BRICS

Basic Research in Computer Science

BRICS RS-96-36 Aceto et al.: On a Question of A. Salomaa

On a Question of A. Salomaa: The Equational Theory of Regular Expressions over a Singleton Alphabet is not Finitely Based

Luca Aceto
Willem Jan Fokkink
Anna Ingólfsdóttir

BRICS Report Series **RS-96-36**

ISSN 0909-0878 **October 1996**

See back inner page for a list of recent publications in the BRICS Report Series. Copies may be obtained by contacting:

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK - 8000 Aarhus C
Denmark

Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through World Wide Web and anonymous FTP:

`http://www.brics.dk/`
`ftp://ftp.brics.dk/pub/BRICS`

On a Question of A. Salomaa

The Equational Theory of Regular Expressions over a Singleton Alphabet is not Finitely Based

Luca Aceto* Wan Fokkink† Anna Ingólfsdóttir‡

Abstract

Salomaa ((1969) *Theory of Automata*, page 143) asked whether the equational theory of regular expressions over a singleton alphabet has a finite equational base. In this paper, we provide a negative answer to this long standing question. The proof of our main result rests upon a model-theoretic argument. For every finite collection of equations, that are sound in the algebra of regular expressions over a singleton alphabet, we build a model in which some valid regular equation fails. The construction of the model mimics the one used by Conway ((1971) *Regular Algebra and Finite Machines*, page 105) in his proof of a result, originally due to Redko, to the effect that infinitely many equations are needed to axiomatize equality of regular expressions. Our analysis of the model, however, needs to be more refined than the one provided by Conway *ibidem*.

AMS Subject Classification (1991): 08A70, 03C05, 68Q45, 68Q68, 68Q70.
CR Subject Classification (1991): D.3.1, F.1.1, F.4.1.
Keywords and Phrases: Regular expressions, equational logic, complete axiomatizations.

1 Introduction

One of the classic topics in the theory of computation is the study of axiomatic characterizations of the algebra of regular expressions. This field of research has been active since Kleene's original paper [8], where regular expressions were first introduced, and has yielded a collection of very deep and beautiful mathematical results. These we now briefly recall for the sake of historical completeness. (The interested reader is invited to consult, e.g., [17, 6, 13, 10, 9]

*BRICS (Basic Research in Computer Science), Centre of the Danish National Research Foundation, Department of Computer Science, Aalborg University, Fr. Bajersvej 7E, 9220 Aalborg Ø, Denmark. Partially supported by the Human Capital and Mobility project Express. Email: `luca@cs.auc.dk`. Fax: +45 9815 9889.

†Utrecht University, Department of Philosophy, Heidelberglaan 8, 3584 CS Utrecht, The Netherlands. Email: `fokkink@phil.ruu.nl`. Fax: +31 30 253 2816.

‡BRICS (Basic Research in Computer Science), Centre of the Danish National Research Foundation, Department of Computer Science, Aalborg University, Fr. Bajersvej 7E, 9220 Aalborg Ø, Denmark. Email: `annai@cs.auc.dk`. Fax: +45 9815 9889.

for more information on the results that have been obtained within this line of research.)

A theorem of Redko's, whose proof was simplified and corrected by Pilling [6, Chapter 11], gives an infinite, complete system of identities for commutative regular expressions [15]. An infinite equational axiomatization of the theory of regular expressions over a singleton alphabet was given by Redko in [14] (cf. also [6, Chapter 4]). (Variations on the aforementioned results of Redko's that apply to regular expressions over a singleton alphabet with multiplicities over the tropical semiring may be found in [5].) The construction of a complete equational axiomatization for regular expressions over an arbitrary alphabet was addressed by Conway in his seminal monograph [6]. *Ibidem* Conway proposed three conjectures, whose solution would yield the desired complete set of equations. It took many years, and Krob's landmark paper [10], to settle two of these conjectures of Conway's, and to obtain the first complete equational axiom system for the theory of regular expressions. An alternative equational axiomatization for regular expressions, developed within the framework of iteration theories [4], may be found in [3]. Finite implicational proof systems for regular expressions have been developed by, e.g., Salomaa [16, 17] and Kozen [9]. (The interested reader is invited to consult [10, Sect. 15] for a thorough discussion of implicational proof systems for regular languages.)

The research reported in this study was inspired by a reading of [17, Chapter III], where Salomaa gives a text-book presentation of results on the algebra of regular expressions known up until 1969. On page 143 of *op. cit.*, Salomaa asked whether the equational theory of regular expressions over a singleton alphabet, say $\{a\}$, has a finite equational base. In this paper, we provide a negative answer to this long standing question. The proof of our main result rests upon a model-theoretic argument. For every finite collection of equations, that are sound in the algebra of regular expressions over the letter a, we build a model in which some instance of the family of equations

$$\mathrm{C14}.n(a) \quad a^* \quad = \quad (a^n)^*(\mathbf{1} + a + \cdots + a^{n-1}) \quad (n > 0)$$

fails. The construction of the model mimics the one used by Conway [6] in his proof of a result to the effect that infinitely many equations are needed to axiomatize equality of regular expressions over a countably infinite alphabet. (The nonexistence of a finite equational axiomatization for the algebra of regular expressions was originally shown by Redko [14]. Redko's proof-theoretic argument shows that that the equational theory of regular expressions over an alphabet containing at least two letters is not finitely based, cf. Thm. 6.2 in [17].) Our analysis of the model, however, needs to be more refined than the one provided by Conway *ibidem* (cf. the proof of Thm. 3.12).

The paper is organized as follows. We begin by briefly reviewing the syntax and semantics of the language of regular expressions over a singleton alphabet (Sect. 2). There we also introduce the problem addressed in the paper (cf. Thm. 2.3), and outline our solution for it. The remainder of the paper is devoted to the proof of our main technical result (Thm. 2.4). This is presented in Sect. 3, and is articulated as follows. We begin by introducing a notion of weight for regular expressions, and study some its properties (Sect. 3.1). Finally, for every finite set of equations sound in the algebra of regular expressions over the letter a, we show how to build a model in which the equation C14.$p(a)$ fails for some prime number p (Sect. 3.2). This is sufficient to ensure that the equality C14.$p(a)$ cannot be proven from the finite collection of equations under consideration.

2 The Problem

We assume familiarity with the basic notions of regular algebra, and refer the interested reader to, e.g., [6, 13] for more information on the subject.

Let Var be a countably infinite set of variables, not containing the distinguished symbol a, with typical elements x, y, z. We shall use α to range over $\{a\} \cup \mathsf{Var}$. The collection $\mathbb{T}(\mathrm{REG}(a))$ of regular expressions over the alphabet $\{a\} \cup \mathsf{Var}$ is given by the following BNF grammar:

$$P ::= \mathbf{0} \mid \mathbf{1} \mid \alpha \mid P + P \mid P \cdot P \mid P^* \ .$$

The set of closed expressions, i.e., expressions that do not contain occurrences of variables, is denoted by $\mathrm{T}(\mathrm{REG}(a))$. We shall use P, Q, R to range over $\mathbb{T}(\mathrm{REG}(a))$. In writing expressions over the above syntax, we shall always assume that the operator $\cdot$ binds stronger than $+$, and occurrences of $\cdot$ will often be omitted. With these conventions, the expression $PQ + R$ stands for $(P \cdot Q) + R$. We shall use the symbol $\equiv$ to stand for syntactic equality of expressions. The set of variables occurring in an expression P will be written $\mathsf{Var}(P)$, and we shall use $\mathsf{StarVar}(P)$ to stand for the set of variables occurring within the scope of a star in P.

Remark: The constant $\mathbf{1}$ is, in fact, a short-hand for the regular expression $\mathbf{0}^*$. However, its rôle in the algebra of regular expressions is so pervasive that, following [6], we prefer to introduce it explicitly in the syntax.

A (closed) substitution is a mapping from variables to (closed) expressions in the language $\mathbb{T}(\mathrm{REG}(a))$. For every expression P and (closed) substitution σ, the (closed) expression obtained by replacing every occurrence of a variable x in P with the (closed) expression $\sigma(x)$ will be written $P\sigma$. We shall use the notation $[Q/x]$ to denote the substitution mapping the variable x to Q, and acting like the identity on all the other variables.

Definition 2.1 *An expression $P \in \mathbb{T}(\mathrm{REG}(a))$ is* $\aleph$-free *iff it does not contain occurrences of the symbol $\aleph$.*

Notation 2.2 *For $I = \{i_1, \ldots, i_n\}$ a finite index set, we write $\sum_{i\in I} P_i$ for $P_{i_1} + \cdots + P_{i_n}$. By convention, $\sum_{i\in\varnothing} P_i$ stands for* $\mathbf{0}$.

For an expression P and a non-negative integer n, we write

$$P^n \triangleq \underbrace{P \cdot P \cdots P}_{n\text{-times}} \ .$$

By convention, P^0 stands for $\mathbf{1}$.

For a positive integer n, we use $P^{<n}$ as a short-hand for $\mathbf{1} + P + P^2 + \cdots + P^{n-1}$.

Every closed expression $P \in \mathrm{T}(\mathrm{REG}(a))$ denotes a regular language $L(P)$ over the alphabet $\{a\}$. This is defined thus:

$$\begin{array}{rcl} L(\mathbf{0}) & \triangleq & \varnothing \\ L(\mathbf{1}) & \triangleq & \{\lambda\} \\ L(a) & \triangleq & \{a\} \\ L(Q+R) & \triangleq & L(Q) \cup L(R) \\ L(QR) & \triangleq & \{st \mid s \in L(Q), t \in L(R)\} \\ L(Q^*) & \triangleq & \{s_1 \cdots s_n \mid n \geq 0, s_i \in L(Q) \ \ (1 \leq i \leq n)\} \end{array}$$

where λ stands for the empty string, and st denotes the string obtained by concatenating s and t.

The algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$ of closed regular expressions modulo language equivalence is constructed in standard fashion. That is, for $P, Q \in \mathbb{T}(\mathrm{REG}(a))$,

$$\begin{array}{l} \mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P = Q \ \ \Leftrightarrow \\ \qquad \text{(for all closed substitutions } \sigma : L(P\sigma) = L(Q\sigma)) \ . \end{array}$$

Each of these algebras has, in fact, the structure of an ordered algebra, in the sense of [2], and, for $P, Q \in \mathbb{T}(\mathrm{REG}(a))$,

$$\begin{array}{l} \mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q \ \ \Leftrightarrow \\ \qquad \text{(for all closed substitutions } \sigma : L(P\sigma) \subseteq L(Q\sigma)) \ . \end{array}$$

In both cases, we say that the relevant (in)equation is *valid*, or *sound*. The collection of equations that are valid in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$ will be denoted by $\mathcal{E}$. We shall use $\mathcal{V}$ (respectively $\mathcal{S}$) to stand for the equations in $\mathcal{E}$ that relate closed (resp. a-free) expressions. Examples of equations in the theory $\mathcal{S}$ are those in Table 1, called the *classical axioms* by Conway [6, page 25], and the laws

$$\begin{array}{rcl} xy & = & yx \\ (x+y)^* & = & x^* y^* \ . \end{array}$$

Unlike the classical axioms, the laws above only hold under the assumption that the alphabet is a singleton.

The following identity is an easy consequence of the classical axioms:

$$\mathbf{0}^* \ = \ \mathbf{1} \ . \tag{1}$$

An example of an equation that is contained in $\mathcal{E}$, but not in $\mathcal{S}$, is

$$a^* + x \ = \ a^* \ .$$

Again, the soundness of the above law depends upon the assumption that the alphabet contains only the letter a.

C1	$x+\mathbf{0}$	$=$	x	C8	$x(y+z)$	$=$	$xy+xz$	
C2	$x+y$	$=$	$y+x$	C9	$(x+y)z$	$=$	$xz+yz$	
C3	$(x+y)+z$	$=$	$x+(y+z)$	C10	$(xy)z$	$=$	$x(yz)$	
C4	$x\mathbf{0}$	$=$	$\mathbf{0}$	C11	$(x+y)^*$	$=$	$(x^*y)^*x^*$	
C5	$\mathbf{0}x$	$=$	$\mathbf{0}$	C12	$(xy)^*$	$=$	$\mathbf{1}+x(yx)^*y$	
C6	$x\mathbf{1}$	$=$	x	C13	$(x^*)^*$	$=$	x^*	
C7	$\mathbf{1}x$	$=$	x	C14.n	x^*	$=$	$(x^n)^*x^{<n}$	$(n>0)$

Table 1: The classical axioms

Remark: As witnessed by the equation $a^*+x=a^*$, the soundness of an identity $P=Q$ in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$ entails neither that P and Q contain the same variables, nor that $\mathsf{StarVar}(P)$ coincides with $\mathsf{StarVar}(Q)$.

In [17, page 143] Salomaa asked whether the equational theories $\mathcal{V}$ and $\mathcal{S}$ are finitely based, i.e., whether there exists a finite subset of $\mathcal{E}$ which proves all the equations in those sets. As communicated to us by Salomaa [18], this problem has been open since 1969, the year of publication of [17]. In the remainder of this paper, we shall provide a negative answer to the aforementioned question of Salomaa.

The main contribution of this study is summarized in the following negative result.

Theorem 2.3 *The equational theories $\mathcal{E}$, $\mathcal{V}$ and $\mathcal{S}$ do not have a finite base, i.e., no finite subset of $\mathcal{E}$ can prove all of the equations in any of the aforementioned theories.*

In order to prove this theorem, we shall show that no finite collection of equations in $\mathcal{E}$ can prove all the instances of the equation schema

$$\mathrm{C14}.n(a) \qquad a^* \;=\; (a^n)^*a^{<n} \quad (n>0)\ .$$

This is the import of the following result.

Theorem 2.4 *For every finite set of equations in $\mathcal{E}$, there is a prime number p such that the equality* C14.$p(a)$ *is not provable from the equations in that set.*

Using Thm. 2.4, it is a simple matter to prove Thm. 2.3.

Proof of Thm. 2.3: We prove, first of all, that the equational theories $\mathcal{V}$ and $\mathcal{E}$ are not finitely based. To this end, let $\mathcal{E}_F$ be a finite subset of $\mathcal{E}$. By Thm. 2.4, there exists a prime number p such that the equality C14.$p(a)$ is not provable from the equations in $\mathcal{E}_F$. As C14.$p(a)$ is contained in the set $\mathcal{V}$—and, *a fortiori*, in $\mathcal{E}$—, it follows that $\mathcal{E}_F$ is neither a base for $\mathcal{V}$ nor for $\mathcal{E}$. Hence the equational theories $\mathcal{V}$ and $\mathcal{E}$ do not have a finite base.

To see that the theory $\mathcal{S}$ has no finite base either, assume, towards a contradiction, that $\mathcal{E}_F$ is a finite base for it. In particular, the axiom system $\mathcal{E}_F$ proves all of the equations C14.n in Table 1. Instantiating these equations, we derive that $\mathcal{E}_F$ proves all of the equalities C14.$n(a)$. However, this contradicts Thm. 2.4. □

In light of the above discussion, all we need to do to prove Thm. 2.3 is to show Thm. 2.4. The remainder of the paper will be devoted to a proof of this result.

3 A proof of Thm. 2.4

The proof of Thm. 2.4 we now proceed to present is based on an adaptation of a beautiful argument due to Conway (cf. [6, Thm. 2, page 105]). In *op. cit.*, Conway offers two proofs of a theorem, originally due to Redko [14], to the effect that equality of regular expressions cannot be axiomatized using a finite number of equations. The argument we present below is inspired by the second of those proofs (cf. [6, Pages 105–107]), and is model-theoretic in nature. In order to show Thm. 2.4, for every finite set of equations that are valid in $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$ we shall build a model that does not satisfy all of the instances of $\mathrm{C14}.n(a)$. The construction of the model relies on the use of prime numbers, as do related arguments presented in, e.g., [1, 6, 7, 11, 19, 20].

The proof of Thm. 2.4 will be delivered in two steps. We begin by studying a notion of weight for the expressions in the language $\mathbb{T}(\mathrm{REG}(a))$ that will be useful in the proof of this result (Sect. 3.1). Finally, for every finite set of equations in $\mathcal{E}$, we show how to build a model in which the equation $\mathrm{C14}.p(a)$ fails for some prime number p larger than the weight of every expression mentioned in the axiom system $\mathcal{E}$ (Sect. 3.2). This is sufficient to ensure that the equality $\mathrm{C14}.p(a)$ cannot be proven from the equations under consideration.

3.1 Weight of a Regular Expression

The length of an expression P is inductively defined thus:

$$\begin{array}{rcl} \mathrm{length}(\mathbf{0}) & \triangleq & 0 \\ \mathrm{length}(\mathbf{1}) & \triangleq & 1 \\ \mathrm{length}(\alpha) & \triangleq & 1 \\ \mathrm{length}(P+Q) & \triangleq & \mathrm{length}(P)+\mathrm{length}(Q) \\ \mathrm{length}(PQ) & \triangleq & \mathrm{length}(P)\mathrm{length}(Q) \\ \mathrm{length}(P^*) & \triangleq & 1\ . \end{array}$$

Note that the length of a regular expression that is simultaneously **0**-free and +-free is 1.

Definition 3.1 *For an expression P, we use* $\mathrm{vars}(P)$ *to denote the total number of occurrences of variables in P, and* $\mathrm{weight}(P)$, *the* weight *of the expression P, to stand for* $2^{\mathrm{vars}(P)}\mathrm{length}(P)$.

Example: For every positive integer n, the expression $(a^n)^*a^{<n}$ has length, and weight, n. □

The following properties of the length and weight of regular expressions will find application in the technical developments to follow (cf. the proof of Thm. 3.12).

Lemma 3.2 *Let N denote the number of occurrences of the variable x in the expression Q.*

1. *Let $[(a+a^2)/x]$ denote the substitution mapping x to $a+a^2$, and acting like the identity on all the other variables. Then the length of $Q[(a+a^2)/x]$ is at most 2^N times the length of Q.*

2. *If $N > 0$ and R is a closed $+$-free expression, then the weight of $Q[R/x]$ is strictly smaller than the weight of Q.*

Proof: Statement 1 follows by a straightforward induction on the structure of Q. Statement 2 is an immediate consequence of the fact that, as R is closed and $+$-free, the length of Q is equal to that of $Q[R/x]$, but $\mathrm{vars}(Q[R/x])$ is strictly smaller than $\mathrm{vars}(Q)$. $\square$

The crux of our proof of Thm. 2.4 is the construction, for every prime number p, of an ordered algebra $\mathcal{M}_p$ over the signature of the language $\mathbb{T}(\mathrm{REG}(a))$ with the following properties:

P1 For every positive integer n, the equation C14.$n(a)$ fails in $\mathcal{M}_p$ iff p divides n.

P2 Every inequation $P \leq Q$, that is sound in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, where Q is an expression whose weight is smaller than p, is valid in $\mathcal{M}_p$.

In fact, if we can construct the algebras $\mathcal{M}_p$ satisfying the above properties, then Thm. 2.4 follows thus:

Proof of Thm. 2.4: Let $\mathcal{E}_F = \{P_i = Q_i \mid i \in I\}$ be a finite subset of $\mathcal{E}$. Let m be the supremum of the weights of the expressions P_i and Q_i ($i \in I$). Choose p as the least prime number greater than m. Then the equations in $\mathcal{E}_F$ and all the instances of C14.$n(a)$ for n not divisible by p are valid in the algebra $\mathcal{M}_p$ (properties P1 and P2). Moreover, the equation C14.$p(a)$ fails in $\mathcal{M}_p$ (property P1). As $\mathcal{M}_p$ is a model of the axiom system $\mathcal{E}_F \cup \{\mathrm{C14}.n(a) \mid n \bmod p \neq 0\}$ in which C14.$p(a)$ fails, it follows that C14.$p(a)$ is not provable from $\mathcal{E}_F \cup \{\mathrm{C14}.n(a) \mid n \bmod p \neq 0\}$. $\square$

In light of the previous discussion, in order to complete the proof of Thm. 2.4, we are left to construct, for every prime number p, an ordered algebra $\mathcal{M}_p$ having the properties P1 and P2 stated above.

3.2 The Algebra $\mathcal{M}_p$

We shall now proceed to build, for every prime number p, an ordered algebra $\mathcal{M}_p$ with the aforementioned properties. The construction we present mimics the one used by Conway in his proof of the non-finite axiomatizability of the theory of regular languages (cf. [6, pp. 105–107]).

Notation 3.3 *In what follows, we shall write ω for the set of natural numbers (with zero), and $[n]$ will stand for the set $\{0, 1, \ldots, n-1\}$.*

The carrier M_p of the algebra $\mathcal{M}_p$ is defined as follows:

- every subset of $[p]$ is in M_p;
- the set of natural numbers ω is in M_p.

The elements of M_p will be partially ordered by set inclusion.

Definition 3.4 *Let p and q be integers. If a positive integer m divides the difference $p - q$, we say that p is congruent to q modulo m and write $p \equiv q \pmod{m}$.*

For every integer p, the unique $q \in [m]$ such that $p \equiv q \pmod{m}$ will be written $p \bmod m$.

Let I and J be sets of integers. We define

$$(I + J) \bmod m \quad \triangleq \quad \{(i + j) \bmod p \mid i \in I, j \in J\} \ .$$

In order to give the set M_p enough structure to serve as a suitable semantic domain for the language $\mathbb{T}(\mathrm{REG}(a))$, we need to define the semantic counterparts of the operations in its signature over it. To this end, we map the constants $\mathbf{0}$, $\mathbf{1}$ and a to the sets $\varnothing$, $\{0\}$ and $\{1\}$, respectively, and stipulate that the semantic counterparts of the other operations are given by the equations in Table 2, where we use the meta-variables e and e' to range over the set M_p. Note that the operations in the algebra $\mathcal{M}_p$ are monotonic with respect to set inclusion. Therefore we have given $\mathcal{M}_p$ the structure of an ordered algebra over the signature of the language $\mathbb{T}(\mathrm{REG}(a))$, in the sense of [2].

SUM	$e + e'$	$=$	$e \cup e'$
COMP	$e \cdot e'$	$=$	$\begin{cases} \omega & \text{if } e = \omega \text{ and } e' \neq \varnothing \\ \omega & \text{if } e \neq \varnothing \text{ and } e' = \omega \\ (e + e') \bmod p & \text{otherwise} \end{cases}$
STAR	e^*	$=$	$\begin{cases} \{0\} & \text{if } e = \varnothing \text{ or } e = \{0\} \\ \omega & \text{otherwise} \end{cases}$

Table 2: The operations of the algebra $\mathcal{M}_p$

An M_p-*environment* is a mapping ρ from variables to the set M_p. For an expression P and an M_p-environment ρ, we shall use $\mathcal{M}_p[\![P]\!]\rho$ to denote the element of M_p that is associated with the expression P by the unique homomorphic extension of ρ to $\mathbb{T}(\mathrm{REG}(a))$. If P is a closed expression, then $\mathcal{M}_p[\![P]\!]\rho$ is independent of the environment ρ. In that case, we shall simply write $\mathcal{M}_p[\![P]\!]$ for the denotation of P in the algebra $\mathcal{M}_p$. It is not hard to see that the equations C1–13 in Table 1 are sound in the algebra $\mathcal{M}_p$.

We now proceed to show that the algebra $\mathcal{M}_p$ meets the requirements P1 and P2 that we set out to achieve. To this end, note, first of all, that the equation C14.$n(a)$ fails in $\mathcal{M}_p$ if n is a multiple of p. In fact, in that case,

$$\mathcal{M}_p[\![a^*]\!] = \omega \not\subseteq [p] = \mathcal{M}_p[\![(a^n)^* a^{<n}]\!] \ .$$

On the other hand, if p does not divide n then the equation C14.$n(a)$ is valid in $\mathcal{M}_p$. This follows because

$$\mathcal{M}_p[\![a^*]\!] = \omega = (\{n \bmod p\})^* \mathcal{M}_p[\![a^{<n}]\!] = \mathcal{M}_p[\![a^n]\!]^* \mathcal{M}_p[\![a^{<n}]\!] = \mathcal{M}_p[\![(a^n)^* a^{<n}]\!]$$

where the second equality from the left holds because of the assumption that n is not divisible by p.

In light of the above discussion, it follows that the ordered algebra $\mathcal{M}_p$ satisfies the requirement P1 set out on page 7. We shall now proceed to show that requirement P2 is also met by $\mathcal{M}_p$, i.e., that every inequation $P \leq Q$, with Q an expression of weight *smaller* than p, which is sound in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, is valid in $\mathcal{M}_p$.

As a stepping stone towards the proof of the fact that $\mathcal{M}_p$ meets requirement P2, we shall now argue that the failure of the equation C14.$p(a)$ in the algebra $\mathcal{M}_p$ is paradigmatic. In fact, if $P \leq Q$ is an inequation that is sound in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, and ρ is an M_p-environment such that $\mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho$, then it must be the case that $\mathcal{M}_p[\![P]\!]\rho = \omega$ and $\mathcal{M}_p[\![Q]\!]\rho = [p]$ (cf. Lem. 3.8(2)). This implies that the algebra $\mathcal{M}_p$ is indeed very close to being a model for the equational theory $\mathcal{E}$. All that we should need to do to turn $\mathcal{M}_p$ into such a model is to identify the elements ω and $[p]$.

The following classic result on the solution of congruence equations (cf., e.g., [12, Corollary 2.9]) will find application in the proof of Lem. 3.7(1) to follow.

Theorem 3.5 *Let p, q, r be integers with p and q relatively prime, i.e. with 1 as their greatest common divisor, and with $q \neq 0$. Then the equation*

$$px \equiv r \pmod{q}$$

in the unknown x has an integer solution x_1. All solutions are given by $x = x_1 + jq$, where $j = 0, \pm 1, \pm 2, \ldots$.

Notation 3.6 *For an M_p-environment ρ, let $\bar{\rho} : \mathsf{Var} \to \mathrm{T}(\mathrm{REG}(a))$ denote the closed substitution which is defined by*

$$\begin{array}{lcll} \bar{\rho}(x) & \triangleq & \sum_{i \in I} a^i & \text{if } \rho(x) = I \subseteq [p] \\ \bar{\rho}(x) & \triangleq & a^* & \text{if } \rho(x) = \omega \ . \end{array}$$

We are now in a position to establish two technical lemmas (Lem. 3.7 and Lem. 3.8). Both these results consist of two statements, the first of which is only used in the proof of the second, and may be skipped on first reading.

Lemma 3.7

1. *Let $Q \in \mathrm{T}(\mathrm{REG}(a))$. Suppose that p is a prime number and $i \in [p]$. If there exist a non-negative integer m and $j \in \{1, \ldots, p-1\}$ such that $a^{mp+j} \in L(Q)$, then $a^{np+i} \in L(Q^*)$ for some non-negative integer n.*

2. *Let $P \in \mathbb{T}(\mathrm{REG}(a))$ and let ρ be an M_p-environment. Suppose that p is a prime number. Then, for every $i \in [p]$, $i \in \mathcal{M}_p[\![P]\!]\rho$ iff $a^{np+i} \in L(P\bar{\rho})$ for some non-negative integer n.*

Proof: We prove the two statements separately.

1. Let $Q \in \mathrm{T}(\mathrm{REG}(a))$. Assume that p is a prime number, and that $i \in [p]$. Suppose, moreover, that there exist a non-negative integer m and $j \in \{1, \ldots, p-1\}$ such that $a^{mp+j} \in L(Q)$. We shall prove that a^{np+i} is contained in $L(Q^*)$ for some non-negative integer n.

   As $a^{mp+j} \in L(Q)$, the string $a^{k(mp+j)}$ is in the language denoted by Q^*, for every non-negative integer k. We shall now argue that it is possible to choose k in such a way that, for some non-negative integer n,

   $$k(mp + j) = np + i \ .$$

   To this end, note that such a k can be found iff the congruence equation in the unknown k

   $$jk \equiv i \pmod p$$

   has a non-negative solution. This is an immediate consequence of Thm. 3.5, because j and p are relatively prime.

2. Let $P \in \mathbb{T}(\mathrm{REG}(a))$, and let p be a prime number. Assume that $i \in [p]$. We prove the statement by induction on the structure of P, and proceed by a case analysis on the form P may take.

   - Case: $P \equiv \mathbf{0}$.
     In this case, $\mathcal{M}_p[\![P]\!]\rho$ and $L(P\bar{\rho})$ are both empty. The claim is thus vacuously true.
   - Case: $P \equiv \mathbf{1}$.
     In this case, $i \in \mathcal{M}_p[\![P]\!]\rho$ holds only for $i = 0$, because $\mathcal{M}_p[\![P]\!]\rho = \{0\}$. Moreover, as $P\bar{\rho} \equiv \mathbf{1}$, the only string in $L(P\bar{\rho})$ is λ.
   - Case: $P \equiv a$.
     In this case, $i \in \mathcal{M}_p[\![P]\!]\rho$ holds only for $i = 1$, because $\mathcal{M}_p[\![P]\!]\rho = \{1\}$. Moreover, as $P\bar{\rho} \equiv a$, the only string in $L(P\bar{\rho})$ is a.
   - Case: $P \equiv x$.
     In this case, $\mathcal{M}_p[\![P]\!]\rho = \rho(x)$ and $P\bar{\rho} = \bar{\rho}(x)$. It follows easily from the definition of $\bar{\rho}$ that $i \in \rho(x)$ iff $a^i \in L(\bar{\rho}(x))$.
   - Case: $P \equiv Q + R$.
     In this case, $\mathcal{M}_p[\![P]\!]\rho = \mathcal{M}_p[\![Q]\!]\rho \cup \mathcal{M}_p[\![R]\!]\rho$. So $i \in \mathcal{M}_p[\![P]\!]\rho$ iff either $i \in \mathcal{M}_p[\![Q]\!]\rho$ or $i \in \mathcal{M}_p[\![R]\!]\rho$. By induction, this is the case iff either $L(Q\bar{\rho})$ or $L(R\bar{\rho})$ contains a string of the form a^{np+i} for some non-negative integer n. Finally, this holds iff the language denoted by $P\bar{\rho} \equiv Q\bar{\rho} + R\bar{\rho}$ contains a string of the form a^{np+i}.
   - Case: $P \equiv QR$.
     As $\mathcal{M}_p[\![P]\!]\rho = \mathcal{M}_p[\![Q]\!]\rho \cdot \mathcal{M}_p[\![R]\!]\rho$, it is not hard to see that $i \in \mathcal{M}_p[\![P]\!]\rho$ iff $j \in \mathcal{M}_p[\![Q]\!]\rho$ and $k \in \mathcal{M}_p[\![R]\!]\rho$, for some $j, k \in [p]$ with $(j + k) \bmod p = i$. By induction, this holds iff $L(Q\bar{\rho})$ and $L(R\bar{\rho})$ contain strings of the form a^{lp+j} and a^{mp+k} for non-negative integers l and m, respectively. Finally, as $(j + k) \bmod p = i$, this is the case iff the language denoted by $P\bar{\rho} \equiv (Q\bar{\rho})(R\bar{\rho})$ contains a string of the form a^{np+i} for some non-negative integer n.
   - Case: $P \equiv Q^*$.
     As $\mathcal{M}_p[\![P]\!]\rho = (\mathcal{M}_p[\![Q]\!]\rho)^*$, it is not hard to see that $i \in \mathcal{M}_p[\![P]\!]\rho$ iff either $j \in \mathcal{M}_p[\![Q]\!]\rho$ for some $j \in \{1, ..., p-1\}$ or $i = 0$. We shall now prove that the language denoted by $P\bar{\rho} \equiv (Q\bar{\rho})^*$ contains a string of the form a^{np+i} for some non-negative integer n iff either $j \in \mathcal{M}_p[\![Q]\!]\rho$ for some $j \in \{1, ..., p-1\}$ or $i = 0$. We establish the two implications separately.

- 'ONLY IF IMPLICATION'. Assume that the language denoted by $P\bar{\rho} \equiv (Q\bar{\rho})^*$ contains the string a^{np+i} for some non-negative integer n and $i \neq 0$. We show that $j \in \mathcal{M}_p[\![Q]\!]\rho$ for some $j \in \{1, ..., p-1\}$.
  As $i \neq 0$, by the definition of $L((Q\bar{\rho})^*)$, there exists a string in the language denoted by $Q\bar{\rho}$ whose length is not a multiple of p. This string is of the form a^{lp+j} for some non-negative integer l and $j \in \{1, ..., p-1\}$. The inductive hypothesis now yields that $j \in \mathcal{M}_p[\![Q]\!]\rho$, and we are done.
- 'IF IMPLICATION'. Assume that $j \in \mathcal{M}_p[\![Q]\!]\rho$ for some $j \in \{1, ..., p-1\}$ or $i = 0$. We shall prove that the language denoted by $P\bar{\rho} \equiv (Q\bar{\rho})^*$ contains a string of the form a^{np+i} for some non-negative integer n. The statement is trivial if $i = 0$, because $\lambda \in L(P\bar{\rho})$.
  Assume therefore that $j \in \mathcal{M}_p[\![Q]\!]\rho$ for some $j \in \{1, ..., p-1\}$. By induction, this holds iff $L(Q\bar{\rho})$ contains a string of the form a^{lp+j} for some non-negative integer l. Finally, by statement 1 of the lemma this implies that the language denoted by $P\bar{\rho} \equiv (Q\bar{\rho})^*$ contains a string of the form a^{np+i} for some non-negative integer n.

This completes the inductive argument for statement 2.

The proof of the lemma is now complete. □

The main use of the above technical result will be in the proof of the following lemma, which will be used repeatedly in the proof of Thm. 3.12 to follow.

Lemma 3.8 *Let $P, Q \in \mathbb{T}(\mathrm{REG}(a))$ and let ρ be an M_p-environment. Suppose that $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q$. Then:*

1. *If $\mathcal{M}_p[\![P]\!]\rho = \omega$, then either $\mathcal{M}_p[\![Q]\!]\rho = \omega$ or $\mathcal{M}_p[\![Q]\!]\rho = [p]$.*
2. *If $\mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho$, then $\mathcal{M}_p[\![P]\!]\rho = \omega$ and $\mathcal{M}_p[\![Q]\!]\rho = [p]$.*

Proof: Suppose that $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q$. We prove the two statements of the lemma separately.

1. As $\mathcal{M}_p[\![P]\!]\rho = \omega$, it follows that $L(P\bar{\rho})$ contains strings of the form a^{n_ip+i} for each $i \in [p]$ (Lem. 3.7(2)). Since $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q$, the language denoted by $P\bar{\rho}$ is included in that denoted by $Q\bar{\rho}$. Therefore $L(Q\bar{\rho})$ contains each of the strings a^{n_ip+i} ($i \in [p]$). Again using Lem. 3.7(2), we obtain that $i \in \mathcal{M}_p[\![Q]\!]\rho$ for every $i \in [p]$. Hence, either $\mathcal{M}_p[\![Q]\!]\rho = \omega$ or $\mathcal{M}_p[\![Q]\!]\rho = [p]$.
2. Suppose that the M_p-environment ρ is such that $\mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho$. We shall show that $\mathcal{M}_p[\![P]\!]\rho = \omega$ and $\mathcal{M}_p[\![Q]\!]\rho = [p]$.
   We begin by proving that $\mathcal{M}_p[\![P]\!]\rho = \omega$. To this end, assume, towards a contradiction, that $\mathcal{M}_p[\![P]\!]\rho = I$ for some $I \subseteq [p]$. According to Lem. 3.7(2), the language denoted by $P\bar{\rho}$ has a string of the form a^{n_ip+i} for each $i \in I$. Since $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q$, the language $L(Q\bar{\rho})$ also contains a string of the form a^{n_ip+i} for each $i \in I$. By Lem. 3.7(2) it follows that $i \in \mathcal{M}_p[\![Q]\!]\rho$ for each $i \in I$. Hence, $\mathcal{M}_p[\![P]\!]\rho \subseteq \mathcal{M}_p[\![Q]\!]\rho$, which contradicts one of the assumptions of the statement.
   Thus $\mathcal{M}_p[\![P]\!]\rho = \omega$ must hold. Since $\mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho$, it follows that $\mathcal{M}_p[\![Q]\!]\rho \neq \omega$. Hence, statement 1 of the lemma yields $\mathcal{M}_p[\![Q]\!]\rho = [p]$.

The proof of the lemma is now complete. □

Definition 3.9

- *We say that an expression* $P \in \mathbb{T}(\mathrm{REG}(a))$ *is* $\mathbf{0}$-reduced *iff it is either* $\mathbf{0}$ *or* $\mathbf{0}$*-free.*
- *Let* X *be a set of variables in* Var*. An* M_p*-environment* ρ *is* non-empty over X *iff* $\rho(x)$ *is non-empty for every variable* $x \in X$*.*

Fact 3.10

1. *Every* $P \in \mathbb{T}(\mathrm{REG}(a))$ *may be proven equal to a* $\mathbf{0}$*-reduced expression, whose weight is at most that of* P*, using axioms C1–2, C4–5 in Table 1 and the derived law (1).*
2. *If* $P \in \mathbb{T}(\mathrm{REG}(a))$ *is* $\mathbf{0}$*-free and the* M_p*-environment* ρ *is non-empty over* $\mathsf{Var}(P)$*, then* $\mathcal{M}_p[\![P]\!]\rho \neq \emptyset$*.*

In the proof of the fact that the algebra $\mathcal{M}_p$ satisfies requirement P2 on page 7, we shall make use of some properties of the semantic mapping $\mathcal{M}_p[\![\cdot]\!]$. For ease of reference, these are collected in the following lemma.

Lemma 3.11 *Let* $P \in \mathbb{T}(\mathrm{REG}(a))$ *be* $\mathbf{0}$*-free, and let* ρ *be an* M_p*-environment that is non-empty over* $\mathsf{Var}(P)$*. Then the following statements hold:*

1. *If* $\rho(x) = \omega$ *for some variable* x *contained in* $\mathsf{Var}(P)$*, then* $\mathcal{M}_p[\![P]\!]\rho = \omega$*.*
2. *If* $\mathcal{M}_p[\![P]\!]\rho = \{i\}$ *for some* $i \in [p]$*, then* $\rho(x)$ *is a singleton for every variable* x *contained in* $\mathsf{Var}(P)$*.*
3. *Assume that* $\mathcal{M}_p[\![P]\!]\rho \neq \omega$*, and that* ρ *maps every variable occurring in* P *to a singleton. Then the length of* P *is greater than, or equal to, the cardinality of* $\mathcal{M}_p[\![P]\!]\rho$*.*
4. *If* $\mathcal{M}_p[\![P]\!]\rho \neq \omega$*, then* $\rho(x)$ *is a singleton for every variable* x *contained in* $\mathsf{StarVar}(P)$*.*
5. *Assume that* $\mathcal{M}_p[\![P]\!]\rho = \omega$*, that* ρ' *is non-empty over* $\mathsf{Var}(P)$ *and coincides with* ρ *over* $\mathsf{StarVar}(P)$*, and that if* $\rho(x) = \omega$ *for an* $x \in \mathsf{Var}(P)$*, then* $\rho'(x) = \omega$*. Then* $\mathcal{M}_p[\![P]\!]\rho' = \omega$*.*
6. *Assume that* $\mathcal{M}_p[\![P]\!]\rho \neq \omega$*, that* ρ' *coincides with* ρ *over* $\mathsf{StarVar}(P)$*, and that* $\rho'(x) \neq \omega$ *for* $x \in \mathsf{Var}(P)$*. Then* $\mathcal{M}_p[\![P]\!]\rho' \neq \omega$*.*

Proof: All the statements can be shown by induction on the structure of the expression P. The details are left to the reader. Here we only remark that the proof for statement 4 uses statement 2 to deal with the case in which P has the form Q^* for some expression Q. In fact, if P has that form and $\mathcal{M}_p[\![P]\!]\rho \neq \omega$, then, by axiom STAR in Table 2, $\mathcal{M}_p[\![Q]\!]\rho$ is included in $\{0\}$. Since Q is $\mathbf{0}$-free and ρ is non-empty over $\mathsf{Var}(Q)$, Fact 3.10(2) yields that $\mathcal{M}_p[\![Q]\!]\rho = \{0\}$. Statement 2 then gives that ρ maps each variable in Q to a singleton. □

Remark: Statement 6 in the above lemma does, in fact, hold for arbitrary expressions P and M_p-environments ρ. However, in what follows, we shall only use it in the restricted form presented above. The provisos of statements 1–5 are instead necessary for their validity.

We are finally in a position to prove that the algebra $\mathcal{M}_p$ satisfies all the inequations $P \leq Q \in \mathcal{E}$, with Q an expression of weight smaller than p. This implies that the algebra $\mathcal{M}_p$ does indeed meet requirement P2.

Theorem 3.12 *If* $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a))) \models P \leq Q$ *and* $\mathrm{weight}(Q)$ *is smaller than* p*, then* $\mathcal{M}_p \models P \leq Q$*.*

Proof: Let $P \leq Q$ be an inequation that is sound in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, but fails in $\mathcal{M}_p$. We shall show that Q must have weight at least p.

Let the weight of an inequation $P \leq Q$ be the sum of the weigths of the expressions P and Q. Assume that $P \leq Q$ is an inequation of minimum weight that is sound in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, but not in $\mathcal{M}_p$. Without loss of generality, we may assume that the expressions P and Q are $\mathbf{0}$-reduced (Fact 3.10(1)), and, in fact, $\mathbf{0}$-free. Since the inequation $P \leq Q$ fails in $\mathcal{M}_p$, there exists an M_p-environment ρ such that

$$\mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho \ .$$

For later use in the proof, we argue, first of all, that ρ must be non-empty over $\mathsf{Var}(P) \cup \mathsf{Var}(Q)$. In fact, assume, towards a contradiction, that there is a variable x occurring in P or Q such that $\rho(x) = \varnothing$. Then,

$$\mathcal{M}_p[\![P[\mathbf{0}/x]]\!]\rho = \mathcal{M}_p[\![P]\!]\rho \not\subseteq \mathcal{M}_p[\![Q]\!]\rho = \mathcal{M}_p[\![Q[\mathbf{0}/x]]\!]\rho \ .$$

This implies that the inequation

$$P[\mathbf{0}/x] \quad \leq \quad Q[\mathbf{0}/x]$$

fails in $\mathcal{M}_p$. As the above inequation is valid in the algebra $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$, this contradicts our assumption that the inequation $P \leq Q$ had minimum weight amongst those valid in $\mathsf{Alg}(\mathrm{T}(\mathrm{REG}(a)))$ that fail in $\mathcal{M}_p$ (Lem. 3.2(2), as x occurs in either P or Q).

We can now proceed to argue that Q must have weight at least p. As the inequation $P \leq Q$ fails in $\mathcal{M}_p$ for the M_p-environment ρ, Lem. 3.8(2) yields that

$$\mathcal{M}_p[\![P]\!]\rho = \omega \not\subseteq [p] = \mathcal{M}_p[\![Q]\!]\rho \ .$$

As $\mathcal{M}_p[\![Q]\!]\rho \neq \omega$, Q is $\mathbf{0}$-free and ρ is non-empty over $\mathsf{Var}(Q)$, it follows that ρ maps no variable in Q to ω (Lem. 3.11(1)), and that ρ maps every variable in $\mathsf{StarVar}(Q)$ to a singleton set (Lem. 3.11(4)). We now proceed with the proof by distinguishing two cases, depending on whether $\mathsf{StarVar}(P)$ is included in $\mathsf{StarVar}(Q)$ or not.

- Case: $\mathsf{StarVar}(P) \subseteq \mathsf{StarVar}(Q)$.

  Consider the M_p-environment ρ' that is defined as follows:

$$\begin{array}{rcll} \rho'(x) & \triangleq & \rho(x) & \text{if } x \in \mathsf{StarVar}(Q) \\ \rho'(x) & \triangleq & \rho(x) & \text{if } \rho(x) = \omega \\ \rho'(x) & \triangleq & \{0\} & \text{otherwise} \ . \end{array}$$

  Since ρ maps no variable in Q to ω and is non-empty over $\mathsf{Var}(P) \cup \mathsf{Var}(Q)$, the same holds for ρ'. Hence, Lem. 3.11(6) gives that $\mathcal{M}_p[\![Q]\!]\rho' \neq \omega$. Furthermore, since $\mathsf{StarVar}(P)$ is included in $\mathsf{StarVar}(Q)$, ρ' coincides with ρ over $\mathsf{StarVar}(P)$. By construction, if $\rho(x) = \omega$ then $\rho'(x) = \omega$. So, by Lem. 3.11(5), we may infer that $\mathcal{M}_p[\![P]\!]\rho' = \omega$. As the inequation $P \leq Q$ fails in $\mathcal{M}_p$ for the M_p-environment ρ', Lem. 3.8(2) yields that

$$\mathcal{M}_p[\![P]\!]\rho' = \omega \not\subseteq [p] = \mathcal{M}_p[\![Q]\!]\rho' \ .$$

As ρ' maps each variable in Q to a singleton set, Lem. 3.11(3) now gives that $p \leq \mathrm{length}(Q) \leq \mathrm{weight}(Q)$, which was to be shown.

- CASE: $\mathsf{StarVar}(P) \not\subseteq \mathsf{StarVar}(Q)$.

  Fix a variable $x_0 \in \mathsf{StarVar}(P) \setminus \mathsf{StarVar}(Q)$. Consider the M_p-environment ρ' that is defined as follows:

$$\begin{array}{rcll} \rho'(x) & \triangleq & \rho(x) & \text{if } x \in \mathsf{StarVar}(Q) \\ \rho'(x_0) & \triangleq & \{1,2\} & \\ \rho'(x) & \triangleq & \{0\} & \text{otherwise} \ . \end{array}$$

  Note, first of all, that ρ' is non-empty over $\mathsf{Var}(P) \cup \mathsf{Var}(Q)$ because so was ρ. Moreover, since ρ maps no variable in Q to ω, the same holds for ρ'. Hence, an application of Lem. 3.11(6) gives that $\mathcal{M}_p[\![Q]\!]\rho' \neq \omega$. Furthermore, since $\rho'(x_0)$ is not a singleton, Lem. 3.11(4) gives that $\mathcal{M}_p[\![P]\!]\rho' = \omega$. As the inequation $P \leq Q$ fails in $\mathcal{M}_p$ for the M_p-environment ρ', Lem. 3.8(2) yields that

$$\mathcal{M}_p[\![P]\!]\rho' = \omega \not\subseteq [p] = \mathcal{M}_p[\![Q]\!]\rho' \ .$$

  Let $[(a+a^2)/x_0]$ stand for the substitution mapping x_0 to the expression $a+a^2$, and acting like the identity on all the other variables. Consider now the M_p-environment ρ'' that is defined as follows:

$$\begin{array}{rcll} \rho''(x_0) & \triangleq & \{0\} & \\ \rho''(x) & \triangleq & \rho'(x) & \text{otherwise} \ . \end{array}$$

  By the standard interplay between substitutions and the interpretation mapping $\mathcal{M}_p[\![\cdot]\!]$, we infer that:

$$[p] = \mathcal{M}_p[\![Q]\!]\rho' = \mathcal{M}_p\left[\!\left[Q[(a+a^2)/x_0]\right]\!\right]\rho'' \ .$$

  Lem. 3.2(1) yields that the length of $Q[(a+a^2)/x_0]$ is at most $2^{\mathrm{vars}(Q)}\mathrm{length}(Q)$, that is the weight of Q. By construction, ρ'' maps each variable to a singleton set. An application of Lem. 3.11(3) now gives that the length of $Q[(a+a^2)/x_0]$ is greater than, or equal to, p. Thus, $p \leq 2^{\mathrm{vars}(Q)}\mathrm{length}(Q)$, which was to be shown.

This completes the proof of the theorem. □

In light of the above discussion, we have finally completed the proof of Thm. 2.4, and therefore of Thm. 2.3.

Acknowledgements: We thank Prof. Arto Salomaa for his encouragement to pursue the research reported in this paper. Stefano Varricchio provided useful comments on a draft of this paper.

References

[1] L. ACETO, W. J. FOKKINK, AND A. INGÓLFSDÓTTIR, *A menagerie of non-finitely based process semantics over BPA*: From ready simulation to*

completed traces, Research Report RS–96–23, BRICS (Basic Research in Computer Science, Centre of the Danish National Research Foundation), Department of Computer Science, Aalborg University, July 1996. Available by anonymous ftp at the address `ftp.brics.aau.dk` in the directory `pub/BRICS/RS/96/23`.

[2] S. L. Bloom, *Varieties of ordered algebras*, J. Comput. System Sci., 13 (1976), pp. 200–212.

[3] S. L. Bloom and Z. Ésik, *Equational axioms for regular sets*, Mathematical Structures in Computer Science, 3 (1993), pp. 1–24.

[4] ——, *Iteration Theories: The Equational Logic of Iterative Processes*, EATCS Monographs on Theoretical Computer Science (W. Brauer, G. Rozenberg and A. Salomaa eds.), Springer-Verlag, 1993.

[5] A. Bonnier-Rigny and D. Krob, *A complete system of identities for one-letter rational expressions with multiplicities in the tropical semiring*, Theoretical Comput. Sci., 134 (1994), pp. 27–50.

[6] J. H. Conway, *Regular algebra and finite machines*, Mathematics Series (R. Brown and J. De Wet eds.), Chapman and Hall, London, United Kingdom, 1971.

[7] Z. Ésik, *Independence of the equational axioms for iteration theories*, J. Comput. System Sci., 36 (1988), pp. 66–76.

[8] S. Kleene, *Representation of events in nerve nets and finite automata*, in Automata Studies, C. Shannon and J. McCarthy, eds., Princeton University Press, 1956, pp. 3–41.

[9] D. Kozen, *A completeness theorem for Kleene algebras and the algebra of regular events*, Information and Computation, 110 (1994), pp. 366–390.

[10] D. Krob, *Complete systems of B-rational identities*, Theoretical Comput. Sci., 89 (1991), pp. 207–343.

[11] ——, *Models of a K-rational identity system*, J. Comput. System Sci., 45 (1992), pp. 396–434.

[12] I. Niven and H. Zuckerman, *An introduction to the theory of numbers (2nd edition)*, John Wiley & Sons, 1960.

[13] D. Perrin, *Finite automata*, in Handbook of Theoretical Computer Science, J. van Leeuwen, ed., vol. B: Formal Models and Semantics, Elsevier Science Publishers B.V., 1990, ch. 1, pp. 1–57.

[14] V. Redko, *On defining relations for the algebra of regular events*, Ukrainskii Matematicheskii Zhurnal, 16 (1964), pp. 120–126. In Russian.

[15] ——, *On the algebra of commutative events*, Ukrainskii Matematicheskii Zhurnal, 16 (1964), pp. 185–195. In Russian.

[16] **A. Salomaa**, *Two complete axiom systems for the algebra of regular events*, J. Assoc. Comput. Mach., 13 (1966), pp. 158–169.

[17] ——, *Theory of Automata*, vol. 100 of International Series of Monographs in Pure and Applied Mathematics (I.N. Sneddon and M. Stark eds.), Pergamon Press, Oxford, 1969.

[18] ——, *Personal communication*, June 1996.

[19] **P. M. Sewell**, *Bisimulation is not finitely (first order) equationally axiomatisable*, in Proceedings 9^{th} Annual Symposium on Logic in Computer Science, Paris, France, IEEE Computer Society Press, 1994, pp. 62–70.

[20] ——, *Nonaxiomatisability of equivalences over finite state processes*, September 1996. Draft paper available from the World Wide Web at the URL `http://www.cl.cam.ac.uk/users/pes20/`.

Recent Publications in the BRICS Report Series

RS-96-36 **Luca Aceto, Willem Jan Fokkink, and Anna Ingólfsdóttir.** ***On a Question of A. Salomaa: The Equational Theory of Regular Expressions over a Singleton Alphabet is not Finitely Based*****. October 1996. 16 pp.**

RS-96-35 **Gian Luca Cattani and Glynn Winskel.** ***Presheaf Models for Concurrency*****. October 1996. 16 pp. Presented at the** ***Annual Conference of the European Association for Computer Science Logic*****, CSL '96.**

RS-96-34 **John Hatcliff and Olivier Danvy.** ***A Computational Formalization for Partial Evaluation (Extended Version)*****. October 1996. To appear in** ***Mathematical Structures in Computer Science*****.**

RS-96-33 **Jonathan F. Buss, Gudmund Skovbjerg Frandsen, and Jeffrey Outlaw Shallit.** ***The Computational Complexity of Some Problems of Linear Algebra*****. September 1996. 39 pp.**

RS-96-32 **P. S. Thiagarajan.** ***Regular Trace Event Structures*****. September 1996. 34 pp.**

RS-96-31 **Ian Stark.** ***Names, Equations, Relations: Practical Ways to Reason about 'new'*****. September 1996. ii+22 pp.**

RS-96-30 **Arne Andersson, Peter Bro Miltersen, and Mikkel Thorup.** ***Fusion Trees can be Implemented with AC^0 Instructions only*****. September 1996. 8 pp.**

RS-96-29 **Lars Arge.** ***The I/O-Complexity of Ordered Binary-Decision Diagram Manipulation*****. August 1996. 35 pp. An extended abstract version appears in Staples, Eades, Kato, and Moffat, editors,** ***Algorithms and Computation: 6th International Symposium*****, ISAAC '95 Proceedings, LNCS 1004, 1995, pages 82–91.**

RS-96-28 **Lars Arge.** ***The Buffer Tree: A New Technique for Optimal I/O Algorithms*****. August 1996. 34 pp. This report is a revised and extended version of the BRICS Report RS-94-16. An extended abstract appears in Akl, Dehne, Sack, and Santoro, editors,** ***Algorithms and Data Structures: 4th Workshop*****, WADS '95 Proceedings, LNCS 955, 1995, pages 334–345.**