UNIVERSITY OF SZEGED Faculty of Science and Informatics

Doctoral School of Informatics Department of Foundations of Computer Science

Partial iteration theories

- abstract of doctoral dissertation -

Tamás Hajgató

Supervisor Dr. Zoltán Ésik Szeged, 2014



Introduction

Fixed point operations occur in just about all areas of theoretical computer science including automata and languages, the semantics of programming languages, process algebra, logical theories of computational systems, programming logics, recursive types and proof theory, computational complexity, etc. The equational properties of the fixed point, or dagger operation can be best described in the context of Lawvere theories of functions over a set equipped with structure, or more generally, in the context of abstract Lawvere theories (or just theories), or cartesian or co-cartesian categories, cf. [Law63, Elg75, BE93, SP00].

Iteration theories were introduced in [BEW80a], and independently and axiomatically in [É80] in order to describe the equational properties of the dagger operation in iterative and rational algebraic theories, cf. [WTWG76, Elg75]. In an iterative theory, dagger is defined by unique fixed points, and in rational theories, by least fixed points. In both types of theories, the dagger operation satisfies the same set of identities. These identities define iteration theories. In [BE93, SP00], it is argued that any nontrivial fixed point model satisfies the iteration theory identities.

In an iteration theory the fixed point operation takes a morphism $f: n \to n + p$ to a morphism $f^{\dagger}: n \to p$ which provides a solution to the fixed point equation

$$\xi = f \cdot \langle \xi, \mathbf{1}_p \rangle$$

in the morphism variable $\xi : n \to p$. If a theory is equipped with an additional structure, such as an additive structure, then the dagger operation is usually related to some "Kleenean operations".

For example, the theory of matrices over a semiring S has an additive structure. Under a natural condition, cf. [BE93], any dagger operation over a matrix theory determines and is determined by a star operation mapping an $n \times n$ square matrix A (i.e., a morphism $A : n \to n$) to an $n \times n$ square matrix A^* . Properties of the dagger operation are then reflected by corresponding properties of the star operation. In **Chapter 2**, which is based on [EH09], we show that this correspondence between the dagger and star operations

can naturally be generalized to arbitrary grove theories.

When S is a semiring of formal power series then the usual partially defined star operation determines and is determined by a partially defined dagger operation. But this is not the only example where it is natural to work with a partial dagger operation, since the dagger operation is necessarily a partial operation in (nontrivial) iterative theories.

In [BEW80b, E82] (see also [BE93], Theorem 6.4.5) it was shown that any iterative theory with at least one "constant" (i.e., morphism $1 \rightarrow 0$) can be turned into an iteration theory that has a total dagger operation. Moreover, the extension of the dagger operation to a total operation only depends on the choice of the constant that serves as the canonical solution of the fixed point equation associated with the identity morphism $1 \rightarrow 1$.

Chapter 3 is based on [EH11a]. Here we provide a generalization of this construction that is applicable to partial iterative theories. We give a sufficient condition ensuring that a partially defined dagger operation of a partial iterative theory can be extended to a total operation so that the resulting theory becomes an iteration theory. We show that this general result can be instantiated to prove that every iterative theory with at least one constant can be extended to an iteration theory. We also apply our main result to theories equipped with an additive structure. We show that our result implies the Matrix Extension Theorem of [BE93] and the Grove Extension Theorem of [BE03]. In the context of these theories, the extension theorem asserts that if we have unique solutions of certain "guarded" fixed point equations, then under certain conditions, the fixed point operation can be extended in a unique way to provide solutions to all fixed point equations such that the resulting theory becomes an iteration theory. Possible applications of these results include Process Algebra, where one usually deals with unique fixed points of guarded fixed point equations (cf. [Fok07]).

Iteration theories can be axiomatized by the Conway theory identities and a group identity associated with each finite (simple) group, cf. [É99]. Whereas the group identities are needed for completeness, several constructions in automata and language theory and other areas of computer science only require the Conway identities.

In [BE93], a general Kleene type theorem was proved for all Conway theories. However, in many models of interest, the dagger operation is only partially defined. **Chapter 4** is based on [EH11b]. Here we provide a Kleene theorem for partial Conway theories. We also discuss several application of this generic result.

Chapter 5 of this thesis is based on [EH14]. Here we give a description of the free iteration semirings using a simple congruence. However, at the time of the writing of this thesis we do not yet have a decidability result for the equational theory of iteration semirings. Moreover, the contents of Chapter 5 are unpublished at this time.

The publications that were used in the writing of this thesis are [EH11b], [EH11a], [EH09] and the forthcoming [EH14]. I have contributed to one more publication. This is [HH13].

Basic Definitions (Chapter 1 of the thesis)

In any category whose objects are the nonnegative integers we will denote the composite of the morphisms $f: n \to p$ and $g: p \to q$ in diagrammatic order as $f \cdot g$. The identity morphism corresponding to object p will be denoted $\mathbf{1}_p$. When n is a nonnegative integer, we will denote the set $\{1, 2, \ldots, n\}$ by [n]. Thus, [0] is the empty set. We assume that the reader has some familiarity with the concept of formal power series and rational power series. See [BR10] and [BR82] for an introduction to this subject.

Let us recall from [BE93] that a (Lawvere) theory T is a small category with objects the nonnegative integers such that each nonnegative integer n is the n-fold coproduct of the object 1 with itself. We assume that each theory T comes with distinguished coproduct injections $i_n : 1 \to n, i \in [n]$, called distinguished morphisms, turning n to an n-fold coproduct of object 1 with itself. By the coproduct property, for each finite sequence of scalar morphisms $f_1, \ldots, f_n : 1 \to p$ there is a unique morphism $f : n \to p$ such that $i_n \cdot f = f_i$, for each $i \in [n]$. This unique morphism is denoted $\langle f_1, \ldots, f_n \rangle$. The operation implicitly defined by the coproduct property is called tupling. In particular, when n = 0, tupling defines a unique morphism $0_p : 0 \to p$, for each $p \ge 0$. Note that $\mathbf{1}_n = \langle \mathbf{1}_n, \ldots, n_n \rangle$ for all nonnegative integers n. In addition, we will always assume that $\mathbf{1}_1 = \mathbf{1}_1$, so that $\langle f \rangle = f$ for each $f : \mathbf{1} \to p$. A theory T is termed trivial if $\mathbf{1}_2 = \mathbf{2}_2$. In a trivial theory, there is at most one morphism $n \to p$, for each $n, p \ge 0$.

Tuplings of distinguished morphisms are called *base morphisms*. For example, 0_n and $\mathbf{1}_n$ are base morphisms. When ρ is a mapping $[n] \to [p]$, there is an associated base morphism $n \to p$, the tupling $\langle (1\rho)_p, \ldots, (n\rho)_p \rangle$ of the distinguished morphisms $(1\rho)_p, \ldots, (n\rho)_p$.

The coproduct structure yields a *pairing* and a *separated sum* operation. Pairing takes a morphism $f : n \to p$ and a morphism $g : m \to p$ to a morphism $n + m \to p$ denoted $\langle f, g \rangle$. Separated sum takes a morphism $f : n \to p$ and a morphism $h : m \to q$ to a morphism $n + m \to p + q$.

A theory T is a subtheory of a theory T' if T is a subcategory of T' and has the same distinguished morphisms as T.

A basic example of a theory is \mathbf{Fun}_A the theory of functions over a set

A. In this theory, a morphism $n \to p$ is a function $f : A^p \to A^n$. Note the reversal of the arrow. The composite of morphisms $f : n \to p$ and $g : p \to q$ is their function composition written from right to left, which is a function $A^q \to A^n$. The distinguished morphisms are the projection functions.

Let $S = (S, +, \cdot, 0, 1)$ be a semiring [Gol99]. The matrix theory Mat_S over S has as morphisms $n \to p$ all $n \times p$ matrices in $S^{n \times p}$. Composition is matrix multiplication defined in the usual way. For each $i \in [p], p \ge 0$, the distinguished morphism $i_p : 1 \to p$ is the $1 \times p$ row matrix with a 1 on the *i*th position and 0's elsewhere. The theory Mat_S comes with a sum operation + defined on each hom-set $\operatorname{Mat}_S(n, p) = S^{n \times p}$. It is known that for each n, ($\operatorname{Mat}_S(n, n), +, \cdot, \mathbf{1}_n, \mathbf{0}_{n,n}$) is a semiring, since the product of two $n \times n$ matrices is an $n \times n$ matrix. In particular, $\operatorname{Mat}_S(1, 1)$ is isomorphic to S.

Let T be a theory. A nonempty collection of morphisms I is an *ideal* [BE93] of T if it is closed under tupling, composition with base morphisms on the left, and composition with arbitrary morphisms on the right. I is *proper* iff $\mathbf{1}_1 \notin I$. Note that every ideal contains the morphisms $0_p, p \ge 0$.

A partial dagger theory is a theory T equipped with a distinguished ideal D(T) and a partially defined dagger operation

$$^{\dagger}: T(n, n+p) \to T(n, p) \qquad \qquad n, p \ge 0$$

defined on morphisms $n \to n + p$ in D(T).

A partial Conway theory is a partial dagger theory subject to a certain set (see Section 1.1 of the thesis) of identities. A partial iteration theory is a partial Conway theory subject to the group identities, one identity per finite group. See Section 1.2 of the thesis for these identities. A partial iterative theory is a partial dagger theory T such that for each $f: n \to n+p$ in D(T), f^{\dagger} is the unique solution of the fixed point equation associated with f:

$$\xi = f \cdot \langle \xi, \mathbf{1}_p \rangle \tag{1}$$

in the variable $\xi : n \to p$. It is known [BE93] that every partial iterative theory is a partial iteration theory. A partial dagger theory is a *dagger theory* iff the distinguished ideal contains every morphism. We define the concepts of *Conway theory* and *iteration theory* in a similar manner.

Examples of iteration theories are the theories of continuous or monotone functions over complete partial orders equipped with the *least fixed point* operation as dagger. See [BE93] for details.

A ranked alphabet Σ is a family of pairwise disjoint sets $(\Sigma_n)_n$, where n ranges over the nonnegative integers. We assume that the reader is familiar with the notion of (total) Σ -trees over a set $X_p = \{x_1, \ldots, x_p\}$ of variables,

defined as usual, see e.g. [BE93]. Below we will denote the collection of finite and infinite Σ -trees by $T_{\Sigma}(X_p)$. We call a tree *proper* if it is not one of the trees x_i . Σ -trees form a theory Σ TR whose morphisms $n \to p$ are the *n*-tuples of trees in $T_{\Sigma}(X_p)$. Composition is defined by substitution for the variables x_i , and for $i \in [p]$, the tree with a single vertex labeled x_i serves as the *i*th distinguished morphism $1 \to p$. Thus, if $t : 1 \to n$ and $t'_1, \ldots, t'_n : 1 \to p$ in Σ TR, then $t \cdot \langle t'_1, \ldots, t'_n \rangle : 1 \to p$ is the tree obtained by substituting a copy of t'_i for each leaf of t labeled x_i , for $i \in [n]$. See [BE93] for details. A tree is called *regular* if up to isomorphism it has a finite number of subtrees. The subtheory of Σ TR containing only the regular Σ -trees is denoted Σ tr.

Let Σ be a ranked alphabet and let T be the theory ΣTR , or the theory Σ tr. Let the ideal D(T) consist of those morphisms $f: n \to p$ in T whose components $i_n \cdot f$, $i \in [n]$, are proper trees. It is known that for each $f: n \to n + p$ in D(T) (1) has a unique solution in the variable $\xi: n \to p$. Denoting this unique solution by f^{\dagger} , T becomes a partial iterative theory. Moreover, if Σ_0 is not empty, so that there is at least one morphism in T(1,0), then for any choice of a morphism $\bot : 1 \to 0$ the partial dagger operation can be *uniquely* extended to a totally defined dagger operation such that T becomes an iteration theory. See [BEW80a] and [E82], or [BE93].

Suppose that Σ contains a single letter \bot that has rank 0. Then any scalar morphism in Σ TR is either a distinguished morphism, or a morphism $\bot_{1,p} = \bot \cdot 0_p : 1 \to p$. Given $f : n \to n + p$, it holds that $f^{\dagger} = f^n \cdot \langle \bot_{n,p}, \mathbf{1}_p \rangle$, where $\bot_{n,p} = \langle \bot_{1,p}, \ldots, \bot_{1,p} \rangle : n \to p, f^0 = \mathbf{1}_n \oplus \mathbf{0}_p$ and $f^{k+1} = f \cdot \langle f^k, \mathbf{0}_n \oplus \mathbf{1}_p \rangle$. Let \bot TR denote this Conway theory. It is known that \bot TR is an initial Conway theory (and an initial iteration theory).

Let $T = \operatorname{Mat}_S$ be a matrix theory. Suppose that $I = (I(n, p))_{n,p}$ is a collection of morphisms containing the zero morphisms $0_{n,p}$ closed under sum and left and right composition with any morphism in T. Then we call I a *two-sided ideal* of T. Each two-sided ideal of T determines and is determined by a two-sided ideal of the semiring S (cf. [Gol99]), since if I is a two-sided ideal of S then the collection of those matrices all of whose entries belong to I_0 is a two-sided ideal of T.

When a matrix theory Mat_S is a Conway theory, the dagger operation determines a *star operation* mapping a matrix $A : n \to n$ to a matrix $A^* : n \to n$ by

$$A^* = (A \mathbf{1}_n)^{\dagger}.$$

In particular, S is equipped with a star operation $*: S \to S$. The equational properties of the dagger operation are then reflected by corresponding properties of the star operation. For example the fixed point identity corresponds

to the identity $A^* = AA^* + \mathbf{1}_n$, $A : n \to n$. Moreover, the double dagger identity corresponds to the identity

$$(A+B)^* = A^*(BA^*)^*$$

and the composition identity corresponds to

$$(AB)^* = 1 + A(BA)^*B$$

and in both identities $A, B : n \to n$. It is known that the star operation on \mathbf{Mat}_S determines and is uniquely determined by the star operation on S. Moreover, S, equipped with this star operation is a *Conway semiring*, or an *iteration semiring* [BE93, É99], if \mathbf{Mat}_S is an iteration theory.

Following [BEK08], we define a *partial Conway semiring* to be a semiring S equipped with a distinguished two-sided ideal I and a star operation $*: I \to S$ such that

$$(a+b)^* = a^*(ba^*)^*, \quad a,b \in I,$$

 $(ab)^* = 1+a(ba)^*b, \quad a \in I \text{ or } b \in I.$

The star operation can be extended to square matrices over I using the well-known matrix formula, see Section 1.2.1 of the thesis (this formula corresponds to the pairing identity as explained in [BE93]). Let $T = \operatorname{Mat}_S$ and denote by D(T) the ideal of those matrices all of whose entries are in I. Then T, equipped with the above dagger operation defined on morphisms $n \to n + p$ in D(T), $n, p \ge 0$, is a partial Conway theory. A partial iteration semiring is a partial Conway semiring subject to a set of identities, one identity per each finite group [BE09]. When S is a partial iteration semiring then $T = \operatorname{Mat}_S$ with D(T) defined as above is a partial iteration theory.

A star congruence on S is a semiring-congruence which preserves the partially defined star operation, i.e. for every $a, b \in I$, whenever a is equivalent to b then a^* is equivalent to b^* .

Recall that $\mathbb{N}^{\mathrm{rat}}\langle\!\langle \Delta^* \rangle\!\rangle$ denotes the semiring of rational power series over the semiring of the nonnegative integers. $\mathbb{N}^{\mathrm{rat}}\langle\!\langle \Delta^* \rangle\!\rangle$ is an example of a partial iteration semiring with the usual definition of star. More can be said. The following theorem is from [BE09]. The partial iteration semiring $\mathbb{N}^{\mathrm{rat}}\langle\!\langle \Delta^* \rangle\!\rangle$ of rational power series over the semiring of the nonnegative integers is freely generated by Δ in the category of partial iteration semirings.

A grove theory [BE93] is a theory equipped with the constants $+: 1 \rightarrow 2$

and $\#: 1 \to 0$ satisfying the following equations:

$$1_2 + 2_2 = 2_2 + 1_2,$$

$$(1_3 + 2_3) + 3_3 = 1_3 + (2_3 + 3_3),$$

$$1_1 + 0_{1,1} = 1_1.$$

The equations above are understood in the following way.

Suppose that $f, g: 1 \to p$ are morphisms in a grove theory. We define

$$f + g = + \cdot \langle f, g \rangle.$$

Moreover, for arbitrary $f = \langle f_1, \ldots, f_n \rangle, g = \langle g_1, \ldots, g_n \rangle : n \to p$ we define

$$f+g=\langle f_1+g_1,\ldots,f_n+g_n\rangle.$$

We say that the grove theory T is a subgrove theory of the grove theory T' if T is a subtheory of T' with the same constants + and #.

It follows that for each $n, p \ge 0$, $(T(n, p), +, 0_{n,p})$ is a commutative monoid. Moreover,

$$(f+g) \cdot h = (f \cdot h) + (g \cdot h),$$

$$0_{m,n} \cdot f = 0_{m,p},$$

for all $f, g: n \to p$ and $h: p \to q$. Note that distributivity on the left need not hold.

Examples of grove theories include all matrix theories Mat_S . In Mat_S , the morphism + is the matrix

$$\begin{pmatrix} 1 & 1 \end{pmatrix} : 1 \rightarrow 2$$

and # is the unique matrix $1 \rightarrow 0$.

A grove theory which is a (partial) Conway theory is a *(partial) Conway* grove theory. A grove theory which is a (partial) iteration theory is a *(partial)* iteration grove theory.

Suppose that L is a complete lattice with least element \bot . Thus, each direct power L^n of L is also a complete lattice. Recall that a function $L^p \to L^n$ is continuous [Sco72, BE93] if it preserves the suprema of (nonempty) directed sets. Let \mathbf{Cont}_L denote the theory of all continuous functions over L. Thus, \mathbf{Cont}_L is the subtheory of \mathbf{Fun}_L determined by the continuous functions.

Let + denote the function $L^2 \to L$, $(x, y) \mapsto x \lor y$, the supremum of the set $\{x, y\}$. It follows that for any $f, g: 1 \to p, f + g$ is the function $L^p \to L$

mapping $x \in L^p$ to $f(x) \vee g(x)$. Moreover, let # denote the least element \bot considered as a function $L^0 \to L$. Then \mathbf{Cont}_L is a grove theory. Note that for each n, p, the morphism $0_{n,p}$ is the function $L^p \to L^n$ which maps each $z \in L^p$ to \bot_n , the least element of L^n .

The theory $\operatorname{Lang}_{\Sigma}$ has morphisms $1 \to p$ the Σ -tree languages $L \subseteq T_{\Sigma}(X_p)$. The morphisms $n \to p$ are the *n*-tuples of morphisms $1 \to p$. Let $L: 1 \to p$ and $L' = (L'_1, \ldots, L'_p): p \to q$. Then $L \cdot L'$ is the collection of all trees in $T_{\Sigma}(X_q)$ that can be obtained by OI-substitution [ES77, ES78], i.e., the set of those trees t such that there is a tree $s \in L$ such that t can be constructed from s by replacing each leaf labeled x_i for $i \in [p]$ by some tree in L'_i so that different occurrences of x_i may be replaced by different trees. The distinguished morphism i_n is the set $\{x_i\}$, and the morphisms + and # are the sets $\{x_1, x_2\}$ and \emptyset , respectively. It then follows that addition is (component-wise) set union, and each component of any $0_{n,p}$ is \emptyset .

Generalized star (Chapter 2 of the thesis)

The contents of this chapter were published in [EH09].

We have seen that in matrix theories the dagger operation determines and is uniquely determined by a star operation. Every matrix theory is a grove theory, but there are grove theories that are not matrix theories. In this chapter, we consider grove theories equipped with a dagger operation and grove theories equipped with a generalized star operation, and under some natural assumptions we establish a correspondence between them in terms of a categorical isomorphism. We then use this isomorphism to relate equational properties of the dagger operation to equational properties of the generalized star operation. Due to this isomorphism such a translation from dagger to generalized star and vice versa is always possible, but we might get rather complicated equations as the result of a direct application of the isomorphism. In Chapter 2 we provide equivalent forms of the iteration theory identities in grove theories that use the generalized star operation instead of dagger, provided that some simple natural assumptions hold. Some of the equivalences proved assume the parameter identity. This is no problem for the applications, since any well-behaved dagger operation does satisfy this identity. For example, when the generalized star fixed point identity (see Section 2) holds, then for each $f: n \to n+p$, f^{\otimes} solves the fixed point equation

$$\xi = f \cdot \langle \xi, 0_n \oplus \mathbf{1}_p \rangle + (\mathbf{1}_n \oplus 0_p)$$

in the variable $\xi: n \to n + p$. When p = 0 this becomes

$$\xi = f \cdot \xi + \mathbf{1}_n.$$

Sections 2.1, 2.2 and 2.3 illustrate that our generalization of the correspondence between the dagger and star operations in matrix theories is well behaved and natural. In Section 2.1 we introduce *Conway and iteration star theories*. An easy corollary of the definitions is that the category of iteration star theories is isomorphic to the category of iteration theories.

In Conway theories, the group identities are implied by a simple implication, called the *functorial dagger implication*. In Section 2.1 we give two versions of the functorial dagger implication expressed with the generalized star operation. In Section 2.2 we introduce the concept of *ordered iteration* grove theory: an iteration grove theory is ordered iff there is a partial order on each hom-set which is preserved by the composition and tupling operations. Moreover, we require that for each p the morphism $0_{1,p}$ is the least morphism $1 \rightarrow p$. In the same section we give an equivalent formulation of the fixed point induction rule (See [Par69, É97]) using the generalized star operation.

Below, by a *dagger term* we will mean any term built in the usual way from symbols representing morphisms in dagger grove theories and the distinguished morphisms by composition, the cartesian operations, sum and dagger. Star terms are defined in the analogous way. Note that each dagger or star term has a source n and a target p, and under each evaluation of the morphism variables, the term evaluates to a morphism $n \to p$ in any dagger theory or generalized star theory. An equation t = t', or inequation $t \leq t'$ between dagger or star terms is a formal (in)equality between terms $t, t' : n \to p$. The validity or satisfaction of an (in)equation in a dagger grove theory or a generalized star theory is defined as usual.

In Section 2.3 we rephrase the a result from [E00] using the generalized star operation. This result of [É00] is as follows:

An (in)equation between dagger terms holds in all theories \mathbf{Cont}_L , where L is any complete lattice iff it holds in all ordered iteration grove theories satisfying $+^{\dagger} = \mathbf{1}_1$.

The last equation can also be written as $(1_2 + 2_2)^{\dagger} = \mathbf{1}_1$. As a corollary of the preceding sections we obtain:

An equation between star terms holds in all theories Cont_L , where L is any complete lattice iff it holds in all ordered iteration star theories satisfying $\mathbf{1}_1^{\otimes} = \mathbf{1}_1$.

In the same section we give a reformulation of an other result from $[\acute{E}00]$.

An equation between dagger terms holds in all theories \mathbf{Cont}_L iff it holds in all ordered idempotent grove theories which are dagger theories satisfying the (scalar versions) of the fixed point identity, the parameter identity, and the fixed point induction rule.

And the same with generalized star operation is as follows:

An equation between star terms holds in all theories \mathbf{Cont}_L iff it holds in all ordered idempotent generalized star theories satisfying the (scalar versions of the) generalized star fixed point identity, the generalized star parameter identity, and the generalized star fixed point induction rule.

The last two results also hold for the broader class of monotone functions.

Suppose that S is a *continuous monoid*, i.e., a commutative monoid S = (S, +, 0) equipped with a partial order \leq such that (S, \leq) is a cpo with least element 0, so that the supremum of each nonempty directed set exists, and the sum operation preserves such suprema (and is thus monotone).

Let Cont_S denote the theory of continuous functions over S. It is an iteration grove theory in the same way as the theory Cont_L , where L is a complete lattice. But unless the monoid S is idempotent, Cont_S is not necessarily idempotent. Note that unlike in [Boz99] or [Kui00], we do not require here any linearity conditions for the functions themselves.

The following results were proved in [É02]. We expressed them with the concepts we worked with.

An (in)equation between dagger terms holds in all theories Cont_S , where S is any continuous monoid iff it holds in all ordered iteration grove theories satisfying $(1_3 + 2_3 + 3_3)^{\dagger\dagger} = (1_2 + 2_2)^{\dagger}$ and $(1_2 + 2_2)^{\dagger} \cdot (f + g) = ((1_2 + 2_2)^{\dagger} \cdot f) + ((1_2 + 2_2)^{\dagger} \cdot g)$.

An (in)equation between dagger terms holds in all theories \mathbf{Cont}_S iff it holds in all ordered dagger grove theories satisfying the (scalar versions) of the fixed point identity, the parameter identity and the fixed point induction rule, together with the equation $(1_3+2_3+3_3)^{\dagger\dagger} = (1_2+2_2)^{\dagger}$ and $(1_2+2_2)^{\dagger} \cdot (f+g) = ((1_2+2_2)^{\dagger} \cdot f) + ((1_2+2_2)^{\dagger} \cdot g)$.

An (in)equation between star terms holds in all theories Cont_S , where S is any continuous monoid iff it holds in all ordered iteration star theories satisfying $\mathbf{1}_1^{\otimes\otimes} = \mathbf{1}_1^{\otimes}$ and $\mathbf{1}_1^{\otimes} \cdot (f+g) = (\mathbf{1}_1^{\otimes} \cdot f) + (\mathbf{1}_1^{\otimes} \cdot g)$, or when it holds in all ordered generalized star theories satisfying the star forms the (scalar versions) of fixed point identity, the parameter identity, the fixed point induction rule, together with the equations $\mathbf{1}_1^{\otimes\otimes} = \mathbf{1}_1^{\otimes}$ and $\mathbf{1}_1^{\otimes} \cdot (f+g) = (\mathbf{1}_1^{\otimes} \cdot f) + (\mathbf{1}_1^{\otimes} \cdot g)$.



Figure 1: γ is on the left and c is on the right.

Dagger Extension Theorem (Chapter 3 of the thesis)

The contents of this chapter were published in [EH11a].

In this section we give a sufficient condition ensuring that the dagger operation of a partial iterative theory be extendible to a total dagger operation such that the resulting theory becomes a Conway theory or an iteration theory.

Let T be a partial dagger theory with dagger operation \dagger_D defined on the morphisms $f: n \to n + p$ in D(T) and let T_0 be a subtheory of T. Suppose that T_0 is a dagger theory with dagger operation $^{\dagger_0}: T_0(n, n+p) \to T_0(n, p), n, p \ge 0.$

A description $(\alpha, a) : n \to q$ of weight s consists of a morphism $\alpha : n \to s + q$ in T_0 and a morphism $a : s \to q$ in D(T). We write $|(\alpha, a)|$ for the morphism $\alpha \cdot \langle a, \mathbf{1}_q \rangle$ in T, and call this morphism the behavior of the description (α, a) . Moreover, for a description $(\alpha, a) : n \to n + p$ of weight s, we define $(\alpha, a)^{\wedge}$ to be the description $(\gamma, c) : n \to p$ of weight s, where

$$\begin{aligned} \gamma &= (\alpha \cdot (\pi_{n,s} \oplus \mathbf{1}_p))^{\mathsf{T}_0} : n \to s+p, \\ c &= (a \cdot \langle \gamma, \mathbf{0}_s \oplus \mathbf{1}_p \rangle)^{\mathsf{T}_D} : s \to p. \end{aligned}$$

see Fig. 1. Here $\pi_{n,s}$ denotes the base morphism $\langle 0_n \oplus \mathbf{1}_s, \mathbf{1}_n \oplus 0_s \rangle : s + n \to n + s$ for all $n, s \ge 0$.

Recall that each partial iterative theory T is a partial iteration theory such that \dagger_D that provides unique solutions to fixed point equations $\xi = f \cdot \langle \xi, \mathbf{1}_p \rangle$, for all $f : n \to n + p$ in D(T). Below we will denote this operation by \dagger_D . The Dagger Extension Theorem is as follows: **Theorem 1** Let T be a partial iterative theory so that T is also a partial dagger theory with the operation \dagger_D defined on the morphisms $f: n \to n + p$ in D(T). Suppose that the following hold:

1.1. T_0 is a subtheory of T and a Conway theory with the operation

$$^{\dagger_0}: T_0(n, n+p) \to T_0(n, p), \qquad n, p \ge 0.$$

- 1.2. Each morphism $n \to p$ in T can be written as $\alpha \cdot \langle a, \mathbf{1}_p \rangle$, where $\alpha : n \to s + p$ is in T_0 and $a : s \to p$ is in D(T).
- 1.3. For all $\alpha : n \to s + n + p$, $\alpha' : n \to r + n + p$ in T_0 and $a : s \to n + p$, $a' : r \to n + p$ in D(T) the following holds:

$$|(\alpha,a)| = |(\alpha',a')| \quad \Longrightarrow \quad |(\alpha,a)^{\wedge}| = |(\alpha',a')^{\wedge}|$$

i.e.,

$$\alpha \cdot \langle a, \mathbf{1}_{n+p} \rangle = \alpha' \cdot \langle a', \mathbf{1}_{n+p} \rangle \implies \gamma \cdot \langle c, \mathbf{1}_p \rangle = \gamma' \cdot \langle c', \mathbf{1}_p \rangle,$$

where

$$(\gamma, c) = (\alpha, a)^{\wedge}$$
 and $(\gamma', c') = (\alpha', a')^{\wedge}$.

Then the operations \dagger_0 and \dagger_D can be uniquely extended to a totally defined operation $^{\dagger}: T(n, n+p) \rightarrow T(n, p)$ such that T equipped with † is a Conway theory. Moreover, if T_0 is an iteration theory then T is an iteration theory.

In Section 3.2 we consider some corollaries of the Dagger Extension Theorem. In the first corollary, we replace Assumption 1.3. of the Dagger Extension Theorem by a condition based on the notion of simulation [BE93] that is useful in many applications.

Call a morphism $f : n \to p$ of a nontrivial theory T ideal if none of the components $i_n \cdot f$ for $i \in [n]$ is a distinguished morphism. An iterative theory [Elg75] is a nontrivial partial iterative theory T such that D(T) is the collection of all ideal morphisms. Thus, each iterative theory comes with a partial dagger operation defined on the ideal morphisms $n \to n + p$.

In Section 3.3.1 we show that the following result from [BEW80b] and [É82] is an instance of the Dagger Extension Theorem.

Suppose that T is an iterative theory and $\perp : 1 \to 0$. Then there is a unique way of defining a dagger operation on T such that T becomes a Conway theory with $\mathbf{1}_1^{\dagger} = \perp$. Moreover, equipped with this dagger operation, T

is an iteration theory.

In Sections 3.3.2 and 3.3.3 we show that the Dagger Extension Theorem is a generalization of the Matrix Extension Theorem found in [BE93], on pages 323-335, and the extension theorem concerning grove theories, found in [BE03]. The proof goes by showing the the assumptions of the Matrix (resp. grove) Extension Theorem implies the assumptions of the Dagger Extension Theorem. The Matrix Extension Theorem (for semirings) is as follows:

Theorem 2 Let S be a semiring with a distinguished two-sided ideal I_0 . Suppose the following:

- 2.1. S_0 is a subsemiring of S that is a Conway semiring with star operation $*_0$.
- 2.2. For each $a \in I_0$ and $b \in S$, the equation x = ax + b has a unique solution in S.
- 2.3. Each $s \in S$ can be written as s = x + a for some $x \in S_0$ and $a \in I_0$.
- 2.4. For all $x, x' \in S_0$ and $a, a' \in I_0$, if x + a = x' + a' then x = x' and a = a'.

Then the operation $*^{\circ}$ can be extended in a unique way to the a star operation $*: S \to S$ such that S becomes a Conway semiring. Moreover, if S_0 is an iteration semiring, then S also becomes an iteration semiring.

Applications of Theorem 2 were given in [BE93] and [BE09]. Here we only mention the following result from [BE93].

Corollary 3 If S is an iteration semiring, then $S\langle\!\langle \Delta^* \rangle\!\rangle$, the semiring of formal power series over an alphabet Δ with coefficients in S is an iteration semiring. The same holds for $S^{rat}\langle\!\langle \Delta^* \rangle\!\rangle$, the semiring of rational power series over Δ with coefficients in S.

Suppose that T is a grove theory and T_0 is a sub-grove theory of T. Moreover, suppose that T_0 is a matrix theory. Note that if an ideal D(T) is closed under composition with arbitrary morphisms from T_0 on the left, then for all $f, g : n \to p$ in D(T) we have $f + g \in D(T)$ and $0_{n,p} \in D(T)$. We call an ideal D(T) a T_0 -*ideal*, if it is closed under composition with arbitrary morphisms from T_0 on the left.

The following is the grove extension theorem:

Theorem 4 Let T be a grove theory and T_0 a sub-grove theory of T that is a matrix theory. Further, assume that the following hold:

- 4.1. D(T) is a T_0 -ideal.
- 4.2. Every morphism in T can be written uniquely as $\alpha + a$, for some α in T_0 and a in D(T).
- 4.3. For all $\alpha : n \to p$ in T_0 and $f, g : p \to q$ in T we have

$$\alpha \cdot (f+g) = (\alpha \cdot f) + (\alpha \cdot g).$$

4.4. T_0 is a Conway theory with dagger operation

$$^{\dagger_0}: T_0(n, n+p) \to T_0(n, p), \qquad n, p \ge 0.$$

4.5. For every $\alpha : n \to p$ in T_0 and $a : n \to n + p$ in D(T), the fixed point equation $\xi = ((0_n \oplus \alpha) + a) \cdot \langle \xi, \mathbf{1}_p \rangle$ has a unique solution.

Then there is a unique way to define a total dagger operation † on T extending \dagger_0 such that T becomes a Conway theory. Further, if T_0 is an iteration theory, so is T.

A corollary of the Grove Extension Theorem is the following, see [BE03]. Recall that a formal tree series $1 \to p$ with coefficients in S is a mapping $T_{\Sigma}(X_p) \to S$ from the set of Σ -trees to a semiring S, cf. [EK03].

Corollary 5 The formal tree series over a ranked alphabet with coefficients in a Conway semiring S form a Conway grove theory containing the rational tree series as a sub-Conway grove theory. When S is an iteration semiring, both theories are iteration grove theories.

Kleene Theorem for Partial Conway theories (Chapter 4 of the thesis)

In this section we give a Kleene-type theorem for partial Conway theories and discuss several applications of this result. The contents of this chapter were published in [EH11b].

Let T be a partial dagger theory, T_0 a subtheory of T, and let A be a set of scalar morphisms in D(T). We write $A(T_0)$ for the set of morphisms $\langle f_1, \ldots, f_n \rangle : n \to p, n, p \ge 0$ such that each f_i is the composition of a morphism in A with a morphism in T_0 . In particular, $0_p \in A(T_0)$ for all $p \geq 0$. Note that if T_0 is T then $A(T_0)$ is the least ideal in T containing the morphisms in A, and if A is the set of scalar morphisms in D(T), then $A(T_0) = D(T)$ for every subtheory T_0 of T.

We say that (T_0, A) is *dagger compatible*, if for each $\alpha : n \to s + n + p$ in T_0 and $a : s \to s + n + p$ in $A(T_0), s, n, p \ge 0$,

$$\alpha \cdot \langle a^{\dagger}, \mathbf{1}_{n+p} \rangle \in D(T) \Longrightarrow \alpha \cdot \langle a, 0_s \oplus \mathbf{1}_{n+p} \rangle \in A(T_0).$$

This condition is fulfilled in a partial dagger theory T if (T_0, A) is strongly dagger compatible:

- 1. For all $\alpha : n \to p \in T_0$ and $a : p \to g \in A(T_0)$, $\alpha \cdot a \in A(T_0)$, i.e., when $A(T_0)$ is closed under left composition with T_0 -morphisms.
- 2. If $\alpha \cdot \langle f, \mathbf{1}_p \rangle \in D(T)$ for some $\alpha : n \to m + p \in T_0$ and $f : m \to p \in D(T)$, then $\alpha = \beta \oplus 0_p$ for some $\beta : n \to m$ in T_0 .

Below, when we write that (T_0, A) is a basis, we will mean that T_0 is a subtheory of T and A is a set of scalar morphisms in D(T).

We introduce the concept of presentation:

A presentation $n \to p$ of dimension s over a basis (T_0, A) is an ordered pair:

$$D = (\alpha, a) : n \to p,$$

where $\alpha : n \to s + p$ is in T_0 and $a : s \to s + p$ is in $A(T_0)$.

The *behavior* of D is the following morphism in T:

$$|D| = \alpha \cdot \langle a^{\dagger}, \mathbf{1}_p \rangle : n \to p$$

In Section 4.1 for every presentation D and E we define presentation $\langle D, E \rangle : n + m \to p$ and $D \cdot E : n \to q$. Moreover, we define $D^{\dagger} : n \to p$ whenever (T_0, A) is dagger compatible of when $T_0 \subseteq D(T)$ is closed under dagger.

Then we proceed to prove that $\langle |D|, |E| \rangle = |\langle D, E \rangle|, |D| \cdot |E| = |D \cdot E|$ and whenever (T_0, A) is dagger compatible or when $T_0 \subseteq D(T)$ is closed under dagger, then $|D|^{\dagger} = |D^{\dagger}|$.

Using these results we obtain the following Kleene-type theorem for partial Conway theories:

Theorem 6 Let T be a partial Conway theory with basis (T_0, A) . Suppose that either (T_0, A) is dagger compatible or $T_0 \subseteq D(T)$ is closed under dagger. Then a morphism f belongs to the least partial Conway subtheory of T containing T_0 and A iff f is the behavior of some presentation over (T_0, A) . In the theorem above the concept of *partial Conway subtheory* is understood in the following way. Suppose that T, T' are partial Conway theories. We say that T is a *partial Conway subtheory* of T', if T is a subtheory of T' and the distinguished ideal of T can be obtained by restricting the distinguished ideal of T' to T. Moreover, we require that the dagger operation of T can be obtained by restricting the dagger operation on T'.

In Section 4.2 we show the following corollary for grove theories:

Corollary 7 Suppose that T is a partial Conway grove theory with basis (T_0, A) such that T_0 is a matrix theory. Suppose that one of the following two conditions holds:

- 1. For all $x : 1 \to p$ in T_0 and $f : 1 \to p \in D(T)$, if $x + f \in D(T)$ then $x = 0_{1,p}$. Moreover, for all $x : 1 \to 1 \in T_0$ and $a, b : 1 \to p \in A(T_0)$, $x \cdot a \in A(T_0)$ and $a + b \in A(T_0)$.
- 2. For every $x : 1 \to 1 \in T_0$, x^* is defined and belongs to T_0 .

Then a morphism $n \to p$ belongs to the least partial Conway subgrove theory of T containing T_0 and A iff it is the behavior of some presentation over (T_0, A) .

In the theorem above the concept of partial Conway subgrove theory is understood in the following way. Suppose that T, T' are partial Conway grove theories. We say that T is a partial Conway subgrove theory of T', if T is a subgrove theory and a partial Conway subtheory of T'.

In Section 4.3 we show various applications of the Kleene theorem for partial Conway theories. We show a Kleene-type theorem for trees, sychronization trees (up to bisimulation), weighted tree automata and Büchi automata. We also show that Schützenberger's theorem, see [Sch61, Sch62] or [KS85] can be obtained as a corollary of our result.

Partial and total iteration semirings (Chapter 5 of the thesis)

In this chapter we give a description of the free iteration semirings using a simple congruence.

Recall that $\mathbb{N}^{\mathrm{rat}} \langle \langle (\Delta + \{ \bot \})^* \rangle \rangle$ denotes the semiring of rational power series over the semiring of nonnegative integers. Here $(\Delta + \{ \bot \})$ is the direct sum of the alphabets Δ and $\{ \bot \}$. First, we extend the partially defined star operation on $\mathbb{N}^{\mathrm{rat}} \langle \langle (\Delta + \{\bot\})^* \rangle \rangle$ to a totally defined star operation in the following way:

$$1^* = \bot$$

and for each $n = 2, 3, \ldots$

$$n^* = \bot^*$$

and for every proper $p \in \mathbb{N}^{\mathrm{rat}} \langle \langle (\Delta + \{\bot\})^* \rangle$ and $n = 1, 2, 3, \ldots$

$$(n+p)^* = (n^*p)^*n^*.$$
 (2)

Notice that star in (2) is well-defined, since n^*p is proper, because p is proper.

Now we define θ as the least star congruence on $\mathbb{N}^{\mathrm{rat}} \langle \langle (\Delta + \{\bot\})^* \rangle \rangle$ such that

$$(\bot + 1)\,\theta\,\bot\tag{3}$$

and

$$(\bot + \bot) \theta \bot. \tag{4}$$

We write F_{Δ} for the star semiring obtained by dividing $\mathbb{N}^{\mathrm{rat}} \langle \langle (\Delta + \{\bot\})^* \rangle \rangle$ with θ .

Remark 8 θ is the least star congruence on $\mathbb{N}^{\mathrm{rat}} \langle\!\langle (\Delta + \{\bot\})^* \rangle\!\rangle$ such that

$$\left(\bot^{k} + \bot^{m}\right)\theta \bot^{\max\{k,m\}} \tag{5}$$

for every $k, m \ge 0$.

Theorem 9 The iteration semiring F_{Δ} is freely generated by Δ in the category of iteration semirings.

Publications

The publications that were used in the writing of the thesis:

[EH09] Zoltán Ésik and Tamás Hajgató. Iteration grove theories with applications. In Symeon Bozapalidis and George Rahonis, editors, *Algebraic Informatics*, volume 5725 of *Lecture Notes in Computer Science*, pages 227-249. Springer-Verlag, 2009.

[EH11a] Zoltán Ésik and Tamás Hajgató. Dagger extension theorem. Mathematical Structures in Computer Science, 21(5):1035–1066, 2011. [EH11b] Zoltán Ésik and Tamás Hajgató. Kleene theorem in partial Conway theories with applications. In Werner Kuich and George Rahonis, editors, *Algebraic Foundations in Computer Science*, volume 7020 of *Lecture Notes in Computer Science*, pages 72–93. Springer-Verlag, 2011.

[EH14] Zoltán Ésik and Tamás Hajgató. On the structure of free iteration semirings. *Submitted for publication*, 2014.

The following publication was not used in the writing of the thesis:

[HH13] Masahito Hasegawa and Tamás Hajgató. Traced *-autonomous categories are compact closed. *Theory and Applications of Categories*, 28(7): 206 – 212, 2013.

Bibliography

- [BE93] Stephen L. Bloom and Zoltán Ésik. Iteration Theories: The Equational Logic of Iterative Processes. Springer-Verlag, 1993.
- [BE03] Stephen L. Bloom and Zoltán Ésik. An extension theorem with an application to formal tree series. *Journal of Automata, Languages and Combinatorics*, 8:145–185, 2003.
- [BE09] Stephen L. Bloom and Zoltán Ésik. Axiomatizing rational power series over natural numbers. *Information and Computation/Information and Control*, 207:793–811, 2009.
- [BEK08] Stephen L. Bloom, Zoltán Ésik, and Werner Kuich. Partial Conway and iteration semirings. *Fundamenta Informaticae*, 86(1,2):19–40, April 2008.
- [BEW80a] Stephen L. Bloom, Calvin C. Elgot, and Jesse B. Wright. Solutions of the iteration equation and extensions of the scalar iteration operation. *SIAM Journal on Computing*, 9:25–45, 1980.
- [BEW80b] Stephen L. Bloom, Calvin C. Elgot, and Jesse B. Wright. Vector iteration in pointed iterative theories. *SIAM Journal on Computing*, 9:525–540, 1980.
- [Boz99] Symeon Bozapalidis. Equational elements in additive algebras. Theory Computing Systems, 32(1):1–33, 1999.
- [BR82] Jean Berstel and Christophe Reutenauer. Recognizable formal power series on trees. *Theoretical Computer Science*, 18:115– 148, 1982.
- [BR10] Jean Berstel and Christophe Reutenauer. Noncommutative Rational Series with Applications. Cambridge University Press, 2010.

- [É80] Zoltán Ésik. Identities in iterative and rational algebraic theories. In Computational Linguistics and Computer Languages, XIV:183-207, 1980.
- [É82] Zoltán Ésik. On generalized iterative algebraic theories. In Computational Linguistics and Computer Languages, XV:95–110, 1982.
- [É97] Zoltán Ésik. Completeness of Park induction. *Theoretical Computer Science*, 177:217–283, 1997.
- [É99] Zoltán Ésik. Group axioms for iteration. Information and Computation/Information and Control, 148:131–180, 1999.
- [É00] Zoltán Ésik. Axiomatizing the least fixed point operation and binary supremum. In Peter Clote and Helmut Schwichtenberg, editors, *CSL*, volume 1862 of *Lecture Notes in Computer Science*, pages 302–316. Springer-Verlag, 2000.
- [É02] Zoltán Ésik. Continuous additive algebras and injective simulations of synchronization trees. Journal of Computer and System Sciences, 12(2):271–300, 2002.
- [EH09] Zoltán Ésik and Tamás Hajgató. Iteration grove theories with applications. In Symeon Bozapalidis and George Rahonis, editors, Algebraic Informatics, volume 5725 of Lecture Notes in Computer Science, pages 227–249. Springer-Verlag, 2009.
- [EH11a] Zoltán Ésik and Tamás Hajgató. Dagger extension theorem. Mathematical Structures in Computer Science, 21(5):1035–1066, 2011.
- [EH11b] Zoltán Ésik and Tamás Hajgató. Kleene theorem in partial Conway theories with applications. In Algebraic Foundations in Computer Science, volume 7020 of Lecture Notes in Computer Science, pages 72–93. Springer-Verlag, 2011.
- [EH14] Zoltán Ésik and Tamás Hajgató. On the structure of free iteration semirings. *Submitted for publication*, 2014.
- [EK03] Zoltán Ésik and Werner Kuich. Formal tree series. Journal of Automata, Languages and Combinatorics, 8:219–285, 2003.

- [Elg75] Calvin C. Elgot. Monadic computation and iterative algebraic theories. *Studies in Logic and the Foundations of Mathematics*, 80:175–230, 1975.
- [ES77] Joost Engelfriet and Erik Meineche Schmidt. IO and OI. I. Journal of Computer and System Sciences, 15(3):328–353, 1977.
- [ES78] Joost Engelfriet and Erik Meineche Schmidt. IO and OI. II. Journal of Computer and System Sciences, 16(1):67–99, 1978.
- [Fok07] Wan Fokkink. Introduction to process algebra. Springer-Verlag, 2007.
- [Gol99] Jonathan S. Golan. *Semirings and their applications*. Kluwer Academic Publishers, 1999.
- [HH13] Masahito Hasegawa and Tamás Hajgató. Traced *-autonomous categories are compact closed. *Theory and Applications of Categories*, 28(7):206 – 212, 2013.
- [KS85] Werner Kuich and Arto Salomaa. Semirings, Automata and Languages. Springer-Verlag, 1985.
- [Kui00] Werner Kuich. Linear systems of equations and automata on distributive multioperator monoids., pages 247–256. Klagenfurt: Verlag Johannes Heyn, 2000.
- [Law63] F. William Lawvere. Functorial semantics of algebraic theories. Proceedings of The National Academy of Sciences, 50:869–872, 1963.
- [Par69] David Park. Fixpoint induction and proofs of program properties. In D. Michie B. Meltzer, editor, *Machine Intelligence*, volume 5. University Press, Edinburgh, 1969.
- [Sch61] Marcel P. Schützenberger. On the definition of a family of automata. Information and Computation/Information and Control, 4:245–270, 1961.
- [Sch62] Marcel P. Schüutzenberger. On a theorem of R. Jungen. Proceedings of The American Mathematical Society, 13, 1962.
- [Sco72] Dana Scott. Continuous lattices, toposes, algebraic geometry and logic. In F. William Lawvere, editor, Proceedings of the 1971 Dalhousie conference, volume 274 of Lecture Notes in Computer Science, pages 97–136. Springer-Verlag, 1972.

- [SP00] Alex K. Simpson and Gordon D. Plotkin. Complete axioms for categorical fixed-point operators. In *Logic in Computer Science*, pages 30–41, 2000.
- [WTWG76] Jesse B. Wright, James W. Thatcher, Eric G. Wagner, and Joseph A. Goguen. Rational algebraic theories and fixed-point solutions. In *IEEE Symposium on Foundations of Computer Science*, pages 147–158, 1976.