle)^{\mathrm{op}} \to S^{\mathrm{op}}\langle\langle A^*\rangle\rangle$. The fact that the star operation is preserved follows using Remark 8.2. Denoting the star operation in $S^{\mathrm{op}}\langle\langle A^*\rangle\rangle$ by $^{\otimes}$ (and the product operation by $\circ$), we have $((s^*)^{\mathrm{op}}, \epsilon) = (s, \epsilon)^* = ((s^{\mathrm{op}})^{\otimes}, \epsilon)$, for all $s \in S\langle\langle A^*\rangle\rangle$. For nonempty words u,

$$\begin{aligned}
((s^*)^{\mathrm{op}}, u) &= (s,\epsilon)^* \sum_{vw = u^{\mathrm{op}},\ v \neq \epsilon} (s, v)(s^*, w) \\
&= (\sum_{wv = u^{\mathrm{op}},\ v \neq \epsilon} (s^*, w)(s, v))(s, \epsilon)^* \\
&= (\sum_{vw = u,\ v \neq \epsilon} (s^*, w^{\mathrm{op}})(s, v^{\mathrm{op}}))(s, \epsilon)^* \\
&= (s^{\mathrm{op}}, \epsilon)^* \circ (\sum_{vw = u,\ v \neq \epsilon} (s^{\mathrm{op}}, v) \circ ((s^{\mathrm{op}}),^{\otimes} w)) \\
&= ((s^{\mathrm{op}})^{\otimes}, u).
\end{aligned}$$

□

COROLLARY 8.8 *If S is a symmetric inductive *-semiring, then so is any semiring $S\langle\langle A^*\rangle\rangle$ of power series.*

Proof. This follows from Theorem 8.4 and Proposition 8.7. □

REMARK 8.9 Suppose that S is a (symmetric) inductive *-semmiring. Then the star operation is uniquely determined by the semiring structure and the partial order. Thus, when $S\langle\langle A^*\rangle\rangle$ is ordered by the pointwise order, the star operation given above is the only one turning $S\langle\langle A^*\rangle\rangle$ into an inductive *-semiring.

9 A Kleene theorem for inductive *-semirings

DEFINITION 9.1 *Suppose that S is a *-semiring and $A \subseteq S$. A* mechanism *[7] over A is a triple $D = (\alpha, M, \beta)$, where $\alpha \in \{0,1\}^{1\times n}$, $\beta \in \{0,1\}^{n\times 1}$ and $M \in (A \cup \{0,1\})^{n\times n}$, for some $n \geq 0$. The* behaviour *of D is*

$$|D| \;=\; \alpha M^* \beta.$$

Mechanisms are called *presentations* in [6].

DEFINITION 9.2 *A* Kleene semiring[3] *is a* **-semiring* S *such that for all* $A \subseteq S$*, the following two sets are equal:*

1. $\mathbb{R}\partial\approx(A)$*, the sub* **-semiring generated by* A*.*
2. $\mathbb{R}(A)$*, the set of all behaviours over* A*.*

REMARK 9.3 For any *-semiring S and $A \subseteq S$, we have $\mathbb{R}(A) \subseteq \mathbb{R}\partial\approx(A)$, by the definition of the star operation on matrices. Thus S is a Kleene semiring iff $\mathbb{R}\partial\approx(A) \subseteq \mathbb{R}(A)$ holds for all $A \subseteq S$.

Suppose that $A \subseteq S$, where S is a *-semiring. For each $a \in A$, let

$$D_a \quad = \quad \left(\begin{bmatrix} 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right).$$

Moreover, let

$$\begin{aligned} D_0 &= ([0],[0],[0]) \\ D_1 &= ([1],[0],[1]). \end{aligned}$$

Then $|D_0| = 0$, and if $0^* = 1$ holds in S, $|D_a| = a$ and $|D_1| = 1$, so that $A \cup \{0,1\} \subseteq \mathbb{R}(A)$.

THEOREM 9.4 *Every Conway semiring is a Kleene semiring.*

Proof. Suppose that S is a Conway semiring and $A \subseteq S$. Since $0^* = 1$ holds in S, we have $A \cup \{0,1\} \subseteq \mathbb{R}(A)$. Thus, we only need to show that $\mathbb{R}(A)$ is closed under the sum, product and star operations. Following the proof of Theorem 8 in Chapter 3 of Conway [7], define

$$\begin{aligned} D &= (\alpha, M, \beta) \\ D' &= (\alpha', M', \beta') \end{aligned}$$

Define

$$\begin{aligned} D + D' &= \left(\begin{bmatrix} \alpha & \alpha' \end{bmatrix}, \begin{bmatrix} M & 0 \\ 0 & M' \end{bmatrix}, \begin{bmatrix} \beta \\ \beta' \end{bmatrix} \right) \\ D \cdot D' &= \left(\begin{bmatrix} \alpha & 0 \end{bmatrix}, \begin{bmatrix} M & \beta\alpha' \\ 0 & M' \end{bmatrix}, \begin{bmatrix} 0 \\ \beta' \end{bmatrix} \right) \\ D^* &= \left(\begin{bmatrix} 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \alpha \\ \beta & M \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) \end{aligned}$$

[3] Sakarovitch [22] defines a Kleene semiring as a *-semiring which can be embedded in a continuous semiring.

Then we have

$$\begin{aligned}
|D + D'| &= |D| + |D'| \\
|D \cdot D'| &= |D| \cdot |D'| \\
|D^*| &= |D|^*.
\end{aligned}$$

$\square$

COROLLARY 9.5 *Every inductive *-semiring is a Kleene semiring.*

For a version of Theorem 9.4, which also holds in all Conway semirings, see [4] or [6].
Suppose that S is a *-semiring and A is a set. We may identify any letter $a \in A$ with the power series r_a such that $(r_a, a) = 1$ and $(r_a, u) = 0$, for all words $u \in A^*$, $u \neq a$. We let $S^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ denote the set $\mathbb{R}\eth\approx(A)$. Note that $S^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is a *-semiring, and when S is ordered, also an ordered semiring. Since equations and implications are preserved by substructures, we have

PROPOSITION 9.6 *If S is a Conway semiring or an iteration semiring, then so is $S^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$, for all $A \subseteq S$. If S is an inductive *-semiring, then so is any $S^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$.*

10 Free inductive *-semirings

Since inductive *-semirings form a quasi-variety of ordered algebras, all free inductive *-semirings exist. In this section we provide an explicit description of the initial inductive *-semiring. In particular, we prove that the continuous *-semiring $\mathbb{N}_\infty$, obtained by adjoining a top element to the semiring $\mathbb{N}$ of natural numbers, is initial in the class of inductive *-semirings. We then conjecture that for any set A, the rational power series in $\mathbb{N}_\infty\langle\langle A^*\rangle\rangle$ form the free inductive *-semiring on the set A.
Since any inductive *-semiring is an iteration semiring, the initial inductive *-semiring is a quotient of the initial iteration semiring. The structure of the initial iteration semiring I_0 was described in [4, 6]. Its elements are

$$0, 1, 2, \ldots, 1^*, (1^*)^2, \ldots, 1^{**}.$$

The operations are the expected ones, so that $x + y$ and xy have their usual meaning for all $x, y \in \{0, 1, \ldots\}$, and

$$x + y \quad = \quad \max\{x, y\}$$

$$xy = \begin{cases} 0 & \text{if } x = 0 \text{ or } y = 0 \\ \max\{x, y\} & \text{if } x \in \{1, 2, \ldots\} \text{ or } y \in \{1, 2, \ldots\} \\ (1^*)^{m+n} & \text{if } x = (1^*)^m,\ y = (1^*)^n \\ 1^{**} & \text{if } x, y \neq 0 \text{ and } (x = 1^{**} \text{ or } y = 1^{**}), \end{cases}$$

if x or y is in the set $\{1^*, (1^*)^2, \ldots, 1^{**}\}$. The star operation is defined so that $0^* = 1$, the star of 1 is the element 1^*, and $x^* = 1^{**}$ for all $x \neq 0, 1$. Of course, the operation max refers to the linear order corresponding to the above sequencing of the elements of I_0. Note that this order is just the sum-order on I_0. But I_0 is not an inductive *-semiring, since

$$\begin{aligned} 2 \cdot 1^* + 1 &= 1^* + 1^* + 1 \\ &= 1^* + 1 \\ &= 1^*, \end{aligned}$$

yet $2^* = 1^{**} \not\leq 1^*$. To turn I_0 into an inductive *-semiring, we need to identify 1^* and 1^{**} and hence to collapse all elements in the set $\{1^*, (1^*)^2, \ldots, 1^{**}\}$. The resulting *-semiring is isomorphic to $\mathbb{N}_\infty$.

Theorem 10.1 *The continuous* **-semiring* $\mathbb{N}_\infty$*, equipped with the natural star operation, is initial in the class of inductive* **-semirings.*

Proof. We have already noted that $\mathbb{N}_\infty$ is an inductive *-semiring. By the above argument, $\mathbb{N}_\infty$ is initial in the class of all iteration semirings satisfying $1^* = 1^{**}$. But any inductive *-semiring S satisfies this equation, so that there is a unique *-semiring morphism $\mathbb{N}_\infty \to S$. Since the order on $\mathbb{N}_\infty$ is the sum-order, this morphism preserves the order. □

Corollary 10.2 *Any inductive* **-semiring is an iteration semiring satisfying* $1^* = 1^{**}$.

In fact, every *complete* (or countably complete) semiring is an iteration semiring satisfying $1^* = 1^{**}$, as shown in [4, 6]. (The fact that any complete semiring is a Conway semiring was established in [19] and [14].) Such a semiring S has a sum operation $\sum_{i \in I} s_i$, defined for all families $s_i \in S$, $i \in I$ which extends the binary sum operation and such that summation is associative and product distributes over all sums. For any complete semiring S and $s \in S$, we define $s^* = \sum_{n \geq 0} s^n$.
Equipped with the sum operation defined in (4), every continuous semiring is complete. On the other hand, there exist complete sum-ordered semirings

which are not inductive. For one example, consider the semiring R_∞^+ of non-negative real numbers with a top element ∞ adjoined, equipped with the sum operation

$$\sum_{i\in I} r_i = \begin{cases} \infty & \text{if } r_i \neq 0 \text{ for an infinite number of } i's, \\ & \text{or } \exists i\ r_i = \infty \\ \text{the usual sum} & \text{otherwise} \end{cases}$$

and multiplication

$$r_1 r_2 = \begin{cases} \infty & \text{if } r_1, r_2 \neq 0 \text{ and } \infty \in \{r_1, r_2\} \\ \text{the usual sum} & \text{otherwise.} \end{cases}$$

In this semiring we have $(1/2)^* = \infty$, but the least solution of the equation $x = x/2 + 1$ is 2.

Remark 10.3 The semiring $\mathbb{N}_\infty$ is also initial in the class of weak inductive *-semirings, and in the class of all continuous *-semirings.

Conjecture 10.4 *For any set A, the semiring $\mathbb{N}_\infty^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is the free inductive *-semiring on A.*

Since any inductive *-semiring is an iteration semiring, this conjecture is implied by the following:

Conjecture 10.5 *For any set A, the (unordered reduct of the) *-semiring $\mathbb{N}_\infty^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is the free iteration semiring on A satisfying the equation $1^* = 1^{**}$.*

If Conjectures 10.4 and 10.5 hold, then we also have:

Conjecture 10.6 *An equation holds in all inductive *-semirings iff it holds in all iteration semirings satisfying $1^* = 1^{**}$.*

The "Boolean versions" of all of the above three conjectures are known to hold.

Theorem 10.7 [18] *For each set A, the semiring $\mathbb{B}^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is freely generated by A in the class of all iteration semirings satisfying $1^* = 1$.*

See also [10]. Since $\mathbb{B}^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is an inductive *-semiring, and in fact a Kozen semiring, we also have

Corollary 10.8 *For each set A, the semiring $\mathbb{B}^{\mathrm{rat}}\langle\langle A^*\rangle\rangle$ is freely generated by A in the class of all idempotent inductive *-semirings.*

Corollary 10.9 [16] *For each set A, the semiring $\mathbb{B}^{\mathrm{rat}}\langle\!\langle A^*\rangle\!\rangle$ is freely generated by A in the class of all Kozen semirings.*

A generalization of Corollary 10.8 has been obtained in [11].

Theorem 10.10 *For any set A and for each natural number $k > 1$, the semiring $\daleth^{\mathrm{rat}}\langle\!\langle A^*\rangle\!\rangle$ is freely generated by the set A in the class of all symmetric inductive *-semirings satisfying the equation $k - 1 = k$.*

Of course, in the above equation, k denotes the k-fold sum of 1 with itself.

Conjecture 10.11 *For any integer $k > 1$, the semiring $\daleth^{\mathrm{rat}}\langle\!\langle A^*\rangle\!\rangle$ is the free iteration semiring on the set A satisfying the equation $k - 1 = 1^*$. Moreover, $\daleth^{\mathrm{rat}}\langle\!\langle A^*\rangle\!\rangle$ is the free inductive *- semiring on the set A satisfying the equation $k - 1 = k$.*

11 Summary

We have studied in detail the relation between 5 classes of *-semirings. In decreasing order of generality, these are Conway semirings, iteration semirings, inductive *-semirings, symmetric inductive *-semirings and continuous *-semirings. Except for continuous *-semirings, each class can be axiomatized within first order logic. Conway semirings and iteration semirings form two varieties of *-semirings, and inductive *-semirings and symmetric inductive *-semirings form two finitely axiomatizable quasi-varieties of ordered *-semirings. In contrast with Conway semirings, *-semirings do not have a finite basis for their identities. In addition to the iteration semiring identities, any iteration *-semiring satisfies equation $1^* = 1^{**}$. We have conjectured that the variety of *-semirings generated by the (unordered reducts of) inductive, symmetric inductive, or continuous *-semirings is exactly the subvariety of iteration *-semirings defined by the equation $1^* = 1^{**}$. The free continuous *-semiring on a set A may be described as the power series semiring $\mathbb{N}_\infty\langle\!\langle A^*\rangle\!\rangle$ (equipped with the pointwise order). We have conjectured that in each of the classes of iteration *-semirings satisfying $1^* = 1^{**}$, inductive *-semirings and symmetric inductive *-semirings, the free *-semirings can be described as the semirings $\mathbb{N}_\infty^{\mathrm{rat}}\langle\!\langle A^*\rangle\!\rangle$ of rational power series in $\mathbb{N}_\infty\langle\!\langle A^*\rangle\!\rangle$, equipped with the ponitwise order where appropriate. The above conjectures may be seen as natural extensions of some of Conway's conjectures [7] regarding the axiomatization of the regular sets, confirmed in Krob [18]. (For an extension of Krob's result in another direction, see Ésik [10].) The results of Krob [18] and those given in Kozen [16] and Ésik and Kuich [11] provide ample evidence for these conjectures.

Continuous *-semirings, Conway semirings and iteration *-semirings have been known to be closed for several constructions including matrix semirings, duals, and power series. In this paper, we have established the same closure properties of symmetric inductive *-semirings. Inductive *-semirings are closed for matrices and power series, but not for duals. From these facts, we have derived a general Kleene theorem applicable to all inductive *-semirings.

References

[1] H. Bekič. Definable operations in general algebras, and the theory of automata and flowcharts, *Technical Report*, IBM Laboratory, Vienna, 1969.

[2] A.J. Blikle. Nets: complete lattices with composition. *Bull. Acad. Polon. Sci. Ser. Math. Astronom. Phys.*, 19:1123–1127, 1971.

[3] S.L. Bloom. Varieties of ordered algebras. *J. Computer System Sciences*, 45:200–212,1976.

[4] S.L. Bloom and Z. Ésik. Matrix and matricial iteration theories, Part I, *Journal of Computer and System Sciences*. 46:381–408, 1993.

[5] S.L. Bloom and Z. Ésik. Equational axioms for regular sets. *Mathematical Structures in Computer Science*, 3:1–24, 1993.

[6] S.L. Bloom and Z. Ésik. *Iteration Theories: the Equational Logic of Iterative Processes.* EATCS Monographs on Theoretical Computer Science. Springer–Verlag, 1993.

[7] J.C. Conway. *Regular Algebra and Finite Machines.* Chapman and Hall, 1971.

[8] B.A. Davey and H.A. Priestly. *Introduction to Lattices and Order.* Cambridge University Press, 1990.

[9] J.W. de Bakker and D. Scott. A theory of programs. IBM, Vienna, 1969.

[10] Z. Ésik. Group axioms for iteration. *Information and Computation*, 148:131–180, 1999.

[11] Z. Ésik and W. Kuich. A generalization of Kozen's axiomatization of the equational theory of regular sets. To appear.

[12] J.S. Golan. *The Theory of Semirings with Applications in Computer Science.* Longman Scientific and Technical, 1993.

[13] M. Goldstern. Vervollständigung von Halbringen. Diploma Thesis, Technical University of Vienna, 1985.

[14] U. Hebish. The Kleene theorem in countably complete semirings. *Bayreuther Mathematische Schriften*, 31:55-66, 1990.

[15] R. Kimmo. *Quantales and Their Applications*. Longman Scientific and Technical, 1990.

[16] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. In *Proc. IEEE Symposium on Logic in Computer Science*, pages 214–225, 1991.

[17] D. Kozen. On Kleene algebras and closed semirings. In *Proc. MFCS '90*, LNCS 452, pages 26–47, Springer–Verlag, 1990.

[18] D. Krob. Complete systems of B-rational identities. *Theoretical Computer Science*, 89:207–343, 1991.

[19] W. Kuich. The Kleene and Parikh theorem in complete semirings. In *Proc. ICALP'87*, LNCS 267, pages 212–225, Springer-Verlag, 1987.

[20] E.G. Manes and M.A. Arbib. *Algebraic Approaches to Program Semantics*, Springer, 1986.

[21] D.M.R. Park. Fixpoint induction and proofs of program properties. In *Machine Intelligence* **5**, D. Michie and B. Meltzer, Eds., pages 59–78, Edinburgh Univ. Press, 1970.

[22] J. Sakarovitch. Kleene's theorem revisited. In: *LNCS 281*, pages 39–50, 1987.

[23] W. Wechler. *Universal Algebra for Computer Scientists*. EATCS Monographs on Theoretical Computer Science, Vol. 25. Springer-Verlag, 1992.

Recent BRICS Report Series Publications

RS-00-27 Zoltán Ésik and Werner Kuich. ***Inductive -Semirings*****. October 2000. 34 pp.**

RS-00-26 František Čapkovič. ***Modelling and Control of Discrete Event Dynamic Systems*****. October 2000. 58 pp.**

RS-00-25 Zoltán Ésik. ***Continuous Additive Algebras and Injective Simulations of Synchronization Trees*****. September 2000. 41 pp.**

RS-00-24 Claus Brabrand and Michael I. Schwartzbach. ***Growing Languages with Metamorphic Syntax Macros*****. September 2000.**

RS-00-23 Luca Aceto, Anna Ingólfsdóttir, Mikkel Lykke Pedersen, and Jan Poulsen. ***Characteristic Formulae for Timed Automata*****. September 2000. 23 pp.**

RS-00-22 Thomas S. Hune and Anders B. Sandholm. ***Using Automata in Control Synthesis — A Case Study*****. September 2000. 20 pp. Appears in Maibaum, editor,** ***Fundamental Approaches to Software Engineering: First International Conference*****, FASE '00 Proceedings, LNCS 1783, 2000, pages 349–362.**

RS-00-21 M. Oliver Möller and Rajeev Alur. ***Heuristics for Hierarchical Partitioning with Application to Model Checking*****. August 2000. 30 pp.**

RS-00-20 Luca Aceto, Willem Jan Fokkink, and Anna Ingólfsdóttir. ***2-Nested Simulation is not Finitely Equationally Axiomatizable*****. August 2000. 13 pp.**

RS-00-19 Vinodchandran N. Variyam. ***A Note on*** $\mathrm{NP} \cap \mathrm{coNP}/\mathrm{poly}$**. August 2000. 7 pp.**

RS-00-18 Federico Crazzolara and Glynn Winskel. ***Language, Semantics, and Methods for Cryptographic Protocols*****. August 2000. ii+42 pp.**

RS-00-17 Thomas S. Hune. ***Modeling a Language for Embedded Systems in Timed Automata*****. August 2000. 26 pp. Earlier version entitled** ***Modelling a Real-Time Language*** **appeared in Gnesi and Latella, editors,** ***Fourth International ERCIM Workshop on Formal Methods for Industrial Critical Systems*****, FMICS '99 Proceedings of the FLoC Workshop, 1999, pages 259–282.**