INFORMATIQUE THÉORIQUE ET APPLICATIONS

L. BERNÁTSKY
Z. ÉSIK

Semantics of flowchart programs and the free Conway theories

Informatique théorique et applications, tome 32, n° 1-3 (1998), p. 35-78.

<http://www.numdam.org/item?id=ITA_1998__32_1-3_35_0>

Informatique théorique et Applications/Theoretical Informatics and Applications
(vol. 32, n° 1-2-3, 1998, pp. 35-78)

SEMANTICS OF FLOWCHART PROGRAMS AND THE FREE CONWAY THEORIES (*)

by L. BERNÁTSKY (1) and Z. ÉSIK (2)

Communicated by W. BRAUER

Abstract. – *Several useful identities involving the fixed point or iteration operation are consequences of just the Conway theory axioms. In this paper we give several characterizations of the free Conway theories including a concrete description based on "aperiodic" homomorphisms of flowchart schemes. It follows from this concrete description that the equations that hold in Conway theories are exactly the valid "group-free" equations of iteration theories, moreover, the equational theory of Conway theories is* **PSPACE***-complete.* © Elsevier, Paris

Résumé. – *Plusieurs identités mettant en jeu les opérateurs de point fixe ou d'itération sont conséquences des seuls axiomes de la théorie de Conway. Nous donnons dans ce papier plusieurs caractérisations des théories libres de Conway, dont une description concrète basée sur des morphismes "apériodiques" de systèmes d'organigrammes. Cette description concrète entraîne que les équations valides dans les théories de Conway sont exactement les équations valides "sans-groupes" des théories d'itération, et de plus, que la théorie équationnelle des théories de Conway est* **PSPACE***-complète.* © Elsevier, Paris

1. INTRODUCTION

The algebraic study of flowchart schemes and flowchart algorithms was initiated in [13] and further developed in [3, 20, 7], to mention only a few references. Schemes may be defined as locally ordered, vertex labeled, finite digraphs with distinguished begin and exit nodes, each labeled by a

(*) Received November 7, 1995, accepted October 30, 1997.

(1) A. József University, Department of Computer Science, Árpád tér 2. H-6720 Szeged, Hungary. Email: benny@inf.u-szeged.hu

Partially supported by the Soros Foundation-Hungary, and by grant F022514 of the National Foundation for Scientific Research of Hungary.

(2) A. József University, Department of Computer Science, Árpád tér 2. H-6270 Szeged, Hungary. Email: esik@inf.u-szeged.hu

Supported in part by grant T22423 of the National Foundation for Scientific Research of Hungary, the Alexander von Humboldt Foundation, and the US-Hungarian Joint Fund under grant no. 351.

Informatique théorique et Applications/Theoretical Informatics and Applications
0988-5004/98/01-02-03/© Elsevier-Paris

non-negative integer, so that each scheme has source n and target p for some non-negative integers n, p. (We use $\mathbf{N}$ to denote the set of nonnegative integers.) The other nodes are consistently labeled by letters in a ranked or doubly ranked alphabet, or signature. Schemes over a signature Σ are equipped with several constants and the operations of sequential composition, pairing or separated sum, which may be viewed as some sort of parallel composition, and a looping operation called iteration. (The paper [7] uses feedback instead of iteration.) In [3], schemes over a signature Σ have been characterized as the free algebra generated by Σ in a variety of $\mathbf{N} \times \mathbf{N}$-sorted algebras axiomatized by a finite number of equation schemes. See also [20, 7] for refinements of this result.

Besides being $\mathbf{N} \times \mathbf{N}$-sorted algebras, flowchart schemes over a signature Σ may be viewed as a small category whose objects are the integers $\mathbf{N}$ and whose morphisms $n \to p$ are the Σ-schemes with source n and target p. Unless Σ is trivial, coproducts do not exist in this category, so that Σ-schemes do not form an algebraic theory in the sense of Lawvere [18]. Nevertheless, schemes are commonly interpreted in such theories which are enriched by a fixed point operation modeling iteration. For example, the theories $\mathbf{Seq}_A$ of sequacious functions [11] on a set A are used to model the stepwise behavior of flowchart algorithms, while the theories $\mathbf{Pfn}_A$ of partial functions on A serve as semantic models for input-output behavior. Another common class of interpretations of schemes is as continuous functions over cpo's. A scheme may be regarded as the graphical representation of a recursive system of fixed point equations. When A is a cpo with a bottom element, and when each letter in Σ is interpreted as a continuous function on A of appropriate arity, the semantics of a scheme $n \to p$ is a continuous function $A^p \to A^n$, i.e., a morphism $n \to p$ in the theory $\mathbf{Th}_A$ of continuous functions over A. This function is obtained as the least solution of the recursive system of equations corresponding to the scheme.

The theories $\mathbf{Seq}_A$, $\mathbf{Pfn}_A$ and $\mathbf{Th}_A$ are all examples of "iteration theories" originally defined in [1, 2] and [15] and studied in [5]. It is shown in [5] that the variety of iteration theories is generated by the theories $\mathbf{Seq}_A$, where A is a set, or by the theories $\mathbf{Th}_A$, where A is a cpo with a bottom element. (The theories of the form $\mathbf{Pfn}_A$ generate the subvariety consisting of the iteration theories with a unique morphism $1 \to 0$.) Thus two schemes are strongly equivalent, i.e. equivalent under all interpretations in the theories $\mathbf{Seq}_A$ (or in the theories $\mathbf{Th}_A$) iff they are equivalent under all interpretations in iteration theories. For this reason iteration theories may be called the "standard" interpretations for flowchart schemes.

It is shown in [5] that the problem of deciding whether an equation holds in all iteration theories can be solved in polynomial time, i.e., the equational theory of iteration theories belongs to **P**. It follows that the strong equivalence problem of flowchart schemes is also in **P**.

In this paper we obtain corresponding results about "nonstandard" interpretations of flowchart schemes. By a nonstandard interpretation we mean a theory enriched with an iteration operation satisfying all equations true of flowcharts. One of the main results, Theorem 3.1 shows that these theories are exactly the *Conway theories*, axiomatized by a small set of equations including the well-known composition identity (11) which implies Elgot's fixed point equation (12). See [5]. Thus the least congruence on Σ-schemes whose quotient is a theory gives the free Conway theory on Σ. The second main result, Theorem 6.1, provides an explicit description of the free Conway theories. The description uses aperiodic morphisms of flowchart schemes, a concept borrowed from automata theory. See [19]. It follows that the equations that hold in Conway theories are exactly the valid "group-free" equations of iteration theories. Finally, we use the explicit description to prove that the Conway-equivalence problem of flowchart schemes is **PSPACE**-complete, cf. Theorem 6.2. It then follows that the equational theory of Conway theories is also **PSPACE**-complete. Theorems 3.1 and 6.1 answer open problems raised in [3] and [5].

Aside from serving as nonstandard interpretation domains for flowchart schemes, our interest in Conway theories stems from several mathematical facts. First, iteration theories are axiomatized by the Conway theory axioms together with a complicated equation scheme, the *commutative identity* [15], or the *group-identities* [14]. (This latter result may be seen as a generalization of Krob's result [17] confirming a conjecture of Conway [9] on the axiomatization of the regular identities.) Comparing the structure of the free Conway theories with that of the free iteration theory, we obtain a clear picture of that part of the equational theory of iteration theories which is captured by the commutative identity, or the group identities. Also, our work explains the role of the commutative identity: it separates nonstandard models from the standard ones by equations. Second, Conway theories are interesting in themselves.

- In a matrix theory [12, 5] equipped with a unary operation $a \mapsto a^*$, the Conway axioms are the two well-known sum and product identities

$$(a + b)^* = (a^* b)^* a^* \tag{1}$$

and

$$(ab)^* = a(ba)^*b + 1. \tag{2}$$

Conway's book [9] contains many interesting identities which are consequences of just the Conway axioms. See also [17, 16].

- It is shown in [5], that a general Kleene-type theorem is a logical consequence of just the Conway axioms.
- It was proved in [4] that the soundness, and relative completeness of the Floyd-Hoare calculus in expressive models, is a consequence of the Conway theory axioms. Thus, even under nonstandard interpretations, one can reason about the correctness of flowchart programs using the Floyd-Hoare rules.

1.1. Basic notions and notations

The set of positive integers is denoted $[\omega]$. Recall that $\mathbf{N}$ is the set of nonnegative integers. For $n \in \mathbf{N}$, $[n]$ denotes the set $\{1, 2, \ldots, n\}$, so that $[0]$ is just another name for the empty set $\emptyset$. A *ranked set* or *signature* is a set Σ of symbols each having a specified rank in $\mathbf{N}$. The collection of those symbols having rank r is denoted Σ_r. For a set A, A^* is the set of all finite words over A, including the empty word ϵ. For a binary relation $f \subseteq A \times B$,

$$\mathrm{dom}(f) := \{a \in A \mid \exists b \in B\ (a, b) \in f\}$$

and

$$\mathrm{rng}(f) := \{b \in B \mid \exists a \in A\ (a, b) \in f\}$$

are the domain and the range of f, respectively. The inverse of the relation f is denoted f^{-1}. When f is a partial function $A \to B$, its kernel $\ker_f$ is the equivalence relation on $\mathrm{dom}(f)$ defined by

$$x \ker_f y \quad \Leftrightarrow \quad f(x) = f(y),$$

for all $x, y \in \mathrm{dom}(f)$. Suppose that S is a set and ρ is an equivalence relation on S. Then S/ρ is the set of all equivalence classes of ρ and, for an element $s \in S$, s/ρ is the equivalence class of s. The composite of two relations $\alpha \subseteq A \times B$ and $\beta \subseteq B \times C$ is denoted $\alpha \circ \beta$, or just $\alpha\beta$.

2. FROM CATEGORIES TO ITERATION THEORIES

A (small) category $\mathcal{C}$ consists of a set $Ob(\mathcal{C})$ of *objects*, and for each pair a, b of objects, a set $\mathcal{C}(a, b)$ of *morphisms* or *arrows* with source a and target

b. We write $f : a \to b$ to indicate that f is a morphism having source a and target b. A category is equipped with an operation of composition

$$\begin{aligned} \mathcal{C}(a,b) \times \mathcal{C}(b,c) &\to \mathcal{C}(a,c) \\ (f,g) &\mapsto f \cdot g, \end{aligned}$$

for all triples a, b, c of objects in $\mathcal{C}$. There is a distinguished morphism $\mathbf{1}_a : a \to a$ for each object a. The composition operation is required to be associative, when defined, and the morphisms $\mathbf{1}_a$ are neutral elements with respect to composition, i.e.,

$$\mathbf{1}_a \cdot f \quad = \quad f \quad = \quad f \cdot \mathbf{1}_b,$$

for all objects a, b and morphisms $f : a \to b$.

An **N**-category is a category whose objects are the nonnegative integers. An **algebraic theory**, or **theory** for short, is an **N**-category T such that for each $n \geq 0$, there are n **distinguished morphisms**

$$i_n : 1 \to n$$

with the following **coproduct property**. For any $p \geq 0$ and each family $f_1, \ldots, f_n$ of morphisms $1 \to p$ there is a unique morphism $f : n \to p$ such that

$$i_n \cdot f = f_i,$$

for all $i \in [n]$. The morphism f determined by the family f_i, $i \in [n]$, is called the **(source) tupling** of the family, and is denoted

$$\langle f_1, \ldots, f_n \rangle.$$

Lastly, the distinguished morphism $1_1 : 1 \to 1$ is the identity $\mathbf{1}_1$, i.e., $1_1 = \mathbf{1}_1$. It follows that

$$\mathbf{1}_n = \langle 1_n, \ldots, n_n \rangle$$

and

$$f = \langle f \rangle, \qquad f : 1 \to p$$

hold in every theory.

The source tupling of the empty family of morphisms $1 \to p$ yields a unique morphism $0_p : 0 \to p$, for all $p \geq 0$. Morphisms formed from the

distinguished morphisms i_n with source tupling are called **base morphisms**. A theory T is called **nontrivial** if the two base morphisms 1_2 and 2_2 are different in T. If T is a nontrivial theory, the base morphisms form a subtheory in T isomorphic to the theory **Tot** of all functions $[n] \to [p]$. In **Tot**, composition is function composition, the identity morphism $\mathbf{1}_n : n \to n$ is the identity function $\mathrm{id}_{[n]} : [n] \to [n]$, and for each $i \in [n]$, $n \geq 0$, the distinguished morphism $i_n : 1 \to n$ is the constant function with value i. We call a base morphism $\rho : n \to p$ surjective/injective if the corresponding function $\rho : [n] \to [p]$ is surjective/injective.

In every theory, the tupling operation can be generalized to morphisms having a common target but arbitrary source by defining

$$\langle f^{(1)}, \ldots, f^{(k)} \rangle := \langle f_1^{(1)}, \ldots, f_{n_1}^{(1)}, \ldots, f_1^{(k)}, \ldots, f_{n_k}^{(k)} \rangle,$$

for all $k \geq 0$ and morphisms $f^{(i)} : n_i \to p$, $i \in [k]$, where $f_j^{(i)}$ denotes the jth component $j_{n_i} \cdot f^{(i)}$ of $f^{(i)}$. From now on, by tupling we mean this generalized tupling operation. In the special case $k = 2$ we call this operation **pairing**.

Suppose T and T' are theories. A **theory morphism** $\varphi : T \to T'$ is a function mapping each morphism $t : n \to p$ in T to a morphism $t\varphi : n \to p$ in T', $n, p \geq 0$. Moreover, φ preserves the composition operation and the distinguished morphisms i_n, $n > 0$, $i \in [n]$. It follows that φ preserves the tupling operation and the identity morphisms $\mathbf{1}_n$. Thus any theory morphism determines a functor which preserves coproducts. Theories and theory morphisms form a category TH. Note that **Tot** is initial object in TH, i.e., for any theory T, there exists a unique theory morphism $\mathbf{Tot} \to T$.

Algebraic theories can be considered as $\mathbf{N} \times \mathbf{N}$-sorted algebras, where the elements of sort (n, p) are all morphisms $f : n \to p$. As an algebra, a theory has operations of tupling and composition together with constants i_n, for all $n > 0$, $i \in [n]$. Each theory satisfies the following **theory identities**:

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h \tag{3}$$

$$\mathbf{1}_n \cdot f = f \tag{4}$$

$$f \cdot \mathbf{1}_p = f \tag{5}$$

$$i_n \cdot \langle f_1, \ldots, f_n \rangle = f_i \tag{6}$$

$$\langle 1_n \cdot f, \ldots, n_n \cdot f \rangle = f \tag{7}$$

$$\mathbf{1}_1 = 1_1, \tag{8}$$

for all $f : n \to p$, $g : p \to q$, $h : q \to r$, and $f_j : 1 \to p$, for $j \in [n]$. Here we regard $\mathbf{1}_n$ as an abbreviation for $\langle 1_n, \ldots, n_n \rangle$. The empty tuple of elements with target p is denoted 0_p. When $n = 0$, equation (7) takes the form

$$0_p = f,$$

for all $f : 0 \to p$. These equations provide an axiomatization of the class of all algebraic theories.

In any theory T, the **separated sum** operation is defined by

$$f \oplus g := \langle f \cdot \kappa_{p,q},\ g \cdot \lambda_{p,q} \rangle : n + m \to p + q,$$

for all morphisms $f : n \to p$ and $g : m \to q$, where

$$\kappa_{p,q} = \langle 1_{p+q}, \ldots, p_{p+q} \rangle : p \to p + q$$

and

$$\lambda_{p,q} = \langle (p+1)_{p+q}, \ldots, (p+q)_{p+q} \rangle : q \to p + q.$$

A **preiteration theory** T is a theory equipped with an **iteration** or **dagger** operation, mapping each morphism $f : n \to n+p$ to a morphism $f^\dagger : n \to p$. Preiteration theories are the objects of the category $\mathrm{TH}^\dagger$. The morphisms of $\mathrm{TH}^\dagger$, called **preiteration theory morphism**, are those theory morphisms which preserve the dagger operation.

A **Conway theory** is a preiteration theory which satisfies the following **Conway identities**:

PARAMETER IDENTITY

$$(f \cdot (\mathbf{1}_n \oplus g))^\dagger = f^\dagger \cdot g, \tag{9}$$

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

DOUBLE DAGGER IDENTITY

$$(f \cdot (\langle \mathbf{1}_n, \mathbf{1}_n \rangle \oplus \mathbf{1}_p))^\dagger = f^{\dagger\dagger}, \tag{10}$$

for all $f : n \to 2n + p$.

COMPOSITION IDENTITY

$$(f \cdot \langle g, 0_n \oplus \mathbf{1}_p \rangle)^\dagger = f \cdot \langle (g \cdot \langle f, 0_m \oplus \mathbf{1}_p \rangle)^\dagger,\ \mathbf{1}_p \rangle, \tag{11}$$

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

The term "Conway identities" comes from the form these identities take in matrix theories over semirings equipped with a * operation, see [5]. For example, the double dagger identity corresponds to the equation (1), and the composition identity to the equation (2). Note that every Conway theory satisfies Elgot's *fixed point identity*

$$f^\dagger = f \cdot \langle f^\dagger, \mathbf{1}_p \rangle, \tag{12}$$

for all $f : n \to n + p$. In *-semirings the fixed point identity takes the form

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

A Conway theory T is called an **iteration theory** if it satisfies the following complicated equation scheme, the **commutative identity**:

$$\langle 1_m \cdot \rho \cdot f \cdot (\rho_1 \oplus \mathbf{1}_p), \ldots, m_m \cdot \rho \cdot f \cdot (\rho_m \oplus \mathbf{1}_p) \rangle^\dagger = \rho \cdot (f \cdot (\rho \oplus \mathbf{1}_p))^\dagger,$$

where $f : n \to m + p$, $\rho : m \to n$ is a surjective base morphism and $\rho_1, \ldots, \rho_m : m \to m$ are base morphisms with $\rho_i \cdot \rho = \rho$, $i \in [m]$.

As many-sorted algebras, both Conway theories and iteration theories form an equational class, so that all free Conway and iteration theories exist. A concrete description of the free iteration theories has been known for a long time, see [5], or Section 5.

Although Conway theories have a much simpler axiomatization than iteration theories, no concrete description of the free Conway theories was known until now. Another interesting aspect is that in spite of the complicated axiomatization of iteration theories, it is decidable in polynomial time if an equation holds in all iteration theories, i.e., the equational theory of iteration theories is in **P**. In contrast of this fact, we prove at the end of the paper that the equational theory of Conway theories is **PSPACE**-complete. Thus, it is very unlikely to find an efficient (polynomial-time) algorithm which would decide if an equation is a logical consequence of the Conway theory axioms.

3. FLOWCHART SCHEMES

In order to help the reader understand the rather uninformative (but technically useful) definition of a flowchart scheme, we begin with an informative definition. Suppose Σ is a signature. A flowchart scheme over Σ, or Σ-scheme for short, is a labeled finite directed graph $\mathcal{S}$. There are three types of nodes of $\mathcal{S}$: input or begin nodes, output or exit nodes, and

internal nodes or states. A Σ-scheme $\mathcal{S}$ having n input nodes and p output nodes is called a scheme from n to p, written $\mathcal{S} : n \to p$. The ith input node of $\mathcal{S}$ is labeled by in_i and the jth output node is labeled by out_j, for each $i \in [n]$ and $j \in [p]$. The states are labeled by symbols σ in Σ. Input nodes have in-degree 0 and out-degree at most 1. Output nodes have out-degree 0. A state s with label $\sigma \in \Sigma_m$ has out-degree at most m and each edge starting from s is labeled by some integer $i \in [m]$, such that different edges have different labels. There is no restriction on the in-degree of states and output nodes.

A Σ-scheme $\mathcal{S}$ can also be considered as a labeled deterministic finite-state automaton with input alphabet $[\omega]$. In the following "official" definition this automata-theoretic approach is used.

DEFINITION 3.1: *Suppose Σ is a signature. A* **Σ-scheme** *is a 6-tuple $\mathcal{S} = (S, \lambda, \alpha, \delta, n, p)$, where*

S is the finite set of states, $S \cap [\omega] = \emptyset$;

$\lambda : S \to \Sigma$ is the labeling function;

$\alpha : [n] \to S \cup [p]$ is the partial start function;

$\delta : S \times [\omega] \to S \cup [p]$ is the partial transition function satisfying

$$\mathrm{dom}(\delta) \subseteq \{(s,t) \in S \times [\omega] \mid \exists n\, t \leq n \wedge \lambda(s) \in \Sigma_n\},$$

$n \in \mathbf{N}$ is the source of $\mathcal{S}$;

$p \in \mathbf{N}$ is the target of $\mathcal{S}$.

Thus, in the official definition, the input and output nodes are not considered to belong to the scheme. Suppose that $i \in [n]$. If $\alpha(i) = s \in S$, then, in the graphical representation, the ith input node is connected by an edge to the internal node s. When $\alpha(i) = j \in [p]$, the ith input node is connected to the jth output node. If $\alpha(i)$ is not defined, then the ith input node has no outgoing edge. Intuitively, this corresponds to the case that, when the flowchart scheme is entered at the ith input node, the computation represented by the scheme diverges. The transition function is interpreted in the same way. If $\delta(s,i) = s'$, where $s, s' \in S$ and $i \in [\omega]$, then, in the graphical representation, the out-edge of s labeled by i is connected to s', and to the jth output node if $\delta(s,i) = j$. If $\delta(s,i)$ is not defined, then s has no out-edge labeled by i. In [3], partially defined start and transition functions are avoided by adding to each scheme a bottom vertex representing divergence.

We let $\mathcal{S}, \mathcal{S}', \mathcal{F}, \mathcal{G}$ and $\mathcal{H}$ denote schemes with underlying state sets S, S', F, G and H, respectively. When the scheme is $\mathcal{S}$ (or $\mathcal{S}'$, respectively) we denote by λ, α and δ (λ', α' and δ', respectively) the labeling, start and transition functions of $\mathcal{S}$ ($\mathcal{S}'$, respectively). For other schemes $\mathcal{F}$, the default notations are $\lambda_{\mathcal{F}}$, $\alpha_{\mathcal{F}}$ and $\delta_{\mathcal{F}}$. Due to these conventions, in most cases it will be enough to specify the source and target of a scheme $\mathcal{S}$ by writing $\mathcal{S} : n \to p$. Even when a full specification of $\mathcal{S}$ is required, we prefer writing $\mathcal{S} = (S, \lambda, \alpha, \delta) : n \to p$ instead of $\mathcal{S} = (S, \lambda, \alpha, \delta, n, p)$.

We extend δ to a partial function $(S \cup [n]) \times [\omega]^* \to S \cup [p]$ by defining

$$\delta(s,u) := \begin{cases} s & \text{if } u \text{ is the empty word } \epsilon, \\ \delta(\delta(s,t),v) & \text{if } u = tv \text{ for some } t \in [\omega] \text{ and } v \in [\omega]^*, \end{cases}$$

$$\delta(i,u) := \begin{cases} \delta(\alpha(i),u) & \text{if } \alpha(i) \in S, \\ \alpha(i) & \text{if } \alpha(i) \in [p] \text{ and } u = \epsilon, \\ \text{undefined} & \text{otherwise,} \end{cases}$$

for all $i \in [n]$, $s \in S$ and $u \in [\omega]^*$. The partial functions $\delta_u : S \cup [n] \to S \cup [p]$ are defined by

$$\delta_u(s) := \delta(s,u),$$

for all $s \in S \cup [n]$ and $u \in [\omega]^*$. Viewing δ_u as a binary relation from $S \cup [n]$ to $S \cup [p]$, we define

$$\delta_u[C,D] := \delta_u \cap (C \times D),$$

for all $C \subseteq S \cup [n]$ and $D \subseteq S \cup [p]$. Note that $\delta_u[C,D]$ is a partial function $C \to D$. The collection of all *nonempty* partial functions $f : C \to D$ induced by the words in $[\omega]^*$ is denoted $\Delta[C,D]$, i.e.,

$$\Delta[C,D] = \{\delta_u[C,D] \mid u \in [\omega]^*\} \setminus \{\emptyset\}.$$

It is not hard to see that the graph-theoretic and automata-theoretic definitions of a Σ-scheme are equivalent. The only reason we have chosen the automata-theoretic definition is because we believe it makes proofs shorter. Nevertheless, many of the proofs become much easier to understand once a picture has drawn.

DEFINITION 3.2: *Suppose $\mathcal{S} : n \to p$ is a scheme. We say $\mathcal{S}$ is a*

partial base scheme *if it has no states, i.e., if $S = \emptyset$,*

base scheme *if it is a partial base scheme and α is a total function $[n] \to [p]$.*

Note that each (partial) base scheme $\mathcal{S} : n \to p$ is totally determined by (and therefore can be identified with) the (partial) function $\alpha : [n] \to [p]$. We will frequently use the following (partial) base schemes:

For all $n, p, q \in \mathbf{N}$,

$\mathbf{1}_n : n \to n$ is the base scheme determined by the identity function $\mathrm{id}_{[n]} : [n] \to [n]$, see Figure 1,

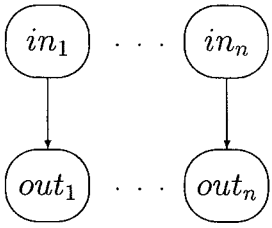

Figure 1. – The base scheme $\mathbf{1}_n : n \to n$.

$0_n : 0 \to n$ is the unique base scheme $0 \to n$, see Figure 2,

Figure 2. – The base scheme $0_n : 0 \to n$.

$i_n : 1 \to n$ is the base scheme determined by the map $1 \mapsto i$, for all $i \in [n]$, see Figure 3,

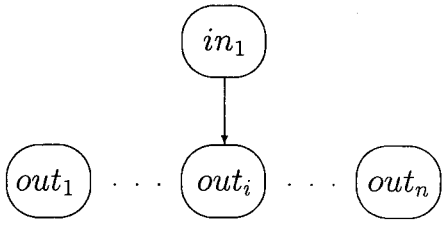

Figure 3. – The base scheme $i_n : 1 \to n$.

$\kappa_{p,q} : p \to p+q$ is the base scheme determined by the inclusion $[p] \to [p+q]$, $x \mapsto x$, see Figure 4,

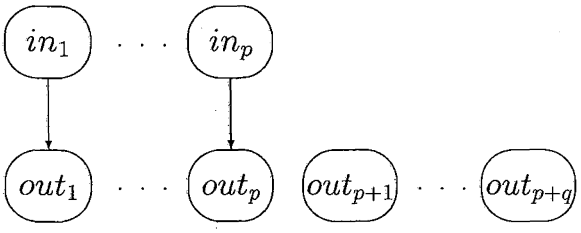

Figure 4. – The base scheme $\kappa_{p,q} : p \to p+q$.

$\lambda_{p,q} : q \to p+q$ is the base scheme determined by the translated inclusion $[q] \to [p+q]$, $x \mapsto p+x$, see Figure 5,

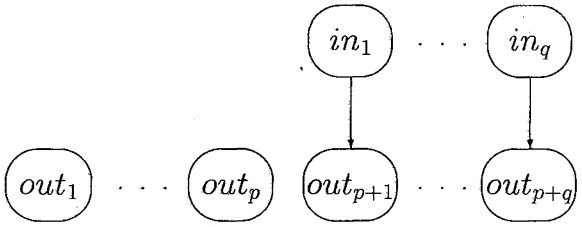

Figure 5. – The base scheme $\lambda_{p,q} : q \to p+q$.

$\perp : 1 \to 0$ is the unique partial base scheme $1 \to 0$, see Figure 6.

Figure 6. – The partial base scheme $\perp : 1 \to 0$.

Two Σ-schemes $\mathcal{S}$ and $\mathcal{S}'$ are called **isomorphic** if they are isomorphic as labeled directed graphs. We identify isomorphic schemes, so that $\mathcal{S} = \mathcal{S}'$ means $\mathcal{S}$ and $\mathcal{S}'$ are isomorphic. Due to this convention, when needed, we may assume without loss of generality that any two schemes $\mathcal{S}$ and $\mathcal{S}'$ have disjoint sets of states.

3.1. The category of Σ-schemes

Σ-schemes $n \to p$ serve as morphisms $n \to p$ in an **N**-category, which we denote by $\Sigma\mathbf{Sch}$. In $\Sigma\mathbf{Sch}$, the identity morphism $\mathbf{1}_n : n \to n$ is the

base scheme $\mathbf{1}_n : n \to n$. Following [13] we define four operations on the morphisms of $\Sigma\mathbf{Sch}$.

DEFINITION 3.3 **Composition**: *Suppose $\mathcal{S} : n \to p$ and $\mathcal{S}' : p \to q$ are Σ-schemes with $S \cap S' = \emptyset$. The Σ-scheme $\mathcal{S} \cdot \mathcal{S}' : n \to q$ has states $S \cup S'$ and satisfies*

$$\lambda_{\mathcal{S}\cdot\mathcal{S}'}(s) = \begin{cases} \lambda(s) & \text{if } s \in S, \\ \lambda'(s) & \text{if } s \in S', \end{cases}$$

$$\alpha_{\mathcal{S}\cdot\mathcal{S}'}(i) = \begin{cases} \alpha(i) & \text{if } \alpha(i) \in S, \\ \alpha'(\alpha(i)) & \text{if } \alpha(i) \in [p], \\ \textit{undefined} & \textit{otherwise}, \end{cases}$$

$$\delta_{\mathcal{S}\cdot\mathcal{S}'}(s,t) = \begin{cases} \delta(s,t) & \text{if } s \in S \text{ and } \delta(s,t) \in S, \\ \alpha'(\delta(s,t)) & \text{if } s \in S \text{ and } \delta(s,t) \in [p], \\ \delta'(s,t) & \text{if } s \in S', \\ \textit{undefined} & \textit{otherwise}, \end{cases}$$

for all $i \in [n]$, $s \in S \cup S'$ and $t \in [\omega]$.

The graph representation of $\mathcal{S} \cdot \mathcal{S}'$ can be constructed from the graph representations of $\mathcal{S} : n \to p$ and $\mathcal{S}' : p \to q$ in the following way: first delete the output nodes of $\mathcal{S}$ and the input nodes of $\mathcal{S}'$ together with all adjacent edges. Then take the disjoint union of the two graphs, and lastly, add a new edge $s \xrightarrow{t} s'$ whenever there was an edge $s \xrightarrow{t} out_j$ in $\mathcal{S}$ and an edge $in_j \longrightarrow s'$ in $\mathcal{S}'$, for some $j \in [p]$. See Figure 7.

DEFINITION 3.4 **Pairing**: *Suppose $\mathcal{S} : n \to p$ and $\mathcal{S}' : m \to p$ are Σ-schemes with $S \cap S' = \emptyset$. The Σ-scheme $\langle \mathcal{S}, \mathcal{S}' \rangle : n + m \to p$ has states $S \cup S'$ and satisfies*

$$\lambda_{\langle \mathcal{S},\mathcal{S}' \rangle}(s) = \begin{cases} \lambda(s) & \text{if } s \in S, \\ \lambda'(s) & \text{if } s \in S', \end{cases}$$

$$\alpha_{\langle \mathcal{S},\mathcal{S}' \rangle}(i) = \begin{cases} \alpha(i) & \text{if } i \in [n], \\ \alpha'(i-n) & \text{if } i \in [n+m] \setminus [n], \end{cases}$$

$$\delta_{\langle \mathcal{S},\mathcal{S}' \rangle}(s,t) = \begin{cases} \delta(s,t) & \text{if } s \in S, \\ \delta'(s,t) & \text{if } s \in S', \end{cases}$$

for all $i \in [n+m]$, $s \in S \cup S'$ and $t \in [\omega]$.

The graph representation of $\langle \mathcal{S}, \mathcal{S}' \rangle$ can be constructed from the graphs of $\mathcal{S} : n \to p$ and $\mathcal{S}' : m \to p$ as follows: first change the label of the ith

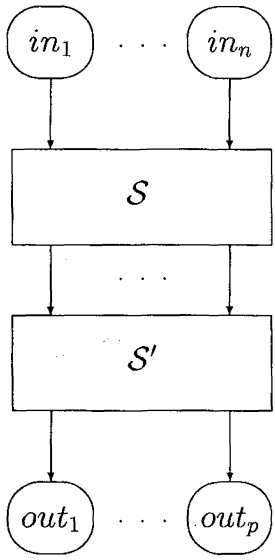

Figure 7. – Composition.

input node of $\mathcal{S}'$ from in_i to in_{n+i}, for each $i \in [m]$. Then take the disjoint union of the graph of $\mathcal{S}$ and the modified graph of $\mathcal{S}'$, and lastly, identify the corresponding output nodes. See Figure 8. As the pairing operation is

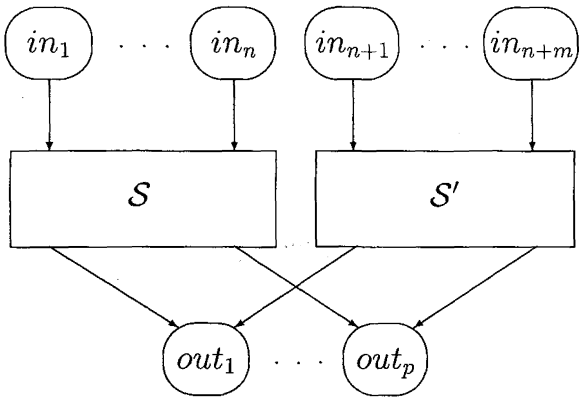

Figure 8. – Pairing.

associative it can be extended to a many-argument tupling operation in a natural way. Note that the empty tuple of Σ-schemes with target p is the base scheme $0_p : 0 \to p$ by definition.

DEFINITION 3.5 **Separated sum**: *Suppose* $\mathcal{S} : n \to p$ *and* $\mathcal{S}' : m \to q$ *are* Σ*-schemes. The separated sum of* $\mathcal{S}$ *and* $\mathcal{S}'$ *is the* Σ*-scheme*

$$\mathcal{S} \oplus \mathcal{S}' := \langle \mathcal{S} \cdot \kappa_{p,q}, \mathcal{S}' \cdot \lambda_{p,q} \rangle : n + m \to p + q.$$

One can construct the graph of $\mathcal{S} \oplus \mathcal{S}'$ in two steps: first change the labels in_i to in_{n+i} and the labels out_j to out_{p+j} in the graph of $\mathcal{S}'$, for all $i \in [m]$ and $j \in [q]$, then take the disjoint union of the two graphs. See Figure 9.

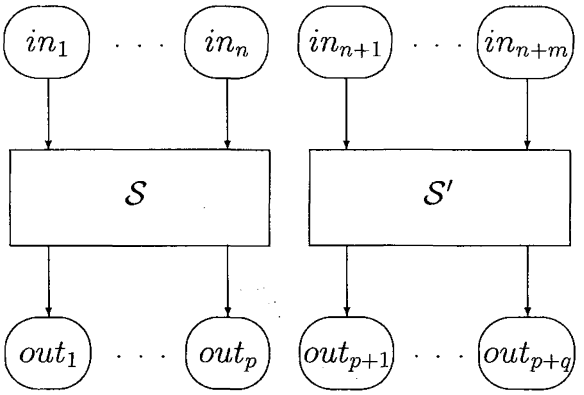

Figure 9. – Separated sum.

REMARK 3.1: *Since separated sum was defined in terms of the other operations and constants, it could be removed from the collection of the basic operations.*

DEFINITION 3.6 **Iteration**: *Suppose* $\mathcal{S} : n \to n + p$ *is a* Σ*-scheme. Then its iterate is the* Σ*-scheme*

$$\mathcal{S}^\dagger = (S, \lambda, \alpha\alpha^*\beta, \delta\alpha^*\beta) : n \to p,$$

where α^* *is the reflexive and transitive closure of* α *considered as a relation* $\alpha \subseteq (S \cup [n+p]) \times (S \cup [n+p])$*, and where* $\beta : S \cup [n+p] \to S \cup [p]$ *is defined by*

$$\beta(s) = s,$$
$$\beta(i) = \begin{cases} i - n & \text{if } i > n, \\ \text{undefined} & \text{if } i \leq n, \end{cases}$$

for all $s \in S$ *and* $i \in [n+p]$.

The graph of $\mathcal{S}^\dagger$ is constructed from the graph of $\mathcal{S} : n \to n+p$ in three steps: first add a new edge $s \xrightarrow{t} s'$ whenever there were edges

$$s \xrightarrow{t} out_{i_1},\ in_{i_1} \longrightarrow out_{i_2},\ in_{i_2} \longrightarrow out_{i_3},\ \ldots,\ in_{i_m} \longrightarrow s',$$

in the original graph of $\mathcal{S}$, for some $i_1, \ldots, i_m \in [n]$, $m > 0$. Then delete the first n output nodes $out_1, \ldots, out_n$ together with all adjacent edges, and lastly, change the labels of the remaining output nodes from out_{n+i} to out_i, for all $i \in [p]$. See Figure 10.

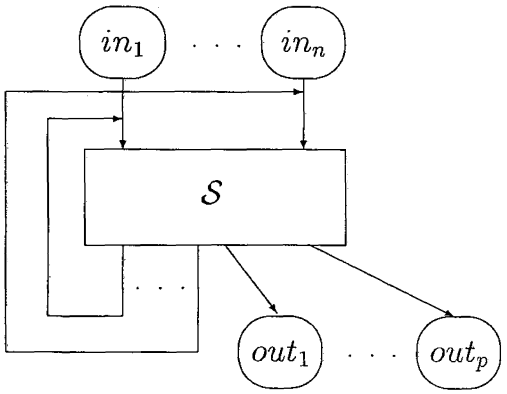

Figure 10. – Iteration.

It is not hard to see that the composition operation of schemes is associative and the base schemes $\mathbf{1}_n$ are left and right units. Thus $\Sigma\mathbf{Sch}$ is a category. On the other hand, $\Sigma\mathbf{Sch}$ can be viewed as an $\mathbf{N} \times \mathbf{N}$-sorted algebra with the four operations defined above along with constants i_n, for all $n > 0$, $i \in [n]$. As such, it is generated by the signature Σ, more precisely, by the inclusion $\eta_\Sigma : \Sigma \to \Sigma\mathbf{Sch}$ mapping each symbol $\sigma \in \Sigma_p$ to the corresponding **atomic scheme** $\widehat{\sigma} : 1 \to p$, see Figure 11. Indeed, each Σ-scheme $\mathcal{S} : n \to p$ can be written as

$$\rho \cdot \langle \langle \widehat{\sigma_1} \cdot \rho_1, \ldots, \widehat{\sigma_m} \cdot \rho_m \rangle^\dagger, \mathbf{1}_p \rangle$$

for some partial base scheme $\rho : n \to m+p$, atomic schemes $\widehat{\sigma_i} : 1 \to p_i$ and partial base schemes $\rho_i : p_i \to m+p$, $i \in [m]$, where $\sigma_i \in \Sigma_{p_i}$ for all $i \in [m]$ and m is the number of states in $\mathcal{S}$. See [13]. Each partial base scheme $\rho : n \to p$ can be expressed uniquely as an n-tuple of some schemes $i_p : 1 \to p$ and $\bot_p : 1 \to p$, where $\bot_p = \bot \cdot 0_p = 1_1^\dagger \cdot 0_p$.

Although $\Sigma\mathbf{Sch}$ is an $\mathbf{N}$-category, it is not a theory: it does not satisfy the theory identities (6) and (7) unless Σ is empty, i.e., when every Σ-scheme

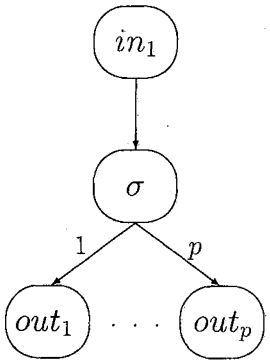

Figure 11. – The atomic scheme $\hat{\sigma} : 1 \to p$.

is a partial base scheme. Interestingly, $\Sigma\mathbf{Sch}$ satisfies two of the defining Conway identities, namely, the parameter and double dagger identities. It also satisfies a weak form of the composition identity:

BASE COMPOSITION IDENTITY

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

for all base schemes $\rho : n \to m+p$ and arbitrary schemes $\mathcal{G} : m \to n+p$.

DEFINITION 3.7: *For each signature* Σ, *let* $\equiv_\Sigma$ *be the least congruence on* $\Sigma\mathbf{Sch}$ *such that the quotient* $\Sigma\mathbf{Sch}/\equiv_\Sigma$ *satisfies the theory identity (7).*

When Σ is understood we omit the subscript in $\equiv_\Sigma$.

LEMMA 3.1: *Suppose* $\mathcal{F} : n \to 2n + m + p$ *and* $\mathcal{G} : m \to 2n + m + p$ *are* Σ*-schemes. Then*

$$\langle \mathcal{F}, \mathcal{F}, \mathcal{G} \rangle^\dagger \equiv \beta \cdot (\langle \mathcal{F}, \mathcal{G} \rangle \cdot (\beta \oplus \mathbf{1}_p))^\dagger,$$

where β *denotes the base scheme* $\langle \mathbf{1}_n, \mathbf{1}_n \rangle \oplus \mathbf{1}_m : 2n + m \to n + m$.

Proof: By the definition of $\equiv$,

$$\begin{aligned} \langle \mathbf{1}_n, \mathbf{1}_n \rangle \cdot \mathcal{F} &\equiv \langle 1_{2n} \cdot \langle \mathbf{1}_n, \mathbf{1}_n \rangle \cdot \mathcal{F}, \ldots, (2n)_{2n} \cdot \langle \mathbf{1}_n, \mathbf{1}_n \rangle \cdot \mathcal{F} \rangle \\ &= \langle 1_n \cdot \mathcal{F}, \ldots, n_n \cdot \mathcal{F}, 1_n \cdot \mathcal{F}, \ldots, n_n \cdot \mathcal{F} \rangle \\ &\equiv \langle \mathcal{F}, \mathcal{F} \rangle. \end{aligned}$$

It follows that

$$\beta \cdot \langle \mathcal{F}, \mathcal{G} \rangle \ = \ \langle \langle \mathbf{1}_n, \mathbf{1}_n \rangle \cdot \mathcal{F}, \mathcal{G} \rangle \ \equiv \ \langle \langle \mathcal{F}, \mathcal{F} \rangle, \mathcal{G} \rangle \ = \ \langle \mathcal{F}, \mathcal{F}, \mathcal{G} \rangle.$$

Thus,

$$\begin{aligned}\langle \mathcal{F}, \mathcal{F}, \mathcal{G}\rangle^\dagger &\equiv (\beta \cdot \langle \mathcal{F}, \mathcal{G}\rangle)^\dagger \\ &= \beta \cdot (\langle \mathcal{F}, \mathcal{G}\rangle \cdot (\beta \oplus \mathbf{1}_p))^\dagger,\end{aligned}$$

by the base composition identity applied to the base scheme $\beta \oplus 0_p : 2n + m \to n + m + p$. □

THEOREM 3.1: *$\Sigma\mathbf{Sch}/\equiv$ is freely generated by the signature Σ in the variety of all Conway theories.*

Proof: It is known that $\Sigma\mathbf{Sch}$ is freely generated by Σ in the smallest variety containing all structures $\Delta\mathbf{Sch}$, for any signature Δ. A complete axiomatization of this variety was given in [3]. Since each of those axioms is a logical consequence of the Conway identities, it follows that the Σ-generated free Conway theory is the quotient $\Sigma\mathbf{Sch}/\sim$, where $\sim$ is the least congruence on $\Sigma\mathbf{Sch}$ for which $\Sigma\mathbf{Sch}/\sim$ is a Conway theory. We are going to show that $\equiv\ = \ \sim$.

The containment $\equiv\ \subseteq\ \sim$ is trivial. The converse containment $\equiv\ \supseteq\ \sim$ is proved by showing that $\Sigma\mathbf{Sch}/\equiv$ is a Conway theory. Except for the composition identity and the two theory identities (6) and (7), all defining axioms of Conway theories hold in $\Sigma\mathbf{Sch}$, and hence in the quotient $\Sigma\mathbf{Sch}/\equiv$. As (7) holds in $\Sigma\mathbf{Sch}/\equiv$ by definition, we are left to show that $\Sigma\mathbf{Sch}/\equiv$ satisfies (6) and the composition identity.

First observe that for any integer $p \geq 0$, $0_p/\equiv$ is the only morphism $0 \to p$ in $\Sigma\mathbf{Sch}/\equiv$. Suppose $\mathcal{F}_1, \ldots, \mathcal{F}_n$ are Σ-schemes $1 \to p$. Then, in $\Sigma\mathbf{Sch}$,

$$\begin{aligned}i_n \cdot \langle \mathcal{F}_1, \ldots, \mathcal{F}_n\rangle &= \langle 0_1 \cdot \mathcal{F}_1, \ldots, 0_1 \cdot \mathcal{F}_{i-1}, \mathcal{F}_i, 0_1 \cdot \mathcal{F}_{i+1}, \ldots, 0_1 \cdot \mathcal{F}_n\rangle \\ &\equiv \langle 0_p, \ldots, 0_p, \mathcal{F}_i, 0_p, \ldots, 0_p\rangle \\ &= \mathcal{F}_i.\end{aligned}$$

Now suppose that $\mathcal{F} : n \to m + p$ and $\mathcal{G} : m \to n + p$ are Σ-schemes and let β denote the base scheme $\langle \mathbf{1}_n, \mathbf{1}_n\rangle \oplus \mathbf{1}_m : 2n + m \to n + m$. Then

$$\begin{aligned}&\mathcal{F} \cdot \langle (\mathcal{G} \cdot \langle \mathcal{F}, 0_m \oplus \mathbf{1}_p\rangle)^\dagger, \mathbf{1}_p\rangle = \\ &= (\mathbf{1}_n \oplus 0_{n+m}) \\ &\cdot \langle \mathcal{F} \cdot (0_{2n} \oplus \mathbf{1}_{m+p}),\ \mathcal{F} \cdot (0_{2n} \oplus \mathbf{1}_{m+p}),\ \mathcal{G} \cdot (0_n \oplus \mathbf{1}_n \oplus 0_m \oplus \mathbf{1}_p)\rangle^\dagger \\ &\equiv (\mathbf{1}_n \oplus 0_{n+m}) \\ &\cdot \beta \cdot (\langle \mathcal{F} \cdot (0_{2n} \oplus \mathbf{1}_{m+p}),\ \mathcal{G} \cdot (0_n \oplus \mathbf{1}_n \oplus 0_m \oplus \mathbf{1}_p)\rangle \cdot (\beta \oplus \mathbf{1}_p))^\dagger \\ &= (\mathbf{1}_n \oplus 0_m) \cdot \langle \mathcal{F} \cdot (0_n \oplus \mathbf{1}_{m+p}),\ \mathcal{G} \cdot (\mathbf{1}_n \oplus 0_m \oplus \mathbf{1}_p)\rangle^\dagger \\ &= (\mathcal{F} \cdot \langle \mathcal{G}, 0_n \oplus \mathbf{1}_p\rangle)^\dagger\end{aligned}$$

by Lemma 3.1 and by the definition of the operations in $\Sigma\mathbf{Sch}$. □

We say that two Σ-schemes are **Conway equivalent** if they are identified by the congruence $\equiv$. Although the previous theorem gives some kind of characterization of $\equiv$, it doesn't give an algorithm to decide the Conway equivalence problem of flowchart schemes. Our next task is to find such an algorithm, based on a structural characterization of $\equiv$.

4. SIMULATIONS

In this subsection we define simulations, i.e., structure preserving relations between schemes. Congruences and homomorphisms of flowchart schemes are then defined as simulations satisfying some further requirements.

In order to simplify our presentation we introduce the following notation: when $f : A \to A'$ and $g : B \to B'$ are partial functions and $\rho \subseteq A' \times B'$ is a binary relation, we write $f(a)\ \rho\ g(b)$ for the statement

$$(a \notin \mathrm{dom}(f) \wedge b \notin \mathrm{dom}(g)) \ \vee\ (f(a), g(b)) \in \rho.$$

DEFINITION 4.1: *Suppose that $\mathcal{S}$ and $\mathcal{S}'$ are Σ-schemes $n \to p$. A binary relation $\gamma \subseteq S \times S'$ is called a* **simulation from $\mathcal{S}$ to $\mathcal{S}'$**, *written $\mathcal{S}\ |\gamma|\ \mathcal{S}'$, if*

$$\alpha(i)\ (\gamma \cup \mathrm{id}_{[p]})\ \alpha'(i) \tag{13}$$

and

$$s\ \gamma\ s' \quad \Rightarrow \quad \lambda(s) = \lambda'(s') \ \wedge\ \delta(s,t)\ (\gamma \cup \mathrm{id}_{[p]})\ \delta'(s',t) \tag{14}$$

hold for all $i \in [n]$, $s \in S$, $s' \in S'$ and $t \in [\omega]$. We write $\mathcal{S} \approx \mathcal{S}'$ and say that the two schemes $\mathcal{S}$ and $\mathcal{S}'$ are **strongly equivalent** *if there exists a simulation from $\mathcal{S}$ to $\mathcal{S}'$. In the special case that the simulation relation γ is a function $S \to S'$, γ is called a* **homomorphism** *from $\mathcal{S}$ to $\mathcal{S}'$. A bijective homomorphism is called an* **isomorphism**. *Another special case is that $\mathcal{S} = \mathcal{S}'$ and the simulation γ is an equivalence relation on S: then we say γ is a* **congruence on** *$\mathcal{S}$.*

Thus, if γ is a simulation from $\mathcal{S}$ to $\mathcal{S}'$, then, by (13) and (14), the following hold for their graphical representations. First, for any $i \in [n]$, the ith input node of $\mathcal{S}$ has an out-edge iff the ith input node of $\mathcal{S}'$ has an out-edge. Moreover, if the ith input node of $\mathcal{S}$ is connected by an edge to an internal node s, then the ith input node of $\mathcal{S}'$ is connected by an edge to an internal node s' with $(s, s') \in \gamma$. If the ith input node of $\mathcal{S}$ is connected to an

output node, then the ith input node of $\mathcal{S}'$ is connected to the corresponding output node of $\mathcal{S}'$. And if $s \in S$ and $s' \in S'$ with $(s, s') \in \gamma$, then, by (14), s and s' have the same label, and for any $t \in [\omega]$, s has an out-edge labeled by t iff s' has one. Moreover, if the target of the out-edge of s labeled by t is an internal node v, then so is the target v' of the corresponding out-edge of s', and $(v, v') \in \gamma$. If the target of the out-edge of s labeled by t is an output node, then the target of the out-edge of s' labeled by t is the corresponding output node of $\mathcal{S}'$.

We usually write $\gamma : \mathcal{S} \to \mathcal{S}'$ to indicate that γ is a homomorphism from $\mathcal{S}$ to $\mathcal{S}'$. Simulations have several nice properties, some of them are listed in the following lemma. See also [20, 7, 5].

LEMMA 4.1: *For all relations φ, ψ and Σ-schemes $\mathcal{F}, \mathcal{G}, \mathcal{H}, \mathcal{F}', \mathcal{G}'$ of appropriate source and target,*

1. $\mathcal{F} \,|\mathrm{id}_F|\, \mathcal{F}$
2. $\mathcal{F} \,|\varphi|\, \mathcal{G} \quad \Rightarrow \quad \mathcal{G} \,|\varphi^{-1}|\, \mathcal{F}$
3. $\mathcal{F} \,|\varphi|\, \mathcal{G} \ \wedge\ \mathcal{G} \,|\psi|\, \mathcal{H} \quad \Rightarrow \quad \mathcal{F} \,|\varphi \circ \psi|\, \mathcal{H}$
4. $\mathcal{F} \,|\varphi|\, \mathcal{F}' \ \wedge\ \mathcal{G} \,|\psi|\, \mathcal{G}' \quad \Rightarrow \quad \langle \mathcal{F}, \mathcal{G} \rangle \,|\varphi \cup \psi|\, \langle \mathcal{F}', \mathcal{G}' \rangle$
5. $\mathcal{F} \,|\varphi|\, \mathcal{F}' \ \wedge\ \mathcal{G} \,|\psi|\, \mathcal{G}' \quad \Rightarrow \quad \mathcal{F} \cdot \mathcal{G} \,|\varphi \cup \psi|\, \mathcal{F}' \cdot \mathcal{G}'$
6. $\mathcal{F} \,|\varphi|\, \mathcal{F}' \ \wedge\ \mathcal{G} \,|\psi|\, \mathcal{G}' \quad \Rightarrow \quad \mathcal{F} \oplus \mathcal{G} \,|\varphi \cup \psi|\, \mathcal{F}' \oplus \mathcal{G}'$
7. $\mathcal{F} \,|\varphi|\, \mathcal{G} \quad \Rightarrow \quad \mathcal{F}^\dagger \,|\varphi|\, \mathcal{G}^\dagger$
8. $\mathcal{F} \,|\varphi|\, \mathcal{G} \ \wedge\ \mathcal{F} \,|\psi|\, \mathcal{G} \quad \Rightarrow \quad \mathcal{F} \,|\varphi \cup \psi|\, \mathcal{G}$
9. $\mathcal{F} \,|\varphi|\, \mathcal{G} \ \wedge\ \mathcal{F} \,|\psi|\, \mathcal{G} \quad \Rightarrow \quad \mathcal{F} \,|\varphi \cap \psi|\, \mathcal{G}$ □

COROLLARY 4.1: *The strong equivalence relation $\approx$ is a congruence on the $\mathbf{N} \times \mathbf{N}$-sorted algebra $\Sigma\mathbf{Sch}$. Moreover, when $\mathcal{S}$ and $\mathcal{S}'$ are strongly equivalent schemes, there exists a smallest simulation*

$$\mathcal{S}\Gamma_{\mathcal{S}'} := \bigcap_{\mathcal{S} \,|\gamma|\, \mathcal{S}'} \gamma$$

and a largest simulation

$$\mathcal{S}\Theta_{\mathcal{S}'} := \bigcup_{\mathcal{S} \,|\gamma|\, \mathcal{S}'} \gamma$$

from $\mathcal{S}$ to $\mathcal{S}'$. □

LEMMA 4.2: *Suppose* $\mathcal{S} : n \to p$ *and* $\mathcal{S}' : n \to p$ *are strongly equivalent* Σ*-schemes,* $\Sigma \cap [p] = \emptyset$. *Then*

$$s \; {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \; s' \quad \Leftrightarrow \quad \exists i \in [n] \; \exists u \in [\omega]^* \; s = \delta(i,u) \; \wedge \; s' = \delta'(i,u)$$

and

$$s \; {}_{\mathcal{S}}\Theta_{\mathcal{S}'} \; s' \quad \Leftrightarrow \quad \forall u \in [\omega]^* \; (\lambda \cup \mathrm{id}_{[p]})(\delta(s,u)) = (\lambda' \cup \mathrm{id}_{[p]})(\delta'(s',u)),$$

for all $s \in S$ *and* $s' \in S'$. *Moreover,* ${}_{\mathcal{S}}\Theta_{\mathcal{S}}$ *is the largest congruence on* $\mathcal{S}$. □

We shall write $\Theta_{\mathcal{S}}$ for ${}_{\mathcal{S}}\Theta_{\mathcal{S}}$.

Thus, two states $s \in S$ and $s' \in S'$ are related by the smallest simulation iff there exist a word $u \in [\omega]^*$ and an integer $i \in [n]$ such that s is the target of the directed path, labeled by u, from node $\alpha(i)$ of $\mathcal{S}$, and s' is the target of the directed path from $\alpha'(i)$ labeled by the same word u. Moreover, s is related to s' by the largest simulation iff for all words $u \in [\omega]^*$ there is a directed path labeled by u from s iff there is a directed path labeled by u from s', and the labels of the targets of these paths agree.

DEFINITION 4.2: *Suppose* $\mathcal{S} : n \to p$ *is a* Σ*-scheme and* ρ *is a congruence on* $\mathcal{S}$. *The* **quotient scheme** $\mathcal{S}/\rho : n \to p$ *with states in the set* S/ρ *is defined by*

$$\lambda_{\mathcal{S}/\rho}(s/\rho) = \lambda(s),$$

$$\alpha_{\mathcal{S}/\rho}(i) = \begin{cases} \alpha(i)/\rho & \text{if } \alpha(i) \in S, \\ \alpha(i) & \text{if } \alpha(i) \in [p], \\ \textit{undefined} & \text{if } \alpha(i) \text{ is undefined,} \end{cases}$$

$$\delta_{\mathcal{S}/\rho}(s/\rho, t) = \begin{cases} \delta(s,t)/\rho & \text{if } \delta(s,t) \in S, \\ \delta(s,t) & \text{if } \delta(s,t) \in [p], \\ \textit{undefined} & \text{if } \delta(s,t) \text{ is undefined,} \end{cases}$$

for all $i \in [n]$, $s \in S$ *and* $t \in [\omega]$.

Congruences and homomorphisms of flowchart schemes behave just like congruences and homomorphisms of algebras. For example, if φ is a homomorphism from a Σ-scheme $\mathcal{S}$ to a Σ-scheme $\mathcal{S}'$ then $\ker_\varphi$ is a congruence on $\mathcal{S}$ and there exists a surjective homomorphism $\varphi_1 : \mathcal{S} \to \mathcal{S}/\ker_\varphi$ and an injective homomorphism $\varphi_2 : \mathcal{S}/\ker_\varphi \to \mathcal{S}'$ such that $\varphi = \varphi_1 \circ \varphi_2$. Conversely, if ρ is a congruence on a scheme $\mathcal{S}$, the function mapping each state s to the congruence class s/ρ is a surjective homomorphism, the **natural homomorphism** from $\mathcal{S}$ to $\mathcal{S}/\rho$.

In the next definition we adopt the universal algebraic concept of a subalgebra to flowchart schemes.

DEFINITION 4.3: *Suppose $\mathcal{S} : n \to p$ and $\mathcal{S}' : n \to p$ are Σ-schemes. $\mathcal{S}'$ is a* **sub-scheme** *of $\mathcal{S}$ if $S' \subseteq S$ and the inclusion $S' \hookrightarrow S$ is a homomorphism from $\mathcal{S}'$ to $\mathcal{S}$. We call $\mathcal{S}'$ a* **proper sub-scheme** *of $\mathcal{S}$ if it is a sub-scheme of $\mathcal{S}$ and $S' \subset S$.*

Each sub-scheme of a scheme $\mathcal{S}$ is totally determined by (and is usually identified with) its set of states. Note that when φ is a simulation from $\mathcal{S}$ to $\mathcal{S}'$, $\mathrm{dom}(\varphi)$ is a sub-scheme of $\mathcal{S}$ and $\mathrm{rng}(\varphi)$ is sub-scheme of $\mathcal{S}'$.

DEFINITION 4.4: *Suppose $\mathcal{S} : n \to p$ is a Σ-scheme. A state $s \in S$ is called* **accessible** *if $s = \delta(i, u)$ holds, for some $i \in [n]$ and $u \in [\omega]^*$, i.e., when in the graphical representation, s lies on a directed path from an input node. Moreover, s is called* **strongly accessible** *if $s = \alpha(i)$ for some $i \in [n]$, i.e., when s is the target of an edge from some input node. We call $\mathcal{S}$ a* **(strongly) accessible scheme** *if each of its states is (strongly) accessible.*

We denote the set of all accessible states of $\mathcal{S}$ by $\mathrm{Acc}(\mathcal{S})$. It is not hard to see that $\mathrm{Acc}(\mathcal{S})$ is the smallest sub-scheme of $\mathcal{S}$, called the **accessible part** of $\mathcal{S}$. Therefore, a scheme is accessible if and only if it has no proper sub-schemes.

LEMMA 4.3: *Suppose $\mathcal{S}$ and $\mathcal{S}'$ are strongly equivalent Σ-schemes. Then $\mathrm{dom}({}_{\mathcal{S}}\Gamma_{\mathcal{S}'}) = \mathrm{Acc}(\mathcal{S})$ and $\mathrm{rng}({}_{\mathcal{S}}\Gamma_{\mathcal{S}'}) = \mathrm{Acc}(\mathcal{S}')$. Moreover,*

$$ {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} = {}_{\mathrm{Acc}(\mathcal{S})}\Gamma_{\mathcal{S}'} = {}_{\mathcal{S}}\Gamma_{\mathrm{Acc}(\mathcal{S}')} = {}_{\mathrm{Acc}(\mathcal{S})}\Gamma_{\mathrm{Acc}(\mathcal{S}')}. $$

□

LEMMA 4.4: *Suppose $\mathcal{S} : n \to p$ and $\mathcal{S}' : n \to p$ are Σ-schemes and $\varphi : \mathcal{S} \to \mathcal{S}'$ is a homomorphism. Define $\psi := \varphi \cap (\mathrm{Acc}(\mathcal{S}) \times S')$, so that ψ is the restriction of φ to the accessible states of $\mathcal{S}$. Then $\psi = {}_{\mathcal{S}}\Gamma_{\mathcal{S}'}$ and ψ is a surjective homomorphism $\mathrm{Acc}(\mathcal{S}) \to \mathrm{Acc}(\mathcal{S}')$.*

Proof: ψ is clearly a homomorphism from $\mathrm{Acc}(\mathcal{S})$ to $\mathcal{S}'$ and, by Lemma 4.3, ${}_{\mathcal{S}}\Gamma_{\mathcal{S}'} = {}_{\mathrm{Acc}(\mathcal{S})}\Gamma_{\mathcal{S}'} \subseteq \psi$. Since $\mathrm{dom}({}_{\mathcal{S}}\Gamma_{\mathcal{S}'}) = \mathrm{dom}(\psi) = \mathrm{Acc}(\mathcal{S})$ and ψ is a function, it follows that $\psi = {}_{\mathcal{S}}\Gamma_{\mathcal{S}'}$ and $\mathrm{rng}(\psi) = \mathrm{rng}({}_{\mathcal{S}}\Gamma_{\mathcal{S}'}) = \mathrm{Acc}(\mathcal{S}')$. □

The next lemma gives various (well known) characterizations of the strong equivalence relation $\approx$ of flowchart schemes. See [5], for example.

LEMMA 4.5: *Suppose* $\mathcal{S} : n \to p$ *and* $\mathcal{S}' : n \to p$ *are* Σ*-schemes,* $\Sigma \cap [p] = \emptyset$. *Then the following statements are equivalent:*

1. $\mathcal{S}$ *and* $\mathcal{S}'$ *are strongly equivalent.*
2. $\forall i \in [n] \;\; \forall u \in [\omega]^* \;\; (\lambda \cup \mathrm{id}_{[p]})(\delta(i,u)) = (\lambda' \cup \mathrm{id}_{[p]})(\delta'(i,u))$.
3. *The relation*

$$\{(s,s') \in S \times S' \mid \exists i \in [n] \;\; \exists u \in [\omega]^* \;\; s = \delta(i,u) \wedge s' = \delta'(i,u)\}$$

   is a simulation from $\mathcal{S}$ *to* $\mathcal{S}'$.
4. *The two schemes* $\mathrm{Acc}(\mathcal{S})/\Theta_{\mathrm{Acc}(\mathcal{S})}$ *and* $\mathrm{Acc}(\mathcal{S}')/\Theta_{\mathrm{Acc}(\mathcal{S}')}$ *are isomorphic.*

□

Every simulation relation γ from a scheme $\mathcal{S}$ to a scheme $\mathcal{S}'$ determines a scheme whose states are the ordered pairs in γ.

DEFINITION 4.5: *Suppose* $\mathcal{S} : n \to p$ *and* $\mathcal{S}' : n \to p$ *are strongly equivalent* Σ*-schemes and* γ *is a simulation from* $\mathcal{S}$ *to* $\mathcal{S}'$. *Then we define the* Σ*-scheme* $[\gamma] := (\gamma, \lambda_{[\gamma]}, \alpha_{[\gamma]}, \delta_{[\gamma]}) : n \to p$, *where*

$$\lambda_{[\gamma]}((s,s')) = \lambda(s),$$

$$\alpha_{[\gamma]}(i) = \begin{cases} (\alpha(i), \alpha'(i)) & \text{if } \alpha(i) \in S, \\ \alpha(i) & \text{if } \alpha(i) \in [p], \\ \textit{undefined} & \text{if } \alpha(i) \text{ is undefined,} \end{cases}$$

$$\delta_{[\gamma]}((s,s'),t) = \begin{cases} (\delta(s,t), \delta'(s',t)) & \text{if } \delta(s,t) \in S, \\ \delta(s,t) & \text{if } \delta(s,t) \in [p], \\ \textit{undefined} & \text{if } \delta(s,t) \text{ is undefined,} \end{cases}$$

for all $i \in [n]$, $(s,s') \in \gamma$, $i \in [n]$ *and* $t \in [\omega]$. *We call the schemes* $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ *and* $[{}_{\mathcal{S}}\Theta_{\mathcal{S}'}]$ *the* **minimal and maximal direct product** *of* $\mathcal{S}$ *and* $\mathcal{S}'$, *respectively.*

Thus, for each $i \in [n]$, the ith input node of the scheme $[\gamma]$ has an out-edge iff the ith input node of $\mathcal{S}$, and hence of $\mathcal{S}'$, has an out-edge. Moreover, when exists, the target of this out-edge is the ordered pair (s,s'), where s and s' are the targets of the out-edges of the ith input nodes of $\mathcal{S}$ and $\mathcal{S}'$, respectively. However, if say s is an output node, the target of the out-edge of the ith input node of $[\gamma]$ is the corresponding output node. Let $(s,s') \in \gamma$ and $t \in [\omega]$. Then, in the graphical representation of the scheme $[\gamma]$, the node (s,s') has an out-edge labeled by t iff s, and hence

s' has an out-edge labeled by t. Suppose that v and v' denote the targets of these edges. Then, since γ is a simulation, v is an internal node iff v' is. In this case, the ordered pair $(v, v') \in \gamma$ is the target of the out-edge of (s, s') labeled by t. Otherwise s and s' are output nodes, and the target is the corresponding output node of $[\gamma]$.

LEMMA 4.6: *Suppose $\mathcal{S} : n \to p$ and $\mathcal{S}' : n \to p$ are strongly equivalent Σ-schemes. Then their minimal direct product $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ is an accessible scheme. Moreover, the two projection functions $\pi : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S$ and $\pi' : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S'$ are homomorphisms, namely, $\pi = {}_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}\Gamma_{\mathcal{S}}$ and $\pi' = {}_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}\Gamma_{\mathcal{S}'}$.*

Proof: Suppose $(s, s') \in {}_{\mathcal{S}}\Gamma_{\mathcal{S}'}$. By Lemma 4.2, there is an integer $i \in [n]$ and a word $u \in [\omega]^*$ such that

$$(s, s') \;=\; (\delta(i, u), \delta'(i, u)) \;=\; \delta_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}(i, u),$$

showing (s, s') is an accessible state of $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$. It is trivial that the two projections are simulations, so they are homomorphisms. Now $\pi = {}_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}\Gamma_{\mathcal{S}}$ and $\pi' = {}_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}\Gamma_{\mathcal{S}'}$, by Lemma 4.4. □

LEMMA 4.7: *Suppose $\mathcal{S}$, $\mathcal{S}'$ and $\overline{\mathcal{S}}$ are Σ-schemes $n \to p$, $\varphi : \overline{\mathcal{S}} \to \mathcal{S}$ and $\varphi' : \overline{\mathcal{S}} \to \mathcal{S}'$. Then there exists a unique homomorphism $\psi : \mathrm{Acc}(\overline{\mathcal{S}}) \to [{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$.*

Proof: By Lemma 4.4, the only possibility for ψ is the least simulation relation ${}_{\overline{\mathcal{S}}}\Gamma_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}$, which is defined, since $\mathcal{S}$, $\mathcal{S}'$, $\overline{\mathcal{S}}$ and $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ are strongly equivalent. To prove it is a function assume that $\delta_{\overline{\mathcal{S}}}(i, u) = \delta_{\overline{\mathcal{S}}}(j, v)$ is a state of $\mathrm{Acc}(\overline{\mathcal{S}})$, for some integers $i, j \in [n]$ and words $u, v \in [\omega]^*$. Then

$$\delta_{\mathcal{S}}(i, u) \;=\; \varphi(\delta_{\overline{\mathcal{S}}}(i, u)) \;=\; \varphi(\delta_{\overline{\mathcal{S}}}(j, v)) \;=\; \delta_{\mathcal{S}}(j, v)$$

and

$$\delta_{\mathcal{S}'}(i, u) \;=\; \varphi'(\delta_{\overline{\mathcal{S}}}(i, u)) \;=\; \varphi'(\delta_{\overline{\mathcal{S}}}(j, v)) \;=\; \delta_{\mathcal{S}'}(j, v),$$

proving $\delta_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}(i, u) = \delta_{[\mathcal{S}\Gamma_{\mathcal{S}'}]}(j, v)$. □

LEMMA 4.8: *Suppose $\mathcal{S} : n \to p$ is an accessible Σ-scheme and ρ is a congruence on $\mathcal{S}$. Then the minimal direct product $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}/\rho}]$ of $\mathcal{S}$ and $\mathcal{S}/\rho$ is isomorphic to $\mathcal{S}$.*

Proof: Since $\mathcal{S}$ is accessible, the states of $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}/\rho}]$ are all pairs $(s, s/\rho)$, $s \in S$, and the projection $\pi : [{}_{\mathcal{S}}\Gamma_{\mathcal{S}/\rho}] \to \mathcal{S}$ is an isomorphism. □

4.1. Aperiodic congruences

In this subsection we define and study some special congruences of flowchart schemes, namely minimal, regular, simple and aperiodic congruences. Although the results of this subsection have little importance of their own, they serve as a technical bases in the course of proving our main result, the characterization of the Conway-equivalence of flowchart schemes.

When A and B are sets, we shall denote by $\mathrm{Const}[A,B]$ and $\mathrm{Biject}[A,B]$ the set of all constant functions and the set of all bijections $A \to B$, respectively. Suppose that ρ is a congruence on a scheme $\mathcal{S}$. The set of all *nonsingleton* equivalence classes of ρ will be denoted by $\mathbf{Cl}(\rho)$. Recall from Lemma 4.1 that the intersection of two (and in fact any nonzero number of) congruences on $\mathcal{S}$ is again a congruence on $\mathcal{S}$. It follows that if C' is a subset of an equivalence class C of ρ then there exists a least congruence $\Theta(C')$ on $\mathcal{S}$, called the **congruence generated by** C', such that $\Theta(C')$ identifies all the elements of C'. Note that $\Theta(C')$ is the least equivalence containing the relation

$$\Theta_0 = \{(\tau(a),\tau(b)) \mid a,b \in C',\ \tau \in \Delta[C,S]\} \subseteq S \times S$$

consisting of all pairs $(c,d) \in S \times S$ such that there exist $a,b \in C'$ and a word $u \in [\omega]^*$ such that c is the target of the directed path from a labeled by u, and d is the target of the corresponding directed path from b. The relation Θ_0 is usually not transitive, in which case $\Theta_0 \neq \Theta(C')$. Also note that if $|C'| \leq 1$, $\Theta(C')$ is the **trivial congruence** id_S on $\mathcal{S}$.

DEFINITION 4.6: *Suppose $\mathcal{S} : n \to p$ is a flowchart scheme and ρ is a congruence on $\mathcal{S}$. The* **rank** *of ρ, denoted by $\#\rho$, is the cardinality of its largest congruence class. A congruence of rank k is also called a* **k-congruence**. *We say ρ is*

minimal *if it is nontrivial and minimal among all nontrivial congruences of $\mathcal{S}$ with respect to set inclusion,*

regular *if it is generated by each one of its nonsingleton classes, i.e., if*

$$\Theta(C) = \rho,$$

for all $C \in \mathbf{Cl}(\rho)$,

simple *if*

$$\Delta[C,D] \subseteq \mathrm{Const}[C,D] \cup \mathrm{Biject}[C,D],$$

for all $C,D \in \mathbf{Cl}(\rho)$,

aperiodic *if*

$$s \rho \delta(s,u) \quad \Rightarrow \quad \exists k \geq 0 \;\; \delta(s,u^k) = \delta(s,u^{k+1}),$$

for all $s \in S$ *and* $u \in [\omega]^*$.

Note that a trivial congruence is simple, regular and aperiodic, by definition. Also note that every 2-congruence is simple and every minimal congruence is regular. However, there exist regular congruences which are not minimal. (For the simplest example, take the scheme $0 \to 0$ having three states labeled by a symbol σ_0 having no transitions. Then the relation that collapses all three states is a regular congruence which is clearly not minimal.)

The word "regular" is used here only as a technical term. The concept of regular congruence has nothing to do with regularity as used in automata theory. Nevertheless, the notion of aperiodic congruence stems from automata theory, since a congruence ρ is aperiodic iff for each congruence class C, the transformation semigroup $(C, \Delta(C,C))$, or the semigroup $\Delta(C,C)$ is aperiodic. See [19].

REMARK 4.1: *Suppose* $\mathcal{S} : n \to p$ *is a flowchart scheme and* ρ *is a congruence on* $\mathcal{S}$. *Then the following statements are equivalent.*

1. ρ *is aperiodic on* $\mathcal{S}$.
2. *None of the partial functions*

$$\{\delta_u[C',C'] \mid u \in [\omega]^*, \; C' \subseteq C \in \mathbf{Cl}(\rho)\}$$

is a nontrivial (cyclic) permutation.

3. $\forall C \in \mathbf{Cl}(\rho) \;\; \forall \tau \in \Delta[C,C] \;\; \exists k \in \mathbf{N} \;\; \tau^k = \tau^{k+1}$.
4. *For all* $C \in \mathbf{Cl}(\rho)$, *no subsemigroup of the monoid* $\Delta[C,C]$ *is a nontrivial group.*

In the next three lemmas we establish a few simple facts about the special congruences defined above.

LEMMA 4.9: *Suppose* ρ *is a simple congruence on the scheme* $\mathcal{S}$. *Then* ρ *is regular if and only if*

$$|\Delta[C,D] \cap \mathrm{Biject}[C,D]| \geq 1,$$

for all $C, D \in \mathbf{Cl}(\rho)$.

Proof: If ρ is simple and the above condition holds then ρ is clearly generated by any one of its nonsingleton equivalence classes. Now assume ρ is simple and the above condition fails, so that there are two nonsingleton equivalence classes C and D of ρ such that $\Delta[C,D] \cap \mathrm{Biject}[C,D] = \emptyset$. Then $\Delta[C,D] \subseteq \mathrm{Const}[C,D]$ and the congruence generated by the class C is properly contained in ρ, since it does not identify the elements of D. □

LEMMA 4.10: *Suppose ρ is a simple congruence on the scheme $\mathcal{S}$. Then ρ is aperiodic if and only if*

$$\Delta[C,C] \cap \mathrm{Biject}[C,C] = \{\mathrm{id}_C\},$$

for all $C \in \mathbf{Cl}(\rho)$.

Proof: Observe that the elements of $\Delta[C,C] \cap \mathrm{Biject}[C,C]$ form a subgroup in the monoid $\Delta[C,C]$. By Remark 4.1, this group has to be trivial. □

LEMMA 4.11: *Suppose ρ is a simple regular congruence on the scheme $\mathcal{S}$. Then ρ is aperiodic if and only if*

$$|\Delta[C,D] \cap \mathrm{Biject}[C,D]| = 1,$$

for all $C, D \in \mathbf{Cl}(\rho)$.

Proof: If ρ is simple and satisfies the above condition, then it is aperiodic by Lemma 4.10. Now assume ρ is simple, regular and aperiodic. By Lemma 4.9 and Lemma 4.10, we only need to show that for all distinct nonsingleton equivalence classes C, D of ρ, there is at most one bijection in $\Delta[C,D]$. Assume τ and τ' are bijections in $\Delta[C,D]$. By Lemma 4.9, there exists a bijection $\pi \in \Delta[D,C]$. Now both functions $\tau \circ \pi$ and $\tau' \circ \pi$ are bijections in $\Delta[C,C]$, so they are equal, by Lemma 4.10. It follows that $\tau = \tau'$. □

Recall that when $\rho' \subseteq \rho$ are two equivalence relations on a set S, their quotient ρ/ρ', defined by

$$\forall s, s' \in S \quad (s/\rho')\ \rho/\rho'\ (s'/\rho') \quad \Leftrightarrow \quad s\ \rho\ s',$$

is an equivalence relation on the set S/ρ' of all equivalence classes of ρ'. It is not hard to see that when $\rho' \subseteq \rho$ are congruences on a scheme $\mathcal{S}$ then the equivalence ρ/ρ' is a congruence on the quotient scheme $\mathcal{S}/\rho'$ and $(\mathcal{S}/\rho')/(\rho/\rho')$ is isomorphic to $\mathcal{S}/\rho$. The following two lemmas show that some nice properties of ρ are inherited to ρ' and ρ/ρ'.

LEMMA 4.12: *Suppose ρ is an aperiodic congruence on the scheme $\mathcal{S}$. If $\rho' \subseteq \rho$ is a congruence on $\mathcal{S}$, then ρ' is aperiodic on $\mathcal{S}$ and the quotient congruence $\overline{\rho} = \rho/\rho'$ is aperiodic on the quotient scheme $\overline{\mathcal{S}} = \mathcal{S}/\rho'$.*

Proof: It is trivial that ρ' is aperiodic. Suppose $C\ \overline{\rho}\ \delta_{\overline{\mathcal{S}}}(C,u)$ for some word $u \in [\omega]^*$ and congruence class $C = s/\rho'$. Then $s\ \rho\ \delta(s,u)$ and since ρ is aperiodic, $\delta(s,u^k) = \delta(s,u^{k+1}) \in S$, for some integer $k \geq 0$. It follows that $\delta_{\overline{\mathcal{S}}}(C,u^k) = \delta_{\overline{\mathcal{S}}}(C,u^{k+1})$. □

LEMMA 4.13: *Suppose ρ is a simple congruence on the scheme $\mathcal{S}$. If $\rho' \subseteq \rho$ is a congruence on $\mathcal{S}$ generated by a class $C \in S/\rho$, then ρ' is simple on $\mathcal{S}$ and the quotient congruence $\overline{\rho} = \rho/\rho'$ is simple on the quotient scheme $\overline{\mathcal{S}} = \mathcal{S}/\rho'$. Moreover, if $C \in \mathbf{Cl}(\rho)$ then $|\mathbf{Cl}(\overline{\rho})| = |\mathbf{Cl}(\rho)| - |\mathbf{Cl}(\rho')| < |\mathbf{Cl}(\rho)|$.*

Proof: The case $|C| = 1$ is trivial, so assume $C \in \mathbf{Cl}(\rho)$. Then

$$\mathbf{Cl}(\rho') \quad = \quad \{D \in \mathbf{Cl}(\rho) \mid \Delta[C,D] \cap \mathrm{Biject}[C,D] \neq \emptyset\} \quad \subseteq \quad \mathbf{Cl}(\rho).$$

Since ρ is simple, it follows that ρ' is simple. The nonsingleton equivalence classes of $\overline{\rho}$ are of the form

$$\overline{D} \quad = \quad \{\{d\} \mid d \in D\} \quad = \quad D/\mathrm{id}_D,$$

where D is a nonsingleton equivalence class of ρ which is not an equivalence class of ρ'. The map $D \mapsto \overline{D}$ is a bijection from $\mathbf{Cl}(\rho) \setminus \mathbf{Cl}(\rho')$ to $\mathbf{Cl}(\overline{\rho})$. In particular, since $\mathbf{Cl}(\rho') \subseteq \mathbf{Cl}(\rho)$ we have

$$|\mathbf{Cl}(\overline{\rho})| \quad = \quad |\mathbf{Cl}(\rho) \setminus \mathbf{Cl}(\rho')| \quad = \quad |\mathbf{Cl}(\rho)| - |\mathbf{Cl}(\rho')| \quad < \quad |\mathbf{Cl}(\rho)|.$$

Suppose $\overline{D}$ and $\overline{E}$ are nonsingleton classes of $\overline{\rho}$. Then

$$\delta_{\overline{\mathcal{S}}}(\{d\},u) = \{e\} \quad \Leftrightarrow \quad \delta(d,u) = e,$$

for all $d \in D$, $e \in E$ and $u \in [\omega]^*$, showing that $\delta_{\overline{\mathcal{S}},u}[\overline{D},\overline{E}]$ is constant/bijective if and only if $\delta_u[D,E]$ is constant/bijective. It follows that $\overline{\rho}$ is simple. □

LEMMA 4.14: *Suppose ρ is a simple congruence on the scheme $\mathcal{S}$. Then there exists a simple regular congruence $\rho' \subseteq \rho$ on $\mathcal{S}$ such that the congruence $\overline{\rho} = \rho/\rho'$ is simple on the quotient scheme $\overline{\mathcal{S}} = \mathcal{S}/\rho'$. Moreover, if ρ is aperiodic so are ρ' and $\overline{\rho}$, and if ρ is nontrivial then ρ' is nontrivial and $|\mathbf{Cl}(\overline{\rho})| = |\mathbf{Cl}(\rho)| - |\mathbf{Cl}(\rho')| < |\mathbf{Cl}(\rho)|$.*

Proof: If ρ is trivial so is the claim, therefore assume that $|\mathbf{Cl}(\rho)| > 0$. Consider the congruences $\Theta(D)$ generated by the nonsingleton classes D of ρ. Since there are finitely many of them, there exists a minimal such congruence, i.e., there is a nonsingleton equivalence class C of ρ such that whenever $\Theta(D) \subseteq \Theta(C)$, for some $D \in \mathbf{Cl}(\rho)$, then $\Theta(D) = \Theta(C)$. Let ρ' be the congruence $\Theta(C)$. Then clearly $\rho' \subseteq \rho$ and both ρ' and $\overline{\rho}$ are simple, by Lemma 4.13. If ρ is aperiodic then ρ' and $\overline{\rho}$ are also aperiodic, by Lemma 4.12. By Lemma 4.13, $|\mathbf{Cl}(\overline{\rho})| = |\mathbf{Cl}(\rho)| - |\mathbf{Cl}(\rho')| < |\mathbf{Cl}(\rho)|$. To prove that ρ' is regular assume that D is a nonsingleton equivalence class of ρ'. Then $\Theta(D) \subseteq \rho'$ and, as noted in the proof of Lemma 4.13, D is a nonsingleton class of ρ. It follows by the minimality of ρ' that $\Theta(D) = \rho'$.□

COROLLARY 4.2: *Suppose ρ is a simple aperiodic congruence on the scheme $\mathcal{S}$. Then there exists an integer $m \geq 1$, a sequence $\mathcal{S}_1, \ldots, \mathcal{S}_m$ of schemes and a sequence $\rho_1, \ldots, \rho_{m-1}$ of simple, aperiodic and regular congruences such that*

$$\begin{aligned} \mathcal{S}_1 &= \mathcal{S}, \\ \mathcal{S}_m &= \mathcal{S}/\rho \quad \textit{and} \\ \mathcal{S}_{i+1} &= \mathcal{S}_i/\rho_i, \end{aligned}$$

for all $i \in [m-1]$.

Proof: By a straightforward induction on $|\mathbf{Cl}(\rho)|$, using Lemma 4.14. □

Minimal congruences identify "as few states as possible", minimal 2-congruences are even more restricted. We end this subsection by showing that every simple aperiodic congruence can be "decomposed" into a sequence of minimal aperiodic 2-congruences.

LEMMA 4.15: *Suppose ρ is a nontrivial, simple, aperiodic and regular congruence on the scheme $\mathcal{S}$. Then there exists a minimal aperiodic 2-congruence $\rho' \subseteq \rho$ on $\mathcal{S}$ such that the quotient congruence $\overline{\rho} = \rho/\rho'$ is simple, aperiodic and regular on the quotient scheme $\overline{\mathcal{S}} = \mathcal{S}/\rho'$. Moreover, $\#\overline{\rho} = \#\rho - 1$.*

Proof: Let $C' = \{a, b\}$ be a two-element subset of a congruence class $C \in \mathbf{Cl}(\rho)$ and $\rho' := \Theta(C')$. Then clearly $\rho' \subseteq \rho$ and both ρ' and $\overline{\rho}$ are aperiodic by Lemma 4.12. We know from Lemma 4.11 that each set $\Delta[D, E]$ contains a unique bijection τ_{DE}, for all $D, E \in \mathbf{Cl}(\rho)$. It follows that $\tau_{DE} \circ \tau_{EF} = \tau_{DF}$ and $\tau_{DD} = \mathrm{id}_D$, for all $D, E, F \in \mathbf{Cl}(\rho)$. Now ρ'

is the least equivalence relation containing

$$\begin{aligned}\beta &:= \{(\tau(a),\tau(b)) \mid \tau \in \Delta[C,S],\ \tau(a) \neq \tau(b)\} \\ &= \{(\tau_{CD}(a),\tau_{CD}(b)) \mid D \in \mathbf{Cl}(\rho)\}.\end{aligned}$$

Since β is transitive, $\rho' = \beta \cup \beta^{-1} \cup \mathrm{id}_S$ is a 2-congruence. To prove ρ' is minimal assume that $\gamma \subseteq \rho'$ is a nontrivial congruence on $\mathcal{S}$. Then γ is generated by two states a', b' with $(a', b') \in \beta$, say $a' = \tau_{CD}(a)$ and $b' = \tau_{CD}(b)$, where D is a nonsingleton class of ρ. But then

$$a \;=\; \tau_{DC}(a') \;\gamma\; \tau_{DC}(b') \;=\; b$$

and since ρ' is generated by $\{a, b\}$, it follows that $\gamma = \rho'$. The congruence classes of $\overline{\rho}$ are of the form

$$D/\rho' = \begin{cases} \{\{d\}\} & \text{if } D = \{d\}, \\ \{\{d\} \mid d \in D \setminus \{\tau_{CD}(a), \tau_{CD}(b)\}\} \cup \{\{\tau_{CD}(a), \tau_{CD}(b)\}\} & \text{if } |D| > 1, \end{cases}$$

where D is an equivalence class of ρ. This shows $\#\overline{\rho} = \#\rho - 1$ and that $\overline{\rho}$ is simple and regular on $\overline{\mathcal{S}}$. □

COROLLARY 4.3: *Suppose ρ is a simple aperiodic congruence on the scheme $\mathcal{S}$. Then there exists an integer $m \geq 1$, a sequence $\mathcal{S}_1, \ldots, \mathcal{S}_m$ of schemes and a sequence $\rho_1, \ldots, \rho_{m-1}$ of minimal aperiodic 2-congruences such that*

$$\begin{aligned}\mathcal{S}_1 &= \mathcal{S}, \\ \mathcal{S}_m &= \mathcal{S}/\rho \quad \textit{and} \\ \mathcal{S}_{i+1} &= \mathcal{S}_i/\rho_i,\end{aligned}$$

for all $i \in [m-1]$.

Proof: By a straightforward induction on $\#\rho$, using Corollary 4.2 and Lemma 4.15. □

4.2. Aperiodic homomorphisms

Suppose Σ is a signature and recall the definition of the category $\Sigma\mathbf{Sch}$ of Σ-schemes from the previous section.

This subsection is devoted to scheme homomorphisms having an aperiodic kernel, or aperiodic homomorphisms, for short. Using these homomorphisms we define two relations $\rightarrow$ and $\Rightarrow$ on $\Sigma\mathbf{Sch}$, the first being strictly

stronger than the second. Nevertheless we prove (see Lemma 4.16) that the equivalences $\overset{*}{\leftrightarrow}$ and $\overset{*}{\Leftrightarrow}$ generated by these relations coincide, and that this equivalence is a congruence of $\Sigma\mathbf{Sch}$. We also show that $\overset{*}{\Leftrightarrow}$ is just the composite of $\Leftarrow$ with $\Rightarrow$. This is done in two steps: in Lemma 4.18, we prove that the relation $\Leftarrow \circ \Rightarrow$ contains the relation $\Rightarrow \circ \Leftarrow$. In particular, it follows that $\overset{*}{\Leftrightarrow} = \overset{*}{\Leftarrow} \circ \overset{*}{\Rightarrow}$. Then in Lemma 4.19, we show that $\Rightarrow$ is reflexive and transitive, so that $\overset{*}{\Rightarrow} = \Rightarrow$ and $\overset{*}{\Leftarrow} = \Leftarrow$.

DEFINITION 4.7: *Suppose that $\mathcal{S}$ and $\mathcal{S}'$ are Σ-schemes and φ is a homomorphism from $\mathcal{S}$ to $\mathcal{S}'$. We write*

$\mathcal{S} \overset{\varphi}{\to} \mathcal{S}'$ *if φ is injective or* $\ker_\varphi$ *is a minimal aperiodic 2-congruence on $\mathcal{S}$,*

$\mathcal{S} \overset{\varphi}{\Rightarrow} \mathcal{S}'$ *if* $\ker_\varphi$ *is an aperiodic congruence on $\mathcal{S}$.*

We define two relations on Σ-schemes by

$$\mathcal{S} \to \mathcal{S}' \quad \Leftrightarrow \quad \exists\varphi\ \mathcal{S} \overset{\varphi}{\to} \mathcal{S}'$$
$$\mathcal{S} \Rightarrow \mathcal{S}' \quad \Leftrightarrow \quad \exists\varphi\ \mathcal{S} \overset{\varphi}{\Rightarrow} \mathcal{S}'.$$

The inverses of these relations are denoted by the corresponding reversed arrows and we use the standard notation for the various closures. For example, $\overset{*}{\Rightarrow}$ is the least reflexive and transitive relation containing $\Rightarrow$ and $\overset{*}{\leftrightarrow}$ is the equivalence relation generated by $\to$.

Using these definitions we can rephrase Corollary 4.3 in the following form.

COROLLARY 4.4: *If ρ is a simple aperiodic congruence on a scheme $\mathcal{S}$ then $\mathcal{S} \overset{*}{\to} \mathcal{S}/\rho$.* □

We summarize the results of this subsection in the following proposition.

PROPOSITION 4.1: *The two equivalence relations $\overset{*}{\leftrightarrow}$ and $\overset{*}{\Leftrightarrow}$ agree on $\Sigma\mathbf{Sch}$. Moreover, $\overset{*}{\Leftrightarrow}$ is a congruence relation on $\Sigma\mathbf{Sch}$ and for all $\mathcal{S}, \mathcal{S}' : n \to p$ in $\Sigma\mathbf{Sch}$,*

$$\mathcal{S} \overset{*}{\Leftrightarrow} \mathcal{S}' \quad \textit{if and only if} \quad \mathcal{S} \overset{\pi}{\Leftarrow} [{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}] \overset{\pi'}{\Rightarrow} \mathcal{S}',$$

where $\pi : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S$ and $\pi' : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S'$ are the two projections.

It is obvious that the relation $\Rightarrow$ properly contains the relation $\to$. We can even give examples when $\mathcal{S} \Rightarrow \mathcal{S}'$ holds, but $\mathcal{S} \overset{*}{\to} \mathcal{S}'$ does not. However, the

next Lemma shows that $\Rightarrow$ is contained in the equivalence relation generated by $\rightarrow$, which is probably the most interesting technical result of our paper.

LEMMA 4.16: $\Rightarrow \subseteq \overset{*}{\leftrightarrow}$.

Proof: Suppose $\mathcal{S}$ and $\mathcal{F}$ are Σ-schemes $n \to p$ with $\mathcal{S} \Rightarrow \mathcal{F}$. Then there exists a homomorphism $\varphi : \mathcal{S} \to \mathcal{F}$ such that $\ker_\varphi$ is an aperiodic congruence on $\mathcal{S}$. As noted before, every homomorphism admits a surjective-injective factorization, i.e., there exist a surjective homomorphism $\varphi_1 : \mathcal{S} \to \mathcal{S}/\ker_\varphi$ and an injective homomorphism $\varphi_2 : \mathcal{S}/\ker_\varphi \to \mathcal{F}$ such that $\varphi = \varphi_1 \circ \varphi_2$. Let us denote $\ker_\varphi$ by ρ. Then $\mathcal{S}/\rho \overset{\varphi_2}{\to} \mathcal{F}$ and the result follows if we show that $\mathcal{S} \overset{*}{\leftrightarrow} \mathcal{S}/\rho$. To prove this we use induction on $\#\rho$. The base case $\#\rho = 1$ is trivial, so assume for the induction step that $\#\rho > 1$.

First we modify the start and transition functions of $\mathcal{S}$ to obtain a new scheme $\mathcal{S}' = (S, \lambda, \alpha', \delta') : n \to p$. The difference between δ and δ' is that if C, D are congruence classes of ρ with $|D| = \#\rho$ and t is an integer such that $\delta_t[C, D]$ is a non-surjective function $C \to D$, then we select an arbitrary element $d \in D \setminus \mathrm{rng}(\delta_t[C, D])$ and define $\delta'_t[C, D]$ to be the constant function with value d. Similarly, for all $i \in [n]$, if $\alpha(i) \in S$ and the congruence class $D = \alpha(i)/\rho$ has exactly $\#\rho$ elements, then we select an arbitrary element $d \in D \setminus \{\alpha(i)\}$ and define $\alpha'(i) := d$.

Note that for all words $u \in [\omega]^*$ and congruence classes C, D of ρ, either $\delta'_u[C, D] = \delta_u[C, D]$ or $\delta_u[C, D]$ is a non-surjective function $C \to D$ and $\delta'_u[C, D]$ is a constant function $C \to D$, such that $\mathrm{rng}(\delta'_u[C, D]) \cap \mathrm{rng}(\delta_u[C, D]) = \emptyset$. It follows that ρ is also an aperiodic congruence on $\mathcal{S}'$ and

$$\mathcal{S} \overset{\varphi_1}{\Rightarrow} \mathcal{S}/\rho \;=\; \mathcal{S}'/\rho \overset{\varphi_1}{\Leftarrow} \mathcal{S}'.$$

Thus $\mathcal{S} \overset{\pi}{\Leftarrow} [_{\mathcal{S}}\Gamma_{\mathcal{S}'}] \overset{\pi'}{\Rightarrow} \mathcal{S}'$, by Theorem 4.1.

Next we prove that

$$\forall i \in [n] \;\; \forall u \in [\omega]^* \;\; (\delta(i, u) \in S \;\wedge\; |\delta(i, u)/\rho| = \#\rho) \Rightarrow \delta(i, u) \neq \delta'(i, u). \tag{15}$$

The proof is by induction on the length of u. If u is the empty word ϵ and $\delta(i, u)/\rho$ has exactly $\#\rho$ elements then

$$\delta(i, u) \;=\; \alpha(i) \;\neq\; \alpha'(i) \;=\; \delta'(i, u),$$

by the definition of α'. Assume for the induction step that $u = vt$, where $v \in [\omega]^*$, $t \in [\omega]$. Let $c := \delta(i, v)$, $c' := \delta'(i, v)$, $d := \delta(i, u) = \delta(c, t)$,

$d' := \delta'(i,u) = \delta'(c',t)$, $C := c/\rho = c'/\rho$, $D := d/\rho = d'/\rho$. Suppose moreover that $|D| = \#\rho$. If the function $\delta_t[C,D]$ is not surjective then $d' \notin \mathrm{rng}(\delta_t[C,D])$, by the definition of δ'. Since $d = \delta(c,t) \in \mathrm{rng}(\delta_t[C,D])$, $d \neq d'$. If $\delta_t[C,D]$ is surjective then $\delta_t[C,D] = \delta'_t[C,D]$ is necessarily a bijection, since $\#\rho = |D| \leq |C| \leq \#\rho$. Using the induction hypothesis we get $c \neq c'$, and thus

$$d = \delta_t(c) \neq \delta_t(c') = \delta'_t(c') = d'.$$

Returning to the main proof, observe that ρ is not just a congruence on the schemes $\mathcal{S}$ and $\mathcal{S}'$ but it is also a simulation from $\mathcal{S}$ to $\mathcal{S}'$. Since ${}_{\mathcal{S}}\Gamma_{\mathcal{S}'}$ is the least simulation, ${}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \subseteq \rho$. Moreover, it follows from (15) that

$${}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \subseteq \rho \setminus \{(s,s) \mid s \in S,\ |s/\rho| = \#\rho\}.$$

Therefore, if (s,s') is a state of $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ then

$$(s,s')/\mathrm{ker}_\pi \subseteq \begin{cases} \{(s,x) \mid x \in s/\rho\} & \text{if } |s/\rho| < \#\rho, \\ \{(s,x) \mid x \in s/\rho,\ x \neq s\} & \text{if } |s/\rho| = \#\rho, \end{cases}$$

showing that $\#\mathrm{ker}_\pi < \#\rho$. By the same argument, $\#\mathrm{ker}_{\pi'} < \#\rho$. Thus, using the induction hypothesis, $\mathcal{S} \overset{*}{\leftrightarrow} [{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}] \overset{*}{\leftrightarrow} \mathcal{S}'$.

Let ρ' denote the equivalence relation on S whose nonsingleton equivalence classes are those equivalence classes C of ρ with $1 < |C| < \#\rho$, i.e.,

$$s\ \rho'\ s' \quad \Leftrightarrow \quad s = s' \ \vee\ (s\ \rho\ s' \ \wedge\ |s/\rho| < \#\rho),$$

for all $s, s' \in S$. Then ρ' is not necessarily a congruence on the scheme $\mathcal{S}$, but it *is* a congruence on $\mathcal{S}'$. This follows from the fact that for any congruence classes C, D of ρ with $|C| < |D| = \#\rho$, $\Delta_{\mathcal{S}'}[C,D] \subseteq \mathrm{Const}[C,D]$. Moreover, $\rho' \subseteq \rho$ and $\#\rho' < \#\rho$. Let $\overline{\mathcal{S}}$ denote the quotient scheme $\mathcal{S}'/\rho'$ and let $\overline{\rho}$ be the quotient congruence ρ/ρ' on $\overline{\mathcal{S}}$. Then, by Lemma 4.12, ρ' is aperiodic on $\mathcal{S}'$ and $\overline{\rho}$ is aperiodic on $\overline{\mathcal{S}}$. We can apply the induction hypothesis once again to obtain $\mathcal{S}' \overset{*}{\leftrightarrow} \overline{\mathcal{S}}$.

Lastly, each nonsingleton congruence class of $\overline{\rho}$ has exactly $\#\rho$ elements and, by the definition of $\mathcal{S}'$, $\overline{\rho}$ is a simple congruence on $\overline{\mathcal{S}}$. By Corollary 4.4, it follows that $\overline{\mathcal{S}} \overset{*}{\to} \overline{\mathcal{S}}/\overline{\rho} = \mathcal{S}'/\rho = \mathcal{S}/\rho$, completing the proof. □

COROLLARY 4.5: $\overset{*}{\leftrightarrow} = \overset{*}{\Leftrightarrow}$. □

Next we prove that $\overset{*}{\Leftrightarrow}$ is a congruence on $\Sigma\mathbf{Sch}$ by showing that the relation $\Rightarrow$ preserves the operations of pairing, composition and iteration. It then follows that $\Rightarrow$ also preserves the separated sum operation.

LEMMA 4.17: *Suppose $\mathcal{F}, \mathcal{G}, \mathcal{F}', \mathcal{G}'$ are Σ-schemes of appropriate sorts. Then*

$$\begin{aligned} \mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{F}' \ \wedge \ \mathcal{G} \overset{\psi}{\Rightarrow} \mathcal{G}' \quad &\Rightarrow \quad \langle \mathcal{F}, \mathcal{G} \rangle \overset{\varphi \cup \psi}{\Rightarrow} \langle \mathcal{F}', \mathcal{G}' \rangle \\ \mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{F}' \ \wedge \ \mathcal{G} \overset{\psi}{\Rightarrow} \mathcal{G}' \quad &\Rightarrow \quad \mathcal{F} \cdot \mathcal{G} \overset{\varphi \cup \psi}{\Rightarrow} \mathcal{F}' \cdot \mathcal{G}' \\ \mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{G} \quad &\Rightarrow \quad \mathcal{F}^\dagger \overset{\varphi}{\Rightarrow} \mathcal{G}^\dagger . \end{aligned}$$

Proof: The first two implications can be handled in the same way, therefore we only prove the first one. Suppose that $\mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{F}'$ and $\mathcal{G} \overset{\psi}{\Rightarrow} \mathcal{G}'$. By Lemma 4.1, $\varphi \cup \psi$ is a simulation from $\langle \mathcal{F}, \mathcal{G} \rangle$ to $\langle \mathcal{F}', \mathcal{G}' \rangle$. Since the set of states of $\langle \mathcal{F}, \mathcal{G} \rangle$ is the disjoint union of those of $\mathcal{F}$ and $\mathcal{G}$, $\varphi \cup \psi$ is a function and $\ker_{\varphi \cup \psi} = \ker_\varphi \cup \ker_\psi$. If C is a congruence class of $\ker_{\varphi \cup \psi}$ then C is either a congruence class of $\ker_\varphi$ and $\Delta_{\langle \mathcal{F}, \mathcal{G} \rangle}[C, C] = \Delta_{\mathcal{F}}[C, C]$ or C is a congruence class of $\ker_\psi$ and $\Delta_{\langle \mathcal{F}, \mathcal{G} \rangle}[C, C] = \Delta_{\mathcal{G}}[C, C]$. Since $\ker_\varphi$ is aperiodic on $\mathcal{F}$ and $\ker_\psi$ is aperiodic on $\mathcal{G}$, $\ker_{\varphi \cup \psi}$ is aperiodic on $\langle \mathcal{F}, \mathcal{G} \rangle$. As for the last implication, if $\mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{G}$ then φ is a homomorphism from $\mathcal{F}^\dagger$ to $\mathcal{G}^\dagger$, by Lemma 4.1. Suppose C is a congruence class of $\ker_\varphi$. Looking at the definition of the iteration operation it is not hard to see that $\Delta_{\mathcal{F}^\dagger}[C, C] \subseteq \Delta_{\mathcal{F}}[C, C] \cup \mathrm{Const}[C, C]$. By Remark 4.1, $\ker_\varphi$ is aperiodic on $\mathcal{F}^\dagger$. □

COROLLARY 4.6: *$\overset{*}{\Leftrightarrow}$ is a congruence relation on* Σ**Sch**. □

Our last goal in this subsection is to give a simple characterization of the congruence $\overset{*}{\Leftrightarrow}$. After proving two lemmas, the results are summarized in Theorem 4.1.

LEMMA 4.18: $(\Rightarrow \circ \Leftarrow) \subseteq (\Leftarrow \circ \Rightarrow)$.

Proof: Suppose that $\mathcal{S} \overset{\varphi}{\Rightarrow} \underline{\mathcal{S}} \overset{\varphi'}{\Leftarrow} \mathcal{S}'$ for some Σ-schemes $\mathcal{S}, \mathcal{S}', \underline{\mathcal{S}} : n \to p$. Then $\mathcal{S}$ and $\mathcal{S}'$ are strongly equivalent, so their minimal direct product $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ exists. By Lemma 4.6, the two projection functions $\pi : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S$ and $\pi' : {}_{\mathcal{S}}\Gamma_{\mathcal{S}'} \to S'$ are homomorphisms from $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ to $\mathcal{S}$ and $\mathcal{S}'$, respectively. In order to prove that $\ker_\pi$ is aperiodic on $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ assume that

$$(s, s') \ \ker_\pi \ \delta_{[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]}((s, s'), w),$$

for some word $w \in [\omega]^*$ and state (s, s') of $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$. Let us write (r, r') for $\delta_{[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]}((s, s'), w)$, so that $r = \delta_{\mathcal{S}}(s, w)$ and $r' = \delta_{\mathcal{S}'}(s', w)$. Since $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ is an accessible scheme, there exist an integer $i \in [n]$ and a word $u \in [\omega]^*$ such that

$$(s, s') \ = \ \delta_{[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]}(i, u) \ = \ (\delta_{\mathcal{S}}(i, u), \delta_{\mathcal{S}'}(i, u)).$$

Thus

$$\begin{aligned} s &= \delta_{\mathcal{S}}(i,u) \\ s' &= \delta_{\mathcal{S}'}(i,u) \\ r &= \delta_{\mathcal{S}}(s,w) \;=\; \delta_{\mathcal{S}}(i,uw) \\ r' &= \delta_{\mathcal{S}'}(s',w) \;=\; \delta_{\mathcal{S}'}(i,uw). \end{aligned}$$

By Lemma 4.4, there is a unique homomorphism from $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ to $\underline{\mathcal{S}}$. By Lemma 4.1, both functions $\pi \circ \varphi$ and $\pi' \circ \varphi'$ are homomorphisms $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}] \to \underline{\mathcal{S}}$, so they are equal. It follows that

$$\varphi(s) \;=\; \varphi'(s')$$

and

$$\varphi(r) \;=\; \varphi'(r').$$

Since $(s,s')\ker_{\pi}(r,r')$, we have $s = r$ and

$$\varphi'(s') \;=\; \varphi(s) \;=\; \varphi(r) \;=\; \varphi'(r'),$$

so that $s' \ker_{\varphi'} r' = \delta_{\mathcal{S}'}(s',w)$. Since $\ker_{\varphi'}$ is aperiodic on $\mathcal{S}'$, there exists an integer $k \geq 0$ such that

$$\delta_{\mathcal{S}'}(s',w^k) = \delta_{\mathcal{S}'}(s',w^{k+1}).$$

On the other hand, since $s = r = \delta_{\mathcal{S}}(s,w)$,

$$\delta_{\mathcal{S}}(s,w^k) = \delta_{\mathcal{S}}(s,w^{k+1}).$$

It follows that

$$\delta_{[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]}((s,s'),w^k) = \delta_{[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]}((s,s'),w^{k+1}),$$

proving $\ker_{\pi}$ is aperiodic on $[{}_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$. A similar argument shows that $\ker_{\pi'}$ is aperiodic. □

COROLLARY 4.7: $\overset{*}{\Leftrightarrow} \;=\; (\overset{*}{\Leftarrow} \circ \overset{*}{\Rightarrow})$. □

LEMMA 4.19: $\Rightarrow \;=\; \overset{*}{\Rightarrow}$

Proof: We have to show that $\Rightarrow$ is reflexive and transitive. Since each trivial congruence is aperiodic, $\Rightarrow$ is reflexive. To prove it is transitive assume that $\mathcal{F} \overset{\varphi}{\Rightarrow} \mathcal{G} \overset{\psi}{\Rightarrow} \mathcal{H}$. Then the composite function $\varphi \circ \psi$ is a homomorphism from $\mathcal{F}$

to $\mathcal{H}$, and the result follows if we can prove that $\ker_{\varphi\circ\psi}$ is aperiodic on $\mathcal{F}$. Suppose $s \ker_{\varphi\circ\psi} \delta_{\mathcal{F}}(s,u)$ for some word $u \in [\omega]^*$ and state s of $\mathcal{F}$. Then

$$\varphi(s) \ker_{\psi} \varphi(\delta_{\mathcal{F}}(s,u)) \;=\; \delta_{\mathcal{G}}(\varphi(s),u).$$

Since $\ker_{\psi}$ is aperiodic, there exists an integer $k \geq 0$ such that $\delta_{\mathcal{G}}(\varphi(s),u^k) = \delta_{\mathcal{G}}(\varphi(s),u^{k+1})$. Let us write s' for $\delta_{\mathcal{F}}(s,u^k)$. Then

$$\begin{aligned}\varphi(s') &= \delta_{\mathcal{G}}(\varphi(s),u^k)\\ &= \delta_{\mathcal{G}}(\varphi(s),u^{k+1})\\ &= \delta_{\mathcal{G}}(\delta_{\mathcal{G}}(\varphi(s),u^k),u)\\ &= \delta_{\mathcal{G}}(\varphi(s'),u)\\ &= \varphi(\delta_{\mathcal{F}}(s',u)).\end{aligned}$$

Thus $s' \ker_{\varphi} \delta_{\mathcal{F}}(s',u)$ and since $\ker_{\varphi}$ is aperiodic on $\mathcal{F}$, there exists an integer $l \geq 0$ such that

$$\delta_{\mathcal{F}}(s,u^{k+l}) \;=\; \delta_{\mathcal{F}}(s',u^l) \;=\; \delta_{\mathcal{F}}(s',u^{l+1}) \;=\; \delta_{\mathcal{F}}(s,u^{(k+l)+1}).$$

□

COROLLARY 4.8: $\overset{*}{\Leftrightarrow} \;=\; (\Leftarrow \circ \Rightarrow)$. □

THEOREM 4.1: *Suppose $\mathcal{S}$ and $\mathcal{S}'$ are Σ-schemes $n \to p$. Then $\mathcal{S} \overset{*}{\Leftrightarrow} \mathcal{S}'$ if and only if $\mathcal{S}$ and $\mathcal{S}'$ are strongly equivalent and $\mathcal{S} \overset{\pi}{\Leftarrow} [_{\mathcal{S}}\Gamma_{\mathcal{S}'}] \overset{\pi'}{\Rightarrow} \mathcal{S}'$, where π and π' are the two projections.*

Proof: Trivially, the above condition is sufficient. To prove it is necessary assume that $\mathcal{S} \overset{*}{\Leftrightarrow} \mathcal{S}'$. Then $\mathcal{S}$ and $\mathcal{S}'$ are strongly equivalent schemes, therefore $[_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$ exists. By Corollary 4.8, there also exists a scheme $\overline{\mathcal{S}}$ such that $\mathcal{S} \overset{\varphi}{\Leftarrow} \overline{\mathcal{S}} \overset{\varphi'}{\Rightarrow} \mathcal{S}'$. Let γ and γ' be the restrictions of φ and φ' to the accessible states of $\overline{\mathcal{S}}$, respectively. Then $\gamma : \mathrm{Acc}(\overline{\mathcal{S}}) \to \mathcal{S}$ and $\gamma' : \mathrm{Acc}(\overline{\mathcal{S}}) \to \mathcal{S}'$, by Lemma 4.4. Further, $\ker_{\gamma}$ and $\ker_{\gamma'}$ are aperiodic congruences on $\mathrm{Acc}(\overline{\mathcal{S}})$, so we have $\mathcal{S} \overset{\gamma}{\Leftarrow} \mathrm{Acc}(\overline{\mathcal{S}}) \overset{\gamma'}{\Rightarrow} \mathcal{S}'$. Let ψ be the unique surjective homomorphism from $\mathrm{Acc}(\overline{\mathcal{S}})$ to $[_{\mathcal{S}}\Gamma_{\mathcal{S}'}]$, which exists by Lemma 4.7. It follows by Lemma 4.4 that $\psi \circ \pi = \gamma = {}_{\overline{\mathcal{S}}}\Gamma_{\mathcal{S}}$ and $\psi \circ \pi' = \gamma' = {}_{\overline{\mathcal{S}}}\Gamma_{\mathcal{S}'}$. Lastly, Lemma 4.12 shows that the congruences $\ker_{\psi}$, $\ker_{\pi}$ and $\ker_{\pi'}$ are all aperiodic, completing the proof. □

COROLLARY 4.9: *Suppose $\mathcal{S}$ is an accessible Σ-scheme and ρ is a congruence on $\mathcal{S}$. Then $\mathcal{S} \overset{*}{\Leftrightarrow} \mathcal{S}/\rho$ if and only if ρ is aperiodic.*

Proof: By Lemma 4.8 and Theorem 4.1. □

5. THE FREE ITERATION THEORIES

Although our interest is in the free Conway theories, we briefly review the description of the free iteration theories. All results in this section are well known and can be found in the book [5].

Note that any signature may be considered as an $\mathbf{N} \times \mathbf{N}$-sorted set in which the sort of a p-ary symbol is the pair $(1, p) \in \mathbf{N} \times \mathbf{N}$.

Suppose Σ is a signature and recall from Corollary 4.1 that the strong equivalence relation $\approx$ is a congruence on $\Sigma\mathbf{Sch}$.

THEOREM 5.1: *The quotient category $\Sigma\mathbf{Sch}/\approx$ is freely generated by Σ in the variety of all iteration theories.* □

REMARK 5.1: *Another description of the free iteration theory on a signature Σ uses regular Σ-trees, cf. [5]. (For a detailed study of infinite and regular trees see also [10].)*

The reader might say that, since iteration theories (Conway theories) form a variety of $\mathbf{N} \times \mathbf{N}$-sorted algebras, the generator set of a free iteration theory (Conway theory) should be an arbitrary $\mathbf{N} \times \mathbf{N}$-sorted set and not just a signature. But every free iteration theory (Conway theory, respectively) is freely generated by a signature, see below.

Suppose that X is an $\mathbf{N} \times \mathbf{N}$-sorted set. The collection of **iteration terms** over X is defined to be the least $\mathbf{N} \times \mathbf{N}$-sorted set $\mathbf{ITerm}_X$ satisfying

$x \in \mathbf{ITerm}_X[n,p]$, for all $x \in X[n,p]$, $n, p \geq 0$;

$\mathbf{1}_n \in \mathbf{ITerm}_X[n,n]$, for all $n \geq 0$;

$0_n \in \mathbf{ITerm}_X[0,n]$, for all $n \geq 0$;

$i_n \in \mathbf{ITerm}_X[1,n]$, for all $n > 0$, $i \in [n]$;

$t \in \mathbf{ITerm}_X[n,p] \wedge t' \in \mathbf{ITerm}_X[m,p] \Rightarrow \langle t, t' \rangle \in \mathbf{ITerm}_X[n+m,p]$;

$t \in \mathbf{ITerm}_X[n,p] \wedge t' \in \mathbf{ITerm}_X[p,q] \Rightarrow (t \cdot t') \in \mathbf{ITerm}_X[n,q]$;

$t \in \mathbf{ITerm}_X[n,p] \wedge t' \in \mathbf{ITerm}_X[m,q] \Rightarrow (t \oplus t') \in \mathbf{ITerm}_X[n+m,p+q]$;

$t \in \mathbf{ITerm}_X[n,n+p] \quad \Rightarrow \quad t^\dagger \in \mathbf{ITerm}_X[n,p]$.

Here, $\mathbf{ITerm}_X[n,p]$ denotes the subcollection of all iteration terms of sort $n \to p$, $n, p \geq 0$. $\mathbf{ITerm}_X$ can be viewed as an $\mathbf{N} \times \mathbf{N}$-sorted algebra

with constants $\mathbf{1}_n$, $\mathbf{0}_n$ and i_n, $n \geq 0$, $i \in [n]$, and the straightforward operations of pairing, composition, separated sum and iteration. As such, it is the absolutely free algebra generated by the $\mathbf{N} \times \mathbf{N}$-sorted set X, i.e., if T is an $\mathbf{N} \times \mathbf{N}$-sorted algebra with the same constants and operations and $\varphi : X \to T$ is a sort-preserving function, then there exists a unique homomorphism $\widehat{\varphi} : \mathbf{ITerm}_X \to T$ such that $\widehat{\varphi}(x) = \varphi(x)$, for all $x \in X$. In particular, this holds when T is a preiteration theory. Suppose that $t : n \to p$ and $t' : n \to p$ are iteration terms over X. We say that T satisfies the equation $t = t'$ if $\widehat{\varphi}(t) = \widehat{\varphi}(t')$ holds for all sort-preserving functions $\varphi : X \to T$, where $\widehat{\varphi} : \mathbf{ITerm}_X \to T$ is the unique homomorphic extension of φ. Note that the theory identities (3–7) and the three Conway identities are infinite collections of equations between iteration terms.

When X is an $\mathbf{N} \times \mathbf{N}$-sorted set, the signature $\Sigma(X)$ corresponding to X is defined by

$$\Sigma(X)_p := \{x_i \mid x \in X[n,p], i \in [n]\},$$

for all $p \geq 0$. Replacing each letter $x \in X[n,p]$ in an iteration term $t \in \mathbf{ITerm}_X[m,q]$ with the n-tuple $\langle x_1, \ldots, x_n \rangle$ we get an iteration term $\Sigma(t) \in \mathbf{ITerm}_{\Sigma(X)}[m,q]$.

LEMMA 5.1: *Suppose that T is a preiteration theory and X is an $\mathbf{N} \times \mathbf{N}$-sorted set. An equation $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm}_X$ holds in T if and only if the equation $\Sigma(t) = \Sigma(t')$ does.* □

PROPOSITION 5.1: *Suppose $\mathcal{V}$ is a variety of preiteration theories and X is an $\mathbf{N} \times \mathbf{N}$-sorted set. Then the X-generated free algebra in $\mathcal{V}$ is isomorphic to the $\Sigma(X)$-generated free algebra in $\mathcal{V}$, the isomorphism is determined by the map*

$$x \in X[n,p] \quad \mapsto \quad \langle x_1, \ldots, x_n \rangle.$$

□

In particular, this applies to the variety of iteration theories and the variety of Conway theories.

DEFINITION 5.1: *Let $\mathbf{X}$ be a fixed $\mathbf{N} \times \mathbf{N}$-sorted set such that $\mathbf{X}[n,p]$ is countably infinite, say $\mathbf{X}[n,p] = \{x_1^{(n,p)}, x_2^{(n,p)}, \ldots\}$, for all $n, p \in \mathbf{N}$. The* **equational theory of a variety** *$\mathcal{V}$ of preiteration theories is the set $Eq(\mathcal{V})$*

of all equations $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm_X}$ which hold in every preiteration theory $T \in \mathcal{V}$.

PROPOSITION 5.2: *It can be decided in polynomial time if two Σ-schemes are strongly equivalent. Consequently, there exists a polynomial time algorithm which decides if an equation $t = t'$, $t, t' \in \mathbf{ITerm_X}$, holds in all iteration theories.* □

6. THE FREE CONWAY THEORIES

In this section we finally complete the characterization of the free Conway theories.

Let us first review what happened so far. In Definition 3.7, we defined $\equiv$ to be the least congruence on the category $\Sigma\mathbf{Sch}$ of all Σ-schemes such that the quotient $\Sigma\mathbf{Sch}/\equiv$ satisfies the theory identity (7). In Theorem 3.1, we proved that $\Sigma\mathbf{Sch}/\equiv$ is the free Conway theory generated by the signature Σ. Then we defined two more congruences $\overset{*}{\leftrightarrow}$ and $\overset{*}{\Leftrightarrow}$ using aperiodic simulations of flowchart schemes and proved that they are equal. A characterization of $\overset{*}{\Leftrightarrow}$ was given in Theorem 4.1.

LEMMA 6.1: $\equiv \; = \; \overset{*}{\leftrightarrow}$.

Proof: In order to prove the containment $\equiv \subseteq \overset{*}{\leftrightarrow}$ we need to show that $\Sigma\mathbf{Sch}/\overset{*}{\leftrightarrow}$ satisfies the theory identity (7). Suppose that $\mathcal{F} : n \to p$ is a Σ-scheme and let $\mathcal{G} := \langle 1_n \cdot \mathcal{F}, \ldots, n_n \cdot \mathcal{F} \rangle$. Then each state s of $\mathcal{F}$ has n copies $s_1, \ldots, s_n$ in $\mathcal{G}$. Let $\varphi : G \to F$ be the function mapping each copy s_i, $i \in [n]$, to s. If $n = 0$ then $\mathcal{G} = 0_p$ and φ is the empty function, which is trivially an injective homomorphism from $\mathcal{G}$ to $\mathcal{F}$. Otherwise φ is a surjective homomorphism and $\ker_\varphi$ is a simple aperiodic congruence on $\mathcal{G}$. In fact, if C and D are two congruence classes of $\ker_\varphi$ then $|C| = |D| = n$ and $\Delta_{\mathcal{G}}[C, D] \subseteq \mathrm{Biject}[C, D]$. By Lemma 4.4, $\mathcal{G} \overset{*}{\to} \mathcal{G}/\ker_\varphi = \mathcal{F}$.

The converse containment $\overset{*}{\leftrightarrow} \; \subseteq \equiv$ follows if we show that $\to \subseteq \equiv$. Assume that $\mathcal{S} \overset{\varphi}{\to} \mathcal{S}'$ for Σ-schemes $\mathcal{S}, \mathcal{S}' : n \to p$ and a homomorphism $\varphi : \mathcal{S} \to \mathcal{S}'$. If φ is injective then

$$\mathcal{S} = \alpha \cdot \langle \mathcal{F}, 1_p \rangle$$

and

$$\mathcal{S}' = \alpha \cdot \langle (1_r \oplus 0_m) \cdot \langle \mathcal{F} \cdot (0_{r+m} \oplus 1_p), \mathcal{G} \cdot (1_r \oplus 0_m \oplus 1_p) \rangle^\dagger, 1_p \rangle,$$

for some Σ-schemes $\mathcal{F} : r \to p$, $\mathcal{G} : m \to r + p$ and partial base scheme $\alpha : n \to r + p$. Without going into the details we just note that $\mathcal{F}$ has the same states as $\mathcal{S}$ and the states of $\mathcal{G}$ are those states of $\mathcal{S}'$ not in the range of φ. Moreover, r is the number of states in $\mathcal{F}$, m is the number of states in $\mathcal{G}$ and both $\mathcal{F}$ and $\mathcal{G}$ are strongly accessible. Since the equation

$$\mathcal{F} = (\mathbf{1}_r \oplus 0_m) \cdot \langle \mathcal{F} \cdot (0_{r+m} \oplus \mathbf{1}_p), \mathcal{G} \cdot (\mathbf{1}_r \oplus 0_m \oplus \mathbf{1}_p) \rangle^\dagger$$

holds in any Conway theory, it follows by Theorem 3.1 that $\mathcal{S} \equiv \mathcal{S}'$.

The second possibility is that $\ker_\varphi$ is a minimal aperiodic 2-congruence on $\mathcal{S}$. Then $\mathcal{S} \overset{\varphi_1}{\to} \mathcal{S}/\ker_\varphi \overset{\varphi_2}{\to} \mathcal{S}'$, where φ_1 is the natural homomorphism and φ_2 is injective. We have just proved above that $\mathcal{S}/\ker_\varphi \equiv \mathcal{S}'$. On the other hand,

$$\mathcal{S} = \alpha \cdot \langle \langle \mathcal{F}, \mathcal{F}, \mathcal{G} \rangle^\dagger, \mathbf{1}_p \rangle$$

and

$$\mathcal{S}/\ker_\varphi = \alpha \cdot \langle \beta \cdot (\langle \mathcal{F}, \mathcal{G} \rangle \cdot (\beta \oplus \mathbf{1}_p))^\dagger, \mathbf{1}_p \rangle,$$

for some Σ-schemes $\mathcal{F} : r \to 2r + m + p$, $\mathcal{G} : m \to 2r + m + p$ and partial base scheme $\alpha : n \to 2r + m + p$, where β denotes the base scheme $\langle \mathbf{1}_r, \mathbf{1}_r \rangle \oplus \mathbf{1}_m : 2r + m \to r + m$. Now $\mathcal{S} \equiv \mathcal{S}/\ker_\varphi$ follows by Lemma 3.1.□

We have proved the following

THEOREM 6.1: $\Sigma\mathbf{Sch}/\overset{*}{\Leftrightarrow}$ *is freely generated by the signature* Σ *in the class of all Conway theories.*

Proof: By Theorem 3.1, Corollary 4.5 and Lemma 6.1. □

By Proposition 5.1, for an arbitrary $\mathbf{N} \times \mathbf{N}$-sorted set X, the free Conway theory generated by X is isomorphic to the free Conway theory generated by the signature $\Sigma(X)$. Thus, Theorem 6.1 describes all of the free Conway theories.

For an $\mathbf{N} \times \mathbf{N}$-sorted set X, let us denote by $\mathbf{ConwayEq}_X$ the set of all equations $t = t'$ between iteration terms t, t' over X which hold in all Conway theories. Thus, according to Definition 5.1, $\mathbf{ConwayEq}_\mathbf{x}$ is the equational theory of Conway theories.

Our last goal is to show that $\mathbf{ConwayEq}_\mathbf{x}$ is **PSPACE**-complete with respect to logspace reductions.

Recall from Definition 4.4 that a strongly accessible Σ-scheme $n \to p$ is one in which every state is a target of an edge starting from an input node in_i, $i \in [n]$. We shall consider the following decision problems.

$\mathbf{AperSch}_\Sigma$: Instance: A strongly accessible Σ-scheme $\mathcal{S} : n \to 0$.
Question: Is $S \times S$ an aperiodic congruence on $\mathcal{S}$?

$\mathbf{AperCong}_\Sigma$: Instance: A strongly accessible Σ-scheme $\mathcal{S} : n \to 0$ and a relation $\rho \subseteq S \times S$.
Question: Is ρ an aperiodic congruence on $\mathcal{S}$?

$\mathbf{SchEq}_\Sigma$: Instance: A pair $(\mathcal{S}, \mathcal{S}')$ of Σ-scheme.
Question: Does $\mathcal{S} \equiv \mathcal{S}'$ hold?

Assuming Σ contains a symbol of rank at least 2, all these problems turn out to be **PSPACE**-complete, as well as the problem of deciding if an equation $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm}_\Sigma$ belongs to $\mathbf{ConwayEq}_\Sigma$.

Recall that a deterministic finite-state automaton (DFA) $\mathbf{A} = (Q, Z, \delta)$ (where Q is the set of states, Z is the input alphabet and δ is the transition function) is called aperiodic if

$$\forall q \in Q \ \forall u \in Z^* \ \exists k \geq 0 \ \ \delta(q, u^k) = \delta(q, u^{k+1}).$$

We are going to use the fact that the following decision problem is **PSPACE**-complete with respect to logspace reductions, see [8].

$\mathbf{AperDFA}_\Sigma$: Instance: A DFA $\mathbf{A} = (Q, \{0,1\}, \delta)$.
Question: Is $\mathbf{A}$ aperiodic?

LEMMA 6.2: *Suppose that Σ is a signature containing a symbol σ_0 of rank $m \geq 2$. Then there exist logspace reductions*

$$\mathbf{AperDFA} \to \mathbf{AperSch}_\Sigma \to \mathbf{AperCong}_\Sigma \to \mathbf{SchEq}_\Sigma \to \mathbf{ConwayEq}_\Sigma \to \mathbf{ConwayEq}_\mathbf{x}.$$

Proof of $\mathbf{AperDFA} \to \mathbf{AperSch}_\Sigma$: Suppose $\mathbf{A} = (Q, \{0,1\}, \delta_A)$ is a DFA, $n := |Q|$. We construct a strongly accessible scheme $\mathcal{S} : n \to 0$ such that $\mathbf{A}$ is aperiodic if and only if $S \times S$ is an aperiodic congruence on $\mathcal{S}$. The states of $\mathcal{S}$ are the states of $\mathbf{A}$, each is labeled by the symbol σ_0. The start function α of $\mathcal{S}$ is an arbitrary bijection $[n] \to Q$ and its transition function δ is defined by

$$\delta(q,t) = \begin{cases} \delta_A(q,0) & \text{if } t = 1, \\ \delta_A(q,1) & \text{if } 2 \leq t \leq m, \end{cases}$$

for all $q \in Q$ and $t \in [m]$.

Proof of $\mathbf{AperSch}_\Sigma \to \mathbf{AperCong}_\Sigma$: The map $\mathcal{S} \mapsto (\mathcal{S}, S \times S)$ is trivially a logspace reduction.

Proof of $\mathbf{AperCong}_\Sigma \to \mathbf{SchEq}_\Sigma$: Suppose $\mathcal{S} : n \to 0$ is a strongly accessible Σ-scheme and $\rho \subseteq S \times S$ is a relation. If ρ is not a congruence on $\mathcal{S}$ then $(\mathcal{S}, \rho)$ is mapped to some fixed pair $(\mathcal{F}, \mathcal{G})$ of Σ-schemes such that $\mathcal{F} \not\equiv \mathcal{G}$. Otherwise $(\mathcal{S}, \rho)$ is mapped to the pair $(\mathcal{S}, \mathcal{S}/\rho)$. All these calculations can be done in logarithmic space. The correctness of the reduction follows by Corollary 4.9.

Proof of $\mathbf{SchEq}_\Sigma \to \mathbf{ConwayEq}_\Sigma$: Let $\psi : \mathbf{ITerm}_\Sigma \to \Sigma\mathbf{Sch}$ be the unique homomorphism mapping each symbol $\sigma \in \Sigma_q$ to the corresponding atomic scheme $\widehat{\sigma} : 1 \to q$. It is easy to find a logspace algorithm which, given a Σ-scheme $\mathcal{S} : n \to p$, constructs an iteration term $\tau_\mathcal{S} \in \mathbf{ITerm}_\Sigma[n, p]$ such that $\psi(\tau_\mathcal{S}) = \mathcal{S}$. The map $(\mathcal{S}, \mathcal{S}') \mapsto (\tau_\mathcal{S} = \tau_{\mathcal{S}'})$ is a logspace reduction.

Proof of $\mathbf{ConwayEq}_\Sigma \to \mathbf{ConwayEq}_\mathbf{X}$: Given an equation $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm}_\Sigma$, replace each symbol $\sigma \in \Sigma_p$ appearing in t or t' with a variable symbol of sort $1 \to p$ in $\mathbf{X}$ such that different symbols are replaced with different variables. □

LEMMA 6.3: $\mathbf{ConwayEq}_\mathbf{X} \in \mathbf{PSPACE}$.

Proof: We outline a nondeterministic polynomial space algorithm which decides if an equation $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm}_\mathbf{X}$ *fails* to hold in some Conway theory. The result then follows by Sawitch's theorem [6]. Recall the definition of the signature $\Sigma(\mathbf{X})$ from the previous section. Let us write Δ for $\Sigma(\mathbf{X})$. By Lemma 5.1, it is enough to check if the equation $\Sigma(t) = \Sigma(t')$ fails in some Conway theory, or equivalently, if it fails in the free Conway theory $\Delta\mathbf{Sch}/\equiv$. Let $\varphi : \mathbf{ITerm}_\Delta \to \Delta\mathbf{Sch}$ be the unique homomorphism mapping each symbol $\sigma \in \Delta_p$ to the corresponding atomic scheme $\widehat{\sigma} : 1 \to p$. Then $\Sigma(t) = \Sigma(t')$ fails in $\Delta\mathbf{Sch}$ if and only if $\varphi(\Sigma(t)) \not\equiv \varphi(\Sigma(t'))$. The two schemes $\mathcal{S} := \varphi(\Sigma(t))$ and $\mathcal{S}' := \varphi(\Sigma(t'))$ can be constructed in polynomial space, as well as their minimal direct product $[_\mathcal{S}\Gamma_{\mathcal{S}'}]$. By Theorem 4.1, our algorithm only has to check if $\mathcal{S}$ and $\mathcal{S}'$ are not strongly equivalent or if at least one of the two congruences $\ker_\pi$ or $\ker_{\pi'}$ is not aperiodic on $[_\mathcal{S}\Gamma_{\mathcal{S}'}]$. It is easy to test if two schemes are not strongly equivalent, so the problem is reduced to testing if a congruence ρ is not aperiodic on a scheme $\mathcal{F}$. This can be done by guessing a congruence class $C \in \mathbf{Cl}(\rho)$, a nonsingleton subset $C' = \{c_1, \ldots, c_m\}$ of C and a word

$u \in [\omega]^*$ such that

$$\delta_{\mathcal{F}}(c_1, u) = c_2, \quad \delta_{\mathcal{F}}(c_2, u) = c_3, \ldots, \delta_{\mathcal{F}}(c_{m-1}, u) = c_m, \quad \delta_{\mathcal{F}}(c_m, u) = c_1. \tag{16}$$

Let n be the number of states in $\mathcal{F}$. It is not allowed to store the whole word u, since it can be approximately as long as $\binom{n}{m} \cdot m!$. Instead, we guess u letter by letter and keep track only of its length and the states c_i and $\delta_{\mathcal{F}}(c_i, u)$, $i \in [m]$. The procedure stops if condition (16) holds or $|u| > \binom{n}{m} \cdot m!$. □

THEOREM 6.2: *Suppose Σ contains a symbol of rank at least 2. Then all the decision problems* $\mathbf{AperSch}_\Sigma$, $\mathbf{AperCong}_\Sigma$, $\mathbf{SchEq}_\Sigma$ *and* $\mathbf{ConwayEq}_\Sigma$ *are* **PSPACE***-complete. It is also* **PSPACE***-complete to decide if an equation $t = t'$ between iteration terms $t, t' \in \mathbf{ITerm}_\mathbf{x}$ holds in all Conway theories.*

Proof: This is an immediate consequence of Lemmas 6.2 and 6.3. □

REFERENCES

1. S. L. BLOOM, C. C. ELGOT and J. B. WRIGHT, Solutions of the iteration equation and extensions of the scalar iteration operation, *SIAM Journal of Computing*, 1980, *9*, pp. 24–65.
2. S. L. BLOOM, C. C. ELGOT and J. B. WRIGHT, Vector iteration in pointed iterative theories, *SIAM Journal of Computing*, 1980, *9*, pp. 525–540.
3. S. L. BLOOM and Z. ÉSIK, Axiomatizing schemes and their behaviours, *Journal of Computing and System Sciences*, 1985, *31*, pp. 375–393.
4. S. L. BLOOM and Z. ÉSIK, Floyd–Hoare logic in iteration theories, *JACM*, 1991, *38*, pp. 887–934.
5. S. L. BLOOM and Z. ÉSIK, Iteration Theories: The Equational Logic of Iterative Processes, *EATCS Monographs on Theoretical Computer Science*, Springer-Verlag, 1993.
6. D. P. BOVET and P. CRESCENZI, *Introduction to the Theory of Complexity*, Prentice-Hall, 1994.
7. V. E. CAZANESCU and Gh. STEFANESCU, Towards a new algebraic foundation of flowchart scheme theory, *Fundamenta Informaticae*, 1990, *13*, pp. 171–210.
8. Sang CHO and Dung T. HUYNH, Finite-automaton aperiodicity is PSPACE-complete, *Theoretical Computer Science*, 1991, *88*, pp. 99–116.
9. J. C. CONWAY, *Regular Algebra and Finite Machines*, Chapman and Hall, 1971.
10. B. COURCELLE, Fundamental properties of infinite trees. In *Theoretical Foundations of Programming Methodology, Munich 1981*, Reidel, 1982.
11. C. C. ELGOT, Monadic computation and iterative algebraic theories. In J. C. Shepherdson, editor, *Logic Colloquium 1973* volume 80 of *Studies in Logic*, Amsterdam, 1975. North Holland.
12. C. C. ELGOT, Matricial Theories, *Journal of Algebra*, 1976, *42*, pp. 391–421.
13. C. C. ELGOT, Structured programmning with and without goto statements. In *IEEE Transactions on Software Engineering*, number 232 in SE-2, 1976, pp. 41–53.
14. Z. ÉSIK, *Group axioms for iteration*, to appear.

15. Z. Ésik, Identities in Iterative and rational algebraic theories, *Computational Linguistics and Computer Languages*, 1980, *14*, pp. 183–207.
16. J. S. Golan, *The theory of semirings with applications in mathematics and theoretical computer science*, Longman Scientific & Technical, 1993.
17. D. Krob, Complete systems of B-rational identities, *Theoretical Computer Science*, 1991, *89*, pp. 207–343.
18. F.W. Lawvere, Functorial Semantics of Algebraic Theories, *Proceedings of the National Academy of Sciences USA*, 1963, *50*, pp. 869–873.
19. J.-E. Pin, *Varieties of Formal Languages*, North Oxford Academic, 1986.
20. Gh. Stefanescu, On Flowchart Theories: Part I. The deterministic case, *JCSS*, 1987, *35*, pp. 163–191.