Acta Cybernetica **14** (1999) 65-82.

Axiomatizing iteration categories

Z. Ésik*†

Dedicated to Ferenc Gécseg on his 60th birthday

Abstract

We associate an identity with every finite automaton and show that a set of equations consiting of some classical identities as well as the equations associated with a subclass of finite automata is complete for iteration theories if and only if every finite simple group divides the semigroup of an automaton in the given subclass. By taking a special subclass with this property, we arrive at the final result of the paper.

1 Introduction

It has been shown in [3] that the axioms of iteration theories capture the equational properties of the fixed point operation in computer science. For a recent overwiew see also [5]. The first axiomatization of iteration theories was given in [8]. This system was simplified in [9] by proving that some classical identities in conjunction with an identity associated with each finite (simple) group is complete. This result confirms a conjecture in [6] in a general setting. In the present paper we give a further simplification of the iteration theory axioms. We associate an identity with every finite automaton and show that a set of equations consiting of some classical identities as well as the equations associated with a subclass of finite automata is complete if and only if every finite simple group divides the semigroup of an automaton in the given subclass. By taking a special subclass with this property, we arrive at our final result.

In this paper, we define theories in a slightly more general way, so that in this context, we prefer the term iteration categories to iteration theories.

*Supported in part by grant no. T22423 of the National Science Foundation of Hungary, the US-Hungarian Joint Fund under grant no. 351, and by the Austrian-Hungarian Action Foundation.

†Department of Computer Science A. József University Árpád tér 2. 6720 Szeged Hungary

2 Preliminaries

2.1 Conway categories and iteration categories

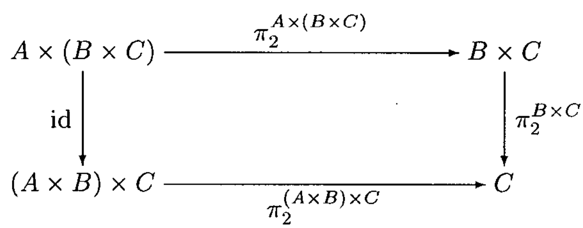
In any category $\mathcal{C}$, we denote composition by $\cdot$. The identity morphism corresponding to a $\mathcal{C}$-object A will be written id_A, or just id.

We will consider **cartesian categories $\mathcal{C}$ with explicit products**. Thus we assume that for any finite family of $\mathcal{C}$-objects C_i, $i \in [n] = \{1, \ldots, n\}$ we are given a product diagram

$$\pi_j^{C_1 \times \ldots \times C_n} : C_1 \times \ldots \times C_n \quad \longrightarrow \quad C_j, \quad j \in [n]$$

with the usual universal property. When $f_i : A \longrightarrow C_i$, $i \in [n]$ is a family of morphisms, the unique mediating morphism $A \longrightarrow C_1 \times \ldots \times C_n$ will be denoted $\langle f_1, \ldots, f_n \rangle$. This morphism is called the **tupling** of the f_i. In particular, when $n = 0$, the empty tuple is the unique morphism $!_A : A \longrightarrow 1$, where 1 is the specified terminal object.

We will assume that product is associative on the nose so that $A \times (B \times C) = (A \times B) \times C$, for all objects A, B, C, and diagrams such as



commute. In particular, we assume that for each object A the projection morphism $\pi_1^A : A \longrightarrow A$ is the identity morphism id_A. It follows that $\langle f \rangle = f$ for all $f : A \longrightarrow B$. We also assume that

$$\langle f, ! \rangle = \langle !, f \rangle = f,$$

for all morphisms $f : A \longrightarrow B$.

In the sequel we will call tuplings of projections as **base morphism**. Note that any base morphism $A^n \longrightarrow A^m$ corresponds to a function $\rho : [m] \longrightarrow [n]$. In fact the base morphism $A^n \longrightarrow A^m$ determined by ρ is given by

$$\langle \pi_{1\rho}^{A^n}, \ldots, \pi_{m\rho}^{A^n} \rangle.$$

We will call a base morphism corresponding to a permutation $[n] \longrightarrow [n]$ a **base permutation**.

For any cartesian category $\mathcal{C}$ we define the bifunctor $\mathcal{C} \times \mathcal{C} \longrightarrow \mathcal{C}$ by

$$f \times g \quad = \quad \langle f \cdot \pi_1^{C \times D},\ g \cdot \pi_2^{C \times D} \rangle,$$

for all $f : C \longrightarrow A$, $g : D \longrightarrow B$.

DEFINITION 2.1 *A* **preiteration category** *is a cartesian category $\mathcal{C}$ equipped with an* **external dagger operation**

$$^{\dagger}: \mathcal{C}(A \times B, A) \quad \rightarrow \quad \mathcal{C}(B, A),$$

see [4].

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

$$(f \cdot (\mathrm{id}_A \times g))^{\dagger} \quad = \quad f^{\dagger} \cdot g, \tag{1}$$

all $f : A \times B \longrightarrow A,\ g : C \longrightarrow B$,

$$f^{\dagger\dagger} \quad = \quad (f \cdot (\Delta \times \mathrm{id}_C))^{\dagger}, \tag{2}$$

where $f : A \times A \times C \longrightarrow A$ and where Δ is the diagonal morphism $\langle \mathrm{id}_A, \mathrm{id}_A \rangle : A \longrightarrow A \times A$.

$$(f \cdot \langle g, \pi_2^{A\times C} \rangle)^{\dagger} \quad = \quad f \cdot \langle (g \cdot \langle f, \pi_2^{B\times C} \rangle)^{\dagger},\ \pi_2^{B\times C} \rangle, \tag{3}$$

for all $f : B \times C \longrightarrow A$, $g : A \times C \longrightarrow B$. Note that the **fixed point identity**

$$f^{\dagger} \quad = \quad f \cdot \langle f^{\dagger}, \mathrm{id}_C \rangle, \quad f : A \times C \longrightarrow A$$

is a particular subcase of the composition identity.

DEFINITION 2.2 [3] *A* **Conway category** *is a preiteration category satisfying the Conway identities.*

Conway categories satisfy several other non-trivial identities including the **Bekič identity** [1] (called the **pairing identity** in [3]):

$$\langle f, g \rangle^{\dagger} \quad = \quad \langle f^{\dagger} \cdot \langle h^{\dagger}, \mathrm{id}_C \rangle,\ h \rangle^{\dagger},$$

for all $f : A \times B \times C \longrightarrow A$ and $g : A \times B \times C \longrightarrow B$, where

$$h \quad = \quad g \cdot \langle f^{\dagger}, \mathrm{id}_{B\times C} \rangle : B \times C \longrightarrow B.$$

We will also make use of the **permutation identity**

$$(\pi \cdot f \cdot (\pi^{-1} \times \mathrm{id}_C))^{\dagger} \quad = \quad \pi \cdot f^{\dagger},$$

for all $f : A^n \times C \longrightarrow A^n$ and all base permutations $\pi : A^n \longrightarrow A^n$. Another useful identity is given by the next lemma.

LEMMA 2.3 *In any Conway category $\mathcal{C}$,*

$$f^{\dagger\cdots\dagger} \quad = \quad (f \cdot (\Delta_n \times \mathrm{id}_p))^{\dagger},$$

for all morphisms $f : A^n \times C \longrightarrow A$, where there are $n > 1$ consecutive daggers on the left hand side and where Δ_n is the diagonal morphism $\langle \mathrm{id}_A, \ldots, \mathrm{id}_A \rangle : A \longrightarrow A^n$.

A full description of the valid identities of Conway categories is given in [2], where it is proved that the problem of deciding whether an equation holds in all Conway categories is PSPACE-complete. It is shown in [4] that the parameter identity corresponds to a naturality condition and that the double dagger identity to a dinaturality condition of the dagger operation.

As argued in [3], all of the fixed point models in computer science satisfy at least the Conway identities. For example, for any set S, the category $\mathbf{Cpo}^S$ of S-sorted cpo's and continuous functions satisfies the Conway identities. In this category, there is a cpo A_w corresponding to any word $w \in S^*$. When $w = s_1 \dots s_n$, the cpo A_w is determined by the cpo's A_{s_i}, in fact A_w is the product $A_{s_1} \times \dots \times A_{s_n}$. The morphisms $A_w \longrightarrow A_v$ are the continuous (or order preserving) functions $A_w \longrightarrow A_v$, and the dagger operation is defined by least fixed points.

We give a semantic definition of iteration categories. For a syntactic characterization the reader is referred to Section 3.

DEFINITION 2.4 *An* **iteration category** *is a preiteration category equipped with a dagger operation which satisfies all of the identities that hold in the categories* $\mathbf{Cpo}^S$.

It is shown in [3], see also [5], that the iteration category identities are *the* standard identities of the fixed point operation in computer science.

2.2 Automata and semigroups

Except for free semigroups, all semigroups will be assumed to be finite. The product of the elements s, t of a semigroup S will be written $s \circ t$, or just st. A subgroup of a semigroup S is a subsemigroup of S which is a group. Following [7, 12], we say that a semigroup S **divides** a semigroup S', denoted $S|S'$, if S is a homomorphic image of a subsemigroup of S'. It is known that the division relation is transitive (and reflexive). Further, a group G divides a semigroup S if and only if 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.

Suppose that X is a finite nonempty set. An X-**automaton** $\mathbf{Q} = (Q, X, \circ)$ is a finite nonempty set Q equipped with a (right) action of X on Q:

$$\begin{array}{rcl} \circ : Q \times X & \longrightarrow & Q \\ (q, x) & \mapsto & q \circ x. \end{array}$$

We will usually write qx for $q \circ x$ and (Q, X) for $(Q, X, \circ)$. The action of X on Q may be extended to an action of the free semigroup X^+ of all finite nonempty words over X such that

$$q(ux) \quad = \quad (qu)x$$

for all $q \in Q$, $u \in X^+$ and $x \in X$.

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

$$q \mapsto qx, \quad q \in Q$$

induced by x is a permutation (constant map, respectively) on Q. We call $\mathbf{Q}$ a **permutation automaton** (**reset automaton**, respectively) if each letter $x \in X$ is a permutation letter (reset letter, respectively). Further, we call $\mathbf{Q}$ a **permutation–reset automaton** if each $x \in X$ is either a permutation letter or a reset letter. For example, the automaton $\mathbf{U} = (\{q_1, q_2\}, \{x_1, x_2, x_3\})$ equipped with the action

$$\begin{aligned} q_i x_j &= q_j \\ q_i x_3 &= q_i, \quad i, j \in [2], \end{aligned}$$

is a permutation-reset automaton, called the **two-state identity-reset automaton**. This automaton is important in the Krohn-Rhodes decomposition theorem, see [11]. In our arguments we will also make use of counters. A **counter of length** n is a (permutation) automaton $(Q, \{x\})$ such that $Q = \{q_0, \ldots, q_{n-1}\}$ has n elements and letter x induces the cyclic permutation $q_i \mapsto q_{i+1 \bmod n}$.

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

$$qx = q(x\varphi),$$

for all $q \in Q$ and $x \in X$.

Suppose that $\mathbf{Q} = (Q, X)$ is an automaton. Recall that each word $u \in X^+$ induces a function $Q \longrightarrow Q$. Equipped with the operation of composition that we now write in diagrammatic order, these functions form a semigroup denoted $S(\mathbf{Q})$. We call $S(\mathbf{Q})$ the **semigroup of Q**. For example, the semigroup of a counter of length n is a cyclic group of order n. When $\mathbf{Q}$ is a permutation automaton, each element of $S(\mathbf{Q})$ is a permutation of the set Q, so that $S(\mathbf{Q})$ is a group. An automaton $\mathbf{Q}$ is called **aperiodic** [7], if each subgroup of $S(\mathbf{Q})$ is trivial. For example, each reset automaton, or more generally, each **definite** automaton [7] is aperiodic. The automaton $\mathbf{U}$ is also aperiodic. We will denote the class of aperiodic automata by $\mathcal{AP}$.

The concept of aperiodic automata may be generalized. Suppose that $\mathcal{G}$ is a class of simple groups closed under division. *We let $\mathcal{Q}_{\mathcal{G}}$ denote the class of all automata $\mathbf{Q}$ such that any simple group divisor of $S(\mathbf{Q})$ is in $\mathcal{G}$.* Thus, when $\mathcal{G}$ is empty, $\mathcal{Q}_{\mathcal{G}}$ is the class $\mathcal{AP}$. When $\mathcal{G}$ is the class of all cyclic groups of prime order, $\mathcal{Q}_{\mathcal{G}}$ is known as the class of **solvable automata**. We denote this class by $\mathcal{SOL}$. We will also make use of the following notation. Suppose that $m \geq 1$ is an integer. Then we let $\mathcal{SOL}_m$ denote the class of all (solvable) automata $\mathbf{Q}$ such that any simple group divisor of $S(\mathbf{Q})$ is a cyclic group of prime order p which divides m. Thus, $\mathcal{SOL}_m = \mathcal{SOL}_n$ if and only if m and n have the same prime divisors. Note that $\mathcal{SOL}_1 = \mathcal{AP}$.

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

$$q(st) = (qs)t$$

for all $q \in Q$ 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

$$qe = q,$$

for all $q \in Q$, (Q, S) is a **transformation group**. See [7]. 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.

Following [11], we now define cascade compositions (or α_0-products) of automata. For this reason, suppose that $\mathbf{Q}_i = (Q_i, X_i)$, $i \in [n]$, $n > 0$, are given automata. Moreover, suppose that X is a new finite nonempty set and for each $i \in [n]$ we are given a function

$$\varphi_i : Q_1 \times \ldots \times Q_{i-1} \times X \quad \longrightarrow \quad X_i.$$

Then the **cascade composition**

$$\prod_{i \in [n]} \mathbf{Q}_i[X, \varphi_i]$$

determined by the functions φ_i is the automaton $(\prod_{i \in [n]} Q_i, X)$ equipped with the X-action

$$(q_1, \ldots, q_n)x = (q_1 y_1, \ldots, q_n y_n),$$

where $y_i = \varphi_i(q_1, \ldots, q_{i-1}, x)$, for all i. Note that when $n = 1$, a cascade composition is just a renaming of $\mathbf{Q}_1$. We will sometimes denote the above cascade composition as

$$\mathbf{Q}_1 \times \ldots \times \mathbf{Q}_n[X, \varphi_1, \ldots, \varphi_n].$$

Two particular subcases of the cascade composition are also important, the quasi-direct product and the direct product. We call the above cascade composition a **quasi-direct product** if each function φ_i is independent of its first $i - 1$ arguments, so that each φ_i can be considered as a function $X \longrightarrow X_i$. If for each i also $X = X_i$ and φ_i is the identity function $X \longrightarrow X$, then the quasi-direct product is the **direct product** $\prod_{i \in [n]} \mathbf{Q}_i$.

We will say that an automaton (Q, X) **has an identity letter** if some $x \in X$ induces the identity function $Q \longrightarrow Q$. Given $\mathbf{Q}$, we will denote by $\mathbf{Q}^1$ an automaton obtained from $\mathbf{Q}$ by adding a letter inducing the identity function $Q \longrightarrow Q$, if $\mathbf{Q}$ has no such letter. Otherwise $\mathbf{Q}^1$ is just $\mathbf{Q}$. This notation is extended to classes of automata in a natural way.

3 Review

In this section we review some of the results of [9] and [10].

Suppose that $\mathbf{Q} = (Q, X)$ is a finite automaton such that $Q = [n]$ and $X = [m]$, for some integers n and m. For each preiteration category C and object A in C, we associate with $\mathbf{Q}$ the base morphisms $\rho_q^{\mathbf{Q}} : A^n \longrightarrow A^m$, $q \in Q$. For each q, $\rho_q^{\mathbf{Q}}$ corresponds to the map

$$\begin{array}{rcl} [m] & \longrightarrow & [n] \\ x & \mapsto & qx. \end{array}$$

Thus,

$$\rho_q^{\mathbf{Q}} \quad = \quad \langle \pi_{q1}^{A^n}, \ldots, \pi_{qm}^{A^n} \rangle.$$

(Recall that $X = [m]$, so that for each $q \in Q = [n]$ and $i \in [m]$, qi is a state of the automaton $\mathbf{Q}$.) The morphisms $\rho_q^{\mathbf{Q}}$, denoted sometimes just ρ_q, are called the **base morphisms associated with the automaton Q**.

We define, for each $g : A^m \times C \longrightarrow A$,

$$g_{\mathbf{Q}} \quad = \quad \langle g \cdot (\rho_1 \times \mathrm{id}_C), \ldots, g \cdot (\rho_n \times \mathrm{id}_C) \rangle : A^n \times C \longrightarrow A^n.$$

DEFINITION 3.1 *The* **automaton-identity** $\Gamma(\mathbf{Q})$ *associated with* $\mathbf{Q}$ *is the equation*

$$(g_{\mathbf{Q}})^\dagger \quad = \quad \Delta_n \cdot (g \cdot (\Delta_m \times \mathrm{id}_C))^\dagger, \quad g : A^m \times C \longrightarrow A. \tag{4}$$

In preiteration categories satisfying the permutation identity we can associate an equation with any automaton not just with those defined on sets of the form $[m]$. In such categories, equations associated with isomorphic automata are equivalent.

Since any transformation semigroup is an automaton, the above definition associates an identity $\Gamma(Q, S)$ with each transformation semigroup (Q, S). When (Q, S) is the transformation semigroup (S, S) equipped with the natural self action, we denote $\Gamma(S, S)$ by $\Gamma(S)$ and call this identity the **semigroup-identity associated with** S. When S is group, $\Gamma(S)$ is a **group-identity**.

The above notation may be extended to classes of automata and semigroups. When $\mathcal{Q}$ is a class of finite automata, $\Gamma(\mathcal{Q})$ consists of all identities $\Gamma(\mathbf{Q})$, $\mathbf{Q} \in \mathcal{Q}$. When $\mathcal{S}$ is a class of finite semigroups, $\Gamma(\mathcal{S})$ is defined similarly.

The axiomatization of iteration categories given in the next theorem is a reformulation of the main result of [8].

THEOREM 3.2 *A Conway category C is an iteration category if and only if each automaton identity holds in C.*

The following stronger results were proved in [9] and [10].

THEOREM 3.3 *Suppose that $\mathcal{S}$ is a given class of semigroups and $\mathbf{Q}$ is an automaton. Then the automaton identity $\Gamma(\mathbf{Q})$ associated with $\mathbf{Q}$ holds in all Conway categories satisfying the semigroup-identities $\Gamma(\mathcal{S})$ if and only if every simple group divisor of $S(\mathbf{Q})$ divides one of the semigroups in $\mathcal{S}$.*

In particular, an automaton identity $\Gamma(\mathbf{Q})$ holds in all Conway categories if and only if $\mathbf{Q} \in \mathcal{AP}$. And if $\mathcal{G}$ is any class of simple groups closed under division, then $\Gamma(\mathbf{Q})$ holds in all Conway categories satisfying the group-identities $\Gamma(\mathcal{G})$ if and only if $\mathbf{Q} \in \mathcal{Q}_{\mathcal{G}}$.

COROLLARY 3.4 [9] *A Conway category is an iteration category if and only if it satisfies the group-identities. Given a class $\mathcal{S}$ of finite semigroups, consider the set of equations $\Gamma(\mathcal{S})$ associated with the semigroups in $\mathcal{S}$. The system consisting of the Conway identities and the equations $\Gamma(\mathcal{S})$ is complete for iteration categories if and only if for every simple group G there is a semigroup $S \in \mathcal{S}$ such that $G|S$.*

In the course of proving Theorem 3.3, the following facts were established in [9].

LEMMA 3.5 *Suppose that $\mathbf{Q}$ is a subautomaton or a renaming of $\mathbf{Q}'$. If C is a Conway category with $C \models \Gamma(\mathbf{Q}')$ then $C \models \Gamma(\mathbf{Q})$.*

LEMMA 3.6 *Let C be a Conway category and suppose that $\mathbf{Q} = \prod_{i\in[n]} \mathbf{Q}_i[X, \varphi_i]$ is a cascade composition. If $C \models \Gamma(\mathbf{Q}_i)$ for all $i \in [n]$, then $C \models \Gamma(\mathbf{Q})$. Moreover, if φ_1 is surjective and if $C \models \Gamma(\mathbf{Q})$ and $C \models \Gamma(\mathbf{Q}_i)$ for all $i > 1$, then $C \models \Gamma(\mathbf{Q}_1)$.*

4 Main results

The main results of this paper are Theorem 4.2, Corollary 4.4 and Theorem 4.5 below. In order to formulate these results, we need one more definition.

The **powers** $f^k : A \times C \to A$, $k \geq 0$, of a morphism $f : A \times C \to A$ in a cartesian category are defined by induction:

$$\begin{aligned} f^0 &= \pi_1^{A\times C} \\ f^{k+1} &= f \cdot \langle f^k, \pi_2^{A\times C} \rangle. \end{aligned}$$

DEFINITION 4.1 *For each $m \geq 1$, the mth* **power identity** *is the equation $\mathbf{P}_m$*

$$(f^m)^\dagger = f^\dagger, \quad f : A \times C \to A.$$

Note that this identity is nontrivial only if $m > 1$. We will prove

THEOREM 4.2 *Suppose that $\mathcal{Q}$ is a class of automata and $\mathbf{Q}$ is an automaton such that every simple group divisor of $S(\mathbf{Q})$ divides the semigroup of some automaton in $\mathcal{Q}$. If C is a Conway category satisfying the identities $\Gamma(\mathcal{Q})$ and a nontrivial power identity, then $C \models \Gamma(\mathbf{Q})$.*

COROLLARY 4.3 *Suppose that a renaming of some automaton in $\mathcal{Q}$ contains a nontrivial counter as a subautomaton. Then the identity $\Gamma(\mathbf{Q})$ associated with an automaton $\mathbf{Q}$ holds in all Conway categories satsifying the identities $\Gamma(\mathcal{Q})$ if and only if every simple group divisor of $S(\mathbf{Q})$ divides the semigroup of an automaton in $\mathcal{Q}$.*

From Corollary 4.3 and Theorem 3.2 we immediately have

COROLLARY 4.4 *Suppose that a renaming of an automaton in $\mathcal{Q}$ contains a nontrivial counter. If every (simple) group is a divisor of the semigroup of an automaton in $\mathcal{Q}$, then the Conway identities and the automaton identites in* $\mathbf{S}(\mathcal{Q})$ *are complete for iteration categories.*

Conversely, if $\mathcal{Q}$ is any class of finite automata such that the Conway identities, the power identities, and the automaton identities in $\Gamma(\mathcal{Q})$ are complete for iteration categories, then every (simple) group divides the semigroup of an automaton in $\mathcal{Q}$.

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

$$(f \cdot (\Delta_2 \times \mathrm{id}_C) \cdot \langle f \cdot \langle \pi_1^{A\times C},\ (f^\dagger)^{n-2}, \pi_2^{A\times C}\rangle,\ \pi_2^{A\times C}\rangle)^\dagger \quad = \quad (f \cdot (\Delta_2 \times \mathrm{id}_C))^\dagger,$$

where f is any morphism $A^2 \times C \longrightarrow A$ in a preiteration category. This identity is a generalization of an identity of regular sets introduced by John Conway in [6]. As an application of Theorem 4.2, we will prove

THEOREM 4.5 *The Conway identities and the equations $\mathbf{S}_n$, for all $n \geq 3$, are complete for iteration categories.*

In order to establish these results, we need to derive the identity $\Gamma(G)$ associated with a group G dividing the semigroup of an automaton $\mathbf{Q}$ from the the identity $\Gamma(\mathbf{Q})$, a nontrivial power identity, and the Conway identities.

5 Identities associated with solvable automata

In this section, we show that in Conway categories, the mth power identity is equivalent to the identity associated with a counter of length m. We then proceed to prove that an automaton identity $\Gamma(\mathbf{Q})$ holds in all Conway categories satisfying the mth power identity if and only if $\mathbf{Q} \in \mathcal{SOL}_m$. We start with a technical lemma.

LEMMA 5.1 *Suppose that $\mathcal{C}$ is a Conway category satisfying the identity $\Gamma(\mathbf{Q})$ associated with a finite automaton $\mathbf{Q}$. Then $\mathcal{C} \models \Gamma(\mathbf{Q}^1)$.*

Proof. Suppose that $\mathbf{Q} = (Q, X)$. If $\mathbf{Q}$ has a letter inducing the identity function $Q \longrightarrow Q$ then $\mathbf{Q}^1 = \mathbf{Q}$ and there is nothing to prove. Otherwise $\mathbf{Q}^1 = (Q, Y)$ with $Y = \{y\} \cup X$ such that y induces the identity function $Q \longrightarrow Q$ and each $x \in X$ induces the same function in $\mathbf{Q}$ as in $\mathbf{Q}^1$. In our argument, we assume that $Q = [n]$, $X = \{i : 2 \leq i \leq m+1\}$, so that $Y = [m+1]$ and $y = 1$.

Suppose that $\mathcal{C}$ is a Conway category and A and C are objects in $\mathcal{C}$. Define

$$\begin{aligned} \rho_i &= \rho_i^{\mathbf{Q}} : A^n \longrightarrow A^m \\ \sigma_i &= \rho_i^{\mathbf{Q}^1} : A^n \longrightarrow A^{1+m}, \end{aligned}$$

for all $i \in [n]$. Then we have

$$\sigma_i = \langle \pi_i^{A^n}, \rho_i \rangle, \tag{5}$$

for all $i \in [n]$. We complete the argument by using the following sublemma whose proof is omitted.

SUBLEMMA 5.2 *Suppose that $f_i : A^{1+n} \times C \longrightarrow A$, $i \in [n]$ in a Conway category $\mathcal{C}$. Then*

$$\langle f_1 \cdot \langle \pi_1^{A^n \times C}, \mathrm{id}_{A^n \times C} \rangle, \ldots, f_n \cdot \langle \pi_n^{A^n \times C}, \mathrm{id}_{A^n \times C} \rangle \rangle^\dagger = \langle f_1^\dagger, \ldots, f_n^\dagger \rangle^\dagger.$$

Suppose now that $f : A^{1+m} \times C \longrightarrow A$. Then, by Sublemma 5.2, equation (5), and the parameter identity,

$$\begin{aligned} (f_{\mathbf{Q}^1})^\dagger &= \langle f^\dagger \cdot (\rho_1 \times \mathrm{id}_C), \ldots, f^\dagger \cdot (\rho_n \times \mathrm{id}_C) \rangle^\dagger \\ &= (g_{\mathbf{Q}})^\dagger, \end{aligned}$$

where g is the morphism $f^\dagger$. Thus, since $\mathcal{C} \models \Gamma(\mathbf{Q})$, we have

$$\begin{aligned} (f_{\mathbf{Q}^1})^\dagger &= (g_{\mathbf{Q}})^\dagger \\ &= \Delta_n \cdot (f^\dagger \cdot (\Delta_m \times \mathrm{id}_C))^\dagger \\ &= \Delta_n \cdot (f \cdot (\Delta_{m+1} \times \mathrm{id}_C))^\dagger, \end{aligned}$$

where the last step follows from Lemma 2.3. □

The following fact is obvious.

LEMMA 5.3 *Suppose that $\mathcal{C}$ is a preiteration category and $m, n \geq 1$. If $\mathcal{C} \models \mathbf{P}_m$ and $\mathcal{C} \models \mathbf{P}_n$, then $\mathcal{C} \models \mathbf{P}_{mn}$.*

For the rest of this section, for each $m \geq 1$ we let $\mathbf{K}_m$ denote a counter of length m.

LEMMA 5.4 *For any Conway category $\mathcal{C}$ and $m \geq 1$, $\mathcal{C} \models \mathbf{P}_m$ if and only if $\mathcal{C} \models \Gamma(\mathbf{K}_m)$.*

Proof. This is obvious if $m = 1$, so we assume $m > 1$. It is easy to see that $\mathcal{C} \models \Gamma(\mathbf{K}_m)$ if and only if

$$\pi_1^{A^m} \cdot (f_{\mathbf{K}_m})^\dagger = f^\dagger,$$

for all $f : A \times C \longrightarrow A$. But since $\mathcal{C}$ is a Conway category,

$$\pi_1^{A^m} \cdot (f_{\mathbf{K}_m})^\dagger = (f^m)^\dagger.$$

Indeed, we have

$$f_{\mathbf{K}_m} = \langle f \cdot (\pi_2^{A^m} \times \mathrm{id}_C), \ldots, f \cdot (\pi_m^{A^m} \times \mathrm{id}_C),\ f \cdot (\pi_1^{A^m} \times \mathrm{id}_C) \rangle : A^m \times C \longrightarrow A^m.$$

Define

$$g \;=\; \langle f\cdot(\pi_2^{A^m}\times \mathrm{id}_C),\ldots,f\cdot(\pi_m^{A^m}\times \mathrm{id}_C)\rangle : A^m\times C\longrightarrow A^{m-1}.$$

Then

$$g^{m-1} \;=\; \langle f^{m-1},\ldots,f\rangle\cdot(\pi_m^{A^m}\times \mathrm{id}_C).$$

Thus, by the fixed point identity,

$$\begin{aligned} g^\dagger &= g^{m-1}\cdot\langle g^\dagger,\mathrm{id}_{A\times C}\rangle \\ &= \langle f^{m-1},\ldots,f\rangle : A\times C\longrightarrow A^{m-1}. \end{aligned}$$

Thus, by the pairing identity,

$$\begin{aligned} \pi_1^{A^m}\cdot(f_{\mathbf{K}_m})^\dagger &= \pi_1^{A^{m-1}}\cdot g^\dagger\cdot\langle h^\dagger,\mathrm{id}_C\rangle \\ &= f^{m-1}\cdot\langle h^\dagger,\mathrm{id}_C\rangle, \end{aligned}$$

where

$$\begin{aligned} h &= f\cdot(\pi_1^{A^m}\times \mathrm{id}_C)\cdot\langle g^\dagger,\mathrm{id}_{A\times C}\rangle \\ &= f\cdot\langle f^{m-1},\pi_2^{A\times C}\rangle \\ &= f^m. \end{aligned}$$

Thus, $h^\dagger=(f^m)^\dagger$ and

$$\begin{aligned} \pi_1^{A^m}\cdot(f_{\mathbf{K}_m})^\dagger &= f^{m-1}\cdot\langle (f^m)^\dagger,\mathrm{id}_C\rangle \\ &= (f^m)^\dagger, \end{aligned}$$

by the composition identity. □

Suppose that $\mathcal{C}$ is a Conway category satisfying the mth power identity $\mathbf{P}_m$. Let Z_m denote the cyclic group Z/mZ of order m. In order to prove that $\mathcal{C}$ satisfies the group-identity $\Gamma(Z_m)$ we need a technical consruction involving automata.

We represent Z_m as the set $\{0,\ldots,m-1\}$ with group operation

$$(i,j) \;\mapsto\; i+j \bmod m.$$

Similarly, we represent $\mathbf{K}_m^1$ as the automaton (Z_m,X), where $X=\{0,1\}$, so that X is a generating set of the group Z_m. The action of X on Z_m is defined by the group operation. Define the quasi-direct product

$$\mathbf{A} \;=\; (A,Z_m) \;=\; (Z_m,Z_m)\times(Z_m,X)^{m-2}[Z_m,\varphi_1,\ldots,\varphi_{m-1}]$$

by

$$\begin{aligned} j\varphi_1 &= j \quad ; \\ j\varphi_i &= \begin{cases} 0 & \text{if } j\neq i \\ 1 & \text{if } j=i, \end{cases} \end{aligned}$$

for all $j \in \{0, \ldots, m-1\}$ and $i \in \{2, \ldots, m-1\}$. Moreover, define

$$\mathbf{B} \;=\; (B, Z_m) \;=\; (Z_m, X)^{m-1}[Z_m, \psi_1, \ldots, \psi_{m-1}]$$

by

$$j\psi_i \;=\; \begin{cases} 0 & \text{if } j \neq i \\ 1 & \text{if } j = i, \end{cases}$$

for all $j \in \{0, \ldots, m-1\}$ and $i \in \{1, \ldots, m-1\}$. Note that $A = B = Z_m^{m-1}$.

LEMMA 5.5 *The automata* **A** *and* **B** *are isomorphic.*

Proof. Define

$$\begin{aligned} \mu : B &\rightarrow A \\ (i_1, \ldots, i_{m-1}) &\mapsto (\sum_{j=1}^{m-1} i_j \cdot j,\ i_2, \ldots, i_{m-1}), \end{aligned}$$

where the sum is taken mod m. Then μ is a bijection. Suppose that $k \in \{0, \ldots, m-1\}$, $k \neq 0$. Then, in **B**,

$$(i_1, \ldots, i_{m-1}) \circ k \;=\; (i_1, \ldots, i_k + 1, \ldots, i_{m-1}).$$

Moreover, in **A**,

$$\mu(i_1, \ldots, i_{m-1}) \circ k \;=\; (k + \sum_{j=1}^{m-1} i_j \cdot j,\ i_2, \ldots, i_k + 1, \ldots, i_{m-1}),$$

if $k > 1$, and

$$\mu(i_1, \ldots, i_{m-1}) \circ k \;=\; (k + \sum_{j=1}^{m-1} i_j \cdot j,\ i_2, \ldots, i_{m-1}),$$

if $k = 1$. In either case, μ preserves the action. □

Thus, by Lemmas 5.4, 5.1 and 3.6, if C is a Conway category satisfying the mth power identity, then, $T \models \Gamma(\mathbf{B})$. But by Lemma 5.5, **A** is isomorphic to **B**, so that $T \models \Gamma(\mathbf{A})$. But then, again by Lemma 3.6, $C \models \Gamma(Z_m, Z_m)$. We have proved

LEMMA 5.6 *Suppose that C is a Conway category satisfying the mth power identity, for some $m \geq 1$. Then $C \models \Gamma(Z_m)$.*

THEOREM 5.7 *Let $m \geq 1$ be any fixed integer. The identity $\Gamma(\mathbf{Q})$ associated with an automaton* **Q** *holds in all Conway categories satisfying the mth power identity if and only if $\mathbf{Q} \in \mathcal{SOL}_m$.*

Proof. Suppose that C is a Conway category with $C \models \mathbf{P}_m$. Then, by Lemma 5.6 and Theorem 3.3, C satisfies the identity $\Gamma(\mathbf{Q})$ associated with any automaton $\mathbf{Q} \in \mathcal{SOL}_m$. On the other hand, if $\mathbf{Q} \notin \mathcal{SOL}_m$, then by Theorem 3.3 there is a Conway category C_0 satisfying $\Gamma(Z_m)$ such that $\Gamma(\mathbf{Q})$ does not hold in C_0. But by Lemma 5.4, the mth power identity holds in C_0. □

COROLLARY 5.8 *The identity associated with an automaton* $\mathbf{Q}$ *holds in all Conway categories satisfying all of power identities if and only if* $\mathbf{Q} \in \mathcal{SOL}$.

6 Proof of Theorem 4.2

Suppose that $\mathbf{Q} = (Q, X)$ is an automaton having an identity letter. Recall that X^+ denotes the free semigroup of all nonempty words over X. Below we write X^* for $X^+ \cup \{\lambda\}$, where λ is the empty word.

Let S denote the semigroup $S(\mathbf{Q})$ and let G be a subgroup of S. Since $\mathbf{Q}$ has an identity letter, S is a monoid whose unit is the identity function $Q \to Q$. Moreover, *there is an integer* $k_0 > 0$ *such that for each* $k \geq k_0$, *any function in* S *is induced by a word in* X^+ *of length* k. For the rest of this section, for any integer $n \geq 0$, we denote by X^n the set of all words $u \in X^*$ of length $|u| = n$. Similarly, G^n is the set of all words in G^* of length n.

For a given word $u \in X^+$, we denote by $\overline{u}$ the function $Q \to Q$ induced by u in $\mathbf{Q}$. Also, when $u = g_1 \dots g_n \in G^+$, then we denote by $\overline{u}$ the composite $g_1 \circ \dots \circ g_n$ of the functions $g_1, \dots, g_n$. (Recall that we write composition in S from left to right.) For a state $q \in Q$, we will just write qu for $q\overline{u}$.

Fix an integer $k \geq k_0$. There exists a function $\psi : G^k \to X^k$ such that $\overline{u} = \overline{u\psi}$ for all $u \in G^k$. Given such a function ψ, for every word $u \in G^k$ we define $u\psi_1 = \text{first}_1(u\psi)$ to be the first letter of $u\psi$, and $u\psi_2 = \text{last}_{k-1}(u\psi)$ to be the suffix of length $k-1$ of $u\psi$. Thus, $u\psi = (u\psi_1)(u\psi_2)$.

Let

$$R = \{(i, u, v, w) : i \in [k],\ u \in G^i,\ v \in X^{k-i},\ w \in G^k,\ v = \text{last}_{k-i}(w\psi)\}.$$

We turn R into a G-automaton by defining

$$(i, u, v, w) \circ g = \begin{cases} (i+1, ug, v', w) & \text{if } v = xv' \text{ with } x \in X \\ (1, g, u\psi_2, u) & \text{if } v = \lambda. \end{cases}$$

LEMMA 6.1 *The automaton* $\mathbf{R} = (R, S)$ *is isomorphic to a subautomaton of a cascade composition of a counter of length* k *with aperiodic automata.*

Proof. When $k = 1$ the automaton $\mathbf{R}$ is definite and hence our claim is obvious. Thus, in the rest of the argument, we assume that $k > 1$. Let $\mathbf{K}$ denote the counter $([k], \{z\})$ such that z induces the cyclic permutation $(12 \dots k)$. Let $\mathbf{R}_1 = (G^k, G \times [k])$ and $\mathbf{R}_2 = (X^{k-1}, X \cup X^{k-1})$ be equipped with the following actions:

$$g_1 \cdots g_k \circ (g, i) = \begin{cases} g_1 \cdots g_{i-1} g g_{i+1} \cdots g_k & \text{if } i \neq 1 \\ g g_0^{k-1} & \text{if } i = 1 \end{cases}$$

$$\begin{aligned} x_1 \dots x_{k-1} \circ x &= x_2 \dots x_{k-1} x \\ x_1 \dots x_{k-1} \circ x'_1 \dots x'_{k-1} &= x'_1 \dots x'_{k-1}, \end{aligned}$$

where $i \in [k]$, $g, g_j \in G$, for all $j \in [k]$, and $x, x_j, x'_j \in X$, for all $j \in [k-1]$, and where g_0 denotes a fixed element (say the unit element) of the group G. Moreover, let $\mathbf{R}_3$ be the automaton $(G^k, G^k \cup \{z\})$ with action

$$\begin{aligned} u \circ v &= v \\ u \circ z &= u, \end{aligned}$$

for all $u, v \in G^k$.

Define the cascade composition $\mathbf{R}' = \mathbf{K} \times \mathbf{R}_1 \times \mathbf{R}_2 \times \mathbf{R}_3[G, \varphi_1, \varphi_2, \varphi_3, \varphi_4]$ as follows. For all $i \in [k]$, $u \in G^k$, $v \in X^{k-1}$ and $g \in G$,

$$\begin{aligned} \varphi_1(g) &= z \\ \varphi_2(i, g) &= \begin{cases} (g, i+1) & \text{if } i < k \\ (g, 1) & \text{if } i = k \end{cases} \\ \varphi_3(i, u, g) &= \begin{cases} x_0 & \text{if } i < k \\ \psi_2(u) & \text{if } i = k \end{cases} \\ \varphi_4(i, u, v, g) &= \begin{cases} z & \text{if } i < k \\ u & \text{if } i = k, \end{cases} \end{aligned}$$

where x_0 is any fixed element of X. It follows that the map

$$(i, u, v, w) \mapsto (i, u g_0^{k-i}, v x_0^{i-1}, w),$$

where $i \in [k]$, $u \in G^i$, $v \in X^{k-i}$, $w \in G^k$, defines an injective homomorphism $\mathbf{R} \to \mathbf{R}'$. Moreover, all the automata $\mathbf{R}_i$, $i = 1, 2, 3$ are aperiodic, in fact $\mathbf{R}_2$ is definite and $\mathbf{R}_3$ is an identity-reset automaton. (Alternatively, one may refer to the Krohn-Rhodes theorem by showing that each of the automata $\mathbf{R}_i$ can be embedded in a cascade composition of $\mathbf{U}$ with itself.) □

COROLLARY 6.2 *If C is a Conway category satisfying the identity $\mathbf{P}_k$, then $C \models \Gamma(\mathbf{R})$.*

Proof. This is immediate from Lemmas 6.1, 3.5 and 3.6. □

Since G is a subgroup of S, there exists a nonempty set $Q_G \subseteq Q$ which is closed under the functions in G and such that (Q_G, G), equipped with the natural action, is a transformation group having a faithful action. See [11]. Thus, each $g \in G$ defines a permutation $Q_G \to Q_G$, moreover, the unit element of G defines the identity function $Q_G \to Q_G$, and finally, for all $g_1, g_2 \in G$ we have $g_1 = g_2$ if and only if $qg_1 = qg_2$, for all $q \in Q_G$.

Now let $\mathbf{M}$ be the cascade composition

$$\mathbf{M} = \mathbf{R} \times \mathbf{Q}[G, \varphi_1, \varphi_2]$$

determined by the identity function $\varphi_1 : G \to G$ and the function $\varphi_2 : R \times G \to X$,

$$\varphi_2((i,u,v,w),g) \quad = \quad \begin{cases} x & \text{if } v = xv' \text{ and } x \in X \\ u\psi_1 & \text{if } v = \lambda. \end{cases}$$

(Note that the definition of φ_2 does not depend on g.) Let $\mathbf{M}' = (M', G)$ be the subautomaton of $\mathbf{M}$ determined by those states

$$((i,u,v,w),q) \in R \times Q$$

such that there exists a $q_1 \in Q_G$ with $q_1 v' = q$, where $v' \in X^i$ is the word $\text{first}_i(w\psi)$. (Such a state $q_1 \in Q_G$ is unique, since $v'v = w\psi$ induces a permutation of Q_G.) Below we will denote q_1 by q^{-1}. Note also that $qvu = q^{-1}v'vu = q^{-1}wu \in Q_G$.

LEMMA 6.3 *Suppose that $\mathcal{C}$ is a Conway category satisfying $\mathbf{P}_k$ and the identity $\Gamma(\mathbf{Q})$. Then $\mathcal{C} \models \Gamma(\mathbf{M})$ and $\mathcal{C} \models \Gamma(\mathbf{M}')$.*

Proof. This follows from Corollary 6.2, Lemma 3.6 and Lemma 3.5. □

Let $\mathbf{Q}_G$ denote the transformation group (Q_G, G).

LEMMA 6.4 *The automaton $\mathbf{M}'$ is isomorphic to the direct product $\mathbf{R} \times \mathbf{Q}_G$ of $\mathbf{R}$ and $\mathbf{Q}_G$. An isomorphism $h : \mathbf{M}' \to \mathbf{R} \times \mathbf{Q}_G$ is given by the map*

$$((i,u,v,w),q) \quad \mapsto \quad ((i,u,v,w),qvu), \qquad \textit{all } ((i,u,v,w),q) \in M'.$$

Proof. We have already noted that $qvu = q^{-1}wu \in Q_G$. Also, if $((i,u,v,w),q_1)$ and $((i,u,v,w),q_2)$ are both in M', then $q_1^{-1} \neq q_2^{-1}$, so that $q_1vu = q_1^{-1}wu \neq q_2^{-1}wu = q_2vu$, since w and u induce permutations $Q_G \to Q_G$. This proves that h is injective. To see that h is also surjective, suppose that $((i,u,v,w),q') \in R \times Q_G$. Let q_1 be the state in Q_G with $q_1wu = q'$. This state exists, since w and u induce permutations $Q_G \to Q_G$. Then let $q = q_1v'$, where $v'v = w\psi$. We have $((i,u,v,w),q) \in M'$ and $h : ((i,u,v,w),q) \mapsto ((i,u,v,w),q')$. It is straightforward to check that h is a homomorphism. □

COROLLARY 6.5 *Suppose that $\mathcal{C}$ is a Conway category satisfying the kth power identity. If $\mathcal{C} \models \Gamma(\mathbf{Q})$, then $\mathcal{C} \models \Gamma(G)$.*

Proof. By Lemma 6.3, we have $\mathcal{C} \models \Gamma(\mathbf{M}')$. Also, by Corollary 6.2, $\mathcal{C} \models \Gamma(\mathbf{R})$. Thus, by Lemma 3.6 and Lemma 6.4, $\mathcal{C} \models \Gamma(\mathbf{Q}_G)$. Since the action of G on Q_G is faithful, $S(\mathbf{Q}_G)$ is isomorphic to G, and thus the automaton (G,G), equipped with the natural self action is isomorphic to a subautomaton of a direct power of $\mathbf{Q}_G$. It follows that $\mathcal{C} \models \Gamma(G)$. □

We are now ready to complete the proof of Theorem 4.2.

Proof of Theorem 4.2. Suppose that $\mathcal{C}$ is a Conway category satisfying the identities in $\Gamma(\mathcal{Q})$ as well as the nth power identity for some $n > 1$. If $\mathbf{Q} \in \mathcal{Q}$, then by Lemma 5.1, $\mathcal{C} \models \Gamma(\mathbf{Q}^1)$. Also, by Lemma 5.3, $\mathcal{C} \models \mathbf{P}_{n^k}$, for all $k \geq 1$. Since for some k all functions in $S(\mathbf{Q}^1)$ are induced by a word of $\mathbf{Q}^1$

of length n^k, by Corollary 6.5 we have $\mathcal{C} \models \Gamma(G)$ for any subgroup G of $S(\mathbf{Q})$. Thus, by Theorem 3.3, $\mathcal{C} \models \Gamma(S(\mathbf{Q}))$. We conclude that $\mathcal{C}$ satisfies the identity associated with the semigroup of any automaton in $\mathcal{Q}$. From this the result follows by Theorem 3.3. □

Proof of Corollary 4.3. One direction is obvious from Theorem 4.2.

For the other direction suppose that we have $\mathcal{C} \models \Gamma(\mathbf{Q})$ for all Conway categories $\mathcal{C}$ with $\mathcal{C} \models \Gamma(\mathcal{Q})$. Let $\mathcal{G}$ denote the class of simple groups dividing the semigroups of the automata in $\mathcal{Q}$. Then, by Theorem 3.3, $\mathcal{C} \models \Gamma(\mathbf{Q})$ holds for all Conway categories $\mathcal{C}$ with $\mathcal{C} \models \Gamma(\mathcal{G})$. Thus, again by Theorem 3.3, any simple group divisor of $S(\mathbf{Q})$ is in $\mathcal{G}$. □

7 Proof of Theorem 4.5

For each $n \geq 3$, consider the automaton $\mathbf{Q}_n = ([n], X)$ such that $X = \{x, y\}$ with x inducing the transposition (12) and y inducing the cyclic permutation $(12\ldots n)$. From Corollary 4.4 we immediately have

COROLLARY 7.1 *The Conway identities and the equations $\Gamma(\mathbf{Q}_n)$, $n \geq 3$ are complete for iteration theories.*

LEMMA 7.2 *For each $n \geq 3$, and for any Conway category $\mathcal{C}$,*

$$\mathcal{C} \models \mathbf{S}_n \quad \Leftrightarrow \quad \mathcal{C} \models \Gamma(\mathbf{Q}_n).$$

Proof. Let $f : A^2 \times C \longrightarrow A$ in a Conway category $\mathcal{C}$, and let g denote the morphism on the left hand side of the equation defining $\mathbf{S}_n$. Below we will write π_i^n for $\pi_i^{A^n}$ and $!_k$ for $!_{A^k}$. Morphism Δ_2 is the diagonal $\langle \mathrm{id}_A, \mathrm{id}_A \rangle : A \longrightarrow A^2$. Note that

$$\begin{aligned} f_{\mathbf{Q}_n} \;=\; & \langle !_1 \times f \cdot (\Delta_2 \times !_{n-3} \times \mathrm{id}_C),\ f \cdot (\mathrm{id}_A \times !_1 \times \mathrm{id}_A \times !_{n-3} \times \mathrm{id}_C), \\ & f \cdot (\langle \pi_3^n, \pi_4^n \rangle \times \mathrm{id}_C),\ \ldots,\ f \cdot (\langle \pi_{n-1}^n, \pi_n^n \rangle \times \mathrm{id}_C),\ f \cdot (\langle \pi_n^n, \pi_1^n \rangle \times \mathrm{id}_C) \rangle. \end{aligned}$$

We will show that

$$\begin{aligned} (f_{\mathbf{Q}_n})^\dagger \;=\; & \langle g,\ f \cdot \langle g, (f^\dagger)^{n-2} \cdot \langle g, \mathrm{id}_C \rangle, \mathrm{id}_C \rangle,\ (f^\dagger)^{n-2} \cdot \langle g, \mathrm{id}_C \rangle,\ \ldots \\ & \ldots,\ f^\dagger \cdot \langle g, \mathrm{id}_C \rangle \rangle. \end{aligned} \tag{6}$$

Indeed, by using Sublemma 5.2, one derives

$$\begin{aligned} (f_{\mathbf{Q}_n})^\dagger \;=\; & \langle !_1 \times f \cdot (\Delta_2 \times !_{n-2} \times \mathrm{id}_C),\ f \cdot (\mathrm{id}_A \times !_1 \times \mathrm{id}_A \times !_{n-3} \times \mathrm{id}_C), \\ & f^\dagger \cdot (\pi_4^n \times \mathrm{id}_C),\ \ldots,\ f^\dagger \cdot (\pi_{n-1}^n \times \mathrm{id}_C),\ f^\dagger \cdot (\pi_1^n \times \mathrm{id}_C) \rangle^\dagger. \end{aligned}$$

Thus, again by the Conway identities,

$$\begin{aligned} (f_{\mathbf{Q}_n})^\dagger \;=\; & \langle !_1 \times f \cdot (\Delta_2 \times !_{n-2} \times \mathrm{id}_C),\ f \cdot (\mathrm{id}_A \times !_1 \times \mathrm{id}_A \times !_{n-3} \times \mathrm{id}_C), \\ & (f^\dagger)^{n-2} \cdot (\pi_1^n \times \mathrm{id}_C),\ \ldots,\ f^\dagger \cdot (\pi_1^n \times \mathrm{id}_C) \rangle^\dagger \\ =\; & \langle g,\ f \cdot \langle g, (f^\dagger)^{n-2} \cdot \langle g, \mathrm{id}_C \rangle, \mathrm{id}_C \rangle,\ (f^\dagger)^{n-2} \cdot \langle g, \mathrm{id}_C \rangle,\ \ldots,\ f^\dagger \cdot \langle g, \mathrm{id}_C \rangle \rangle. \end{aligned}$$

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

$$\pi_1^n \cdot (f_{\mathbf{Q}_n})^\dagger = (f \cdot (\Delta_2 \times \mathrm{id}_C))^\dagger = f^{\dagger\dagger}.$$

But then,

$$\begin{aligned} f^\dagger \cdot \langle g, \mathrm{id}_C \rangle &= f^\dagger \cdot \langle f^{\dagger\dagger}, \mathrm{id}_C \rangle \\ &= f^{\dagger\dagger} \end{aligned}$$

and by induction,

$$(f^\dagger)^i \cdot \langle g, \mathrm{id}_C \rangle = f^{\dagger\dagger},$$

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

$$\begin{aligned} f \cdot \langle g, (f^\dagger)^{n-2} \cdot \langle g, \mathrm{id}_C \rangle, \mathrm{id}_C \rangle &= f \cdot \langle f^{\dagger\dagger}, f^{\dagger\dagger}, \mathrm{id}_C \rangle \\ &= f \cdot (\Delta_2 \times \mathrm{id}_C) \cdot \langle (f \cdot (\Delta_2 \times \mathrm{id}_C))^\dagger, \mathrm{id}_C \rangle \\ &= (f \cdot (\Delta_2 \times \mathrm{id}_C))^\dagger \\ &= f^{\dagger\dagger}. \end{aligned}$$

Thus, if $C \models \mathbf{S}_n$, then, by (6),

$$(f_{\mathbf{Q}_n})^\dagger = \Delta_n \cdot (f \cdot (\Delta_2 \times \mathrm{id}_C))^\dagger = f^{\dagger\dagger},$$

proving $C \models \Gamma(\mathbf{Q}_n)$. The converse implication is now obvious. □

Proof of Theorem 4.5. By Corollary 7.1, the Conway identities and the equations $\Gamma(\mathbf{Q}_n)$, $n \geq 3$ are complete. But by Lemma 7.2, in Conway categories each identity $\Gamma(\mathbf{Q}_n)$ is equivalent to the equation $\mathbf{S}_n$. □

References

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

[2] L. Bernátsky and Z. Ésik, Semantics of flowchart programs and the free Conway theories. *Theoretical Informatics and Applications*, 32(1998), 35–78.

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

[4] S.L. Bloom and Z. Ésik, Fixed point operations on ccc's. Part 1. *Theoretical Computer Science*, 155(1996), 1–38.

[5] S.L. Bloom and Z. Ésik, The equational logic of fixed points. *Theoretical Computer Science*, 179(1997), 1–60.

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

[7] S. Eilenberg, *Automata, Languages, and Machines*, vol. B. Academic Press, 1976.

[8] Z. Ésik, Identities in iterative and rational algebraic theories. *Computational Linguistics and Computer Languages*, 14(1980), 183-207.

[9] Z. Ésik, Group axioms for iteration. *Information and Computation.* To appear.

[10] Z. Ésik, The power of the group axioms for iteration. *International J. Algebra and Computation.* To appear.

[11] F. Gécseg, *Products of Automata*, Springer, 1986.

[12] G. Lallement, *Semigroups and Combinatorial Applications.* Wiley-Interscience, 1979.