Equational Properties of Fixed Point Operations in Cartesian Categories: An Overview

Zoltán Ésik(✉)

Department of Computer Science, University of Szeged, Szeged, Hungary
ze@inf.u-szeged.hu

Abstract. Several fixed point models share the equational properties of iteration theories, or iteration categories, which are cartesian categories equipped with a fixed point or dagger operation subject to certain axioms. After discussing some of the basic models, we provide equational bases for iteration categories and offer an analysis of the axioms. Although iteration categories have no finite base for their identities, there exist finitely based implicational theories that capture their equational theory. We exhibit several such systems. Then we enrich iteration categories with an additive structure and exhibit interesting cases where the interaction between the iteration category structure and the additive structure can be captured by a finite number of identities. This includes the iteration category of monotonic or continuous functions over complete lattices equipped with the least fixed point operation and the binary supremum operation as addition, the categories of simulation, bisimulation, or language equivalence classes of processes, context-free languages, and others. Finally, we exhibit a finite equational system involving residuals, which is sound and complete for monotonic or continuous functions over complete lattices in the sense that it proves all of their identities involving the operations and constants of cartesian categories, the least fixed point operation and binary supremum, but not involving residuals.

1 Introduction

The semantics of recursion and iteration is usually captured by fixed points of functions, functors, or other constructors. Fixed point operations have been widely used in several branches of computer science including automata and formal language theory and its generalizations, the semantics of programming languages, abstract data types, process algebra and concurrency, rewriting, programming logics and verification, complexity theory, and many other fields. The study of the equational properties of fixed point operations was initiated in the late 1960's, see [7,25–27,63,65,66,68,73] for a sampling of some early references.

Iteration theories were introduced in 1980 in [9] and [27]. (In [27], they were called generalized iterative theories.) The results obtained until the mid 1990's

Z. Ésik—Partially supported by grant no. ANN 110883 from the National Foundation for Scientific Research of Hungary.

G.F. Italiano et al. (Eds.): MFCS 2015, Part I, LNCS 9234, pp. 18–37, 2015.
DOI: 10.1007/978-3-662-48057-1_2

(summarized in [12,15]) indicated that they give a full account of the equational properties of most fixed point operations used in computer science.

The aim of this paper is to provide an overview of some old (see e.g. [27,32–34]) and some recent results (see e.g. [39,41,42]). Unlike in [12], instead of Lawvere theories [55,62], here we base our treatment on the slightly more general cartesian categories [5] and many-sorted theories [72]. There are several other alternative formalisms such as *abstract clones* [23], or the functional languages of μ-*terms* [4], or '*let rec expressions*', etc.

The paper is organized as follows. In Sect. 2, we define some of the basic fixed point models such as the cartesian categories of monotonic or continuous functions of complete partial orders (cpo's) or complete lattices, or the categories of complete metric spaces and contractions, trees and regular trees, etc. Our models will be equipped with a parametrized fixed point operation, also called dagger, such as the least or the unique fixed point operation. The main result of this section shows that our basic models satisfy the very same set of identities involving the operations and constants of cartesian categories and the fixed point operation. These identities define iteration theories, or iteration categories. In Sect. 3, we give axioms for iteration categories, and in Sect. 4, we offer an analysis of the axioms. Although there is no finite base of identities for iteration categories, in Sect. 5 we exhibit several finite axiom systems involving identities and implications (quasi-identities) that capture the equational theory of iteration categories. In Sect. 6, we enrich some of our models with an additive structure. The main results indicate that in many models of computational interest, the interaction between the iteration category structure and the additive structure can be described by a finite number of additional identities. This holds for example for the cartesian categories of monotonic or continuous functions of complete lattices with the least fixed point operation and the binary pointwise supremum operation as addition. Finally, in Sect. 7, we add residuation to the operations. We recall a recent result showing that there is a finite system of identities involving residuals, which is sound in the standard models of complete lattices and monotonic or continuous functions and complete for the identities not involving residuation.

Some Notation. We will denote the composition of morphisms $f : A \to B$ and $g : B \to C$ in a category $\mathcal{C}$ by $g \circ f : A \to C$ and the identity morphism corresponding to an object A by id_A. For a nonnegative integer $n \in \mathbb{N}$, we let $[n]$ denote the set $\{1, \ldots, n\}$, so that $[0]$ is the empty set. When X is a set, we denote by X^* the set of all finite sequences or words over X including the empty sequence ϵ.

2 Models

All categories $\mathcal{C}$ considered in this paper will be *cartesian categories* [5]. Thus we require the existence of a *product diagram*

$$\pi_i^{C_1 \times \cdots \times C_n} : C_1 \times \cdots \times C_n \to C_i, \quad i \in [n],$$

for any family of objects C_i, $i \in [n]$, $n \geq 0$, with the usual universal property. When $f_i : A \to C_i$, $i \in [n]$, is a family of morphisms in $\mathcal{C}$, the unique mediating morphism $f : A \to C_1 \times \cdots \times C_n$ with $\pi_i^{C_1 \times \cdots \times C_n} \circ f = f_i$ for all $i \in [n]$ will be denoted $\langle f_1, \ldots, f_n \rangle$. The morphism f is called the *(target) tupling* of the f_i. When $n = 0$, the tupling f is the unique morphism $!_A : A \to T$, where T is a fixed terminal object. It holds that

$$\mathsf{id}_{C_1 \times \cdots \times C_n} = \langle \pi_1^{C_1 \times \cdots \times C_n}, \ldots, \pi_n^{C_1 \times \cdots \times C_n} \rangle$$

for all objects $C_1, \ldots, C_n$, $n \geq 0$, i.e., the identity morphisms are tuplings of projections. A *Lawvere theory* [62] is a cartesian category whose objects are the nonnegative integers such that each object n is the n-fold product of the generating object 1.

Our cartesian categories $\mathcal{C}$ will be equipped with a *dagger operation* mapping a morphism $f : A \times C \to A$ to a morphism $f^\dagger : C \to A$. We list some of the categories of our interest.

1. $\mathbf{CPO}_m$ (resp. $\mathbf{CPO}_c$) is the category of *cpo*'s and monotonic (resp. continuous) functions, see e.g. [24,53]. The dagger operation is the (parametrized) least fixed point operation. In more detail, if $f : A \times B \to A$ is monotonic, where A, B are cpo's, then for each $y \in B$, $f^\dagger(y)$ is the least (pre-)fixed point of the monotonic function $f_y : A \to A$ defined by $f_y(x) = f(x, y)$ for all $x \in A$. It is known that $f^\dagger : B \to A$ is also monotonic, and when f is continuous, then so is $f^\dagger$.
2. $\mathbf{CL}_m$ (resp. $\mathbf{CL}_c$), the category of *complete lattices* and monotonic (resp. continuous) functions. The dagger operation is again the (parametrized) least fixed point operation.
3. Let $\mathbf{CM}$ denote the cartesian category of all *pointed complete metric spaces* and contractions (we only consider metric spaces such that the distance of any two points is at most 1.) Thus, when $M = (M, x_0, d)$ and $M' = (M', x_0', d')$ are pointed complete metric spaces and $f : M \to M'$ in $\mathbf{CM}$, then $d'(f(x), f(y)) \leq d(x, y)$ holds for all $x, y \in M$. The product of a family of metric spaces is equipped with the usual maximum distance.
   Regarding $\mathbf{CM}$, we introduce only a partial dagger operation. However, this partial dagger operation will still be sufficient for our purposes. The partial dagger operation is given as follows. Suppose that $f : A \times B \to A$ in $\mathbf{CM}$, where A and B are pointed complete metric spaces with distinguished points x_0 and y_0. Then $f^\dagger$ is defined iff $\lim_{n\to\infty} f_y^n(x_0)$ exists for all $y \in B$. Moreover, in this case, $f^\dagger(y) = \lim_{n\to\infty} f_y^n(x_0)$ for all y. It is not difficult to prove that when $f^\dagger$ is defined, then it is a contraction $B \to A$. Also, when f_y is a *proper contraction*, then $f^\dagger(y)$ is the unique fixed point of f_y by Banach's theorem.
4. Suppose that S is a set of *sorts* and Σ is an S-sorted *signature*, so that it contains a set of symbols $\Sigma_{u,s}$ for each $u \in S^*$ and $s \in S$. The objects of the category $\mathbf{Tree}_\Sigma$ of Σ*-trees* are all words in S^*. A morphism $u \to s$ ($u = s_1 \ldots s_n \in S^*, s \in S$) is a partial Σ-tree of sort s in the sorted variables $X_u = \{x_1^u, \ldots, x_n^u\}$. Such a tree may be seen as a labeled digraph, or as a

partial function $\mathbb{N}^* \to (\Sigma \cup X_u)^*$, subject to certain properties, cf. [53,72]. When $u, v \in S^*$ with $s = s_1 \dots s_n$, a morphism $u \to v$ is an n-tuple $f = (f_1, \dots, f_n)$, where each f_i is a tree $u \to s_i$.
Composition is given by substitution for the variables and categorical product corresponds to concatenation on objects. The projection morphisms are the trees with a single node, labeled by a variable. Trees $u \to v$ may be equipped with either a complete partial order [53], or a complete metric [3] and a distinguished point, the undefined tree. When $f : u \times v \to u$, then f induces a function over $\mathbf{Tree}_\Sigma(v, u)$ defined by $g \mapsto f \circ \langle g, \mathsf{id}_v \rangle$. The dagger operation returns the least fixed point of this function, or alternatively, we may define $f^\dagger$ using the complete metric as for **CM**.
5. Consider the model $\mathbf{Tree}_\Sigma$ and let $u, v \in S^*$ and $s \in S$. As usual, call a tree $f : u \to s$ *regular* if it has a finite number of subtrees, cf. [53]. Moreover, when $f : u \to v$, then call f regular if its components are. It is known that regular trees form a cartesian subcategory of $\mathbf{Tree}_\Sigma$ closed under dagger. We denote this category by $\mathbf{Reg}_\Sigma$.

We now define terms that will be used to denote morphisms in our models. Suppose that S_0 is a set of *basic types* (or *sorts*) $a, b, c, \dots$. The set of *product types* consists of all finite, possibly empty sequences $u, v, w, \dots$ in S_0^*. We usually denote such a sequence u by $a_1 \times \cdots \times a_n$, where $a_i \in S_0$, for all $i \in [n]$, and call the integer $|u| = n$ the length of u. Moreover, when $u = a_1 \times \cdots \times a_m$ and $v = b_1 \times \cdots \times b_n$, we let $u \times v = a_1 \times \cdots \times a_m \times b_1 \times \cdots \times b_n$.

For each $u, v \in S_0^*$, let $\Delta_{u,v}$ be a countably infinite set of 'morphism variables'. Then the sets $\mathrm{TERM}_{u,v}$ of *(typed) dagger terms*, where $u, v \in S_0^*$, are defined by:

1. $\pi_i^u \in \mathrm{TERM}_{u,a_i}$ for all $u = a_1 \times \cdots \times a_n \in S_0^*$ and $i \in [n]$.
2. $f \in \mathrm{TERM}_{u,v}$ for all $f \in \Delta_{u,v}$, $u, v \in S_0^*$.
3. If $t \in \mathrm{TERM}_{u,v}$ and $t' \in \mathrm{TERM}_{v,w}$, where $u, v, w \in S_0^*$, then $t' \circ t \in \mathrm{TERM}_{u,w}$.
4. If $t_i \in \mathrm{TERM}_{u,a_i}$ for all $i \in [n]$, $n \geq 0$, where $u \in S_0^*$ and $a_i \in S_0$ for all $i \in [n]$, then $\langle t_1, \dots, t_n \rangle \in \mathrm{TERM}_{u,v}$, where $v = a_1 \times \cdots \times a_n$.
5. If $t \in \mathrm{TERM}_{u \times v,u}$, then $t^\dagger \in \mathrm{TERM}_{v,u}$, where $u, v \in S_0^*$.

Below, instead of $t \in \mathrm{TERM}_{u,v}$, we will usually write $t : u \to v$.

When $u, v \in S_0^*$ with $u = a_1 \times \cdots \times a_m$ and $v = b_1 \times \cdots \times b_n$, we define $\pi_u^{u \times v} = \langle \pi_1^{u \times v}, \dots, \pi_m^{u \times v} \rangle : u \times v \to u$ and $\pi_v^{u \times v} = \langle \pi_{m+1}^{u \times v}, \dots, \pi_{m+n}^{u \times v} \rangle : u \times v \to v$. Sometimes we will also write $\pi_{(1)}^{u \times v}$ for $\pi_u^{u \times v}$ and $\pi_{(2)}^{u \times v}$ for $\pi_v^{u \times v}$. More generally, we define $\pi_{(i)}^{u_1 \times \cdots \times u_n}$ for each $u_1, \dots, u_n \in S_0^*$ and $i \in [n]$ in the same way. We will abbreviate the term $(\pi_u^{u \times v})^\dagger$ by $\perp_{v,u}$.

Suppose that $u = a_1 \times \cdots \times a_m$ and $\rho : [n] \to [m]$. Let $v = a_{\rho(1)} \times \cdots \times a_{\rho(n)}$. Then we associate with ρ (and u) the *base term*

$$\langle \pi_{\rho(1)}^u, \dots, \pi_{\rho(n)}^u \rangle : u \to v,$$

also denoted ρ. When $m = n$ and ρ is a bijective function, we call it a *base permutation term*. In particular, $\langle \pi_1^u, \dots, \pi_m^u \rangle$ is a base permutation term that we denote by id_u. The *inverse* ρ^{-1} of a base permutation term $u \to u$ associated with a bijection $\rho : [n] \to [n]$ with respect to $u \in S_0^*$ is the term associated with the inverse ρ^{-1} of ρ.

For any terms $t : u \to v$ and $t' : u \to w$, where v and w have length m and n, resp., we write $\langle t, t' \rangle$ as an abbreviation for

$$\langle \pi_1^v \circ t, \ldots, \pi_m^v \circ t, \pi_1^w \circ t', \ldots, \pi_n^w \circ t' \rangle : u \to v \times w.$$

Moreover, when $t : u \to v$ and $t' : u' \to v'$, we define $t \times t' : u \times u' \to v \times v'$ as the term $\langle t \circ \pi_u^{u \times u'}, t' \circ \pi_{u'}^{u \times u'} \rangle$.

When $\mathcal{C}$ is a cartesian category with a dagger operation and each basic type $a \in S_0$ is interpreted as an object $A = [\![a]\!]$ of $\mathcal{C}$, then each $u = a_1 \times \cdots \times a_n \in S_0^*$ can naturally be interpreted as the object $A_1 \times \cdots \times A_n$, where $A_i = [\![a_i]\!]$ for all $i \in [n]$. In particular, $[\![\epsilon]\!]$ is a fixed terminal object T (see also above). We assume that $[\![uv]\!] = [\![u]\!] \times [\![v]\!]$, for all $u, v \in S_0^*$.

And if each $f \in \Delta_{u,v}$, $u, v \in S_0^*$, is interpreted as a morphism $[\![u]\!] \to [\![v]\!]$ in $\mathcal{C}$, then each term $t \in \mathrm{TERM}_{u,v}$, $u, v \in S_0^*$, can be interpreted as a morphism $[\![t]\!] : [\![u]\!] \to [\![v]\!]$ in $\mathcal{C}$. The constant π_i^u, where $u = a_1 \times \cdots \times a_n$ and $i \in [n]$, is interpreted as the projection $[\![a_1]\!] \times \cdots \times [\![a_n]\!] \to [\![a_i]\!]$ according to a selected product diagram. We will assume that the selected product diagrams are 'associative on the nose'. In particular, we assume that when $n = 1$ and $i = 1$, then the projection π_i^u is the appropriate identity morphism. We skip the straightforward definition but remark that when t is a base term, its interpretation is a tupling of projections, called a *base morphism*.

Suppose that t and t' are in $\mathrm{TERM}_{u,v}$. Then we say that the formal equality $t = t'$ is an *identity*. Let $\mathcal{C}$ be a cartesian category with a dagger operation. We say that an identity $t = t'$ *holds in* $\mathcal{C}$, or *is satisfied by* $\mathcal{C}$, or *is valid in* $\mathcal{C}$, if $[\![t]\!] = [\![t']\!]$ holds for all interpretations over $\mathcal{C}$. The *equational theory* of $\mathcal{C}$ is the set of all identities satisfied by $\mathcal{C}$.

The following theorem summarizes several results treated in [12]. (Regarding **CM**, we only consider those interpretations that assign to each $f \in \Delta_{u,v}$ a function which is a tupling of proper contractions and projections, and the projections are assumed to pereserve the distinguished points.)

Theorem 1. *The categories* $\mathbf{CPO}_m, \mathbf{CPO}_c, \mathbf{CL}_m, \mathbf{CL}_c, \mathbf{CM}, \mathbf{Tree}_\Sigma, \mathbf{Reg}_\Sigma$ *satisfy the same set of identities.*

Motivated by Theorem 1, we adopt the following semantic definition of iteration categories.

Definition 1. *We define an* iteration category *to be a cartesian category* $\mathcal{C}$ *with a dagger operation satisfying all identities that hold in* $\mathbf{CPO}_m$. *An* iteration theory *is an iteration category which is a Lawvere theory.*

We say that a cartesian category $\mathcal{C}$ is nontrivial if there is some object A such that $\pi_1^{A \times A} \neq \pi_2^{A \times A}$. An equivalent condition is that some hom-set $\mathcal{C}(A, B)$ has at least two morphisms. It is shown in essence in [71] that if $\mathcal{C}$ is nontrivial cartesian category with a dagger operation which is an iteration category, then either $\mathcal{C}$ satisfies exactly the identities that hold in all iteration categories, or it satisfies exactly the identities satisfied by those iteration categories having a unique morphism $T \to A$ for each object A, where T is a terminal object.

Some further iteration categories or theories are the continuous and rational theories of [73], Elgot's (pointed) iterative theories [26], matrix theories over complete or inductive semirings [12,45]. theories of synchronization trees and bisimulation equivalence classes of synchronization trees [13], matricial theories of languages of finite and infinite words [12], theories of continuous functors [10] and functor theories over algebraically complete categories [49], iteration 2-theories [19], or the more recent cartesian categories of stratified complete lattices [43,50] used to solve fixed point equations involving non-monotonic functions, or the categories of formal power series over complete semirings [48].

The fixed point operation appears in several different forms. In cartesian categories with an appropriate additive structure on the hom-sets, it may be replaced by a *generalized star operation* $f \mapsto f^*$, where $f : A \times B \to A$ and $f^* : A \times B \to A$, or sometimes even by a star operation mapping a morphism $f : A \to A$ to a morphism $f^* : A \to A$, as in matrix theories over semirings. For details, see [12]. It is known that in cartesian categories, the fixed point operation is equivalent to a certain *trace* or *feedback operation* that maps a morphism $f : A \times B \to A \times C$ to a morphism $\uparrow f : B \to C$. See [6] and [22,54,56], or [12].

3 Axiomatization

In the previous section, we gave a semantic definition of iteration categories. In this section, we provide equational axioms for them consisting of axioms for cartesian categories, and axioms involving dagger.

A possible set of cartesian axioms is [72]:

$$\begin{aligned} h \circ (g \circ f) &= (h \circ g) \circ f, \quad f : u \to v, g : v \to w, h : w \to z \\ \mathsf{id}_v \circ f &= f = f \circ \mathsf{id}_u, \quad f : u \to v \\ \pi_i^v \circ \langle f_1, \dots, f_n \rangle &= f_i, \quad v = a_1 \times \cdots \times a_n,\ f_i : u \to a_i,\ i \in [n] \\ \langle \pi_1^v \circ f, \dots, \pi_n^v \circ f \rangle &= f, \quad f : u \to v,\ |v| = n \\ \pi_1^a &= \langle \pi_1^a \rangle \end{aligned}$$

Any model of these identities satisfies $g = \langle g \rangle$, where $g : u \to a$. Also, the following hold, for appropriate f, g, h, k:

$$\begin{aligned} \langle \langle f, g \rangle, h \rangle &= \langle f, \langle g, h \rangle \rangle \\ (f \times g) \times h &= f \times (g \times h) \\ (f \times g) \circ \langle h, k \rangle &= (f \circ h) \times (g \circ k) \end{aligned}$$

Below we will implicitly always assume the cartesian identities.

The *Conway identities* [12] are the *parameter* (1), *double dagger* (2) and *composition identities* (3) given below.

$$(f \circ (\mathsf{id}_u \times g))^\dagger = f^\dagger \circ g, \quad f : u \times v \to u,\ g : w \to v \tag{1}$$
$$(f \circ (\langle \mathsf{id}_u, \mathsf{id}_u \rangle \times \mathsf{id}_v))^\dagger = f^{\dagger\dagger}, \quad f : u \times u \times v \to u \tag{2}$$
$$(f \circ \langle g, \pi_w^{u\times w} \rangle)^\dagger = f \circ \langle (g \circ \langle f, \pi_w^{v \times w} \rangle)^\dagger, \mathsf{id}_w \rangle \tag{3}$$

where in the last identity, $f : v \times w \to u$, $g : u \times w \to v$.

Definition 2. *A* Conway category *is a cartesian category equipped with a dagger operation satisfying the Conway identities.*

The terminology follows [12] and is due to the form of these identities in matrix theories. Note that in Conway categories, the *fixed point identity*

$$f^\dagger = f \circ \langle f^\dagger, \mathsf{id}_v \rangle, \quad f : u \times v \to u \tag{4}$$

is a particular instance of the composition identity, and the identity

$$(f \circ \pi_v^{u \times v})^\dagger = f, \quad f : v \to u \tag{5}$$

is a particular instance of the fixed point identity (4), while

$$(f \circ \pi_{u \times v}^{u \times v \times w})^\dagger = f^\dagger \circ \pi_v^{v \times w}, \quad f : u \times v \to u \tag{6}$$

is an instance of the parameter identity (1). The parameter, double dagger and composition identities are sometimes called the identities of *naturality*, *diagonality* and *dinaturality*, see e.g. [71].

Conway categories satisfy several other non-trivial identities including the *Bekić identity* [7,25] (called the *pairing identity* in [12])

$$\langle f, g \rangle^\dagger = \langle f^\dagger \circ \langle h^\dagger, \mathsf{id}_w \rangle,\ h^\dagger \rangle \tag{7}$$

or its 'dual form'

$$\langle f, g \rangle^\dagger = \langle k^\dagger,\ \overline{g}^\dagger \circ \langle k^\dagger, \mathsf{id}_w \rangle \rangle, \tag{8}$$

where $f : u \times v \times w \to u$ and $g : u \times v \times w \to v$ and

$$h = g \circ \langle f^\dagger, \mathsf{id}_{v \times w} \rangle : v \times w \to v$$
$$k = f \circ \langle \pi_u^{u \times w}, \overline{g}^\dagger, \pi_w^{u \times w} \rangle : u \times w \to u$$

with $\overline{g} = g \circ (\langle \pi_v^{u \times v}, \pi_u^{u \times v} \rangle \times \mathsf{id}_w) : v \times u \times w \to v$. We will also make use of the *permutation identity* that holds in all Conway categories:

$$(\pi \circ f \circ (\pi^{-1} \times \mathsf{id}_v))^\dagger = \pi \circ f^\dagger, \tag{9}$$

where $f : u \times v \to u$ and $\pi : u \to u$ is a base permutation term. An alternative axiomatization of Conway categories consists of the identities (5), (6), (7) and (9). For this and related facts, we refer to [12].

The Conway identities are quite powerful, for example, a general 'Kleene theorem' holds in all Conway categories, and both the soundness and relative completeness of Hoare's logic can be proved just from the Conway identities, cf. [11,12]. However, they are not complete for iteration categories. The missing ingredient is captured by the notion of identities associated with finite automata. In order to define these identities, we need to introduce some definitions and notation.

Suppose that $\mathbf{Q} = (Q, Z)$ is a *(deterministic) finite automaton*, where Q is the finite nonempty set of *states*, Z is the finite nonempty set of *input letters* together with a *right action* $Q \times Z \to Q$, $(q, z) \mapsto qz$. Let $Q = \{q_1, \ldots, q_n\}$ and $Z = \{z_1, \ldots, z_m\}$, say. For each $i \in [n]$, let

$$\rho_i^{\mathbf{Q}} = \langle \pi^{u^n}_{(iz_1)}, \ldots, \pi^{u^n}_{(iz_m)} \rangle : u^n \to u^m,$$

$u \in S_0^*$, *where we identify each state q_i with the integer i*. Moreover, let $f^{\mathbf{Q}} : u^n \times w \to u^n$ be the tupling of the terms $f \circ (\rho_i^{\mathbf{Q}} \times \mathsf{id}_w) : u^n \times w \to u$, where $f : u^m \times w \to u^n$.

Definition 3. [32] *The* identity $\mathbf{C}(\mathbf{Q})$ associated with $\mathbf{Q}$ *is*

$$(f^{\mathbf{Q}})^\dagger = \tau_n \circ (f \circ (\tau_m \times \mathsf{id}_w))^\dagger,$$

where $f : u^m \times w \to u$, $\tau_n : u \to u^n$ is the diagonal $\langle \mathsf{id}_u, \ldots, \mathsf{id}_u \rangle$ *and τ_m is defined similarly. Suppose that a state $q = q_i$ of $\mathbf{Q}$ is distinguished, so that $(\mathbf{Q}, q)$ is an* initialized finite automaton*. The identity $\mathbf{C}(\mathbf{Q}, q)$ associated with $(\mathbf{Q}, q)$ is*

$$\pi^{u^n}_{(i)} \circ (f^{\mathbf{Q}})^\dagger = (f \circ (\tau_m \times \mathsf{id}_w))^\dagger,$$

where $f : u^m \times w \to u$.

Suppose that $\mathcal{C}$ is a Conway category. Since the permutation identity holds in $\mathcal{C}$, the validity of the identity associated with a finite automaton $\mathbf{Q}$ does not depend on the enumeration of the states or input letters. Also, $\mathbf{C}(\mathbf{Q})$ holds in $\mathcal{C}$ iff $\mathbf{C}(\mathbf{Q}, q)$ holds for all states q of $\mathbf{Q}$.

Theorem 2. [27] *The Conway identities and the identities associated with finite automata form a complete set of identities of iteration categories.*

Hence, these identities form a sound and complete axiomatization of iteration categories. In [27], the 'commutative identities' were used instead of the identities associated with finite automata. However, these are a very close variant of the identities associated with finite automata.

4 Analysis of the Axioms

Are all identities associated with finite automata strictly needed for completeness in Theorem 2? When is a set of identities consisting of the Conway identities and a subcollection of the identities associated with finite automata complete? In this section, we provide an answer to this question using the Krohn-Rhodes decomposition of finite automata [51,52,61] and a result from [35].

Suppose that $\mathbf{Q} = (Q, Z)$ is a finite automaton. The action of Z on Q is extended in the usual way to a right action $Q \times Z^* \to Q$ of Z^* on Q. When $\alpha \in Z^*$, we call the function $Q \to Q$ defined by $q \mapsto q\alpha$ for all $q \in Q$ the *function induced by* α and denote it by $\alpha^{\mathbf{Q}}$. These functions form a (finite) monoid $M(\mathbf{Q})$ whose multiplication is given by $\alpha^{\mathbf{Q}}\beta^{\mathbf{Q}} = (\alpha\beta)^{\mathbf{Q}} = \beta^{\mathbf{Q}} \circ \alpha^{\mathbf{Q}}$, for all $\alpha, \beta \in Z^*$.

Suppose that S and S' are finite semigroups. As usual, we say that S *divides* S', or S *is a divisor of* S', if S is a homomorphic image of a subsemigroup of S'. It is clear that this *divisibility relation* is transitive. It is known that if a group G is a divisor of a finite semigroup S, then there is a group H in S such that G is a homomorphic image of H. Moreover, we say that a finite group G is *simple* if it is nontrivial and has no nontrivial homomorphic image other than groups isomorphic to G (or equivalently, its only nontrivial normal subgroup is G itself).

Let $(\mathbf{Q}, q)$ be an initialized finite automaton, where $\mathbf{Q} = (Q, Z)$. We call $(\mathbf{Q}, q)$ an *initially connected finite automaton* if $Q = \{q\alpha : \alpha \in Z^*\}$.

Below we will write $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$ to mean that the cartesian category $\mathcal{C}$ equipped with a dagger operation satisfies $\mathbf{C}(\mathbf{Q})$. We will use similar notation for initially connected finite automata $(\mathbf{Q}, q)$.

Theorem 3. [33,42] *Suppose that $\mathcal{Q}$ is a set of finite automata (initially connected finite automata, resp.). Then the Conway identities and the identities associated with the members of $\mathcal{Q}$ form a complete set of identities for iteration categories iff for each finite simple group G there is some $\mathbf{Q}$ in $\mathcal{Q}$ ($(\mathbf{Q}, q) \in \mathcal{Q}$) such that G divides the monoid $M(\mathbf{Q})$ of $\mathbf{Q}$.*

The first part is from [33], and the second is from [42]. Each finite monoid M may be seen as a finite automaton $\mathbf{Q}_M = (M, M)$ equipped with the natural right action given by the multiplication operation of M. Hence, we may define the identity $\mathbf{C}(M)$ associated with M as the identity $\mathbf{C}(\mathbf{Q}_M)$ associated with $\mathbf{Q}_M$.

Corollary 1. [32] *Suppose that $\mathcal{M}$ is a set of finite monoids. Then the Conway identities and the identities associated with the members of $\mathcal{M}$ form a complete set of identities of iteration categories iff for each finite simple group G there is some $M \in \mathcal{M}$ such that G divides M.*

For each $n \geq 3$, consider the n-state initially connected automaton $(\mathbf{Q}_n, q_1)$ with state set $\{q_1, \ldots, q_n\}$, an input letter inducing the cyclic permutation $(q_1 \ldots q_n)$ and a letter inducing the transposition $(q_1 q_2)$, so that the monoid of $\mathbf{Q}_n$ is the symmetric group S_n of degree n. Then the Conway identities together with any infinite subsystem of the identities associated with the initially connected automata $(\mathbf{Q}_n, q_1)$ are complete for iteration categories, since every finite group can be embedded in any large enough symmetric group. It is shown in [33] that in Conway categories, the identity associated with $(\mathbf{Q}_n, q_1)$ may be reduced to

$$(f \circ (\tau_2 \times \mathsf{id}_w) \circ \langle f \circ \langle \pi_u^{u\times w}, (f^\dagger)^{n-2}, \pi_w^{u\times w} \rangle \ \pi_w^{u\times w} \rangle)^\dagger = (f \circ (\tau_2 \times \mathsf{id}_w))^\dagger \quad (10)$$

where $f : u^2 \times w \to u$ and $\tau_2 = \langle \mathsf{id}_u, \mathsf{id}_u \rangle : u \to u^2$. (Here, $(f^\dagger)^1 = f^\dagger$ and $(f^\dagger)^m = f^\dagger \circ \langle (f^\dagger)^{m-1}, \pi_w^{u\times w} \rangle$ for all $m \geq 2$.)

Theorem 4. [33] *The Conway identities together with any infinite subcollection of the identities (10) are complete for iteration categories.*

Theorem 3 follows from Theorem 2 and the following result:

Theorem 5. [33,42] *Suppose that $\mathcal{Q}$ is a set of finite automata (initially connected finite automata, resp.) and $\mathbf{Q}$ is a finite automaton. Then $\mathbf{C}(\mathbf{Q})$ holds in all Conway categories satisfying the identities associated with the members of $\mathcal{Q}$ iff for every simple group divisor G of $M(\mathbf{Q})$ there is some $\mathbf{Q}' \in \mathcal{Q}$ ($(\mathbf{Q}', q') \in \mathcal{Q}$, resp.) such that G divides $M(\mathbf{Q}')$.*

In the rest of this section we outline a proof of one direction of Theorem 5 which, by using recent advances [42], is simpler than the one in [33].

We start by recalling the *cascade composition* of finite automata [51,52]. Let $\mathbf{Q} = (Q, X)$ and $\mathbf{Q}' = (Q', Y)$ be finite automata. Suppose that φ is a function $Q \times X \to Y$. For each $q \in Q$ and $x \in X$, we will denote $\varphi(q, x)$ by ${}^q x$. The cascade composition of $\mathbf{Q}$ and $\mathbf{Q}'$ with respect to the connecting function φ is defined as the finite automaton $\mathbf{Q} \ltimes_\varphi \mathbf{Q}' = (Q \times Q', X)$ with action $(q, q')x = (qx, q'{}^q x)$ for all $q \in Q, q' \in Q'$ and $x \in X$.

The *direct product* is a special case of the cascade composition. It is obtained by letting $X = Y$ and choosing φ to be the identity function $X \to X$. Another special case arises when $\mathbf{Q}$ is a trivial 1-state automaton. Then φ may be viewed as a function $X \to Y$, so that the cascade composition is obtained from $\mathbf{Q}'$ by changing the input set Y to X and defining the function induced by each letter $x \in X$ as the function induced by some letter $y \in Y$ in $\mathbf{Q}'$. In this special case, we call the cascade composition a *letter renaming* of $\mathbf{Q}'$.

Theorem 6. [32] *Suppose that $\mathcal{C}$ is a Conway category. Let $\mathbf{Q} = \mathbf{Q}_1 \ltimes_\varphi \mathbf{Q}_2$ be a cascade product of finite automata $\mathbf{Q}_1$ and $\mathbf{Q}_2$. If $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_2)$ then $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$ iff $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_1)$.*

Proposition 1. [32] *Suppose that $\mathcal{C}$ is a Conway category. If $\mathbf{Q}'$ is a subautomaton of a finite automaton $\mathbf{Q}$ and $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$, then $\mathcal{C} \models \mathbf{C}(\mathbf{Q}')$.*

Suppose that $\mathbf{Q} = (Q, X)$ and $\mathbf{Q} = (Q, Y)$ are finite automata with the same set of states. We say that $\mathbf{Q}'$ is a *word renaming* of $\mathbf{Q}$ if each function induced by a letter $y \in Y$ in $\mathbf{Q}'$ is induced by some word $\alpha \in X^*$ in $\mathbf{Q}$.

Theorem 7. [42] *Suppose that $\mathcal{C}$ is a Conway category. If a finite automaton $\mathbf{Q}'$ is a word renaming of $\mathbf{Q}$, and if $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$, then $\mathcal{C} \models \mathbf{C}(\mathbf{Q}')$.*

Let $\mathbf{U}$ denote a 2-state automaton with 3 input letters, inducing the identity function and the 2 constant functions on the set of states. It is easy to see that the following holds.

Proposition 2. [32] *The identity* $\mathbf{C}(\mathbf{U})$ *holds in all Conway categories.*

Let $\mathcal{Q}$ be a set of finite automata and $\mathcal{C}$ a Conway category satisfying the identities associated with the members of $\mathcal{Q}$. Let $\mathbf{Q}$ be a finite automaton such that every finite simple group dividing the monoid of $\mathbf{Q}$ divides the monoid of some automaton in $\mathcal{Q}$. In order to prove the sufficiency part of Theorem 5, we need to show that $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$.

By the Krohn-Rhodes decomposition theorem, $\mathbf{Q}$ can be constructed from the automata in $\mathcal{Q} \cup \{\mathbf{U}\}$ by taking word renamings, cascade compositions, subautomata and homomorphic images. While it is obvious by induction from the above results that if $\mathbf{Q}$ can be constructed from $\mathcal{Q} \cup \{\mathbf{U}\}$ by using only word renamings, cascade compositions and subautomata, then the identity associated with $\mathbf{Q}$ holds in $\mathcal{C}$, there seems to be no simple way of extending the induction to homomorphic images. We outline a possible solution below.

If $\mathbf{Q} = (Q, Z) \in \mathcal{Q}$ with $M = M(\mathbf{Q})$, then consider the finite automaton $\mathbf{Q}' = (Q, M)$ where $qm = qu^{\mathbf{Q}}$ for all $q \in Q$ and $m = u^{\mathbf{Q}} \in M$. By Theorem 7, $\mathcal{C} \models \mathbf{C}(\mathbf{Q}')$. Consider now the monoid automaton $\mathbf{Q}_M = (M, M)$. It is well-known that $\mathbf{Q}_M$ can be embedded in a direct power of $\mathbf{Q}'$. Thus, by Theorem 6, it follows that $\mathcal{C} \models \mathbf{C}(M)$. Also, if H is any group in M, then it follows using Proposition 1 (and letter renaming) that $\mathcal{C} \models \mathbf{C}(H)$. Consider a normal subgroup N of H and the automata $\mathbf{Q}_{H/N}$ and $\mathbf{Q}_N$ associated with H/N and N, resp. We have that $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_N)$. It is well-known that $\mathbf{Q}_H$ is isomorphic to a cascade product of a letter renaming of $\mathbf{Q}_{H/N}$ and $\mathbf{Q}_N$, and since $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_H)$ and $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_N)$, it follows from Theorem 6 that $\mathcal{C} \models \mathbf{C}(\mathbf{Q}_{H/N})$. Since every simple group divisor of M divides some group H in M, and if N is a normal subgroup of H then every simple group divisor of H divides either N or H/N, it follows now by induction that $\mathcal{C}$ satisfies the identity associated with any simple group divisor of $M = M(\mathbf{Q})$. Since $\mathbf{Q} \in \mathcal{Q}$ was arbitrary, we established that $\mathcal{C}$ satisfies the identity associated with every simple group dividing the monoid of some automaton in $\mathcal{Q}$. Also, by a similar argument, we have:

Fact. If H is a finite group such that every simple group dividing H divides the monoid of some member of $\mathcal{Q}$, then $\mathcal{C} \models \mathbf{C}(H)$.

Call a finite automaton $\mathbf{Q} = (Q, Z)$ a *permutation automaton* if each $z \in Z$ induces a permutation of Q. It follows that $\alpha^{\mathbf{Q}}$ is a permutation of Q for all $\alpha \in Z^*$, so that $M(\mathbf{Q})$ is a group. Moreover, call $\mathbf{Q} = (Q, Z)$ a *permutation-reset automaton* if each $z \in Z$ induces a permutation or a constant map. Using the above fact, it follows as in Sects. 13 and 14 of [32] that if $\mathbf{Q}$ is a permutation-reset automaton such that every simple group divisor of $M(\mathbf{Q})$ divides the monoid of some automaton in $\mathcal{Q}$, then $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$. In order to complete the proof of the sufficiency part of Theorem 5, we need to establish this for all finite automata.

Suppose that $\mathbf{Q} = (Q, X)$ and $\mathbf{Q}' = (Q', X)$ are finite automata and $h : Q \to Q'$ is a surjective homomorphism $\mathbf{Q} \to \mathbf{Q}'$. Call h a *regular permutation-reset homomorphism* if the following conditions hold:

- For any two nontrivial congruence classes C, C' of $\ker(h)$ there is a word $\alpha \in X^*$ such that the restriction of $\alpha^{\mathbf{Q}}$ onto C is a bijection $C \to C'$.
- If C, C' are congruence classes of $\ker(h)$ and $\alpha \in Z^*$ such that $\alpha^{\mathbf{Q}}$ maps C into C', then the restriction of $\alpha^{\mathbf{Q}}$ onto C is either a constant function or a bijection.

Let C be a congruence class of $\ker(h)$. Denote by $M(C)$ the monoid of all functions $C \to C$ obtained as restrictions of functions $Q \to Q$ in $M(\mathbf{Q})$. When $\mathcal{G}$ is a set of finite simple groups, call h a *$\mathcal{G}$-homomorphism* if for any congruence class C of $\ker(h)$, every simple group divisor of $M(C)$ divides a group in $\mathcal{G}$. A novel proof of the Krohn-Rhodes theorem in [35] is based on the following result:

Theorem 8. [35] *Let $\mathcal{G}$ be a set of finite simple groups and suppose that $\mathbf{Q} = (Q, X)$ and $\mathbf{Q}' = (Q', X)$ are finite automata and $h : Q \to Q'$ is a surjective $\mathcal{G}$-homomorphism $\mathbf{Q} \to \mathbf{Q}'$. Then there is a sequence $\mathbf{Q}_0, \ldots, \mathbf{Q}_n$ of finite automata such that $\mathbf{Q}_0 = \mathbf{Q}$, $\mathbf{Q}_n = \mathbf{Q}'$ and for each $i \in [n]$, there is a regular permutation-reset $\mathcal{G}$-homomorphism $\mathbf{Q}_{i-1} \to \mathbf{Q}_i$ or $\mathbf{Q}_i \to \mathbf{Q}_{i-1}$.*

The next proposition is the final ingredient in our proof of the sufficiency part of Theorem 5. Let $\mathcal{G}$ be as above.

Proposition 3. [32] *Suppose that $\mathbf{Q} = (Q, X)$ and $\mathbf{Q}' = (Q', X)$ are finite automata and $h : Q \to Q'$ is a regular permutation-reset $\mathcal{G}$-homomorphism $\mathbf{Q} \to \mathbf{Q}'$. Suppose that $\mathcal{C}$ is a Conway category satisfying the identities $\mathbf{C}(G)$ associated with the members G of $\mathcal{G}$. Then $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$ iff $\mathcal{C} \models \mathbf{C}(\mathbf{Q}')$.*

Actually this result follows from Theorem 6 by a construction showing that if h is a regular permutation-reset $\mathcal{G}$-homomorphism, then $\mathbf{Q}$ can be embedded in a cascade product of $\mathbf{Q}'$ and a permutation-reset automaton whose simple group divisors are divisors of groups in $\mathcal{G}$.

The proof of the sufficiency part of Theorem 5 can now be completed as follows. Suppose that $\mathcal{Q}$ is a set of finite automata. Let $\mathcal{G}$ contain an isomorphic copy of the simple group divisors of the monoids of the automata in $\mathcal{Q}$. Let $\mathcal{C}$ be a Conway category satisfying all identities associated with the members of $\mathcal{Q}$. We already know that $\mathcal{C}$ satisfies the identity of any finite permutation-reset automaton $\mathbf{Q}$ such that any finite simple group dividing $M(\mathbf{Q})$ is isomorphic to a group in $\mathcal{G}$.

Now let $\mathbf{Q}$ denote a finite automaton such that every simple group divisor of $M(\mathbf{Q})$ has an isomorphic copy in $\mathcal{G}$. We want to prove that $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$.

Consider the unique homomorphism from $\mathbf{Q}$ onto a trivial 1-state automaton $\mathbf{Q}'$. By Theorem 8, there is a finite sequence $\mathbf{Q}_0, \ldots, \mathbf{Q}_n$ of finite automata such that $\mathbf{Q}_0 = \mathbf{Q}$, $\mathbf{Q}_n = \mathbf{Q}'$ and for each $i \in [n]$, there is a regular permutation-reset $\mathcal{G}$-homomorphism $\mathbf{Q}_{i-1} \to \mathbf{Q}_i$ or $\mathbf{Q}_i \to \mathbf{Q}_{i-1}$. It follows by repeated use of Proposition 3 that $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$ iff $\mathcal{C} \models \mathbf{C}(\mathbf{Q}')$. But the latter identity is easily shown to hold in all Conway categories by repeated use of the double dagger identity.

For initially connected finite automata, the sufficiency of Theorem 5 now follows from:

Proposition 4. [42] *Suppose that* $(\mathbf{Q}, q)$ *is an initially connected finite automaton and* $\mathcal{C}$ *is a Conway category. If* $\mathcal{C} \models \mathbf{C}(\mathbf{Q}, q)$ *then* $\mathcal{C} \models \mathbf{C}(\mathbf{Q})$.

Suppose that $\mathcal{G}$ is a set of nontrivial finite groups. Then there is a 'variety' $\mathcal{V}_{\mathcal{G}}$ of Conway categories corresponding to $\mathcal{G}$ which consists of those Conway categories satisfying the identities associated with the members of $\mathcal{G}$. (We have $\mathcal{V}_{\mathcal{G}_1} \subseteq \mathcal{V}_{\mathcal{G}_2}$) iff every finite simple group dividing a group in $\mathcal{G}_1$ divides a group in $\mathcal{G}_2$.) The free categories (or rather, theories) in $\mathcal{V}_{\mathcal{G}}$ have been described in [36]. In the particular case when $\mathcal{G}$ is empty, this description agrees with the characterization of the free Conway categories [8].

5 Implicational Axiomatizations

As a corollary of Theorem 3, we obtain:

Theorem 9. [18] *There is no finite complete set of identities of iteration categories.*

For a more direct proof, we refer to [18]. Many non-finitely based equational theories have a relatively finite axiomatization with respect to iteration categories (or theories), for example the equational theory of regular languages, or bisimilarity equivalence classes of regular processes. See Sect. 6. Theorem 9 can also be derived using these relative axiomatization results.

Although the equational theory of iteration categories is not finitely based, it can be captured by a finite number of implications involving equalities, and sometimes other relations depending on the context.

Our starting point is the identities associated with finite automata. In Conway categories, these are all consequences of the *weak functoriality* implications:

$$f \circ (\tau_n \times \mathsf{id}_w) = \tau_n \circ g \Rightarrow f^\dagger = \tau_n \circ g^\dagger, \quad n \geq 2,$$

for all $f : u^n \times w \to u^n$ and $g : u \times w \to u$, where $\tau_n : u \to u^n$ is the n-fold tupling $\langle \mathsf{id}_u, \ldots, \mathsf{id}_u \rangle$. Indeed, let $f : u^m \times w \to u$ and $g = f \circ (\tau_m \times \mathsf{id}_w)$, then using the notation introduced in Definition 3, we clearly have $f^{\mathbf{Q}} \circ (\tau_n \times \mathsf{id}_w) = \tau_n \circ g$, hence $(f^{\mathbf{Q}})^\dagger = \tau_n \circ g^\dagger$, by weak functoriality. Since the weak functoriality implications hold in $\mathbf{CPO}, \mathbf{CPO}_m, \mathbf{CM}, \Sigma\mathbf{Tree}$ and many other models, we immediately obtain:

Proposition 5. *An identity holds in all iteration categories iff it holds in all Conway categories satisfying weak functoriality.*

The weak functoriality implications already appear in [27], where Proposition 5 is implicit. In fact, the commutative identities were introduced in [27] just in order to make one step further by replacing these implications with weaker and pure equational axioms that still guarantee completeness. The existence of an iteration theory not satisfying the weak functoriality implication for $n = 2$ was pointed out in [28]. It is shown in [29] that in Conway categories, if the weak functoriality implications hold when u is a basic type a, then so do the generic forms of these implications. Moreover, as shown in [14], for each $n \geq 2$, there is a Conway category satisfying the weak functorial implication for all $2 \leq m \leq n$. but not satisfying this implication for $n + 1$.

Another variant of Proposition 5 concerns functoriality with respect to 'pure' [12] or 'strict' morphisms:

Proposition 6. *An identity holds in all iteration categories iff it holds in all Conway categories satisfying the following rule:*

$$f \circ (h \times \mathsf{id}_w) = h \circ g \ \wedge \ h \circ \bot_{\epsilon,u} = \bot_{\epsilon,v} \Rightarrow f^\dagger = h \circ g^\dagger$$

for all $f : u \times w \to u$*,* $g : v \times w \to v$ *and* $h : u \to v$*.*

Again, this implication holds in most standard models. Thus, Proposition 6 is clear from Proposition 5 since any base morphism is pure.

There are several other similar completeness results, including e.g. the implication

$$f^{\dagger\dagger} = g^{\dagger\dagger} \Rightarrow f^{\dagger\dagger} = (f \circ \langle g^\dagger, \mathsf{id}_{u\times w}\rangle)^\dagger,$$

where $f, g : u \times u \times w \to w$, introduced in [12] as a generalization of an axiom proposed for regular languages in [2], a version of the *Scott induction principle* [44], or the (conditional) *unique fixed point rule* of Elgot [26], cf. [12,27].

In the ordered setting, the *fixed point induction rule* (or *least pre-fixed point rule*) also gives rise to completeness. Call a cartesian category $\mathcal{C}$ *ordered* if each hom-set $\mathcal{C}(A, B)$ comes with a partial order $\leq$ preserved by composition and tupling. For example, $\mathbf{CPO}_m, \mathbf{CPO}_c, \mathbf{CL}_m, \mathbf{CL}_c$, equipped with the pointwise order of functions, are all ordered. The cartesian categories $\mathbf{Tree}_\Sigma$ and $\mathbf{Reg}_\Sigma$ can also be turned into ordered cartesian categories. Each of the above models satisfies the fixed point induction rule:

$$f \circ \langle g, \mathsf{id}_v\rangle \leq g \Rightarrow f^\dagger \leq g, \tag{11}$$

for all $f : u \times v \to u$ and $g : v \to u$.

Theorem 10. [30] *An identity holds in all iteration categories iff it holds in all ordered cartesian categories equipped with a dagger operation satisfying the fixed point (4) and parameter identities (1) and the fixed point induction rule (11).*

In all such theories, the dagger operation is also monotonic. There is another, stronger version of this result.

Theorem 11. [30] *An identity holds in all iteration categories iff it holds in all ordered cartesian categories equipped with a dagger operation satisfying the fixed point (4), parameter (1) and pairing identities (7) and a weak form of the fixed point induction rule:* $f \circ \langle g, \mathsf{id}_v\rangle = g \Rightarrow f^\dagger \leq g$*, where* $f : u \times v \to u$ *and* $g : v \to u$*.*

A natural question concerns the axiomatic characterization of the inequalities $t \leq t'$ between dagger terms that hold in the models $\mathbf{CPO}_m, \mathbf{CPO}_c$, etc. Call an iteration category $\mathcal{C}$ an *ordered iteration category* if it is an ordered cartesian category such that dagger is monotonic and $\perp_{B,A} \leq f$ for all $f : B \to A$, where $\perp_{B,A} = (\pi_A^{A\times B})^\dagger$. Then an inequality $t \leq t'$ holds in all cartesian categories $\mathbf{CPO}_m$ or in any of the standard ordered models mentioned above iff it holds in all ordered iteration theories.

6 Relative Axiomatization

Several iteration categories have an additional structure, such as a partial order or an additive structure. For example, each hom-set of the cartesian category $\mathbf{CL}_m$ or $\mathbf{CL}_c$ is partially ordered by the pointwise ordering, and the binary supremum operation gives rise to an additive structure.

In this section, we are interested in the interaction between the iteration category structure and the additional structure. We review several relative axiomatization results showing that this interaction can often be described by a finite number of additional identities. We extend our dagger terms with the formation of terms of the form $t+t'$, where $t, t' : u \to v$. Below we will often write $t \leq t'$ as an abbreviation for the identity $t+t' = t'$, where t, t' are extended terms $u \to v$.

We start by recalling a result from [34] that provides a characterization of the identities of the models $\mathbf{CL}_m$ or $\mathbf{CL}_c$ equipped with binary supremum as the $+$ operation.

Theorem 12. [34] *An identity between extended terms holds in all cartesian categories* $\mathbf{CL}_m$ *or* $\mathbf{CL}_c$ *iff it holds in all iteration categories with an additive structure satisfying the following identities:*

$$(f+g)+h = f+(g+h), \quad f,g,h : u \to v \tag{12}$$

$$f+g = g+f, \quad f,g : u \to v \tag{13}$$

$$f + \perp_{u,v} = f, \quad f : u \to v \tag{14}$$

$$(f+g)\circ h = (f\circ h) + (g \circ h), \quad f,g : v \to w, h : u \to v \tag{15}$$

$$(\pi_{(1)}^{u^2} + \pi_{(2)}^{u^2})^\dagger = \mathsf{id}_u \tag{16}$$

$$f^\dagger \leq (f+g)^\dagger, \quad f,g : u \times v \to u \tag{17}$$

In any model $\mathcal{C}$ of these axioms, the $+$ operation is idempotent and defines a partial order on each hom-set: when $f, g : A \to B$, then $f \leq g$ iff $f+g = g$, so that $f+g$ is the supremum of f and g. It is clear that the operation $+$ is monotonic in both arguments, moreover, it follows by (15) that composition is monotonic in the first argument. The last axiom asserts that dagger is monotonic, and together with the other axioms implies that composition is also monotonic in the second argument.

The fixed point induction rule (11) holds in the categories $\mathbf{CL}_m$ and $\mathbf{CL}_c$. Combining Theorem 12 with Theorem 10 we obtain:

Corollary 2. [34] *An identity between extended terms holds in all cartesian categories* $\mathbf{CL}_m$ *or* $\mathbf{CL}_c$ *iff it holds in all cartesian categories equipped with a dagger operation satisfying the fixed point (4) and parameter identities (1), the fixed point induction rule (11), and the identities (12) – (16).*

In fact, (16) may be replaced in Corollary 2 by the following identity:

$$f + f = f, \quad f : u \to v \tag{18}$$

There is a connection to formal languages, and context-free languages in particular. Suppose that Σ is a finite alphabet and consider the category whose objects are the finite sets with an A-indexed family $f = (f_a)_{a \in A}$ of languages (or just context-free languages) in $(B \cup \Sigma)^*$ as a morphism $B \to A$. Composition is defined by substitution and the identity morphism id_A is the family $(\{a\})_{a \in A}$. This category $\mathbf{Lang}_\Sigma$ (or $\mathbf{CF}_\Sigma$ in the context-free case) has finite products given on objects by disjoint union. Moreover, it has a $+$ operation defined by set union, and a dagger operation defined by least fixed points. Indeed, we may view a morphism $A \times B \to A$ as a 'generalized context-free grammar' with nonterminals in A and terminal symbols in $B \cup \Sigma$, possibly having an infinite number of rules. Then for each $a \in A$, the a-component of $f^\dagger : B \to A$ is the language generated from the nonterminal a.

Theorem 13. [39] *An identity between extended terms holds in all cartesian categories* $\mathbf{Lang}_\Sigma$ *or* $\mathbf{CF}_\Sigma$ *iff it holds in all iteration categories with an additive structure satisfying the identities (12) – (17).*

It is remarkable that the very same identities also characterize *simulation equivalence* [64,67] of processes, or *synchronization trees* (i.e., unfoldings of processes). For details, we refer to [34].

There are several further relative axiomatization results. We mention a few. *Bisimulation equivalence* [64,67] is weaker than simulation equivalence and can be characterized by the first five identities (12) – (16) of Theorem 12, cf. [13]. For *probabilistic* and *weighted bisimulation*, we refer to [1,40]. In order to get language equivalence, one needs to add

$$\begin{aligned} f \circ (g + h) &= (f \circ g) + (f \circ h), \quad f : v \to w, g, h : u \to v \\ f \circ \bot_{u,v} &= \bot_{u,w}, \quad f : v \to w \end{aligned}$$

Since by these identities, dagger can be replaced by a star operation and vice versa, cf. [12], this is a categorical version of Krob's result [60] on the axiomatization of the equational theory of (regular) languages equipped with the regular operations. For extensions of Krob's theorem to rational power series we refer to [17,46]. For implicational axiomatization of regular languages see [20,21,57–60], for rational power series [17,47], and for regular tree languages and tree series [16,31,37,38].

7 Adding Residuation

By Theorem 9, iteration categories have no finite base for their identities. The same fact holds for the identities between extended terms involving + that hold in the models $\mathbf{CL}_m$ or $\mathbf{CL}_c$. In this section, we consider these standard models together with + and (left) residuation. Following [41], we provide a simple system of identities, involving the operations and constants of cartesian categories, dagger, + and residuation, which, in addition to being sound, is complete for the set of valid identities not involving residuation. A similar program was carried out in [69] for Kleene algebras. Besides Corollary 2, the main tool of the completeness proof, borrowed from [69,70], is that the fixed point induction rule can be transformed into an identity involving residuals.

Suppose that $\mathcal{C}$ is a cartesian category equipped with a + operation satisfying the identities (12) – (15) and (18). In particular, $\mathcal{C}$ is an ordered cartesian category. We say that $\mathcal{C}$ is *residuated* if $\mathcal{C}$ is equipped with a binary operation

$$\begin{aligned}\mathcal{C}(A,C)\times\mathcal{C}(A,B) &\to \mathcal{C}(B,C)\\ (h,g) &\mapsto h \Leftarrow g\end{aligned}$$

such that $f\circ g \leq h$ iff $f \leq (h \Leftarrow g)$ for all $f: B\to C$, $g: A\to B$ and $h: A\to C$. We call $h \Leftarrow g$ the *(left) residual of h by g*. For example, $\mathbf{CL}_m$ and $\mathbf{CL}_c$ are residuated. If $h: A\to C$ and $g: A\to B$, then $h\Leftarrow g$ is the pointwise supremum of all $f: B\to C$ with $f\circ g\leq h$.

The property of being residuated can be expressed by identities.

Proposition 7. *Suppose that $\mathcal{C}$ is a cartesian category equipped with operations + and $\Leftarrow$ satisfying (12) – (15) and (18). Then $\mathcal{C}$ is residuated iff*

$$\begin{aligned}(h\Leftarrow g)\circ g \leq h, &\quad g: u\to v,\ h: u\to w\\ f \leq (f\circ g)\Leftarrow g, &\quad f: v\to w,\ g: u\to v\end{aligned}$$

and

$$h\Leftarrow g \leq (h+h')\Leftarrow g, \quad g: u\to v,\ h,h': u\to w$$

hold.

The main result of this section is:

Theorem 14. [41] *An identity between dagger terms possibly involving + (but not involving $\Leftarrow$) holds in all cartesian categories $\mathbf{CL}_m$ or $\mathbf{CL}_c$ iff it holds in all cartesian categories equipped with a + operation satisfying (12) – (15), (18), which are residuated and satisfy the fixed point identity (4), the parameter identity (1) and*

$$\begin{aligned}(g\Leftarrow\langle g,\mathsf{id}_v\rangle)^\dagger \leq g, &\quad g: v\to u\\ f^\dagger \leq (f+g)^\dagger, &\quad f,g: u\times v\to u.\end{aligned}$$

Actually some of the identities are redundant, see [41].

References

1. Aceto, L., Ésik, Z., Ingólfsdóttir, A.: Equational axioms for probabilistic bisimilarity. In: Kirchner, H., Ringeissen, C. (eds.) AMAST 2002. LNCS, vol. 2422, pp. 239–254. Springer, Heidelberg (2002)
2. Arkhangelsky, K.B., Gorshkov, P.V.: Implicational axioms for the algebra of regular languages. Dokl. Akad. Nauk USSR Ser. A **10**, 67–69 (1967). (in Russian)
3. Arnold, A., Nivat, M.: Metric interpretations of infinite trees and semantics of non deterministic recursive programs. Theor. Comput. Sci. **11**, 181–205 (1980)
4. Arnold, A., Niwinski, D.: Rudiments of μ-Calculus. North-Holland, Amsterdam (2001)
5. Barr, M., Wells, C.: Category theory for computing science. Reprints Theory Appl. Categories (22), 172 (2012)
6. Bartha, M.: A finite axiomatization of flowchart schemes. Acta Cybern. **8**, 203–217 (1987)
7. Bekić, H.: Definable operation in general algebras, and the theory of automata and flowcharts. Technical report, IBM Vienna (1969). Reprinted in: Programming Languages and Their Definition - Hans Bekić (1936–1982). LNCS, vol. 177, pp. 30–55. Springer, Heidelberg (1984)
8. Bernátsky, L., Ésik, Z.: Semantics on flowchart programs and the free Conway theories. ITA **32**, 35–78 (1998)
9. Bloom, S.L., Elgot, C., Wright, J.B.: Solutions of the iteration equation and extensions of the scalar iteration operation. SIAM J. Comput. **9**, 25–45 (1980)
10. Bloom, S.L., Ésik, Z.: Equational logic of circular data type specification. Theor. Comput. Sci. **63**, 303–331 (1989)
11. Bloom, S.L., Ésik, Z.: Floyd-Hoare logic in iteration theories. J. ACM **38**, 887–934 (1991)
12. Bloom, S.L., Ésik, Z.: Iteration Theories. Springer, Heidelberg (1993)
13. Bloom, S.L., Ésik, Z., Taubner, D.: Iteration theories of synchronization trees. Inf. Comput. **102**, 1–55 (1993)
14. Bloom, S.L., Ésik, Z.: Some quasi-varieties of iteration theories. In: Main, M.G., Melton, A.C., Mislove, M.W., Schmidt, D., Brookes, S.D. (eds.) MFPS 1993. LNCS, vol. 802, pp. 378–409. Springer, Heidelberg (1994)
15. Bloom, S.L., Ésik, Z.: The equational logic of fixed points (Tutorial). Theor. Comput. Sci. **179**, 1–60 (1997)
16. Bloom, S.L., Ésik, Z.: An extension theorem with an application to formal tree series. J. Automata Lang. Comb. **8**, 145–185 (2003)
17. Bloom, S.L., Ésik, Z.: Axiomatizing rational power series over natural numbers. Inf. Comput. **207**, 793–811 (2009)
18. Bloom, S.L., Ésik, Z.: Iteration algebras are not finitely axiomatizable. In: Gonnet, G.H., Viola, A. (eds.) LATIN 2000. LNCS, vol. 1776, pp. 367–376. Springer, Heidelberg (2000)
19. Bloom, S.L., Ésik, Z., Labella, A., Manes, E.G.: Iteration 2-theories. Appl. Categorical Struct. **9**, 173–216 (2001)
20. Boffa, M.: Une remarque sur les systémes complets d'identités rationnelles. ITA **24**, 419–428 (1990)
21. Boffa, M.: Une condition impliquant toutes les identités rationnelles. ITA **29**, 515–518 (1995)
22. Cazanescu, V.E., Stefanescu, G.: Towards a new algebraic foundation of flowchart scheme theory. Fund. Inform. **13**, 171–210 (1990)

23. Cohn, P.M.: Universal algebra, 2nd edn. D. Reidel, Dordrecht (1981)
24. Davey, B.A., Priestly, H.A.: Introduction to lattices and order. Cambridge Univ. Press, Cambridge (1990)
25. De Bakker, J.W., Scott, D.: A theory of programs. Technical report, IBM Vienna (1969)
26. Elgot, C.C.: Monadic computation and iterative algebraic theories. In: Logic Colloquium 1973, Bristol. Studies in Logic and the Foundations of Mathematics, vol. 80, pp. 175–230. North-Holland, Amsterdam (1975)
27. Ésik, Z.: Identities in iterative and rational theories. Comput. Linguist. Comput. Lang. **14**, 183–207 (1980)
28. Ésik, Z.: Independence of the equational axioms of iteration theories. JCSS **36**, 66–76 (1988)
29. Ésik, Z.: A note on the axiomatization of iteration theories. Acta Cybern. **9**, 375–384 (1990)
30. Ésik, Z.: Completeness of park induction. Theor. Comput. Sci. **177**, 217–283 (1997)
31. Ésik, Z.: Axiomatizing the equational theory of regular tree languages (Extended abstract). In: Meinel, C., Morvan, M. (eds.) STACS 1998. LNCS, vol. 1373, pp. 455–465. Springer, Heidelberg (1998)
32. Ésik, Z.: Group axioms for iteration. Inf. Comput. **148**, 131–180 (1999)
33. Ésik, Z.: Axiomatizing iteration categories. Acta Cybern. **14**, 65–82 (1999)
34. Ésik, Z.: Axiomatizing the least fixed point operation and binary supremum. In: Clote, P.G., Schwichtenberg, H. (eds.) CSL 2000. LNCS, vol. 1862, pp. 302–316. Springer, Heidelberg (2000)
35. Ésik, Z.: A proof of the Krohn-Rhodes decomposition theorem. Theor. Comput. Sci. **234**, 287–300 (2000)
36. Ésik, Z.: The power of the group axioms for iteration. Int. J. Algebr. Comput. **10**, 349–373 (2000)
37. Ésik, Z.: Axiomatizing the equational theory of regular tree languages. J. Log. Algebr. Program. **79**, 189–213 (2010)
38. Ésik, Z.: Multi-linear iterative K-semialgebras. Electr. Notes Theor. Comput. Sci. **276**, 159–170 (2011)
39. Ésik, Z.: A connection between concurrency and language theory. Electr. Notes Theor. Comput. Sci. **298**, 143–164 (2013)
40. Ésik, Z.: Axiomatizing weighted synchronization trees and weighted bisimilarity. Theor. Comput. Sci. **534**, 2–23 (2014)
41. Ésik, Z.: Residuated park theories. J. Log. Comput. **25**, 453–471 (2015)
42. Ésik, Z.: Equational axioms associated with finite automata for fixed point operations in cartesian categories. Math. Struct. Comput. Sci. (to appear)
43. Ésik, Z.: Equational properties of stratified least fixed points (extended abstract). In: de Paiva, V., de Queiroz, R., Moss, L.S., Leivant, D., de Oliveira, A. (eds.) WoLLIC 2015. LNCS, vol. 9160, pp. 174–188. Springer, Heidelberg (2015)
44. Ésik, Z., Bernátsky, L.: Scott induction and equational proofs. Electr. Notes Theor. Comput. Sci. **1**, 154–181 (1985)
45. Ésik, Z., Kuich, W.: Inductive star-semirings. Theor. Comput. Sci. **324**, 3–33 (2004)
46. Ésik, Z., Kuich, W.: Free iterative and iteration K-semialgebras. Algebra Univers. **67**, 141–162 (2012)
47. Ésik, Z., Kuich, W.: Free inductive K-semialgebras. J. Log. Algebr. Program. **82**, 111–122 (2013)
48. Ésik, Z., Kuich, W.: Solving fixed-point equations over complete semirings (to appear)

49. Ésik, Z., Labella, A.: Equational properties of iteration in algebraically complete categories. Theor. Comput. Sci. **195**, 61–89 (1998)
50. Ésik, Z., Rondogiannis, P.: A fixed point theorem for non-monotonic functions. Theor. Comput. Sci. **574**, 18–38 (2015)
51. Gécseg, F.: Products of Automata. Springer, Berlin (1986)
52. Ginzburg, A.: Algebraic Theory of Automata. Academic Press, New-York (1968)
53. Goguen, J.A., Thatcher, J.W., Wagner, E.G., Wright, J.B.: Initial algebra semantics and continuous algebras. J. ACM **24**, 68–95 (1977)
54. Hasegawa, M.: Recursion from cyclic sharing: traced monoidal categories and models of cyclic lambda calculi. In: de Groote, P., Hindley, J.R. (eds.) TLCA 1997. LNCS, vol. 1210, pp. 196–213. Springer, Heidelberg (1997)
55. Hyland, M., Power, J.: The category theoretic understanding of universal algebra: Lawvere theories and monads. Electr. Notes Theor. Comput. Sci. **172**, 437–458 (2007)
56. Joyal, A., Street, R., Verity, D.: Traced monoidal categories. Math. Proc. Camb. Philos. Soc. **3**, 447–468 (1996)
57. Kozen, D.: A completeness theorem for Kleene algebras and the algebra of regular events. In: LICS 1991, pp. 214–225. IEEP Press (1991)
58. Kozen, D.: A completeness theorem for Kleene algebras and the algebra of regular events. Inf. Comput. **110**, 366–390 (1994)
59. Krob, D.: A complete system of B-rational identities. In: Paterson, M. (ed.) ICALP 1990. LNCS, vol. 443, pp. 60–73. Springer, Heidelberg (1990)
60. Krob, D.: Complete systems of B-rational identities. Theor. Comput. Sci. **89**, 207–343 (1991)
61. Krohn, K., Rhodes, J.L.: Algebraic theory of machines, I, principles of finite semigroups and machines. Trans. Am. Math. Soc. **116**, 450–464 (1965)
62. Lawvere, F.W.: Functorial semantics of algebraic theories. Proc. Nat. Acad. Sci. (USA) **50**, 869–872 (1963)
63. Lehmann, D., Smyth, M.B.: Algebraic specification of data types: a synthetic approach. Math. Sys. Theory **14**, 97–139 (1981)
64. Milner, R.: Communication and Concurrency. Prentice-Hall, New York (1989)
65. Niwinski, D.: Equational μ-calculus. In: Skowron, A. (ed.) Computation Theory. LNCS, vol. 208, pp. 169–176. Springer, Heidelberg (1985)
66. Niwinski, D.: On fixed-point clones (extended abstract). In: Kott, L. (ed.) ICALP 1986. LNCS, vol. 226, pp. 464–473. Springer, Heidelberg (1986)
67. Park, D.M.R.: Concurrency and automata on infinite sequences. In: Deussen, P. (ed.) Theoretical Computer Science. LNCS, vol. 104, pp. 167–183. Springer, Heidelberg (1981)
68. Plotkin, G.: Domains. The Pisa notes. The University of Edinburgh, Edinburgh (1983)
69. Pratt, V.: Action logic and pure induction. In: van Eijck, J. (ed.) Logics in AI 1990. LNCS, vol. 478, pp. 97–120. Springer, Heidelberg (1990)
70. Santocanale, L.: On the equational definition of the least prefixed point. Theor. Comput. Sci. **295**, 341–370 (2003)
71. Simpson, A.K., Plotkin, G.D.: Complete axioms for categorical fixed-point operators. In: LICS 2000, pp. 30–41. IEEE Press (2000)
72. Wagner, E.G., Bloom, S.L., Thatcher, J.W.: Why algebraic theories. In: Algebraic Methods in Semantics, pp. 607–634. Cambridge University Press, New York (1986)
73. Wright, J.B., Thatcher, J.W., Wagner, E.G., Goguen, J.A.: Rational algebraic theories and fixed-point solutions. In: FOCS 1976, pp. 147–158. IEEE Press (1976)

http://www.springer.com/978-3-662-48056-4

Mathematical Foundations of Computer Science 2015
40th International Symposium, MFCS 2015, Milan, Italy,
August 24-28, 2015, Proceedings, Part I
Italiano, G.F.; Pighizzini, G.; Sannella, D.T. (Eds.)
2015, XXVI, 459 p. 51 illus., Softcover
ISBN: 978-3-662-48056-4