Fundamenta Informaticae 68 (2005) 1–10
IOS Press

On Finite Model Property of the Equational Theory of Kleene Algebras

Ewa Palka*
Faculty of Mathematics and Computer Science
Adam Mickiewicz University of Poznań
ul. Umultowska 87, 61-614 Poznań, Poland
pewka@amu.edu.pl

Abstract. The finite model property of the equational fragment of the theory of Kleene algebras is a consequence of Kozen's [3] completeness theorem. We show that, conversely, this completeness theorem can be proved assuming the finite model property of this fragment.

Keywords: Kleene algebras, action algebras, regular expressions, finite model property

1. Introduction

The Kozen completeness theorem [3] states that, for any regular expressions α, β, α equals β in the sense of regular expressions iff the equality α=β is valid in all Kleene algebras. The proof is complicated; it applies Conway-style [2] matrix representation of finite state automata and basic constructions of these automata. Krob [4] presents another approach, using infinite systems of equations characterizing finite state automata.

The aim of this paper is to show a natural connection between the Kozen completeness theorem and the finite model property of the theory of Kleene algebras in the scope of equations. Precisely, we mean the following condition:

(FMP$_K$) for any terms α, β, if α=β is not valid in the class of Kleene algebras, then α=β is not true in some finite Kleene algebra under some assignment.

*The author acknowledges the supervision of this research by Prof. Wojciech Buszkowski
Address for correspondence: Faculty of Mathematics and Computer Science, Adam Mickiewicz University of Poznań, ul. Umultowska 87, 61-614 Poznań, Poland

In Section 3 we show that (FMP$_K$) is a consequence of the Kozen completeness theorem (the proof is routine). In section 4 we prove the converse: (FMP$_K$) entails the Kozen completeness theorem. This proof applies some properties of action algebras in the sense of Pratt [5]. In particular, an essential lemma states that if α equals β in the sense of regular expressions, then α=β is valid in all complete action algebras (announced without proof in Buszkowski [1]).

Thus, an independent proof of (FMP$_K$) would provide a quite different proof of the Kozen completeness theorem, based on purely logical tools. We defer this task to further research.

2. Preliminaries

This chapter presents some preliminaries. We define two types of algebras, namely Kleene algebras and action algebras. A *Kleene algebra* [3] is an algebraic structure $\mathcal{A}$=$(A, +, \cdot, *, 0, 1)$ with two distinguished constants 0 and 1, two binary operations $+$ and $\cdot$, and a unary operation $*$ satisfying the following axioms.

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

$$a + b = b + a \tag{2}$$

$$a + 0 = a \tag{3}$$

$$a + a = a \tag{4}$$

$$a(bc) = (ab)c \tag{5}$$

$$1a = a \tag{6}$$

$$a1 = a \tag{7}$$

$$a(b + c) = ab + ac \tag{8}$$

$$(a + b)c = ac + bc \tag{9}$$

$$0a = 0 \tag{10}$$

$$a0 = 0 \tag{11}$$

$$1 + aa^* \leq a^* \tag{12}$$

$$1 + a^*a \leq a^* \tag{13}$$

$$\text{if } ax \leq x \text{ then } a^*x \leq x \tag{14}$$

$$\text{if } xa \leq x \text{ then } xa^* \leq x \tag{15}$$

where $\leq$ denotes the partial order on A, defined as follows:

$$a \leq b \Leftrightarrow a + b = b \tag{16}$$

The class of Kleene algebras is denoted KA. Axioms (1)-(4) say that $(A, +, 0)$ is an idempotent commutative monoid, and axioms (5)-(7) say that $(A, \cdot, 1)$ is a monoid. Note that axioms (12)-(15) say essentialy that the operation $*$ behaves like the asterate operator on sets of strings or the reflexive transitive closure operator on binary relations.

We say that a Kleene algebra is $*$-*continuous* if it satisfies the infinitary condition:

$$xy^*z = \sup_{n \geq 0} xy^n z \tag{17}$$

where $y^0 = 1$, $y^{n+1} = yy^n$. We will use the following properties of Kleene algebras:

$$1 \leq a^* \tag{18}$$

$$a \leq a^* \tag{19}$$

$$\text{if } a \leq b \text{ and } c \leq d \text{ then } ac \leq bd \tag{20}$$

$$a \leq x \text{ and } b \leq x \text{ iff } a + b \leq x \tag{21}$$

Pratt [5] defines an *action algebra* as an algebra $\mathcal{A}$=$(A, +, \cdot, *, \rightarrow, \leftarrow, 0, 1)$ such that $+$,$\cdot$,$*$,0,1 are as above, and $\rightarrow$,$\leftarrow$ are binary operations, satisfying axioms (1)-(7) and the following:

$$a \leq c \leftarrow b \text{ iff } ab \leq c \text{ iff } b \leq a \rightarrow c \tag{22}$$

$$1 + a^*a^* + a \leq a^* \tag{23}$$

$$\text{if } 1 + bb + a \leq b \text{ then } a^* \leq b \tag{24}$$

where the relation $\leq$ is as above. We use (RES) to denote the axiom (22). Operations $\rightarrow$ and $\leftarrow$ are called *the right residuation* and *the left residuation*, respectively. Pratt [5] shows that every action algebra is a Kleene algebra.
A structure $(A, \cdot, \leq)$ where $(A, \cdot)$ is a semigroup and $\leq$ is a partial order on A which satisfies the condition

$$\text{(MON) if } a \leq b \text{ then } ca \leq cb \text{ and } ac \leq bc$$

is called a *partially ordered semigroup* (p.o. semigroup).

Lemma 2.1. If in a p.o. semigroup $(A, \cdot, \leq)$, for all b,$c \in A$, there exist $\max\{z : zb \leq c\}$ and $\max\{z : bz \leq c\}$, then operations $\rightarrow$ and $\leftarrow$ defined by

$$c \leftarrow b = \max\{z : zb \leq c\}$$
$$b \rightarrow c = \max\{z : bz \leq c\}$$

satisfy (RES).

Proof:
We prove (RES). We prove that $ab \leq c$ iff $b \leq a \rightarrow c$. Assume $ab \leq c$. Then $b \in \{z : az \leq c\}$, so $b \leq a \rightarrow c$. Conversely assume $b \leq a \rightarrow c$. By (MON) the set $\{z : az \leq c\}$ is a lower cone, which means:

$$\text{if } z' \leq z \text{ and } az \leq c \text{ then } az' \leq c$$

Since $(a \rightarrow c) \in \{z : az \leq c\}$, we have $b \in \{z : az \leq c\}$, which yields $ab \leq c$. The proof of $ab \leq c \Leftrightarrow a \leq c \leftarrow b$ is symmetric. □

Lemma 2.2. [5] Every finite Kleene algebra expands to an action algebra.

Proof:
Let $\mathcal{A}$ be a finite Kleene algebra. By Lemma 2.1, it suffices to show that, for all b,$c$$\in$$A$, there exist $\max\{z : zb \leq c\}$ and $\max\{z : bz \leq c\}$. Since the set $\{z : zb \leq c\}$ is finite and 0 belongs to this set, we have $\{z : zb \leq c\} = \{z_1, \ldots, z_k\}$, for $k \geq 1$. We have $z_i b \leq c$ for all $1 \leq i \leq k$, so by (21) we have $z_1 b + \cdots + z_k b \leq c$. So, by (9), $(z_1 + \cdots + z_k)b \leq c$. Accordingly we have $z_1 + \cdots + z_k \in \{z : zb \leq c\}$. Obviously $z_i \leq z_1 + \cdots + z_k$ for all $1 \leq i \leq k$, so $z_1 + \cdots + z_k = \max\{z : zb \leq c\}$. The proof of the existence of $\max\{z : bz \leq c\}$ is symmetric. □

A partially ordered set $(A, \leq)$ is called *complete* if, for every $X \subseteq A$, there exist $\sup X$ and $\inf X$. An action algebra $\mathcal{A}$ is called *complete* if the set $(A, \leq)$ is complete. The class of complete action algebras is denoted CACT.

Lemma 2.3. Every complete action algebra is a $*$-continuous Kleene algebra.

Proof:
Let $\mathcal{A}$ be a complete action algebra. So $\mathcal{A}$ is a Kleene algebra.

(1) We first show that

$$a \sup X = \sup\{ax : x \in X\}$$
$$(\sup X)a = \sup\{xa : x \in X\}.$$

We use (RES). We show that $a \sup X = \sup\{ax : x \in X\}$. It suffices to show that

$$a \sup X \leq z \text{ iff for every } x \in X \ ax \leq z$$

($\Rightarrow$) is obvious, because $x \leq \sup X$ for $x \in X$. We prove ($\Leftarrow$). Assume that, for every $x \in X$, $ax \leq z$. By (RES), for every $x \in X$, $x \leq a \rightarrow z$. So $\sup X \leq a \rightarrow z$ and, by (RES), $a \sup X \leq z$. The proof of $(\sup X)a = \sup\{xa : x \in X\}$ is symmetric.

(2) As a consequence, we get:

$$a(\sup X)b = \sup\{axb : x \in X\}.$$

(3) Now we show that $y^* = \sup\{y^n : n \geq 0\}$
Let $b = \sup\{y^n : n \geq 0\}$. We have $y^n \leq y^*$, for every n (induction on n, using (23)). Hence $b \leq y^*$. By (24), it is sufficent to show that $1 + y + bb \leq b$. We only show that $bb \leq b$. Since $bb = \sup\{y^n : n \geq 0\}b$, hence:

$$\begin{aligned}
bb &= \sup\{y^n b : n \geq 0\} \\
&= \sup\{y^n \sup\{y^m : m \geq 0\} : n \geq 0\} \\
&= \sup\{\sup\{y^{n+m} : m, n \geq 0\}\} \\
&= \sup\{b\} \\
&= b
\end{aligned}$$

(4) From (2) and (3), we infer:

$$xy^*z = \sup\{xy^n z : n \geq 0\}$$

$\square$

We fix a standard first order language $\mathcal{L}$ of Kleene algebras, with operation symbols $+$,$\cdot$,$*$ and individual constants 0,1. VAR denotes the set of individual variables. We also admit an additional finite set Σ of individual constants, and the extended language is denoted $\mathcal{L}_\Sigma$. Lower Greek characters α, β, γ,... represent terms of $\mathcal{L}_\Sigma$.

Let $\mathcal{A}$ be a Kleene algebra. By a model (on $\mathcal{A}$) we mean a pair $(\mathcal{A}, \mu)$ such that $\mu : VAR \cup \Sigma \to A$ is an assignment which extends to a language homomorphism, by setting:

$$\mu(0) = 0$$
$$\mu(1) = 1$$
$$\mu(\alpha + \beta) = \mu(\alpha) + \mu(\beta)$$
$$\mu(\alpha\beta) = \mu(\alpha)\mu(\beta)$$
$$\mu(\alpha^*) = \mu(\alpha)^*$$

An equality $\alpha = \beta$ *is true in model* $(\mathcal{A}, \mu)$ if $\mu(\alpha) = \mu(\beta)$; as usual, we write $(\mathcal{A}, \mu) \models \alpha = \beta$. Eq$_\Sigma$(KA) denotes the set of equalities $\alpha = \beta$ of language $\mathcal{L}_\Sigma$, which are true in all models. If $\mathcal{K}$ is a class of algebras, then we write $\models_\mathcal{K} \alpha = \beta$ if $\alpha = \beta$ is true in all models $(\mathcal{A}, \mu)$ such that $\mathcal{A} \in \mathcal{K}$.

Let $\mathcal{G}$=$(G, \cdot, 1)$ be a monoid. We denote $P(G)$=$\{X : X \subseteq G\}$. We construct a powerset algebra $\mathcal{P}(\mathcal{G})$=$(P(G), +, \cdot, *, \mathbf{0}, \mathbf{1})$ such that $+$,$\cdot$,$*$ are operations on sets, defined as follows:

$$XY = \{ab : a \in X, b \in Y\}$$
$$X + Y = X \cup Y$$
$$X^0 = \{1\}$$
$$X^{n+1} = X^n X \text{ for } n \geq 0$$
$$X^* = \bigcup_{n=0}^{\infty} X^n$$
$$\mathbf{0} = \emptyset$$
$$\mathbf{1} = \{1\}$$

Fact 2.1. The powerset algebra $\mathcal{P}(\mathcal{G})$ over the monoid $\mathcal{G}$ is a Kleene algebra. Actually, $\mathcal{P}(\mathcal{G})$ is a complete action algebra with residuation operations defined as follows:

$$X \to Y = \{a \in G : (\forall b \in X)\ ba \in Y\}$$
$$Y \leftarrow X = \{a \in G : (\forall b \in X)\ ab \in Y\}$$

Let Σ be a nonempty, finite alphabet. Σ^* denotes the set of finite strings on Σ. For $x, y \in \Sigma^*$, xy denotes the concatenation of strings x and y. ε denotes the empty string. Subsets of Σ^* are called *languages* on Σ. The algebra $(\Sigma^*, \cdot, \varepsilon)$ is the free monoid generated by Σ. The powerset algebra $\mathcal{P}(\Sigma^*)$ over $(\Sigma^*, \cdot, \varepsilon)$ is called the *algebra of languages* on Σ.

In what follows we identify the alphabet Σ with the set of additional individual constant of $\mathcal{L}_\Sigma$. Variable free terms of $\mathcal{L}_\Sigma$ are called *regular expressions* on Σ. REG(Σ) denotes the set of regular expressions on Σ. For an assigment $L : VAR \cup \Sigma \to P(\Sigma^*)$, satisfying $L(a) = \{a\}$, for all $a \in \Sigma$, and $\alpha \in REG(\Sigma)$, the language $L(\alpha)$ is called the *language denoted* by the regular expression α. Languages denoted by regular expressions on Σ are called *regular languages* on Σ. For α, $\beta \in REG(\Sigma)$, we say that α and β are *equal as regular expressions* if $L(\alpha) = L(\beta)$.

3. The Kozen theorem entails FMP$_K$

Our purpose is to show that FMP$_K$ is a consequence of the Kozen completeness theorem.

An equivalence relation $\sim$ on Σ^* is called a *congruence* on Σ^* if it satisfies the condition:

$$\text{if } x_1 \sim y_1 \text{ and } x_2 \sim y_2 \text{ then } x_1x_2 \sim y_1y_2$$

The cardinality of the family of equivalence classes of $\sim$ is called the index of $\sim$. Let $L \subseteq \Sigma^*$ be a language on Σ. We define a binary relation $\sim_L$ on Σ^* as follows:

$$x \sim_L y \text{ iff for all } u, w \in \Sigma^* \ (uxw \in L \text{ iff } uyw \in L)$$

We say that a relation $\sim$ is compatible with $L \subseteq \Sigma^*$ if, for any $x, y \in \Sigma^*$, if $x \sim y$ and $x \in L$, then $y \in L$. The following fact is well-known.

Fact 3.1. For any language L$\subseteq\Sigma^*$, $\sim_L$ is the largest congruence on Σ^* compatible with L. L is a regular language iff $\sim_L$ is of finite index.

We fix regular expressions α, $\beta\in REG(\Sigma)$. Let $\gamma_1, \dots, \gamma_k$ denote all subterms of α, β. We define $L_i = L(\gamma_i)$ and, for $x, y \in \Sigma^*$, $x \sim y$ iff $x \sim_{L_i} y$, for all $i = 1, \dots, k$.

Fact 3.2. The relation $\sim$ is a congruence on Σ^* compatible with every language L_i and it is of finite index.

Accordingly we can construct a quotient structure $\Sigma^*/\sim$. We set:

$$[x] = \{y \in \Sigma^* : x \sim y\}$$
$$[x][y] = [xy]$$
$$1 = [\varepsilon]$$

Further, we form the powerset algebra $\mathcal{P}(\Sigma^*/\sim)$, and we consider an assigment $\mu : VAR \cup \Sigma \to P(\Sigma^*/\sim)$, satisfying:

$$\mu(a) = \{[a]\}, \text{ for } a \in \Sigma.$$

Then, we have the following equalities:

$$\mu(0) = \emptyset$$
$$\mu(1) = \{[\varepsilon]\}$$
$$\mu(\alpha + \beta) = \mu(\alpha) \cup \mu(\beta)$$
$$\mu(\alpha\beta) = \mu(\alpha)\mu(\beta)$$
$$\mu(\alpha^*) = \mu(\alpha)^*$$

By Fact 3.2, $\Sigma^*/\sim$ and $\mathcal{P}(\Sigma^*/\sim)$ are finite algebras. The following lemma is crucial.

Lemma 3.1. For any $\gamma \in \{\gamma_1, \dots, \gamma_k\}$, we have

$$\mu(\gamma) = \{[x] : x \in L(\gamma)\} \tag{25}$$

Proof:
We show:

$$[x] \in \mu(\gamma) \text{ iff } x \in L(\gamma)$$

The proof is by induction on the complexity of γ. We consider six cases.

Case 1. $\gamma \equiv a$, $a \in \Sigma$. Let $[x] \in \mu(a)$. By the construction of μ, we have $[x] = [a]$, so $x \sim a$. Since $L(a) = \{a\}$ and $\sim$ is compatible with $L(a)$, then $x \in L(a)$. Let $x \in L(a)$. Since $L(a) = \{a\}$, then $x = a$. Hence $[x] = [a]$. But $[a] \in \mu(a)$, so $[x] \in \mu(a)$.

Case 2. $\gamma \equiv 0$. Since $\mu(0) = \emptyset$ and $L(0) = \emptyset$, then $\mu(0) = L(0)$.

Case 3. $\gamma \equiv 1$. Let $[x] \in \mu(1)$. By the construction of μ, we have $[x] = [\varepsilon]$, so $x \sim \varepsilon$ and $\varepsilon \in L(1)$. Then $x \in L(1)$. Let $x \in L(1)$. Hence $x = \varepsilon$. So $[x] = [\varepsilon]$. But $[\varepsilon] \in \mu(1)$. Finally, $[x] \in \mu(1)$.

Case 4. $\gamma \equiv \gamma_1 + \gamma_2$. $[x] \in \mu(\gamma_1 + \gamma_2)$ iff $[x] \in \mu(\gamma_1)$ or $[x] \in \mu(\gamma_2)$ iff $x \in L(\gamma_1)$ or $x \in L(\gamma_2)$ iff $x \in L(\gamma_1 + \gamma_2)$.

Case 5. $\gamma \equiv \gamma_1\gamma_2$. Let $[x] \in \mu(\gamma_1\gamma_2) = \mu(\gamma_1)\mu(\gamma_2)$. There exist $y, z \in \Sigma^*$ such that $[x] = [y][z]$, where $[y] \in \mu(\gamma_1)$ and $[z] \in \mu(\gamma_2)$. Thus, by the induction hypothesis, $y \in L(\gamma_1)$ and $z \in L(\gamma_2)$, so $yz \in L(\gamma_1)L(\gamma_2)$. Since $[x] = [y][z] = [yz]$, then $x \sim yz$ and $yz \in L(\gamma_1)L(\gamma_2) = L(\gamma_1\gamma_2)$. By compatibility, $x \in L(\gamma_1\gamma_2)$. Let $x \in L(\gamma_1\gamma_2) = L(\gamma_1)L(\gamma_2)$. There exist $y, z \in \Sigma^*$ such that $x = yz$ and $y \in L(\gamma_1)$, $z \in L(\gamma_2)$. Thus, by the induction hypothesis, $[y] \in \mu(\gamma_1)$ and $[z] \in \mu(\gamma_2)$. Since $x = yz$, we have $[x] = [yz] = [y][z] \in \mu(\gamma_1)\mu(\gamma_2) = \mu(\gamma_1\gamma_2)$. So $[x] \in \mu(\gamma_1\gamma_2)$.

Case 6. $\gamma \equiv \eta^*$. Let $[x] \in \mu(\eta^*) = \mu(\eta)^*$. There exists $n \geq 0$ such that $[x] = [x_1] \cdots [x_n]$ and $[x_i] \in \mu(\eta)$, for every $1 \leq i \leq n$. Hence, by the induction hypothesis, $x_i \in L(\eta)$, for every $1 \leq i \leq n$. Thus $x_1 \cdots x_n \in L(\eta)^n \subseteq L(\eta^*)$. Since $x \sim x_1 \cdots x_n$, then $x \in L(\eta^*)$. Let $x \in L(\eta^*) = L(\eta)^*$. So there exists $n \geq 0$ such that $x = x_1 \cdots x_n$ and $x_i \in L(\eta)$, for every $1 \leq i \leq n$. Thus, by the induction hypothesis, $[x_i] \in \mu(\eta)$, for every $1 \leq i \leq n$. Since $x = x_1 \cdots x_n$, then $[x] = [x_1 \cdots x_n] = [x_1] \cdots [x_n] \in \mu(\eta)^n \subseteq \mu(\eta^*)$. So $[x] \in \mu(\eta^*)$. □

Theorem 3.1. FMP_K holds for $\text{Eq}_\Sigma(\text{KA})$.

Proof:
Let $\alpha, \beta \in REG(\Sigma)$. Assume $\alpha{=}\beta \notin Eq_\Sigma(KA)$. By the Kozen theorem [3], $L(\alpha) \neq L(\beta)$. Accordingly $L(\alpha) - L(\beta) \neq \emptyset$ or $L(\beta) - L(\alpha) \neq \emptyset$. We consider the first case. Let $x \in L(\alpha) - L(\beta)$. By Lemma 3.1, $[x] \in \mu(\alpha) - \mu(\beta)$. Consequently $\mu(\alpha) \neq \mu(\beta)$, whence $\alpha = \beta$ is not true in the finite algebra $\mathcal{P}(\Sigma^*/\sim)$. □

4. FMP_K entails the Kozen theorem

First, we show that α and β are equal as regular expressions if and only if the equality $\alpha = \beta$ is true in all complete action algebras, namely:

$$L(\alpha) = L(\beta) \text{ iff } \models_{CACT} \alpha = \beta$$

We set $a_1 \cdots a_k \equiv \varepsilon$, for $k = 0$, if treated as a string on Σ and $a_1 \cdots a_k \equiv 1$, for $k = 0$, if treated as a term of $\mathcal{L}_\Sigma$.

Lemma 4.1. For all $a_1, \ldots, a_k \in \Sigma$, $k \geq 0$ and for every $\alpha \in REG(\Sigma)$, the following property is true

$$\text{if } a_1 \cdots a_k \in L(\alpha) \text{ then } \models_{KA} a_1 \cdots a_k \leq \alpha \tag{26}$$

Proof:
The proof is by induction on the complexity of the regular expression α.

Case 1. $\alpha \equiv 0$. Then $L(0) = \emptyset$. The right hand side of (26) is false, so the whole conditional is true.

Case 2. $\alpha \equiv a$, $a \in \Sigma$. Since $a_1 \cdots a_k \in L(a)$, we have $k = 1$ and $a_1 = a$. Clearly, $\models_{KA} a \leq a$.

Case 3. $\alpha \equiv \beta + \gamma$. So $L(\beta + \gamma) = L(\beta) \cup L(\gamma)$. Let $a_1 \cdots a_k \in L(\alpha)$. Consider two subcases.

(3.1) $a_1 \cdots a_k \in L(\beta)$. By the induction hypothesis $\models_{KA} a_1 \cdots a_k \leq \beta$. Since $\models_{KA} \beta \leq \beta + \gamma$, then, by transitivity, we have $\models_{KA} a_1 \cdots a_k \leq \beta + \gamma$.

(3.2) $a_1 \cdots a_k \in L(\gamma)$. The proof is symmetric.

Case 4. $\alpha \equiv \beta\gamma$. So $L(\beta\gamma) = L(\beta)L(\gamma)$. Let $a_1 \cdots a_k \in L(\alpha)$. Then, there exist $x \in L(\beta)$, $y \in L(\gamma)$ such that $a_1 \cdots a_k = xy$. By the induction hypothesis $\models_{KA} x \leq \beta$ and $\models_{KA} y \leq \gamma$, hence by (20), $\models_{KA} xy \leq \beta\gamma$. So $\models_{KA} a_1 \cdots a_k \leq \beta\gamma$.

Case 5. $\alpha \equiv \beta^*$. So $L(\alpha) = \bigcup_{n=0}^{\infty} L(\beta)^n$. Let $a_1 \cdots a_k \in L(\alpha)$. There exists $n \geq 0$ such that $a_1 \cdots a_k \in L(\beta)^n$. Divide the string $a_1 \cdots a_k$ into n substrings. Then, there exist $x_1, \ldots, x_n \in L(\beta)$ such that $a_1 \cdots a_k = x_1 \cdots x_n$. If $n = 0$, then $k = 0$, and we have $\models_{KA} 1 \leq \beta^*$. Let $n \neq 0$. By the induction hypothesis $\models_{KA} x_j \leq \beta$ for $j = 1, \ldots, n$. By (20), we have $\models_{KA} a_1 \cdots a_k \leq \beta^n$. Since $\models_{KA} \beta^n \leq \beta^*$, then $\models_{KA} a_1 \cdots a_k \leq \beta^*$. Finally, $\models_{KA} a_1 \cdots a_k \leq \alpha$.

Case 6. $\alpha \equiv 1$. Let $a_1 \cdots a_k \in L(1)$. Then, $k = 0$ and $\models_{KA} 1 \leq 1$. □

Let us introduce some helpful definitions. For $\alpha \in REG(\Sigma)$, define $d(\alpha)$ as follows

$$\begin{aligned} d(0) &= 0 \\ d(a) &= 0 \\ d(\alpha + \beta) &= \max(d(\alpha), d(\beta)) \\ d(\alpha\beta) &= \max(d(\alpha), d(\beta)) \\ d(\alpha^*) &= d(\alpha) + 1 \end{aligned}$$

The number $d(\alpha)$ is called the $*$-*depth* of α.

Let $r(\alpha, n)$ be the number of occurrences of subterms β^* of expression α such that $d(\beta^*) = n$. Clearly,

$$\begin{aligned} r(\alpha + \beta, n) &= r(\alpha, n) + r(\beta, n) \\ r(\alpha\beta, n) &= r(\alpha, n) + r(\beta, n) \\ r(\alpha^*, n) &\geq r(\alpha, n) \end{aligned}$$

We define *simple expressions* (on Σ). $0, 1, a$ ($a \in \Sigma$) and α^* (for any α) are simple expressions; if $\alpha_1, \ldots, \alpha_n$ are simple expressions, then $\alpha_1 \cdots \alpha_n$ is a simple expression.

Fact 4.1. For every regular expression α there exist simple expressions $\beta_1, \ldots \beta_k$ such that $\models_{KA} \alpha = \beta_1 + \cdots + \beta_k$ and, for every $n \geq 1$ and $1 \leq i \leq k$, $r(\alpha, n) \geq (\beta_i, n)$.

Proof:
The proof is by induction on the complexity of the regular expression α. Consider the following cases.

Case 1. $\alpha \equiv 0$ or $\alpha \equiv 1$ or $\alpha \equiv \beta^*$. So α is a simple expression and we assume that $k = 1, \beta_1 \equiv \alpha$.

Case 2. $\alpha \equiv \beta + \gamma$. By the induction hypothesis there exist simple expressions $\beta_1, \ldots, \beta_k$ and $\gamma_1, \ldots, \gamma_l$ such that $\models_{KA} \beta = \beta_1 + \cdots + \beta_k$ and $\models_{KA} \gamma = \gamma_1 + \cdots + \gamma_l$ and $r(\beta, n) \geq r(\beta_i, n)$, for $1 \leq i \leq k$, and $r(\gamma, n) \geq r(\gamma_j, n)$, for $1 \leq j \leq l$. Since $\models_{KA} \beta + \gamma = \beta_1 + \cdots + \beta_k + \gamma_1 + \cdots + \gamma_l$, and

$$r(\beta_i, n) \leq r(\beta, n) \leq r(\beta + \gamma, n), \text{ for every } 1 \leq i \leq k,$$
$$r(\gamma_j, n) \leq r(\gamma, n) \leq r(\beta + \gamma, n), \text{ for every } 1 \leq j \leq l,$$

then we get the thesis.

Case 3. $\alpha \equiv \beta\gamma$. By the induction hypothesis there exist simple expressions $\beta_1, \ldots, \beta_k$ and $\gamma_1, \ldots, \gamma_l$ such that $\models_{KA} \beta = \beta_1 + \cdots + \beta_k$ and $\models_{KA} \gamma = \gamma_1 + \cdots + \gamma_l$ and $r(\beta, n) \geq r(\beta_i, n)$, for $1 \leq i \leq k$, and $r(\gamma, n) \geq r(\gamma_j, n)$, for $1 \leq j \leq l$. Since $\models_{KA} (\beta_1 + \cdots + \beta_k)(\gamma_1 + \cdots + \gamma_l) = (\beta_1\gamma_1 + \cdots + \beta_1\gamma_l) + \cdots + (\beta_k\gamma_1 + \cdots + \beta_k\gamma_l)$, and

$$r(\beta_i\gamma_j, n) = r(\beta_i, n) + r(\gamma_j, n) \leq r(\beta, n) + r(\gamma, n) = r(\beta\gamma, n), \text{ for every } 1 \leq i \leq k \text{ and } 1 \leq j \leq l,$$

then we get the thesis. □

Define $r(\alpha)$ as the number of subterms β^* of expression α such that $d(\beta^*)$ is maximal in α. If α is $*$-free, then $r(\alpha) = 0$. Else $r(\alpha) = r(\alpha, n)$, where n is the biggest number $k \geq 1$ such that $r(\alpha, k) \neq 0$.

Lemma 4.2. $L(\alpha) \subseteq L(\beta)$ iff $\models_{CACT} \alpha \leq \beta$

Proof:
($\Leftarrow$) is obvious, because the algebra of languages is in the class CACT. The proof of ($\Rightarrow$) is by induction on $d(\alpha)$. Let $L(\alpha) \subseteq L(\beta)$. By Fact 4.1 there exist simple expressions $\beta_1, \ldots, \beta_k$ such that $\models_{KA} \alpha = \beta_1 + \cdots + \beta_k$. Hence $L(\alpha) = L(\beta_1) \cup \cdots \cup L(\beta_k)$, so $L(\beta_i) \subseteq L(\beta)$, for every $i = 1, \ldots, k$. We show that $\models_{CACT} \beta_i \leq \beta$. Consider the following cases.

Case 1. $d(\alpha) \equiv 0$. By Fact 4.1 $d(\beta_i) \leq d(\alpha)$, so $d(\beta_i) = 0$. Thus every β_i is $*$-free, so $\beta_i \equiv 0$ or $\beta_i \equiv a_1 \cdots a_k$, for $k \geq 0$. If $\beta_i \equiv 0$, then $\models_{KA} \beta_i \leq \beta$. If $\beta_i \equiv a_1 \cdots a_k$, then by Lemma 4.1 $\models_{KA} \beta_i \leq \beta$. Since $\models_{KA} \beta_i \leq \beta$, for every $1 \leq i \leq k$, so $\models_{KA} \alpha \leq \beta$, and consequently $\models_{CACT} \alpha \leq \beta$.

Case 2. $d(\alpha) \equiv m, m > 0$. We fix $i \in \{1, \ldots, k\}$. By Fact 4.1 $d(\beta_i) \leq d(\alpha)$. If $d(\beta_i) < d(\alpha)$, then we use the induction hypothesis. Let $d(\beta_i) = d(\alpha)$. We switch on the second induction - on $r(\alpha)$ (That means: we prove the thesis for $d(\alpha) = m$ by induction on $r(\alpha)$; actually, we substitute β_i for α). Clearly, $r(\beta_i) \neq 0$. Let $\beta_i = \gamma_1 \cdots \gamma_l$, where γ_i are simple expressions of the form $0, 1, a$ or δ^*. There exists $j \in \{1, \ldots, l\}$ such that $d(\gamma_j) = d(\beta_i) = m$. Clearly, $\gamma_j = \delta^*$ and $d(\beta_i) = d(\delta) + 1$. We have $L(\beta_i) = \bigcup_{n=0}^{\infty} L(\gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l)$ and consequently $L(\gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l) \subseteq L(\beta)$, for all $n \in \omega$. Since either $d(\gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l) < d(\beta_i)$, or $r(\gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l) < r(\beta_i)$, then $\models_{CACT} \gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l \leq \beta$, by the induction hypothesis. By Lemma 2.3, we have $\mu(\gamma_1 \cdots \gamma_{j-1}\delta^*\gamma_{j+1} \cdots \gamma_l) = \sup_{n\in\omega}\{\gamma_1 \cdots \gamma_{j-1}\delta^n\gamma_{j+1} \cdots \gamma_l\}$, in every model $(\mathcal{A}, \mu)$ such that $\mathcal{A}\in$CACT; and consequently $\models_{CACT} \gamma_1 \cdots \gamma_{j-1}\delta^*\gamma_{j+1} \cdots \gamma_l \leq \beta$. Thus $\models_{CACT} \beta_i \leq \beta$, which yields $\models_{CACT} \alpha \leq \beta$, as above. □

Lemma 4.3. $L(\alpha) = L(\beta)$ iff $\models_{CACT} \alpha = \beta$

Proof:
$L(\alpha) = L(\beta)$ iff $L(\alpha) \subseteq L(\beta)$ and $L(\beta) \subseteq L(\alpha)$ iff (by Lemma 4.2) $\models_{CACT} \alpha \leq \beta$ and $\models_{CACT} \beta \leq \alpha$ iff $\models_{CACT} \alpha = \beta$. □

Theorem 4.1. FMP_K entails the Kozen theorem.

Proof:
Let $\alpha, \beta \in REG(\Sigma)$. We show: if $\not\models_{KA} \alpha = \beta$ then $L(\alpha) \neq L(\beta)$. Let $\not\models_{KA} \alpha = \beta$. By FMP_K, there exists a finite Kleene algebra $\mathcal{A}$ such that $\not\models_{\mathcal{A}} \alpha = \beta$. By Lemma 2.2, $\mathcal{A}$ is a complete action algebra. So $\not\models_{CACT} \alpha = \beta$. By Lemma 4.3 $L(\alpha) \neq L(\beta)$. □

References

[1] Buszkowski, W.: On complete action algebras, in: *Volume of Abstracts of 11th International Congress of Logic, Methodology and Philosophy of Science*, Cracow, 1999, 483.

[2] Conway, J.H.: *Regular Algebras and Finite Machines*, Chapman and Hall, London, 1974.

[3] Kozen, D.: A completeness theorem for Kleene algebras and the algebra of regular events, *Information and Computation* 110, 1994, 366-390.

[4] Krob, D.: Complete systems of β-rational identities, *Theoretical Computer Science* 89, 1991, 207-343.

[5] Pratt V.: Action Logic and Pure Induction, in: *Logics in AI* (J. Vav Eijck, Ed.), LNAI 478, Springer, Berlin, 1991, 97-120.