# Myhill–Nerode Relations on Automatic Systems and the Completeness of Kleene Algebra

Dexter Kozen

Department of Computer Science
Cornell University
Ithaca, NY 14853-7501, USA
kozen@cs.cornell.edu

**Abstract.** It is well known that finite square matrices over a Kleene algebra again form a Kleene algebra. This is also true for infinite matrices under suitable restrictions. One can use this fact to solve certain infinite systems of inequalities over a Kleene algebra. *Automatic systems* are a special class of infinite systems that can be viewed as infinite-state automata. Automatic systems can be collapsed using Myhill–Nerode relations in much the same way that finite automata can. The Brzozowski derivative on an algebra of polynomials over a Kleene algebra gives rise to a triangular automatic system that can be solved using these methods. This provides an alternative method for proving the completeness of Kleene algebra.

## 1 Introduction

Kleene algebra (KA) is the algebra of regular expressions. It dates to a 1956 paper of Kleene [7] and was further developed in the 1971 monograph of Conway [4]. Kleene algebra has appeared in one form or another in relational algebra [16, 20], semantics and logics of programs [8, 17], automata and formal language theory [14, 15], and the design and analysis of algorithms [1, 6, 9]. Many authors have contributed over the years to the development of the algebraic theory; see [11] and references therein. There are many competing definitions and axiomatizations, and in fact there is no universal agreement on the definition of Kleene algebra.

In [10], a Kleene algebra was defined to be an idempotent semiring such that $a^*b$ is the least solution to $b + ax \leq x$ and $ba^*$ the least solution to $b + xa \leq x$. This is a finitary universal Horn axiomatization (universally quantified equations and equational implications). These axioms were shown in [10] to be sound and complete for the equational theory of the regular sets, improving a 1966 result of Salomaa [19]. Salomaa's axiomatization is sound and complete for the regular sets, but his axiom for * involves a nonalgebraic side condition that renders it unsound over other interpretations of importance, such as relational models. In contrast, the axiomatization of [10] is sound over a wide variety of models that arise in computer science, including relational models. No finitary axiomatization consisting solely of equations exists [18].

Matrices over a Kleene algebra, under the proper definition of the matrix operators, again form a Kleene algebra. This fundamental construction has many applications: the solution of systems of linear inequalities, construction of regular expressions equivalent to a given finite automaton, an algebraic treatment of finite automata in terms of their transition matrices, shortest path algorithms in directed graphs. In [10] it is used to encode algebraically various combinatorial constructions in the theory of finite automata, including determinization via the subset construction and state minimization via the formation of a quotient modulo a Myhill–Nerode relation (see [5, 12]). A key theorem of Kleene algebra used in both these constructions is

$$ax = xb \to a^*x = xb^*. \tag{1}$$

Intuitively, $x$ represents a transformation between two state spaces, and $a$ and $b$ are transition relations of automata on those respective state spaces. The theorem represents a kind of bisimulation relationship. The completeness proof depends on the uniqueness of minimal deterministic automata: given two regular expressions representing the same regular set, it is shown how the construction of the unique minimal deterministic automaton can be carried out purely algebraically and the equivalence deduced from the axioms of Kleene algebra.

In this paper we give a new proof of completeness that does not depend on the uniqueness of minimal automata. Our approach is via a generalization of Myhill–Nerode relations. We introduce *automatic systems*, a special class of infinite systems that can be viewed as infinite-state automata. Automatic systems can be collapsed using Myhill–Nerode relations in much the same way that finite automata can. Again, the chief property describing the relationship between the collapsed and uncollapsed systems is (1). The Brzozowski derivative [3] on an algebra of polynomials over a Kleene algebra gives rise to a triangular automatic system that can be solved using these methods. Completeness is proved essentially by showing that two equivalent systems have a common Myhill–Nerode unwinding.

## 2 Kleene Algebra

Kleene algebra was introduced by S. C. Kleene (see [4]). We define a Kleene algebra to be an idempotent semiring such that $a^*b$ is the least solution to $b + ax \leq x$ and $ba^*$ the least solution to $b + xa \leq x$. This axiomatization is from [10], to which we refer the reader for further definitions and basic results.

The free Kleene algebra $\mathcal{F}_\Sigma$ on a finite set of generators $\Sigma$ is normally constructed as the set of regular expressions over $\Sigma$ modulo the Kleene algebra axioms. This is the same as $\mathbf{2}[\Sigma]$, the algebra of Kleene polynomials over indeterminates $\Sigma$, where $\mathbf{2}$ is the two-element Kleene algebra. As shown in [10], $\mathcal{F}_\Sigma$ is isomorphic to $\mathbf{Reg}_\Sigma$, the Kleene algebra of regular sets of strings over $\Sigma$.

The evaluation morphism $\varepsilon : \mathbf{2}[\Sigma] \to \mathbf{2}$, where $\varepsilon(a) = 0$ for $a \in \Sigma$, corresponds to the *empty word property* (EWP) discussed by Salomaa [2, 19]. This map satisfies the property that $\varepsilon(\beta) = 1$ if $1 \leq \beta$, 0 otherwise.

## 3 Generalized Triangular Matrices

Let $A$ be a set and $\leq$ a preorder (reflexive and transitive) on $A$. The preordered set $A$ is *finitary* if all principal upward-closed sets $A_\alpha \stackrel{\text{def}}{=} \{\beta \in A \mid \alpha \leq \beta\}$ are finite.

A (*generalized*) *triangular matrix* on a finitary preordered set $A$ over a Kleene algebra $K$ is a map $e : A^2 \to K$ such that $e_{\alpha,\beta} = 0$ whenever $\alpha \not\leq \beta$. The family of generalized triangular matrices on $A$ over $K$ is denoted $\mathrm{Mat}(A, K)$.

There are several ways this definition generalizes the usual notion of triangular matrix. Ordinarily, the index set is finite and totally ordered, usually $\{1, \ldots, n\}$ with its natural order, and *triangular* is defined with respect to this order. In the present development, the index set $A$ can be infinite and the order can be any finitary preorder. There can be pairwise incomparable elements, as well as "loops" with distinct elements $\alpha, \beta$ such that $\alpha \leq \beta$ and $\beta \leq \alpha$.

Nevertheless, the restrictions we have imposed are sufficient to allow the definition of the usual matrix operations on $\mathrm{Mat}(A, K)$. For $e, f \in \mathrm{Mat}(A, K)$, let

$$(e+f)_{\alpha,\beta} \stackrel{\text{def}}{=} e_{\alpha,\beta} + f_{\alpha,\beta} \qquad \mathbf{1}_{\alpha,\beta} \stackrel{\text{def}}{=} \begin{cases} 1, \text{ if } \alpha = \beta \\ 0, \text{ otherwise} \end{cases}$$

$$(ef)_{\alpha,\beta} \stackrel{\text{def}}{=} \sum_{\gamma} e_{\alpha,\gamma} f_{\gamma,\beta} \qquad \mathbf{0}_{\alpha,\beta} \stackrel{\text{def}}{=} 0.$$

Because $A$ is finitary, the sum in the definition of matrix product is finite. It is not difficult to verify that the structure $\mathrm{Mat}(A, K)$ forms an idempotent semiring under these definitions.

Now we wish to define the operator $^*$ on $\mathrm{Mat}(A, K)$ so as to make it a Kleene algebra. That $A$ is finitary is elemental here. We define $e_{\alpha,\beta}$ to be $(e \restriction A_\alpha)^*_{\alpha,\beta}$, where $e \restriction A_\alpha$ is the restriction of $e$ to domain $A_\alpha^2$. Since $A_\alpha$ is finite, $e \restriction A_\alpha$ is a finite square submatrix of $e$, so $(e \restriction A_\alpha)^*$ exists. Actually, we could have restricted $e$ to any finite upward-closed subset $B \subseteq A$ containing $\alpha$ and gotten the same result.

Formally, let $\mathbf{1}_B$ denote the restriction of $\mathbf{1}$ to domain $A \times B$, where $B \subseteq A$ is upward-closed. The restriction of $e$ to domain $B^2$ can be represented matricially by $\mathbf{1}_B^T\, e\, \mathbf{1}_B$. If $B$ is finite, then $\mathbf{1}_B^T\, e\, \mathbf{1}_B$ is a finite square matrix, therefore the $^*$ operator can be applied to obtain the matrix $(\mathbf{1}_B^T\, e\, \mathbf{1}_B)^*$. We define

$$e^* \stackrel{\text{def}}{=} \sup_B \mathbf{1}_B\, (\mathbf{1}_B^T\, e\, \mathbf{1}_B)^*\, \mathbf{1}_B^T, \tag{2}$$

where the supremum is taken over all finite upward-closed subsets $B \subseteq A$. It can be shown by elementary arguments that the value of the right-hand side of (2) at $\alpha, \beta$ is a constant independent of $B$ if $\alpha \in B$ and 0 if $\alpha \notin B$. Since there is at least one finite upward-closed subset of $A$ containing $\alpha$ (namely $A_\alpha$), the supremum exists.

## 4 Infinite Systems of Linear Inequalities

We can exploit the Kleene algebra structure of $\mathrm{Mat}(A, K)$ to solve triangular systems of linear inequalities indexed by the infinite set $A$. Such a system is represented by a triangular matrix $e \in \mathrm{Mat}(A, K)$ and vector $c : A \to K$ as

$$\sum_{\beta} e_{\alpha,\beta} X_\beta + c_\alpha \leq X_\alpha, \quad \alpha \in A,$$

where $X$ is a vector of indeterminates. This is equivalent to the infinite matrix-vector inequality $eX + c \leq X$.

A solution of the system $(A, e, c)$ over $K$ is a map $\sigma : A \to K$ such that

$$\sum_{\beta} e_{\alpha,\beta}\sigma_\beta + c_\alpha \leq \sigma_\alpha, \quad \alpha \in A,$$

or in other words $e\sigma + c \leq \sigma$. As in the finite case, the unique least solution to this system is $e^*c$.

## 5 Automatic Systems

We now focus on index sets $A$ of a special form. Let $\Sigma$ be a finite set of functions acting on $A$. The value of the function $a \in \Sigma$ on $\alpha \in A$ is denoted $\alpha a$. Each finite-length string $x \in \Sigma^*$ induces a function $x : A \to A$ defined inductively by

$$\alpha\varepsilon \stackrel{\text{def}}{=} \alpha \qquad \alpha(xa) \stackrel{\text{def}}{=} (\alpha x)a.$$

Define $\alpha \leq \beta$ if $\beta = \alpha x$ for some $x \in \Sigma^*$. This is a preorder on $A$, and it is finitary iff for all $\alpha \in A$, the set $A_\alpha = \{\alpha x \mid x \in \Sigma^*\}$ is finite. Since $\Sigma$ is assumed to be finite, it follows from König's lemma that $A$ is finitary iff every $\leq$-chain $\alpha_0 \leq \alpha_1 \leq \cdots$ has only finitely many distinct elements; equivalently, for every $\alpha$, every sufficiently long string $x \in \Sigma^*$ has two distinct prefixes $y$ and $z$ such that $\alpha y = \alpha z$.

Now let $e \in \mathrm{Mat}(A, K)$ be a triangular matrix and $c : A \to K$ a vector over $A$ representing a triangular system of linear inequalities as described in the last section. Assume further that if $\beta \neq \alpha a$ for any $a \in \Sigma$, then $e_{\alpha,\beta} = 0$. The system of inequalities represented by $e$ and $c$ is thus

$$\sum_{a \in \Sigma} e_{\alpha,\alpha a} X_{\alpha a} + c_\alpha \leq X_\alpha, \quad \alpha \in A.$$

A linear system of this form is called *automatic*. This name is meant to suggest a generalization of finite-state automata over $\mathbf{Reg}_\Sigma$ to infinite-state systems over arbitrary Kleene algebras. One can regard $A$ as a set of states and elements of $\Sigma$ as input symbols. An ordinary finite-state automaton is essentially a finite automatic system over the Kleene algebra $\mathbf{Reg}_\Sigma$.

## 6 Myhill–Nerode Relations

Myhill–Nerode relations are fundamental in the theory of finite-state automata. Among other applications, they allow an automaton to be collapsed to a unique equivalent minimal automaton. Myhill–Nerode relations can also be defined on finitary automatic systems.

Given a finitary automatic system $S = (A, e, c)$, an equivalence relation $\equiv$ on $A$ is called *Myhill–Nerode* if the following conditions are satisfied: for all $\alpha, \beta \in A$ and $a \in \Sigma$,

(i) if $\alpha \equiv \beta$, then $\alpha a \equiv \beta a$;
(ii) if $\alpha \equiv \beta$, then $\sum_{\alpha b \equiv \alpha a} e_{\alpha,\alpha b} = \sum_{\beta b \equiv \beta a} e_{\beta,\beta b}$;
(iii) if $\alpha \equiv \beta$, then $c_\alpha = c_\beta$.

For any Myhill–Nerode relation $\equiv$ on $S = (A, e, c)$, we can construct a quotient system $S/\equiv$ as follows:

$$\begin{aligned}
[\alpha] &\stackrel{\text{def}}{=} \{\beta \in A \mid \beta \equiv \alpha\} & (e/\equiv)_{[\alpha],[\alpha]a} &\stackrel{\text{def}}{=} \textstyle\sum_{\alpha b \equiv \alpha a} e_{\alpha,\alpha b} \\
[\alpha]a &\stackrel{\text{def}}{=} [\alpha a] & (c/\equiv)_{[\alpha]} &\stackrel{\text{def}}{=} c_\alpha \\
A/\equiv &\stackrel{\text{def}}{=} \{[\alpha] \mid \alpha \in A\} & S/\equiv &\stackrel{\text{def}}{=} (A/\equiv,\, e/\equiv,\, c/\equiv).
\end{aligned}$$

The matrix $e/\equiv$ and vector $c/\equiv$ are well defined by the restrictions in the definition of Myhill–Nerode relation. The original system $S$ can be thought of as an "unfolding" of the collapsed system $S/\equiv$.

The set $\Sigma$ acts on $A/\equiv$ by $[\alpha]a \stackrel{\text{def}}{=} [\alpha a]$. This is well defined by clause (i) in the definition of Myhill–Nerode relation. The preorder $\leq$ on $A/\equiv$ is defined as in Section 5. This relation is easily checked to be reflexive, transitive, and finitary on $A/\equiv$. Moreover, the matrix $e/\equiv$ is triangular. Thus $S/\equiv$ is an automatic system.

We now describe the relationship between the solutions of the systems $S$ and $S/\equiv$. First, any solution of the collapsed system $S/\equiv$ can be lifted to a solution of the original system $S$. If $\sigma : A/\equiv \to K$ is a solution of $S/\equiv$, define $\widehat{\sigma} : A \to K$ by $\widehat{\sigma}_\alpha \stackrel{\text{def}}{=} \sigma_{[\alpha]}$. It is easily verified that $\widehat{\sigma}$ is a solution of $S$:

$$\begin{aligned}
\sum_{a \in \Sigma} e_{\alpha,\alpha a} \widehat{\sigma}_{\alpha a} + c_\alpha &= \sum_{a \in \Sigma} e_{\alpha,\alpha a} \sigma_{[\alpha a]} + c_\alpha \\
&= \sum_{a \in \Sigma} (e/\equiv)_{[\alpha],[\alpha a]} \sigma_{[\alpha a]} + (c/\equiv)_{[\alpha]} \\
&\leq \sigma_{[\alpha]} = \widehat{\sigma}_\alpha.
\end{aligned}$$

It is more difficult to argue that $\widehat{\sigma}$ is the least solution to $S$. The unfolded system $S$ is less constrained than $S/\equiv$, and it is conceivable that a smaller solution could be found in which different but $\equiv$-equivalent $\alpha, \beta$ are assigned different values, whereas in the collapsed system $S/\equiv$, $\alpha$ and $\beta$ are unified and must have the same value. We show that this cannot happen.

*Example 1.* Consider the $2 \times 2$ system

$$\begin{aligned}
aY + c &\leq X \\
aX + c &\leq Y.
\end{aligned}$$

This is represented by the matrix-vector equation

$$\begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \end{bmatrix} + \begin{bmatrix} c \\ c \end{bmatrix} \leq \begin{bmatrix} X \\ Y \end{bmatrix}.$$

We can collapse this system by a Myhill–Nerode relation to the single inequality $aX + c \le X$. The least solution of the $2 \times 2$ system is given by

$$\begin{aligned}
\begin{bmatrix} X \\ Y \end{bmatrix} &= \begin{bmatrix} 0 & a \\ a & 0 \end{bmatrix}^* \cdot \begin{bmatrix} c \\ c \end{bmatrix} \\
&= \begin{bmatrix} (aa)^* & (aa)^*a \\ (aa)^*a & (aa)^* \end{bmatrix} \cdot \begin{bmatrix} c \\ c \end{bmatrix} \\
&= \begin{bmatrix} (aa)^*c + (aa)^*ac \\ (aa)^*ac + (aa)^*c \end{bmatrix} \\
&= \begin{bmatrix} a^*c \\ a^*c \end{bmatrix},
\end{aligned}$$

which is the same as that obtained by lifting the least solution $a^*c$ of the collapsed system $aX + c \le X$.

We show that in general, the least solution of $S$ is obtained by lifting the least solution of $S/\equiv$. Define $\chi : A \times A/\equiv \to K$ by

$$\chi_{\alpha,[\beta]} \stackrel{\text{def}}{=} \begin{cases} 1, \text{ if } \alpha \equiv \beta \\ 0, \text{ otherwise.} \end{cases}$$

The matrix $\chi$ is called the *characteristic matrix* of $\equiv$. To lift a solution from $S/\equiv$ to $S$, we multiply it on the left by $\chi$; thus in the above example, $\widehat{\sigma} = \chi\sigma$.

Now for any $\alpha, \gamma$,

$$\begin{aligned}
(e\chi)_{\alpha,[\gamma]} &= \sum_{\alpha a} e_{\alpha,\alpha a}\chi_{\alpha a,[\gamma]} \\
&= \sum_{\alpha a \equiv \gamma} e_{\alpha,\alpha a} \\
&= (e/\equiv)_{[\alpha],[\gamma]} \\
&= \sum_{[\beta]} \chi_{\alpha,[\beta]}(e/\equiv)_{[\beta],[\gamma]} \\
&= (\chi(e/\equiv))_{\alpha,[\gamma]},
\end{aligned}$$

therefore $e\chi = \chi(e/\equiv)$. By (1) (see [13]), $e^*\chi = \chi(e/\equiv)^*$. Since $c = \chi(c/\equiv)$, we have

$$e^*c = e^*\chi(c/\equiv) = \chi(e/\equiv)^*(c/\equiv),$$

which shows that the least solution $e^*c$ of $S$ is obtained by lifting the least solution $(e/\equiv)^*(c/\equiv)$ of $S/\equiv$.

## 7 Brzozowski Derivatives

For $x \in \Sigma^*$, the *Brzozowski derivative* was originally defined by Brzozowski [3, 4] as a map $2^{\Sigma^*} \to 2^{\Sigma^*}$ such that

$$D_x(A) \stackrel{\text{def}}{=} \{y \in \Sigma^* \mid xy \in A\};$$

that is, the set of strings obtained by removing $x$ from the front of a string in $A$. It follows from elementary arguments that $D_x(A)$ is a regular set if $A$ is.

Here we wish to consider $D_x$ as an operator on $\mathcal{F}_\Sigma$. Without knowing that $\mathcal{F}_\Sigma \cong \mathbf{Reg}_\Sigma$, we could have defined $D_x$ on $\mathcal{F}_\Sigma$ inductively as follows. For $a \in \Sigma$,

$$\begin{aligned} D_a(0) \;&=\; D_a(1) = D_a(b) \stackrel{\text{def}}{=} 0, \quad b \neq a \\ D_a(a) &\stackrel{\text{def}}{=} 1 \\ D_a(\alpha+\beta) &\stackrel{\text{def}}{=} D_a(\alpha) + D_a(\beta) \\ D_a(\alpha\beta) &\stackrel{\text{def}}{=} D_a(\alpha)\beta + \varepsilon(\alpha)D_a(\beta) \\ D_a(\alpha^*) &\stackrel{\text{def}}{=} D_a(\alpha)\alpha^*, \end{aligned} \tag{3}$$

where $\varepsilon : \mathcal{F}_\Sigma \to \mathbf{2}$ is the evaluation morphism $\varepsilon(a) = 0$, $a \in \Sigma$. We then define inductively

$$D_\varepsilon(\alpha) \stackrel{\text{def}}{=} \alpha \qquad D_{xa}(\alpha) \stackrel{\text{def}}{=} D_a(D_x(\alpha)).$$

This definition agrees with Brzozowski's on $\mathbf{Reg}_\Sigma$ [3]. However, we must argue axiomatically that it is well defined on elements of $\mathcal{F}_\Sigma$; that is, if $\alpha = \beta$ is a theorem of Kleene algebra, then $D_a(\alpha) = D_a(\beta)$. This can be done by induction on the lengths of proofs. We argue the case of the Horn axiom $\alpha\gamma + \beta \leq \gamma \to \alpha^*\beta \leq \gamma$ explicitly. Suppose we have derived $\alpha^*\beta \leq \gamma$ by this rule, having previously proved $\alpha\gamma + \beta \leq \gamma$. By the induction hypothesis, we have $D_a(\alpha\gamma+\beta) \leq D_a(\gamma)$ and we wish to prove that $D_a(\alpha^*\beta) \leq D_a(\gamma)$.

$$\begin{aligned} D_a(\alpha^*\beta) &= D_a(\alpha^*)\beta + \varepsilon(\alpha^*)D_a(\beta) \\ &= D_a(\alpha)\alpha^*\beta + D_a(\beta) \\ &\leq D_a(\alpha)\gamma + D_a(\beta) \\ &\leq D_a(\alpha)\gamma + \varepsilon(\alpha)D_a(\gamma) + D_a(\beta) \\ &= D_a(\alpha\gamma+\beta) \\ &\leq D_a(\gamma). \end{aligned}$$

The following lemmas list some basic properties of Brzozowski derivatives. All of these properties are well known and are easily derived by elementary inductive arguments using the laws of Kleene algebra.

**Lemma 1.** *Let $R : \mathcal{F}_\Sigma \to \mathbf{Reg}_\Sigma$ be the canonical interpretation $R(a) = \{a\}$.*

(i) *For $a \in \Sigma$, $aD_a(\beta) \leq \beta$;*
(ii) *If $1 \leq \beta$, then for $m \geq n = |x|$, $D_x(\beta^m) = D_x(\beta^n)\beta^{m-n}$;*
(iii) *For $n = |x|$, $D_x(\alpha^*) = D_x((1+\alpha)^n)\alpha^*$;*
(iv) $D_x(\alpha\beta) = D_x(\alpha)\beta + \sum_{x=yz} \varepsilon(D_y(\alpha))D_z(\beta)$;
(v) $\varepsilon(D_x(\alpha\beta)) = \sum_{x=yz} \varepsilon(D_y(\alpha)D_z(\beta))$;
(vi) $D_x(\alpha^*) = D_x(1) + D_x(\alpha)\alpha^* + \sum_{\substack{x=yz \\ z\neq x}} \varepsilon(D_y(\alpha))D_z(\alpha^*)$;

(vii) $x \in R(\alpha)$ *iff* $\varepsilon(D_x(\alpha)) = 1$.

*Proof.* All follow by elementary inductive arguments from the definition of $D_x$ and the laws of Kleene algebra. We prove (vii) explicitly. Proceeding by induction on $\alpha$, the base cases $\alpha = 0, 1$, or $a \in \Sigma$ are immediate. For expressions of the form $\alpha + \beta$, the result follows from the linearity of $R$, $\varepsilon$, and $D_x$. For the other compound expressions,

$$\begin{aligned}
x \in R(\alpha\beta) &\iff \exists y, z\ x = yz \wedge y \in R(\alpha) \wedge z \in R(\beta) \\
&\iff \exists y, z\ x = yz \wedge \varepsilon(D_y(\alpha)) = 1 \wedge \varepsilon(D_z(\beta)) = 1 \\
&\iff \sum_{x=yz} \varepsilon(D_y(\alpha)D_z(\beta)) = 1 \\
&\iff \varepsilon(D_x(\alpha\beta)) = 1 \qquad \text{by (v);}
\end{aligned}$$

$$\begin{aligned}
x \in R(\alpha^*) &\iff x \in R((1+\alpha)^n), \quad \text{where } n = |x| \\
&\iff \varepsilon(D_x((1+\alpha)^n)) = 1 \\
&\iff \varepsilon(D_x((1+\alpha)^n))\varepsilon(\alpha^*) = 1 \\
&\iff \varepsilon(D_x((1+\alpha)^n)\alpha^*) = 1 \\
&\iff \varepsilon(D_x(\alpha^*)) = 1 \qquad \text{by (iii).}
\end{aligned}$$

## 8 Brzozowski Systems

A class of automatic systems can be defined in terms of Brzozowski derivatives. We take the set $A$ in Section 5 to be $\mathcal{F}_\Sigma$ and define the action of $a \in \Sigma$ on $\mathcal{F}_\Sigma$ as $D_a$. That is, for all $\alpha \in \mathcal{F}_\Sigma$, $\alpha a \stackrel{\text{def}}{=} D_a(\alpha)$. We must argue that the induced preorder is finitary. The proof of Brzozowski (see [4]) depends on the interpretation $\mathbf{Reg}_\Sigma$, but we must argue axiomatically.

**Lemma 2.** *For any $\alpha$, the set $\{\alpha x \mid x \in \Sigma^*\} = \{D_x(\alpha) \mid x \in \Sigma^*\}$ is finite.*

*Proof.* The proof proceeds by induction on $\alpha$. For $\alpha$ of the form 0, 1, or $a \in \Sigma$, the result is easy. For $\alpha + \beta$, the result follows from the linearity of $D_x$ and the induction hypothesis. For $\alpha\beta$, the result follows from Lemma 1(iv) and the induction hypothesis. Finally, for $\alpha^*$, the result follows from Lemma 1(vi) and the induction hypothesis.

Now consider the system $S = (\mathcal{F}_\Sigma, e, c)$, where

$$e_{\alpha,\alpha a} \stackrel{\text{def}}{=} \sum_{\alpha b = \alpha a} b \qquad c_\alpha \stackrel{\text{def}}{=} \varepsilon(\alpha).$$

We call this system the *Brzozowski system* on $\Sigma$. The least solution of this system over $\mathcal{F}_\Sigma$ is $\ell = e^* c$. The key property that we need is that $\ell$, considered as a map $\ell : \mathcal{F}_\Sigma \to \mathcal{F}_\Sigma$, is a homomorphism. We show in fact that $\ell$ is $\iota$, the identity on $\mathcal{F}_\Sigma$.

**Lemma 3.** *The identity map $\iota : \alpha \mapsto \alpha$ is the least solution to the Brzozowski system.*

*Proof.* First we show that $\ell \leq \iota$. It suffices to show that $\iota$ is a solution to $S$. We must argue that for all $\alpha \in \mathcal{F}_\Sigma$,

$$\sum_{a \in \Sigma} aD_a(\alpha) + \varepsilon(\alpha) \leq \alpha.$$

But this is immediate from Lemma 1(i) and the property $\varepsilon(\beta) \leq \beta$ noted in Section 2.

Now we show that $\iota$ is the least solution to $S$. The major portion of the work is involved in showing that if $\alpha \leq \beta$, then $\ell_\alpha \leq \ell_\beta$. We use the Myhill–Nerode theory developed in Section 6 to find a common unwinding of the Brzozowski system $S$, allowing us to compare $\ell_\alpha$ and $\ell_\beta$.

First, lift the system $S$ to the product $\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma$ under each of the two projection maps to obtain two systems $U = (\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma, e, c)$ and $V = (\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma, e, d)$, where

$$e_{(\gamma,\delta),(\gamma,\delta)a} \stackrel{\text{def}}{=} \sum_{\substack{\gamma b = \gamma a \\ \delta b = \delta a}} b \qquad c_{\gamma,\delta} \stackrel{\text{def}}{=} \varepsilon(\gamma) \qquad d_{\gamma,\delta} \stackrel{\text{def}}{=} \varepsilon(\delta).$$

The relations defined by the two projections,

$$(\gamma,\delta) \equiv_1 (\gamma',\delta') \stackrel{\text{def}}{\iff} \gamma = \gamma' \qquad (\gamma,\delta) \equiv_2 (\gamma',\delta') \stackrel{\text{def}}{\iff} \delta = \delta',$$

are Myhill–Nerode.

Now restrict these systems to the finite induced subsystems on

$$(\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma)_{(\alpha,\beta)} = \{(\alpha x, \beta x) \mid x \in \Sigma^*\}$$

to obtain $U' = ((\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma)_{(\alpha,\beta)}, e', c')$ and $V' = ((\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma)_{(\alpha,\beta)}, e', d')$, where $e'$, $c'$, and $d'$ are $e$, $c$, and $d$, respectively, restricted to $(\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma)_{(\alpha,\beta)}$. The least solution of $U'$ is $e'^* c'$ and the least solution of $V'$ is $e'^* d'$. Moreover, by linearity, $\varepsilon(D_x(\alpha)) \leq \varepsilon(D_x(\beta))$ for all $x \in \Sigma^*$, therefore $c' \leq d'$ and

$$\ell_\alpha = (e'^* c')_{\alpha,\beta} \leq (e'^* d')_{\alpha,\beta} = \ell_\beta.$$

We have shown that $\alpha \leq \beta$ implies $\ell_\alpha \leq \ell_\beta$. It follows that

$$\ell_\alpha + \ell_\beta \leq \ell_{\alpha+\beta}. \tag{4}$$

Now we show that $\alpha \leq \ell_\alpha$ for all $\alpha$ by induction on $\alpha$. We actually show by induction that $\alpha \ell_\beta \leq \ell_{\alpha\beta}$ for all $\alpha$ and $\beta$ by induction on $\alpha$.

For atomic expressions, we have

$$\begin{aligned}
\ell_{0\beta} &= \ell_0 = 0 = 0\ell_\beta; \\
\ell_{1\beta} &= \ell_\beta = 1\ell_\beta; \\
\ell_{b\beta} &= \sum_{a \in \Sigma} a\ell_{D_a(b\beta)} + \varepsilon(b\beta) \\
&= \sum_{a \in \Sigma} a\ell_{D_a(b)\beta} \\
&= b\ell_{D_b(b)\beta} \\
&= b\ell_\beta, \quad b \in \Sigma.
\end{aligned}$$

For compound expressions,

$$\begin{aligned}
(\alpha+\gamma)\ell_\beta &= \alpha\ell_\beta + \gamma\ell_\beta \\
&\le \ell_{\alpha\beta} + \ell_{\gamma\beta} && \text{by the induction hypothesis} \\
&\le \ell_{(\alpha+\gamma)\beta} && \text{by (4);}
\end{aligned}$$

$$\begin{aligned}
\alpha\gamma\ell_\beta &\le \alpha\ell_{\gamma\beta} && \text{by the induction hypothesis on } \gamma \\
&\le \ell_{\alpha\gamma\beta} && \text{by the induction hypothesis on } \alpha.
\end{aligned}$$

Finally, to show $\alpha^*\ell_\beta \le \ell_{\alpha^*\beta}$, by an axiom of Kleene algebra it is enough to show $\ell_\beta + \alpha\ell_{\alpha^*\beta} \le \ell_{\alpha^*\beta}$. We have

$$\begin{aligned}
\ell_\beta + \alpha\ell_{\alpha^*\beta} &\le \ell_\beta + \ell_{\alpha\alpha^*\beta} && \text{by the induction hypothesis} \\
&\le \ell_{\beta+\alpha\alpha^*\beta} && \text{by (4)} \\
&= \ell_{\alpha^*\beta}.
\end{aligned}$$

Thus $\ell_\alpha \le \alpha$ since $\iota$ is a solution and $\ell$ is the least solution, and $\alpha \le \ell_\alpha$ by taking $\beta = 1$ in the argument above, therefore $\ell_\alpha = \alpha$.

## 9 Completeness

The completeness result of [10], which states that the free Kleene algebra $\mathcal{F}_\Sigma$ and the Kleene algebra of regular sets $\mathbf{Reg}_\Sigma$ are isomorphic, follows from the considerations of the previous sections. Let $R : \mathcal{F}_\Sigma \to \mathbf{Reg}_\Sigma$ be the canonical interpretation in which $R(a) = \{a\}$. If $R(\alpha) = R(\beta)$, then for all $x \in \Sigma^*$, $x \in R(\alpha)$ iff $x \in R(\beta)$, therefore by Lemma 1(vii), $\varepsilon(D_x(\alpha)) = \varepsilon(D_x(\beta))$. This says that the common unwinding of the Brzozowski system $S$ on $\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma$ restricted to $(\mathcal{F}_\Sigma \times \mathcal{F}_\Sigma)_{(\alpha,\beta)}$ gives identical systems, therefore their solutions are equal. In particular, $\ell_\alpha = \ell_\beta$. By Lemma 3, $\alpha = \beta$.

## 10 The Commutative Case

A similar completeness result holds for *commutative* Kleene algebra, in which we postulate the commutativity axiom $\alpha\beta = \beta\alpha$. The free commutative Kleene algebra on $n$ generators is the Kleene algebra $\mathbf{Par}_n$ of regular subsets of $\mathbb{N}^n$. Elements of $\mathbb{N}^n$ are often called *Parikh vectors*. We interpret regular expressions over $\Sigma = \{a_1, \ldots, a_n\}$ as follows:

$$\begin{aligned}
L(a_i) &\stackrel{\text{def}}{=} \{(\underbrace{0,\ldots,0}_{i-1},1,\underbrace{0,\ldots,0}_{n-i})\} \\
L(\alpha+\beta) &\stackrel{\text{def}}{=} L(\alpha) \cup L(\beta) \\
L(\alpha\beta) &\stackrel{\text{def}}{=} \{u+v \mid u \in L(\alpha),\ v \in L(\beta)\} \\
L(\alpha^*) &\stackrel{\text{def}}{=} \bigcup_m L(\alpha)^m \\
L(0) &\stackrel{\text{def}}{=} \varnothing \\
L(1) &\stackrel{\text{def}}{=} \{(0,\ldots,0)\}.
\end{aligned}$$

A set of Parikh vectors is *regular* if it is $L(\alpha)$ for some $\alpha$. The family of all regular sets of Parikh vectors forms a commutative Kleene algebra under the above operations. We denote this algebra by $\mathbf{Par}_n$.

The completeness result follows from a characterization due to Redko (see [4]) of the equational theory of $\mathbf{Par}_n$ as the consequences of a certain infinite but easily-described set of equations, namely the equational axioms for commutative idempotent semirings plus the equations

$$\begin{aligned} (x+y)^* &= (x^*y)^*x^* & x^{**} &= x^* \\ (xy)^*x &= x(yx)^* & x^*y^* &= (xy)^*(x^*+y^*) \\ x^* &= 1+xx^* & x^* &= (x^m)^*(1+x)^{m-1}, \quad m \geq 1. \end{aligned}$$

All these are theorems of commutative Kleene algebra.

The proof of Redko, as given in [4], is quite involved and depends heavily on commutativity. We began this investigation in a attempt to give a uniform completeness proof for both the noncommutative and commutative case. Our hope was to give a simpler algebraic proof along the lines of [10] for commutative Kleene algebra, although the technique of [10] does not apply directly, since minimal automata are not unique. For example, the three-state deterministic automata corresponding to the expressions $(ab)^*$ and $(ba)^*$ are both minimal and represent the same set of Parikh vectors $\{(m,m) \mid m \geq 0\}$. The usual construction of the canonical deterministic automaton directly from the set itself (see [12, Lemma 16.2]) yields infinitely many states.

Nevertheless, one can define the free commutative Kleene algebra $\mathcal{C}_\Sigma$ on generators $\Sigma$ and attempt to show that $L$, factored through $\mathcal{C}_\Sigma$, gives an isomorphism $\mathcal{C}_\Sigma \to \mathbf{Par}_n$. The Brzozowski derivatives $D_a : \mathcal{C}_\Sigma \to \mathcal{C}_\Sigma$ are defined differently on products in the commutative case:

$$D_a(\alpha\beta) \stackrel{\text{def}}{=} D_a(\alpha)\beta + \alpha D_a(\beta).$$

The action of $D_a$ on other expressions is as defined in Section 7. As in that section, we can argue that $D_a$ respects the axioms of Kleene algebra. Here we must also show that it respects the commutativity axiom; in other words, $D_a(\alpha\beta) = D_a(\beta\alpha)$. Also, for any $x, y \in \Sigma^*$, $D_{xy}(\alpha) = D_{yx}(\alpha)$. Unfortunately, the principal upward closed sets $\{D_x(\alpha) \mid x \in \Sigma^*\}$ are not necessarily finite, and it is not clear how to define a Kleene algebra structure of infinite matrices as in Section 3. Nevertheless, the set $\{D_x(\alpha) \mid x \in \Sigma^*\}$ does exhibit a regular $(n-1)$-dimensional linear geometric structure which is respected by the action of the Brzozowski derivatives. It remains a topic for future investigation to see how this structure can be exploited.

## Acknowledgements

The support of the National Science Foundation under grant CCR-9708915 is gratefully acknowledged.

## References

1. Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley, Reading, Mass., 1975.

2. Roland Carl Backhouse. *Closure Algorithms and the Star-Height Problem of Regular Languages*. PhD thesis, Imperial College, London, U.K., 1975.
3. Janusz A. Brzozowski. Derivatives of regular expressions. *J. Assoc. Comput. Mach.*, 11:481–494, 1964.
4. John Horton Conway. *Regular Algebra and Finite Machines*. Chapman and Hall, London, 1971.
5. J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation*. Addison-Wesley, 1979.
6. Kazuo Iwano and Kenneth Steiglitz. A semiring on convex polygons and zero-sum cycle problems. *SIAM J. Comput.*, 19(5):883–901, 1990.
7. Stephen C. Kleene. Representation of events in nerve nets and finite automata. In C. E. Shannon and J. McCarthy, editors, *Automata Studies*, pages 3–41. Princeton University Press, Princeton, N.J., 1956.
8. Dexter Kozen. On induction vs. *-continuity. In Kozen, editor, *Proc. Workshop on Logic of Programs*, volume 131 of *Lecture Notes in Computer Science*, pages 167–176, New York, 1981. Springer-Verlag.
9. Dexter Kozen. *The Design and Analysis of Algorithms*. Springer-Verlag, New York, 1991.
10. Dexter Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Infor. and Comput.*, 110(2):366–390, May 1994.
11. Dexter Kozen. Kleene algebra with tests and commutativity conditions. In T. Margaria and B. Steffen, editors, *Proc. Second Int. Workshop Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, volume 1055 of *Lecture Notes in Computer Science*, pages 14–33, Passau, Germany, March 1996. Springer-Verlag.
12. Dexter Kozen. *Automata and Computability*. Springer-Verlag, New York, 1997.
13. Dexter Kozen. Typed Kleene algebra. Technical Report 98-1669, Computer Science Department, Cornell University, March 1998.
14. Werner Kuich. The Kleene and Parikh theorem in complete semirings. In T. Ottmann, editor, *Proc. 14th Colloq. Automata, Languages, and Programming*, volume 267 of *Lecture Notes in Computer Science*, pages 212–225, New York, 1987. EATCS, Springer-Verlag.
15. Werner Kuich and Arto Salomaa. *Semirings, Automata, and Languages*. Springer-Verlag, Berlin, 1986.
16. K. C. Ng. *Relation Algebras with Transitive Closure*. PhD thesis, University of California, Berkeley, 1984.
17. Vaughan Pratt. Dynamic algebras as a well-behaved fragment of relation algebras. In D. Pigozzi, editor, *Proc. Conf. on Algebra and Computer Science*, volume 425 of *Lecture Notes in Computer Science*, pages 77–110, Ames, Iowa, June 1988. Springer-Verlag.
18. V. N. Redko. On defining relations for the algebra of regular events. *Ukrain. Mat. Z.*, 16:120–126, 1964. In Russian.
19. Arto Salomaa. Two complete axiom systems for the algebra of regular events. *J. Assoc. Comput. Mach.*, 13(1):158–169, January 1966.
20. Alfred Tarski. On the calculus of relations. *J. Symb. Logic*, 6(3):65–106, 1941.