Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Left-handed completeness

Dexter Kozen [a,*], Alexandra Silva [b,*]

[a] Computer Science Department, Cornell University, Ithaca, NY 14853-7501, USA
[b] Department of Computer Science, University College London, Gower Street, London WC1E 6BT, UK

ARTICLE INFO

Article history:
Received 1 August 2018
Received in revised form 24 October 2019
Accepted 26 October 2019
Available online xxxx

In memory of Maurice Nivat

Keywords:
Nivat
Kleene algebra
Completeness

ABSTRACT

We give a new proof of the completeness of the left-handed star rule of Kleene algebra. The proof is significantly shorter than previous proofs and exposes the rich interaction of algebra and coalgebra in the theory of Kleene algebra.

1. Introduction

Axiomatizations of the equational theory of the regular sets over a finite alphabet have received much attention over the years. The topic was introduced in the seminal 1956 paper of Kleene [8], who left axiomatization as an open problem. Salomaa [18] gave two complete axiomatizations, but these depended on rules of inference that were sound under the standard interpretation but not under other natural interpretations. Conway, in his monograph [3], coined the term *Kleene algebra* (KA) and contributed substantially to the understanding of the question of axiomatization. An algebraic solution was presented by Kozen [11,12], who postulated two equational implications, similar to the inference rules of Salomaa; but unlike Salomaa's rules, they are universal Horn formulas, therefore sound over a variety of nonstandard interpretations. The main goal of this paper is to show that only one of the two implications is enough to guarantee completeness.

This result, which we shall call *left-handed completeness*, is a known result. It was claimed without proof by Conway [3, Theorem 12.5]. The only extant proof, by Boffa [1], relies on a lengthy (137 journal pages!) result of Krob [15], who presented a schematic equational axiomatization representing infinitely many equations. Krob's result was also later reworked and generalized in the framework of iteration theories [5].

Purely equational axiomatizations are undesirable for several reasons. From a practical point of view, they are inadequate for reasoning in the presence of other equational assumptions, which is almost always the case in real-life applications. For example, consider the redundant assignment $x := 1\,;\, x := 1$ and let a stand for $x := 1$. We have $aa = a$, since the assignment is redundant. We would expect this equation to imply $a^* = 1 + a$ (intuitively, performing the assignment $x := 1$ any number of times is equivalent to performing it zero or one times), but this is not entailed by the equational theory plus the extra equation $aa = a$. To see this, consider the free R-algebra (Conway's terminology for an algebra satisfying all the equations of the regular sets) on the finite monoid $\{1, a\}$, where $aa = a$. This algebra contains six elements: $0, 1, a, 1 + a, a^*, aa^*$. The elements a^* and $1 + a$ are distinct, even under the assumption $aa = a$, which is not at all desirable. This is an example of a

* Corresponding authors.
E-mail addresses: kozen@cs.cornell.edu (D. Kozen), alexandra.silva@ucl.ac.uk (A. Silva).

https://doi.org/10.1016/j.tcs.2019.10.040
0304-3975/

finite algebra that satisfies all the equations of KA but is not a KA itself, because in a finite KA a star is always equal to a finite sum of powers. This example shows that purely equational axiomatizations would be inadequate for even the simplest verification tasks involving iteration in the presence of other equations.

On the other hand, characterizing a^* as a least fixpoint is a natural and powerful device, and is satisfied in virtually all models that arise in real life. However, there are interesting and useful models that satisfy only one of the two star rules. These models appear in program analysis and abstract interpretation [9,10] and proof theory for partial correctness logic [14]. For such applications, it is useful to know that only one of the rules is needed for equational completeness.

Even though we present a new proof of a known result, there is added value in the exploration of the exquisite interplay between algebra and coalgebra in the theory of regular sets, which is visible throughout the technical development of the paper and notably in the novel definition of a *differential Kleene algebra*, which captures abstractly the relationship between the algebraic and coalgebraic structure of KA. The (syntactic) Brzozowski derivative provides the link from the algebraic to the coalgebraic view of regular expressions, whereas the canonical embedding of a given coalgebra into a matrix algebra plays the converse role. This interplay between algebra and coalgebra, first explored in [7,16], has opened the door to far-reaching extensions of Kleene's theorem and Kleene algebras [19].

Another contribution is a clear characterization of how far one can go in the proof of completeness with just equations. We show that the equational implication is needed only at two places (Lemmas 3.3 and 4.3). Furthermore, we show that the existence of least solutions implies uniqueness of solutions in the free algebra, which neatly ties our axiomatization with the original axiomatization of Salomaa.

This paper is a full version of [13] containing detailed proofs of all results. Since the appearance of this paper, other authors have investigated left-handed Kleene algebra and alternative proofs of completeness [4,6].

2. Axiomatization

2.1. Left-handed Kleene algebra

A *weak Kleene algebra* (*weak* KA) is an idempotent semiring with star satisfying

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

The second and third equations of (1) are called *sliding* and *denesting*, respectively. The axioms (1) were studied in depth by Conway [3] under the names *productstar* for the combination of the first two in the single equation $(ab)^* = 1 + a(ba)^*b$, *sumstar*, and *starstar*, respectively. Although incomplete, these equations are sufficient for many arguments involving the star operator.

Conway studied many other useful families of axioms, including the *powerstar rules*

$$a^* = (a^n)^* \sum_{i=0}^{n-1} a^i, \tag{2}$$

although we will not need them here.

A *left-handed Kleene algebra* (LKA) is a weak KA satisfying a certain universal Horn formula, called the *left-handed star rule*, which may appear in either of the two equivalent forms

$$b + ax \le x \Rightarrow a^*b \le x \qquad ax \le x \Rightarrow a^*x \le x, \tag{3}$$

where $\le$ is the natural partial order given by $a \le b \Leftrightarrow a + b = b$. One consequence is the *left-handed bisimulation rule*

$$ax \le xb \Rightarrow a^*x \le xb^*.$$

2.2. Matrices

Let $\mathrm{Mat}(S, K)$ be the family of square matrices with rows and columns indexed by a finite set S with entries in a semiring K. Conway [3] shows that under the appropriately defined matrix operations, the axioms (1) imply themselves for matrices. This is also true for (3) [12]. It is known for the powerstar rules (2) too, but only in a weaker form [3].

The *characteristic matrix* P_f of a function $f : S \to S$ has $(P_f)_{st} = 1$ if $f(s) = t$, 0 otherwise. A matrix is a *function matrix* if it is P_f for some f; that is, each row contains exactly one 1 and all other entries are 0.

Let $S_1, \ldots, S_n \subseteq S$ be a partition of S. A matrix $A \in \mathrm{Mat}(S, K)$ is said to be *block diagonal with blocks* $S_1, \ldots, S_n$ if $A_{st} = 0$ whenever s and t are in different blocks.

Lemma 2.1. *Let $A, P_f \in \mathrm{Mat}(S, K)$ with P_f the characteristic matrix of a function $f : S \to S$. The following are equivalent:*

(i) *A is block diagonal with blocks refining the kernel of f; that is, if $A_{st} \neq 0$, then $f(s) = f(t)$;*
(ii) *$AP_f = DP_f$ for some diagonal matrix D;*
(iii) *$AP_f = DP_f$, where D is the diagonal matrix $D_{ss} = \sum_{f(s)=f(t)} A_{st}$.*

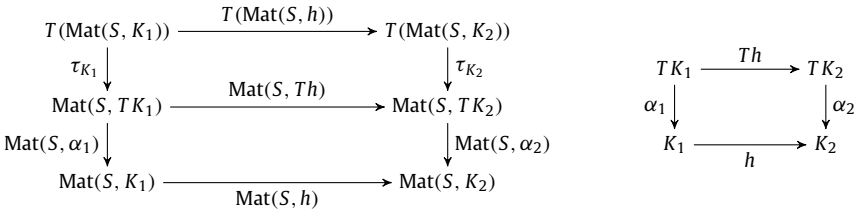

Fig. 1. Weak KA homomorphisms.

Proof. Suppose $AP_f = DP_f$, where D is diagonal. Then

$$(DP_f)_{su} = \sum_t D_{st}(P_f)_{tu} = D_{ss}(P_f)_{su} \qquad (AP_f)_{su} = \sum_t A_{st}(P_f)_{tu} = \sum_{u=f(t)} A_{st},$$

so if $A_{st} \neq 0$ and $f(t) = u$, then $D_{ss}(P_f)_{su} \neq 0$, therefore $f(s) = u$. Thus, (ii) implies (i).

If (i) holds, then $A_{st} = 0$ if $f(s) \neq f(t)$, therefore

$$(AP_f)_{su} = \sum_{u=f(t)} A_{st} = \sum_{u=f(t)=f(s)} A_{st} = \left(\sum_{f(s)=f(t)} A_{st} \right) (P_f)_{su} = D_{ss}(P_f)_{su} = (DP_f)_{su},$$

where D is the diagonal matrix with $D_{ss} = \sum_{f(s)=f(t)} A_{st}$. Thus, (i) implies (iii). We can now conclude the proof, since (iii) implies (ii) trivially. □

For any function $h : K_1 \to K_2$, let $\widehat{h} = \mathrm{Mat}(S, h) : \mathrm{Mat}(S, K_1) \to \mathrm{Mat}(S, K_2)$ denote the function on matrices obtained by applying h componentwise; that is, for $A \in \mathrm{Mat}(S, K_1)$, $\widehat{h}(A)_{st} = h(A_{st})$.

Lemma 2.2. *If $h : K_1 \to K_2$ is a weak* KA *homomorphism, then so is $\widehat{h} : \mathrm{Mat}(S, K_1) \to \mathrm{Mat}(S, K_2)$. Thus the matrix construction* $\mathrm{Mat}(S, -)$ *constitutes an endofunctor on the categories of weak and left-handed Kleene algebras.*

Proof. The KA operations on matrices are defined uniformly in terms of regular expressions on their components; for example,

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix}^* = \begin{bmatrix} (a + bd^*c)^* & (a + bd^*c)^*bd^* \\ (d + ca^*b)^*ca^* & (d + ca^*b)^* \end{bmatrix}$$

Composing these definitions, any KA expression over matrices $e(A_1, \ldots, A_m)$, $A_i \in \mathrm{Mat}(S, K)$, can be transformed inductively to a matrix E of expressions over K, and the value of $e(A_1, \ldots, A_m)$ in the matrix algebra is the matrix obtained by evaluating the components of E in K.

Formally, the transformation of an expression over matrices to a matrix of expressions constitutes a natural transformation $\tau : T(\mathrm{Mat}(S, -)) \to \mathrm{Mat}(S, T(-))$, where T is the term monad for the signature of KA. Viewing weak KAs as Eilenberg-Moore algebras with evaluation maps $\alpha : TK \to K$, the evaluation mechanism for matrices can be formally described as

$$\widehat{\alpha} \circ \tau_K = \mathrm{Mat}(S, \alpha) \circ \tau_K : T(\mathrm{Mat}(S, K)) \to \mathrm{Mat}(S, K).$$

The desired conclusion of the lemma is expressed by the commutativity of the outer rectangle in the left-hand diagram of Fig. 1. In that diagram, the upper rectangle commutes because τ is a natural transformation, and the lower rectangle commutes because it is the Set functor $\mathrm{Mat}(S, -)$ applied to the right-hand diagram, which commutes since h is a homomorphism. □

2.3. Differential Kleene algebra

A *differential Kleene algebra* (DKA) K is a weak KA containing a (finite) set $\Sigma \subseteq K$, called the *actions*, and a subalgebra C, called the *observations*, such that

(i) $ac = ca$ for all $a \in \Sigma$ and $c \in C$, and
(ii) C and Σ generate K,

$$\begin{aligned}
\delta_a(e_1+e_2) &= \delta_a(e_1)+\delta_a(e_2) & \varepsilon(e_1+e_2) &= \varepsilon(e_1)+\varepsilon(e_2)\\
\delta_a(e_1e_2) &= \delta_a(e_1)e_2+\varepsilon(e_1)\delta_a(e_2) & \varepsilon(e_1e_2) &= \varepsilon(e_1)\varepsilon(e_2)\\
\delta_a(e^*) &= \varepsilon(e^*)\delta_a(e)\,e^* & \varepsilon(e^*) &= \varepsilon(e)^*\\
\delta_a(b) &= \begin{cases}1 & \text{if } a=b,\\ 0 & \text{if } a\neq b,\end{cases} \quad b\in\Sigma & \varepsilon(b) &= 0,\ b\in\Sigma\\
\delta_a(c) &= 0,\ c\in C & \varepsilon(c) &= c,\ c\in C
\end{aligned}$$

Fig. 2. Brzozowski derivatives.

and supporting a *Brzozowski derivative* consisting of a pair of functions $\varepsilon : K \to C$ and $\delta_a : K \to K$ for $a \in \Sigma$ satisfying the equations in Fig. 2. Thus $\varepsilon : K \to C$ is a retract (a KA homomorphism that is the identity on C, which immediately implies $0, 1 \in C$). The functions δ_a and ε impart a coalgebra structure of signature $-^{\Sigma} \times C$ in addition to the Kleene algebra structure.

This definition is a modest generalization of the usual situation in which $C = \mathbb{2} = \{0, 1\}$ and the function ε and δ_a are the (syntactic) Brzozowski derivatives. We will be primarily interested in matrix DKAs in which C is the set of square matrices over $\mathbb{2}$ (see Theorem 2.5 below).

2.4. Examples

One example of a DKA with observations $\mathbb{2}$ is $\mathsf{Brz} = (2^{\Sigma^*}, \delta, \varepsilon)$, where $\varepsilon(A) = 1$ iff A contains the null string and 0 otherwise, and $\delta_a : 2^{\Sigma^*} \to 2^{\Sigma^*}$ is the classical *Brzozowski derivative*

$$\delta_a(A) = \{x \in \Sigma^* \mid ax \in A\}.$$

This is the final coalgebra of the functor $-^{\Sigma} \times \mathbb{2}$ [16]. It is also an LKA under the usual set-theoretic operations.

Another example is the free LKA K_Σ on generators Σ. It is also a DKA, where δ_a and ε are defined inductively on the syntax of regular expressions according to Fig. 2. The maps δ_a and ε are easily shown to be well defined modulo the axioms of LKA.

These structures possess both an algebra and a coalgebra structure, and in fact are bialgebras [7]. Our main result essentially shows that the latter is isomorphically embedded in the former.

2.5. Properties of DKAs

Silva [19] calls the following result the *fundamental theorem* in analogy to a similar result proved for infinite streams by Rutten [17], closely related to the fundamental theorem of calculus. It is fundamental in the sense that it connects the differential structure, given by δ_a and ε, with the axioms of LKA. We show here that the result holds under weaker assumptions than those assumed in [19]: in fact, we prove this theorem using only equations.

Theorem 2.3. *Let K be a* DKA. *For all elements $e \in K$,*

$$e = \sum_{a\in\Sigma} a\delta_a(e) + \varepsilon(e). \tag{4}$$

Proof. We proceed by induction on the generation of e from Σ and C using only equations of weak KA and properties of derivatives. For $e \in C$, $\varepsilon(e) = e$ and $\delta_a(e) = 0$, thus (4) holds. For $e = a \in \Sigma$, the right-hand side of (4) reduces to a, thus (4) holds in this case as well.

For the induction step, the case of $+$ is straightforward. For multiplication,

$$\begin{aligned}
e_1e_2 &= (\sum_{a\in\Sigma} a\delta_a(e_1) + \varepsilon(e_1))e_2 = \sum_{a\in\Sigma} a\delta_a(e_1)e_2 + \varepsilon(e_1)(\sum_{a\in\Sigma} a\delta_a(e_2) + \varepsilon(e_2))\\
&= \sum_{a\in\Sigma} a\delta_a(e_1)e_2 + \sum_{a\in\Sigma} a\varepsilon(e_1)\delta_a(e_2) + \varepsilon(e_1)\varepsilon(e_2)\\
&= \sum_{a\in\Sigma} a(\delta_a(e_1)e_2 + \varepsilon(e_1)\delta_a(e_2)) + \varepsilon(e_1e_2) = \sum_{a\in\Sigma} a\delta_a(e_1e_2) + \varepsilon(e_1e_2).
\end{aligned}$$

For e^*, we use the identity

$$(x+y)^* = y^* + y^*x(x+y)^*, \tag{5}$$

which follows easily from the axioms of weak KA. Using this identity with $x = \sum_{a\in\Sigma} a\delta_a(e)$ and $y = \varepsilon(e)$,

$$e^* = (\sum_{a\in\Sigma} a\delta_a(e) + \varepsilon(e))^* = \varepsilon(e)^* \sum_{a\in\Sigma} a\delta_a(e)e^* + \varepsilon(e)^* \qquad \text{by (5)}$$
$$= \sum_{a\in\Sigma} a\varepsilon(e)^*\delta_a(e)e^* + \varepsilon(e)^* = \sum_{a\in\Sigma} a\delta_a(e^*) + \varepsilon(e^*). \qquad \square$$

2.6. *Matrix* DKA*s*

We have already argued that $\mathrm{Mat}(S,K)$ is a weak KA if K is and an LKA if K is. In this section we show that the coalgebraic structure of Fig. 2 can be similarly lifted to matrices (Theorem 2.5).

Let $\widehat{\delta}_a = \mathrm{Mat}(S,\delta_a)$ and $\widehat{\varepsilon} = \mathrm{Mat}(S,\varepsilon)$ as described in §2.2. Let $\Delta(a) \in \mathrm{Mat}(S,K)$ be the diagonal matrix with $\Delta(a)_{ss} = a$.

Lemma 2.4. *Let K be a* DKA. *Then* $\mathrm{Mat}(S,K)$ *satisfies* (4)*; that is,*

$$E = \sum_{a\in\Sigma} \Delta(a)\widehat{\delta}_a(E) + \widehat{\varepsilon}(E). \tag{6}$$

Proof. For indices $s,t \in S$,

$$E_{st} = \sum_{a\in\Sigma} a\delta_a(E_{st}) + \varepsilon(E_{st}) = \sum_{a\in\Sigma} \Delta(a)_{ss}\widehat{\delta}_a(E)_{st} + \widehat{\varepsilon}(E)_{st}$$
$$= \sum_{a\in\Sigma}\sum_u \Delta(a)_{su}\widehat{\delta}_a(E)_{ut} + \widehat{\varepsilon}(E)_{st} = \sum_{a\in\Sigma} (\Delta(a)\widehat{\delta}_a(E))_{st} + \widehat{\varepsilon}(E)_{st}$$
$$= (\sum_{a\in\Sigma} \Delta(a)\widehat{\delta}_a(E) + \widehat{\varepsilon}(E))_{st}.$$

As $s,t \in S$ were arbitrary, (6) follows. $\square$

Theorem 2.5. *Let K be a* DKA *with observations C and actions Σ. Then* $\mathrm{Mat}(S,K)$ *is a* DKA *with observations* $\mathrm{Mat}(S,C)$ *and actions* $\Delta(a)$, $a \in \Sigma$.

Proof. Embed K into $\mathrm{Mat}(S,K)$ by $a \mapsto \Delta(a)$. By (i) for K, $\Delta(a)A = A\Delta(a)$ for $A \in \mathrm{Mat}(S,C)$, therefore (i) holds for $\mathrm{Mat}(S,K)$, and it is easily shown that $\mathrm{Mat}(S,K)$ is generated by $\mathrm{Mat}(S,C)$ and $\Delta(a)$ for $a \in \Sigma$, so (ii) holds as well.

We now verify the Brzozowski properties of Fig. 2. For $\widehat{\varepsilon}$, this is immediate from Lemma 2.2. For $\widehat{\delta}_a$, all cases are straightforward except multiplication and star. For multiplication, for indices $s,t \in S$,

$$\widehat{\delta}_a(AB)_{st} = \delta_a((AB)_{st}) = \sum_u \delta_a(A_{su}B_{ut}) = \sum_u \delta_a(A_{su})B_{ut} + \sum_u \varepsilon(A_{su})\delta_a(B_{ut})$$
$$= \sum_u \widehat{\delta}_a(A)_{su}B_{ut} + \sum_u \widehat{\varepsilon}(A)_{su}\widehat{\delta}_a(B)_{ut} = (\widehat{\delta}_a(A)B + \widehat{\varepsilon}(A)\widehat{\delta}_a(B))_{st}.$$

As s,t were arbitrary,

$$\widehat{\delta}_a(AB) = \widehat{\delta}_a(A)B + \widehat{\varepsilon}(A)\widehat{\delta}_a(B). \tag{7}$$

For star, we again use (5), this time with $x = \sum_{a\in\Sigma} \Delta(a)\widehat{\delta}_a(E)$ and $y = \widehat{\varepsilon}(E)$. By this and Lemma 2.4, we have

$$E^* = \widehat{\varepsilon}(E^*) + \sum_{a\in\Sigma} \widehat{\varepsilon}(E^*)\Delta(a)\widehat{\delta}_a(E)E^*.$$

By linearity of $\widehat{\delta}_a$,

$$\widehat{\delta}_a(E^*) = \widehat{\delta}_a(\widehat{\varepsilon}(E^*)) + \sum_{b\in\Sigma} \widehat{\delta}_a(\widehat{\varepsilon}(E^*)\Delta(b)\widehat{\delta}_b(E)E^*)$$
$$= \widehat{\delta}_a(\widehat{\varepsilon}(E^*)) + \sum_{b\in\Sigma} \widehat{\delta}_a(\widehat{\varepsilon}(E^*))\Delta(b)\widehat{\delta}_b(E)E^*$$
$$+ \sum_{b\in\Sigma} \widehat{\varepsilon}(E^*)\widehat{\delta}_a(\Delta(b))\widehat{\delta}_b(E)E^* + \sum_{b\in\Sigma} \widehat{\varepsilon}(E^*)\widehat{\varepsilon}(\Delta(b))\widehat{\delta}_a(\widehat{\delta}_b(E)E^*) \tag{8}$$
$$= \widehat{\varepsilon}(E^*) \sum_{b\in\Sigma} \Delta(\delta_a(b))\widehat{\delta}_b(E)E^* \tag{9}$$
$$= \widehat{\varepsilon}(E^*)\widehat{\delta}_a(E)E^*. \tag{10}$$

Step (8) follows from two applications of (7). Step (9) follows from the facts $\widehat{\delta}_a(\widehat{\varepsilon}(E^*)) = 0$, $\widehat{\varepsilon}(\Delta(b)) = 0$, and $\widehat{\delta}_a(\Delta(b)) = \Delta(\delta_a(b))$. Step (10) follows from the fact that $\Delta(\delta_a(b))$ is the identity matrix if $a = b$ and the zero matrix if $a \neq b$. □

2.7. Systems of linear equations

A *system of (left-)linear equations* over a weak KA K is a coalgebra (S, D, E) of signature $-^{\Sigma} \times K$, where $\Sigma \subseteq K$, $D : S \to S^{\Sigma}$, and $E : S \to K$. A finite system corresponds to a finite coalgebra, that is the set of states S is finite. We curry D so as to write $D_a : S \to S$ for $a \in \Sigma$. The map $D : \Sigma \to S \to S$ extends uniquely to a monoid homomorphism $D : \Sigma^* \to S \to S$, thus we have $D_x : S \to S$ for $x \in \Sigma^*$. A *solution* in K is a map $\varphi : S \to K$ such that

$$\varphi(s) = \sum_{a \in \Sigma} a\varphi(D_a(s)) + E(s). \tag{11}$$

Every finite system of linear equations has a solution. To see this, form an associated matrix $A \in \mathrm{Mat}(S, K)$, where

$$A = \sum_{a \in \Sigma} \Delta(a) P(a) \in \mathrm{Mat}(S, K),$$

where $\Delta(a)$ is the diagonal matrix with diagonal entries a and $P(a)$ is the characteristic matrix of the function D_a. Regarding φ and E as column vectors indexed by S, the solution condition (11) takes the form $\varphi = A\varphi + E$. Since $\mathrm{Mat}(S, K)$ is a weak KA, the vector A^*E is a solution by the weak KA axiom $a^* = 1 + aa^*$. We call this solution the *canonical solution*. If in addition K is an LKA, then the canonical solution is also the least solution.

If K is freely generated by Σ, then the map $a \mapsto \Delta(a)P(a)$ extends uniquely to a KA homomorphism $\chi : K \to \mathrm{Mat}(S, K)$, called the *standard embedding*. It will follow from our results that χ is injective.

Lemma 2.6. *Suppose (K, δ, ε) is a* DKA *with observations C and actions Σ and (S, D, E) a system of equations with $E : S \to C$. Then $\varphi : S \to K$ is a solution iff it is a coalgebra homomorphism $\varphi : (S, D, E) \to (K, \delta, \varepsilon)$.*

Proof. Suppose (K, δ, ε) is a DKA. If $\varphi : S \to K$ is a solution, then applying δ_a and ε to both sides of (11),

$$\delta_a(\varphi(s)) = \sum_{b \in \Sigma} \delta_a(b)\varphi(D_b(s)) + \sum_{b \in \Sigma} \varepsilon(b)\delta_a(\varphi(D_b(s))) + \delta_a(E(s)) = \varphi(D_a(s))$$

$$\varepsilon(\varphi(s)) = \sum_{b \in \Sigma} \varepsilon(b)\varepsilon(\varphi(D_b(s))) + \varepsilon(E(s)) = E(s),$$

so φ is a coalgebra homomorphism. Conversely, if φ is a coalgebra homomorphism, then by Theorem 2.3,

$$\varphi(s) = \sum_{a \in \Sigma} a\delta_a(\varphi(s)) + \varepsilon(\varphi(s)) = \sum_{a \in \Sigma} a\varphi(D_a(s)) + E(s),$$

so (11) holds. □

2.8. Bisimilarity and completeness

Let (S, D, E) be a coalgebra of signature $-^{\Sigma} \times 2$. We say that states $s, t \in S$ are *bisimilar*, and write $s \approx t$, if $E(D_x(s)) = E(D_x(t))$ for all $x \in \Sigma^*$. The relation $\approx$ is the maximal bisimulation on S and is the kernel of the unique coalgebra morphism $L_S : S \to \mathrm{Brz}$, where

$$L_S(s) = \{x \in \Sigma^* \mid E(D_x(s)) = 1\}.$$

Soundness and completeness can be expressed in these terms. Let E be a set of equations or equational implications on regular expressions, and let $\mathrm{Con}\, E$ be the set of consequences of E in ordinary equational logic. The axioms E are *sound* if $\mathrm{Con}\, E$ refines bisimilarity; equivalently, if the Brzozowski derivative is well-defined on the free weak KA modulo E. A sound set of axioms are *complete* if $\mathrm{Con}\, E$ and bisimilarity coincide; that is, if the unique coalgebra morphism to the final coalgebra Brz is injective. We have mentioned above that the LKA axioms are sound; indeed, soundness has been shown in [12] for a larger set of axioms, namely those of KA. To prove that they are complete, our task is to show that the unique coalgebra morphism $L_{K_\Sigma} : K_\Sigma \to \mathrm{Brz}$ is injective.

This characterization of soundness and completeness was first observed by Jacobs [7] for classical regular expressions and KA and largely explored in the thesis of Silva [19] for generalized regular expressions. See [19] for a comprehensive introduction to this characterization.

3. Decompositions

3.1. Simple strings

Let (S, D, E) be a finite coalgebra of type $-^{\Sigma} \times 2$. Let K_Σ be the free LKA on generators Σ. Extend D to a monoid homomorphism $D : \Sigma^* \to S \to S$. The corresponding characteristic matrices P also extend homomorphically by matrix multiplication, giving a map $P : \Sigma^* \to \mathrm{Mat}(S, 2)$. Let $\chi : K_\Sigma \to \mathrm{Mat}(S, K_\Sigma)$ with $\chi(a) = \Delta(a)P(a)$ be the standard embedding as defined in § 2.7.

Call $x \in \Sigma^*$ *simple* if $P(y) \neq P(z)$ for all distinct suffixes y, z of x. If x is simple, then so are all its suffixes. Define

$$M = \{x \mid x \text{ is simple}\}$$

$$M_x = \{y \mid |y| > 0 \text{ and } P(yx) = P(x), \text{ but all proper suffixes of } yx \text{ are simple}\}.$$

Let $n = |S|$. If $y \in M_x$, then $1 + |x| \leq |yx| \leq n^n$, as each function $S \to S$ is represented at most once as $P(z)$ for a proper suffix z of yx.

We now define a family of elements R_x, $T_{y,x}$, and V_x of K_Σ for $x, y \in \Sigma^*$.

$$R_x = \left(\sum_{y \in M_x} T_{y,x}\right)^* \qquad T_{1,x} = 1 \qquad T_{ay,x} = R_{ayx} a T_{y,x},\ a \in \Sigma \tag{12}$$

$$V_x = T_{x,1} R_1 \qquad V = \sum_{x \in M} V_x. \tag{13}$$

Intuitively, if x is a simple word labeling a path from s to t, then all words represented by V_x lead from s to t, and V represents all words in Σ^*. The expressions R_x and $T_{y,x}$ allow the encoding of loops.

The definitions of R_x and $T_{y,x}$ in (12) are by mutual induction, but it is not immediately clear that the definition is well-founded: note that R_x depends on $T_{y,x}$ for $y \in M_x$, which depends on R_{yx}. To prove well-foundedness, we define a binary relation $\succ$ on tuples (R, x) and (T, y, x) defined as follows. For $x, y \in \Sigma^*$ and $a \in \Sigma$, let

$$(R, x) \succ (T, y, x),\ y \in M_x \qquad (T, ay, x) \succ (R, ayx) \qquad (T, ay, x) \succ (T, y, x).$$

The relation $\succ$ describes the dependencies in the definition (12).

Lemma 3.1. *The relation $\succ$ is well-founded; that is, there are no infinite $\succ$-paths.*

Proof. Assign numbers to the tuples as follows:

$$(R, x) \mapsto \begin{cases} \binom{n^n - |x| + 2}{2} - 1 & \text{if } |x| \leq n^n, \\ 0 & \text{otherwise,} \end{cases} \qquad (T, y, x) \mapsto \begin{cases} \binom{n^n - |x| + 1}{2} - 1 + |y| & \text{if } |x| \leq n^n - 1, \\ |y| & \text{otherwise.} \end{cases}$$

As observed above, if $y \in M_x$, then $1 \leq |y| \leq n^n - |x|$. Using this fact, one can show by elementary arithmetic that the numbers assigned to the tuples are nonnegative and decrease strictly with $\succ$. □

Note that $R_x = 1$ for $|x| \geq n^n$, since the sum in the definition of R_x in (12) is vacuous in that case. It follows inductively that $T_{y,x} = y$ for $|x| \geq n^n$.

Lemma 3.2. *For all $x, y \in \Sigma^*$ and $a \in \Sigma$,*

(i) $V_1 = R_1$ *and* $V_{ax} = R_{ax} a V_x$.
(ii) $V_{yx} = T_{y,x} V_x$.

Proof. For (i),

$$V_1 = T_{1,1} R_1 = R_1 \qquad V_{ax} = T_{ax,1} R_1 = R_{ax} a T_{x,1} R_1 = R_{ax} a V_x.$$

For (ii), we proceed by induction on $|y|$. The basis $V_x = T_{1,x} V_x$ is immediate. For the induction step, using (i),

$$V_{ayx} = R_{ayx} a V_{yx} = R_{ayx} a T_{y,x} V_x = T_{ay,x} V_x. \quad \square$$

In the following two lemmas, we will exploit the fact that $R_z V_z = V_z$, which can be proven by case analysis on z using the fact that $R_z R_z = R_z$.

Lemma 3.3. $\left(\sum_{a\in\Sigma} a\right)^* = V$.

Proof. For the forward inequality, we use the left-handed star rule (3). Let $x \in M$ and $a \in \Sigma$. By Lemma 3.2(i),

$$aV_x \le R_{ax} a V_x = V_{ax}.$$

If $ax \in M$, then $V_{ax} \le V$. If $ax \notin M$, say $x = yz$ with $P(ax) = P(ayz) = P(z)$, then $ay \in M_z$ and $z \in M$. By Lemma 3.2,

$$V_{ax} = V_{ayz} = T_{ay,z} V_z \le R_z V_z = V_z \le V.$$

The fact that $R_z V_z = V_z$ follows from Lemma 3.2(i), since V_z begins with R_z, and R_z is a star (definition (12)), so $R_z R_z = R_z$. Thus in either case, $aV_x \le V$. Since $a \in \Sigma$ and $x \in M$ were arbitrary, $(\sum_{a\in\Sigma} a)V \le V$. Also $1 \le V$, since $1 \le V_1 = R_1$. By (3), $(\sum_{a\in\Sigma} a)^* \le V$.

The reverse inequality follows from monotonicity. □

3.2. Pumping

Every string can be reduced to a simple string by repeatedly removing certain substrings while preserving the value of the map P. This is the well-known *pumping lemma* from automata theory. If y is not simple, find a suffix vw such that $P(vw) = P(w)$ and $v \neq \varepsilon$, and remove v. The resulting string is shorter and P is preserved. Repeating this step eventually produces a string $x \in M$ such that $P(y) = P(x)$. If we always choose the shortest eligible suffix vw, so that $v \in M_w$—this strategy is called *right-to-left greedy*—we obtain a particular element $\gamma(y) \in M$ related to the construction of V_y.

Lemma 3.4. *For all $y \in \Sigma^*$, $V_y \le V_{\gamma(y)}$.*

Proof. If $v \in M_w$, then, by Lemma 3.2(ii), we have that $V_{vw} = T_{v,w} V_w \le V_w$, since $T_{v,w} \le R_w$ and $R_w V_w \le V_w$. The result follows inductively from the right-to-left construction of $\gamma(y)$. □

3.3. Decompositions

Let (S, D, E) be a finite coalgebra of type $-^{\Sigma} \times \mathbb{2}$ with standard embedding

$$\chi : K_\Sigma \to \mathrm{Mat}(S, K_\Sigma) \qquad \chi(a) = \Delta(a) P(a).$$

Let $e \in K_\Sigma$. A *decomposition* of e (with respect to χ) is a family of expressions $e_x \in K_\Sigma$ indexed by $x \in M$ (recall that M is the set of simple strings) such that

(a) $e = \sum_x e_x$, and
(b) $\chi(e_x) = \Delta(e_x) P(x)$ for all $x \in M$.

It follows that

$$\chi(e) = \sum_x \Delta(e_x) P(x). \tag{14}$$

If P, Q are function matrices, we say that the decomposition *respects* P, Q if in addition

(c) $P(x)Q = P$ for all x such that $e_x \neq 0$.

We say that e is *decomposable* if it has a decomposition. We will eventually show that all expressions are decomposable.

Lemma 3.5. *Let $x \mapsto e_x$ be a decomposition of e. The decomposition respects P, Q iff $\chi(e)Q = \Delta(e)P$.*

Proof. If the decomposition respects P, Q, then

$$\chi(e)Q = \sum_x \Delta(e_x) P(x) Q = \sum_x \Delta(e_x) P = \Delta(\sum_x e_x) P = \Delta(e) P.$$

Conversely, if $e_x \neq 0$ and $P(x)Q \neq P$, then $\Delta(e_x)P(x)Q \neq \Delta(e_x)P$, therefore

$$\chi(e)Q = \sum_x \Delta(e_x) P(x) Q \neq \Delta(e) P. \quad \square$$

We have specified the index set M in the definition of decomposition to emphasize that the $P(x)$ must be generated by the $P(a)$, but in fact any finite index set will do, provided the function matrices are so generated.

Lemma 3.6. *Let e_α and P_α be finite indexed collections of elements of K_Σ and function matrices, respectively, such that*

$$e = \sum_\alpha e_\alpha \qquad \chi(e_\alpha) = \Delta(e_\alpha) P_\alpha$$

and such that each P_α is $P(y_\alpha)$ for some $y_\alpha \in \Sigma^*$. Then $e_x = \sum_{x=\gamma(y_\alpha)} e_\alpha$ is a decomposition of e.

Proof. By Lemma 3.4, if $x = \gamma(y_\alpha)$, then $P(x) = P(y_\alpha)$. Easy calculations then show

$$e = \sum_x e_x \qquad \chi(e_x) = \Delta(e_x) P(x). \quad \square$$

Decompositions can be combined additively or multiplicatively. The *sum* and *product* of two decompositions $F : M \to K_\Sigma$ and $G : M \to K_\Sigma$ are, respectively, the decompositions

$$(F + G)(x) = F(x) + G(x) \qquad (F \times G)(x) = \sum_{x=\gamma(yz)} F(y) G(z),$$

respectively.

Lemma 3.7.

(i) *If F is a decomposition of e and G is a decomposition of d, then $F + G$ is a decomposition of $e + d$. If F and G both respect P, Q, then so does $F + G$.*
(ii) *If F is a decomposition of e and G is a decomposition of d, then $F \times G$ is a decomposition of ed. If F respects P, Q and G respects Q, R, then $F \times G$ respects P, R.*

Proof. Both (i) and (ii) are quite easy. We argue (ii) explicitly. Given $F : x \mapsto e_x$ and $G : x \mapsto d_x$, we have

$$ed = (\sum_y e_y)(\sum_z d_z) = \sum_{(y,z)} e_y d_z = \sum_x \sum_{x=\gamma(yz)} e_y d_z = \sum_x (F \times G)(x),$$

$$\chi(e_y d_z) = \Delta(e_y) P(y) \Delta(d_z) P(z) = \Delta(e_y d_z) P(yz) = \Delta(e_y d_z) P(\gamma(yz)),$$

therefore

$$\chi(\sum_{x=\gamma(yz)} e_y d_z) = \sum_{x=\gamma(yz)} \Delta(e_y d_z) P(\gamma(yz)) = \Delta(\sum_{x=\gamma(yz)} e_y d_z) P(x),$$

and $P(\gamma(yz))R = P(yz)R = P(y)Q = P$. $\square$

To handle star, we describe a monad structure on systems built on top of the string monad. The motivation is that we wish to consider the elements of M as single letters of an alphabet. To avoid confusion, we use $\alpha, \beta, \ldots$ to denote words in M^*. In §2.7, we constructed the standard embedding χ with respect to a coalgebra (S, D, E) of type $-^\Sigma \times C$. Now we wish to do the same for the alphabet M. We thus have a coalgebra $(S, \widehat{D})$ with $\widehat{D}_x : S \to S$ of type $-^M$ with $\widehat{D}_x = D_x$. The only difference is that on the left-hand side, x is considered as a single letter, whereas on the right-hand side, D_x is defined inductively from D_a for $a \in \Sigma$. The standard embedding is η, defined in the same way for (S, M) as χ was defined for (S, D):

$$\eta : K_M \to \mathrm{Mat}(S, K_M) \qquad \eta(x) = \Delta(x) P(x), \ x \in M.$$

Now let $\widehat{M}$ be constructed as in §3.1 for the alphabet M as M was constructed for Σ.

Lemma 3.8. *Suppose that $(\sum_{x \in M} x)^* \in K_M$ has a decomposition d_α, $\alpha \in \widehat{M}$ with respect to η and that $e \in K_\Sigma$ has a decomposition $\sigma : x \mapsto e_x$ with respect to χ. Let $\mu(x) = \sum_{x=\gamma(\alpha)} d_\alpha$. Then $\sigma\mu : x \mapsto \sigma(\sum_{x=\gamma(\alpha)} d_\alpha)$ is a decomposition of e^* with respect to χ. Moreover, if the decomposition of e respects Q, Q, then so does the decomposition of e^*.*

Proof. By Lemma 2.2, the map σ extends uniquely to a homomorphism

$$\sigma : K_M \to K_\Sigma \qquad \widehat{\sigma} : \mathrm{Mat}(S, K_M) \to \mathrm{Mat}(S, K_\Sigma).$$

We have

$$e = \sum_{x\in M} e_x \qquad \chi(e_x) = \Delta(e_x)P(x) \qquad (\sum_{x\in M} x)^* = \sum_\alpha d_\alpha \qquad \eta(d_\alpha) = \Delta(d_\alpha)P(\alpha).$$

Then for all $x \in M$,

$$\chi\sigma(x) = \chi(e_x) = \Delta(e_x)P(x) = \Delta(\sigma(x))P(x) = \widehat{\sigma}(\Delta(x)P(x)) = \widehat{\sigma}\eta(x).$$

As $\chi\sigma$ and $\widehat{\sigma}\eta$ are homomorphisms and agree on the generators $x \in M$ of K_M, they coincide.

Now $\sigma\mu : x \mapsto \sigma(\sum_{x=\gamma(\alpha)} d_\alpha)$ is a decomposition of e^* with respect to χ:

$$e^* = (\sum_x e_x)^* = \sigma((\sum_x x)^*) = \sigma(\sum_\alpha d_\alpha) = \sum_\alpha \sigma(d_\alpha) = \sum_x \sigma(\sum_{x=\gamma(\alpha)} d_\alpha) = \sum_x \sigma\mu(x)$$

$$\chi(\sigma\mu(x)) = \chi\sigma(\sum_{x=\gamma(\alpha)} d_\alpha) = \sum_{x=\gamma(\alpha)} \widehat{\sigma}\eta(d_\alpha) = \sum_{x=\gamma(\alpha)} \widehat{\sigma}(\Delta(d_\alpha)P(\alpha))$$

$$= \sum_{x=\gamma(\alpha)} \Delta(\sigma(d_\alpha))P(x) = \Delta(\sigma(\sum_{x=\gamma(\alpha)} d_\alpha))P(x) = \Delta(\sigma\mu(x))P(x).$$

Finally, if the decomposition of e respects Q, Q, then by Lemma 3.5, $\chi(e)Q = \Delta(e)Q$. By Lemma 2.1, $\chi(e)$ is block diagonal with blocks refining the kernel of Q, therefore so is $\chi(e^*)$. Again by Lemma 2.1,

$$\chi(e^*)Q = \sum_x \Delta(\sigma\mu(x))P(x)Q = DQ$$

for some diagonal matrix D. Thus $P(x)Q = Q$ for all x such that $\sigma\mu(x) \neq 0$, so the decomposition of e^* respects Q, Q. □

3.4. Existence of decompositions

Let (S, D, E) be a finite coalgebra of type $-^\Sigma \times C$ with standard embedding $\chi : K_\Sigma \to \mathrm{Mat}(S, K_\Sigma)$. Let $M \subseteq \Sigma^*$ and $M_x \subseteq \Sigma^*$ for $x \in M$ be defined as in §3.1. Let R_x, $T_{y,x}$, and $V_x \in K_\Sigma$ be as defined in §3.1 with respect to M and M_x.

In the following, the term *decomposition* refers to decompositions with respect to χ. A *universal decomposition* is a decomposition for the universal expression $(\sum_{a\in\Sigma} a)^*$.

We remark that Lemmas 3.9 and 3.10 are co-dependent and require proof by mutual induction on the well-founded relation $\succ$ and on dimension of the associated matrices. Lemma 3.9 can be proved for permutations without reference to Lemma 3.10 (this is the basis of the induction), but the general case requires Lemma 3.10 for lower dimension; and the proof of Lemma 3.10 depends on Lemma 3.9 for permutations.

Lemma 3.9. *For $x, y \in \Sigma^*$,*

(i) *$T_{y,x}$ has a decomposition respecting $P(yx), P(x)$;*
(ii) *R_x has a decomposition respecting $P(x), P(x)$;*
(iii) *$x \mapsto V_x$ is a universal decomposition.*

Proof. The proof is by induction on the well-founded relation $\succ$, using the fact that χ and Δ are homomorphisms, and on dimension. Let us assume that the lemma is true for all matrices of smaller dimension.

For (i), $T_{1,x} = 1$ has the trivial decomposition $1 \mapsto 1$ and $x \mapsto 0$ for all $x \in M - \{1\}$, and this clearly respects $P(x), P(x)$.

For ay, we have $T_{ay,x} = R_{ayx}aT_{y,x}$. By the induction hypothesis, we have a decomposition for R_{ayx} respecting $P(ayx), P(ayx)$ and a decomposition for $T_{y,x}$ respecting $P(yx), P(x)$. We also have the trivial decomposition $a \mapsto a$ and $x \mapsto 0$ for all $x \in M - \{a\}$, which respects $P(ayx), P(yx)$. By Lemma 3.7(ii), the product of these three decompositions in the appropriate order is a decomposition for $T_{ay,x}$ respecting $P(ayx), P(x)$.

For (ii), we have $R_x = e^*$, where $e = \sum_{y\in M_x} T_{y,x}$. By the induction hypothesis, we can assume decompositions of $T_{y,x}$ for each $y \in M_x$ respecting $P(yx), P(x)$. Since $P(yx) = P(x)$ for $y \in M_x$, these decompositions also respect $P(x), P(x)$. By Lemma 3.7(i), the sum of these decompositions gives a decomposition of e respecting $P(x), P(x)$. By Lemma 3.5, $\chi(e)P(x) = \Delta(e)P(x)$.

If $P(x)$ is invertible, then $\chi(e) = \Delta(e)$, therefore

$$\chi(R_x) = \chi(e)^* = \Delta(e)^* = \Delta(R_x).$$

In this case, we can decompose R_x trivially as $1 \mapsto R_x$ and $y \mapsto 0$ for $y \in M \setminus \{1\}$, which respects $P(x), P(x)$, and we are done.

If $P(x)$ is not invertible, we can use Lemma 3.10 to reduce the problem to a lower dimension. By that lemma, we have a universal decomposition that we can use with Lemma 3.8 to obtain a decomposition of e^* respecting $P(x), P(x)$.

For (iii),

$$\begin{aligned}\chi(V_x) &= \chi(T_{x,1})\chi(R_1) = \chi(T_{x,1})P(1)\chi(R_1) = \Delta(T_{x,1})P(x)\Delta(R_1)\\ &= \Delta(T_{x,1}R_1)P(x) = \Delta(V_x)P(x).\end{aligned}$$

Combined with Lemma 3.3, this makes $x \mapsto V_x$ a universal decomposition. □

Lemma 3.10. *There exists a universal decomposition.*

Proof. The proof is by induction on dimension and on the number of letters of Σ. We can assume by Lemma 3.9 that we already have a universal decomposition for the subalphabet of Σ consisting of all a such that $P(a)$ is invertible. Now we show how to add in the rest of the elements of Σ one by one.

Suppose we have constructed a universal decomposition $x \mapsto e_x$ for a subalphabet $\Gamma \subseteq \Sigma$ including all a such that $P(a)$ is invertible. Let $e = \sum_{a\in\Gamma} a$ and $a \in \Sigma \setminus \Gamma$. We have

$$e^* = \sum_x e_x \qquad \chi(e_x) = \Delta(e_x)P(x),$$

and we wish now to construct a decomposition for $(a + e)^*$.

Since $P(a)$ is not a permutation, the range of the corresponding function is a proper subset $C \subset S$. Equivalently stated, the $S \times (S \setminus C)$ submatrix of $P(a)$ is the zero matrix.

We can reduce to a lower dimensional $C \times C$ problem. Let X be the $S \times C$ matrix whose $C \times C$ submatrix is the identity matrix and whose other entries are 0, and let X^T be its transpose. Then $X^T X$ is the $C \times C$ identity matrix and XX^T is the $S \times S$ matrix whose $C \times C$ submatrix is I and whose other entries are 0.

Let G be the subalgebra of $\mathrm{Mat}(S, K_\Sigma)$ consisting of matrices that are *block lower triangular* in the sense that their $C \times (S \setminus C)$ submatrices are 0. All $P(xa)$ are block lower triangular in this sense. Consider the map $A \mapsto X^T AX$, which takes an $S \times S$ matrix to its $C \times C$ submatrix. It is easily shown that if A, B are block lower triangular, then so are $A + B$, AB, and A^*; moreover,

$$X^T(A + B)X = X^T AX + X^T BX \qquad X^T ABX = X^T AXX^T BX \qquad X^T A^* X = (X^T AX)^*,$$

therefore restricted to G, the map $A \mapsto X^T AX : G \to \mathrm{Mat}(C, K_\Sigma)$ is a KA homomorphism. In addition, the following facts are easily verified:

$$P(xa) = P(xa)XX^T \qquad X^T A = X^T AXX^T,\ A \in G. \tag{15}$$

To construct a decomposition of $(a + e)^*$, observe that

$$(a + e)^* = (e^* a)^* e^* = (1 + e^* a(e^* a)^*)e^*.$$

By Lemma 3.7, we know how to combine decompositions additively and multiplicatively, and we have decompositions of a, e^*, and 1. It thus suffices to construct a decomposition of $a(e^*a)^*$. To this end, let

$$Q(x) = X^T P(xa)X \in \mathrm{Mat}(C, \mathbb{2})$$

and consider the system

$$\eta : K_M \to \mathrm{Mat}(C, K_M) \qquad \eta(x) = \Delta(x)Q(x)$$

of dimension $C \times C$. By the induction hypothesis on dimension, we have a universal decomposition with respect to η:

$$(\sum_{x\in M} x)^* = \sum_{\alpha\in\widehat{M}} d_\alpha \qquad \eta(d_\alpha) = \Delta(d_\alpha)Q(\alpha).$$

Let

$$R(\alpha) = P(a)XQ(\alpha)X^T,\ \alpha \in \widehat{M} \qquad \sigma(x) = e_x a,\ x \in M.$$

The map σ extends uniquely to a KA homomorphism $\sigma : K_M \to K_\Sigma$. We claim that $a\sigma(d_\alpha)$ and $R(\alpha)$, $\alpha \in \widehat{M}$, form a decomposition of $a(e^*a)^*$ with respect to χ. We must show that

$$a(e^*a)^* = \sum_\alpha a\sigma(d_\alpha) \qquad \chi(a\sigma(d_\alpha)) = \Delta(a\sigma(d_\alpha))R(\alpha). \tag{16}$$

According to Lemma 3.6, we must also show that the $R(\alpha)$ are generated by the $P(a)$, $a \in \Sigma$. The left-hand equation of (16) is a straightforward calculation:

$$a(e^*a)^* = a(\sum_x e_x a)^* = a\sigma((\sum_x x)^*) = a\sigma(\sum_\alpha d_\alpha) = \sum_\alpha a\sigma(d_\alpha).$$

That the $R(\alpha)$ are generated by the $P(a)$ can be shown inductively using (15):

$$R(1) = P(a)XQ(1)X^T = P(a)XX^TP(a)XX^T = P(a^2)$$
$$R(x\alpha) = P(a)XQ(x\alpha)X^T = P(a)XQ(x)Q(\alpha)X^T = P(a)XX^TP(xa)XQ(\alpha)X^T = P(ax)R(\alpha).$$

It remains to prove the right-hand equation of (16). Since

$$\chi\sigma(x) = \chi(e_x a) = \Delta(e_x)P(x)\Delta(a)P(a) = \Delta(e_x a)P(xa),$$

the map $\chi\sigma : K_M \to \mathrm{Mat}(S, K_\Sigma)$ takes values in G. As mentioned above, the map $A \mapsto X^TAX$ is a homomorphism on G, therefore the composition $X^T(\chi\sigma(-))X : K_M \to \mathrm{Mat}(C, K_\Sigma)$ is a homomorphism.

Now $X^T(\chi\sigma(-))X = \widehat{\sigma}\eta$, as they are both homomorphisms $K_M \to \mathrm{Mat}(C, K_\Sigma)$ and agree on the generators $x \in M$:

$$X^T(\chi\sigma(x))X = X^T(\chi(e_x a))X = X^T(\Delta(e_x a)P(xa))X = \Delta(e_x a)X^TP(xa)X = \Delta(e_x a)Q(x)$$
$$\widehat{\sigma}\eta(x) = \widehat{\sigma}(\Delta(x)Q(x)) = \Delta(\sigma(x))Q(x) = \Delta(e_x a)Q(x).$$

Thus the value they take on $d_\alpha \in K_M$ is the same:

$$X^T\chi(\sigma(d_\alpha))X = \widehat{\sigma}\eta(d_\alpha) = \widehat{\sigma}(\Delta(d_\alpha)Q(\alpha)) = \Delta(\sigma(d_\alpha))Q(\alpha). \tag{17}$$

Calculating, we find

$$\begin{aligned}
\chi(a\sigma(d_\alpha)) &= \Delta(a)P(a)\chi(\sigma(d_\alpha)) \\
&= \Delta(a)P(a)XX^T\chi(\sigma(d_\alpha))XX^T && \text{by (15) and (16)} \\
&= \Delta(a)P(a)X\Delta(\sigma(d_\alpha))Q(\alpha)X^T && \text{by (17)} \\
&= \Delta(a)\Delta(\sigma(d_\alpha))P(a)XQ(\alpha)X^T \\
&= \Delta(a\sigma(d_\alpha))R(\alpha) && \text{by definition of } R(\alpha). \quad \square
\end{aligned}$$

Theorem 3.11. *All expressions are decomposable.*

Proof. We proceed by induction on the structure of the expression. Every element $a \in \{0, 1\} \cup \Sigma$ has a trivial decomposition $1 \mapsto a$ and $x \mapsto 0$ for $x \in M \setminus \{1\}$. Closure under sum and product follow from Lemma 3.7. For star, suppose we have a decomposition e_x, $x \in M$, of e. By Lemma 3.10, we have a decomposition for the universal expression $(\sum_{x\in M} x)^*$. Lemma 3.8 then provides a decomposition for e^* via the substitution $x \mapsto e_x$. $\square$

4. Completeness

Recall from §2.8 that to prove that the LKA axioms are complete, we must show that the unique coalgebra morphism $L_{K_\Sigma} : K_\Sigma \to \mathsf{Brz}$ is injective, where Brz (defined in §2.4) is the final coalgebra for the functor $-^\Sigma \times 2$.

Recall also that any coalgebra (S, D, E) for that functor gives rise to an associated matrix

$$A = \sum_{a\in\Sigma} \Delta(a)P(a) \in \mathrm{Mat}(S, K_\Sigma),$$

where $\Delta(a)$ is the diagonal matrix with diagonal entries a and $P(a)$ is the characteristic matrix of the function D_a, and that the map $a \mapsto \Delta(a)P(a)$ extends to the standard embedding $\chi : K_\Sigma \to \mathrm{Mat}(S, K_\Sigma)$ as defined in §2.7. Let $\approx$ be the relation of bisimilarity as defined in §2.8.

Lemma 4.1. *Let $s, t \in S$. If $s \approx t$ then $(A^*E)_s = (A^*E)_t$.*

Proof. We have

$$A = \sum_{a\in\Sigma} \Delta(a)P(a) = \sum_{a\in\Sigma} \chi(a) = \chi(\sum_{a\in\Sigma} a),$$

thus by Lemma 3.9,

$$A^* = \chi(\sum_{a\in\Sigma} a)^* = \chi((\sum_{a\in\Sigma} a)^*) = \chi(\sum_{x\in M} V_x) = \sum_{x\in M} \chi(V_x) = \sum_{x\in M} \Delta(V_x)P(x).$$

Now for any $s \in S$,

$$\begin{aligned}(A^*E)_s &= (\sum_{x\in M} \Delta(V_x)P(x)E)_s = \sum_{x\in M} V_x(P(x)E)_s \\ &= \sum_{x\in M} V_x \sum_{u\in S} P(x)_{su}E_u = \sum_{x\in M} V_x E(D_x(s)).\end{aligned}$$

If $s \approx t$, then $E(D_x(s)) = E(D_x(t))$ for all $x \in \Sigma^*$, therefore

$$(A^*E)_s = \sum_{x\in M} V_x E(D_x(s)) = \sum_{x\in M} V_x E(D_x(t)) = (A^*E)_t. \quad \square$$

Consider a finite subcoalgebra (S, δ, ε) of K_Σ, where δ and ε comprise the Brzozowski derivative as defined in Fig. 2. Recall that every $e \in K_\Sigma$ generates a finite subcoalgebra, since it has finitely[1] many Brzozowski derivatives [16].

Lemma 4.2. $e = (\chi(e)E)_e$.

Proof. Theorem 3.11 guarantees a decomposition e_x, $x \in M$ of e. If $e_x \neq 0$, then there exists $y \in \Sigma^*$ such that $y \leq e_x$. Since χ is monotone,

$$\Delta(y)P(y) = \chi(y) \leq \chi(e_x) = \Delta(e_x)P(x),$$

therefore $P(y) = P(x)$. Moreover, $1 \leq \delta_y(e_x) \leq \delta_y(e)$, therefore $\varepsilon(\delta_y(e)) = 1$. Since $P(y) = P(x)$, $\varepsilon(\delta_x(e)) = 1$.

We have shown that if $e_x \neq 0$, then $\varepsilon(\delta_x(e)) = 1$; in other words, $e_x = e_x\varepsilon(\delta_x(e))$. Using (14),

$$(\chi(e)E)_e = (\sum_x \Delta(e_x)P(x)E)_e = \sum_x e_x(P(x)E)_e = \sum_x e_x\varepsilon(\delta_x(e)) = \sum_x e_x = e. \quad \square$$

Lemma 4.3. $e = (A^*E)_e$.

Proof. By Lemma 4.2, Lemma 3.3, and the monotonicity of χ,

$$e = (\chi(e)E)_e \leq (\chi((\sum_{a\in\Sigma} a)^*)E)_e = (\chi(\sum_{a\in\Sigma} a)^*E)_e = (A^*E)_e.$$

For the reverse inequality, Theorem 2.3 says that the identity map $e \mapsto e$ is a solution to (11), and as noted in §2.7, A^*E is the least solution in a LKA. $\square$

Theorem 4.4 *(Completeness). If $d \approx e$ then $d = e$.*

Proof. Immediate from Lemmas 4.1 and 4.3. $\square$

An interesting consequence is that the canonical solution in K_Σ is not only the least, but in fact the *unique* solution.

Theorem 4.5 *(Uniqueness of the canonical solution). For all finite coalgebras (S, D, E) specifying a system of linear equations as described in §2.7, there is a unique solution $\varphi : S \to K_\Sigma$.*

Proof. We have argued in §2.7 that $\varphi(s) = (A^*E)_s$ is a solution. For uniqueness, let $h : (S, D, E) \to (K_\Sigma, \delta, \varepsilon)$ be any solution. By Lemma 2.6, both φ and h are coalgebra homomorphisms. For all $s \in S$, $h(s) \approx s$ and $\varphi(s) \approx s$, therefore $h(s) \approx \varphi(s)$. By Theorem 4.4, $h(s) = \varphi(s)$. $\square$

[1] The finiteness of the subcoalgebra generated by $e \in K_\Sigma$ only requires the axioms for associativity, commutativity, and idempotence of $+$ (hence, only equations).

5. Discussion

In this paper, we have given a new, significantly shorter proof of the completeness of the left-handed star rule of Kleene algebra. In this section, we discuss connections with existing work and give pointers for future work.

We have shown that the left-handed star rule is needed only to guarantee the existence of least solutions. It would be interesting to explore how one could prove the existence of least solutions just using the equations assumed by Krob [15], which are of the form

$$M^* = \sum_{m \in M} \varepsilon_M^{-1}(m)$$

for M a finite monoid.

A well-known algorithm to obtain the minimal deterministic automaton is the *Brzozowski algorithm* [2]. Starting from a possibly nondeterministic automaton, (i) reverse the transitions, exchanging final and initial states, then (ii) perform the subset construction, removing inaccessible states; then repeat (i) and (ii). The resulting automaton is a minimal automaton for the original language.

Starting from a finite automaton (S, D, E) with a start state s, we can build an automaton $(2^S, \widehat{D}, \widehat{E})$ with start state E, and

$$\widehat{D}(f) = D \circ f \qquad \widehat{E} = \xi(s),$$

where $\xi(s)$ denotes the characteristic function of the singleton set containing s. This new automaton recognizes the reverse of the original language. Interestingly, this is also reflected in the construction of the expressions V_f for the new automaton. There is apparently a relationship to the Brzozowski construction, but the exact relationship remains to be explored.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Maurice Boffa, Une condition impliquant toutes les identités rationnelles, Inform. Théor. Appl. (Theor. Inform. Appl.) 29 (6) (1995) 515–518.
[2] Janusz A. Brzozowski, Canonical regular expressions and minimal state graphs for definite events, in: Mathematical Theory of Automata, in: MRI Symposia Series, vol. 12, Polytechnic Press, Polytechnic Institute of Brooklyn, N.Y., 1962, pp. 529–561.
[3] John Horton Conway, Regular Algebra and Finite Machines, Chapman and Hall, London, 1971, Dover edition, 2012.
[4] Anupam Das, Amina Doumane, Damien Pous, Left-handed completeness for Kleene algebra, via cyclic proofs, in: Gilles Barthe, Geoff Sutcliffe, Margus Veanes (Eds.), LPAR-22. 22nd International Conference on Logic for Programming, Artificial Intelligence and Reasoning, in: EPiC Series in Computing, vol. 57, EasyChair, 2018, pp. 271–289.
[5] Zoltán Ésik, Group axioms for iteration, Inf. Comput. 148 (2) (1999) 131–180.
[6] Simon Foster, Georg Struth, On the fine-structure of regular algebra, J. Autom. Reason. 54 (2) (2015) 165–197.
[7] Bart Jacobs, A bialgebraic review of deterministic automata, regular expressions and languages, in: K. Futatsugi, et al. (Eds.), Essays Dedicated to Joseph A. Goguen, in: Lecture Notes in Computer Science, vol. 4060, Springer, 2006, pp. 375–404.
[8] Stephen C. Kleene, Representation of events in nerve nets and finite automata, in: C.E. Shannon, J. McCarthy (Eds.), Automata Studies, Princeton University Press, Princeton, N.J., 1956, pp. 3–41.
[9] Łucja Kot, Dexter Kozen, Second-Order Abstract Interpretation Via Kleene Algebra, Technical Report TR2004-1971, Computer Science Department, Cornell University, December 2004.
[10] Łucja Kot, Dexter Kozen, Kleene algebra and bytecode verification, in: Fausto Spoto (Ed.), Proc. 1st Workshop Bytecode Semantics, Verification, Analysis, and Transformation, Bytecode'05, April 2005, pp. 201–215.
[11] Dexter Kozen, A completeness theorem for Kleene algebras and the algebra of regular events, in: Proc. 6th Symp. Logic in Comput. Sci., IEEE, Amsterdam, July 1991, pp. 214–225.
[12] Dexter Kozen, A completeness theorem for Kleene algebras and the algebra of regular events, Inf. Comput. 110 (2) (May 1994) 366–390.
[13] Dexter Kozen, Alexandra Silva, Left-handed completeness, in: Wolfram Kahl, Timothy G. Griffin (Eds.), Relational and Algebraic Methods in Computer Science - 13th International Conference, RAMiCS 2012, Cambridge, UK, September 17-20, 2012. Proceedings, in: Lecture Notes in Computer Science, vol. 7560, Springer, 2012, pp. 162–178.
[14] Dexter Kozen, Jerzy Tiuryn, Substructural logic and partial correctness, Trans. Comput. Log. 4 (3) (July 2003) 355–378.
[15] Daniel Krob, A complete system of B-rational identities, Theor. Comput. Sci. 89 (2) (October 1991) 207–343.
[16] Jan J.M.M. Rutten, Automata and coinduction (an exercise in coalgebra), in: Davide Sangiorgi, Robert de Simone (Eds.), CONCUR, in: Lecture Notes in Computer Science, vol. 1466, Springer, 1998, pp. 194–218.
[17] Jan J.M.M. Rutten, A coinductive calculus of streams, Math. Struct. Comput. Sci. 15 (1) (2005) 93–147.
[18] Arto Salomaa, Two complete axiom systems for the algebra of regular events, J. Assoc. Comput. Mach. 13 (1) (January 1966) 158–169.
[19] Alexandra Silva, Kleene Coalgebra, PhD thesis, University of Nijmegen, 2010.