Left-Handed Completeness

Dexter Kozen
Computer Science Department
Cornell University

RAMiCS, September 19, 2012

Joint work with
Alexandra Silva
Radboud University Nijmegen
and CWI Amsterdam

Result

A new proof of the completeness of left-handed KA

Axioms of KA

Idempotent Semiring Axioms

$$p + (q + r) = (p + q) + r \qquad p(qr) = (pq)r$$
$$p + q = q + p \qquad 1p = p1 = p$$
$$p + 0 = p \qquad p0 = 0p = 0$$
$$p + p = p$$
$$p(q + r) = pq + pr \qquad a \leq b \overset{\text{def}}{\iff} a + b = b$$
$$(p + q)r = pr + qr$$

Axioms for *

$$1 + pp^* \leq p^* \qquad q + px \leq x \;\Rightarrow\; p^*q \leq x$$
$$1 + p^*p \leq p^* \qquad q + xp \leq x \;\Rightarrow\; qp^* \leq x$$

Axioms of KA

Idempotent Semiring Axioms

$$p + (q + r) = (p + q) + r \qquad p(qr) = (pq)r$$
$$p + q = q + p \qquad 1p = p1 = p$$
$$p + 0 = p \qquad p0 = 0p = 0$$
$$p + p = p$$
$$p(q + r) = pq + pr \qquad a \leq b \overset{\text{def}}{\iff} a + b = b$$
$$(p + q)r = pr + qr$$

Axioms for *

$$1 + pp^* \leq p^* \qquad q + px \leq x \;\Rightarrow\; p^*q \leq x$$
~~$1 + p^*p \leq p^*$~~ ~~$q + xp \leq x \;\Rightarrow\; qp^* \leq x$~~

Left-Handed Completeness

This is a known result!

- claimed without proof by Conway (1971)

The only extant proofs are by Krob/Boffa (95) and Ésik (99)

- Krob gives an equational axiomatization with infinitely many equations of a specified form
- an entire journal issue of TCS (137 pages!)
- later reworked in the context of iteration theories by Ésik, but essentially the same proof (50 pages)
- Boffa observed that all Krob's equations were provable with the left-handed rule

Krob's Equations

- Idempotent semiring axioms
- Conway axioms
  - $p^* = p^* p^* = p^{**}$
  - $(p+q)^* = p^*(qp^*)^*$
  - $(pq)^* = 1 + p(qp)^* q$
- $M^* = \sum_{m \in M} \varepsilon_M^{-1}(m)$ for all finite monoids M, where $\varepsilon_M : M^* \to M$ is the unique monoid homomorphism such that $\varepsilon_M(m) = m$

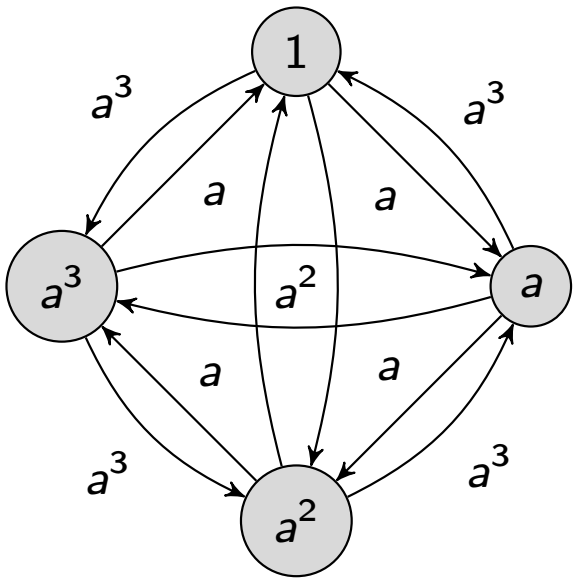
No finite set of equations suffices (Redko 64)

Monoid Equations

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

for all finite monoids M, where $\varepsilon_M : M^* \to M$ is the unique monoid homomorphism such that $\varepsilon_M(m) = m$

Take $M = a^*/(a^4 = 1) = \{1, a, a^2, a^3\}$



$$a^* = (1 + a + a^2 + a^3)(a^4)^*$$

Purely Equational Axiomatizations

Purely equational axiomatizations are undesirable from a practical point of view: they do not interact well with equations assumptions, which is almost always the case in real-life applications

For example, consider the redundant assignment $x := 1; x := 1$.

- let $a = x := 1$
- have $aa = a$, since the assignment is redundant
- would expect this to imply $a^* = 1 + a$, but this is not a consequence of the equational theory of KA plus $aa = a$
- the free R-algebra on the monoid $a^*/(aa = a) = \{0, 1, a, 1 + a, a^*, aa^*\}$. In particular, $a^* \neq 1 + a$.

This algebra that satisfies all the equations of KA but is not a KA itself – in a finite KA a star is always equal to a finite sum of powers

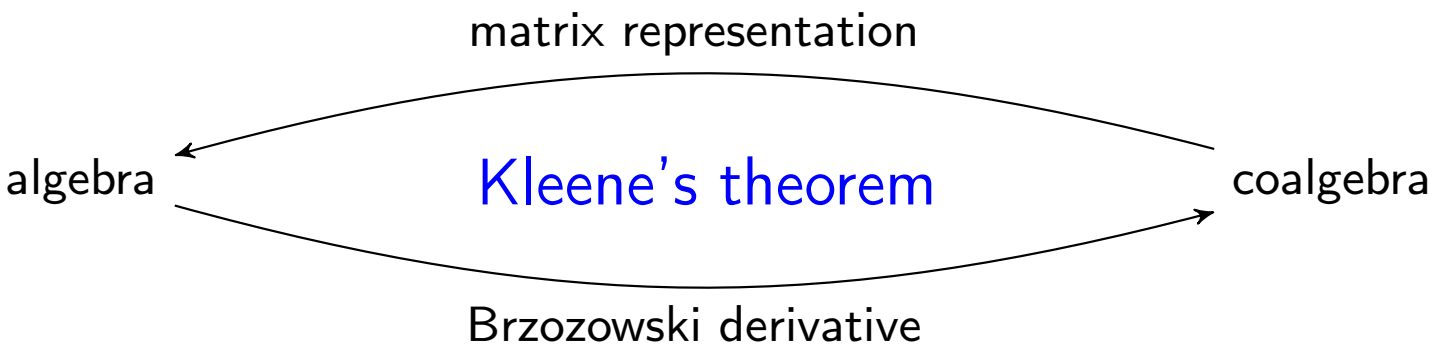
Practical Motivation

Characterizing a^* as a least fixpoint is natural and powerful 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, so it is useful to know that only one of the rules is needed for equational completeness

Technical Motivation

- We define differential Kleene algebra, which captures abstractly the interplay between algebra and coalgebra in the theory of regular sets
- the (syntactic) Brzozowski derivative on regular expressions maps algebra to coalgebra
- the canonical embedding of a coalgebra into a matrix algebra plays the converse role



Left-Handed Kleene Algebra

A weak KA is an idempotent semiring with star satisfying the Conway equations

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

Incomplete, but sufficient for many arguments involving *.

A left-handed Kleene algebra (LKA) is a weak KA satisfying the left-handed star rule

$$b + ax \leq x \Rightarrow a^*b \leq x \qquad \text{or} \qquad ax \leq x \Rightarrow a^*x \leq x$$

where $a \leq b \Leftrightarrow a + b = b$. One consequence is the left-handed bisimulation rule

$$ax \leq xb \Rightarrow a^*x \leq xb^*$$

Matrices

Let $\mathrm{Mat}(S, K)$ be the family of square matrices with rows and columns indexed by S with entries in K.

The characteristic matrix P_f of a function $f : S \to S$ has $(P_f)_{st} = 1$ if $f(s) = t$, 0 otherwise. M is a function matrix if it is P_f for some f.

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

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 $D_{ss} = \sum_{f(s)=f(t)} A_{st}$.*

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 $c \in C$

ii. C and Σ generate K

iii. K supports a Brzozowski derivative consisting of functions $\varepsilon\colon K \to C$ and $\delta_a\colon K \to K$, $a \in \Sigma$, satisfying

$$\delta_a(e_1 + e_2) = \delta_a(e_1) + \delta_a(e_2) \qquad \varepsilon(e_1 + e_2) = \varepsilon(e_1) + \varepsilon(e_2)$$

$$\delta_a(e_1 e_2) = \delta_a(e_1)e_2 + \varepsilon(e_1)\delta_a(e_2) \qquad \varepsilon(e_1 e_2) = \varepsilon(e_1)\varepsilon(e_2)$$

$$\delta_a(e^*) = \varepsilon(e^*)\delta_a(e)\,e^* \qquad \varepsilon(e^*) = \varepsilon(e)^*$$

$$\delta_a(b) = \begin{cases} 1 & \text{if } a = b, \\ 0 & \text{if } a \neq b, \end{cases} \quad b \in \Sigma \qquad \varepsilon(b) = 0,\ b \in \Sigma$$

$$\delta_a(c) = 0,\ c \in C \qquad \varepsilon(c) = c,\ c \in C$$

Differential Kleene Algebra

$$\delta_a(e_1 + e_2) = \delta_a(e_1) + \delta_a(e_2) \qquad \varepsilon(e_1 + e_2) = \varepsilon(e_1) + \varepsilon(e_2)$$

$$\delta_a(e_1 e_2) = \delta_a(e_1)e_2 + \varepsilon(e_1)\delta_a(e_2) \qquad \varepsilon(e_1 e_2) = \varepsilon(e_1)\varepsilon(e_2)$$

$$\delta_a(e^*) = \varepsilon(e^*)\delta_a(e)\,e^* \qquad \varepsilon(e^*) = \varepsilon(e)^*$$

$$\delta_a(b) = \begin{cases} 1 & \text{if } a = b, \\ 0 & \text{if } a \neq b, \end{cases} \quad b \in \Sigma \qquad \varepsilon(b) = 0,\ b \in \Sigma$$

$$\delta_a(c) = 0,\ c \in C \qquad \varepsilon(c) = c,\ c \in C$$

Thus $\varepsilon\colon K \to C$ is a retract (a KA homomorphism that is the identity on C, which immediately implies $0, 1 \in C$).

This definition is a generalization of the usual situation in which $C = \mathbb{2} = \{0, 1\}$ and the function ε and δ_a are the (syntactic) Brzozowski derivatives.

Extension to Matrices

Lemma

If K is a DKA *with actions Σ and observations C, then* $\mathrm{Mat}(S, K)$ *is a* DKA *with actions $\Delta(a)$ and observations* $\mathrm{Mat}(S, C)$ *under the pointwise operations.*

We are primarily interested in matrix KAs in which C is the set of square matrices over $\mathbb{2}$.

Examples

1. A DKA with observations $\mathfrak{2}$ is $\mathrm{Brz} = (2^{\Sigma^*}, \delta, \varepsilon)$, where $\varepsilon(A) = 1$ iff A contains the null string and 0 otherwise, and $\delta_a : 2^{\Sigma^*} \to 2^{\Sigma^*}$ is the usual Brzozowski derivative

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

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

2. 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. The maps δ_a and ε are well defined modulo the axioms of LKA.

The following comes from an observation of Jacobs (2006) for KA.

Lemma

The axioms of LKA *are complete iff the unique homomorphism* $L_{K_\Sigma} : K_\Sigma \to \mathrm{Brz}$ *is injective.*

The Fundamental Theorem (Silva 2010)

The following result characterizes the relationship between algebraic and coalgebraic structure of DKA's.

Theorem

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

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

Consequences of the Fundamental Theorem

Let K be a DKA. Define the C-free part of $e \in K$ to be

$$e' = \sum_{a \in \Sigma} a\delta_a(e).$$

By the fundamental theorem, $e = e' + \varepsilon(e)$ and $\varepsilon(e') = 0$.

Theorem

The map $e \mapsto e'$ is linear and satisfies the following derivation properties:

$$1' = 0 \qquad (de)' = d'e + de' \qquad e^{*\prime} = \varepsilon(e^*)(e' \cdot \varepsilon(e^*))^+$$

The decomposition $e = e' + \varepsilon(e)$ is unique such that $\varepsilon(e') = 0$.

Systems of Linear Equations as Coalgebras

A system of (left-)linear equations over a weak KA K is a coalgebra (S, D, E), where $\Sigma \subseteq K$, $D_a \colon S \to S$, and $E \colon S \to K$.

A solution in K is a map $\varphi : S \to K$ such that

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

Canonical Solution and Standard Embedding

Given a finite system of linear equations, form the matrix

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

where

- $\Delta(a)$ is the diagonal matrix with diagonal entries a
- $P(a)$ is the characteristic matrix of the function D_a.

The solution condition is $\varphi = A\varphi + E$. Since $\mathrm{Mat}(S, K)$ is a weak KA, the vector A^*E is a solution, called 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 an injective KA homomorphism $\chi : K \to \mathrm{Mat}(S, K)$, called the standard embedding.

Decompositions

Let (S, D, E) be a finite coalgebra with standard embedding

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

Let $e \in K_\Sigma$. Let M be a finite set with a map $\gamma : \Sigma^* \to M$ such that $P(x) = P(\gamma(x))$. A decomposition of e is a family of expressions $e_x \in K_\Sigma$ indexed by M 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

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

The decomposition respects P, Q if in addition

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

Decompositions

Lemma

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

Lemma

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

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

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.

Decompositions

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

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

Lemma

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.*

Star

Star is handled with a kind of monad structure $M \mapsto \widehat{M}$ (details omitted).

Lemma

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* e^*.

Universal Decomposition

A universal decomposition is a decomposition for the universal expression $(\sum_{a \in \Sigma} a)^*$.

Corollary

There exists a universal decomposition.

Corollary

Every expression has a decomposition.

Completeness

Let (S, D, E) be a coalgebra of signature $-^{\Sigma} \times 2$. Let $L_S \colon S \to \mathrm{Brz}$ be the unique homomorphism to the final coalgebra

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

Recall that for a coalgebra (S, D, E) we form an associated matrix

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

where $\Delta(a)$ is the diagonal matrix with diagonal entries a and $P(a)$ is the characteristic matrix of the function D_a.

Lemma

If $L_S(s) = L_S(t)$ *then* $(A^* E)_s = (A^* E)_t$.

Completeness

Recall that every $e \in K_\Sigma$ generates a finite subcoalgebra, since it has finitely many Brzozowski derivatives modulo the weak KA axioms (actually only associativity, commutativity, and idempotency of $+$ are needed for finiteness).

Let $\chi\colon K_\Sigma \to \mathrm{Mat}(S, K_\Sigma)$ be the standard embedding.

Lemma

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

Completeness

Lemma

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

Proof.

By the previous lemma and the monotonicity of χ,

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

For the reverse inequality, the fundamental theorem says that the identity map $e \mapsto e$ is a solution, and $A^* E$ is the least solution. $\square$

Theorem (Completeness)

If $L_{K_\Sigma}(d) = L_{K_\Sigma}(e)$ *then* $d = e$.

Conclusion

We have given a new, shorter proof of the completeness of the left-handed star rule of Kleene algebra.

We have shown that the left-handed star rule is needed only to guarantee the existence of least solutions.

Some pressing questions remain:

- Can we replace the left-handed rule with a neutral rule such as $e^2 \leq 1 + e \Rightarrow e^* = 1 + e$?
- Can we significantly simplify Krob's proof using these techniques?

Thanks!