A Sound and Complete Calculus for finite Stream Circuits

Stefan Milius
Institut für Theoretische Informatik
Technische Universität Braunschweig, Germany
mail@stefan-milius.eu

***Abstract*—Stream circuits are a convenient graphical way to represent streams (or stream functions) computed by finite dimensional linear systems. We present a sound and complete expression calculus that allows us to reason about the semantic equivalence of finite closed stream circuits. For our proof of the soundness and completeness we build on recent ideas of Bonsangue, Rutten and Silva. They have provided a "Kleene theorem" and a sound and complete expression calculus for coalgebras for endofunctors of the category of sets. The key ingredient of the soundness and completeness proof is a syntactic characterization of the final locally finite coalgebra. In the present paper we extend this approach to the category of real vector spaces. We also prove that a final locally finite (dimensional) coalgebra is, equivalently, an initial iterative algebra. This makes the connection to existing work on the semantics of recursive specifications.**

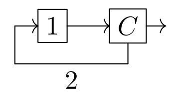
***Keywords*-Kleene algebra, coalgebra, streams, regular expressions**

I. Introduction

Regular expressions are a well-known tool to specify the behavior of finite automata. Kleene's classical theorem [1] states that the semantics of every finite automaton can be expressed by a regular expression. Furthermore, Kleene algebras provide a sound and complete calculus for the behavioral equivalence of finite automata, see [2]. More precisely, putting the laws of Kleene algebras on the set of regular expressions allows one to algebraically reason about the equivalence of automata: two expressions are equal under the laws iff the behavior of the two automata specified by them is the same.

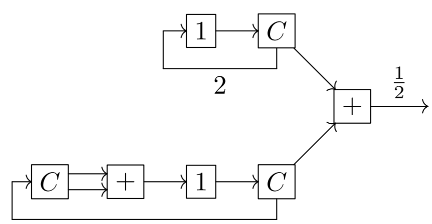
Recently, Bonsangue, Rutten and Silva [3], [4], [5] and these authors and Bonchi [6] have provided analogs of the classical results for a large class of systems (such as Mealy machines, non-deterministic, weighted and probabilistic automata) in a uniform way. The idea is to express the type of a class of systems by an endofunctor on the category Set. The respective systems then arise as coalgebras for that endofunctor. Then one can derive from the structure of the given endofunctor the syntax and axioms for a sound and complete expression calculus. The ideas for this go back to earlier work by Bonsangue and Kurz [7]. At the heart of the soundness and completeness proofs lies a coalgebraic characterization of the set of expressions modulo axioms: this set forms the final locally finite coalgebra; for ordinary regular expressions this elegant presentation of the soundness and completeness for Kleene algebras is due to Jacobs [8].

In this paper we consider a different base category than Set—the category of $\mathsf{Vec}_{\mathbb{R}}$ of real vector spaces. Our aim is to provide a sound and complete calculus of expressions to reason about linear systems. Such systems can be presented in terms of stream circuits such as



(1)

We show that every finite stream circuit that is *valid*, i. e., every loop passes through a register, can equivalently be expressed by an expression in our calculus. This is an analog of Kleene's theorem in our setting of stream circuits. Moreover, our calculus allows us to reason about the equivalence of such circuits. For example, the stream circuit in (1) defines the stream σ whose n-th element is 2^n, and the same stream is defined by the more complicated stream circuit below:



(2)

Then the two expressions for the depicted circuits can be proven to be equal using the rules of our calculus. Our main result is that two expression can be equated iff they express the same linear system; this is an analog of the soundness and completeness result for Kleene algebras.

In order to establish soundness and completeness we consider the set $\mathsf{Exp}/{=}$ of expressions of our calculus modulo the (equivalence relation induced by) the axioms and rules, and we establish the following universal property: $\mathsf{Exp}/{=}$ is the final locally finite dimensional coalgebra for the functor given by $X \mapsto \mathbb{R}\times X$ on $\mathsf{Vec}_{\mathbb{R}}$. This is analogous to the result in [5] that the expressions modulo rules are the final locally finite coalgebra. Our proof is simpler than the one given in loc. cit., and in our setting of linear systems we need to replace *finite* by *finite dimensional* systematically. In Section III we shall see that both characterizations fit

Supported by the German Research Foundation (DFG) under project MI 717/2–1.

into the same general framework. We provide a category-theoretic formulation of local finiteness of coalgebras, and we prove that a final locally finite (dimensional) coalgebra for an endofunctor is, equivalently, an initial iterative algebra in the sense of [9], [10] for the same endofunctor. This also yields a precise connection of the work in [5] with the work on iterative algebras/theories by Bloom and Ésik [11]. Then in Section IV we introduce our calculus for linear systems, and in Section V we prove its soundness and completeness.

We believe that the work in this paper is a first step to obtain a uniform method to derive concrete sound and complete expression calculi for endofunctors on a general algebraic category (in lieu of $\mathsf{Vec}_{\mathbb{R}}$)—we discuss this and other conclusions and directions for future work in Section VI a bit more.

II. Preliminaries

Here we present the basic definitions needed throughout this paper. We shall write Set for the category of sets and functions, and we write $\mathsf{Vec}_{\mathbb{R}}$ for the category of real vectors spaces and linear maps. In Section III we shall also consider more general categories. In our categories of interest finite products exist, and we denote the product of two objects X_1 and X_2 by $X_1 \times X_2$ with the projection functions $\pi_i : X_1 \times X_2 \to X_i$.

A. Coalgebras

Let $\mathscr{A}$ be a category, and let $H : \mathscr{A} \to \mathscr{A}$ be an endofunctor. Recall that a coalgebra for H is a pair (C, c) consisting of an object C and the structure morphism $c : C \to HC$. Take, for example, $\mathscr{A} = \mathsf{Set}$. Then coalgebras can be understood as systems with a set C of states where the functor H describes the type of transitions that the states can perform, and the structure map c determines the transition structure or dynamics of the system, see e. g. [12]. Concrete examples of coalgebras for set endofunctors include various kinds of automata (deterministic, non-deterministic, Mealy, Moore), stream systems, probabilistic automata, weighted ones, labelled transition systems and many others.

A coalgebra homomorphism from a H-coalgebra (C, c) to another one (D, d) is a morphism $h : C \to D$ of $\mathscr{A}$ preserving the transition structure, i. e., such that $d \cdot h = Hh \cdot c$.

A H-coalgebra (T, t) is said to be *final* (or, *terminal*), if for every H-coalgebra (C, c) there exists a unique coalgebra homomorphism $c^\dagger : C \to T$. It is easy to see that (T, t) is, if it exists[1], uniquely determined up to isomorphism. Moreover, the structure map $t : T \to HT$ is an isomorphism by Lambek's Lemma [13]. For an endofunctor of Set, the elements of a final coalgebra provide the semantics of states of systems that are regarded as H-coalgebras.

Finality also provides the basis for semantic equivalence. Let (C, c) and (D, d) be two coalgebras for an endofunctor H on Set with a final coalgebra (T, t). (In fact, any other *concrete*[2] category such as $\mathsf{Vec}_{\mathbb{R}}$ is fine, too.) Then two states $x \in C$ and $y \in D$ are called *behavioral equivalent* if $c^\dagger(x) = c^\dagger(y)$, and we shall write $x \sim y$. If H preserves weak pullbacks then behavioral equivalence coincides with the well-known notion of bisimilarity. The states x and y are called bisimilar if they are in a special relation called a *bisimulation* [14]. We shall not define that concept here as it is not needed in the present paper; for details see [12]. Let us just remark that the coalgebraic notion of bisimulation generalizes the concepts of the same name known for concrete classes of systems, e. g., for deterministic automata or labelled transition systems (where coalgebraic bisimulation coincides with Milner's strong bisimulation). The requirement that H preserve weak pullbacks is not very restrictive; many functors of interest in coalgebra theory do indeed preserve weak pullbacks. An exception is Giry's probabilistic monad on the category of analytic spaces.

Finally, let (C, c) be a coalgebra for an endofunctor H. Recall that a subcoalgebra of C is given by a subset S carrying a coalgebra structure $s : S \to HS$ such that the inclusion map $i : S \to C$ is a coalgebra homomorphism. Now assume that H preserves weak pullbacks and let $s \in C$. Then the subcoalgebra $\langle s \rangle \subseteq C$ generated by s is given as the intersection of all subcoalgebra of C containing s. Notice that this is true for endofunctors H of Set as well as for those on $\mathsf{Vec}_{\mathbb{R}}$.

B. Linear Systems and Stream Circuits

We now recall some basic notions from the coalgebraic stream calculus [15] needed in this paper.

In this paper we consider streams of reals[3], i. e., infinite sequences $\sigma = (\sigma(0), \sigma(1), \sigma(2), \ldots)$ of real numbers. We shall also consider the following operations on the set $\mathbb{R}^\omega$ of all streams, for all $r \in \mathbb{R}$, $\sigma, \tau \in \mathbb{R}^\omega$ and $n \geq 0$:

$(r\sigma)(n)$	$=$	$r\sigma(n)$	scalar product
$(\sigma + \tau)(n)$	$=$	$\sigma(n) + \tau(n)$	sum
$(\sigma \times \tau)(n)$	$=$	$\sum_{i=0}^{n} \sigma(i) \cdot \tau(n-i)$	convolution product

Of course, sum and convolution product are both commutative and associative. Notice also that every stream σ has an additive inverse

$$-\sigma = (-\sigma(0), -\sigma(1), -\sigma(2), \ldots)$$

with $\sigma + (-\sigma) = (0, 0, \ldots)$. If σ is a stream with $\sigma(0) \neq 0$ then there is a unique multiplicative inverse σ^{-1} with $\sigma \times \sigma^{-1} = (1, 0, 0, 0, \ldots)$.

[1] Existence of a final coalgebra can be assured by mild assumptions on H, e.ġ. every bounded endofunctor of Set has a final coalgebra.

[2] Recall that a category $\mathscr{A}$ is called *concrete* if it comes equipped with a faithful functor $U : \mathscr{A} \to \mathsf{Set}$.

[3] The restriction to $\mathbb{R}$ is not essential; in fact, our results hold more generally for streams over an arbitrary field k.

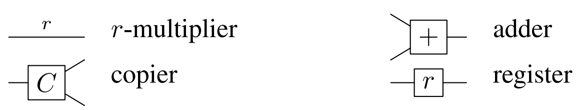
An important subclass of all streams are the *rational streams*, see [16]; a stream ρ is called rational if it can be written as a convolution product $\rho = \sigma \times \tau^{-1}$ where σ and τ are so-called polynomial streams, i. e., they have finitely many non-zero entries only.

One way to represent streams is by linear systems. A linear system is a triple $(C, \langle c_0, c_1 \rangle)$ where C is a real vector space (the state space of the system), $c_0 : C \to \mathbb{R}$ and $c_1 : C \to C$ are linear functions (called the output and transition function, respectively). Equivalently, $(C, \langle c_0, c_1 \rangle)$ is a coalgebra for the functor H given by $X \mapsto \mathbb{R} \times X$ on the category $\mathsf{Vec}_{\mathbb{R}}$. Notice that $\mathbb{R}^\omega$ is a real vector space with the scalar product and sum as defined above. Together with the head and tail functions $\mathsf{hd}(\sigma) = \sigma(0)$ and $\mathsf{tl}(\sigma) = (\sigma(1), \sigma(2), \ldots)$ we see that $\mathbb{R}^\omega$ is a linear system. Indeed, $(\mathbb{R}^\omega, \langle \mathsf{hd}, \mathsf{tl} \rangle)$ is the final coalgebra for H. For every linear system $(C, \langle c_0, c_1 \rangle)$ the unique homomorphism into the final coalgebra $\mathbb{R}^\omega$ assigns to every state s of the system C the stream

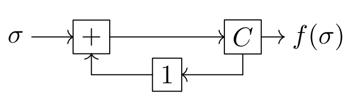
$$(c_0(s), c_0(c_1(s)), c_0(c_1(c_1(s))), \ldots)$$

given by the output behavior of that state. We also say that s represents the above stream. It has been proved by Rutten [16] that the rational streams are precisely those streams represented by the states of finite dimensional linear systems, i. e., linear systems where the state space is finite dimensional.

Another, equivalent, way to represent rational streams is by finite stream circuits. Stream circuits are a convenient graphical way to specify (computations on) streams. They are defined as pictorial compositions of the following basic stream circuits



The r-multiplier multiplies all elements in a stream by $r \in \mathbb{R}$, the adder computes the sum of two streams, the copier yields two copies of a stream, and the register prepends $r \in \mathbb{R}$ to a stream σ to yield $r : \sigma$ (we shall call r the initial value of the register). The stream circuits are then built from the basic circuits by plugging wires together, and there may also be feedback (loops). We already saw two examples of closed stream circuits in the introduction, and here is a simple example of an open one (we direct the wires to illustrate the dataflow from input to output):



A stream circuit is called *valid* if all its loops pass through at least one register.

It turns out that finite closed valid stream circuits represent precisely the rational streams. Rutten [16] has proved this for a certain restricted class of stream circuits. However, it is not difficult to prove that this holds in general.

Theorem II.1. *Let $\sigma \in \mathbb{R}^\omega$ be a stream. Then the following are equivalent:*
(1) The stream σ is represented by a state of a finite dimensional system.
(2) The stream σ is computable by a finite valid closed stream circuit.[4]

Finally, let us collect some technical preliminaries that we will need subsequently. We denote by $L : \mathsf{Set} \to \mathsf{Set}$ the functor assigning to a set X the (underlying set of the) free vector space on X. So LX consists of formal linear combinations of elements of X. Actually, L is a monad on Set with its unit $\eta : Id \to L$ given object wise by the universal maps $\eta_X : X \to LX$ of the free vector spaces. We also have a distributive law $\lambda : LH \to HL$ of L over the functor $HX = \mathbb{R} \times X$ on Set:

$$\lambda_X : \sum_{i=1}^{n} s_i(r_i, x_i) \mapsto \left(\sum_{i=1}^{n} s_i r_i, \sum_{i=1}^{n} s_i x_i \right). \qquad (3)$$

Notice that we make no notational distinction between this functor H and its lifting to the category of real vector spaces.

III. Locally finitely presentable coalgebras

In the work of Bonsangue, Rutten and Silva [5] locally finite coalgebras play an important rôle, and in our work in the present paper locally finite dimensional coalgebras are important. More precisely, expressions modulo rules form a final locally finite (or locally finite dimensional, respectively) coalgebra. In this section we provide a general framework that gives a uniform explanation of this phenomenon.

Finiteness of objects is captured categorically by the notion of a locally finitely presentable category, see e. g. [17]. We briefly recall the basics. A functor is called *finitary* if it preserved filtered colimits. An object X of a category $\mathscr{A}$ is called *finitely presentable* if its hom-functor $\mathscr{A}(X, -)$ preserves filtered colimits. A category $\mathscr{A}$ is called *locally finitely presentable* (lfp, for short) provided that $\mathscr{A}$ is cocomplete and it has a set of finitely presentable objects such that every object of $\mathscr{A}$ is a filtered colimit of objects from that set.

Examples of lfp categories are the category Set of sets and maps, posets and monotone maps, graphs and their homomorphisms, the category $\mathsf{Vec}_{\mathbb{R}}$ of real vector spaces and linear maps, groups and their homomorphisms, and more generally, every finitary variety of algebras. The corresponding finitely presentable objects are as expected: finite sets, posets or graphs, finite dimensional vector spaces, and those groups or algebras that can be presented by finitely many generators and equations.

The category of complete partial orders (cpos) and continuous maps is not locally finitely presentable; there are no non-trivial finitely presentable objects.

[4]All the omitted proofs may be found in the appendix.

Assumption III.1. Throughout this section we assume that $\mathscr{A}$ is a locally finitely presentable category and $H : \mathscr{A} \to \mathscr{A}$ is a finitary endofunctor.

Example III.2. There two examples of interest in this paper.
(1) Every Kripke polynomial functor of Set as in [5] is finitary.
(2) The functor $H = \mathbb{R} \times (-)$ on $\mathsf{Vec}_{\mathbb{R}}$ is finitary.

Remark III.3. It is easy to verify that an object X is finitely presentable iff the following holds: every morphism $f : X \to C$, where $C = \operatorname{colim} C_i$ is a filtered colimit with the colimit injections $c_i : C_i \to C$, has an essentially unique factorization through one of the colimit injections c_i. More precisely, two conditions are fulfilled: (i) there exists a C_i and a morphism $f' : X \to C_i$ such that $c_i \cdot f' = f$ and (ii) for every two parallel morphisms $f', f'' : X \to C_i$ with $c_i \cdot f' = c_i \cdot f''$ there exists an object C_j and a connecting morphism $c_{ij} : C_i \to C_j$ in the diagram such that $c_{ij} \cdot f' = c_{ij} \cdot f''$.

Remark III.4. We shall need a number of properties of lfp categories; and we recall those from [17]:

1) every finite colimit of finitely presentable objects is itself finitely presentable,
2) in $\mathscr{A}$ every morphism f can be factorized as a strong epimorphism followed by a monomorphism. This factorization system has the following unique diagonalization property: for every commutative square $m \cdot f = g \cdot e$ where m is a monomorphism and e a strong epimorphism there exists a unique diagonal morphism d with $m \cdot d = g$ and $f = d \cdot e$.

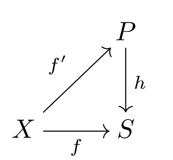
In addition to the above properties we shall need the following

Lemma III.5. *Every split quotient of a finitely presentable object is itself finitely presentable.*

Notation III.6. We denote by $\mathsf{Coalg_f}(H)$ the category of all coalgebras $p : P \to HP$ with a finitely presentable carrier P.

Definition III.7. A coalgebra (S, s) is called *locally finitely presentable* if the following conditions are fulfilled:

(1) Every morphism $f : X \to S$ with X finitely presentable factors through a coalgebra homomorphism where the domain has finitely presentable carrier; more precisely, given f there exists a coalgebra (P, p) from $\mathsf{Coalg_f}(H)$, a homomorphism $h : (P, p) \to (S, s)$ and a morphism $f' : X \to P$ such that the triangle below commutes:



(2) The factorization in (1) is essentially unique in the sense that for every $f'' : X \to P$ with $h \cdot f'' = f$ there exists a coalgebra (Q, q) in $\mathsf{Coalg_f}(H)$ with a coalgebra homomorphism $h' : (Q, q) \to (S, g)$ and a coalgebra homomorphism $\ell : (P, p) \to (Q, q)$ with $\ell \cdot f' = \ell \cdot f''$.

For finitary endofunctors on Set and $\mathsf{Vec}_{\mathbb{R}}$ preserving monomorphisms, condition (2) in Definition III.7 is not necessary. In addition, condition (1) can be weakened to hold only for subobjects. More precisely, consider for a coalgebra (S, s) the following condition:

(1') for every subobject $f : X \to S$ where X is finitely presentable there exists a subcoalgebra $h : (P, p) \to (S, s)$ with P finitely presentable that contains X, i. e., there is a (mono-)morphism $f' : X \to P$ with $h \cdot f' = f$.

Lemma III.8. *Suppose that in $\mathscr{A}$ epimorphisms split and that H preserves monomorphisms. Then a coalgebra is locally finitely presentable iff condition (1') above is satisfied.*

In our work below we shall make use of the following lemma.

Lemma III.9. *Under the assumptions in Lemma III.8 every quotient of a locally finitely presentable coalgebra is itself locally finitely presentable.*

Example III.10. (1) For $\mathscr{A} = \mathsf{Set}$ a coalgebra is locally finitely presentable iff every finite subset of its carrier is contained in a finite subcoalgebra. If, moreover, H preserves weak pullbacks, a coalgebra (S, g) is locally finitely presentable iff for every $s \in S$ the subcoalgebra $\langle s \rangle$ is finite, i. e., (S, g) is locally finite. So, in particular, for any Kripke polynomial functor local finiteness of a coalgebra in the sense of [5] coincides with our concept of local finite presentability.

(2) For $\mathscr{A} = \mathsf{Vec}_{\mathbb{R}}$ and H preserving weak pullbacks, a coalgebra (S, g) is locally finitely presentable iff for every $s \in S$ the subcoalgebra $\langle s \rangle$ is finite dimensional, i. e., (S, g) is locally finite dimensional. In particular, this holds for $H = \mathbb{R} \times (-)$.

Observation III.11. (1) Every filtered colimit of coalgebras from $\mathsf{Coalg_f}(H)$ is obviously locally finitely presentable.

(2) Fix some H-coalgebra (S, g), and consider the category $\mathscr{D} = \mathsf{Coalg_f}(H)/(S, g)$ whose objects are coalgebra homomorphisms $f : (P, p) \to (S, g)$, where (P, p) is a coalgebra from $\mathsf{Coalg_f}(H)$ and whose morphisms are commutative triangles. We have the canonical functor $D : \mathscr{D} \to \mathsf{Coalg_f}(H)$ mapping an object of $\mathscr{D}$ to its domain. This functor D is an essentially small filtered diagram. Indeed, $\mathsf{Coalg_f}(H)$ has up to isomorphism only a set of objects (since $\mathscr{A}$ is locally small) and there is only a set of homomorphism $f : (P, p) \to (S, g)$. Furthermore, $\mathsf{Coalg_f}(H)$ is finitely

cocomplete since $\mathscr{A}$ is finitely cocomplete and finitely presentable objects are closed under finite colimits. Thus, $\mathsf{Coalg_f}(H)$ is a filtered category and therefore $\mathscr{D}$ is a filtered category.

Theorem III.12. *Every locally finitely presentable coalgebra (S, g) is the colimit of its canonical diagram D.*

Remark. More precisely, (S, g) is the colimit of D with the injections given by $\mathsf{in}_p : (P, p) \to (S, g)$ for every object $((P, p), \mathsf{in}_p)$ of $\mathscr{D}$.

Corollary III.13. *A coalgebra is locally finitely presentable iff it is a colimit of a filtered diagram of coalgebras from $\mathsf{Coalg_f}(H)$.*

Indeed, this follows from Theorem III.12 and Observation III.11(1).

The following theorem gives us a useful technical condition to establish finality of a coalgebra in the category of all locally finitely presentable coalgebras for H; finality only has to be checked for all coalgebras from $\mathsf{Coalg_f}(H)$.

Theorem III.14. *A locally finitely presentable coalgebra (R, r) is final in the category of all locally finitely presentable H-coalgebras iff for every coalgebra (P, p) in $\mathsf{Coalg_f}(H)$ there is a unique homomorphism from (P, p) to (R, r).*

As a consequence of the results of this section we see that the final locally finitely presentable coalgebra exists and can be constructed as the colimit of the inclusion functor of $\mathsf{Coalg_f}(H)$ into the category of all coalgebras for H.

This is exactly the construction given in [10] of the initial iterative algebra for H. We shall not recall the notion of iterative algebras here as this plays no rôle in the present paper.

Corollary III.15. *The final locally finitely presentable coalgebra for H exists and is equivalently described as the initial iterative algebra for H.*

This result makes an explicit connection of the work here and in [5] to iterative theories of Elgot [18]. Indeed, in [10] we have shown that the monad of free iterative algebras for H is the free iterative monad $\mathcal{R}$ on H. Thus, our Corollary V.9 below and the corresponding theorem in [5] provide a new syntactic characterization of the closed terms in the free iterative theory (i. e., $\mathcal{R}0$, where 0 denotes the initial object).

Example III.16. We mention a number of key examples of final locally finitely presentable H-coalgebras R; for further examples see e. g. [10], [19].

(1) Let $H = H_\Sigma$ be a polynomial endofunctor on Set associated to a signature Σ of operation symbols with prescribed arities. Then the final coalgebra for H consists of all (finite and infinite) Σ-trees and R consists of all *rational* Σ-trees (where recall that a Σ-tree is a rooted and ordered tree t labelled in Σ such that a node with n children is labelled by an n-ary operation symbol, and t is rational if it has, up to isomorphism, only finitely many subtrees, see [20]).

(2) For the special case $HX = 2 \times X^A$ on Set, where $2 = \{0, 1\}$, a coalgebra is a deterministic automaton, and the terminal coalgebra is carried by the set of $\mathcal{P}(A^*)$ of all formal languages on A. Here R is the subcoalgebra given by all regular languages.

(3) For the functor $HX = \mathbb{R} \times X$ on Set, R consists of all streams σ that are eventually periodic, i. e., $\sigma = u\overline{v}$ where u and v are finite words on $\mathbb{R}$. However, for the lifting of H to $\mathsf{Vec}_\mathbb{R}$, R is the subcoalgebra of $\mathbb{R}^\omega$ given by all rational streams. Indeed, it follows from the work in [9] that the initial iterative H-algebra is, equivalently, the subcoalgebra of $\mathbb{R}^\omega$ of all streams represented by finite dimensional linear systems.

IV. A Language of Expressions for Linear Systems

In this section we define a language of *linear expressions* representing streams that are outputs of finite closed valid stream circuits, and we show that for every linear expression we can construct a finite dimensional linear system (S, g) with a state $s \in S$ having the same behavior. We conclude that every stream represented by a linear expression is rational.

We begin by defining the language of expressions.

Definition IV.1. Let X be a set of fixpoint variables ranged over by x. The set of all linear expressions is defined by the following BNF grammar:

$$\begin{array}{lll} E & ::= & \mu x.E \mid rE \mid E + E \mid r : E \mid r : F \\ F & ::= & x \mid rF \mid F + F \end{array}$$

where $r \in \mathbb{R}$.

As usual, a variable x is *free* in an expression A if it does not occur within the scope of any binding operator μx, and an expression is called *closed* if it does not have any free variables.

Notation IV.2. (1) Given a mapping σ assigning to each free variable x of an expression A an expression $\sigma(x)$ we denote by $A[\sigma]$ the simultaneous substitution of $\sigma(x)$ for x. As usual, we assume (without loss of generality) that no free variable of any $\sigma(x)$ is bound in A. We also write $A[B/x]$ for $A[\sigma]$ where $\sigma(x) = B$ and $\sigma(y) = y$ for $y \neq x$.

(2) We denote by Exp the set of all closed expressions.

Remark IV.3. (1) Notice that besides the μ-operator, our expression syntax has two types of syntactic operators: rE and $E+E$ reflect the algebraic operations of sum and scalar product of object of our base category $\mathsf{Vec}_\mathbb{R}$ and $r : E$ reflects the behavior type given by the functor H. Indeed, on the final coalgebra $\mathbb{R}^\omega$ we have semantic operations given by stream sum, scalar product of streams (giving the vector space structure) and the prefixing operations $r : \sigma = (r, \sigma_0, \sigma_1, \sigma_2, \ldots)$ for every $r \in \mathbb{R}$ and every stream $\sigma = (\sigma_0, \sigma_1, \sigma_2, \ldots)$. The prefixing operations form the inverse of the structure $\langle \mathsf{hd}, \mathsf{tl} \rangle$ of the final H-coalgebra $\mathbb{R}^\omega$.

(2) To keep the syntax a little simpler we neither include a constant 0 nor an inverse operation. The constant zero stream is represented by $\mu x.(0 : x)$, and the additive inverse of an expression A is represented by $(-1)A$.

(3) Note that we defined the expression syntax in a way that every every bound variable occurs *guarded*, i. e., in an expression $\mu x.A$ any occurrence of x is within the scope of a prefixing operator $r : (-)$.

(4) The above definition follows ideas in [4], [6]. However, putting, in addition, the operations of sum and scalar product into the syntax is new. This reflects the fact that expressions ought to denote elements of the final coalgebra $\mathbb{R}^\omega$ of the functor $HX = \mathbb{R} \times X$ on the category $\mathsf{Vec}_\mathbb{R}$ of real vector spaces in lieu of the category Set.

In order to be able to argue by structural induction on the syntax of expressions we define a measure function on expressions. This function essentially measures the number of those μ-operators in an expression that do not occur within the scope of any $r : (-)$-operator.

Definition IV.4. We define a function N assigning to any expression a natural number as follows:

$$\begin{aligned} N(x) &= 0 \\ N(r : A) &= 0 \\ N(rA) &= N(A) + 1 \\ N(A_1 + A_2) &= \max\{N(A_1), N(A_2)\} + 1 \\ N(\mu x.A) &= N(A[\mu x.A/x]) + 1 \end{aligned}$$

Notice that N is well-defined; indeed, only the last clause seems to be problematic here. But recall that in A every occurrence of x is within the scope of some $r : (-)$. Hence, by the second line of the definition, $N(A[\mu x.A/x])$ does not depend on $N(\mu x.A)$.

In order to give a semantics to expressions in Exp we would like to define a coalgebra structure on Exp. Then the unique homomorphism from Exp into the final coalgebra $\mathbb{R}^\omega$ assigns to every expression the stream it denotes. Unfortunately, Exp does not form a linear space. However, it is easy define a coalgebra structure on the free real vector space $L\mathsf{Exp}$ instead. To this end, we first define a function $t : \mathsf{Exp} \to LH\mathsf{Exp}$. Notice that $LH\mathsf{Exp}$ is the linear space of formal linear combinations of elements $(r, A) \in \mathbb{R} \times \mathsf{Exp}$. We define $t(A)$ by induction on $N(A)$ as follows:

$$\begin{aligned} t(r : A) &= (r, A) \\ t(rA) &= rt(A) \\ t(A_1 + A_2) &= t(A_1) + t(A_2) \\ t(\mu x.A) &= t(A[\mu x.A/x]). \end{aligned}$$

Now recall the distributive law λ from (3) and form the function

$$c_0 = (\,\mathsf{Exp} \xrightarrow{t} LH\mathsf{Exp} \xrightarrow{\lambda_{\mathsf{Exp}}} HL\mathsf{Exp}\,)$$

whose codomain is a linear space. Hence, we can extend this function to a linear map

$$c : L\mathsf{Exp} \to HL\mathsf{Exp}, \tag{4}$$

i. e., c is the unique linear function such that

$$c \cdot \eta_{\mathsf{Exp}} = \lambda_{\mathsf{Exp}} \cdot t.$$

Notation IV.5. In the following we abuse notation and simply write A for the trivial linear combination $\eta_{\mathsf{Exp}}(A) \in L\mathsf{Exp}$.

Every closed linear expression A denotes a stream $[\![A]\!]$. To define the semantics function $[\![-]\!] : \mathsf{Exp} \to \mathbb{R}^\omega$ let ℓ be the unique coalgebra homomorphism from $(L\mathsf{Exp}, c)$ to the final coalgebra $(\mathbb{R}^\omega, \langle \mathsf{hd}, \mathsf{tl} \rangle)$. Then we have

$$[\![-]\!] = (\,\mathsf{Exp} \xrightarrow{\eta_{\mathsf{Exp}}} L\mathsf{Exp} \xrightarrow{\ell} \mathbb{R}^\omega). \tag{5}$$

We shall now show that the semantics of an expression is always a rational stream.

Theorem IV.6. *For every expression A there exists a finite dimensional system (S, g) and a state $s \in S$ with $A \sim s$.*

Proof: We prove that the subcoalgebra $\langle A \rangle$ of $L\mathsf{Exp}$ is finite dimensional. Let A be any closed linear expression. We write $B \leq A$ if B is a subexpression of A.

Take any subexpression $r : B$ of A. For every free variable x in $r : B$ there exists some subterm $\mu x.C_x \leq A$ with $r : B \leq \mu x.C_x \leq A$ such that x is bound by the μ-operator at the head of $\mu x.C_x$. Now let σ be the map mapping every free variable x of B to $\mu x.C_x$ and consider the expression $B' = B[\sigma]$. This expression is closed, whence in Exp. Notice also that whenever B is closed then we have $B' = B$.

We will now prove that $M = \{\, A \,\} \cup \{\, B' \mid r : B \leq A \,\}$ forms a basis of a subcoalgebra of $L\mathsf{Exp}$. To do this it suffices to prove for every $E \in M$ by induction on $N(E)$ that

$$c_0(E) = (r, \sum_{i=1}^{n} r_i E_i) \tag{6}$$

for some $r, r_1, \ldots, r_n \in \mathbb{R}$ and some expressions $E_1, \ldots, E_n \in M$.

Suppose first that $E = r : F$. Then $c_0(E) = (r, F)$. If $E = A$, then F is a closed subexpression of A, and so we have $F \in M$. Otherwise we have some $B' \in M$ with $B' = E = r : F$ and $B' = B[\sigma]$ for the corresponding $B \leq A$ and the substitution σ. It follows that $B = r : C$ for some expression $C \leq A$, and, thus, we have $F = C' = C[\sigma]$ which implies that $F \in M$.

For $E = E_1 + E_2$ we have $c_0(E) = c_0(E_1) + c_0(E_2)$ and so (6) follows by the induction hypothesis. Similarly, for $E = rF$ we have $c_0(E) = rc_0(F)$. Finally, for $E = \mu x.F$ we have

$$c_0(E) = c_0(F[\mu x.F/x]),$$

and therefore (6) follows by the induction hypothesis once more. ■

Corollary IV.7. *The coalgebra $L\mathsf{Exp}$ is locally finite dimensional*

Corollary IV.8. *For every expression A, $[\![A]\!]$ is a rational stream.*

Indeed, take a finite dimensional linear system (S, g) and $s \in S$ with $A \sim s$ according to Theorem IV.6. Then $[\![A]\!]$ is equal to the image of s under the unique coalgebra homomorphism $S \to R^\omega$, and this is a rational stream, see Section II-B.

V. Axiomatization of semantic equivalence

In this section we will prove an analog of Kleene's well-known theorem for finite deterministic automata. More precisely, we prove that for every finitely dimensional linear system $g : S \to \mathbb{R} \times S$ and every $s \in S$ there exists a linear expressions expressing the behavior of s.

Furthermore, we are going to provide a sound and complete axiomatization of semantic equivalence of expressions. In other words, we give a syntactic characterization of the coalgebra of all rational streams as a quotient of linear expressions modulo the least equivalence relation $=$ given by appropriate axioms and rules. As in [5] soundness and completeness follow easily from the following characterization of $\mathsf{Exp}/=$ by a universal property: $\mathsf{Exp}/=$ is the final locally finite dimensional coalgebra for H.

We begin by presenting the axioms and rules of the logical calculus:

1) Vector space axioms. For each axiom of vector spaces we have an axiom of the logical calculus. Here is a complete list:

$$\begin{array}{cc} (A+B)+C = A+(B+C) & 1A = A \\ A+B = B+A & r(sA) = (rs)A \\ A+\mu x.(0:x) = A & r(A+B) = rA+rB \\ A+(-1)A = \mu x.(0:x) & (r+s)A = rA+sA \end{array}$$

2) Behavioral Differential Equations. The specification of stream sum and scalar product yield two axioms of our calculus:

$$\begin{array}{rcl} r:A+s:B &=& (r+s):(A+B) \\ r(s:A) &=& (rs):(rA) \end{array}$$

(notice that on the right-hand side of the above equations the operations on the left of ":" are addition and multiplication, respectively, of real numbers and the operations on the right of ":" are the syntactic $+$ and scalar multiplication of linear expressions).

3) α-equivalence. This states that renaming of bound variables does not matter:

$$\mu x.A = \mu y.A[y/x]$$

4) Replacement rule:

$$\frac{B = C}{A[B/x] = A[C/x]}$$

provided that the substitutions are free.

5) Fixpoint axiom. This states that μ-provides a fixpoint operator:

$$\mu x.A = A[\mu x.A/x]$$

6) Uniqueness of fixed points:

$$\frac{A = B[A/x]}{A = \mu x.B}$$

Notation V.1. (1) Of course, we write $=$ for the least equivalence of Exp given by the above axioms and rules, and we write $q : \mathsf{Exp} \to \mathsf{Exp}/=$ for the canonical quotient map.

(2) It is obvious that $\mathsf{Exp}/=$ carries the structure of a vector space with operations given by scalar multiplication and addition of expressions, and with the zero vector $\mu x.0 : x$. Equivalently, $\mathsf{Exp}/=$ is an Eilenberg-Moore algebra for the free vector space monad L, and we denote by $a : L(\mathsf{Exp}/=) \to \mathsf{Exp}/=$ the corresponding algebra structure.

Example V.2. To illustrate how our calculus works we give expressions for the circuits in (1) and (2) and prove them equivalent. The (output stream of) the circuit (1) is represented by the expression $A = \mu x.1 : 2x$. For (2) we obtain the expression

$$B = \frac{1}{2}(\mu x.1 : (x+x) + \mu y.1 : 2y)$$

Let us write $B' = \mu x.1 : (x+x)$ and $B'' = \mu y.1 : 2y$ so that $B = \frac{1}{2}(B' + B'')$. We have $B'' = A$ by α-equivalence. By the fixpoint rule we have $B' = 1 : B' + B'$ and this is $1 : 2B' = (1 : 2x)[B'/x]$ by the vector space axioms. Now an application of the uniqueness rule yields $B' = A$. Thus, we have

$$B = \frac{1}{2}(B' + B'') = \frac{1}{2}(A + A) = A,$$

using the replacement rule and the vector space axioms.

A. Soundness and Kleene's Theorem

Our goal in this subsection is to show that the calculus introduced above is sound. We will also prove that the behavior of any state of a finite dimensional linear system can, equivalently, be described by a linear expression; this is an analog of Kleene's theorem. Before we come to these main results we will need to prove a number of technical lemmas.

Lemma V.3. *There is a coalgebra structure* $\overline{c} : \mathsf{Exp}/{=} \to H(\mathsf{Exp}/{=})$ *such that* $a \cdot Lq : L\mathsf{Exp} \to \mathsf{Exp}/{=}$ *is a coalgebra homomorphism.*

Lemma V.4. *For every finite dimensional system* (S, g) *there exists a coalgebra homomorphism* $h : (S, g) \to (\mathsf{Exp}/{=}, \overline{c})$.

Our proofs of this result and Lemma V.8 below are simpler than the corresponding proofs in [5], and we believe that this simplification also applies to the setting of loc. cit. We will sketch our proof here; the details are given in the Appendix.

Sketch of Proof: Let (S, g) be a finite dimensional linear system. Take a basis $\{ s_1, \dots, s_n \}$ for S and let

$$g(s_i) = \left(r_i, \sum_{j=1}^{n} r_{ij} s_j \right), \quad i = 1, \dots, n. \tag{7}$$

We shall construct expressions $\langle\langle s_i \rangle\rangle$, $i = 1, \dots, n$, by an n-step process. Our expressions will involve the variables $x_1, \dots, x_n$. For every i, let

$$A_i^0 = \mu x_i.(r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)).$$

Now define for $k = 0, \dots, n-1$

$$A_i^{k+1} = \begin{cases} A_i^k\{A_{k+1}^k / x_{k+1}\} & \text{if } i \neq k+1 \\ A_i^k & \text{if } i = k+1 \end{cases}$$

where $\{A/x\}$ denotes syntactic replacement (i. e., substitution without renaming of bound variables). It is easy to see that the set of free variables of A_i^k is $\{x_{k+1}, \dots x_n\} \setminus \{ x_i \}$, and moreover, every occurrence of those variables is free. Now let $\langle\langle s_i \rangle\rangle = A_i^n$ and let $h : S \to \mathsf{Exp}/{=}$ be the unique linear map with $h(s_i) = [\langle\langle s_i \rangle\rangle]$. One now proves that h is a coalgebra homomorphism; this involves using all the axioms and rules of our expression calculus except for the uniqueness rule. ■

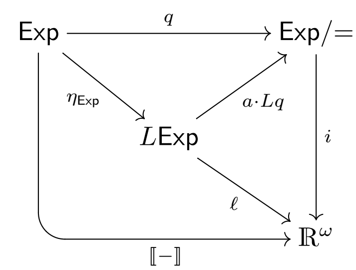
We are ready to prove our version of Kleene's theorem stating that every state of a finite dimensional system can be described by a linear expression.

Corollary V.5. *For every state* s *of a finite dimensional linear system* (S, g) *there is an expression* $\langle\langle s \rangle\rangle$ *with* $s \sim \langle\langle s \rangle\rangle$.

Proof: Indeed, take a homomorphism $h : S \to \mathsf{Exp}/{=}$ and let $\langle\langle s \rangle\rangle$ be any representative of the equivalence class $h(s)$ in Exp (considered as an element of the coalgebra $L\mathsf{Exp}$ via η_{Exp}). We have the coalgebra homomorphism $a \cdot Lq$ (see Lemma V.3) with $h(s) = a \cdot Lq(\langle\langle s \rangle\rangle)$ in $\mathsf{Exp}/{=}$. Thus, s and $\langle\langle s \rangle\rangle$ are behavioral equivalent as desired. ■

Theorem V.6. (Soundness) *Whenever we have* $A = B$ *for two linear expressions, then* $[\![A]\!] = [\![B]\!]$.

Proof: Let $i : \mathsf{Exp}/{=} \to \mathbb{R}^\omega$ be the unique homomorphism of coalgebras. We will verify that the following diagram commutes (notice that ℓ is the homomorphism from (5)):



(8)

Indeed, the lower left-hand triangle commutes by the definition (5) of $[\![-]\!]$. The lower right-hand triangle consists of coalgebra homomorphisms, and so it commutes by the universal property of the final coalgebra. Finally, the upper triangle commutes using that η is a natural transformation and the unit law $a \cdot \eta_{\mathsf{Exp}/=} = id$ of the Eilenberg-Moore algebra a.

Now $A = B$ holds iff $q(A) = q(B)$, and this implies $[\![A]\!] = [\![B]\!]$. ■

B. Completeness

In this subsection we prove the completeness of our logical calculus. The main technical tool to establish this result is a characterization of the coalgebra $\mathsf{Exp}/{=}$ by a universal property: this coalgebra is the final locally finite dimensional coalgebra for H.

We present the proof of the main results in form of a number of technical lemmas.

Lemma V.7. *The coalgebra structure* $\overline{c} : \mathsf{Exp}/{=} \to H(\mathsf{Exp}/{=})$ *is a linear isomorphism.*

Lemma V.8. *Let* (S, g) *be a finite dimensional linear system. Then there exists a unique coalgebra homomorphism from* (S, g) *to* $(\mathsf{Exp}/{=}, \overline{c})$.

Corollary V.9. *The coalgebra* $(\mathsf{Exp}/{=}, \overline{c})$ *is the final locally finite coalgebra for* H.

Proof: That $\mathsf{Exp}/{=}$ is locally finite dimensional follows from Corollary IV.7: for every equivalence class $[A]$ in $\mathsf{Exp}/{=}$ the subcoalgebra $\langle [A] \rangle$ is a quotient of the subcoalgebra $\langle A \rangle$ of $L\mathsf{Exp}$ via the restriction of the homomorphism $a \cdot Lq : L\mathsf{Exp} \to \mathsf{Exp}/{=}$. Hence, since $\langle A \rangle$ is finite dimensional, so is $\langle [A] \rangle$.

The universal property of the coalgebra $\mathsf{Exp}/{=}$ now follows from Lemma V.8 and Theorem III.14 applied to the case $\mathscr{A} = \mathsf{Vec}_{\mathbb{R}}$ and $HX = \mathbb{R} \times X$. ∎

Lemma V.10. *The coalgebra homomorphism $i : \mathsf{Exp}/{=} \to R^\omega$ is injective.*

Sketch of Proof: Take the factorization of i into a surjective followed by an injective linear map:

$$i = (\,\mathsf{Exp}/{=} \xrightarrow{e} I \xrightarrow{m} \mathbb{R}^\omega\,)$$

Observe that the functor $HX = \mathbb{R} \times X$ preserves monomorphisms. By the unique diagonalization property we see that I carries the structure of a coalgebra such that e and m are coalgebra homomorphisms:

$$\begin{array}{ccc} \mathsf{Exp}/{=} & \xrightarrow{\overline{c}} & \mathbb{R} \times \mathsf{Exp}/{=} \\ {\scriptstyle e}\downarrow & & \downarrow{\scriptstyle \mathbb{R}\times e} \\ I & \dashrightarrow & \mathbb{R} \times I \\ {\scriptstyle m}\downarrow & & \downarrow{\scriptstyle \mathbb{R}\times m} \\ \mathbb{R}^\omega & \xrightarrow{\langle \mathsf{hd}, \mathsf{tl} \rangle} & \mathbb{R} \times \mathbb{R}^\omega \end{array}$$

Using Theorem III.14, it is now easy to prove that (a) I is locally finite dimensional, and (b) I is the final locally finite dimensional H-coalgebra, see the Appendix for details.

From item (b) we now conclude that $\mathsf{Exp}/{=}$ and I are isomorphic via the homomorphism e since final objects are unique up to isomorphism. Thus, $i = m \cdot e$ is a monomorphism as desired. ∎

Corollary V.11. *The coalgebra $\mathsf{Exp}/{=}$ is isomorphic to the coalgebra of rational streams.*

Theorem V.12. (Completeness) *For any two expressions A and B with $[\![A]\!] = [\![B]\!]$ we have $A = B$ in $\mathsf{Exp}/{=}$.*

Proof: Recall the commutative diagram (8).

Now if $[\![A]\!] = [\![B]\!]$, we have, since i is a monomorphism, that $q(A) = q(B)$, and equivalently $A = B$ holds. ∎

VI. Conclusions and Future Research

We have presented an expression calculus for finite closed valid stream circuits or, equivalently, states of finite dimensional linear systems. Our main results are a version of Kleene's theorem for finite dimensional linear systems and the soundness and completeness of our calculus for reasoning about the semantic equivalence of finite closed valid stream circuits. We also gave a general category-theoretic account of the notion of locally finite coalgebras for set functors. We introduced the notion of a locally finitely presentable coalgebra and we proved that these coalgebras are precisely the filtered colimits of coalgebras with a finitely presentable carrier. It follows that for a finitary endofunctor H of an lfp category the final locally finitely presentable coalgebra exists and is precisely the same as an initial iterative algebra for H (cf. [10]). For endofunctors of Set preserving weak pullbacks (and therefore monomorphisms) our notion coincides with that of [5]. For weak pullback preserving functors on $\mathsf{Vec}_{\mathbb{R}}$ our notion yields locally finitely dimensional coalgebras.

An immediate question for future work is the decidability of the calculus of the present paper. Furthermore, it should not be difficult to develop a general calculus which is parametric in the endofunctor H. Analogously as in the work of Bonsangue, Rutten and Silva [4], [5] our approach here should provide a Kleene theorem and a sound and complete expression calculus for various types of linear systems in a uniform way. It will also be interesting to try and develop a calculus for the semantic equivalence of open stream circuits. In this respect work on the formal language of recursion by Moschovakis et al [21] and Moss [22] and work on iteration theories [11] may well turn out to be relevant.

Finally, it should be interesting to generalize our results from the category of vector spaces to categories of algebras for a monad. More detailed, we see that our calculus is a combination of an equational presentation of vector spaces with the behavioral differential equations for the operations provided by $HX = \mathbb{R} \times X$ (which are essentially captured by the distributive law λ), and this is extended by a unique fixed point operator.

A possible generalization of our results should start with a finitary monad M of Set, a finitary functor H on Set and a distributive law λ of M over H. Then H has a lifting $\overline{H}$ to the category Set^M of Eilenberg-Moore algebras and the terminal coalgebra T for H is equipped with an M-algebra structure such that it is the terminal coalgebra for $\overline{H}$. It should be interesting to see whether an equational presentation of M and a concrete description of λ can be combined with a unique fixed point operator to obtain a sound and complete expression calculus for $\overline{H}$-coalgebras in Set^M.

Acknowledgments

The author wishes to thank Jiří Adámek and Larry Moss for useful discussions, and Alexandra Silva for her very helpful comments.

References

[1] S. C. Kleene, "Representation of events in nerve nets and finite automata," in *Automata Studies*, ser. Annals of Mathematics Studies, C. E. Shannon and J. McCarthy, Eds. Princeton University Press, 1956, no. 34, pp. 3–41.

[2] D. Kozen, "A completeness theorem for Kleene algebras and the algebra of regular events," *Inform. and Comput.*, vol. 110, no. 2, pp. 366–390, 1994.

[3] M. M. Bonsangue, J. J. M. M. Rutten, and A. Silva, "Coalgebraic logic and synthesis of mealy machines," in *Proc. Foundations of Software Science and Computation Structures (FOSSACS)*, ser. Lecture Notes Comput. Sci., vol. 4962. Springer, 2008, pp. 231–245.

[4] ——, "A Kleene theorem for polynomial coalgebras," in *Proc. Foundations of Software Science and Computation Structures (FOSSACS)*, ser. Lecture Notes Comput. Sci., L. de Alfaro, Ed., vol. 5504. Springer, 2009.

[5] ——, "An algebra for Kripke polynomial coalgebras," in *Proc. 24th Annual Symposium on Logic in Computer Science (LICS'09)*. IEEE Computer Society, 2009, pp. 49–58.

[6] F. Bonchi, M. M. Bonsangue, J. J. M. M. Rutten, and A. Silva, "Deriving syntax and axioms for quantitative regular behaviours," in *Proc. 20th International Conference on Concurrency Theory (CONCUR)*, 2009.

[7] M. Bonsangue and A. Kurz, "Presenting functors by operations and equations," in *Proc. Foundations of Software Science and Computation Structures (FOSSACS)*, ser. Lecture Notes Comput. Sci., vol. 3921. Springer, 2006.

[8] B. Jacobs, "A bialgebraic review of deterministic automata, regular expressions and languages," in *Goguen Festschrift*, ser. Lecture Notes Comput. Sci., vol. 4060, 2006.

[9] J. Adámek, S. Milius, and J. Velebil, "Free iterative theories: a coalgebraic view," *Math. Structures Comput. Sci.*, vol. 13, no. 2, pp. 259–320, 2003.

[10] J. Adámek, S. Milius, and J. Velebil, "Iterative algebras at work," *Math. Structures Comput. Sci.*, vol. 16, no. 6, pp. 1085–1131, 2006.

[11] S. L. Bloom and Z. Ésik, *Iteration Theories: the equational logic of iterative processes*, ser. EATCS Monographs on Theoretical Computer Science. Springer, 1993.

[12] J. J. M. M. Rutten, "Universal coalgebra: a theory of systems," *Theoret. Comput. Sci.*, vol. 249, no. 1, pp. 3–80, 2000.

[13] J. Lambek, "A fixpoint theorem for complete categories," *Math. Z.*, vol. 103, pp. 151–161, 1968.

[14] P. Aczel and N. Mendler, "A final coalgebra theorem," in *Proc. Category Theory and Computer Science (CTCS)*, ser. Lecture Notes Comput. Sci., vol. 389, 1989, pp. 357–365.

[15] J. J. M. M. Rutten, "A coinductive calculus of streams," *Math. Structures Comput. Sci.*, vol. 15, no. 1, pp. 93–147, 2005.

[16] ——, "Rational streams coalgebraically," *Log. Methods Comput. Sci.*, vol. 4, no. 3:9, p. 22 pp., 2008.

[17] J. Adámek and J. Rosický, *Locally presentable and accessible categories*. Cambridge University Press, 1994.

[18] C. C. Elgot, "Monadic computation and iterative algebraic theories," in *Logic Colloquium '73*. Amsterdam: North-Holland Publishers, 1975.

[19] J. Adámek, S. Milius, and J. Velebil, "Semantics of higher-order recursion schemes," in *Proc. Coalgebraic and Algebraic Methods in Computer Science (CALCO'09)*, ser. Lecture Notes Comput. Sci., A. Kurz, M. Lenisa, and A. Tarlecki, Eds., vol. 5728. Springer, 2009, pp. 49–63.

[20] S. Ginali, "Regular trees and the free iterative theory," *J. Comput. System Sci.*, vol. 18, pp. 228–242, 1979.

[21] A. J. C. Hurkens, M. McArthur, Y. N. Moschovakis, L. S. Moss, and G. T. Whitney, "The logic of recursive equations," *J. Symbolic Logic*, vol. 63, no. 2, pp. 451–478, 1998.

[22] L. S. Moss, "Recursion and corecursion have the same equational logic," *Theoret. Comput. Sci.*, vol. 294, pp. 233–267, 2003.

APPENDIX

Proof of Theorem II.1: (1) $\Rightarrow$ (2). Let (S, g) be a finite dimensional linear system. Pick a basis $\{ s_1, \ldots, s_n \}$ of S. It suffices to construct for every basis vector s_i a finite closed valid stream circuit representing the same stream as s_i. Suppose that we have

$$g(s_i) = (r_i, \sum_{j=1}^{n} r_{ij} s_j), \qquad i = 1, \ldots, n.$$

Using this information we construct a stream circuit as follows: take for every basis vector s_i a register m_i with the initial value r_i; use for each i adders and r-multipliers in the obvious way to compute from the outputs of m_j, $j = 1, \ldots, n$, the input stream of m_i according to the second component of $g(s_i)$. Clearly this yields a finite closed valid stream circuit computing at the output of the register m_i the stream represented by s_i.

(2) $\Rightarrow$ (1). Suppose we are given a finite closed valid stream circuit C. Let σ be the stream computed at some output wire o. We shall provide a finite dimensional linear system with a state representing σ. Let X be the set of registers of the given stream circuit C. The state space of the desired linear system is LX. To provide the necessary coalgebra structure $c : LX \to \mathbb{R} \times LX$ it suffices to provide for every $x \in X$ some pair $c(x) \in \mathbb{R} \times LX$. The first component of $c(x)$ is the initial value of the register x. And the second component of $c(x)$ is a formal linear combination of elements of X whose syntax tree t_x is constructed as follows: initialize t_x to be empty and traverse C backwards starting at the input wire of x; whenever an adder is met add a $+$-node to t and compute the two subtrees rooted at the node by recursively traversing the input wires of the adder; for an r-multiplier add a node labelled the corresponding scalar multiplication to t_x and to compute the subtree rooted at the new node by traversing C at the input wire of the r-multiplier; if the output wire of a copier is met during traversal of C just continue traversing at its input wire; finally, if a register $y \in X$ is met add a leaf labelled y to t_x. Since C is a finite circuit where every loop passes through at least one register, it is clear that this process stops after finitely many steps with a (syntax tree of a) finite linear combination t_x. It is also easy to prove by structural induction on t_x that the stream represented by the state x in the linear system LX is the same as the stream computed as the output of the register x. Finally, the state representing the output o is obtained by constructing an element t_o of LX in the same way as t_x above but by starting traversal of the circuit C at the wire o instead. ■

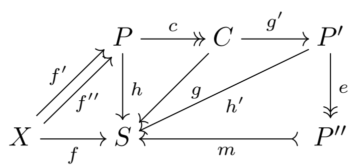
Proof of Lemma III.5: Let $q : Y \to X$ be a split epimorphism with finitely presentable domain Y. We show that X is finitely presentable, too. Choose some morphism $m : X \to Y$ with $q \cdot m = id_X$. Now suppose we have some morphism $f : Y \to C$ where $C = \operatorname{colim} C_i$ is a filtered colimit with injections $c_i : C_i \to C$. Since X is finitely presentable, we have some C_i and some morphism $f' : X \to C_i$ such that $c_i \cdot f' = f \cdot q$. Then we also have $c_i \cdot f' \cdot m = f \cdot q \cdot m = f$.

For the essential uniqueness assume that $f', f'' : Y \to C_i$ are two morphisms with $c_i \cdot f' = c_i \cdot f'' = f$. Then also $c_i \cdot f' \cdot q = c_i \cdot f'' \cdot q$. So, since X is finitely presentable, there exists some C_j and some connecting morphism $c_{ij} : C_i \to C_j$ in the diagram such that $c_{ij} \cdot f' \cdot q = c_{ij} \cdot f'' \cdot q$. Hence, we also have $c_{ij} \cdot f' = c_{ij} \cdot f''$, since q is an epimorphism. ■

Proof of Lemma III.8: We proceed in two steps:

(i) we prove that under the current assumptions condition (1) in Definition III.7 implies condition (2), and
(ii) then we prove that conditions (1) and (1') are equivalent.

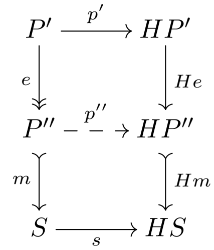
Ad (i). Suppose that (S, s) is coalgebra satisfying condition (1) of Definition III.7. We have to prove condition (2). Let $f : X \to S$ be a morphism with a finitely presentable domain, let $h : (P, p) \to (S, g)$ be a coalgebra homomorphism, where P is finitely presentable, and let $f', f'' : X \to P$ be such that $h \cdot f' = h \cdot f''$. Now take the coequalizer $c : P \to C$ of f' and f'' in $\mathscr{A}$. Since both X and P are finitely presentable, so is C, see Remark III.4(1). By the universal property of C we obtain a morphism $g : C \to S$ such that $g \cdot c = h$. Now we apply condition (1) to obtain a coalgebra (P', p') with P' finitely presentable, a morphism $g' : C \to P'$ and a coalgebra homomorphism $h' : (P', p') \to (S, s)$ such that $h' \cdot g' = g$. Now we factorize $h' = m \cdot e$ as a strong epimorphism $e : P' \to P''$ followed by a monomorphism $m : P'' \to S$. All in all we have the following commutative diagram:



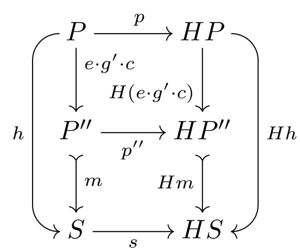
(9)

Because epimorphisms split by hypothesis, we see that P'' is a finitely presentable object (see Lemma III.5). Since H preserves monomorphisms we obtain, by the unique diagonalization property, a coalgebra structure on P'' such that e and

m are homomorphisms:



To complete the first step of the proof we show that $e \cdot g' \cdot c : P' \to P''$ is a coalgebra homomorphism merging f' and f''. Indeed, the latter is clear since $c \cdot f' = c \cdot f''$, and for the former consider the following diagram:



The outside of the diagram commutes since h is coalgebra homomorphism, the left-hand and right-hand parts commute since $h' = m \cdot e$ and by (9). Since the lower inner square commutes, we see that the upper inner square commutes when extended by Hm. So since Hm is a monomorphism the desired upper square commutes.

Ad (ii). Let (S, s) be a coalgebra. To prove that $(1) \Rightarrow (1')$ let $f : X \to S$ be a subobject. By (1) we have the coalgebra homomorphism $h : (P, p) \to (S, s)$ and $f' : X \to P$ with $h \cdot f' = f$. Now factorize $h = m \cdot e$ as a strong epimorphism followed by a monomorphism. Then the codomain is the desired subcoalgebra of S.

For the implication $(1') \Rightarrow (1)$ suppose that $f : X \to S$ is an arbitrary morphism. Take a strong epi-mono factorization $f = m \cdot e$ and apply (1') to m; so m factors through some subcoalgebra of S via some morphism m'. Then $m' \cdot e$ is the desired factorization. ■

Proof of Lemma III.9: Let (S, s) be a locally finitely presentable coalgebra and let $e : (S, s) \to (T, t)$ be an epimorphic coalgebra homomorphism, i. e., e is a coalgebra homomorphism that is an epimorphism in $\mathscr{A}$. Take some morphism $m : T \to S$ such that $e \cdot m = id_T$.

Now suppose that $f : X \to T$ is a morphism with finitely presentable domain. Since S is locally finitely presentable we have a coalgebra (P, p) with P finitely presentable, a morphism $f' : X \to P$ and a coalgebra homomorphism $h : (P, p) \to (S, s)$ such that $m \cdot f = h \cdot f'$. Then also $f = e \cdot h \cdot f'$, i. e., we have found an appropriate factorization of f. Thus, from the fact that under our assumptions condition (1) of Definition III.7 implies condition (2) (see the proof of Lemma III.8), we conclude that (T, t) is locally finitely presentable. ■

Proof of Theorem III.12: Denote by $\mathscr{A}_{\mathsf{fp}}$ the full subcategory of $\mathscr{A}$ given by all finitely presentable objects. Recall that $S = \operatorname{colim} D'$ where $D' : \mathscr{A}_{\mathsf{fp}}/S \to \mathscr{A}$ is the canonical diagram of all finitely presentable objects over S, see [17]. We shall show that the forgetful functor $U' : \mathscr{D} \to \mathscr{A}_{\mathsf{fp}}/S$ given by the forgetful functor $U : \mathsf{Coalg_f}(H) \to \mathscr{A}_{\mathsf{fp}}$ is cofinal. Indeed, for every (X, f) in $\mathscr{A}_{\mathsf{fp}}/S$ we have $((P, p), h)$ in $\mathscr{D}$ and a morphism $f' : (X, f) \to (P, h)$ in $\mathscr{A}_{\mathsf{fp}}/S$ by the fact that (S, g) is locally finitely presentable (use condition (1) in Definition III.7). Now given two morphisms $f' : (X, f) \to U'((P, p), h))$ and $f'' : (X, f) \to U'((P', p'), h')$ in $\mathscr{A}_{\mathsf{fp}}/S$ one easily finds morphisms g' and g'' in $\mathscr{D}$ with $U'(g') \cdot f' = U'(g'') \cdot f''$ using the filteredness of $\mathscr{D}$ as well as condition (2) in Definition III.7. ■

Proof of Theorem III.14: Necessity is clear. For sufficiency let (S, g) be locally finitely presentable and take any $((P, p), \mathsf{in}_p)$ in $\mathscr{D}$, see Observation III.11(2). Since (P, p) is a coalgebra in $\mathsf{Coalg_f}(H)$ we have a unique homomorphism $p^\sharp : (P, p) \to (R, r)$. Then by the uniqueness we see that all the homomorphisms $p^\sharp$ form a cocone; indeed, for every homomorphism $k : (P, p) \to (Q, q)$ in $\mathsf{Coalg_f}(H)$ we have $p^\sharp = q^\sharp \cdot k$. Thus, by the universal property of the colimit (S, g) there exists a unique homomorphism $h : (S, g) \to (R, r)$ with

$$h \cdot \mathsf{in}_p = p^\sharp \qquad \text{for all } ((P, p), \mathsf{in}_p) \text{ in } \mathscr{D}.$$

Since this equation must hold for every homomorphism from (S, g) to (R, r) by hypothesis we are done. ■

Proof of Lemma V.3: We first show that the map

$$m = (\,\mathsf{Exp} \xrightarrow{t} LH\mathsf{Exp} \xrightarrow{\lambda_{\mathsf{Exp}}} HL\mathsf{Exp} \xrightarrow{HLq} HL(\mathsf{Exp}/{=}) \xrightarrow{Ha} H(\mathsf{Exp}/{=})\,)$$

is well-defined on equivalence classes.

(1) One first verifies this for the vector space axioms. Let A be an expression with $m(A) = (r, [B])$. Then one easily checks that

$$m(A + \mu x.0 : x) = m(r + 0, [B + \mu x.0 : x]) = m(r, [B]) = m(A)$$

For the axiom $A + (-1)A = \mu x.0 : x$ we first compute

$$t(A + (-1)A) = t(A) - t(A) = 0 \in LH\mathsf{Exp}.$$

Clearly, this is mapped to $(0, [\mu x.0 : x])$ by $Ha \cdot HLq \cdot \lambda_{\mathsf{Exp}}$. Hence we have

$$m(A + (-1)A) = (0, [\mu x.0 : x]) = m(\mu x.0 : x).$$

For all the other vector space axioms, already t is well-defined: for example we have

$$t(r(A + B)) = r(t(A) + t(B)) = rt(A) + rt(B) = t(rA) + t(rB) = t(rA + rB).$$

The verification of the other vector space axioms is immediate and left to the reader.

(2) For the first of the behavioral differential equations we have

$$m(r : A + s : B) = (r, [A]) + (s, [B]) = (r + s, [A + B]) = m((r + s) : (A + B))$$

and similarly for the second one.

(3) For α-equivalence we have:

$$m(\mu y.A[y/x]) = m(A[y/x][\mu y.A[y/x]/y]) = m(A[\mu y.A[y/x]/x) = m(A[\mu x.A/x]) = m(\mu x.A),$$

where all equations except the last but one are clear. To see that the last but one equation also holds assume that

$$t(A) = \sum_{i=1}^{n} r_i(s_i, B_i)$$

for some $r_i, s_i \in \mathbb{R}$ and $B_i \in \mathsf{Exp}$, $i = 1, \dots, n$. Since substitutions in the expression A always happen within the scope of some $r : (-)$ operator we obtain

$$t(A[\mu x.A/x]) = \sum_{i=1}^{n} r_i(s_i, B_i[\mu x.A/x]) \qquad \text{and} \qquad t(A[\mu y.A[y/x]/x) = \sum_{i=1}^{n} r_i(s_i, B_i[\mu y.A[y/x]/x])$$

Now let

$$k = \sum_{i=1}^{n} r_i s_i.$$

Then one easily computes that

$$m(A[\mu x.A/x]) = \left(k, \left[\sum_{i=1}^{n} r_i B_i[\mu x.A/x]\right]\right) \qquad \text{and} \qquad m(A[\mu y.A[y/x]/x) = \left(k, \left[\sum_{i=1}^{n} r_i B_i[\mu y.A[y/x]/x]\right]\right)$$

(notice that the big square brackets indicate equivalence classes). So since $\mu x.A = \mu y.A[y/x]$ by α-equivalence, we see by applying the replacement rule that the above two equivalence classes in the right-hand components are equal.

(4) For the fixpoint axiom we see that t is well-defined by definition.

(5) For the uniqueness rule, assume that $A = B[A/x]$ with $m(A) = m(B[A/x])$. Then we have

$$m(\mu x.B) = m(B[\mu x.B/x]) = m(B[A/x]) = m(A),$$

where the last but one equation follows again by replacement using a similar argument than for α-equivalence above.

(6) For the replacement rule assume that $B = C$ in $\mathsf{Exp}/{=}$ with $m(B) = m(C)$. Then we must prove that for every expression A with one free variable x we have $m(A[B/x]) = m(A[C/x])$. This is done by induction on $N(A)$. Indeed, for $A = x$ we are done. For the case $A = r : A_0$ we have

$$m(A[B/x]) = (r, [A_0[B/x]]) = (r, [A_0[C/x]]) = m(A[C/x]).$$

Now let $A = rA_0$ so that $A[B/x] = r(A_0[B/x])$ and similarly for C. By the induction hypothesis we have $m(A_0[B/x]) = m(A_0[C/x])$ and this is some pair $(s, [D])$, say. It is easy to calculate that

$$m(rA_0[B/x]) = (rs, r[D]) = m(rA_0[C/x]).$$

The case $A = A_1 + A_2$ is analogous.

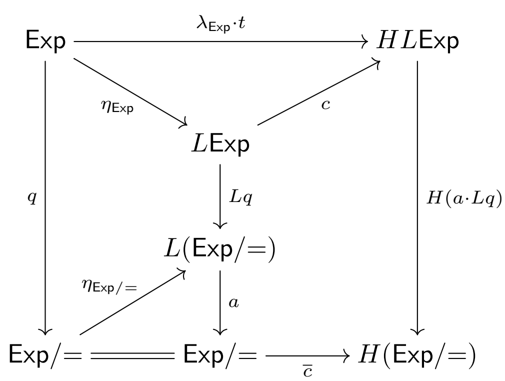
Finally, let $A = \mu y.A_0$. By the induction hypothesis we have

$$m(A_0[\mu y.A_0/y][B/x]) = m(A_0[\mu y.A_0/y][C/x]).$$

So we can compute

$$\begin{array}{rcll} m(A[B/x]) & = & m(\mu y.A_0[B/x]) & \text{since } A = \mu y.A_0 \\ & = & m(A_0[B/x][\mu y.A_0[B/x]/y]) & \text{since } m \text{ is well-defined for the fixpoint rule} \\ & = & m(A_0[\mu y.A_0/y][B/x]) & \text{by the properties of substitution} \\ & = & m(A_0[\mu y.A_0/y][C/x]) & \text{by induction hypothesis} \\ & = & m(A[C/x]) & \text{similar computation backwards.} \end{array}$$

We are finished with the proof that m is well-defined. Thus, we can define a coalgebra structure $\overline{c} : \mathsf{Exp}/{=} \to H(\mathsf{Exp}/{=})$ by putting $\overline{c}([A]) = m(A)$. It now follows that $a \cdot Lq$ is a coalgebra homomorphism as desired; indeed, consider the diagram below:



(10)

This diagram commutes: the outside commutes by the definition of $\overline{c}$, the left-hand part by the naturality of $\eta : Id \to L$, the upper triangle commutes by the definition of the linear map c and the lower left-hand triangle is the unit law of the Eilenberg-Moore algebra $(\mathsf{Exp}/{=}, a)$ for L. This shows that the desired right-hand part commutes when precomposed with η_{Exp}, and since all morphisms in this part are linear maps, this part commutes by the universal property of the free vector space $L\mathsf{Exp}$. ■

Proof of Lemma V.4: Let (S, g) be a finite dimensional linear system. Take a basis $\{ s_1, \ldots, s_n \}$ for S and let

$$g(s_i) = \left(r_i, \sum_{j=1}^{n} r_{ij} s_j \right), \qquad i = 1, \ldots, n. \tag{11}$$

We shall construct expressions $\langle\langle s_i \rangle\rangle$ for every $i = 1, \ldots, n$ by an n-step process. Our expressions will involve the variables $x_1, \ldots, x_n$. For every i, let

$$A_i^0 = \mu x_i.(r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)).$$

Now define for $k = 0, \ldots, n-1$

$$A_i^{k+1} = \begin{cases} A_i^k\{A_{k+1}^k/x_{k+1}\} & \text{if } i \neq k+1 \\ A_i^k & \text{if } i = k+1 \end{cases}$$

where $\{A/x\}$ denotes syntactic replacement (i. e., substitution without renaming of bound variables). It is easy to see that the set of free variables of A_i^k is $\{x_{k+1}, \ldots x_n\} \setminus \{ x_i \}$, and moreover, every occurrence of those variables is free.

We also see that for every i,

$$\begin{array}{rcl} A_i^n & = & A_i^0\{A_1^0/x_1\}\{A_2^1/x_2\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^{i}/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\} \qquad (12) \\ & = & A_i^{i-1}\{A_{i+1}^{i}/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\}. \qquad (13) \end{array}$$

Observe that A_i^n is a closed term. Moreover, the variable x_i from A_i^0 is never syntactically replaced and it is bound by the outermost μx_i. All other occurrences of x_i in A_i^n are not bound by this μ-operator (but by μ-operators further inside the term). We define

$$\langle\langle s_i \rangle\rangle = A_i^n.$$

From now on we shall abuse notation and we will denote equivalence classes $[A]$ of expressions in $\mathsf{Exp}/{=}$ simply by expressions A representing them.

We will now prove that the desired coalgebra homomorphism $h : S \to \mathsf{Exp}/{=}$ is the linear map given by $h(s_i) = \langle\langle s_i \rangle\rangle$. It suffices to verify that $Hh \cdot g(s_i) = \overline{c} \cdot h(s_i)$ holds for all basis vectors s_i. We first establish that we have the provable equalities

$$\langle\langle s_i \rangle\rangle = r_i : (r_{i1}\langle\langle s_1 \rangle\rangle + \cdots + r_{in}\langle\langle s_n \rangle\rangle), \qquad i = 1, \ldots, n. \tag{14}$$

To see this we compute as follows (and we explain the computation steps below):

$$\begin{array}{rcl}
\langle\langle s_i \rangle\rangle & \stackrel{\text{(i)}}{=} & A_i^n \\
& \stackrel{\text{(ii)}}{=} & A_i^0\{A_1^0/x_1\}\{A_2^1/x_2\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\} \\
& \stackrel{\text{(iii)}}{=} & r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)\{A_1^0/x_1\}\{A_2^1/x_2\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\}[A_i^n/x_i] \\
& \stackrel{\text{(iv)}}{=} & r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)\{A_1^0/x_1\}\{A_2^1/x_2\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\}\{A_i^n/x_i\} \\
& \stackrel{\text{(v)}}{=} & r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)\{A_1^0/x_1\}\cdots\{A_n^{n-1}/x_n\} \\
& \stackrel{\text{(vi)}}{=} & r_i : (\sum_{j=1}^{n} r_{ij}A_j^{j-1}\{A_{j+1}^j/x_{j+1}\}\cdots\{A_n^{n-1}/x_n\}) \\
& \stackrel{\text{(vii)}}{=} & r_i : (\sum_{j=1}^{n} r_{ij}\langle\langle s_j \rangle\rangle)
\end{array}$$

Indeed, step (i) is the definition of $\langle\langle s_i \rangle\rangle$, equation (ii) holds due to (12), for step (iii) one applies the fixpoint axiom, equation (iv) holds since A_i^n has no free variables, in step (vi) we just perform the syntactic replacement, and the last equation (vii) holds due to (13). It remains to verify equation (v). Here we use the fact that the following syntactic identity holds

$$A\{B/x\}\{C\{B/x\}/y\} \equiv A\{C/y\}\{B/x\}. \tag{15}$$

Let us write A for $r_i : (r_{i1}x_1 + \cdots + r_{in}x_n)$, for short. Using (12), repeated application of (15) yields

$$\begin{array}{l}
A\{A_1^0/x_1\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\}\{A_i^n/x_i\} \\
= \quad A\{A_1^0/x_1\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_i^{n-1}/x_i\}\{A_n^{n-1}/x_n\} \\
\vdots \\
= \quad A\{A_1^0/x_1\}\cdots\{A_{i-1}^{i-2}/x_{i-1}\}\{A_i^{i-1}/x_i\}\{A_{i+1}^i/x_{i+1}\}\cdots\{A_n^{n-1}/x_n\}.
\end{array}$$

We are done with the verification of (14). Finally we verify that h is a coalgebra homomorphism; indeed, for every basis vector s_i we have

$$\begin{array}{rcll}
\overline{c} \cdot h(s_i) & = & \overline{c}(\langle\langle s_i \rangle\rangle) & \text{definition of } h \\
& = & \overline{c}(r_i : (r_{i1}\langle\langle s_1 \rangle\rangle + \cdots + r_{in}\langle\langle s_n \rangle\rangle)) & \text{by (14)} \\
& = & (r_i, (r_{i1}\langle\langle s_1 \rangle\rangle + \cdots + r_{in}\langle\langle s_n \rangle\rangle)) & \text{definition of } \overline{c} \\
& = & (r_i, (r_{i1}h(s_1) + \cdots + r_{in}h(s_n))) & \text{definition of } h \\
& = & (r_i, h(r_{i1}s_1 + \cdots + r_{in}s_n)) & \text{since } h \text{ is linear} \\
& = & Hh(r_i, r_{i1}s_1 + \cdots + r_{in}s_n) & \\
& = & Hh \cdot g(s_i) &
\end{array}$$

This completes the proof. ■

Proof of Lemma V.10: Let us define a map $\overline{d} : \mathbb{R} \times \mathsf{Exp}/{=} \to \mathsf{Exp}/{=}$ by

$$\overline{d}(r, [A]) = [r : A].$$

This map is well-defined by the replacement rule, and it is easy to see that $\overline{d}$ is linear. We obviously have $\overline{c} \cdot \overline{d} = id$.

Now we verify that $\overline{d} \cdot \overline{c} = id$, i.e., we show that for every expression A we have $\overline{d} \cdot \overline{c}(A) = A$ by induction on $N(A)$. Indeed, for $A = r : B$ we compute (dropping equivalence classes as usual)

$$\overline{d} \cdot \overline{c}(A) = \overline{d}(r, B) = r : B = A.$$

For $A = B + C$ we have

$$\overline{d} \cdot \overline{c}(A) = \overline{d}(\overline{c}(B) + \overline{c}(C)) = \overline{d} \cdot \overline{c}(B) + \overline{d} \cdot \overline{c}(C) = B + C = A,$$

using the induction hypothesis in the last but one step. The case $A = rB$ is completely analogous, and we leave it to the reader. Finally, for $A = \mu x.B$ we have

$$\overline{d} \cdot \overline{c}(A) = \overline{d} \cdot \overline{c}(B[A/x]) = B[A/x] = \mu x.B = A,$$

where in the second step we use the induction hypothesis. ■

Proof of Lemma V.8: We only need to verify the uniqueness; the existence of a homomorphism was proved in Lemma V.4.

So suppose we have a coalgebra homomorphism $m : (S, g) \to (\mathsf{Exp}/{=}, \overline{c})$. We will prove that m is equal to the homomorphism h from Lemma V.4. As before we fix a basis $\{ s_1, \ldots, s_n \}$ of S. Then it suffices to prove for every basis vector $s_i \in S$ that $m(s_i) = \langle\langle s_i \rangle\rangle$. Let us write m_i for $m(s_i)$, for short. Let $g(s_i)$ be as in (11). Then we compute

$$\begin{aligned} m_i &= \overline{c}^{-1} \cdot Hm \cdot g(s_i) && (m \text{ homomorphism and Lemma V.10}) \\ &= \overline{c}^{-1} \cdot Hm(r_i, \sum_{j=1}^{n} r_{ij} s_j) && (\text{by (11)}) \\ &= \overline{c}^{-1}(r_i, \sum_{j=1}^{n} r_{ij} m(s_j)) \\ &= r_i : (\sum_{j=1}^{n} r_{ij} m_j). \end{aligned} \tag{16}$$

For the proof that $m_i = \langle\langle s_i \rangle\rangle$, we show the case $n = 3$ in detail; the general case is completely analogous and is left to the reader.

We start by proving that $m_1 = A_1^0[m_2/x_2][m_3/x_3]$ by an application of the uniqueness rule; indeed, from (16) we get

$$\begin{aligned} m_1 &= r_1 : r_{11} m_1 + r_{12} m_2 + r_{13} m_3 \\ &= ((r_1 : (r_{11} x_1 + r_{12} x_2 + r_{13} x_3)[m_2/x_2][m_3/x_3])[m_1/x_1] \end{aligned}$$

Next, we prove that $m_2 = A_2^1[m_3/x_3]$. Notice that $A_1^0[m_2/x_2][m_3/x_3] = A_1^0[m_3/x_3][m_2/x_2]$ since m_2 and m_3 are closed. Then, applying (16), we have

$$\begin{aligned} m_2 &= r_2 : (r_{21} m_1 + r_{22} m_2 + r_{23} m_3) \\ &= r_2 : (r_{21} A_1^0[m_2/x_2][m_3/x_3] + r_{22} m_2 + r_{23} m_3) \\ &= \big(r_2 : (r_{21} A_1^0[m_3/x_3] + r_{22} x_2 + r_{23} m_3)\big)\, [m_2/x_2] \end{aligned}$$

and so we can apply the uniqueness rule to obtain the desired equation.

Now we are able to prove that

$$m_1 = A_1^0\{A_2^1/x_2\}[m_3/x_3].$$

Notice first that we have $A_1^0\{A_2^1/x_2\} = A_1^0[A_2^1/x_2]$ since x_1 (which is bound in A_1^0) is not free in A_2^1. Now we obtain

$$\begin{aligned} A_1^0[A_2^1/x_2][m_3/x_3] &= A_1^0[m_3/x_3][A_2^1[m_3/x_3]/x_2] \\ &= A_1^0[m_3/x_3][m_2/x_2] \\ &= m_1. \end{aligned}$$

Finally, we show that $m_3 = A_3^2$ by another application of the uniqueness rule; we have

$$\begin{aligned} m_3 &= r_3 : (r_{31} m_1 + r_{32} m_2 + r_{33} m_3) \\ &= r_3 : (r_{31} A_1^0\{A_2^1/x_2\}[m_3/x_3] + r_{32} A_2^1[m_3/x_3] + r_{33} m_3) \\ &= (r_3 : (r_{31} A_1^0\{A_2^1/x_2\} + r_{32} A_2^1 + r_{33} x_3))[m_3/x_3]. \end{aligned}$$

So we have proved

$$m_3 = A_3^2 = A_3^3 = \langle\langle s_3 \rangle\rangle.$$

This implies that

$$m_2 = A_2^1[m_3/x_3] = A_2^1[A_3^2/x_3] = A_2^1\{A_3^2/x_3\} = A_2^3 = \langle\langle s_2 \rangle\rangle,$$

where the third equation holds since the bound variables x_1 and x_2 of A_2^1 are also bound in A_3^2. Similarly, we have

$$m_1 = A_1^0\{A_2^1/x_2\}[m_3/x_3] = A_1^0\{A_2^1/x_2\}[A_3^2/x_3] = A_1^0\{A_2^1/x_2\}\{A_3^2/x_3\} = A_1^3 = \langle\langle s_1 \rangle\rangle.$$

This completes the proof. ■

Proof of Lemma V.10: Take the factorization of i into a surjective followed by an injective linear map:

$$i = (\,\mathsf{Exp}/{=} \xrightarrow{e} \!\!\!\!\rightarrow I \rightarrowtail^{m} \mathbb{R}^\omega\,)$$

Observe that the functor $HX = \mathbb{R} \times X$ preserves monomorphisms. By the unique diagonalization property we see that I carries the structure of a coalgebra such that e and m are coalgebra homomorphisms:

$$\begin{array}{ccc}
\mathsf{Exp}/{=} & \xrightarrow{\overline{c}} & \mathbb{R} \times \mathsf{Exp}/{=} \\
{\scriptstyle e}\downarrow & & \downarrow{\scriptstyle \mathbb{R}\times e} \\
I & \dashrightarrow & \mathbb{R} \times I \\
{\scriptstyle m}\downarrow & & \downarrow{\scriptstyle \mathbb{R}\times m} \\
\mathbb{R}^\omega & \xrightarrow{\langle \mathsf{hd}, \mathsf{tl} \rangle} & \mathbb{R} \times \mathbb{R}^\omega
\end{array}$$

It is now easy to show that (a) I is locally finite dimensional, and (b) I is the final locally finite dimensional H-coalgebra.

Ad (a): This follows from Lemma III.9 since $\mathsf{Exp}/{=}$ is locally finite dimensional and since $HX = \mathbb{R} \times X$ preserves monomorphisms.

Ad (b): for every finite dimensional coalgebra (S, g) we have the homomorphism $e \cdot h : S \to I$, where h is the homomorphism obtained by Lemma V.4. This must be unique; indeed, if $h' : S \to I$ is any other homomorphism we have $m \cdot h' = m \cdot e \cdot h$ by the finality of $\mathbb{R}^\omega$. So since m is a monomorphism we also have $h' = e \cdot h$. That I is the final locally finite dimensional coalgebra now follows from Theorem III.14.

From item (b) we now conclude that $\mathsf{Exp}/{=}$ and I are isomorphic via the homomorphism e since final objects are unique up to isomorphism. Thus, $i = m \cdot e$ is a monomorphism as desired. ■