Information and Computation **148**, 131–180 (1999)
Article ID inco.1998.2746, available online at http://www.idealibrary.com on IDEAL®

Group Axioms for Iteration

Department of Computer Science, A. József University, 6720 Szeged, Aradi v. tere 1, Hungary
E-mail: esik@inf.u-szeged.hu

Iteration theories provide a sound and complete axiomatization of the equational properties of the iteration (or fixed point) operation in many models of theoretical computer science including ordered and metric structures, trees and synchronization trees. All known equational axiomatizations of iteration theories consist of a small set of equational axioms for Conway theories and a complicated equation scheme, the commutative identity. Here we associate an identity with each finite semigroup. We prove that the set consisting of the Conway identities and the group identities associated with the finite (simple) groups is complete. Moreover, we prove that the Conway identities and a subcollection of the semigroup identities associated with a subclass of the finite semigroups is complete iff each finite (simple) group divides one of the semigroups in the subclass. We also formulate a conjecture and study its consequences. The results are a generalization of Krob's axiomatization of the equational theory of the regular sets.

1. INTRODUCTION

Iteration theories were introduced in [2, 3] and independently in [12]. The axioms of iteration theories capture the equational properties of the iteration operation in several models related to computer science, including the following:

- Continuous functions on cpo's, or continuous ordered theories [40], where iteration is defined by least fixed points.
- Contraction theories over complete metric spaces, or Elgot's iterative theories [10], where iteration is defined by unique fixed points.
- Matrix theories over complete or countably complete semirings, where iteration is defined in terms of infinite geometric sums [4].
- Tree theories [4], synchronization trees [30, 4].

* Partially supported by Grant T22423 of the National Foundation of Hungary for Scientific Research, the US–Hungarian Joint Fund under Grant 351, the Austrian–Hungarian Action Foundation, the Japan Society for the Promotion of Science, and by the Fulbright Foundation.

0890-5401/99 $30.00

• Functor theories on ω-categories or algebraically complete categories, where iteration is defined via initial algebras [4, 18].

For a detailed study of iteration theories we refer to [4].

All known equational axiomatizations of iteration theories consist of a small set of equational axioms for Conway theories and a complicated equation scheme, the commutative identity. Here we associate an identity with each finite automaton and each finite semigroup, see also [14]. We prove that the set consisting of the Conway identities and the group identities associated with the finite (simple) groups is complete. Moreover, we prove that the Conway identities and a subcollection of the semigroup identities associated with a subclass S_i, $i \in I$ of the finite semigroups is complete iff each finite (simple) group divides one of the semigroups S_i. Then we formulate a conjecture and prove that it implies that the Conway identities and an equation $\mathbf{S}_n$ associated with each integer $n \geqslant 3$ are complete. The equation $\mathbf{S}_n$ is a simplified form of the identity associated with the n-state automaton whose input letters induce a cyclic permutation and a transposition of the state set.

Suppose that G is a finite group on the set $[n]$ of the first n integers. Suppose further that we work with continuous functions on a cpo A. Take any continuous function $f: A^{n+p} \to A$, and consider the least solution of the system of fixed point equations in the variables $x_1, ..., x_n$ and parameters $y_1, ..., y_p$

$$\begin{aligned} x_1 &= f(x_{11}, ..., x_{1n}, y_1, ..., y_p) \\ &\vdots \\ x_n &= f(x_{n1}, ..., x_{nn}, y_1, ..., y_p), \end{aligned} \tag{1}$$

where ij denotes the product of $i \in [n]$ and $j \in [n]$ in the group G. Second, consider the single fixed point equation

$$x = f(x, ..., x, y_1, ..., y_p) = h(x, y_1, ..., y_p)$$

obtained by identifying the first n variables. Then h is a continuous function $A^{1+p} \to A$, so for each value in A of the parameters $y_1, ..., y_p$, the fixed point equation (2) has a least solution $h^\dagger(y_1, ..., y_p)$. (It is known that $h^\dagger$, as a function of the parameters is also continuous.) The group identity associated with G asserts that the components of the least solution of (1) are all equal to $h^\dagger(y_1, ..., y_p)$. Under the Conway identities, this assertion is equivalent to the fact that $h^\dagger(y_1, ..., y_p)$ is the first component of the least solution of (1). Moreover, identities associated with isomorphic groups are equivalent.

The main difficulty in our completeness proof is to establish the commutative identity in Conway theories satisfying the group identities. We briefly outline our argument. As mentioned above, we associate an identity $\mathbf{C}(A, X)$ with each finite automaton (A, X) and an identity $\mathbf{C}(S)$ with each finite semigroup S. Then we prove that if a Conway theory T satisfies an identity $\mathbf{C}(G)$ associated with a finite group G, then the "vector form" of $\mathbf{C}(G)$ also holds in T. Since the Conway identities also imply their own vector forms, we conclude that whenever an identity is

a logical consequence of the Conway identities and some set of the group identities, then the vector form of this identity also holds in all Conway theories satisfying the given set of group identities. Then we prove that in Conway theories, if the identity $\mathbf{C}(A, X)$ associated with a finite automaton (A, X) holds, then so does the identity $\mathbf{C}(B, X)$, where (B, X) is a subautomaton of (A, X). We also establish a related fact for the "renaming" of the input symbols. Then we prove that in Conway theories satisfying a certain collection of the group identities, if the identity $\mathbf{C}(A, X)$ associated with a finite automaton (A, X) holds, then so does the identity $\mathbf{C}(B, X)$, where (B, X) is a homomorphic image of (A, X) under a "permutation-reset" homomorphism. As a further result of this sort, we prove that if the automaton (C, X) is obtained from the automata (A, X) and (B, Y) by cascade composition, and if $\mathbf{C}(A, X)$ and the vector form of $\mathbf{C}(B, Y)$ hold in a Conway theory T, then the identity $\mathbf{C}(C, X)$ also holds in T. Moreover, we establish the identity associated with the 2-state identity-reset automaton in any Conway theory. In conclusion, by a variant of the Krohn–Rhodes Decomposition Theorem for finite automata proved in [15], we obtain that if a Conway theory T satisfies the group identities, then each identity associated with any finite automaton holds in T, as well as its vector form. This completes the proof of the completeness of the Conway identities and the group identities, since it has been shown in [14] that in Conway theories the vector forms of the identities associated with finite automata are equivalent to the commutative identity. A more elaborate argument proves that any identity associated with a finite automaton (A, X) is a logical consequence of the Conway identities and those group identities associated with the (simple) group divisors of the semigroup of (A, X). We do not repeat the proof [12] that the Conway identities and the commutative identity are complete. This argument is based on an equational formalization of the minimization of flowchart schemes.

Our concept of a group identity, or the identity associated with a finite automaton or semigroup originates in [7], see also [26]. In fact, in matrix theories over Conway semirings [4, 22], each identity involving the iteration operation has an equivalent form involving the Kleene star operation. See [4]. In such theories, the semigroup identities take the form of Conway's semigroup identities [7]. It was conjectured in [7] and proved by Krob in [26] that a small set of equational axioms including the Conway identities and the group identities form a complete axiomatization of the equational theory of the regular sets. The results of the present paper may be seen as a generalization of Krob's result. In fact, the use of the Krohn–Rhodes Decomposition Theorem was facilitated by Krob's paper. He gave a translation of a standard proof of the Krohn–Rhodes Decomposition Theorem [28] into the equational theory of the regular sets, by reproducing, step by step, the whole proof in equational logic. In contrast, our completeness argument uses the improved Krohn–Rhodes decomposition [15] as a subroutine. No part of its proof is reproduced. Moreover, several arguments in [26] make use of the fact that the additive structure is idempotent. This condition is not available in our setting.

Apart from the fact that the results of this paper imply Krob's, the completeness of the Conway identities and the group axioms for iteration theories has many applications. First, it follows that the Conway identities and a simple version of Park's fixed point induction principle are complete for the equational theory of

iteration theories. (In fact, one does not need the full strength of the Conway identities for this fact.) This result, originally proved in [14], may be seen as a generalization of Kozen's axiomatization [25] of the equational theory of the regular sets (or of the variety generated by the Kleene algebras of binary relations). A second application concerning finite state process behaviors will also be treated here, others elsewhere.

The equational theory of iteration may be studied in several frameworks including clones, theories, sorted theories, cartesian categories, or the simple algebraic language of μ-terms and the closely related "where-expressions" of [32]. Although we state and prove our results in terms of theories, they can be translated to each of the other frameworks with no problem at all. See [6, 24]. Here we only give a translation into the language of μ-terms.

The rest of the paper is organized as follows. In Sections 2, 3, and 4, we recall the concepts of theories, Conway theories, and iteration theories. Then, in Section 5 we define the vector forms of identities. Section 6 is devoted to some basic concepts on automata and semigroups. Section 7 contains the definition of the identity $\mathbf{C}(A, X)$ associated with an automaton (A, X) together with the definition of the identity $\mathbf{C}(S)$ associated with a semigroup S. The main results are formulated in Section 8. In Section 9, we recall the Krohn–Rhodes Decomposition Theorem and the variant proved in [15]. Then, in Section 10, we prove that under the Conway identities, each group identity implies its own vector form. Sections 11 and 12 contain the main lemmas concerning the constructions of subautomata, renaming, and cascade composition. In Sections 13 and 14, we study the identities associated with permutation automata and permutation-reset automata. Permutation-reset homomorphisms are dealt with in Section 15. The proof of the completeness of the Conway identities and the group identities is finally completed in Section 16. Section 17 is devoted to a conjecture and its consequences. μ-terms are considered in Section 18. The completeness of the Park induction principle is proved in Section 19. The other applications are treated in Section 20. Here, we also show how our results imply Krob's. Some further results are mentioned in Section 21.

2. THEORIES

For an integer $n \geqslant 0$, we let $[n]$ denote the set $\{1, ..., n\}$. Thus $[0]$ is the empty set.

Theories were defined by Lawvere [27] in order to provide a categorical framework for equational logic. There is a short definition of theories.

DEFINITION 2.1. A *theory* is a small category T whose set of objects is the natural numbers $n \geqslant 0$, and in which each object n is the n-fold coproduct of object 1 with itself.

In any theory T, we write composition in diagrammatic order. Thus, if $f: n \to p$ and $g: p \to q$ in T, $f \cdot g$ is a morphism $n \to q$. The identity morphism $n \to n$ is denoted $\mathbf{1}_n$. The fact that each object n is the n-fold coproduct of object 1 with itself can be expressed in more detail by the following condition: There exist *distinguished*

morphisms $i_n: 1 \to n$, $i \in [n]$, such that for any sequence of morphisms $f_i: 1 \to p$, $i \in [n]$, $p \geqslant 0$, there is a unique morphism $f: n \to p$ with

$$i_n \cdot f = f_i, \qquad i \in [n]. \tag{3}$$

In particular, there is a unique morphism $0 \to p$ which we will denote by 0_p.

We will assume that each theory T comes with given distinguished morphisms i_n. Moreover, we require that the morphism 1_1 is the identity morphism $\mathbf{1}_1$. (See below for the justification of this assumption.)

Remark 2.2. Sometimes theories are defined dually, replacing coproducts with products. Another alternative is to reverse the natural direction of the arrows. For example, if A is a set, the theory $\mathbf{Pow}_A$ has morphisms $n \to p$ all functions $A^p \to A^n$. Composition is function composition in the reverse order, and for each $i \in [n]$, $n > 0$, the distinguished morphism i_n is the ith projection $A^n \to A$.

DEFINITION 2.3. Suppose that T and T' are theories. A *theory morphism* $T \to T'$ is a functor $\varphi: T \to T'$, which preserves the objects and the distinguished morphisms, so that

$$i_n \varphi = i_n,$$

for all $i \in [n]$, $n \geqslant 0$.

Since a theory morphism $\varphi: T \to T'$ is the identity map on objects, we may identify it with a family of maps $T(n, p) \to T'(n, p)$. Here, $T(n, p)$ denotes the hom-set of T-morphisms $n \to p$. An isomorphism $\varphi: T \to T'$ is a theory morphism which is bijective on the hom-sets.

A morphism with source 1 will be called *scalar*. Suppose that f_i is a scalar morphism $1 \to p$, for each $i \in [n]$. The morphism $f: n \to p$ determined by the coproduct property (3) will be denoted $\langle f_1, ..., f_n \rangle$. This operation of *tupling* creates a bijection between the sets $T(1, p)^n$ and $T(n, p)$. It follows that $\mathbf{1}_n = \langle 1_n, ..., n_n \rangle$, for all $n \geqslant 0$. Moreover, since $1_1 = \mathbf{1}_1$, we have $\langle f \rangle = f$, for all scalar morphisms $f: 1 \to p$.

Suppose that T is a theory. A *subtheory* T' of T is a subcategory which contains the distinguished morphisms and is closed under tupling. Equivalently, a theory T' is a subtheory of T if $T'(n, p)$ is a subset of $T(n, p)$, for each $n, p \geqslant 0$, and the inclusion $T'(n, p) \to T(n, p)$ is a theory morphism.

DEFINITION 2.4. Suppose that T is a theory. A *base morphism* $n \to p$ in T is a morphism $\langle f_1, ..., f_n \rangle$, such that each morphism f_i is a distinguished morphism $1 \to p$.

In a theory T, the base morphisms form the smallest subtheory of T. Base morphisms will be denoted by Greek letters. In nontrivial theories, each base morphism $\rho: n \to p$ is uniquely determined by a function $\hat{\rho}: [n] \to [p]$

$$i_n \cdot \rho = j_p \qquad \text{iff} \quad i\hat{\rho} = j,$$

for all $i \in [n]$ and $j \in [p]$. (A theory T is nontrivial if $1_2 \neq 2_2$ iff $T(1, 2)$ is not a singleton set iff some home-set $T(n, p)$ has at least 2 elements.) We will usually identify a base morphism with the corresponding function and call a base morphism injective, surjective, or bijective according to whether the corresponding function has the appropriate property. A bijective base morphism is sometimes called a base permutation. Note that the composite of two base morphisms is determined by the composite of the corresponding functions. For example, the base morphism

$$\tau_n := \langle 1_1, ..., 1_1 \rangle : n \to 1 \tag{4}$$

is surjective, for each $n \geqslant 1$.

2.1. Pairing and Separated Sum

Suppose that T is a theory. Given integers $n, m \geqslant 0$, let $\kappa : n \to n+m$ and $\lambda : m \to n+m$ denote the base morphisms corresponding to the inclusion $[n] \to [n+m]$ and the translated inclusion $[m] \to [n+m]$. Then the diagram determined by the morphisms κ and λ is a coproduct diagram. Thus, for each $f : n \to p$ and $g : m \to p$, there exists a unique morphism $\langle f, g \rangle : n+m \to p$ such that

$$\kappa \cdot \langle f, g \rangle = f$$
$$\lambda \cdot \langle f, g \rangle = g.$$

The morphism $\langle f, g \rangle$ is called the *pairing* of f and g. The pairing operation is associative and the zero morphisms 0_p act as identities

$$\langle f, \langle g, h \rangle \rangle = \langle \langle f, g \rangle, h \rangle$$
$$\langle f, 0_p \rangle = f = \langle 0_p, f \rangle,$$

for all $f : n \to p$, $g : m \to p$ and $h : k \to p$. Moreover,

$$\langle f, g \rangle \cdot h = \langle f \cdot h, g \cdot h \rangle,$$

for all $f : n \to p$, $g : m \to p$ and $h : p \to q$. Using these identities, it is possible to define the tupling

$$\langle f_1, ..., f_n \rangle : k \to p$$

of any family of morphisms $f_i : k_i \to p$, $i \in [n]$, $n \geqslant 0$. Here k is the sum $k_1 + \cdots + k_n$.

Another derived operation in theories is the operation of *separated sum*. Suppose that $f : n \to p$ and $g : m \to q$ in the theory T. Let κ and λ be the base morphisms defined above, and let $\kappa' : p \to p+q$ and $\lambda' : q \to p+q$ be defined similarly. Then we define

$$f \oplus g = \langle f \cdot \kappa', g \cdot \lambda' \rangle : n+m \to p+q.$$

Note that $f \oplus g$ is the unique morphism $n+m \to p+q$ such that

$$\kappa \cdot (f \oplus g) = f \cdot \kappa'$$
$$\lambda \cdot (f \oplus g) = g \cdot \lambda'.$$

Separated sum satisfies the identities

$$f \oplus (g \oplus h) = (f \oplus g) \oplus h$$
$$f \oplus 0_0 = f = 0_0 \oplus f$$
$$(f \oplus g) \cdot \langle h, k \rangle = \langle f \cdot h, g \cdot k \rangle$$
$$(f \oplus g) \cdot (h \oplus k) = f \cdot h \oplus g \cdot k,$$

whenever the morphisms f, g, h, and k have appropriate source and target.

2.2. *Theories as Algebras*

An algebraic theory may be viewed as an $\mathcal{N} \times \mathcal{N}$-sorted universal algebra, equipped with the operations of composition and tupling, and constants i_n. (Here, $\mathcal{N}$ denotes the set of nonnegative integers.) As such, theories form a variety defined by equations expressing the fact that composition is associative and the morphisms $\mathbf{1}_n = \langle 1_n, ..., n_n \rangle$ are identities. Moreover, $1_1 = \mathbf{1}_1$ and

$$i_n \cdot \langle f_1, ..., f_n \rangle = f_i$$
$$\langle 1_n \cdot f, ..., n_n \cdot f \rangle = f,$$

for all $f_i \colon 1 \to p$, $i \in [n]$, and for all $f \colon n \to p$. A theory morphism $T \to T'$ is a homomorphism of the corresponding many-sorted algebras.

3. CONWAY THEORIES

We start with a technical definition.

A *preiteration theory* is an algebraic theory T enriched with an iteration or dagger operation

$$^\dagger \colon T(n, n+p) \to T(n, p)$$
$$f \mapsto f^\dagger$$

defined for each n, $p \geqslant 0$. No particular properties of iteration are required. However, $0_p^\dagger = 0_p$, for each $p \geqslant 0$, since 0_p is the unique morphism $0 \to p$. A morphism $\varphi \colon T \to T'$ of preiteration theories is a theory morphism which preserves the dagger operation.

DEFINITION 3.1. A *Conway theory* is a preiteration theory T in which iteration satisfies the following identities.

1. Scalar parameter identity

$$(f \cdot (\mathbf{1}_1 \oplus g))^\dagger = f^\dagger \cdot g,$$

all $f: 1 \to 1 + p$, $g: p \to q$.

2. Scalar composition identity

$$(f \cdot \langle g, 0_1 \oplus \mathbf{1}_p \rangle)^\dagger = f \cdot \langle (g \cdot \langle f, 0_1 \oplus \mathbf{1}_p \rangle)^\dagger, \mathbf{1}_p \rangle,$$

all $f, g: 1 \to 1 + p$.

3. Scalar double dagger identity

$$f^{\dagger\dagger} = (f \cdot (\tau_2 \oplus \mathbf{1}_p))^\dagger,$$

all $f: 1 \to 2 + p$. (Recall that $\tau_2 = \langle 1_1, 1_1 \rangle$ is the unique base morphism $2 \to 1$.)

4. Scalar pairing identity

$$\langle f, g \rangle^\dagger = \langle f^\dagger \cdot \langle h^\dagger, \mathbf{1}_p \rangle, h^\dagger \rangle,$$

all $f: n \to n + 1 + p$, $g: 1 \to n + 1 + p$, where

$$h = g \cdot \langle f^\dagger, \mathbf{1}_{1+p} \rangle : 1 \to 1 + p.$$

Suppose that T and T' are Conway theories. A morphism $T \to T'$ is a preiteration theory morphism.

Remark 3.2. The term Conway theory is due to the fact the above identities take in matrix theories over semirings, cf. [7, 4]. In such theories Mat_S equipped with an iteration operation, if the parameter identity holds, the dagger operation determines, and is determined by a star operation on the n by n matrices, or by a star operation on the semiring S. The scalar double dagger identity corresponds to the equation $(a + b)^* = (a^* b)^* a^*$, and the scalar composition identity to the equation $(ab)^* = 1 + a(ba)^* b$, all $a, b \in S$. Semirings satisfying these two equations are called Conway semirings, cf. [4, 22].

By the scalar pairing identity, the dagger operation in Conway theories is uniquely determined by its restriction to the scalar morphisms $1 \to 1 + p$. Thus the essential axioms are the first three, i.e., the scalar parameter, scalar composition, and scalar double dagger identities.

The following identities hold in Conway theories.

1. Fixed point identity

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

all $f: n \to n + p$. When $n = 1$, this identity is called the *scalar fixed point identity*.

2. Left zero identity

$$(0_n \oplus f)^\dagger = f,$$

all $f: n \to p$. When $n = 1$, this identity is called the *scalar left zero identity*.

3. Right zero identity

$$(f \oplus 0_q)^\dagger = f^\dagger \oplus 0_q,$$

all $f: n \to n + p$. When $n = 1$, this identity is called the *scalar right zero identity*.

4. Parameter identity

$$(f \cdot (\mathbf{1}_n \oplus g))^\dagger = f^\dagger \cdot g,$$

all $f: n \to n + p$, $g: p \to q$.

5. Composition identity

$$(f \cdot \langle g, 0_n \oplus \mathbf{1}_p \rangle)^\dagger = f \cdot \langle (g \cdot \langle f, 0_m \oplus \mathbf{1}_p \rangle)^\dagger, \mathbf{1}_p \rangle,$$

all $f: n \to m + p$, $g: m \to n + p$.

6. Double dagger identity

$$f^{\dagger\dagger} = (f \cdot (\langle \mathbf{1}_n, \mathbf{1}_n \rangle \oplus \mathbf{1}_p))^\dagger,$$

all $f: n \to n + n + p$.

7. (Left) pairing identity

$$\langle f, g \rangle^\dagger = \langle f^\dagger \cdot \langle h^\dagger, \mathbf{1}_p \rangle, h^\dagger \rangle,$$

all $f: n \to n + m + p$, $g: m \to n + m + p$, where

$$h = g \cdot \langle f^\dagger, \mathbf{1}_{m+p} \rangle : m \to m + p.$$

8. Right pairing identity

$$\langle f, g \rangle^\dagger = \langle h^\dagger, (g \cdot \rho)^\dagger \cdot \langle h^\dagger, \mathbf{1}_p \rangle \rangle,$$

all $f: n \to n + m + p$, $g: m \to n + m + p$, where

$$\rho = \langle 0_m \oplus \mathbf{1}_n, \mathbf{1}_m \oplus 0_n \rangle \oplus \mathbf{1}_p : n + m + p \to m + n + p$$
$$h = f \cdot \langle \mathbf{1}_n \oplus 0_p, (g \cdot \rho)^\dagger, 0_n \oplus \mathbf{1}_p \rangle : n \to n + p.$$

9.

$$\langle f \cdot (\mathbf{1}_n \oplus 0_m \oplus \mathbf{1}_p), 0_n \oplus g \rangle^\dagger = \langle f^\dagger, g^\dagger \rangle, \tag{5}$$

all $f: n \to n + p$, $g: m \to m + p$.

10. Permutation identity

$$(\pi \cdot f \cdot (\pi^{-1} \oplus \mathbf{1}_p))^\dagger = \pi \cdot f^\dagger,$$

for all $f: n \to n+p$ and for all base permutations $\pi: n \to n$. Here π^{-1} denotes the inverse of π.

Remark 3.3. The pairing identity is sometimes called Bekič's identity, see [35, 39].

The following theorem provides two equivalent axiomatizations of Conway theories. For proofs and original references, see [4].

THEOREM 3.4. *A preiteration theory T is a Conway theory iff T satisfies either the zero identities, the pairing identity and the permutation identity, or the parameter, composition, and double dagger identities.*

Below we will use the term *Conway identities* to refer either to the set of equations that hold in all Conway theories, or to a concrete equational axiomatization of Conway theories.

EXAMPLE 3.5. Suppose that A is a cpo (with least element). Let T denote the subtheory of the theory $\mathbf{Pow}_A$ determined by the continuous functions $A^p \to A^n$, $n, p \geqslant 0$. If $f: n \to n+p$ in T, i.e., f is a continuous function $A^{n+p} \to A^n$, then for each value $y \in A^p$ there is a least element $x \in A^n$ such that

$$x = f(x, y). \tag{6}$$

Denoting this least fixed point x by $f^\dagger(y)$, the resulting function $f^\dagger: A^p \to A^n$ is continuous, hence a morphism $n \to p$ in T. In fact, equipped with this operation, T is an iteration theory. Moreover, an equation involving dagger holds in all iteration theories iff it holds in all theories of continuous functions on cpo's. See [12].

We briefly explain the meaning of some Conway identities in the theory T. The meaning of the fixed point identity should be clear,

$$f(f^\dagger(y), y) = f^\dagger(y)$$

for all $f: A^{n+p} \to A^n$ in T and $y \in A^p$. The fact that the parameter identity holds in T means that for any $f: A^{n+p} \to A^n$ and $g: A^q \to A^p$ in T, and for any $z \in A^q$, the least solution of the equation

$$x = f(x, g(z))$$

can be obtained by applying $f^\dagger$ to $g(z)$, where $f^\dagger$ is the least solution of the fixed point equation (6). The pairing identity can be explained as follows. Suppose that $f: A^{n+m+p} \to A^n$ and $g: A^{n+m+p} \to A^m$ are in T. Consider the system of equations in the variables $x \in A^n$ and $y \in A^m$

$$x = f(x, y, z) \tag{7}$$

$$y = g(x, y, z), \tag{8}$$

where the parameter z is in A^p. The least solution of this system can be computed by successive elimination of the variables as follows. The least solution of the first equation (7) is $f^\dagger(y, z)$, a function of y and z. Substituting this for x in (8), we obtain the equation

$$y = g(f^\dagger(y, z), y, z). \tag{9}$$

Introducing the notation $h(y, z)$ for the function on the right-hand side, the least solution of (9) is $h^\dagger(z)$. The pairing identity asserts that $h^\dagger(z)$ is also the second component of the least solution of the original system of equations (7, 8), and that the first component is $f^\dagger(h^\dagger(z), z)$. Note that the pairing identity is not symmetric. For symmetric versions, see [4]. The permutation identity asserts that permuting the rows of a system of equations has the expected effect, the least fixed point solutions are permuted in the same way.

4. ITERATION THEORIES

Conway theories have many interesting properties, e.g., there is a general form of Kleene's theorem which holds in all Conway theories, and the Conway identities imply the soundness of the Floyd–Hoare logic and Cook's completeness theorem, cf. [4]. Nevertheless the Conway axioms are too weak to capture all of the equational properties of iteration in computer science. A complete axiomatization of the equational properties of iteration may be obtained by adding the commutative identity to the Conway axioms.

Suppose that $f = \langle f_1, ..., f_k \rangle : k \to n + p$, $f_i : 1 \to n + p$, $i \in [k]$ in an algebraic theory T. Suppose further that $g_i : n \to m$, for each $i \in [k]$. We define

$$f \| (g_1, ..., g_k) = \langle f_1 \cdot (g_1 \oplus \mathbf{1}_p), ..., f_k \cdot (g_k \oplus \mathbf{1}_p) \rangle : k \to m + p.$$

DEFINITION 4.1. The *commutative identity* is the equation

$$((\tau \cdot f) \| (\rho_1, ..., \rho_m))^\dagger = \tau \cdot (f \cdot (\tau \oplus \mathbf{1}_p))^\dagger,$$

where $f : n \to m + p$, and where $\tau : m \to n$ is a surjective base morphism and the morphisms $\rho_i : m \to m$ are base with $\rho_i \cdot \tau = \tau$, $i \in [m]$. When $n = 1$, this equation is called the *scalar commutative identity*.

DEFINITION 4.2. An *iteration theory* is a Conway theory satisfying the commutative identity. A morphism of iteration theories is a preiteration theory morphism.

EXAMPLE 4.3. We explain the meaning of the scalar commutative identity in the theory T of Example 3.5. Suppose that $f : A^{m+p} \to A$ in T, and consider the system of equations

$$x_1 = f(x_{1\rho_1}, ..., x_{m\rho_1}, y)$$
$$\vdots$$
$$x_m = f(x_{1\rho_m}, ..., x_{m\rho_m}, y),$$

where $y \in A^p$ and each ρ_i is a function $[m] \to [m]$. (Since $n = 1$, τ is the unique function $[m] \to [1]$, so that there is no extra condition on the functions ρ_i.) By the scalar commutative identity, the components of the least solution of this system are all equal to the least solution of the single equation

$$x = f(x, ..., x, y)$$

obtained by identifying the first m variables.

In preiteration theories, the commutative identity is implied by a weak form of the functorial implication.

DEFINITION 4.4. Suppose that T is a preiteration theory and that $\mathscr{C}$ is a class of morphisms in T. We say that T satisfies the *functional implication* for $\mathscr{C}$ if whenever the square

$$\begin{array}{ccc} n & \xrightarrow{f} & n+p \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h \oplus \mathbf{1}_p} \\ m & \xrightarrow[g]{} & m+p \end{array}$$

commutes, where h is a morphism in $\mathscr{C}$, then so does the triangle

$$\begin{array}{ccc} n & \xrightarrow{f^\dagger} & p \\ {\scriptstyle h}\downarrow & \nearrow_{g^\dagger} & \\ m & & \end{array}$$

A particular subcase is important here, the case that $\mathscr{C}$ is the class of all surjective base morphisms. In this case, we call the functorial implication the *weak functorial implication.*

Remark 4.5. The functorial implication was used by Eilenberg [9] and Plotkin [35] in their characterization of the fixed point operation on continuous functions over cpo's. In [29], a version of the functorial implication is part of the axioms imposed on iteration.

The following facts are proved in [4], where original references may be found.

LEMMA 4.6. *If a preiteration theory T satisfies the weak functorial implication, then the commutative identity holds in T.*

LEMMA 4.7. *Suppose that T is a Conway theory. Then T satisfies the functorial implication for all injective base morphisms. Moreover, if T satisfies the weak functorial*

implication, then T is an iteration theory and satisfies the functorial implication for all base morphisms.

LEMMA 4.8. *Suppose that T is a Conway theory. If T satisfies the functorial implication for the base surjections $\tau_n: n \to 1$, $n \geqslant 1$, then T satisfies the weak functorial implication.*

Conway theories and iteration theories are defined by equations. Thus both Conway theories and iteration theories form a variety of preiteration theories. The Conway theories satisfying the weak functorial implication form a quasi-variety properly included in the class of iteration theories, cf. [5, 13]. Nevertheless the Conway theories satisfying the weak functorial implication generate the variety of iteration theories.

The structure of the free iteration theories was described in [12], see also [2, 3, 11]. The description is based on regular trees that represent the behavior of finite flowchart schemes. For an explicit description of the free Conway theories, see [1].

5. VECTOR FORMS OF IDENTITIES

Suppose that T is a theory and k is a positive integer. Since each object nk, $n \geqslant 0$ is the n-fold coproduct of object k with itself, the full subcategory spanned by these objects is a theory that we denote by Tk. Formally, Tk has morphisms $n \to p$ the T-morphisms $nk \to pk$, i.e., $Tk(n, p) = T(nk, pk)$. Suppose that $f: n \to p$ and $g: p \to q$ in Tk. Their composite in Tk is the T-morphism $f \cdot g: nk \to qk$, so that composition in Tk is the composition inherited from T. For each $i \in [n]$, $n \geqslant 0$, the ith distinguished morphism $1 \to n$ in Tk is the T-morphism

$$0_{(i-1)k} \oplus \mathbf{1}_k \oplus 0_{(n-i)k},$$

which we will denote by $i_n^{(k)}$. The distinguished morphisms determine the tupling operation. It follows that the tupling of the Tk-morphisms $f_1, ..., f_n: 1 \to p$ is their tupling $\langle f_1, ..., f_n \rangle$ in T.

Note that the identity morphism $\mathbf{1}_n^{(k)}: n \to n$ in Tk is the T-identity $\mathbf{1}_{nk}: nk \to nk$. Moreover, the unique Tk-morphism $0_n^{(k)}: 0 \to n$ is the T-morphism 0_{nk}. Generalizing this notation, we will denote a base morphism $n \to p$ in Tk as $\rho^{(k)}$. Given a function $\hat{\rho}: [n] \to [p]$, the corresponding base morphism in Tk is

$$\rho^{(k)} = \langle (1\hat{\rho})_p^{(k)}, ..., (n\hat{\rho})_p^{(k)} \rangle.$$

The morphism $\rho^{(k)}: n \to p$ can also be described as the base T-morphism corresponding to the following function $[nk] \to [pk]$. First, represent an integer in $[nk]$ as a pair $\langle i, j \rangle_{n,k} = (i-1)k + j$, where $i \in [n]$ and $j \in [k]$. The subscripts n, k will sometimes be omitted, so that we write $\langle i, j \rangle$, for short. Then $\rho^{(k)}: n \to p$ is the base T-morphism determined by the function

$$\langle i, j \rangle_{n,k} \mapsto \langle i\hat{\rho}, j \rangle_{p,k},$$

for all $i \in [n]$, $j \in [k]$. Note that this function maps the ith block of k integers in $[nk]$ to the $(i\hat{\rho})$th block in $[pk]$. In particular,

$$\tau_n^{(k)} = \langle \mathbf{1}_k, ..., \mathbf{1}_k \rangle : n \to 1 \in Tk.$$

(Recall Eq. (4).) *From now on, when the integer k is understood, we will just write $\vec{\rho}$ for $\rho^{(k)}$.*

When T is a preiteration theory, Tk is also a preiteration theory. The iteration operation in Tk is that inherited from T, so that for $f: n \to n+p$ in Tk, the iterate of f is the T-morphism $f^\dagger : nk \to pk$.

THEOREM 5.1. *If T is a Conway theory, then so is Tk, for each $k \geqslant 1$.*

Proof. Immediate from Theorem 3.4. ∎

An *equation* or *identity* in the language of preiteration theories is an equation $t = t'$ between sorted terms $n \to p$ built in the usual way from $\mathcal{N} \times \mathcal{N}$ sorted variables and constants i_p and 0_p using the operations of composition, tupling and iteration. (The constants $\mathbf{1}_n$ and the operations of pairing and separated sum as well as constants for the base morphisms may be defined in terms of the other operations and constants.)

Suppose that T is a preiteration theory and that Φ is a set of equations. We write $T \models \Phi$ when each equation $t = t'$ in Φ holds in T, or is satisfied by T. If Φ is the singleton $\{t = t'\}$, we write $T \models t = t'$ for $T \models \Phi$. Suppose that $T \models \Phi$ implies $T \models t = t'$, for all preiteration theories T. Then $t = t'$ is a logical consequence of Φ, denoted $\Phi \models t = t'$.

DEFINITION 5.2. Suppose that T is a preiteration theory and that $t = t'$ is an equation. We say that the *vector form of $t = t'$ holds in T*, or is satisfied by T, if $Tk \models t = t'$, for each $k \geqslant 1$.

The above definition can be extended to sets of equations in the obvious way.

An alternative definition is also possible. For a given equation $t = t'$ and integer $k \geqslant 1$, let $\vec{t} = \vec{t}'$ denote the equation obtained from $t = t'$ by replacing each variable of sort $n \to p$ by a variable of sort $nk \to pk$, and each base morphism ρ by $\vec{\rho}$. Then the vector form of $t = t'$ holds in T iff $T \models \vec{t} = \vec{t}'$, for each $k \geqslant 1$.

As an example, consider the scalar parameter identity

$$(f \cdot (\mathbf{1}_1 \oplus g))^\dagger = f^\dagger \cdot g, \qquad f: 1 \to 1 + p, \quad g: p \to q.$$

For an integer $k \geqslant 1$, its kth vector form is

$$(f \cdot (\mathbf{1}_k \oplus g))^\dagger = f^\dagger \cdot g, \qquad f: k \to k + pk, \quad g: pk \to qk. \tag{10}$$

When T is a Conway theory, the vector form of the scalar parameter identity holds in T as do the vector forms of all of the defining identities. For any preiteration theory T satisfying the right zero identity, Eq. (10) holds in T iff the parameter identity does. (Note that the right zero identity is a particular subcase of the parameter identity.)

LEMMA 5.3. *Suppose that Ax is some set of equations such that each preiteration theory satisfying Ax satisfies the vector forms of the equations in Ax. Suppose that $Ax \models t = t'$. Then for each preiteration theory T, if $T \models Ax$ then T satisfies the vector form of the equation $t = t'$.*

Proof. Suppose that $T \models Ax$. Then $Tk \models Ax$, for each $k \geqslant 1$. Since $Ax \models t = t'$, $Tk \models t = t'$. ∎

COROLLARY 5.4. *If an equation holds in all Conway theories, then so does its vector form.*

Proof. Immediate from Theorem 5.1 and Lemma 5.3. ∎

Sometimes instead of the theory Tk, we will work in a "dual" theory kT.

Suppose that T is a theory and $k \geqslant 1$. The theory kT is defined as follows. For each $n, p \geqslant 0$,

$$kT(n, p) = T(kn, kp) = Tk(n, p).$$

The composition operation in kT agrees with that in Tk and hence with the composition operation in T. However, for each $n \geqslant 0$ and $i \in [n]$, the ith distinguished morphism $1 \to n$ in kT is the base T-morphism $i_n^{[k]}$ corresponding to the map

$$[k] \to [kn]$$
$$j \mapsto \langle j, i \rangle_{k,n} = (j-1)\, n + i.$$

More generally, when ρ is a function $[n] \to [p]$, the base morphism determined by ρ in kT is the base T-morphism $\rho^{[k]}$ corresponding to the map

$$[kn] \to [kp]$$
$$\langle i, j \rangle_{k,n} \mapsto \langle i, j\rho \rangle_{k,n},$$

so that

$$\rho^{[k]} = \rho \oplus \cdots \oplus \rho : kn \to kp \in T.$$

In particular, $\mathbf{1}_n^{[k]} = \mathbf{1}_{kn} = \mathbf{1}_n^{(k)}$ and $0_n^{[k]} = 0_{kn} = 0_n^{(k)}$, for all $n \geqslant 0$. Moreover, $\tau_n^{[k]}$ is the base T-morphism $\tau_n \oplus \cdots \oplus \tau_n : kn \to k$. (Recall Eq. (4).)

From now on, when the integer k is clear from the context, we will just write $\bar{\rho}$ for $\rho^{[k]}$.

LEMMA 5.5. *The theories Tk and kT are isomorphic.*

Proof. For each $p, q \geqslant 0$, let $\pi_{p,q}$ denote the base morphism given by the map

$$[pq] \to [qp]$$
$$\langle i, j \rangle_{p,q} \mapsto \langle j, i \rangle_{q,p},$$

all $i \in [p]$, $j \in [q]$. Note that $\pi_{p,q}$ is a base permutation with inverse $\pi_{p,q}^{-1} = \pi_{q,p}$. The required isomorphism $\varphi: Tk \to kT$ is the theory morphism defined by

$$f: n \to p \in Tk \mapsto \pi_{k,n} \cdot f \cdot \pi_{p,k} \in kT, \qquad n, p \geqslant 0.$$

Indeed, for each $n, p \geqslant 0$, φ induces a bijective function $Tk(n, p) \to kT(n, p)$. Suppose that $f: n \to p$ and $g: p \to q$ in Tk. Since

$$\pi_{k,n} \cdot f \cdot g \cdot \pi_{q,k} = \pi_{k,n} \cdot f \cdot \pi_{p,k} \cdot \pi_{k,p} \cdot g \cdot \pi_{q,k},$$

φ preserves composition. Also,

$$\bar{\iota}_n = j \overset{\bar{\iota}_n}{\longmapsto} \langle i, j \rangle_{n,k} \overset{\pi_{n,k}}{\longmapsto} \langle j, i \rangle_{k,n},$$

for all $i \in [n]$ and $j \in [k]$. Thus φ preserves the distinguished morphisms. ∎

One can use the above lemma to derive formulas for the tupling and separated sum operations in the theory kT. Suppose that $f_i: 1 \to p$ in kT, for all $i \in [n]$. Then $\langle f_1, ..., f_n \rangle$ is a morphism $n \to p$ in kT, but this morphism is not the tupling of the f_i in the theory kT, determined by the coproduct structure given by the injections $\bar{\iota}_n$. In fact, the tupling of the f_i in kT is the morphism

$$[f_1, ..., f_n] = \pi_{k,n} \cdot \langle f_1, ..., f_n \rangle.$$

Note that if $f_i = \langle f_{i,1}, ..., f_{i,k} \rangle$, where $f_{i,j}: 1 \to kp$ in T, then

$$[f_1, ..., f_n] = \langle f_{1,1}, ..., f_{n,1}, ..., f_{1,k}, ..., f_{n,k} \rangle.$$

This fact may be generalized to tuplings of vector morphisms in kT in a straightforward way.

The separated sum operation in kT, that we denote by $\otimes$, is also different from the corresponding operation in Tk. To give the form of the $\otimes$-operation, let us introduce for each $p, q, r \geqslant 0$ the base permutation $\delta_{p,q,r}: pq + pr \to p(q + r)$:

$$\langle i, j \rangle_{p,q} \mapsto \langle i, j \rangle_{p,q+r}, \qquad \text{all} \quad i \in [p], \quad j \in [q]$$

$$pq + \langle i, j \rangle_{p,r} \mapsto \langle i, q + j \rangle_{p,q+r}, \qquad \text{all} \quad i \in [p], \quad j \in [r].$$

Using these base permutations, we have, for all $f: n \to p$ and $g: m \to q$ in kT,

$$f \otimes g = \delta_{k,n,m}^{-1} \cdot (f \oplus g) \cdot \delta_{k,p,q}.$$

When T is a preiteration theory, so is each theory kT with the following operation ‡. If $f: n \to n + p$ in kT, then $f: kn \to k(n + p)$ in T, so that $f \cdot \delta_{k,n,p}^{-1}: kn \to kn + kp$ in T. We define

$$f^{\ddagger} = (f \cdot \delta_{k,n,p}^{-1})^{\dagger}: n \to p \in kT.$$

LEMMA 5.6. *If the permutation and parameter identities hold in T, then for each $k \geqslant 1$, the preiteration theories Tk and kT are isomorphic.*

Proof. We show that the theory morphism φ defined in the proof of Lemma 5.5 preserves dagger. Let $f: n \to n+p$ in Tk. Then, writing δ for $\delta_{k,n,p}$,

$$\begin{aligned}(f\varphi)^{\ddagger} &= (\pi_{k,n} \cdot f \cdot \pi_{n+p,k})^{\ddagger} \\ &= (\pi_{k,n} \cdot f \cdot (\pi_{n,k} \oplus \pi_{p,k}) \cdot \delta)^{\ddagger} \\ &= (\pi_{k,n} \cdot f \cdot (\pi_{n,k} \oplus \pi_{p,k}) \cdot \delta \cdot \delta^{-1})^{\dagger} \\ &= (\pi_{k,n} \cdot f \cdot (\pi_{n,k} \oplus \pi_{p,k}))^{\dagger} \\ &= \pi_{k,n} \cdot f^{\dagger} \cdot \pi_{p,k} \\ &= f^{\dagger}\varphi,\end{aligned}$$

by the permutation and parameter identities, and since $(\pi_{n,k} \oplus \pi_{p,k}) \cdot \delta = \pi_{n+p,k}$. ∎

Using the isomorphism φ, if the parameter and permutation identities hold in T, then for each $k \geqslant 1$, the theory Tk satisfies an identity iff kT does. Thus, we may establish the vector form of an identity in T by proving that the identity holds in all theories kT.

6. AUTOMATA AND SEMIGROUPS

Except for free semigroups, all semigroups will be assumed to be finite. The product of the elements s, t in a semigroup will be written $s \circ t$, or just st.

We will use standard terminology. A subgroup of a semigroup S is a subsemigroup of S which is a group. Following [8, 28], we say that a semigroup S *divides* a semigroup S', denoted $S \mid S'$, if S is a homomorphic image of a subsemigroup of S'. It is known, see e.g. [8], that the division relation is transitive (and reflexive). Further, a group G divides a semigroup S iff G is a homomorphic image of a subgroup of S. A group G is called *simple* if it is nontrivial and has no proper nontrivial normal subgroup.

A (*finite*) *automaton* $(A, X, \circ)$ consists of the finite nonempty sets A and X and a (right) action of X on A:

$$\circ: A \times X \to A$$

$$(a, x) \mapsto a \circ x.$$

We will usually write ax for $a \circ x$ and (A, X) for $(A, X, \circ)$. The action of X on A may be extended to an action of the free semigroup X^+ such that

$$a(ux) = (au)x$$

for all $a \in A$, $u \in X^+$ and $x \in X$. (We will represent X^+ as the semigroup of all nonempty words over the set X.) Suppose that $C \subseteq A$ and $u \in X^+$. Then we will write Cu to denote the set $\{cu: c \in C\}$. The set AX is defined by $AX = \bigcup_{x \in X} Ax$.

Suppose that (A, X) is an automaton. A letter $x \in X$ is a permutation letter (reset letter, respectively) if the function

$$a \mapsto ax, \qquad a \in A$$

is a permutation map (constant map, respectively) on A. We call (A, X) a *permutation automaton* (*reset automaton*, respectively) if each letter $x \in X$ is a permutation letter (reset letter, respectively). Further, we call (A, X) a *permutation–reset automaton* if each $x \in X$ is either a permutation letter or a reset letter. For example, the automaton $\mathbf{U} = (\{a_1, a_2\}, \{x_1, x_2, x_3\})$ equipped with the action

$$a_i x_j = a_j$$

$$a_i x_3 = a_i$$

$i, j \in [2]$ is a permutation-reset automaton, called the *two-state identity-reset automaton.*

Homomorphisms, subautomata, and congruences of automata are defined in the usual way. The automaton (A, X) is called a *renaming* of the automaton (A, Y) if there is a function $\varphi: X \to Y$ such that

$$ax = a(x\varphi),$$

for all $a \in A$ and $x \in X$.

Suppose that (A, X) is an automaton. Recall that each word $u \in X^+$ induces a function $A \to A$. Equipped with the operation of composition (which we write in diagrammatic order), these functions form a semigroup denoted $S(A, X)$. We call $S(A, X)$ the *semigroup of the automaton* (A, X). When (A, X) is a permutation automaton, each element of $S(A, X)$ is a permutation of the set A, so that $S(A, X)$ is a group that we prefer to denote by $G(A, X)$. An automaton (A, X) is called *aperiodic* [8], if each subgroup of $S(A, X)$ is trivial. For example, each reset automaton, or more generally, each *definite* automaton [8] is aperiodic. The semigroup $S(\mathbf{U})$ of the two-state identity-reset automaton will be important in Section 9. Note that $S(\mathbf{U})$ is a 3-element monoid whose nonidentity elements are right zeros.

Sometimes we will use the following extension of the notion of the semigroup of an automaton. Suppose that (A, X) is an automaton and C is a nonempty subset of A. Then we denote by $S(C)$ the collection of all functions $s: C \to C$ such that there is a function $s' \in S(A, X)$ with $cs = cs'$, for all $c \in C$. Again, the set $S(C)$ is a semigroup, and $S(C) \mid S(A, X)$.

When (A, X) is an automaton such that $X = S$ is a semigroup and the action is compatible with the semigroup operation, i.e.,

$$a(st) = (as)t,$$

for all $a \in A$ and $s, t \in S$, we call the automaton (A, S) a *transformation semigroup*. (Note that we are not requiring that the action is faithful.) When S is a group with unit e and

$$ae = a,$$

for all $a \in A$, (A, S) is a *transformation group*. See [8]. Note that each transformation group is a permutation automaton.

For each semigroup S there is a corresponding transformation semigroup (S, S) equipped with the natural self action $(s, t) \mapsto st$. When S is a group, (S, S) is a transformation group.

7. IDENTITIES ASSOCIATED WITH AUTOMATA AND SEMIGROUPS

Suppose that $(A, X) = (A, X, \circ)$ is a finite automaton such that $A = [n]$ and $X = [m]$, for some integers n and m. In each theory T, we associate with (A, X) the base morphisms $\rho_i^{(A, X)}: m \to n$, $i \in [n]$ defined by

$$j_m \cdot \rho_i^{(A, X)} = (i \circ j)_n, \qquad \text{all} \quad j \in [m], \quad \text{i.e.,}$$

$$\rho_i^{(A, X)} = \langle (i \circ 1)_n, (i \circ 2)_n, ..., (i \circ m)_n \rangle.$$

From now on, we write just ij instead of $i \circ j$. The morphism $(ij)_n$ is the corresponding base morphism $1 \to n$. The morphisms $\rho_i^{(A, X)}$, denoted sometimes just ρ_i, are called the *base morphisms associated with the automaton* (A, X).

Let $f = \langle f_1, ..., f_n \rangle$ be a morphism $n \to m + p$ in a preiteration theory T. We define

$$f \bullet (A, X) = f \| (\rho_1^{(A, X)}, ..., \rho_n^{(A, X)}): n \to n + p.$$

Thus,

$$f \bullet (A, X) = \langle f_1 \cdot (\rho_1^{(A, X)} \oplus \mathbf{1}_p), ..., f_n \cdot (\rho_n^{(A, X)} \oplus \mathbf{1}_p) \rangle.$$

Further, we define, for each $g: 1 \to m + p$,

$$\begin{aligned} g_{(A, X)} &= (\tau_n \cdot g) \bullet (A, X) \\ &= \langle g \cdot (\rho_1^{(A, X)} \oplus \mathbf{1}_p), ..., g \cdot (\rho_n^{(A, X)} \oplus \mathbf{1}_p) \rangle: n \to n + p. \end{aligned}$$

DEFINITION 7.1. The *automaton identity* $\mathbf{C}(A, X)$ associated with (A, X) is

$$g^\dagger_{(A, X)} = \tau_n \cdot (g \cdot (\tau_m \oplus \mathbf{1}_p))^\dagger, \qquad g: 1 \to m + p. \tag{11}$$

Note that when $m \leqslant n$, this identity is an instance of the scalar commutative identity. Moreover, in preiteration theories satisfying the functorial implication for injective morphisms, each automaton-identity is equivalent to an instance of the scalar commutative identity.

In preiteration theories T satisfying the permutation identity, that we assume from now on, it is possible to associate an identity with any automaton or semigroup, not just with those defined on the sets $[n]$. In such theories, identities associated with isomorphic automata or semigroups are equivalent.

Since any transformation semigroup is an automaton, the above definition associates an identity $\mathbf{C}(A, S)$ with each transformation semigroup (A, S). When (A, S) is the transformation semigroup (S, S) equipped with the natural self action, we denote $\mathbf{C}(S, S)$ by $\mathbf{C}(S)$ and call this identity the *semigroup identity associated with S*. Accordingly we write g_S for $g_{(S, S)}$ and ρ_i^S for $\rho_i^{(S, S)}$. When S is group, $\mathbf{C}(S)$ is a *group identity*.

The above notation may be extended to classes of semigroups. When $\mathscr{S}$ is a class of finite semigroups, $\mathbf{C}(\mathscr{S})$ consists of the identities $\mathbf{C}(S)$, $S \in \mathscr{S}$.

EXAMPLE 7.2. Let $\mathbf{U}$ be the two-state identity-reset automaton, then $\mathbf{C}(\mathbf{U})$ is

$$\langle f \cdot (\langle 1_2, 2_2, 1_2 \rangle \oplus \mathbf{1}_p), f \cdot (\langle 1_2, 2_2, 2_2 \rangle \oplus \mathbf{1}_p) \rangle^\dagger$$
$$= \tau_2 \cdot (f \cdot (\tau_3 \oplus \mathbf{1}_p))^\dagger, \qquad f: 1 \to 3 + p.$$

Suppose that G is the group of order 3. Then $\mathbf{C}(G)$ is

$$\langle f, f \cdot (\langle 2_3, 3_3, 1_3 \rangle \oplus \mathbf{1}_p), f \cdot (\langle 3_3, 1_3, 2_3 \rangle \oplus \mathbf{1}_p) \rangle^\dagger = \tau_3 \cdot (f \cdot (\tau_3 \oplus \mathbf{1}_p))^\dagger,$$
$$f: 1 \to 3 + p.$$

Each automaton identity or semigroup identity has a vector form. Suppose that (A, X) is an automaton with $A = [n]$ and $X = [m]$. Let us write ρ_i for $\rho_i^{(A, X)}$, $i \in [n]$. Recall that for each $k \geqslant 1$, $\vec{\rho}_i$ is a base morphism $m \to n$ in Tk and a base morphism $mk \to nk$ in T. When $F = \langle F_1, ..., F_n \rangle : nk \to mk + q$, where $k \geqslant 1$ and $F_i : k \to mk + q$ for each $i \in [n]$, define

$$F \bullet (A, X) = F \| (\vec{\rho}_1, ..., \vec{\rho}_n)$$
$$= \langle F_1 \cdot (\vec{\rho}_1 \oplus \mathbf{1}_q), ..., F_n \cdot (\vec{\rho}_n \oplus \mathbf{1}_q) \rangle : nk \to nk + q.$$

Moreover, let us denote

$$F_{(A, X)} = (\vec{\tau}_n \cdot F) \bullet (A, X)$$
$$= \langle F \cdot (\vec{\rho}_1 \oplus \mathbf{1}_q), ..., F \cdot (\vec{\rho}_n \oplus \mathbf{1}_q) \rangle.$$

for all $F : k \to mk + q$.

The vector form of $\mathbf{C}(A, X)$ is the identity:

$$F^{\dagger}_{(A, X)} = \vec{\tau}_n \cdot (F \cdot (\vec{\tau}_m \oplus \vec{\mathbf{1}}_p))^{\dagger},$$

where $F: k \to mk + pk$. Note that if the right zero identity holds in T then T satisfies the vector form of $\mathbf{C}(A, X)$ iff

$$F^{\dagger}_{(A, X)} = \vec{\tau}_n \cdot (F \cdot (\vec{\tau}_m \oplus \mathbf{1}_q))^{\dagger},$$

for all $F: k \to mk + q$ in T.

Sometimes we will consider the "dual" vector form of the identity $\mathbf{C}(A, X)$. Let $G = \langle G_1, ..., G_k \rangle: k \to k(m + p)$ in a preiteration theory T with $G_i: 1 \to k(m + p)$, $i \in [k]$. Then, in kT,

$$G_{(A, X)} = [G \cdot (\bar{\rho}_1 \otimes \overleftarrow{\mathbf{1}}_p), ..., G \cdot (\bar{\rho}_n \otimes \overleftarrow{\mathbf{1}}_p)]$$

so that in T,

$$\begin{aligned} G_{(A, X)} &= \pi_{k, n} \cdot \langle G \cdot \delta^{-1} \cdot (\bar{\rho}_1 \oplus \overleftarrow{\mathbf{1}}_p) \cdot \delta', ..., G \cdot \delta^{-1} \cdot (\bar{\rho}_n \oplus \overleftarrow{\mathbf{1}}_p) \cdot \delta' \rangle \\ &= \pi_{k, n} \cdot \langle (G \cdot \delta^{-1}) \cdot (\bar{\rho}_1 \oplus \overleftarrow{\mathbf{1}}_p), ..., (G \cdot \delta^{-1}) \cdot (\bar{\rho}_n \oplus \overleftarrow{\mathbf{1}}_p) \rangle \cdot \delta', \end{aligned}$$

where $\delta = \delta_{k, m, p}$ and $\delta' = \delta_{k, n, p}$. Thus, writing $H = G \cdot \delta^{-1}$ and $H_i = G_i \cdot \delta^{-1}$, $i \in [k]$,

$$G_{(A, X)} = \pi_{k, n} \cdot \langle H \cdot (\bar{\rho}_1 \oplus \overleftarrow{\mathbf{1}}_p), ..., H \cdot (\bar{\rho}_n \oplus \overleftarrow{\mathbf{1}}_p) \rangle \cdot \delta',$$

so that

$$\begin{aligned} G^{\ddagger}_{(A, X)} &= (\pi_{k, n} \cdot \langle H \cdot (\bar{\rho}_1 \oplus \overleftarrow{\mathbf{1}}_p), ..., H \cdot (\bar{\rho}_n \oplus \overleftarrow{\mathbf{1}}_p) \rangle)^{\dagger} \\ &= \langle (\tau_n \cdot H_1) \| (\bar{\rho}_1, ..., \bar{\rho}_n), ..., (\tau_n \cdot H_k) \| (\bar{\rho}_1, ..., \bar{\rho}_n) \rangle^{\dagger}, \end{aligned}$$

where the operation $\|$ is evaluated in the theory T. Also,

$$\begin{aligned} \bar{\tau} \cdot (G \cdot (\bar{\tau}_m \otimes \overleftarrow{\mathbf{1}}_p))^{\ddagger} &= \bar{\tau}_n \cdot (G \cdot \delta^{-1} \cdot (\bar{\tau}_m \oplus \overleftarrow{\mathbf{1}}_p) \cdot \delta')^{\ddagger} \\ &= \bar{\tau}_n \cdot (H \cdot (\bar{\tau}_m \oplus \overleftarrow{\mathbf{1}}_p))^{\dagger}. \end{aligned}$$

Thus, the dual vector form of the identity $\mathbf{C}(A, X)$,

$$G^{\ddagger}_{(A, X)} = \bar{\tau} \cdot (G \cdot (\bar{\tau} \oplus \overleftarrow{\mathbf{1}}_p))^{\ddagger}$$

becomes

$$H^{\dagger}_{(A, X)} = \bar{\tau}_n \cdot (H \cdot (\bar{\tau}_m \oplus \mathbf{1}_{kp}))^{\dagger}, \tag{12}$$

where

$$H_{(A,X)} = \langle (\tau_n \cdot H_1) \| (\bar{\rho}_1, ..., \bar{\rho}_n), ..., (\tau_n \cdot H_k) \| (\bar{\rho}_1, ..., \bar{\rho}_n) \rangle.$$

Again, we may substitute q for kp.

We end this section with the following lemma, proved in [14].

LEMMA 7.3. *In Conway theories, the commutative identity is equivalent to the vector forms of the identities associated with finite automata. Hence a Conway theory T is an iteration theory iff T satisfies the vector form of each identity $\mathbf{C}(A, X)$ associated with a finite automaton (A, X).*

8. THE MAIN RESULT

The main result of the paper is the following theorem.

THEOREM 8.1. *Suppose that $\mathscr{S}$ is a class of finite semigroups. Then the Conway identities and the semigroup identities $\mathbf{C}(\mathscr{S})$ form a complete axiomatization of iteration theories iff each finite (simple) group is a divisor of some semigroup in $\mathscr{S}$.*

From Theorem 8.1, we immediately have the following corollary.

COROLLARY 8.2. *The Conway identities and the group identities corresponding to the finite (simple) groups form a complete axiomatization of iteration theories.*

COROLLARY 8.3. *The Conway identities and the scalar commutative identity are a complete axiomatization of iteration theories.*

Proof. Each group identity is an instance of the scalar commutative identity. ∎

COROLLARY 8.4 [13]. *Iteration theories do not have a "finite" axiomatization.*

9. THE KROHN–RHODES DECOMPOSITION

In this section we review a basic result of Krohn and Rhodes [8, 20, 28] for the decomposition of automata using cascade composition. This result will play a prominent role in our completeness argument. We start by defining the cascade composition.

Suppose that (A, X) and (B, Y) are finite automata and

$$\varphi: A \times X \to Y$$
$$(a, x) \mapsto {}^{a}x$$

is a given function. The cascade composition of (A, X) and (B, Y) with respect to φ is the automaton

$$(B, Y) \times_{\varphi} (A, X) = (B \times A, X),$$

equipped with the X-action

$$(b, a)x = (b^a x, ax),$$

for all $a \in A$, $b \in B$ and $x \in X$.

Remark 9.1. Many authors define the cascade composition of the automata (A, X) and (B, Y) in the opposite order writing $(A, X) \times_\varphi (B, Y)$.

Recall that **U** denotes the two-state identity reset automaton.

THEOREM 9.2. Krohn–Rhodes Decomposition Theorem, Part 1. *Let K denote a nonempty class of automata and let $\bar{K}$ denote the least class of automata containing K and closed under cascade composition, renaming, subautomata and homomorphic images. If S is a simple group or one of the divisors of the semigroup of the automaton* **U**, *and if S divides the semigroup of an automaton in $\bar{K}$, then S also divides the semigroup of an automaton in K.*

THEOREM 9.3. Krohn–Rhodes Decomposition Theorem, Part 2. *Suppose that (A, X) is an automaton. Let $\mathcal{G}$ denote the class of simple groups G such that $G \mid S(A, X)$. Then (A, X) is contained in the least class of automata containing* **U** *and the automata (G, G) equipped with the natural self action, for all $G \in \mathcal{G}$, closed under the cascade composition, renaming, subautomata, and homomorphic images.*

Actually, we will make use of a variant of the Krohn–Rhodes Decomposition Theorem proved in [15]. In order to state this result, we need some more definitions.

Suppose that $\equiv$ is a congruence of the automaton (A, X). We call $\equiv$ a *permutation-reset congruence* if the following conditions hold:

- For any two (nonsingleton) $\equiv$-equivalence classes C and C', and for each letter $x \in X$ with $Cx \subseteq C'$, either $Cx = C'$ or Cx is a singleton subset of C'.
- For any two distinct nonsingleton $\equiv$-equivalence classes C and C' there is a word $u \in X^+$ with $Cu = C'$.

Thus, any two nonsingleton $\equiv$-equivalence classes have equal number of elements.

Let $\mathcal{G}$ be a class of simple groups closed under division. We call a congruence $\equiv$ on the automaton (A, X) a *$\mathcal{G}$-congruence* if for each $\equiv$-equivalence class C, each simple group divisor of $S(C)$ is in $\mathcal{G}$. A *permutation-reset $\mathcal{G}$-congruence* is a permutation-reset congruence which is a $\mathcal{G}$-congruence. Further, we call $\equiv$ an *elementary congruence* if Cx is a singleton for each equivalence class C and letter $x \in X$, and if for each equivalence class C at most one element in C belongs to AX. A 1-*elementary congruence* is an elementary congruence which has a single nonsingleton equivalence class, and, moreover, this equivalence class has exactly two elements. Note that any elementary congruence is a $\mathcal{G}$-congruence, for any $\mathcal{G}$.

Suppose that (A, X) and (B, X) are automata and φ is a homomorphism $(A, X) \to (B, X)$. We call φ a permutation-reset homomorphism or a $\mathcal{G}$-homomorphism if $\ker(\varphi)$, the kernel of φ has the appropriate property. Elementary and 1-elementary homomorphisms are defined in the same way.

Remark 9.4. For technical reasons, a permutation-reset congruence is termed a simple regular congruence in [15].

THEOREM 9.5 [15]. *Suppose that* (A, X) *is an automaton. Let* $\mathscr{G}$ *denote the class of simple groups* G *such that* $G \mid S(A, X)$. *Then*:

1. (A, X) *is contained in the least class of automata containing the two-state identity-reset automaton* $\mathbf{U}$ *and the automata* (G, G) *equipped with the natural self action, for all* $G \in \mathscr{G}$, *closed under the cascade composition, renaming, subautomata and* $\mathscr{G}$*-homomorphic images, or permutation-reset* $\mathscr{G}$*-homomorphic images.*

2. *There is a sequence*

$$(A_1, X), ..., (A_k, X), \qquad k \geqslant 1$$

of automata such that (A_1, X) *is trivial, i.e., a one-state automaton,* (A_k, X) *is* (A, X), *and for each* $i \in [k-1]$, *either* (A_i, X) *is a homomorphic image of* (A_{i+1}, X) *under a surjective (permutation-reset)* $\mathscr{G}$*-homomorphism, or there is a surjective (permutation-reset)* $\mathscr{G}$*-homomorphism* $(A_i, X) \to (A_{i+1}, X)$.

In addition to Theorem 9.5, we will refer to the following lemma, which gives one step in the proof of Theorem 9.5.

LEMMA 9.6 [15]. *Let* $\mathscr{G}$ *be a class of simple groups closed under division. Suppose that* (A, X) *and* (B, X) *are finite automata and* h *is a surjective permutation-reset* $\mathscr{G}$*-homomorphism* $(A, X) \to (B, X)$. *Then there is a permutation-reset automaton* (C, Y) *and a cascade composition* $(C \times B, X) = (C, Y) \times_\varphi (B, X)$ *such that the following conditions hold*:

- (A, X) *is isomorphic to a subautomaton of* $(C \times B, X)$.
- *There is a surjective elementary homomorphism* $(C \times B, X) \to (A, X)$.
- *If* G *is a simple group with* $G \mid S(C, Y)$, *then* $G \in \mathscr{G}$.

10. GROUP IDENTITIES

In this section, T denotes a preiteration theory satisfying at least the permutation and parameter identities.

Assume that S is a semigroup on the set $[n]$. For each $i \in [n]$, denote the morphism $\rho_i^S : n \to n$ by just ρ_i. Note that

$$\rho_i \cdot \rho_j = \rho_{ji},$$

for all $i, j \in [n]$, so that the structure of S is encoded in the compositional structure of the base morphisms ρ_i. Recall that for an integer $k \geqslant 1$,

$$\bar{\tau}_n = \tau_n \oplus \cdots \oplus \tau_n : kn \to k$$

$$\bar{\rho}_i = \rho_i \oplus \cdots \oplus \rho_i : kn \to kn,$$

for all $i \in [n]$. Below we will sometimes use these notations for different values of k. Nevertheless, the correct value will always be clear from the context.

DEFINITION 10.1. Suppose that $g: kn \to k'n + p$ in T, where $k, k' \geqslant 1$. We say that g *commutes with the base morphisms associated with* S if

$$\bar{\rho}_i \cdot g = g \cdot (\bar{\rho}_i \oplus \mathbf{1}_p),$$

for all $i \in [n]$.

Note that the notation $\bar{\rho}_i$ stands for a morphism $kn \to kn$ on the left hand side, and for a morphism $k'n \to k'n$ on the right-hand side of (13).

Below, we give a characterization of the morphisms that commute with the base morphisms associated with a group.

LEMMA 10.2. *Suppose that* $f: 1 \to kn + p$ *in* T, *where* $k \geqslant 1$. *If*

$$g = (\tau_n \cdot f) \,\|\, (\bar{\rho}_1, ..., \bar{\rho}_n): n \to kn + p, \tag{14}$$

i.e.,

$$g = \langle f \cdot (\bar{\rho}_1 \oplus \mathbf{1}_p), ..., f \cdot (\bar{\rho}_n \oplus \mathbf{1}_p) \rangle,$$

then g *commutes with the base morphisms associated with* S. *Conversely, if* S *is a group* (*or a monoid*), *and if morphism* $g: n \to kn + p$ *commutes with the base morphisms associated with* S, *then* g *is determined by a morphism* $f: 1 \to kn + p$ *as in* (14).

Proof. Assuming (14), we have

$$\begin{aligned} j_n \cdot \rho_i \cdot g &= (ij)_n \cdot g \\ &= f \cdot (\bar{\rho}_{ij} \oplus \mathbf{1}_p) \\ &= f \cdot (\bar{\rho}_j \oplus \mathbf{1}_p) \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \\ &= j_n \cdot g \cdot (\bar{\rho}_i \oplus \mathbf{1}_p), \end{aligned}$$

for all $i, j \in [n]$.

Suppose now that S is a group and $g: n \to kn + p$ commutes with the base morphisms associated with S. Without loss of generality we may assume that the unit element of S is the integer 1. Then,

$$\begin{aligned} i_n \cdot g &= 1_n \cdot \rho_i \cdot g \\ &= 1_n \cdot g \cdot (\bar{\rho}_i \oplus \mathbf{1}_p), \end{aligned}$$

for all $i \in [n]$. Thus, Eq. (14) holds for the morphism $f = 1_n \cdot g$. ∎

For the rest of this section we assume that S is in fact a group. Henceforth we denote S by G.

COROLLARY 10.3. *Suppose that* $g: kn \to k'n + p$ *in* T, *where* $k, k' \geqslant 1$. *Then* g *commutes with the base morphisms associated with* G *iff there is a morphism* $f = \langle f_1, ..., f_k \rangle: k \to k'n + p$ *such that*

$$g = \langle (\tau_n \cdot f_1) \| \bar{R}, ..., (\tau_n \cdot f_k) \| \bar{R} \rangle,$$

where $\bar{R} = (\bar{\rho}_1, ..., \bar{\rho}_n)$.

Proof. Clearly, g commutes with the base morphisms associated with G iff $g = \langle g_1, ..., g_k \rangle$ for some morphisms $g_i: n \to k'n + p$, $i \in [k]$ which commute with the base morphisms associated with G. Hence the result follows from Lemma 10.2. ∎

COROLLARY 10.4. *For any integer* $k \geqslant 1$, *the* k*th vector form of the identity* $\mathbf{C}(G)$ *holds in* T *iff*

$$g^\dagger = \bar{\tau}_n \cdot (\overleftarrow{1}_n \cdot g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger, \tag{15}$$

for each morphism $g: kn \to kn + p$ *that commutes with the base morphisms associated with* G.

Proof. This follows from Corollary 10.3 and Eq. (12). ∎

Note that the morphism $\overleftarrow{1}_n \cdot g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$ can be constructed from $g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$ as follows. First, we divide the components of $g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$ into k blocks of length n, then we select the first component of each block. The morphism $\overleftarrow{1}_n \cdot g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$ is the tupling of these components. The identity (15) asserts that the first n components of $g^\dagger$ are all equal to the first component of $(\overleftarrow{1}_n \cdot g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger$, the second n components to the second component of $(\overleftarrow{1}_n \cdot g \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger$, etc.

LEMMA 10.5. *If* $g: n \to kn + p$ *commutes with the base morphisms associated with* G, *where* $k \geqslant 2$, *then so does the morphism* $g^\dagger: n \to (k-1)\, n + p$.

Proof. Since G is a group, each ρ_i (and each $\bar{\rho}_i$) is a base permutation. Thus, for each $i \in [n]$,

$$\begin{aligned}
\rho_i \cdot g^\dagger &= (\rho_i \cdot g \cdot (\rho_i^{-1} \oplus \mathbf{1}_{(k-1)\, n + p}))^\dagger \\
&= (g \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \cdot (\rho_i^{-1} \oplus \mathbf{1}_{(k-1)\, n + p}))^\dagger \\
&= (g \cdot (\rho_i \oplus \bar{\rho}_i \oplus \mathbf{1}_p) \cdot (\rho_i^{-1} \oplus \mathbf{1}_{(k-1)\, n + p}))^\dagger \\
&= (g \cdot (\mathbf{1}_n \oplus \bar{\rho}_i \oplus \mathbf{1}_p))^\dagger \\
&= g^\dagger \cdot (\bar{\rho}_i \oplus \mathbf{1}_p),
\end{aligned}$$

by the parameter and permutation identities, and since g commutes with the base morphisms associated with G. ∎

Remark 10.6. Defining $\rho_i^{[0]} = 0_0$, for all $i \in [n]$, the previous proof works even for $k = 1$. Thus, for any $f: 1 \to n + p$ in a Conway theory and for any group G

of order n, the components of $f^\dagger_G$ are equal. It follows that $T \models \mathbf{C}(G)$ iff the equation

$$1_n \cdot f^\dagger_G = (f \cdot (\tau_n \oplus \mathbf{1}_p))^\dagger$$

holds in T, for all $f: 1 \to n+p$.

The main result of this section is the following proposition, which asserts that in conjunction with the Conway identities, any group identity implies its vector form.

PROPOSITION 10.7. *Suppose that T is a Conway theory satisfying $\mathbf{C}(G)$. Then the vector form of $\mathbf{C}(G)$ holds in T.*

Proof. We need to show that

$$f^\dagger_G = \bar{\tau}_n \cdot (f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger, \tag{16}$$

for all $f = \langle f_1, ..., f_k \rangle: k \to kn+p$ and $k \geqslant 1$. Recall that

$$f_G = \langle (\tau_n \cdot f_1) \parallel \bar{R}, ..., (\tau_n \cdot f_k) \parallel \bar{R} \rangle,$$

where $\bar{R} = (\bar{\rho}_1, ..., \bar{\rho}_n)$. See (12).

When $k = 1$, (16) holds by assumption. We proceed by induction on k. When $k > 1$, we apply the pairing identity to compute $f^\dagger_G$ and $(f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger$. Hence we define

$$\begin{aligned}
g_1 &= (\tau_n \cdot f_1) \parallel \bar{R}: n \to kn+p \\
g_2 &= \langle (\tau_n \cdot f_2) \parallel \bar{R}, ..., (\tau_n \cdot f_k) \parallel \bar{R} \rangle: (k-1)\, n \to kn+p \\
h_1 &= f_1 \cdot (\bar{\tau}_n \oplus \mathbf{1}_p): 1 \to k+p \\
h_2 &= \langle f_2, ..., f_k \rangle \cdot (\bar{\tau}_n \oplus \mathbf{1}_p): k-1 \to k+p,
\end{aligned}$$

so that g_1 is the tupling of the first n, and g_2 is the tupling of the last $(k-1)n$ components of f_G, moreover, h_1 is the first component, and h_2 is the tupling of the last $k-1$ components of $f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$. Thus,

$$\begin{aligned}
f_G &= \langle g_1, g_2 \rangle \\
f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) &= \langle h_1, h_2 \rangle.
\end{aligned}$$

Note that since

$$f_G \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) = \bar{\tau}_n \cdot f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p),$$

we have

$$g_1 \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) = \tau_n \cdot h_1: n \to k+p \tag{17}$$

$$g_2 \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) = \bar{\tau}_n \cdot h_2: (k-1)\, n \to k+p. \tag{18}$$

Since by Corollary 10.3 f_G commutes with the base morphisms associated with G, so do the morphisms g_1 and g_2, i.e.,

$$\rho_i \cdot g_1 = g_1 \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \colon n \to kn + p \tag{19}$$

$$\bar{\rho}_i \cdot g_2 = g_2 \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \colon (k-1)\, n \to kn + p, \tag{20}$$

for all $i \in [n]$.

By the pairing identity,

$$f_G^\dagger = \langle g_1^\dagger \cdot \langle u^\dagger, \mathbf{1}_p \rangle, u^\dagger \rangle \tag{21}$$

$$(f \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger = \langle h_1^\dagger \cdot \langle v^\dagger, \mathbf{1}_p \rangle, v^\dagger \rangle, \tag{22}$$

where

$$u = g_2 \cdot \langle g_1^\dagger, \mathbf{1}_{(k-1)n+p} \rangle \colon (k-1)\, n \to (k-1)\, n + p$$

$$v = h_2 \cdot \langle h_1^\dagger, \mathbf{1}_{k-1+p} \rangle \colon k-1 \to k-1+p.$$

We show that $g_1^\dagger$ and u commute with the base morphisms associated with G. Indeed, by (19) and Lemma 10.5,

$$\rho_i \cdot g_1^\dagger = g_1^\dagger \cdot (\bar{\rho}_i \oplus \mathbf{1}_p), \tag{23}$$

for all $i \in [n]$. Also, by (20) and (23),

$$\begin{aligned}
\bar{\rho}_i \cdot u &= \bar{\rho}_i \cdot g_2 \cdot \langle g_1^\dagger, \mathbf{1}_{(k-1)n+p} \rangle \\
&= g_2 \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \cdot \langle g_1^\dagger, \mathbf{1}_{(k-1)n+p} \rangle \\
&= g_2 \cdot \langle \rho_i \cdot g_1^\dagger, \bar{\rho}_i \oplus \mathbf{1}_p \rangle \\
&= g_2 \cdot \langle g_1^\dagger \cdot (\bar{\rho}_i \oplus \mathbf{1}_p), \bar{\rho}_i \oplus \mathbf{1}_p \rangle \\
&= g_2 \cdot \langle g_1^\dagger, \mathbf{1}_{(k-1)n+p} \rangle \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \\
&= u \cdot (\bar{\rho}_i \oplus \mathbf{1}_p),
\end{aligned}$$

for all $i \in [n]$. Thus, by the induction assumption and Corollary 10.4,

$$u^\dagger = \bar{\tau}_n \cdot (\overleftarrow{1}_n \cdot u \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger \colon (k-1)\, n \to p. \tag{24}$$

We will show below that the morphism $\overleftarrow{1}_n \cdot u \cdot (\bar{\tau}_n \oplus \mathbf{1}_p)$ appearing in the right-hand side of (24) is in fact the morphism v defined above. Indeed, using the parameter identity,

$$\begin{aligned}
u \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) &= g_2 \cdot \langle g_1^\dagger, \mathbf{1}_{(k-1)n+p} \rangle \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) \\
&= g_2 \cdot \langle g_1^\dagger \cdot (\bar{\tau}_n \oplus \mathbf{1}_p), \bar{\tau}_n \oplus \mathbf{1}_p \rangle \\
&= g_2 \cdot \langle (g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p))^\dagger, \bar{\tau}_n \oplus \mathbf{1}_p \rangle.
\end{aligned} \tag{25}$$

Since g_1 commutes with the base morphism associated with G, so does $g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p)$. Indeed, by (19),

$$\begin{aligned}\rho_i \cdot g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p) &= g_1 \cdot (\bar{\rho}_i \oplus \mathbf{1}_p) \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p) \\ &= g_1 \cdot (\rho_i \oplus \bar{\tau}_n \oplus \mathbf{1}_p) \\ &= g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p) \cdot (\rho_i \oplus \mathbf{1}_{k-1+p}),\end{aligned}$$

for all $i \in [n]$. Thus, since $T \models \mathbf{C}(G)$,

$$\begin{aligned}(g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p))^\dagger &= \tau_n \cdot (1_n \cdot g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p) \cdot (\tau_n \oplus \mathbf{1}_{k-1+p}))^\dagger \\ &= \tau_n \cdot (1_n \cdot g_1 \cdot (\bar{\tau}_n \oplus \mathbf{1}_p))^\dagger \\ &= \tau_n \cdot (1_n \cdot \tau_n \cdot h_1)^\dagger \\ &= \tau_n \cdot h_1^\dagger, \end{aligned} \tag{26}$$

by (17). Thus, substituting $\tau_n \cdot h_1^\dagger$ for $(g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p))^\dagger$ in (25),

$$\begin{aligned}u \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) &= g_2 \cdot \langle \tau_n \cdot h_1^\dagger, \bar{\tau}_n \oplus \mathbf{1}_p \rangle \\ &= g_2 \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) \cdot \langle h_1^\dagger, \mathbf{1}_{k-1+p} \rangle \\ &= \bar{\tau}_n \cdot h_2 \cdot \langle h_1^\dagger, \mathbf{1}_{k-1+p} \rangle \\ &= \bar{\tau}_n \cdot v,\end{aligned}$$

by (18). Thus,

$$\overleftarrow{1}_n \cdot u \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) = v,$$

so that

$$u^\dagger = \bar{\tau}_n \cdot v^\dagger, \tag{27}$$

by (24). Thus, using (26),

$$\begin{aligned}g_1^\dagger \cdot \langle u^\dagger, \mathbf{1}_p \rangle &= g_1^\dagger \cdot \langle \bar{\tau}_n \cdot v^\dagger, \mathbf{1}_p \rangle \\ &= g_1^\dagger \cdot (\bar{\tau}_n \oplus \mathbf{1}_p) \cdot \langle v^\dagger, \mathbf{1}_p \rangle \\ &= (g_1 \cdot (\mathbf{1}_n \oplus \bar{\tau}_n \oplus \mathbf{1}_p))^\dagger \cdot \langle v^\dagger, \mathbf{1}_p \rangle \\ &= \tau_n \cdot h_1^\dagger \cdot \langle v^\dagger, \mathbf{1}_p \rangle. \end{aligned} \tag{28}$$

Equation (16) now follows from (27), (28), (21), and (22). ∎

COROLLARY 10.8. *Suppose that $\mathscr{G}$ is some class of finite groups. Let Ax denote the set consisting of the Conway identities and the group identities $\mathbf{C}(\mathscr{G})$. If t and t'*

are terms with $Ax \models t = t'$, *then the vector form of* $t = t'$ *holds in all Conway theories satisfying* $\mathbf{C}(\mathscr{G})$.

Proof. Immediate from Theorem 5.1, Lemma 5.3, and Proposition 10.7. ∎

11. A FEW SIMPLE FACTS

In this section we assume that T is a preiteration theory which satisfies at least the permutation identity.

Suppose that (A, X) is an automaton and φ is a given function $Y \to X$, where Y is a finite nonempty set. Define the action of Y on A by

$$ay = a(y\varphi),$$

for all $a \in A$, $y \in Y$. Let (A, Y) denote the resulting automaton.

LEMMA 11.1. *If* $T \models \mathbf{C}(A, X)$ *then* $T \models \mathbf{C}(A, Y)$. *If* φ *is surjective and if* $T \models \mathbf{C}(A, Y)$, *then* $T \models \mathbf{C}(A, X)$.

Proof. Let $A = [n]$, $X = [m]$ and $Y = [k]$, say. Thus φ induces a base morphism $k \to m$ in T. Let $\rho_i: m \to n$ and $\rho_i': k \to n$, $i \in [n]$ denote the base morphisms associated with the automata (A, X) and (A, Y), respectively. Then

$$\rho_i' = \varphi \cdot \rho_i, \tag{29}$$

for all $i \in [n]$.

Let $f: 1 \to k + p$. By (29),

$$f_{(A, Y)} = (f \cdot (\varphi \oplus \mathbf{1}_p))_{(A, X)}.$$

Thus, if $T \models \mathbf{C}(A, X)$, then

$$\begin{aligned} f^\dagger_{(A, Y)} &= (f \cdot (\varphi \oplus \mathbf{1}_p))^\dagger_{(A, X)} \\ &= \tau_n \cdot (f \cdot (\varphi \oplus \mathbf{1}_p) \cdot (\tau_m \oplus \mathbf{1}_p))^\dagger \\ &= \tau_n \cdot (f \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger, \end{aligned}$$

proving $T \models \mathbf{C}(A, Y)$.

Suppose now that φ is surjective. Then there exists an injective base morphism $\alpha: m \to k$ with $\alpha \cdot \varphi = \mathbf{1}_m$. Let $f: 1 \to m + p$ in T. Then, by (29),

$$\begin{aligned} f_{(A, X)} &= (f \cdot (\alpha \cdot \varphi \oplus \mathbf{1}_p))_{(A, X)} \\ &= (f \cdot (\alpha \oplus \mathbf{1}_p))_{(A, Y)}. \end{aligned}$$

Thus, if $T \models \mathbf{C}(A, Y)$, then it follows as above that $T \models \mathbf{C}(A, X)$. ∎

LEMMA 11.2. *Suppose that* (A, X) *is a subautomaton of* (B, X). *If* T *satisfies the functorial implication for injective base morphisms and* $T \models \mathbf{C}(B, X)$, *then* $T \models \mathbf{C}(A, X)$.

Proof. Let $A=[n]$, $B=[m]$ and $X=[k]$, say. Let $\rho_i: k \to n$, $i \in [n]$ denote the base morphisms associated with (A, X), and let $\rho'_j: k \to m$, $j \in [m]$ denote the base morphisms associated with (B, X). Since (A, X) is a subautomaton of (B, X), we have $\rho'_i = \rho_i$, for all $i \in [n]$. Thus, if α denotes the base morphism corresponding to the inclusion of $[n]$ into $[m]$, we have

$$f_{(A, X)} \cdot (\alpha \oplus \mathbf{1}_p) = \alpha \cdot f_{(B, X)},$$

for all $f: 1 \to k+p$. Thus, if T satisfies the functorial implication for injective base morphisms and if $T \models \mathbf{C}(B, X)$, then

$$\begin{aligned} f^\dagger_{(A, X)} &= \alpha \cdot f^\dagger_{(B, X)} \\ &= \alpha \cdot \tau_m \cdot (f \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger \\ &= \tau_n \cdot (f \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger. \quad \blacksquare \end{aligned}$$

COROLLARY 11.3. *Suppose that S is a finite semigroup and S' is a subsemigroup of S. Suppose that T satisfies the functorial implication for base injections and that $T \models \mathbf{C}(S)$. Then $T \models \mathbf{C}(S')$.*

Proof. Since S and S' are semigroups, both (S, S) and (S', S'), equipped with the natural self action are transformation semigroups and hence automata. Let (S, S') denote the transformation semigroup obtained from (S, S) by restricting the action of S to S'. Then, by Lemma 11.1, $T \models \mathbf{C}(S, S')$, hence $T \models \mathbf{C}(S', S')$, by Lemma 11.2. $\blacksquare$

Suppose that (A, X) and (B, X) are given automata. The *disjoint sum* of (A, X) and (B, X) is the automaton $(C, X) = (C, X, \circ)$ defined on the disjoint union $C = A \uplus B$ equipped with the X-action

$$c \circ x = \begin{cases} ax & \text{if} \quad c = a \in A \\ bx & \text{if} \quad c = b \in B, \end{cases}$$

where ax and bx are taken in the automata (A, X) and (B, X), respectively.

LEMMA 11.4. *Suppose that the automaton (A, X) is the disjoint sum of the automata (A_1, X) and (A_2, X). Suppose that the identity (5) holds in T. If $T \models \mathbf{C}(A_i, X)$, for $i = 1, 2$, then $T \models \mathbf{C}(A, X)$.*

Proof. Suppose that $X=[k]$ and $A_i=[n_i]$, $i=1, 2$. We may represent A as the set $[n_1+n_2]$ such that (A_1, X) is the subatomaton determined by the set $[n_1]$. But then,

$$f_{(A, X)} = \langle f_{(A_1, X)} \cdot (\mathbf{1}_{n_1} \oplus 0_{n_2} \oplus \mathbf{1}_p),\ 0_{n_1} \oplus f_{(A_2, X)} \rangle.$$

Thus, using Eq. (5),

$$f^\dagger_{(A, X)} = \langle f^\dagger_{(A_1, X)}, f^\dagger_{(A_2, X)} \rangle.$$

The result follows. (Note that the converse of this lemma also holds, if (5) and $\mathbf{C}(A, X)$ hold in T, then $T \models \mathbf{C}(A_1, X)$ and $T \models \mathbf{C}(A_2, X)$.) ▮

12. CASCADE COMPOSITION

In this section, T denotes a preiteration theory satisfying at least the permutation and parameter identities.

Suppose that (A, X) and (B, Y) are finite automata and

$$\varphi: A \times X \to Y$$
$$(a, x) \mapsto {}^a x$$

is a given function. Recall that the cascade composition of (A, X) and (B, Y) with respect to φ is the automaton

$$(B, Y) \times_\varphi (A, X) = (B \times A, X),$$

equipped with the X-action

$$(b, a)x = (b\, {}^a x, ax),$$

for all $a \in A$, $b \in B$ and $x \in X$. In the next lemma we assume that $A = [n]$, $B = [m]$, $X = [k]$ and $Y = [r]$. Moreover, we represent $[m] \times [n]$ as the set $[mn]$ with $\langle i, j \rangle = \langle i, j \rangle_{m,n}$ corresponding to the ordered pair $(i, j) \in [m] \times [n]$.

Below we will write $\vec{\rho}$ to denote a base morphism in the theory Tn.

LEMMA 12.1. *Suppose that the vector form of* $\mathbf{C}(B, Y)$ *holds in* T. *Then for all* $f: n \to k + p$,

$$((\vec{\tau}_m \cdot f) \bullet (B \times A, X))^\dagger = \vec{\tau}_m \cdot (f \bullet (A, X))^\dagger. \tag{30}$$

Proof. Using the above notation, the base morphisms associated with $(B \times A, X)$ are the morphisms

$$\rho_{\langle i, j \rangle}: k \to mn, \qquad i \in [m], \quad j \in [n]$$
$$u \mapsto \langle i({}^j u), ju \rangle, \qquad u \in [k].$$

Let us introduce the notations

$$\kappa_i = \rho_i^{(B, Y)}: r \to m$$
$$\lambda_j = \rho_j^{(A, X)}: k \to n,$$

for all $i \in [m]$, $j \in [n]$. Then,

$$\rho_{\langle i, j \rangle} = \sigma_j \cdot \vec{\kappa}_i \tag{31}$$
$$\lambda_j = \sigma_j \cdot \vec{\tau}_r, \tag{32}$$

where $\sigma_j: k \to rn$ is the base morphism corresponding to the function

$$u \mapsto \langle {}^j u,\ ju \rangle_{r,n}, \qquad u \in [k].$$

Indeed, we have

$$\sigma_j \cdot \vec{\kappa}_i: u \mapsto \langle {}^j u,\ ju \rangle \mapsto \langle i({}^j u),\ ju \rangle$$
$$\sigma_j \cdot \vec{\tau}_r: u \mapsto \langle {}^j u,\ ju \rangle \mapsto ju.$$

Suppose that $f = \langle f_1, ..., f_n \rangle: n \to k + p$. Define

$$F = f \parallel (\sigma_1, ..., \sigma_n): n \to rn + p.$$

Then,

$$F_{(B,\ Y)} = (\vec{\tau}_m \cdot F) \parallel (\vec{\kappa}_1, ..., \vec{\kappa}_m): mn \to mn + p.$$

See Section 7. For each $\langle i, j \rangle \in [mn]$, $\langle i, j \rangle_{mn} \cdot F_{(B,\ Y)}$, the $\langle i, j \rangle$ th component of $F_{(B,\ Y)}$ is the same morphism as the $\langle i, j \rangle$ th component of $(\vec{\tau}_m \cdot f) \bullet (B \times A, X)$. Indeed,

$$\begin{aligned}
\langle i, j \rangle_{mn} \cdot F_{(B,\ Y)} &= j_n \cdot F \cdot (\vec{\kappa}_i \oplus \mathbf{1}_p) \\
&= f_j \cdot (\sigma_j \oplus \mathbf{1}_p) \cdot (\vec{\kappa}_i \oplus \mathbf{1}_p) \\
&= f_j \cdot (\rho_{\langle i, j \rangle} \oplus \mathbf{1}_p) \\
&= \langle i, j \rangle_{mn} \cdot ((\vec{\tau}_m \cdot f) \bullet (B \times A, X)),
\end{aligned}$$

by (31). Thus,

$$F_{(B,\ Y)} = ((\vec{\tau}_m \cdot f) \bullet (B \times A, X)). \tag{33}$$

Also,

$$F \cdot (\vec{\tau}_r \oplus \mathbf{1}_p) = f_{(A,\ X)}, \tag{34}$$

by Eq. (32). But since the vector form of $\mathbf{C}(B, Y)$ holds,

$$F^{\dagger}_{(B,\ Y)} = \vec{\tau}_m \cdot (F \cdot (\vec{\tau}_r \oplus \mathbf{1}_p))^{\dagger}. \tag{35}$$

Eq. (30) follows from (33), (34), and (35). ▮

COROLLARY 12.2. *Under the assumptions of Lemma* 12.1, *if T satisfies the vector form of* $\mathbf{C}(B, Y)$, *then* $T \models \mathbf{C}(B \times A, X)$ *iff* $T \models \mathbf{C}(A, X)$.

Proof. Suppose that $g: 1 \to k+p$ in T. Define $f = \tau_n \cdot g: n \to k+p$. Then,

$$\begin{aligned} g_{(B\times A, X)} &= (\tau_{mn} \cdot g) \bullet (B \times A, X) \\ &= (\vec{\tau}_m \cdot f) \bullet (B \times A, X) \end{aligned}$$

and

$$g_{(A, X)} = f \bullet (A, X).$$

Thus, by Lemma 12.1,

$$g^\dagger_{(B\times A, X)} = \tau_{mn} \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger \tag{36}$$

iff

$$g^\dagger_{(A, X)} = \tau_n \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger. \tag{37}$$

Indeed, if (36) holds, then, using Lemma 12.1,

$$\begin{aligned} g^\dagger_{(A, X)} &= (f \bullet (A, X))^\dagger \\ &= \vec{1}_m \cdot ((\vec{\tau}_m \cdot f) \bullet (B \times A, X))^\dagger \\ &= \vec{1}_m \cdot g^\dagger_{(B\times A, X)} \\ &= \vec{1}_m \cdot \tau_{mn} \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger \\ &= \tau_n \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger. \end{aligned}$$

And if (37) holds, then

$$\begin{aligned} g^\dagger_{(B\times A, X)} &= ((\vec{\tau}_m \cdot f) \bullet (B \times A, X))^\dagger \\ &= \vec{\tau}_m \cdot (f \bullet (A, X))^\dagger \\ &= \vec{\tau}_m \cdot g^\dagger_{(A, X)} \\ &= \vec{\tau}_m \cdot \tau_n \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger \\ &= \tau_{mn} \cdot (g \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger. \quad \blacksquare \end{aligned}$$

13. IDENTITIES ASSOCIATED WITH PERMUTATION AUTOMATA

In this section, T denotes a Conway theory.

Suppose that G is a finite group and H is a subgroup of G. Then G/H, the set of right cosets modulo H equipped with the natural right action of G is a permutation automaton.

PROPOSITION 13.1. *For each finite group G and each subgroup H of G, $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(G/H, G)$ and $T \models \mathbf{C}(H)$.*

Proof. Recall that both (G, G) and (H, H), equipped with the natural self action are transformation groups. It is known that (G, G) is isomorphic to a cascade composition

$$(H, H) \times_{\varphi} (G/H, G).$$

See, e.g., [8]. Thus, by Corollary 12.2 and Proposition 10.7, if $T \models \mathbf{C}(H)$ then $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(G/H, G)$. But if $T \models \mathbf{C}(G)$ then $T \models \mathbf{C}(H)$, since H is a subgroup of G. See Corollary 11.3. ∎

COROLLARY 13.2. *Suppose that G is a finite group and N is a normal subgroup of G. Then $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(N)$ and $T \models \mathbf{C}(G/N)$.*

Proof. By Proposition 13.1, $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(N)$ and $T \models \mathbf{C}(G/N, G)$. Let $\varphi: G \to G/N$ be the natural homomorphism. Since $Ng_1Ng_2 = Ng_1g_2$, for all $g_1, g_2 \in G$, and since φ is surjective, it follows from Lemma 11.1 that $T \models \mathbf{C}(G/N, G)$ iff $T \models \mathbf{C}(G/N)$. ∎

A transformation group (A, G) is *strongly connected* (or transitive), if for any $a, b \in A$ there is a $g \in G$ with $ag = b$. For any transformation group (A, G) and $a \in A$ we define $H_a = \{h \in G: ah = a\}$. Note that H_a is a subgroup of G.

COROLLARY 13.3. *Suppose that (A, G) is a strongly connected transformation group. Let $a_0 \in A$. Then $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(H_{a_0})$ and $T \models \mathbf{C}(A, G)$.*

Proof. (A, G) is isomorphic to the transformation group $(G/H_{a_0}, G)$. ∎

COROLLARY 13.4. *Suppose that (A, G) is a transformation group. Then $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(A, G)$ and $T \models \mathbf{C}(H_a)$, for each $a \in A$.*

Proof. Each transformation group (A, G) is the disjoint sum of its strongly connected components. Hence the result follows from Corollary 13.3 and Lemma 11.4. ∎

PROPOSITION 13.5. *Suppose that G is a finite group. Let $\mathcal{G}$ denote the class of simple groups H with $H \mid G$. Then $T \models \mathbf{C}(G)$ iff $T \models \mathbf{C}(\mathcal{G})$.*

Proof. We prove this fact by induction on the order n of G. The basis case that $n = 1$ is obvious. Let $n > 1$ and assume that $T \models \mathbf{C}(G)$. If $H \in \mathcal{G}$ then there is a subgroup G' of G such that H is a homomorphic image of G'. Hence there is a normal subgroup N of G' such that the groups H and G'/N are isomorphic. Since $T \models \mathbf{C}(G)$ and since G' and N are subgroups of G, $T \models \mathbf{C}(G')$ and $T \models \mathbf{C}(N)$. Thus, by Corollary 13.2, $T \models \mathbf{C}(H)$.

Suppose now that $T \models \mathbf{C}(\mathcal{G})$. If G is trivial then so is the identity $\mathbf{C}(G)$. If G is simple, then $G \in \mathcal{G}$ and $T \models \mathbf{C}(G)$. If G is nontrivial and not simple, then it has a nontrivial normal subgroup N. Each simple group divisor of N or G/N divides G and is thus in $\mathcal{G}$. Thus, by the induction assumption, $T \models \mathbf{C}(N)$ and $T \models \mathbf{C}(G/N)$. But then $T \models \mathbf{C}(G)$. ∎

COROLLARY 13.6. *Let (A, X) be a permutation automaton and $G = G(A, X)$. Let $\mathcal{G}$ denote the class of simple groups H with $H \mid G$. It $T \models \mathbf{C}(\mathcal{G})$ then $T \models C(A, X)$.*

Proof. If $T \models \mathbf{C}(\mathscr{G})$ then $T \models \mathbf{C}(G)$, by Proposition 13.5. The elements of the group G are permutations $A \to A$. Thus (A, G), equipped with the action $ag = g(a)$, all $a \in A$ and $g \in G$, is a transformation group. Since $T \models \mathbf{C}(G)$, we have $T \models \mathbf{C}(A, G)$, by Corollary 13.4. But then, $T \models \mathbf{C}(A, X)$, by Lemma 11.1. ▮

14. IDENTITIES ASSOCIATED WITH PERMUTATION-RESET AUTOMATA

Suppose that (A, X) and (A, Y) are finite automata. We say that (A, Y) is an *extension* of (A, X) if $X \subseteq Y$ and each letter $x \in X$ induces equal functions $A \to A$ in (A, X) and (A, Y). If in addition each letter $y \in Y - X$ is a reset letter of (A, Y), then (A, Y) is a *reset extension* of (A, Y).

Assume that T is a Conway theory.

LEMMA 14.1 *If (A, Y) is a reset extension of (A, X), then $T \models \mathbf{C}(A, Y)$ iff $T \models \mathbf{C}(A, X)$.*

Proof. By Lemma 11.1, if $T \models \mathbf{C}(A, Y)$ then $T \models \mathbf{C}(A, X)$. Moreover, it is sufficient to prove the converse implication for the case that $Y = X \uplus A$ (disjoint union), and each $a \in A$ induces the constant function $A \to A$ with value a. Thus, if $X = [k]$, $A = [n]$ and $Y = [k+n]$, say, and if $f: 1 \to k+n+p$ in T, then

$$f_{(A, Y)} = f_{(A, X)} \cdot (\langle \mathbf{1}_n, \mathbf{1}_n \rangle \oplus \mathbf{1}_p),$$

so that

$$f^{\dagger}_{(A, Y)} = f^{\dagger\dagger}_{(A, X)},$$

by the double dagger identity. Thus, if $T \models \mathbf{C}(A, X)$, then

$$\begin{aligned} f^{\dagger}_{(A, Y)} &= (f^{\dagger}_{(A, X)})^{\dagger} \\ &= (\tau_n \cdot (f \cdot (\tau_k \oplus \mathbf{1}_{n+p}))^{\dagger})^{\dagger}. \end{aligned}$$

Let g denote the morphism $(f \cdot (\tau_k \oplus \mathbf{1}_{n+p}))^{\dagger}$. Then,

$$(\tau_n \cdot g)^{\dagger} = \tau_n \cdot (g \cdot (\tau_n \oplus \mathbf{1}_p))^{\dagger},$$

by the composition identity. Thus,

$$\begin{aligned} f^{\dagger}_{(A, Y)} &= \tau_n \cdot (g \cdot (\tau_n \oplus \mathbf{1}_p))^{\dagger} \\ &= \tau_n \cdot ((f \cdot (\tau_k \oplus \mathbf{1}_{n+p}))^{\dagger} \cdot (\tau_n \oplus \mathbf{1}_p))^{\dagger} \\ &= \tau_n \cdot (f \cdot (\tau_k \oplus \tau_n \oplus \mathbf{1}_p))^{\dagger\dagger} \\ &= \tau_n \cdot (f \cdot (\tau_{k+n} \oplus \mathbf{1}_p))^{\dagger}, \end{aligned}$$

by the parameter and double dagger identities. ▮

The above proof also works in the case that $k = 0$. Thus we have:

COROLLARY 14.2. *Each identity associated with any reset automaton holds in T. Moreover, the vector form of any such identity holds in T.*

COROLLARY 14.3. *Suppose that (A, X) is a permutation-reset automaton. Let $\mathscr{G}$ denote the simple group divisors of $S(A, X)$. If $T \models \mathbf{C}(\mathscr{G})$ then $T \models \mathbf{C}(A, X)$, moreover, the vector form of $\mathbf{C}(A, X)$ also holds in T.*

Proof. The case that (A, X) is a reset automaton is handled by the previous corollary. Suppose that (A, X) is a reset extension of a permutation automaton (A, Y). Then $\mathscr{G}$ is the class of all simple group divisors of $G(A, Y)$. Thus, if $T \models \mathbf{C}(\mathscr{G})$, then $T \models \mathbf{C}(A, Y)$ and $T \models \mathbf{C}(A, X)$, by Lemma 14.1 and Corollary 13.6. Further, the vector form of $\mathbf{C}(A, X)$ holds in T, by Corollary 10.8. ∎

COROLLARY 14.4. *The identity $\mathbf{C}(\mathbf{U})$ associated with the two-state identity-reset automaton holds in any Conway theory.*

15. PERMUTATION-RESET HOMOMORPHISMS

LEMMA 15.1. *Suppose that (A, X) and (B, X) are finite automata and τ is a surjective elementary homomorphism $(A, X) \to (B, X)$. Then, for any Conway theory T, $T \models \mathbf{C}(A, X)$ iff $T \models \mathbf{C}(B, X)$.*

Proof. Since each elementary homomorphism is the composite of a sequence of 1-elementary morphisms, we may assume that τ is 1-elementary. Further, we may assume without loss of generality that $A = [n+2]$, $B = [n+1]$ and $X = [k]$, moreover that the morphism $n+2 \to n+1$ corresponding to τ is the base morphism $\tau_2 \oplus \mathbf{1}_n$, and that the integer 1 is not in the set AX. It follows that if $\rho_1, ..., \rho_{n+1}$ denote the base morphisms $k \to n+1$ associated with (B, X), then the base morphisms associated with (A, X) are $\rho'_1 = 0_1 \oplus \rho_1$, $\rho'_2 = 0_1 \oplus \rho_1$, ..., $\rho'_{n+2} = 0_1 \oplus \rho_{n+1}$. Thus, if $f: 1 \to k+p$, then there exist morphisms $g: 1 \to n+1+p$ and $h: n \to n+1+p$ with

$$f_{(A, X)} = \langle 0_1 \oplus g, 0_1 \oplus g, 0_1 \oplus h \rangle$$

$$f_{(B, Y)} = \langle g, h \rangle.$$

By the left zero identity, $(0_1 \oplus g)^\dagger = g$. Also

$$(0_1 \oplus g) \cdot \langle g, \mathbf{1}_{n+1+p} \rangle = g.$$

Thus, by the pairing and fixed point identities,

$$\begin{aligned} \langle 0_1 \oplus g, 0_1 \oplus g \rangle^\dagger &= \langle g \cdot \langle g^\dagger, \mathbf{1}_{n+p} \rangle, g^\dagger \rangle \\ &= \langle g^\dagger, g^\dagger \rangle. \end{aligned}$$

Define

$$\begin{aligned}\bar{h} &= h \cdot \langle g^\dagger, \mathbf{1}_{n+p} \rangle \\ &= (0_1 \oplus h) \cdot \langle g^\dagger, g^\dagger, \mathbf{1}_{n+p} \rangle.\end{aligned}$$

Then,

$$\begin{aligned}f^\dagger_{(A,X)} &= \langle \langle g^\dagger, g^\dagger \rangle \cdot \langle \bar{h}^\dagger, \mathbf{1}_p \rangle, \bar{h}^\dagger \rangle \\ &= \tau \cdot \langle g^\dagger \cdot \langle \bar{h}^\dagger, \mathbf{1}_p \rangle, \bar{h}^\dagger \rangle \\ &= \tau \cdot f^\dagger_{(B,Y)},\end{aligned}$$

again by the pairing identity. It follows that

$$f^\dagger_{(A,X)} = \tau_{n+2} \cdot (f \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger$$

iff

$$f^\dagger_{(B,Y)} = \tau_{n+1} \cdot (f \cdot (\tau_k \oplus \mathbf{1}_p))^\dagger. \quad \blacksquare$$

PROPOSITION 15.2. *Suppose that $\mathscr{G}$ is a class of simple groups closed under division and T is a Conway theory with $T \models \mathbf{C}(\mathscr{G})$. Let (A, X) and (B, X) be finite automata and suppose that h is a surjective permutation-reset $\mathscr{G}$-homomorphism $(A, X) \to (B, X)$. Then $T \models \mathbf{C}(A, X)$ iff $T \models \mathbf{C}(B, X)$.*

Proof. By Lemma 9.6, there exists a permutation-reset automaton (C, Y) and a cascade composition $(C \times B, X) = (C, Y) \times_\varphi (B, X)$ such that the following conditions hold:

- (A, X) is isomorphic to a subautomaton of $(C \times B, X)$.
- There is a surjective elementary homomorphism $(C \times B, X) \to (A, X)$.
- If G is a simple group with $G \mid S(C, Y)$, then $G \in \mathscr{G}$.

By Corollary 14.3, the vector form of $\mathbf{C}(C, Y)$ holds in T. Thus, by Corollary 12.2, $T \models \mathbf{C}(B, X)$ iff $T \models \mathbf{C}(C \times B, X)$. But (A, X) is a subautomaton of $(C \times B, X)$, so if $T \models \mathbf{C}(B, X)$ then $T \models \mathbf{C}(A, X)$. See Lemma 11.2. Suppose now that $T \models \mathbf{C}(A, X)$. Then, since (A, X) is a homomorphic image of $(C \times B, X)$ under an elementary homomorphism, we have $T \models \mathbf{C}(B, X)$, by Lemma 15.1. $\blacksquare$

COROLLARY 15.3. *Suppose that the automaton (B, X) is a quotient of (A, X) under a $\mathscr{G}$-homomorphism, for a class $\mathscr{G}$ of simple groups closed under division. Then in any Conway theory T satisfying the group identities $\mathbf{C}(\mathscr{G})$, we have $T \models \mathbf{C}(A, X)$ iff $T \models \mathbf{C}(B, X)$.*

Proof. Immediate from Proposition 15.2 and the fact, proved in [15], that if (B, X) is a quotient of (A, X) under a $\mathscr{G}$-homomorphism, then there is a sequence

$$(A, X) = (A_0, X), (A_1, X), ..., (A_m, X) = (B, X)$$

such that for each $i \in [m]$, either (A_i, X) is a quotient of the automaton (A_{i-1}, X) under a permutation-reset $\mathscr{G}$-homomorphism, or there is a surjective permutation-reset $\mathscr{G}$-homomorphism $(A_i, X) \to (A_{i-1}, X)$. ▮

16. PROOF OF THE MAIN RESULTS

In this section we finally complete the proof of Theorem 8.1, restated here as Corollary 16.7.

THEOREM 16.1. *Suppose that T is a Conway theory and (A, X) is a finite automaton. Suppose that $T \models \mathbf{C}(G)$ for all simple groups G with $G \mid S(A, X)$. Then $T \models \mathbf{C}(A, X)$. Moreover, T satisfies the vector form of the identity $\mathbf{C}(A, X)$.*

Proof. Let $\mathscr{G}$ denote the class of simple groups G with $G \mid S(A, X)$. By Theorem 9.5, there is a sequence of automata (A_i, X), $i \in [k]$ such that (A_1, X) is trivial, (A_k, X) is (A, X), and for each $i \in [k-1]$ either (A_i, X) is a homomorphic image of (A_{i+1}, X) under a surjective permutation-reset $\mathscr{G}$-homomorphism, or conversely. By Corollary 14.3, $T \models \mathbf{C}(B, Y)$ for each permutation-reset automaton (B, Y) such that each simple group divisor of $S(B, Y)$ is in $\mathscr{G}$. Thus, by Proposition 15.2, $T \models \mathbf{C}(A_i, X)$ iff $T \models \mathbf{C}(A_{i+1}, X)$, for each $i \in [k-1]$. But $T \models \mathbf{C}(A_1, X)$, since (A_1, X) is trivial. The fact that T satisfies the vector form of $\mathbf{C}(A, X)$ follows from Corollary 10.8. ▮

Remark 16.2. In the above argument, we used part 2 of Theorem 9.5. There is an alternative argument based on part 1, and Lemma 11.2, Proposition 15.2, and Corollary 12.2. Note that $\mathbf{C}(\mathbf{U})$ holds in any Conway theory, by Corollary 14.4.

COROLLARY 16.3. *The vector form of any identity associated with an aperiodic automaton holds in all Conway theories.*

For a full account of the identities that hold in Conway theories see [1].

COROLLARY 16.4. *Suppose that S is a semigroup. Let $\mathscr{G}$ denote the class of simple group divisors of S. If T is a Conway theory then $T \models \mathbf{C}(S)$ iff $T \models \mathbf{C}(\mathscr{G})$. Moreover, in this case, T satisfies the vector form of the identity $\mathbf{C}(S)$.*

Proof. If S does not have a unit element, let S^1 denote the monoid obtained from S by adding a unit, and let S^1 be S if S is a monoid. Then (S^1, S), equipped with the natural right action is a transformation semigroup and hence an automaton. Moreover, the semigroup of (S^1, S) is isomorphic to S. Thus, if $T \models \mathbf{C}(\mathscr{G})$, then $T \models \mathbf{C}(S^1, S)$, by Theorem 16.1. But then, since the transformation semigroup (S, S) equipped with the natural self action is a subautomaton of (S^1, S), we have $T \models \mathbf{C}(S)$, by Lemma 11.2. Moreover, by our previous results, the vector form of $\mathbf{C}(S)$ also holds in T.

Suppose now that $T \models \mathbf{C}(S)$. If G is a group in $\mathscr{G}$, then G is a homomorphic image of a subgroup H of S. But then, $T \models \mathbf{C}(H)$, by Corollary 11.3, and $T \models \mathbf{C}(G)$, by Proposition 13.5. ▮

COROLLARY 16.5. *Let (A, X) be an automaton and $\mathscr{S}$ a class of finite semigroups such that each simple group divisor of $S(A, X)$ divides one of the semigroups in $\mathscr{S}$. Then, if T is a Conway theory with $T \models \mathbf{C}(\mathscr{S})$, then T satisfies the vector form of $\mathbf{C}(A, X)$.*

Proof. Immediate from Theorem 16.1 and Corollary 16.4. ▮

The following proposition can be extracted from [7], see also [26].

PROPOSITION 16.6. *Suppose that $\mathscr{G}$ is a class of simple groups closed under division. If G is a simple group not in $\mathscr{G}$, or if G is a group which has a simple group divisor not included in $\mathscr{G}$, then there is a Conway theory T with $T \models \mathbf{C}(\mathscr{G})$ but $T \not\models \mathbf{C}(G)$.*

In fact, it is shown in [7] that there exists a Conway semiring [4, 7, 22] S such that S and thus the matrix theory Mat_S over S satisfies the *-forms of the identities in $\mathbf{C}(\mathscr{G})$ but does not satisfy the *-form of the identity $\mathbf{C}(G)$. But since S is a Conway semiring, $T = Mat_S$ is a Conway theory.

COROLLARY 16.7. *Let $\mathscr{S}$ be a class of semigroups. Then the Conway identities and the semigroup identities $\mathbf{C}(\mathscr{S})$ form a complete axiomatization of iteration theories iff for each finite simple group G there is a semigroup $S \in \mathscr{S}$ such that $G \mid S$.*

Proof. First recall that each semigroup identity holds in all iteration theories. Suppose that any simple group divides one of the semigroups in $\mathscr{S}$. If T is a Conway theory satisfying $\mathbf{C}(\mathscr{S})$, then, by Corollary 16.5, T satisfies the vector forms of all of the identities associated by finite automata. Hence T is an iteration theory, by Lemma 7.3.

For the converse direction, suppose that the Conway identities and the equations $\mathbf{C}(\mathscr{S})$ give a complete axiomatization of iteration theories. Let $\mathscr{G}$ denote the simple group divisors of the semigroups in $\mathscr{S}$. By Corollary 16.4, if T is any Conway theory, $T \models \mathbf{C}(\mathscr{S})$ iff $T \models \mathbf{C}(\mathscr{G})$. Thus, the Conway identities and the group identities $\mathbf{C}(\mathscr{G})$ are also complete. But then, $\mathscr{G}$ is the class of all finite simple groups, by Proposition 16.6. ▮

COROLLARY 16.8. *Suppose that $\mathscr{S}$ and $\mathscr{S}'$ are two classes of finite semigroups. Let $\mathbf{V}(\mathscr{S})$ denote the variety of Conway theories T such that $T \models \mathbf{C}(\mathscr{S})$, and define $\mathbf{V}(\mathscr{S}')$ in the same way. Then $\mathbf{V}(\mathscr{S}) \subseteq \mathbf{V}(\mathscr{S}')$ iff each simple group divisor of any semigroup in $\mathscr{S}'$ divides one of the semigroups in $\mathscr{S}$.*

17. A CONJECTURE AND ITS CONSEQUENCES

Suppose that G is a finite group and X is a nonempty set of generators of G. Then (G, X), equipped with the natural action, is a permutation automaton and thus has the associated identity $\mathbf{C}(G, X)$.

Suppose the Conway identities and the identity $\mathbf{C}(G, X)$ imply the group identity $\mathbf{C}(G)$. Then, since under the Conway identities each group identity implies its own vector form, it follows by Lemma 11.1 that under the Conway identities, the identity $\mathbf{C}(G, X)$ also implies its vector form. The converse direction is formalized by following result:

THEOREM 17.1. *Suppose that G is a finite group and X is a set of generators of G. If T is a Conway theory satisfying the vector form of the identity $\mathbf{C}(G, X)$, then the group identity $\mathbf{C}(G)$ holds in T.*

A proof of Theorem 17.1 may be found in [16]. The argument in [16] is separated into two parts. The case that G is a cyclic group uses quasi-direct products of commutative permutation automata, and the general case a construction from [19] involving cascade compositions of an automaton with counters and definite automata. It is shown that if G is a cyclic group of order m, then under the Conway identities, the group identity $\mathbf{C}(G)$ is equivalent to the mth *power identity*

$$(f^m)^\dagger = f^\dagger, \qquad f: n \to n+p.$$

The *powers* $f^k: n \to n+p$ of a morphism $f: n \to n+p$ are defined by induction

$$f^0 = \mathbf{1}_n \oplus 0_p$$
$$f^{k+1} = f \cdot \langle f^k, 0_n \oplus \mathbf{1}_p \rangle.$$

By Theorem 17.1, the following two conjectures are equivalent.

Conjecture 17.1. In Conway theories, each identity $\mathbf{C}(G, X)$, associated with a finite group G and a nonempty set X of generators of G, implies its vector form.

Conjecture 17.2. In Conway theories, each identity $\mathbf{C}(G, X)$, associated with a finite group G and a non-empty set X of generators of G, implies the group identity $\mathbf{C}(G)$.

By Theorem 8.1, if any of the above conjectures holds, then so does the following:

Conjecture 17.3. Suppose that (G_i, X_i), $i \in I$ is a given collection of group–generating set pairs. Then the Conway identities and the identities $\mathbf{C}(G_i, X_i)$, $i \in I$ form a complete axiomatization of iteration theories iff each finite (simple) group is the divisor of a group G_{i_0}, for some $i_0 \in I$.

The fact that this condition is necessary for completeness is known from Theorem 8.1.

For each $n \geqslant 1$, let S_n denote the symmetric group of degree n represented as the group of all permutations $[n] \to [n]$. When $n \geqslant 3$, S_n has a 2-element generating set $X = \{t_n, c_n\}$, where t_n is the transposition (12) and c_n is the cyclic permutation $c_n = (12 \ldots n)$. Moreover, S_2 is isomorphic to the cyclic group of order 2. By Theorem 8.1 we have:

PROPOSITION 17.2. *If Conjecture* 17.1 *or Conjecture* 17.3 *holds, then the Conway identities and the equations $\mathbf{C}(S_n, X_n)$, $n \geqslant 3$ give a complete axiomatization of iteration theories.*

The rest of this section is devoted to simplifying of the identities $\mathbf{C}(S_n, X_n)$. Given the integer $n \geqslant 3$, let H denote the subgroup of S_n determined by the permutations

that fix the integer 1. Then for all $g, g' \in S_n$, $g' \in Hg$ iff $1g = 1g'$. It follows that the transformation groups $(S_n/H, S_n)$ and $([n], S_n)$, both equipped with the natural action, are isomorphic. Moreover, H is isomorphic to S_{n-1}. Since the transformation group (S_n, S_n) is isomorphic to a cascade composition of (H, H) and $(S_n/H, S_n)$, we have:

LEMMA 17.3. *There exists a cascade composition of* (S_{n-1}, S_{n-1}) *and* $([n], X_n)$ *which is isomorphic to* (S_n, X_n).

COROLLARY 17.4. *Suppose that* T *is a Conway theory satisfying the identities* $\mathbf{C}([n], X_n)$ *and* $\mathbf{C}(S_{n-1})$. *Then* $\mathbf{C}(S_n, X_n)$ *holds in* T.

COROLLARY 17.5. *If Conjecture* 17.1 *or Conjecture* 17.3 *is true, then the Conway identities and the equations* $\mathbf{C}([n], X_n)$, $n \geqslant 3$ *give a complete axiomatization of iteration theories.*

Proof. By the obvious induction argument noting that the identity $\mathbf{C}(S_2)$ holds in all Conway theories satisfying any one of the identities $\mathbf{C}([n], X_n)$, $n \geqslant 3$. (Use the fact that $([2], \{t_n\})$ is a subautomaton of $([n], \{t_n\})$.) ∎

Let us now define, for each $n \geqslant 3$, the identity $\mathbf{S}_n$:

$$(f \cdot (\tau_2 \oplus \mathbf{1}_p) \cdot \langle f \cdot \langle \mathbf{1}_1 \oplus 0_p, (f^\dagger)^{n-2}, 0_1 \oplus \mathbf{1}_p \rangle, 0_1 \oplus \mathbf{1}_p \rangle)^\dagger$$
$$= (f \cdot (\tau_2 \oplus \mathbf{1}_p))^\dagger, \qquad f\colon 1 \to 2 + p.$$

LEMMA 17.6. *For each* $n \geqslant 3$, *and for any Conway theory* T,

$$T \models \mathbf{S}_n \Leftrightarrow T \models \mathbf{C}([n], X_n).$$

From Lemma 17.6 and Corollary 17.5 we immediately have:

THEOREM 17.7. *If Conjecture* 17.1 *or Conjecture* 17.3 *is true, then the Conway identities and the equations* $\mathbf{S}_n$, *for* $n \geqslant 3$, *form a complete axiomatization of iteration theories.*

Proof of Lemma 17.6. Let $f\colon 1 \to 2 + p$ is Conway theory, and let g denote the morphism on the right-hand side of the equation defining $\mathbf{S}_n$. Note that

$$f_{([n], X_n)} = \langle 0_1 \oplus f \cdot (\tau_2 \oplus 0_{n-2} \oplus \mathbf{1}_p), f \cdot (\mathbf{1}_1 \oplus 0_1 \oplus \mathbf{1}_1 \oplus 0_{n-3} \oplus \mathbf{1}_p),$$
$$f \cdot (\langle 3_n, 4_n \rangle \oplus \mathbf{1}_p), \ldots, f \cdot (\langle (n-1)_n, n_n \rangle \oplus \mathbf{1}_p), f \cdot (\langle n_n, 1_n \rangle \oplus \mathbf{1}_p) \rangle.$$

We will show that

$$f^\dagger_{([n], X_n)} = \langle g, f \cdot \langle g, (f^\dagger)^{n-2} \cdot \langle g, \mathbf{1}_p \rangle, \mathbf{1}_p \rangle, (f^\dagger)^{n-2} \cdot \langle g, \mathbf{1}_p \rangle, \ldots, f^\dagger \cdot \langle g, \mathbf{1}_p \rangle \rangle. \tag{38}$$

Indeed, by using only the Conway identities, one derives

$$f^{\dagger}_{([n],\, X_n)} = \langle 0_1 \oplus f\cdot(\tau_2 \oplus 0_{n-2} \oplus \mathbf{1}_p), f\cdot(\mathbf{1}_1 \oplus 0_1 \oplus \mathbf{1}_1 \oplus 0_{n-3} \oplus \mathbf{1}_p),$$
$$f^{\dagger}\cdot(4_n \oplus \mathbf{1}_p), \ldots, f^{\dagger}\cdot((n-1)_n \oplus \mathbf{1}_p), f^{\dagger}\cdot(1_n \oplus \mathbf{1}_p)\rangle^{\dagger}.$$

Thus, again by the Conway identities,

$$\begin{aligned} f^{\dagger}_{([n],\, X_n)} &= \langle 0_1 \oplus f\cdot(\tau_2 \oplus 0_{n-2} \oplus \mathbf{1}_p), f\cdot(\mathbf{1}_1 \oplus 0_1 \oplus \mathbf{1}_1 \oplus 0_{n-3} \oplus \mathbf{1}_p), \\ &\quad (f^{\dagger})^{n-2}\cdot(1_n \oplus \mathbf{1}_p), \ldots, f^{\dagger}\cdot(1_n \oplus \mathbf{1}_p)\rangle^{\dagger} \\ &= \langle g, f\cdot\langle g, (f^{\dagger})^{n-2}\cdot\langle g, \mathbf{1}_p\rangle, \mathbf{1}_p\rangle, (f^{\dagger})^{n-2}\cdot\langle g, \mathbf{1}_p\rangle, \ldots, f^{\dagger}\cdot\langle g, \mathbf{1}_p\rangle\rangle. \end{aligned}$$

Thus, if $\mathbf{S}_n$ holds in T, then

$$1_n \cdot f^{\dagger}_{([n],\, X_n)} = (f\cdot(\tau_2 \oplus \mathbf{1}_p))^{\dagger} = f^{\dagger\dagger}.$$

But then,

$$\begin{aligned} f^{\dagger}\cdot\langle g, \mathbf{1}_p\rangle &= f^{\dagger}\cdot\langle f^{\dagger\dagger}, \mathbf{1}_p\rangle \\ &= f^{\dagger\dagger} \end{aligned}$$

and by induction,

$$(f^{\dagger})^{i}\cdot\langle g, \mathbf{1}_p\rangle = f^{\dagger\dagger},$$

for all $i \geqslant 1$. Thus, also

$$\begin{aligned} f\cdot\langle g, (f^{\dagger})^{n-2}\cdot\langle g, \mathbf{1}_p\rangle, \mathbf{1}_p\rangle &= f\cdot\langle f^{\dagger\dagger}, f^{\dagger\dagger}, \mathbf{1}_p\rangle \\ &= f\cdot(\tau_2 \oplus \mathbf{1}_p)\cdot\langle (f\cdot(\tau_2 \oplus \mathbf{1}_p))^{\dagger}, \mathbf{1}_p\rangle \\ &= (f\cdot(\tau_2 \oplus \mathbf{1}_p))^{\dagger} \\ &= f^{\dagger\dagger}. \end{aligned}$$

Thus, if $T \models \mathbf{S}_n$, then, by (38),

$$f^{\dagger}_{([n],\, X_n)} = \tau_n \cdot (f\cdot(\tau_2 \oplus \mathbf{1}_p))^{\dagger} = f^{\dagger\dagger},$$

proving $T \models \mathbf{C}([n], X_n)$. The converse implication is now obvious. ∎

We end this section with the following

Conjecture 17.4. The Conway identities and the equations $\mathbf{S}_n$, $n \geqslant 3$ form a complete axiomatization of iteration theories.

18. A SIMPLE μ-LANGUAGE

In this section, we briefly outline how the completeness of the group identities for iteration theories may be expressed in a simple algebraic language.

Suppose that $\Sigma = \bigcup_n \Sigma_n$ is a signature containing a denumerable set Σ_n of n-ary function symbols for each $n \geqslant 0$. Suppose that X is a countably infinite set disjoint from Σ. The set of *μ-terms*, denoted T_Σ, is defined to be the smallest set of expressions satisfying the following:

- $\Sigma_0 \cup X \subseteq T_\Sigma$,
- $\sigma \in \Sigma_n,\ t_1, ..., t_n \in T_\Sigma,\ n > 0 \Rightarrow \sigma(t_1, ..., t_n) \in T_\Sigma$,
- $t \in T_\Sigma,\ x \in X \Rightarrow \mu x.t \in T_\Sigma$.

The variable x is bound in $\mu x.t$. We identify μ-terms which differ only in their bound variables (α-conversion). Hence, when needed, we may tacitly assume that a variable occurring bound in a μ-term is different from any other variable under consideration.

The set of free variables of the term t is defined as usual. We will sometimes write $t \equiv t[x_1, ..., x_n]$ to indicate that the pairwise distinct variables x_i, $i \in [n] = \{1, ..., n\}$, *may* have a free occurrence, but *no bound* occurrence, in t. (Thus, $\equiv$ denotes syntactic equality. Note that writing $t[x_1, ..., x_n]$ we do not mean that all free variables of t appear on the list $x_1, ..., x_n$.) Further, if $t \equiv t[x_1, ..., x_n]$ and t_i, $i \in [n]$ are μ-terms, we let

$$t[t_1/x_1, ..., t_n/x_n]$$

denote the term obtained by substituting the term t_i for the variable x_i in t, for each $i \in [n]$. By our convention about the bound variables, no free variable may become bound as the result of the substitution. Thus, if $t \equiv \sigma(x_1, ..., x_n)$, the term $\sigma(t_1, ..., t_n)$ is $t[t_1/x_1, ..., t_n/x_n]$.

Note the following fact about substitution. Suppose that $t \equiv t[x, y_1, ..., y_m] \in T_\Sigma$ and $t'_1, ..., t'_m \in T_\Sigma$. Then, if x does not occur free in any t'_j,

$$(\mu x.t)[t'_1/y_1, ..., t'_m/y_m] \equiv \mu x.(t[t'_1/y_1, ..., t'_m/y_m]).$$

Suppose that

$$t_i \equiv t_i[x_1, ..., x_n], \qquad i \in [n], \quad n \geqslant 1$$

are μ-terms. We define the term

$$\mu[x_1, ..., x_n].[t_1, ..., t_n]$$

by induction on n. When $n = 1$, this term is $\mu x.t_1[x_1]$. Assuming $n > 1$, we define:

$$\mu[x_1, ..., x_n].[t_1, ..., t_n] \equiv \mu[x_1, ..., x_{n-1}].[t_1[\mu x_n.t_n/x_n], ..., t_{n-1}[\mu x_n.t_n/x_n]].$$

Note that this definition is based on the right pairing identity.

μ-terms are commonly interpreted in continuous or regular Σ-algebras [21, 23, 37], or iterative Σ-algebras [33, 38], or more generally in iteration algebras [4]. The completeness of the Conway identities and the group axioms for iteration theories may be translated into a sound and complete deductive system for proving that two terms denote equal functions under all such interpretations. In addition to the usual axioms and rules for substitution and for manipulating equations, this formal system has the following axioms:

- Double Iteration Axiom

$$\mu z.t[z/x, z/y] = \mu x.\mu y.t,$$

for all terms $t \equiv t[x, y] \in T_\Sigma$, where z is a new variable.

- Composition Axiom

$$\mu x.t[t'/x] = t[\mu x.t'[t/x]/x],$$

for all $t[x], t'[x] \in T_\Sigma$.

- Group Axioms

For each finite group G on a set $[n]$, and for each μ-term $t \equiv t[x_1, ..., x_n]$,

$$\mu[x_1, ..., x_n].[t[x_{11}/x_1, ..., x_{1n}/x_n], ..., t[x_{n1}/x_1, ..., x_{nn}/x_n]] = \mu y.t[y/x_1, ..., y/x_n],$$

where y is a new variable and for any $i, j \in [n]$, ij stands for the product of i and j in the group G.

By (39), we do not need an axiom corresponding to the scalar parameter identity, this axiom is implicit in the syntax.

19. A WEAK FORM OF THE FIXED POINT INDUCTION

In this section, consider ordered preiteration theories, i.e., preiteration theories T equipped with a partial order such that the theory operations are monotonic. When T also satisfies the Conway identities, we call T an ordered Conway theory.

Suppose that T is an ordered preiteration theory. We say that T satisfies the *weak Park induction principle* cf. [34, 39], if

$$f \cdot \langle g, \mathbf{1}_p \rangle = g \Rightarrow f^\dagger \leqslant g,$$

for all $f: n \to n + p$ and $g: n \to p$.

THEOREM 19.1. *Any ordered Conway theory satisfying the weak Park induction principle is an iteration theory.*

Proof. Suppose that T is an ordered Conway theory which satisfies the weak Park induction principle. By Corollary 8.2, we need to show that T satisfies the

group identities. But let G be a finite group on the set $[n]$, and let $f: 1 \to n+p$ in T. Define $g = f \cdot (\tau_n \oplus \mathbf{1}_p)$. Then the square below commutes:

$$\begin{array}{ccc} n & \xrightarrow{f_G} & n+p \\ {\scriptstyle \tau_n}\downarrow & & \downarrow{\scriptstyle \tau_n \oplus \mathbf{1}_p} \\ 1 & \xrightarrow[g]{} & 1+p \end{array} \tag{40}$$

Thus,

$$\begin{aligned} f_G \cdot \langle \tau_n \cdot g^\dagger, \mathbf{1}_p \rangle &= f_G \cdot (\tau_n \oplus \mathbf{1}_p) \cdot \langle g^\dagger, \mathbf{1}_p \rangle \\ &= \tau_n \cdot g \cdot \langle g^\dagger, \mathbf{1}_p \rangle \\ &= \tau_n \cdot g^\dagger, \end{aligned}$$

by (40) and the (scalar) fixed point identity. Thus,

$$f_G^\dagger \leqslant \tau_n \cdot g^\dagger,$$

since the weak Park induction principle holds in T.

In order to prove that $\tau_n \cdot g^\dagger \leqslant f_G^\dagger$, note that the components of $f_G^\dagger$ are pairwise equal. See Remark 10.6. Thus, if α denotes the distinguished morphism 1_n, then $f_G^\dagger = \tau_n \cdot \alpha \cdot f_G{}^\dagger$ and

$$\begin{aligned} g \cdot \langle \alpha \cdot f_G^\dagger, \mathbf{1}_p \rangle &= \alpha \cdot \tau_n \cdot g \cdot \langle \alpha \cdot f_G^\dagger, \mathbf{1}_p \rangle \\ &= \alpha \cdot f_G \cdot (\tau_n \oplus \mathbf{1}_p) \cdot \langle \alpha \cdot f_G^\dagger, \mathbf{1}_p \rangle \\ &= \alpha \cdot f_G \cdot \langle \tau_n \cdot \alpha \cdot f_G^\dagger, \mathbf{1}_p \rangle \\ &= \alpha \cdot f_G \cdot \langle f_G^\dagger, \mathbf{1}_p \rangle \\ &= \alpha \cdot f_G^\dagger. \end{aligned}$$

Thus,

$$g^\dagger \leqslant \alpha \cdot f_G^\dagger, \tag{41}$$

so that

$$\begin{aligned} \tau_n \cdot g^\dagger &\leqslant \tau_n \cdot \alpha \cdot f_G^\dagger \\ &= f_G^\dagger. \quad \blacksquare \end{aligned}$$

Remark 19.2. In the above proof, we used very little of the assumption that the theory operations preserve the partial order. Also, the assumption that T is a Conway theory may be weakened, since the composition identity follows from the fixed point identity and the weak Park induction principle.

COROLLARY 19.3. *Iteration theories are the variety of preiteration theories generated by the unordered reducts of the ordered Conway theories satisfying the weak Park induction principle. Thus an equation holds in all iteration theories iff it holds in all Conway theories satisfying the weak Park induction principle.*

Proof. This follows from Theorem 19.1 and the fact that each free iteration theory may be turned into an ordered theory satisfying the weak Park induction principle. ∎

There is a variant of the Park induction principle which involves the implication

$$f \cdot \langle g, \mathbf{1}_p \rangle \leqslant g \Rightarrow f^\dagger \leqslant g, \qquad f: n \to n+p, \quad g: n \to p,$$

or this implication just in case $n = 1$. See [14] for more results. A 2-categorical generalization can be found in [18].

20. APPLICATIONS

As shown in [4], the bisimilarity equivalence classes of finite state processes with multiple entries and exits over a set A of action symbols form an iteration theory $\mathbf{BFP}_A$. In addition to the iteration theory structure, $\mathbf{BFP}_A$ is equipped with an additive structure satisfying:

$$(f+g)+h = f+(g+h) \tag{42}$$

$$f+g = g+f \tag{43}$$

$$f+\perp_{np} = f \tag{44}$$

$$(f+g)\cdot k = f\cdot k + g\cdot k \tag{45}$$

$$(1_2+2_2)^\dagger = \mathbf{1}_1, \tag{46}$$

where $f, g, h: n \to p$, $k: p \to q$, and where $\perp_{np}$ is an abbreviation for $(\mathbf{1}_n \oplus 0_p)^\dagger$. (Alternatively, instead of the addition operation, we may consider a constant $+: 1 \to 2$ and require a few axioms involving the constant $+$, or we may take the above axioms only for $n = 1$. The fact that the additive structure is idempotent is a consequence of these axioms.) In fact, it is shown in [4] that each theory $\mathbf{BFP}_A$ is freely generated by the set A in the variety of enriched iteration theories axiomatized by the iteration theory identities and the axioms (42)–(46). Thus, the Conway identities, the group identities, and Eqs. (42)–(46) give a complete axiomatization of finite state process behaviors. Moreover, if Conjecture 17.1 is true, then the set consisting of the Conway identities, the equations $\mathbf{S}_n$, $n \geqslant 3$, and the axioms (42)–(46) are also complete.

As a second application, consider language equivalence $\sim$ on finite state processes, or finite state process behaviors. The quotient theory $\mathbf{BFP}_A/\sim$ may be represented as the matrix theory $\mathbf{Reg}_A$ over the *-semiring of the regular sets over A (See Remark 3.2). Now it is proved in [4] that the star forms of the axioms for finite state process

behaviors and their *duals* give a complete axiomatization of the equational theory of the regular sets. (Hence, Corollary 8.4 and Sewell's result [36] that finite state process behaviors do not have a finite axiomatization follow from Redko's result [7] that the regular sets (on one letter) do not have a finite axiomatization.) But the set consisting of the Conway theory axioms and the group identities is self dual, so we end up with a system consisting of the Conway identities, the group identities and a finite number of natural equations involving the additive structure. The completeness of this system is the result of Krob [26]. As a corollary, we also obtain that *language equivalence* $\sim$ *is the finest congruence on finite state process behaviors such that in the quotient* $\mathbf{BFP}_A/\sim$ *composition distributes over finite sums on the left*. Although this result is expected, no (direct) proof seems to be known. Also, it does not follow from other axiomatizations, such as Milner's [31]. In fact, a large part of the analysis carried out in the present paper seems to be necessary in order to establish this result. By Theorem 17.1 and the above discussion, Conjecture 17.1 for the regular sets is equivalent to Krob's conjecture [26] that, under the Conway semiring identities and the equation $1^* = 1$, for any finite group G and set X of generators of G, the star form of the identity with (G, X) implies the star form of the identity $\mathbf{C}(G)$. For each $n \geqslant 3$, the star form of the identity $\mathbf{S}_n$ is

$$[(x+y)(x+y(x^*y)^{n-2})]^* \left[1 + (x+y) \sum_{j=0}^{n-2} (yx^*)^j \right] = (x+y)^*. \tag{47}$$

The completeness of the Conway semiring identities in conjunction with the equation $1^* = 1$ and the identities (47) with respect to the equational theory of the regular languages was conjectured by Conway, see [7]. Thus, by Theorem 17.7, if Conjecture 17.1 is true, then so is Conway's.

Finally, we note that it follows from the completeness of the Conway and group identities for iteration theories that each iteration semiring is a symmetric iteration semiring. This solves an open problem in [4].

21. FURTHER RESULTS

In [17], we give a concrete description of the free theories in the class of Conway theories satisfying the semigroup identities $\mathbf{C}(\mathscr{S})$, for any class $\mathscr{S}$ of finite semigroups. Proposition 16.6 also follows from this concrete description. We also prove a converse of Theorem 16.1: For any class $\mathscr{G}$ of simple groups closed under division, and for any automaton (A, X), if $Ax \models \mathbf{C}(A, X)$ holds for the set Ax of axioms consisting of the Conway identities and the group identities $\mathbf{C}(\mathscr{G})$, then any simple group divisor of $S(A, X)$ belongs to $\mathscr{G}$. Moreover, we prove that if (A_i, X_i), $i \in I$ is a given set of finite automata and (A, X) is a given automaton, and if $Ax \models \mathbf{C}(A, X)$ holds for the set Ax consisting of the Conway identities and the identities $\mathbf{C}(A_i, X_i)$, $i \in I$, then any simple group divisor of $S(A, X)$ divides the semigroup of at least one of the automata (A_i, X_i). Thus, if the Conway identities and some subcollection $\mathbf{C}(A_i, X_i)$ of the identities associated with a given set of finite automata (A_i, X_i), $i \in I$, is complete for the equational theory of iteration theories, then for any finite simple group G there is some $i_0 \in I$ with $G \mid S(A_{i_0}, X_{i_0})$. Further, we show that if

$\mathscr{G}$ is an effectively given set of simple groups closed under division, then it is decidable if an equation holds in the variety of Conway theories satisfying the group identities $\mathbf{C}(\mathscr{G})$.

ACKNOWLEDGMENTS

The author thanks S. L. Bloom and L. Bernátsky for carefully reading the manuscript.

Received February 27, 1996; final manuscript received March 2, 1998

REFERENCES

1. Bernátsky, L., and Ésik, Z. (1998), Semantics of flowchart programs and the free Conway theories, *RAIRO Theoret. Inform. Appl.* **32**, 35–78.
2. Bloom, S. L., Elgot, C. C., and Wright, J. B. (1980), Solutions of the iteration equation and extension of the scalar iteration operation, *SIAM J. Comput.* **9**, 26–45.
3. Bloom, S. L., Elgot, C. C., and Wright, J. B. (1980), Vector iteration in pointed iterative theories, *SIAM J. Comput.* **9**, 525–540.
4. Bloom, S. L., and Ésik, Z. (1993), "Iteration Theories: The Equational Logic of Iterative Processes," EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin.
5. Bloom, S. L., and Ésik, Z. (1994), Some quasi-varieties of iteration theories, *in* "Proceedings, Mathematical Foundations of Programming Semantics '93," LNCS 802, pp. 378–409, Springer-Verlag, Berlin.
6. Bloom, S. L., and Ésik, Z. (1994), Solving polynomial fixed point equations, *in* "Proceedings, Mathematical Foundations of Computer Science '94," LNCS 841, pp. 52–67, Springer-Verlag, Berlin.
7. Conway, J. C. (1971), "Regular Algebra and Finite Machines," Chapman and Hall, London.
8. Eilenberg, S. (1976), "Automata, Languages, and Machines," Vol. B., Academic Press, New York.
9. Eilenberg, S., The category $\mathscr{C}$, unpublished handwritten manuscript.
10. Elgot, C. C. (1975), Monadic computation and iterative algebraic theories, *in* "Proceedings, Logic Colloquium '73," Studies in Logic, Vol. 80, pp. 175–230, North Holland, Amsterdam.
11. Elgot, C. C., Bloom, S. L., and Tindell, R. (1978), On the algebraic structure of rooted trees, *J. Comput. System Sci.* **16**, 362–399.
12. Ésik, Z. (1980), Identities in iterative and rational algebraic theories, *Computational Linguistics and Computer Languages* **14**, 183–207.
13. Ésik, Z. (1988), Independence of the equational axioms of iteration theories, *J. Comput. System Sci.* **36**, 66–76.
14. Ésik, Z. (1997), Completeness of Park induction, *Theoret. Comput. Sci.* **177**, 217–283.
15. Ésik, Z., A proof of the Krohn–Rhodes decomposition theorem, submitted for publication.
16. Ésik, Z., Axiomatizing iteration categories, *Acta Cybernet.*, to appear.
17. Ésik, Z., The power of the group axioms for iteration, *Int. J. Algebra Comput.*, to appear.
18. Ésik, Z., and Labella, A. (1988), Equational properties of iteration in algebraically complete categories, *Theoret. Comput. Sci.* **195**, 61–89.
19. Ésik, Z., and Virágh, J. (1986), On products of automata with identity, *Acta Cybernet.* **7**, 299–311.
20. Ginzburg, A. (1968), "Algebraic Theory of Automata," Academic Press, New York.
21. Goguen, J. A., Thatcher, J. W., Wagner, E. G., and Wright, J. B. (1977), Initial algebra semantics and continuous algebras, *J. Assoc. Comput. Mach.* **24**, 68–95.

22. Golan, J. S. (1992), "The Theory of Semirings with Applications in Computer Science," Longman, Harlow.
23. Guessarian, I. (1981), "Algebraic Semantics," LNCS 99, Springer-Verlag, Berlin.
24. Hurkens, A. J. C., McArthur, M., Moschovakis, Y. N., Moss, L., and Whitney, G., The logic of recursive equations, *J. Symbolic Logic*, to appear.
25. Kozen, D. (1994), A completeness theorem for Kleene algebras and the algebra of regular events, *Inform. and Comput.* **110**, 366–390.
26. Krob, D. (1991), Complete systems of B-rational identities, *Theoret. Comput. Sci.* **89**, 207–343.
27. Lawvere, F. L. (1963), Functorial semantics of algebraic theories, *Proc. Nat. Acad. Sci.* **50**, 869–873.
28. Lallement, G. (1979), "Semigroups and Combinatorial Applications," Wiley–Interscience, New York.
29. Manes, E. G. (1992), "Predicate Transformer Semantics," Cambridge Univ. Press, Cambridge.
30. Milner, R. (1980), "A Calculus for Communicating Systems," LNCS 92, Springer-Verlag, Berlin.
31. Milner, R. (1984), A complete inference system for a class of regular behaviours, *J. Comput. System Sci.* **28**, 439–466.
32. Moschovakis, Y. N. (1983), Abstract recursion as a foundation for the theory of algorithms, *in* "Proceedings, Logic Colloquium Aachen '83," LNM 1104, pp. 289–364, Springer-Verlag, Berlin.
33. Nelson, E. (1983), Iterative algebras, *Theoret. Comput. Sci.* **25**, 67–94.
34. Park, D. M. R. (1970), Fixpoint induction and proofs of program properties, *in* "Machine Intelligence **5**" (D. Michie and B. Meltzer, Eds.), pp. 59–78, Edinburgh Univ. Press, Edingburgh.
35. Plotkin, G. D. (1983), "Domains," lecture notes, Department of Computer Science, University of Edinburgh.
36. Sewell, P. (1994), Bisimulation is not finitely (first order) equationally axiomatisable, *in* "Proceedings, Logic in Computer Science 9," pp. 62–70.
37. Tiuryn, J. (1978), Fixed points and algebras with infinitely long expressions, Part I: Regular algebras, *Fund. Inform.* **2**, 103–128.
38. Tiuryn, J. (1980), Unique fixed points vs. least fixed points, *Theoret. Comput. Sci.* **12**, 229–254.
39. Winskel, G. (1993), "The Formal Semantics of Programming Languages," Foundations of Computing Series, MIT Press, Cambridge, MA.
40. Wright, J. B., Thatcher, J. W., Goguen, J., and Wagner, E. G. (1976), Rational algebraic theories and fixed-point solutions, *in* "Proceedings, 17th IEEE Symp. Foundations of Computing, Houston, Texas."