A relation between unambiguous regular expressions and abstract data types

Viorel PREOTEASA*
Department of Computer Science †
Academy of Economic Studies
Calea Dorobanţilor 15-17
71131 Bucharest, Romania

November 15, 1999

Abstract

Using a categorical model of abstract data types [2, 3, 13, 15], we show, following the Kozen's technique [10] and Tarjan's constructions for a deterministic automaton [16], that if two unambiguous regular expressions define the same regular language, then they represent two isomorphic abstract data types.

1 Introduction

In regular algebra (the algebra of regular languages) it is common to use the symbols of ordinary arithmetic, "0", "1", "+" and "·", to denote the empty set, the set containing the empty word, the union operator and the so-called "product" operator, respectively. This overloading of symbols serves a useful purpose: addition and product of languages enjoy many algebraic properties in common with addition and product in ordinary arithmetic. By exploiting the commonality, it is possible to transfer known results and methods in one domain to the other domain. A notable, and now well-known, example (see e.g. [16]) is the use of the Gauss-Jordan elimination method for determining the inverse of a real matrix to solve the all-paths problem on directed graphs.

In datatype algebra, the arithmetic operators are also overloaded to denote direct sum and cartesian product (and indeed exponentiation, i.e. function spaces). This serves once again the useful purpose of emphasising the commonality in algebraic properties: sum and product of types are, for example, associative and commutative, and product distributes through addition. But in this case the properties only hold "up to isomorphism". That is, an equality in arithmetic becomes an isomorphism of datatypes.

Given an arbitrary regular expression, this overloading of the meaning of the operators allows the expression to be interpreted in three different ways: as a language (a set of

*This work was carried out with the support of a Tempus scholarship whilst the author was visiting Eindhoven University of Technology.

†Current address: Turku Center for Computer Science, DataCity, Lemminkäisenkatu 14 A, FIN-20520 Turku, Finland, email: viorel.preoteasa@abo.fi

words), as an arithmetic expression, and as a datatype. When interpreting the expression as an arithmetic expression the meaning of a^* is $1/(1-a)$. When interpreting the expression as a datatype the meaning of a^* is the type list of a's.

As part of the task of formalising the relationship between the use of matrix-inversion algorithms in real arithmetic and path algorithms in regular algebra, Tarjan [16] proved the remarkable result that if any two unambiguous regular expressions are equal when interpreted as languages, then they are equal when interpreted as arithmetic expressions. Our goal is to show that if two unambiguous regular expressions define the same regular language, then they define two isomorphic abstract data types in a categorical model of abstract data types.

We do this by following the method used in [10]. In that paper, Kozen gives a complete set of axioms for a regular algebra. He then proves that, if two regular expressions define the same language, then the equality between them can be proved completely algebraically using the stated axioms. For abstract data types all of these axioms are valid (up to isomorphism) with the exception of the idempotency of $+$ (union). If we take two unambiguous regular expressions which specify the same language, and we show that their equality can be proved using just those axioms which are valid for abstract data types, this is enough to prove that they represent isomorphic data types

Kozen's method consists in modelling algebraically the well-known technique of constructing a reduced deterministic finite automaton recognizing a given regular language. That is, he shows how to model algebraically the separate phases of that construction: the compositional construction of a non-deterministic automaton, the elimination of empty-word edges, the construction of the subset automaton, etc.

We have been unable to use Kozen's technique directly. The problem is that, in the algebra of regular languages, the property of being a 0-1 matrix is preserved by all three operators (addition, product and iteration). This is not the case in datatype algebra. To overcome this problem our strategy is to construct a deterministic automaton in one go, following the example of Tarjan [16].

The model for abstract data types is a categorical one as in [3, 2, 13, 15] where the abstract data types are viewed as objects in a category and the fact that two abstract data types specify the same type is given by an isomorphism between them in this category. The advantage of this approach is that we can obtain other interpretations of regular expressions just taking a particular case of such category.

2 Category of abstract data types

We recall the categorical model for abstract data type presented in [3] as an application of general fixed-point theorems in category theory. Our intention, in this section, is to reformulate some results from [3] for matrices over abstract data types, proved using some results from [3].

We suppose that some notions as category, initial algebra, functor, natural transformation and adjunction are known [1, 5, 11, 14]. We denote the categories with the calligraphic uppercase letters ($\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\ldots$), the functors with F, G, $\ldots$, $\oplus$, $\otimes$, $\odot$, $\ldots$. When we denote a functor with $\oplus$, $\ldots$, this is a bifunctor and we denote with $x \oplus y$ the application of such functor to (x, y). We also denote with $\mathsf{Id}_a : a \to a$ the identity morphism and with $\mathbf{Id}_{\mathcal{C}} : \mathcal{C} \to \mathcal{C}$ the identity functor. First we will present some results about initial algebra in category theory.

Lemma 2.1

1. Let $F, G : \mathcal{C} \to \mathcal{D}$, $H, K : \mathcal{E} \to \mathcal{F}$ and $\oplus : \mathcal{D} \times \mathcal{F} \to \mathcal{H}$ be functors and $\alpha : F \to G$, $\beta : H \to K$ be natural isomorphisms. Then $(\alpha \oplus \beta) : (F \oplus H) \to (G \oplus K)$ is a natural isomorphism, where $F \oplus H$ and $G \oplus K$ are the functors obtained by functor composition, and $(\alpha \oplus \beta)_{a,b} = \alpha_a \oplus \beta_b$

2. Let $F, G : \mathcal{C} \times \mathcal{D} \to \mathcal{E}$ be functors, $\eta : F \to G$ be a natural isomorphism and $f : a \to b$ be an isomorphism in $\mathcal{C}$. Let $H, K : \mathcal{D} \to \mathcal{C}$, $H(x) = F(a, x)$, $H(h) = F(\mathsf{Id}_a, h)$, $K(x) = G(b, x)$, $K(h) = G(\mathsf{Id}_b, h)$, and $\gamma_x = F(f, \mathsf{Id}_x) \circ \eta_{b,x}$ for all x and h in $\mathcal{D}$. Then H, K are functors and $\gamma : H \to K$ is a natural isomorphism.

3. If the functor $F : \mathcal{C} \to \mathcal{C}$ has an initial algebra (α, a) and $f : a \to b$ is an isomorphism, then $(F(f^{-1}) \circ \alpha \circ f, b)$ is an initial algebra for F.

4. Let $F : \mathcal{C} \to \mathcal{C}$ and $G : \mathcal{D} \to \mathcal{D}$ be functors such that (α, a) is an initial algebra for F and (β, b) is an initial algebra for G. Then $((\alpha, \beta), (a, b))$ is an initial algebra for $(F, G) : \mathcal{C} \times \mathcal{D} \to \mathcal{C} \times \mathcal{D}$.

Proof. Simple verification. □

Proposition 2.2 (Fusion Rule) Let $F : \mathcal{C} \to \mathcal{D}$, $H : \mathcal{D} \to \mathcal{D}$ and $G : \mathcal{C} \to \mathcal{C}$ be functors. If there is $\eta : F \circ H \to G \circ F$ a natural isomorphism, G has an initial algebra (α, a) and F has an upper adjoint, then $(\eta_a \circ F(\alpha), F(a))$ is an initial algebra of H.

Proof. Corollary 6.12 from [3] page 81. □

Corollary 2.3 Let $H, G : \mathcal{C} \to \mathcal{C}$ be functors such that G has an initial algebra (α, a) and there is a natural isomorphism $\eta : H \to G$. Then $(\eta_a \circ \alpha, a)$ is an initial algebra of the functor H.

Proof. Applying Proposition 2.2 with $\mathbf{Id}_{\mathcal{C}}$ instead of F. □

Proposition 2.4 (Exchange Rule) Let $F : \mathcal{D} \to \mathcal{C}$, $G : \mathcal{C} \to \mathcal{D}$ and $H : \mathcal{C} \to \mathcal{D}$ be functors such that both G and H have upper adjoints. If there is $\eta : G \circ F \circ H \to H \circ F \circ G$ a natural isomorphism, $G \circ F$ has an initial algebra (α, a) and $H \circ F$ has an initial algebra (β, b), then $a \cong b$.

Proof. Theorem 6.69 from [3] page 99. □

Let $F : \mathcal{D} \times \mathcal{C} \to \mathcal{C}$ be a functor such that for any object d in $\mathcal{C}$ the functor $G_d : \mathcal{C} \to \mathcal{C}$, given by $G_d(x) = F(d, x)$ and $G_d(f) = F(\mathsf{Id}_d, f)$, has an initial algebra $(\alpha_d, \varpi_F(d))$. Let $f : a \to b$ be a morphism and $\varpi_F(f) : \varpi_F(a) \to \varpi_F(b)$ be the unique morphism such that the following diagram is commutative.

$$\begin{tikzcd}
F(a, \varpi_F(b)) \arrow[r, "F(f, \mathsf{Id}_{\varpi_F(b)})"] & F(b, \varpi_F(b)) \arrow[r, "\alpha_b"] & \varpi_F(b) \\
F(a, \varpi_F(a)) \arrow[u, "F(\mathsf{Id}_a, \varpi_F(f))"] \arrow[rr, "\alpha_a"] & & \varpi_F(a) \arrow[u, "\varpi_F(f)"']
\end{tikzcd}$$

Lemma 2.5 The application $\varpi_F : \mathcal{C} \to \mathcal{C}$ is a functor. $\square$

Lemma 2.6 Let $F, G : \mathcal{D} \times \mathcal{C} \to \mathcal{C}$ be functors such that there is $\eta : F \to G$ a natural isomorphism, and for all x in $\mathcal{D}$, $F(x, \_) : \mathcal{C} \to \mathcal{C}$ has an initial algebra $(\alpha_x, \varpi_F(x))$. Then, for all x in $\mathcal{D}$, $G(x, \_)$ has an initial algebra $(\eta_{x,\varpi_F(x)} \circ \alpha_x, \varpi_F(x))$ and $\varpi_F = \varpi_G$

Proof. Using Lemma 2.1.2 it follows that $\eta_{x,\_}$ is a natural isomorphism and using Corollary 2.3 it follows that $(\eta_{x,\varpi_F(x)} \circ \alpha_x, \varpi_F(x))$ is an initial algebra of the functor $G(x, \_)$. If x is an object in $\mathcal{D}$, then $\varpi_G(x) = \varpi_F(x)$. Let $f : x \to y$ be a morphism in $\mathcal{D}$. To prove that $\varpi_G(f) = \varpi_F(f)$ it is enough to prove that the following diagram is comutative.

$$\begin{tikzcd}
G(x, \varpi_G(y)) \arrow[r, "G(f, \mathsf{Id}_{\varpi_G(y)})"] & G(y, \varpi_G(y)) \arrow[r, "\eta_{y,\varpi_G(y)} \circ \alpha_y"] & \varpi_G(y) \\
G(x, \varpi_G(x)) \arrow[u, "G(\mathsf{Id}_x, \varpi_F(f))"] \arrow[rr, "\eta_{x,\varpi_G(x)} \circ \alpha_x"] & & \varpi_G(x) \arrow[u, "\varpi_F(f)"']
\end{tikzcd}$$

Using the fact that η is natural morphism and G is functor it follows that the above diagram is commutative and, because $\varpi_G(f)$ is the unique morphism which make it commutative, it follows that $\varpi_G(f) = \varpi_F(f)$. $\square$

Proposition 2.7 (Diagonal Rule) Let $\oplus : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ be a functor such that for all x in $\mathcal{C}$, $x \oplus \_$ has an initial algebra $(\alpha_x, \varpi_\oplus x)$. If the functor $x \mapsto x \oplus x$ has an initial algebra (α, a), then (β, a) is an initial algebra for $\varpi_\oplus$, where β is the unique morphism such that the following diagram is commutative.

$$\begin{tikzcd}
a \oplus a \arrow[r, "\alpha"] & a \\
a \oplus \varpi_\oplus a \arrow[u, "\mathsf{Id}_a \oplus \beta"] \arrow[r, "\alpha_a"] & \varpi_\oplus a \arrow[u, "\beta"']
\end{tikzcd}$$

Proof. Theorem 6.48 from [3] page 105. $\square$

Let $F : \mathcal{C} \to \mathcal{D}$, $G : \mathcal{C} \to \mathcal{E}$ and $\oplus : \mathcal{D} \times \mathcal{E} \to \mathcal{H}$ be functors. We denote with $F \overset{\triangle}{\oplus} G$ the functor $\triangle \circ (F \oplus G)$ where $\triangle : \mathcal{C} \to \mathcal{C} \times \mathcal{C}$ is the functor given by $\triangle(x) = (x, x)$.

Proposition 2.8 (Mutual Recursion) Let $\odot : \mathcal{D}\times\mathcal{C} \to \mathcal{C}$ and $\otimes : \mathcal{C}\times\mathcal{D} \to \mathcal{D}$ be functors such that, for all x in $\mathcal{C}$ and y in $\mathcal{D}$, the functors $x \otimes \_$, $y \odot \_$, $\varpi_\otimes \overset{\triangle}{\odot} \mathbf{Id}_\mathcal{C}$ and $\varpi_\odot \overset{\triangle}{\otimes} \mathbf{Id}_\mathcal{C}$ have initial algebras. Then the functor $F : \mathcal{C} \times \mathcal{D} \to \mathcal{C} \times \mathcal{D}$ defined by $F(x, y) = (y \odot x, x \otimes y)$ has an initial algebra with the carrier (a, b) where a, b are the carriers of the initial algebras of $\varpi_\otimes \overset{\triangle}{\odot} \mathbf{Id}_\mathcal{C}$ and $\varpi_\odot \overset{\triangle}{\otimes} \mathbf{Id}_\mathcal{C}$, respectively.

Proof. Theorem 6.51 from [3] page 108. □

Let $\mathcal{C}$ be a category and a, b be two objects from $\mathcal{C}$.

Definition 2.9 The *binary direct sum* of a and b is an object denoted $a+b$ from $\mathcal{C}$ with two morphisms $\mathsf{I}^1_{a,b} : a \to a+b$ and $\mathsf{I}^2_{a,b} : b \to a+b$ such that, for every morphisms $f : a \to c$ and $g : b \to c$, there is a unique morphism denoted $[f, g] : a+b \to c$ such that $\mathsf{I}^1_{a,b} \circ [f, g] = f$ and $\mathsf{I}^2_{a,b} \circ [f, g] = g$. We say that a category *has binary direct sums* if a binary direct sum exists for each pair of objects. □

Let $f : a \to b$ and $g : c \to d$ be two morphisms and let $f + g : a+c \to b+d$ be the morphism given by $f + g = [f \circ \mathsf{I}^1_{b,d}, g \circ \mathsf{I}^2_{b,d}]$. Then next lemma is abvious.

Lemma 2.10 The application $+ : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor. □

Definition 2.11 The *binary direct product* of a and b is an object denoted $a \cdot b$ from $\mathcal{C}$ with two morphisms $\mathsf{P}^1_{a,b} : a \cdot b \to a$ and $\mathsf{P}^2_{a,b} : a \cdot b \to b$ such that, for every morphisms $f : c \to a$ and $g : c \to b$, there is a unique morphism denoted $\langle f, g\rangle : c \to a \cdot b$ such that $\langle f, g\rangle \circ \mathsf{P}^1_{a,b} = f$ and $\langle f, g\rangle \circ \mathsf{P}^2_{a,b} = g$. We say that a category *has binary direct products* if a binary direct product exists for each pair of objects.

Let $f : a \to b$ and $g : c \to d$ be two morphisms. If $f \cdot g : a \cdot c \to b \cdot d$ is the morphism given by $f \cdot g = \langle \mathsf{P}^1_{a,c} \circ f, \mathsf{P}^2_{a,c} \circ g\rangle$, then we have immediately:

Lemma 2.12 The application $\cdot : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ is a functor. □

Given a category $\mathcal{C}$ we denote with 0 an initial object in $\mathcal{C}$ (if it exists) and with 1 a final object (also if it exists). Let $\mathsf{Init}_a : 0 \to a$ and $\mathsf{Final}_a : a \to 1$ be the unique morphisms.

Lemma 2.13 If $\mathcal{C}$ has binary direct sums and an initial object 0, then $a + 0 \cong 0 + a \cong a$. If $\mathcal{C}$ has binary direct products and final object 1, then $a \cdot 1 \cong 1 \cdot a \cong a$.

Proof. The isomorphism between a and $a + 0$ is given by $\mathsf{I}^1_{a,0}$ and $[\mathsf{Id}_a, \mathsf{Init}_a]$ and the isomorphism between a and $a \cdot 1$ is given by $\mathsf{P}^1_{a,1}$ and $\langle \mathsf{Id}_a, \mathsf{Final}_a\rangle$ □

Definition 2.14 We say that a category is *distributive* [6, 7] if it satisfies

1. has binary direct sums and products;
2. has an initial object 0, and
3. the canonical morphisms $\mathsf{ldistr}_{a,b,c} : a{\cdot}b+a{\cdot}c \to a{\cdot}(b+c)$, $\mathsf{rdistr}_{a,b,c} : a{\cdot}c+b{\cdot}c \to a{\cdot}(b+c)$, $\mathsf{lzero}_a : 0 \cdot a \to 0$, and $\mathsf{rzero}_a : a \cdot 0 \to 0$ are isomorphisms. □

Definition 2.15 Let $\mathcal{C}$ be a category. We call the category $\mathcal{C}$ *a category of abstract data types* if

1. it is cartesian closed [1, 5, 11, 14] (i.e. has binary direct products, a final object 1 and the functor $\_ \cdot a$ has an upper adjoint);
2. it has binary direct sums and an initial object 0;
3. the functor $x \mapsto 1 + a \cdot x$ has an initial algebra (α_a, a^*) for every $a \in |\mathcal{C}|$, where a^* is $\varpi_F(a)$ with $F(a, x) = 1 + a \cdot x$. Also we denote with f^* the morphism $\varpi_F(f)$ for a morphism f in $\mathcal{C}$.

We refer to the objects of $\mathcal{C}$ as *abstract data types*. Two abstract data types a, b are *isomorphic*, denoted $a \cong b$, if they are isomorphic as objects in the category $\mathcal{C}$. □

The same model for data types can be found in [2, 3, 13, 15]. In [13], instead of our condition 3. it is required to have an initial algebra for a colection of functors in order to obtain other data types, like trees for example.

The condition "$\_ \cdot a$ has an upper adjoint" is stronger than the axioms from [10], meaning that this adjuction gives us a new operation (exponent) which has no correspondent in our syntax. We need it for proving some isomorphism between matrices over abstract data types. The main point in which we need this condition is to show that $a^* \cdot b$ is the carrier of an initial algebra of the functor $x \mapsto b + a \cdot x$.

Exemple 2.16 The category Sets, which has the sets as objects and the functions between them as morphisms, is a category of abstract data types. $a + b$ is the disjoint union of a, b; $a \cdot b$ is the cartesian product of a, b; a^b is the set of functions from a to b; and a^* is the set of lists with elements of a, i.e., $\bigcup_{n \geq 0} a^n$ □

Exemple 2.17 Let $\mathcal{H} = (H, \wedge, \vee, \rightarrow, 0, 1)$ be a Heyting algebra [4] (a distributive lattice with 0 and an operation denoted $\rightarrow$ which satisfies $a \wedge b \leq c$ iff $a \leq b \rightarrow c$ for any $a, b, c \in H$). If the poset $(H, \leq)$ is viewed as a category, then it is a category of abstract data types, where $a + b$ is the lattice join of a, b; $a \cdot b$ is the lattice meet of a, b; a^b is $a \rightarrow b$; and $a^* = 1$. □

Some non-trivial examples of such categories can be also found in [13].

Lemma 2.18 A category of abstract data types is a distributive category.

Proof. Because the functor $\_ \cdot a$ has an upper adjoint then $\_ \cdot a$ distributes over every colimit. Hence $\_ \cdot a$ also distributes over the binary direct sums and over the initial object, which are colimits. □

We assume that $\mathcal{C}$ is a category of abstract data types. Let a, b, c be objects from $\mathcal{C}$. We define below several morfisms.

1. The *sum comutativity* morphism $\mathsf{scomut}_{a,b} : a + b \rightarrow b + a$ given by

$$\mathsf{scomut}_{a,b} = [\mathsf{I}^2_{b,a}, \mathsf{I}^1_{b,a}].$$

2. The *sum associativity* morphism $\mathsf{sassoc}_{a,b,c} : a + (b + c) \rightarrow (a + b) + c$ given by

$$\mathsf{sassoc}_{a,b,c} = [\mathsf{I}^1_{a,b} \circ \mathsf{I}^1_{a+b,c}, [\mathsf{I}^2_{a,b} \circ \mathsf{I}^1_{a+b,c}, \mathsf{I}^2_{a+b,c}]]$$

3. The *product associativity* morphism $\mathsf{passoc}_{a,b,c} : a\cdot(b\cdot c)\to(a\cdot b)\cdot c$ given by

$$\mathsf{passoc}_{a,b,c} = \langle\langle \mathsf{P}^1_{a,b\cdot c}, \mathsf{P}^2_{a,b\cdot c}\circ \mathsf{P}^1_{b,c}\rangle, \mathsf{P}^2_{a,b\cdot c}\circ \mathsf{P}^2_{b,c}\rangle$$

4. The *distributivity* morphisms $\mathsf{ldistr}_{a,b,c} : a\cdot b + a\cdot c\to a\cdot(b+c)$ and $\mathsf{rdistr}_{a,b,c} : a\cdot c+b\cdot c\to (a+b)\cdot c$ given by

$$\mathsf{ldistr}_{a,b,c} = [\mathsf{Id}_a\cdot \mathsf{I}^1_{b,c}, \mathsf{Id}_a\cdot \mathsf{I}^2_{b,c}]$$

and

$$\mathsf{rdistr}_{a,b,c} = [\mathsf{I}^1_{a,b}\cdot \mathsf{Id}_c, \mathsf{I}^2_{a,b}\cdot \mathsf{Id}_c].$$

Lemma 2.19 The transformations scomut, sassoc, passoc, ldistr, rdistr, $\mathsf{P}^1_{\_,1}$, $\mathsf{P}^2_{1,\_}$, $\mathsf{P}^1_{0,\_}$, $\mathsf{P}^2_{\_,0}$, $\mathsf{I}^1_{\_,0}$, $\mathsf{I}^2_{0,\_}$ are natural isomorphisms. □

3 Matrix categories over abstract data types

Let $\mathcal{C}$ be an arbitrary category of abstract data types. Let $\mathcal{M}_{m,n}(\mathcal{C})$ be the category which has as objects the matrices over the objects of $\mathcal{C}$ with m rows and n columns and as morphisms the matrices of the same dimension over morphisms of $\mathcal{C}$ between the components of object matrices. We think about $\mathcal{M}_{1,1}(\mathcal{C})$ as $\mathcal{C}$. We also extend the isomorphis relation $\cong$ from objects to matrices. On objects and morphisms of $\mathcal{M}_{m,n}(\mathcal{C})$ we define $+_{m,n}$ by component-wise application of $+$. With this operation the category $\mathcal{M}_{m,n}(\mathcal{C})$ becomes a category which has binary direct sums. Also $\mathcal{M}_{m,n}(\mathcal{C})$ has an initial object $0_{m,n}$. We also define an application $\cdot_{m,n,k}$ from $\mathcal{M}_{m,n}(\mathcal{C})\times\mathcal{M}_{n,k}(\mathcal{C})$ to $\mathcal{M}_{m,k}(\mathcal{C})$ as the usual product of matrices.

Observation 3.1 Let $F:\mathcal{M}_{m,n}(\mathcal{C})\to\mathcal{M}_{p,q}(\mathcal{C})$ be an application such that

$$F(X) = (F_{i,j}(x_{1,1}, x_{1,2},\ldots,x_{m,n}))_{i,j\in[p]\times[q]}$$

where $X=(x_{l,k})$ and $F_{i,j}$ is functor from $\mathcal{C}^{m\cdot n}$ to $\mathcal{C}$ for all i,j. Then F is a functor. □

Corollary 3.2 The operations $+_{m,n}$ and $\cdot_{m,n,k}$ are functors.

Proof. Any component of the result matrix is a composition of $+$ and $\cdot$ which are functors. It follows that the operations on matrices are functors. □

We denote with $\mathbf{I}_n$ the unit matrix from $\mathcal{M}_{n,n}(\mathcal{C})$ which has 1 on the main diagonal and 0 elsewhere. We overload the operators $+$, $\cdot$, 0 and $\mathbf{I}$ by using them both for matrices and category $\mathcal{C}$.

Let $y\mapsto y^a$, $f\mapsto f^a$ be the adjoint of the functor $\_\cdot a$. For $Y,Z\in|\mathcal{M}_{m,n}(\mathcal{C})|$, $A\in|\mathcal{M}_{n,k}(\mathcal{C})|$ and $f:Y\to Z$, we define

$$Y^A\in\mathcal{M}_{m,n}(\mathcal{C}),\quad Y^A=\left(\prod_{l=1}^{k} y_{i,l}^{a_{j,l}}\right)_{i,j}$$

and

$$f^A : Y^A\to Z^A,\quad f^A=\left(\prod_{l=1}^{k} f_{i,l}^{a_{j,l}}\right)_{i,j}$$

Lemma 3.3 The application $\_^A : \mathcal{M}_{m,k}(\mathcal{C}) \to \mathcal{M}_{m,n}(\mathcal{C})$ is a functor and it is an upper adjoint for the functor $\_ \cdot A : \mathcal{M}_{m,n}(\mathcal{C}) \to \mathcal{M}_{m,k}(\mathcal{C})$.

Proof. Using Observation 3.1 it follows that $\_^A$ is a functor because $\prod_{l=1}^{k} y_{i,l}^{a_{j,l}}$ is a composition of functors.

To prove that $\_^A$ is an upper adjoint for $\_ \cdot A$ it is enough to give a morphism $\mathsf{eval}_{Y,A} : (Y^A) \cdot A \to Y$ such that, for every morphism $f : X \cdot A \to Y$, there is a unique morphism $\Lambda(f) : X \to Y^A$ such that the following diagram is commutative.

$$\begin{tikzcd}
X \cdot A \arrow[rr, "f"] \arrow[dr, "\Lambda(f) \cdot \mathsf{Id}_A"'] & & Y \\
& Y^A \cdot A \arrow[ur, "\mathsf{eval}_{Y,A}"'] &
\end{tikzcd}$$

We prove this by induction on m, n and k. If $m = n = k = 1$, then it is true. Let

$$A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}, \quad X = \begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix}, \quad Y = \begin{pmatrix} Y_{11} & Y_{12} \\ Y_{21} & Y_{22} \end{pmatrix}$$

and

$$\mathsf{eval}_{Y,A} = (\alpha_{ij})_{i,j \in \{1,2\}}$$

where

$$\alpha_{ij} = [(\mathsf{P}^j_{Y_{i1}^{A_{11}}, Y_{i2}^{A_{12}}} \cdot \mathsf{Id}_{A_{1j}}) \circ \mathsf{eval}_{Y_{ij}, A_{1j}}, (\mathsf{P}^j_{Y_{i1}^{A_{21}}, Y_{i2}^{A_{22}}} \cdot \mathsf{Id}_{A_{2j}}) \circ \mathsf{eval}_{Y_{ij}, A_{2j}}].$$

If

$$\Lambda(f) = \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix},$$

then we should have, for all $i, j \in \{1, 2\}$, that

$$(g_{i1} \cdot \mathsf{Id}_{A_{1j}} + g_{i2} \cdot \mathsf{Id}_{A_{2j}}) \circ \alpha_{ij} = f_{ij}.$$

Because $f_{ij} : X_{i1} \cdot A_{1j} + X_{i2} \cdot A_{2j} \to Y_{ij}$ it follows that $f_{ij} = [f_{ij}^1, f_{ij}^2]$. It follows that

$$g_{i1} \circ \mathsf{P}^j_{Y_{i1}^{A_{11}}, Y_{i2}^{A_{12}}} = \Lambda(f_{ij}^1) \text{ and } g_{i2} \circ \mathsf{P}^j_{Y_{i1}^{A_{21}}, Y_{i2}^{A_{22}}} = \Lambda(f_{ij}^2),$$

thus

$$g_{ij} = \langle \Lambda(f_{i1}^j), \Lambda(f_{i2}^j) \rangle. \tag{1}$$

This proves the uniqueness and, if we take g_{ij} as in (1), then $\Lambda(f)$ is the unique morphism such that the above diagram commutes. □

Lemma 3.4

1. The operation $+$ on matrices is commutative and associative, and scomut, sassoc are natural isomorphisms;

2. The operation $\cdot$ on matrices is associative and passoc is a natural isomorphism.

3. The operation $\cdot$ is distributive over $+$ at left and right, and ldistr, rdistr are natural isomorphisms.

4. $\mathbf{I}_n \cdot A \cong A \cong A \cdot \mathbf{I}_m$, $0 \cdot A \cong 0 \cong A \cdot 0$, $0 + A \cong A \cong A + 0$, and the isomorphisms are natural transformations.

Proof. Since the set objects of $\mathcal{C}$ quotiented by the isomorphism relation has the semiring structure with operations $\{+, \ \cdot, \ 0, \ 1\}$, all applications in discussion are isomorphisms. The naturality is given by the fact that an isomorphism between two matrices arises from isomorphisms between the matrices components which are natural. $\square$

Proposition 3.5 Suppose that the functor which maps T to $\mathbf{I} + A \cdot T$ has an initial algebra (α, A^*) with A, A^* square matrices with the same dimension. Then

1. The functor which maps T to $X + A \cdot T$ has an initial algebra $(\beta_X, \ A^* \cdot X)$, where

$$\beta_X = ((\mathsf{P}^2_{1,x})^{-1} + \mathsf{passoc}_{A,A^*,X}) \circ \mathsf{rdistr}_{1,A \cdot A^*,X} \circ (\alpha \cdot \mathsf{Id}_X).$$

2. For any morphism $f : X \to Y$, the following diagram is commutative

$$\begin{tikzcd}
Y + A \cdot (A^* \cdot Y) \arrow[r, "\beta_Y"] & A^* \cdot Y \\
X + A \cdot (A^* \cdot X) \arrow[u, "f + \mathsf{Id}_A \cdot (\mathsf{Id}_{A^*} \cdot f)"'] \arrow[r, "\beta_X"] & A^* \cdot X \arrow[u, "\mathsf{Id}_{A^*} \cdot f"']
\end{tikzcd}$$

i.e., $\varpi_H(f) = \mathsf{Id}_{A^*} \cdot f$ where $H(X,T) = X + A \cdot T$.

Proof. Let $F(T) = T \cdot X$, $G(T) = \mathbf{I} + A \cdot T$ and $H(T) = X + A \cdot T$. Then F has an upper adjoint and

$$F \circ H(T) = X + A \cdot (T \cdot X) \text{ and } H \circ F(T) = (\mathbf{I} + A \cdot T) \cdot X.$$

It follows that there is a natural isomorphism $\eta : F \circ H \to G \circ F$ given by

$$\eta_T = ((\mathsf{P}^2_{1,X})^{-1} + \mathsf{passoc}_{A,T,X}) \circ \mathsf{rdistr}_{1,A \cdot T,X}.$$

Applying the Fusion Rule (Lemma 2.2) to the functors F, G and H, it follows that

$$(\eta_{A^*} \circ F(\alpha), F(A^*)) = (\beta_X, A^* \cdot X)$$

is an initial algebra for the functor H.
2. It is enough to prove

$$\mathsf{I}^1_{X,A\cdot(A^*\cdot X)} \circ (f + \mathsf{Id}_A \cdot (\mathsf{Id}_{A^*} \cdot f)) \circ \beta_Y = \mathsf{I}^1_{X,A\cdot(A^*\cdot X)} \circ \beta_X \circ (\mathsf{Id}_{A^*} \cdot f)$$

and

$$\mathsf{I}^2_{X,A\cdot(A^*\cdot X)} \circ (f + \mathsf{Id}_A \cdot (\mathsf{Id}_{A^*} \cdot f)) \circ \beta_Y = \mathsf{I}^2_{X,A\cdot(A^*\cdot X)} \circ \beta_X \circ (\mathsf{Id}_{A^*} \cdot f)$$

which are true by simple verification. $\square$
We recall the following definition from [8, 10]

Definition 3.6 Let $A \in \mathcal{M}_{n,n}(\mathcal{C})$. We define $A^* \in \mathcal{M}_{n,n}(\mathcal{C})$ inductively as

- $(a)^* = (a^*)$;
- $\begin{pmatrix} a & D \\ E & G \end{pmatrix}^* = \begin{pmatrix} (a + D \cdot (G^* \cdot E))^* & (a + D \cdot (G^* \cdot E))^* \cdot (D \cdot G^*) \\ (G + E \cdot (a^* \cdot D))^* \cdot (E \cdot a^*) & (G + E \cdot (a^* \cdot D))^* \end{pmatrix}$

where $a \in |\mathcal{C}|$, $D \in |\mathcal{M}_{1,n}(\mathcal{C})|$, $E \in |\mathcal{M}_{n,1}(\mathcal{C})|$ and $G \in |\mathcal{M}_{n,n}(\mathcal{C})|$ □

Observation 3.7 If A is an $n \times n$ matrix over the real numbers with $*$ defined for A as in Definition 3.6 where $a^* = 1/(1-a)$ for any real number $a \neq 1$, then A^* (if it exists) is $(\mathbf{I} - A)^{-1}$. □

Theorem 3.8 Let A be an object from $\mathcal{M}_{m,m}(\mathcal{C})$ and B an object from $\mathcal{M}_{m,n}(\mathcal{C})$. Then the functor $F : \mathcal{M}_{m,n}(\mathcal{C}) \to \mathcal{M}_{m,n}(\mathcal{C})$ defined by $F(X) = B + A \cdot X$ has an initial algebra with the carrier $A^* \cdot B$.

Proof. If $n = n_1 + n_2$ then $B = (B_1,\, B_2)$ and $X = (X_1,\, X_2)$. It follows that

$$F(X) = (B_1,\, B_2) + A \cdot (X_1,\, X_2) = (B_1 + A \cdot X_1,\ B_2 + A \cdot X_2).$$

If the functors $F_1(X_1) = B_1 + A \cdot X_1$ and $F_2(X_2) = B_2 + A \cdot X_2$ have initial algebras α_1 α_2, respectively, then, using Lemma 2.1.4, it follows that F has an initial algebra $(\alpha_1,\, \alpha_2)$. It is therefore enough to prove the statement for $n = 1$.

We will prove it by induction on m. If $m = 1$ the statement is true by Proposition 3.5. Suppose that the statement is true for m. Let

$$B = \begin{pmatrix} b \\ C \end{pmatrix},\ A = \begin{pmatrix} a & D \\ E & G \end{pmatrix},\ X = \begin{pmatrix} x \\ Y \end{pmatrix},$$

with $a, b \in |\mathcal{C}|$; $C, Y, E \in |\mathcal{M}_{m,1}(\mathcal{C})|$; $D \in |\mathcal{M}_{1,m}(\mathcal{C})|$ and $G \in |\mathcal{M}_{m,m}(\mathcal{C})|$. Let

$$Y \odot x = b + (a \cdot x + D \cdot Y) \text{ and } x \otimes Y = C + (E \cdot x + G \cdot Y).$$

Using these notations, the functor F becomes

$$F\begin{pmatrix} x \\ Y \end{pmatrix} = \begin{pmatrix} Y \odot x \\ x \otimes Y \end{pmatrix}.$$

Let K be the functor given by $K(Y, x) = (b + D \cdot Y) + a \cdot x$. Using the inductive hypothesis and Proposition 3.5, it follows that

$$\varpi_K(Y) = a^* \cdot (b + D \cdot Y) \text{ and } \varpi_K(f) = \mathsf{Id}_{a^*} \cdot (\mathsf{Id}_b + \mathsf{Id}_D \cdot f).$$

There is $\eta : K \to \odot$ a natural isomorphism, hence, using Lemma 2.6, it follows that

- The functor $Y \odot \_$ has an initial algebra;
- $\varpi_\odot(Y) = a^* \cdot (b + D \cdot Y)$;
- $\varpi_\odot(f) = \mathsf{Id}_{a^*} \cdot (\mathsf{Id}_b + \mathsf{Id}_D \cdot f)$.

Applying similar arguments for $\otimes$ we obtain that

- The functor $x \otimes \_$ has an initial algebra;
- $\varpi_\otimes(x) = G^* \cdot (C + E \cdot x)$;
- $\varpi_\otimes(f) = \mathsf{Id}_{G^*} \cdot (\mathsf{Id}_C + \mathsf{Id}_E \cdot f)$.

We now prove that the functor $\varpi_\otimes \overset{\triangle}{\odot} \mathsf{Id}_\mathcal{C}$ has an initial algebra, where

$$(\varpi_\otimes \overset{\triangle}{\odot} \mathsf{Id}_\mathcal{C})(x) = b + (a \cdot x + D \cdot (G^* \cdot (C + E \cdot x)))$$

and

$$(\varpi_\otimes \overset{\triangle}{\odot} \mathsf{Id}_\mathcal{C})(f) = \mathsf{Id}_b + (\mathsf{Id}_a \cdot f + \mathsf{Id}_D \cdot (\mathsf{Id}_{G^*} \cdot (\mathsf{Id}_C + \mathsf{Id}_E \cdot f))).$$

There is a natural isomorphism $\gamma : \varpi_\otimes \overset{\triangle}{\odot} \mathbf{Id}_\mathcal{C} \to H$ where $H(x) = (b + D \cdot (G^* \cdot C)) + (a + D \cdot (G^* \cdot E)) \cdot x$. Using the inductive hypothesis, it follows that H has an initial algebra with the carrier $(a + D \cdot (G^* \cdot E))^* \cdot (b + D \cdot (G^* \cdot C))$, hence the functor $\varpi_\otimes \overset{\triangle}{\odot} \mathbf{Id}_\mathcal{C}$ has an initial algebra with the carrier $(a + D \cdot (G^* \cdot E))^* \cdot (b + D \cdot (G^* \cdot C))$.

Using similar arguments, it follows that the functor $\varpi_\odot \overset{\triangle}{\otimes} \mathbf{Id}_\mathcal{C}$ has an initial algebra with the carrier $(G + E \cdot (a^* \cdot D))^* \cdot (C + E \cdot (a^* \cdot b))$.

Using the Mutual Recursion (Proposition 2.8), it follows that the functor F has an initial algebra with the carrier

$$U = \begin{pmatrix} (a + D \cdot (G^* \cdot E))^* \cdot (b + D \cdot (G^* \cdot C)) \\ (G + E \cdot (a^* \cdot D))^* \cdot (C + E \cdot (a^* \cdot b)) \end{pmatrix}.$$

Therefore

$$U \cong \begin{pmatrix} (a + D \cdot (G^* \cdot E))^* & (a + D \cdot (G^* \cdot E))^* \cdot (D \cdot G^*) \\ (G + E \cdot (a^* \cdot D))^* \cdot (E \cdot a^*) & (G + E \cdot (a^* \cdot D))^* \end{pmatrix} \cdot \begin{pmatrix} b \\ C \end{pmatrix}.$$

By Lemma 2.1.3, we get that F has an initial algebra with the carrier $A^* \cdot B$. □

Corollary 3.9

$$\begin{pmatrix} U & V \\ W & Z \end{pmatrix}^* \cong \begin{pmatrix} (U + V \cdot (Z^* \cdot W))^* & (U + V \cdot (Z^* \cdot W))^* \cdot (V \cdot Z^*) \\ (Z + W \cdot (U^* \cdot V))^* \cdot (W \cdot U^*) & (Z + W \cdot (U^* \cdot V))^* \end{pmatrix}$$

for $U \in |\mathcal{M}_{n,n}(\mathcal{C})|$, $V \in |\mathcal{M}_{n,m}(\mathcal{C})|$, $W \in |\mathcal{M}_{m,n}(\mathcal{C})|$ and $Z \in |\mathcal{M}_{m,m}(\mathcal{C})|$. □

Theorem 3.10 Let $A \in |\mathcal{M}_{n,n}(\mathcal{C})|$. Then there is ${}^*A \in |\mathcal{M}_{n,n}(\mathcal{C})|$ such that, for every $B \in |\mathcal{M}_{m,n}(\mathcal{C})|$, $B \cdot {}^*A \in |\mathcal{M}_{n,n}(\mathcal{C})|$ is the carrier of an initial algebra of the functor $F : \mathcal{M}_{m,n}(\mathcal{C}) \to \mathcal{M}_{m,n}(\mathcal{C})$ given by $F(X) = B + X \cdot A$. □

We now are able to prove some isomorphisms between matrices on abstract data types.

Theorem 3.11 Let A, B, C be matrices of appropriate types. Then

1. $A \cong B$ and $C \cong D \;\Rightarrow\; A + C \cong B + D$;
2. $A \cong B$ and $C \cong D \;\Rightarrow\; A \cdot C \cong B \cdot D$;
3. $A \cong B \;\Rightarrow\; A^* \cong B^*$;
4. $A^* \cong \mathbf{I} + A \cdot A^*$;
5. $A + B \cong B + A$;
6. $A + (B + C) \cong (A + B) + C$;
7. $A \cdot (B \cdot C) \cong (A \cdot B) \cdot C$
8. $A \cdot (B + C) \cong A \cdot B + A \cdot C$;
9. $(A + B) \cdot C \cong A \cdot C + B \cdot C$;
10. $A + 0 \cong 0 + A \cong A$;
11. $A \cdot \mathbf{I}_n \cong \mathbf{I}_m \cdot A \cong A$;
12. $A \cdot 0 \cong 0 \cdot A \cong 0$;
13. $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}^* \cong \begin{pmatrix} A^* & A^* \cdot B \cdot C^* \\ 0 & C^* \end{pmatrix}$;
14. $\begin{pmatrix} 0 & A \\ 0 & 0 \end{pmatrix}^* \cong \begin{pmatrix} \mathbf{I}_n & A \\ 0 & \mathbf{I}_m \end{pmatrix}$;
15. $0^* \cong \mathbf{I}_n$;
16. $A \cdot X \cong X \cdot B \;\Rightarrow\; A^* \cdot X \cong X \cdot {}^*B$;
17. $A^* \cong {}^*A$
18. $(A \cdot B)^* \cdot A \cong A \cdot (B \cdot A)^*$;
19. $(B + A)^* \cong A^* \cdot (B \cdot A^*)^*$.

Proof. (1.), (2.) and (3.) are true because $+$, $\cdot$ and $*$ are functors on matrices.

(4.) is true because $F(a) \cong a$ where a is the carrier of an initial algebra of F.

(5.) to (12.) are true because they are true on the base category $\mathcal{C}$ and give a semiring structure on objects of $\mathcal{C}$ quotiented by $\cong$.

(13.) From Corollary 3.9.

(14.) and (15.) follow from (13.) by induction, because we have $0^* = 1$ in $\mathcal{C}$.

(16.) Let $F(T) = X + T$, $G(T) = A \cdot T$ and $H(T) = T \cdot B$. Then $G \circ F \circ H(T) = (X + A \cdot T) \cdot B$ and $H \circ F \circ G(T) = A \cdot (X + T \cdot B)$. Using Lemma 2.1, we obtain that

$$\eta_T = \mathsf{rdistr}_{X, A\cdot T, B} \circ (f + \mathsf{Id}_{(A\cdot T)\cdot B}) \circ (\mathsf{Id}_{A\cdot X} + \mathsf{passoc}^{-1}_{A,T,B}) \circ \mathsf{ldistr}^{-1}_{A,X,T\cdot B}$$

is a natural isomorphism between $G \circ F \circ H$ and $H \circ F \circ G$. Because $G \circ F(T) = X + A \cdot T$ has an initial algebra with the carrier $A^* \cdot X$ and $H \circ F(T) = X + T \cdot B$ has an initial algebra with the carrier $X \cdot {}^*B$, it follows using the Exchange Rule (Proposition 2.4)

$$A^* \cdot X \cong X \cdot {}^*B$$

(17.) and (18.) are instances of (16.).

(19.) Let $\oplus : \mathcal{M}_{n,n}(\mathcal{C}) \times \mathcal{M}_{n,n}(\mathcal{C}) \to \mathcal{M}_{n,n}(\mathcal{C})$ be the functor given by $X \oplus Y = (\mathbf{I}_n + B \cdot X) + A \cdot Y$. Using Corollary 2.3 we have that the functor $X \mapsto X \oplus X$ has an initial algebra with the carrier $(B + A)^*$. The functor $\varpi_\oplus : \mathcal{M}_{n,n}(\mathcal{C}) \to \mathcal{M}_{n,n}(\mathcal{C})$ is given by $\varpi_\oplus(X) = A^* \cdot (\mathbf{I} + B \cdot X)$ and $\varpi_\oplus(f) = \mathsf{Id}_{A^*} \cdot (\mathsf{Id}_1 + \mathsf{Id}_B \cdot f)$. There exists $\eta : \varpi_\oplus \to F$ a natural isomorphism where $F(X) = A^* + (A^* \cdot B) \cdot X$. Using again Corollary 2.3, it follows that $\varpi_\oplus$ has an initial algebra with the carrier $(A^* \cdot B)^* \cdot A^*$. But the Diagonal Rule (Proposition 2.7) gives that the functor $\varpi_\oplus$ has an initial algebra with the carrier $(B + A)^*$. Thus by (17.), we have that

$$(B + A)^* \cong A^* \cdot (B \cdot A^*)^*. \qquad \square$$

Observation 3.12 If the matrices from Theorem 3.11 are matrices over the real numbers, then all isomorphisms from Theorem 3.11 are equalities between matrices over the real numbers whenever $*$ is defined.

4 Regular expressions, abstract data types, finite automata

Let Ω be a fixed non-empty alphabet and $\mathsf{RegExp}(\Omega)$ the set of the regular expressions over Ω (the set of all terms over Ω with the operations $+$, $\cdot$, $*$, 0 and 1).
Let $\mathcal{C}$ be a fixed category of abstract data types.

Definition 4.1 An application $\mathsf{type} : \mathsf{RegExp}(\Omega) \to |\mathcal{C}|$ is called *an interpretation of the the regular expressions over* Ω *as* $\mathcal{C}$*–data types* (or just *interpretation*, when $\mathcal{C}$ and Ω are fixed) if it satisfies:

- $\mathsf{type}(0) = 0$;
- $\mathsf{type}(1) = 1$;
- $\mathsf{type}(R + Q) = \mathsf{type}(R) + \mathsf{type}(Q)$;
- $\mathsf{type}(R \cdot Q) = \mathsf{type}(R) \cdot \mathsf{type}(Q)$;
- $\mathsf{type}(R^*) = \mathsf{type}(R)^*$; $\square$

To give an interpretation it is enough to give an application $\mathsf{type} : \Omega \to |\mathcal{C}|$ which can be extended canonically to an interpretation. Let type be a fixed interpretation.
Let R be a regular expression.

Definition 4.2 The *language* of R, $\sigma(R) \subseteq \Omega^\star$ is defined inductively as:

1. $\sigma(0) = \emptyset$;

2. $\sigma(1) = \{1\}$;
3. $\sigma(\alpha) = \{\alpha\}$, for any $\alpha \in \Omega$;
4. $\sigma(R_1 + R_2) = \sigma(R_1) \cup \sigma(R_2)$;
5. $\sigma(R_1 \cdot R_2) = \sigma(R_1)\sigma(R_2)$;
6. $\sigma(R^*) = (\sigma(R))^*$;

where $\Omega^\star$ is the free monoid generated by Ω (the monoid of words over the alphabet Ω). □

Let Q be a regular expression. We define $\mathbf{E}(Q) \in \{0, 1\}$ by $\mathbf{E}(Q) = 1$ if and only if $\sigma(Q) \neq \emptyset$.

Definition 4.3 Let Q, R be two regular expressions. Q and R are *strongly equivalent*, written $Q \equiv R$, if $\sigma(Q) = \sigma(R)$ and $\mathsf{type}(Q) \cong \mathsf{type}(R)$). □

The relation $\equiv$ is a congruence (it is compatible with $+$, $\cdot$ and $*$). It can be extended to matrices. Two matrices A, B of the same type over $\mathsf{RegExp}(\Omega)$ are in the relation $\equiv$ if and only if $a_{i,j} \equiv b_{i,j}$ where $A = (a_{i,j})$ and $B = (b_{i,j})$.

Lemma 4.4 Let R be a regular expression. Then $R \equiv 0$ if and only if $\sigma(R) = \emptyset$. □

On matrices over $\mathsf{RegExp}(\Omega)$ we define $+$, $\cdot$, $*$, $0_{n,m}$, $\mathbf{I}_n$ in the same way as for matrices over the objects of $\mathcal{C}$. We also denote with $\mathcal{M}_{n,m}(T)$ the set of $n \times m$ matrices over the set T.

Theorem 4.5 Theorem 3.11 is true if we replace $\cong$ with $\equiv$ and A, B, C with matrices of appropriate types over $\mathsf{RegExp}(\Omega)$.

Proof. Theorem 3.11 and [10]. □

We recall Tarjan's definition [16] of an unambiguous regular expression.

Definition 4.6 We define inductively that R is an *unambiguous regular expression* by:

1. 1, 0 and $\alpha \in \Omega$ are unambiguous regular expressions;
2. $R_1 + R_2$ is unambiguous if $\sigma(R_1) \cap \sigma(R_2) = \emptyset$ and R_1, R_2 are unambiguous regular expressions;
3. $R_1 \cdot R_2$ is unambiguous if each $w \in \sigma(R_1)\sigma(R_2)$ is uniquely decomposable in $w = w_1 w_2$ with $w_i \in \sigma(R_i)$ and R_1, R_2 are unambiguous regular expressions;
4. R_1^* is unambiguous if $R_1 \neq 1$ and each nonempty $w \in \sigma(R_1^*)$ is uniquely decomposable into $w = w_1 w_2 \ldots w_k$ with $w_i \in \sigma(R_1)$ and R_1 is unambiguous regular expression. □

Observation 4.7 If R^* is an unambiguous regular expression then $1 \notin \sigma(R)$. □

We recall from [16] the definition of equational characterisation for a regular expression, but our relation "$\equiv$" has another meaning.

Definition 4.8 An unambiguous regular expression Q is *equationally characterised* in terms of unambiguous regular expressions Q_1, Q_2, ..., Q_q if $Q_1 = Q$ and there are $h : \Omega \times [q] \to [q]$, and $\mathbf{D} : \{Q_1, \ldots, Q_q\} \to \{0, 1\}$ such that

$$Q_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot Q_{h(\alpha,i)} + \mathbf{D}(Q_i) \tag{2}$$

for any $i \in [q]$. We refer to (2) as an *equational characterisation* of Q. □

With $[q]$ we denote the set of numbers 1, 2, ..., q.
Let R_i be unambiguous regular expressions such that $R_i \equiv Q_i$. Then

$$R_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot R_{h(\alpha,i)} + \mathbf{D}(R_i)$$

is an equational characterisation for R_1 where $\mathbf{D}(R_i) = \mathbf{D}(Q_i)$.
Let Q be an unambiguous regular expression. Then $1 \in \sigma(Q)$ if and only if $\mathbf{D}(Q) = 1$ in any equational characterisation of Q.

Definition 4.9 We call a *deterministic automaton* a structure $\mathcal{A} = (u, A, v)$ where u, v are column vectors of dimension q with elements in $\{0, 1\}$ and $A = (a_{i,j})$ is a $q \times q$–matrix with elements regular expression of the form $\sum_{\alpha \in U} \alpha$ for some $U \subseteq \Omega$ such that $\sum_{j \in [q]} a_{i,j}$ is unambiguous regular expression. A deterministic automaton is *complete* if $\sigma(\sum_{j \in [q]} a_{i,j}) = \Omega$.
The *regular expression associated* to the deterministic automaton $\mathcal{A}$ is $u^T \cdot A^* \cdot v$ and the *language* of automaton is $\sigma(u^T \cdot A^* \cdot v)$. □

This definition is a version of a definition from [10] and is equivalent to the classical definition of an automaton over an alphabet Ω as found in [9, 12].

Definition 4.10 A deterministic automaton $\mathcal{A} = (u, A, v)$ is *accessible* if $\bigcup_{n \geq 0} S_n = [q]$ where $S_0 = \{i \mid u_i = 1\}$ and $S_{n+1} = S_n \cup \{j \mid \exists i \in S_n,\ a_{i,j} \neq 0\}$. □

Definition 4.11 The *deterministic automaton associated* to the equational characterisation (2) of Q is $\mathcal{A} = (u,\ A,\ v)$ where $A = (a_{k,l})_{k,l \in [q]}$ with $a_{k,l} = \mathbf{E}(Q_l) \cdot \sum_{\substack{\alpha \in \Omega, \\ h(\alpha,k)=l}} \alpha$, $u = (1, 0, \ldots, 0)^T$, $v = (v_1, \ldots, v_q)^T$, $v_i = \mathbf{D}(Q_i)$. It can be seen that $\mathcal{A}$ is a deterministic automaton. □

Definition 4.12 The *complete deterministic automaton associated* to the equational characterisation (2) of Q is $\mathcal{A} = (u,\ A,\ v)$ where $A = (a_{k,l})_{k,l \in [q]}$ with $a_{k,l} = \sum_{\substack{\alpha \in \Omega, \\ h(\alpha,k)=l}} \alpha$, $u = (1, 0, \ldots, 0)^T$, $v = (v_1, \ldots, v_q)^T$, $v_i = \mathbf{D}(Q_i)$. It can be seen that $\mathcal{A}$ is a complete deterministic automaton. □

The application $h : \Omega \times [q] \to [q]$ (from (2)) can be thought of as the transition function of automaton $\mathcal{A}$ which has $[q]$ as the set of states.

We notice that the complete deterministic automaton $\mathcal{A} = (u,\ A,\ v)$ associated to (2) is accessible if and only if $\bigcup_{n \geq 0} S_n = [q]$ where $S_0 = \{i \mid u_i = 1\}$ and $S_{n+1} = S_n \cup \{h(\alpha, i) \mid \alpha \in \Omega,\ i \in S_n\}$.

5 Equational characterisation, associated automaton

In this section we construct a minimal automaton $\mathcal{A} = (u, A, v)$ for an unambiguous regular expression Q such that $Q \equiv u^T \cdot A^* \cdot v$.

Lemma 5.1 Let $u,\ v,\ A,\ s,\ t,\ B$, and X be matrices of appropriate types over $\mathsf{RegExp}(\Omega)$. If $u^T \equiv s^T \cdot X$, $X \cdot A \equiv B \cdot X$, and $t \equiv X \cdot v$ then $u^T \cdot A^* \cdot v \equiv s^T \cdot B^* \cdot t$.

Proof. Because $X \cdot A \equiv B \cdot X$ it follows, using Theorem 4.5, that $X \cdot A^* \equiv B^* \cdot X$. Then

$$u^T \cdot A^* \cdot v \equiv s^T \cdot X \cdot A^* \cdot v \equiv s^T \cdot B^* \cdot X \cdot v \equiv s^T \cdot B^* \cdot t \qquad \square$$

This Lemma is the *key lemma* to pass from an automaton $\mathcal{A}$ with n states to an automaton $\mathcal{B}$ with m states such that the unambiguous regular expressions associated to $\mathcal{A}$ and $\mathcal{B}$ are strongly equivalent. Kozen [10] also uses this result but without mentioning it explicitly.

Suppose that Q and R are unambiguous regular expressions such that $\sigma(Q) \neq \emptyset$ and $\sigma(R) \neq \emptyset$. Let

$$Q_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot Q_{h(\alpha,i)} + \mathbf{D}(Q_i), \quad i \in [q], \tag{3}$$

be an equational characterisation of $Q = Q_1$ such that

$$Q_1 \equiv u^T \cdot A^* \cdot v,$$

where $\mathcal{A} = (u,\ A,\ v)$ is the deterministic automaton associated to (3).

We do the same for R. Let

$$R_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot R_{f(\alpha,i)} + \mathbf{D}(R_i), \quad i \in [r], \tag{4}$$

be an equational characterisation of $R = R_1$ such that

$$R_1 \equiv s^T \cdot B^* \cdot t,$$

where $\mathcal{B} = (s,\ B,\ t)$ is the deterministic automaton associated to (4) ($B = (b_{k,l})_{k,l \in [r]}$ with $b_{k,l} = \mathbf{E}(R_l) \cdot \sum_{\substack{\alpha \in \Omega, \\ f(\alpha,k)=l}} \alpha$, $s = (1, 0, \ldots, 0)^T$, $t = (t_1, \ldots, t_r)^T$, $t_i = \mathbf{D}(R_i)$).

We now construct an equational characterisation for $Q + R$ such that $Q + R \equiv P$, where P is the regular expression associated to the deterministic automaton which corresponds to the equational characterisation of $Q + R$.

Lemma 5.2 Let Q, R be an unambiguous regular expressions as before. Suppose that $Q+R$ is an unambiguous regular expression. Then there is an equational characterisation

$$P_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,i)} + \mathbf{D}(P_i), \quad i \in [p] \tag{5}$$

for $P_1 = Q + R$ such that $P_1 \equiv x^T \cdot C^* \cdot y$, where $\mathcal{C} = (x,\ C,\ y)$ is the deterministic automaton associated to (5) ($C = (c_{k,l})_{k,l \in [r]}$ with $c_{k,l} = \mathbf{E}(P_l) \cdot \sum_{\substack{\alpha \in \Omega, \\ g(\alpha,k)=l}} \alpha$, $x = (1, 0, \ldots, 0)^T$, $y = (y_1, \ldots, y_p)^T$, $y_i = \mathbf{D}(P_i)$).
Moreover, the complete automaton associated to (5) is accessible.

Proof. If $i \in [q]$ and $m \in [r]$, then

$$Q_i + R_m \equiv \sum_{\alpha \in \Omega} \alpha \cdot (Q_{h(\alpha,i)} + R_{f(\alpha,m)}) + \mathbf{D}(Q_i) + \mathbf{D}(R_m),$$

using commutativity of $+$ and distributivity of $\cdot$ on $+$. If $Q_i + R_m$ is an unambiguous expression, then the expressions $Q_{h(\alpha,i)} + R_{f(\alpha,m)}$, $\alpha \in \Omega$ and $\mathbf{D}(Q_i) + \mathbf{D}(R_m)$ are unambiguous.

Let $z\colon [q] \times [r] \to \mathcal{P}([q] \times [r])$ be an application given by

$$z(i, m) = \{(g(\alpha, i), f(\alpha, m)) \mid \alpha \in \Omega\},$$

and $Z_0 = \{(1,1)\}$, $Z_{k+1} = Z_k \cup \bigcup_{w \in Z_k} z(w)$. Let $Z = \bigcup_{k \geq 0} Z_k$ and $p = |Z|$. Then $Z = \{(i_1, m_1), \ldots, (i_p, m_p)\}$, where $(i_1, m_1) = (1,1)$. Because $Q_1 + R_1$ is an unambiguous regular expression, we have for all $k \in [p]$ that $Q_{i_k} + R_{m_k}$ and $\mathbf{D}(Q_{i_k}) + \mathbf{D}(R_{m_k})$ are unambiguous regular expressions.

Let $P_k = Q_{i_k} + R_{m_k}$ and $\mathbf{D}(P_k) = \mathbf{D}(Q_{i_k}) + \mathbf{D}(R_{m_k})$ for all $k \in [p]$. Then P_k is an unambiguous regular expression and there is $g : \Omega \times [p] \to [p]$ such that

$$P_k \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,k)} + \mathbf{D}(P_k).$$

The numbers $g(\alpha, k)$ are chosen such that

$$g(\alpha, k) = j \;\Leftrightarrow\; (i_j, m_j) = (h(\alpha, i_k), f(\alpha, m_k)). \tag{6}$$

Let $y^1 = (y^1_1, \ldots, y^1_p)^T$ and $y^2 = (y^2_1, \ldots, y^2_p)^T$ such that $y^1_k = \mathbf{D}(Q_{i_k})$ and $y^2_k = \mathbf{D}(R_{m_k})$. Then $y \equiv y^1 + y^2$ because $\mathbf{D}(Q_{i_k}) + \mathbf{D}(R_{m_k})$ is an unambiguous regular expression. We prove that:

1. $x^T \cdot C^* \cdot y^1 \equiv u^T \cdot A^* \cdot v$ and
2. $x^T \cdot C^* \cdot y^2 \equiv s^T \cdot B^* \cdot t$.

For 1. we find $X \in \mathcal{M}_{p,q}(\{0,1\})$ such that

$$X \cdot A \equiv C \cdot X, \;\; y^1 \equiv X \cdot v \text{ and } u^T \equiv x^T \cdot X. \tag{7}$$

Take

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_p \end{pmatrix} \quad X_k = (x_{k,1}, \ldots, x_{k,q}),\; x_{k,l} \in \{0,1\},$$

where $x_{k,l} = 1$ if and only if $i_k = l$ and $\sigma(Q_l) \neq \emptyset$. With this X the relations (7) are true. It follows, using Lemma 5.1, that $x^T \cdot C^* \cdot y^1 \equiv u^T \cdot A^* \cdot v$.
In the same way we can prove that $x^T \cdot C^* \cdot y^2 = s^T \cdot B^* \cdot t$.
Using these two relations we can prove that $P \equiv x^T \cdot C^* \cdot y$.

$$P = Q + R \equiv u^T \cdot A^* \cdot v + s^T \cdot B^* \cdot t \equiv$$

$$x^T \cdot C^* \cdot y^1 + x^T \cdot C^* \cdot y^2 \equiv x^T \cdot C^* \cdot (y^1 + y^2) \equiv x^T \cdot C^* \cdot y.$$

To prove that the complete automaton associated to (5) is accessible it is enough to show that $[p] \subseteq \bigcup_{n \geq 0} S_n$ where $S_0 = \{i \mid x_i = 1\} = \{1\}$ and $S_{n+1} = S_n \cup \{g(\alpha, k) \mid \alpha \in \Omega,\; k \in S_n\}$. Let

$k \in [p]$. Then there is $n \geq 0$ such that $(i_k, m_k) \in Z_n$, and so there are $k_0 = 1$, k_1, …, $k_n = k \in [p]$ and α_0, …, $\alpha_{n-1} \in \Omega$ such that $(i_{k_{j+1}}, m_{k_{j+1}}) = (h(\alpha_j, i_{k_j}), f(\alpha_j, m_{k_j}))$. Finnaly, using (6), we obtain $k_{j+1} = g(\alpha_j, k_j)$, so $k \in S_n$. $\square$

We construct now an equational characterisation for $Q \cdot R$ such that $Q \cdot R \equiv P$, where P is the regular expression associated to the deterministic automaton which corresponds to the equational characterisation of $Q \cdot R$.

Lemma 5.3 Let Q, R be unambiguous regular expressions as before. Suppose that $Q \cdot R$ is an unambiguous regular expression. Then there is an equational characterisation

$$P_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,i)} + \mathbf{D}(P_i), \quad i \in [p] \tag{8}$$

for $P_1 = Q \cdot R$ such that $P_1 \equiv x^T \cdot C^* \cdot y$ where $\mathcal{C} = (x, C, y)$ is the deterministic automaton associated to (8).
Moreover, the complete automaton associated to (8) is accessible.

Proof. Let $1 \leq i \leq q$, $n \in \mathbf{N}$ and $1 \leq m_1 < m_2 < \ldots < m_n \leq r$. Suppose that the expression $Q_i \cdot R + \sum_{j=1}^{n} R_{m_j}$ is unambiguous, and let $[\![n, i]\!] = [n]$ if $\mathbf{D}(Q_i) = 0$ or $[\![n, i]\!] = [n] \cup \{0\}$ if $\mathbf{D}(Q_i) = 1$, and let $m_0 = 1$. Then:

$$Q_i \cdot R + \sum_{j=1}^{n} R_{m_j} \equiv \sum_{\alpha \in \Omega} \alpha \cdot \left(Q_{h(\alpha,i)} \cdot R + \sum_{j \in [\![n,i]\!]} R_{f(\alpha,m_j)} \right) + \sum_{j \in [\![n,i]\!]} \mathbf{D}(R_{m_j})$$

and the regular expressions $Q_{h(\alpha,i)} \cdot R + \sum_{j \in [\![n,i]\!]} R_{f(\alpha,m_j)}$, for $\alpha \in \Omega$ and $\sum_{j \in [\![n,i]\!]} \mathbf{D}(R_{m_j})$ are unambiguous.

Let $z \colon [q] \times \mathcal{P}([r]) \to \mathcal{P}([q] \times \mathcal{P}([r]))$ given by

$$z(i, \{m_1, m_2, \ldots, m_n\}) = \left\{ \left(h(\alpha, i),\ \{f(\alpha, m_j) \mid j \in [\![n, i]\!],\ \sigma(R_{f(\alpha,m_j)}) \neq \emptyset\} \right) \ \mid \alpha \in \Omega \right\}$$

Let $Z_0 = \{(0, \emptyset)\}$, $Z_{k+1} = Z_k \cup \bigcup_{t \in Z_k} z(t)$. Let $Z = \bigcup_{k \geq 0} Z_k$ and $p = |Z|$, then

$$Z = \left\{ \left(i_1, \{m_1^i, \ldots, m_{n_1}^i\} \right), \ \ldots, \ \left(i_p, \{m_1^p, \ldots, m_{n_p}^p\} \right) \right\}$$

such that $\left(i_1, \{m_1^i, \ldots, m_{n_1}^i\} \right) = (1, \emptyset)$.

Let $m_0^k = 1$, $P_k = Q_{i_k} \cdot R + \sum_{j=1}^{n_k} R_{m_j^k}$ and $\mathbf{D}(P_k) = \sum_{j \in [\![n_k, i_k]\!]} \mathbf{D}(R_{m_j^k})$ for all $k \in [p]$. Then P_k and $\mathbf{D}(P_k)$ are unambiguous expressions and there is $g : \Omega \times [p] \to [p]$ such that

$$P_k \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,i)} + \mathbf{D}(P_k).$$

The numbers $g(\alpha, k)$ are chosen such that

$$g(\alpha, k) = z \ \Leftrightarrow \ (i_z = h(\alpha, i_k) \text{ and}$$
$$\left\{ m_1^z, \ \ldots, \ m_{n_z}^z \right\} = \left\{ f(\alpha, m_j^k) \mid j \in [\![n_k, i_k]\!],\ \sigma(R_{f(\alpha,m_j^k)}) \neq \emptyset \right\} \Big). \tag{9}$$

We prove that the relation $x^T \cdot C^* \cdot y \equiv Q \cdot R$ is true. We have

$$Q \cdot R \equiv u^T \cdot A^* \cdot v \cdot s^T \cdot B^* \cdot t \equiv (u^T, 0) \cdot \begin{pmatrix} A^* & A^* \cdot v \cdot s^T \cdot B^* \\ 0 & B^* \end{pmatrix} \cdot \begin{pmatrix} 0 \\ t \end{pmatrix} \equiv$$

$$(u^T, 0) \cdot \begin{pmatrix} A & v \cdot s^T \\ 0 & B \end{pmatrix}^* \cdot \begin{pmatrix} 0 \\ t \end{pmatrix} \equiv (u^T, 0) \cdot \left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} + J \right)^* \cdot \begin{pmatrix} 0 \\ t \end{pmatrix} \equiv$$

$$(u^T, 0) \cdot J^* \cdot \left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot J^* \right)^* \cdot \begin{pmatrix} 0 \\ t \end{pmatrix},$$

where

$$J = \begin{pmatrix} 0 & v \cdot s^T \\ 0 & 0 \end{pmatrix}.$$

It follows that

$$Q \cdot R \equiv (u^T, 0) \cdot J^* \cdot \left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot J^* \right)^* \cdot \begin{pmatrix} 0 \\ t \end{pmatrix}. \tag{10}$$

We find $X \in \mathcal{M}_{p,q+r}(\{0, 1\})$ such that :

$$X \cdot \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot J^* = C \cdot X, \quad (u^T, 0) \cdot J^* = x^T \cdot X \text{ and } X \cdot \begin{pmatrix} 0 \\ t \end{pmatrix} = y. \tag{11}$$

Let

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_p \end{pmatrix} \text{ such that } X_k \text{ is the row } (X_k^1, X_k^2),$$

where

$$X_k^1 = (x_{k,1}, \ldots, x_{k,q}), \ x_{k,j} = 1 \Leftrightarrow i_k = j \text{ and } Q_j \neq \emptyset;$$

$$X_k^2 = (x_{k,q+1}, \ldots, x_{k,q+r}), x_{k,q+j} = 1 \text{ iff } \left(j \in \{m_1^k, \ldots, m_{n_k}^k\}\right) \text{ or } (j = 1 \text{ and } \mathbf{D}(Q_{i_k}) = 1).$$

At least one of the sentences separated with 'or' is false because P_k is an unambiguous regular expression. With this X the requirements (11) are true. It follows, using Lemma 5.1, that

$$(u^T, 0) \cdot J^* \cdot \left(\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \cdot J^* \right)^* \cdot \begin{pmatrix} 0 \\ t \end{pmatrix} \equiv x^T \cdot C^* \cdot y.$$

Using the conditions (10) now we obtain $P = Q \cdot R \equiv x^T \cdot C^* \cdot y$.

The proof of the fact that the complete automaton associated to (8) is accessible is similar to the proof of Lemma 5.2, using (9) and the definition of the sets Z_k. □

We now construct an equational characterisation for $Q \cdot Q^*$ such that $Q \cdot Q^* \equiv P$, where P is the regular expression associated to the deterministic automaton which corresponds to the equational characterisation of $Q \cdot Q^*$.

Lemma 5.4 Let Q be an unambiguous regular expression as before. Suppose that Q^* is an unambiguous regular expression. Then there is an equational characterisation

$$P_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,i)} + \mathbf{D}(P_i), \quad i \in [p] \tag{12}$$

for $P_1 = Q \cdot Q^*$ such that $P_1 \equiv x^T \cdot C^* \cdot y$ where $\mathcal{C} = (x, C, y)$ is the deterministic automaton associated to (12).

Moreover, the complete automaton associated to (12) is accessible.

Proof. Because Q^* is an unambiguous regular expression, it follows that $1 \notin \sigma(Q)$ (or $\mathbf{D}(Q) = 0$). We have

$$Q^* \equiv 1 + Q \cdot Q^* \equiv \sum_{\alpha \in \Omega} \alpha \cdot Q_{h(\alpha,1)} \cdot Q^* + 1.$$

Let $n \geq 1$ and $1 \leq m_1 <, \ldots, < m_n \leq q$. Suppose that $\sum_{i=1}^{n} Q_{m_i} \cdot Q^*$ is an unambiguous regular expression. We denote $m = (m_1, \ldots, m_n)$ and let $\mathbf{D}(m) = 1$ if and only if there is $i \in [n]$ such that $\mathbf{D}(Q_{m_i}) = 1$ (there is at most one i with this property) otherwise $\mathbf{D}(m) = 0$. Let $[\![n, m]\!] = [n]$ if $\mathbf{D}(m) = 0$, or $[\![n, m]\!] = [n] \cup \{0\}$ if $\mathbf{D}(m) = 1$. With this notations we have:

- $\sum_{i=1}^{n} Q_{m_i} \cdot Q^* \equiv \sum_{\alpha \in \Omega} \alpha \cdot \sum_{i \in [\![n,m]\!]} Q_{h(\alpha,m_i)} \cdot Q^* + \mathbf{D}(m)$ and
- $\sum_{i \in [\![n,m]\!]} Q_{h(\alpha,m_i)} \cdot Q^*$ is an unambiguous regular expression for each $\alpha \in \Omega$.

where $m_0 = 1$.

Let $z \colon \mathcal{P}([q]) \to \mathcal{P}(\mathcal{P}([q]))$ be the application given by:

$$z(\{m_1, \ldots, m_n\}) = \Big\{\{h(\alpha, m_i) \mid i \in [\![n, m]\!],\ \sigma(Q_{h(\alpha,m_i)}) \neq \emptyset\} \mid \alpha \in \Omega\Big\}$$

and let $Z_0 = \{\{1\}\}$, $Z_{k+1} = Z_k \cup \bigcup_{w \in Z_k} z(w)$, $Z = \bigcup_{k \geq 0} Z_k$, $p = |Z|$ and $Z = \Big\{\{m^1_1, \ldots, m^1_{n_1}\}, \ldots, \{m^p_1, \ldots, m^p_{n_p}\}\Big\}$ with $\{m^1_1, \ldots, m^1_{n_1}\} = \{1\}$. In the same way as before we define m^k, $\mathbf{D}(m^k)$ and m^k_0.

Let for all $k \in [p]$ $P_k = \sum_{i=1}^{n_k} Q_{m^k_i} \cdot Q^*$, and $\mathbf{D}(P_k) = \mathbf{D}(m^k)$. It follows that P_k and $\mathbf{D}(P_k)$ for all $k \in [p]$ are unambiguous regular expressions and there is $g : \Omega \times [p] \to [p]$ such that

$$P_k \equiv \sum_{\alpha \in \Omega} \alpha \cdot P_{g(\alpha,k)} + \mathbf{D}(P_k).$$

The numbers $g(\alpha, k)$ are chosen such that

$$g(\alpha, k) = e \ \Leftrightarrow\ \Big\{m^e_1, \ldots, m^e_{n_e}\Big\} = \Big\{h(\alpha, m^k_j) \mid j \in [\![n_k, m^k]\!],\ \sigma(Q_{h(\alpha,m^k_j)}) \neq \emptyset\Big\}. \tag{13}$$

We prove that the relation $x^T \cdot C^* \cdot y \equiv Q \cdot Q^*$ is true. We have:

$$Q \cdot Q^* \equiv u^T \cdot A^* \cdot v \cdot (u^T \cdot A^* \cdot v)^* \equiv$$
$$u^T \cdot A^* \cdot (v \cdot u^T \cdot A^*)^* \cdot v \equiv$$
$$u^T \cdot (A + v \cdot u^T)^* \cdot v \equiv$$
$$u^T \cdot (v \cdot u^T)^* \cdot (A \cdot (v \cdot u^T)^*)^* \cdot v.$$

It follows that

$$Q \cdot Q^* \equiv u^T \cdot (v \cdot u^T)^* \cdot (A \cdot (v \cdot u^T)^*)^* \cdot v. \tag{14}$$

We want to find $X \in \mathcal{M}_{p,q}(\{0,1\})$ such that

$$u^T \cdot (v \cdot u^T)^* \equiv x^T \cdot X, \quad X \cdot (A \cdot (v \cdot u^T)^*) \equiv C \cdot X, \text{ and } X \cdot v \equiv y. \tag{15}$$

Take

$$X = \begin{pmatrix} X_1 \\ \vdots \\ X_p \end{pmatrix}, \quad X_k = (x_{k,1}, \ldots, x_{k,q}), \quad x_{k,l} \in \{0,1\},$$

such that $x_{k,l} = 1$ if and only if $l \in \{m_1^k, \ldots, m_{n_k}^k\}$ or ($l = 1$ and $\mathbf{D}(P_k) = 1$). At least one of the sentences connected with 'or' is false. With X as before, it follows that the relations (15) are true. Then Lemma 5.1 gives that

$$u^T \cdot (v \cdot u^T)^* \cdot (A \cdot (v \cdot u^T)^*)^* \cdot v \equiv x^T \cdot C^* \cdot y$$

which implies, using (14), that

$$Q \cdot Q^* \equiv x^T \cdot C^* \cdot y.$$

The proof of the fact that the complete automaton associated to (12) is accessible is similar to the proof of Lemma 5.2, using (13) and the definition of the sets Z_k. □

We can prove now using the above lemmas that an unambiguous regular expression Q has an equational characterisation such that $Q \equiv S$ where S is the regular expression associated to the deterministic automaton which corresponds to the equational characterisation of Q.

Theorem 5.5 Let Q be an unambiguous regular expression. Then Q has an equational characterisation

$$Q_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot Q_{h(\alpha,i)} + \mathbf{D}(Q_i), \quad i \in [q], \tag{16}$$

in terms of $Q_1, Q_2, \ldots, Q_q$ such that

$$Q_1 \equiv u^T \cdot A^* \cdot v,$$

where $\mathcal{A} = (u, A, v)$ is the complete deterministic automaton associated to (16).
Moreover, $\mathcal{A}$ is accessible.

Proof. If $\sigma(Q) = \emptyset$, then the statement is true. Suppose that $\sigma(Q) \neq \emptyset$.

We first prove by induction on the structure of Q that Q has an equational characterisation

$$Q_i \equiv \sum_{\alpha \in \Omega} \alpha \cdot Q_{h(\alpha,i)} + \mathbf{D}(Q_i), \quad i \in [q], \tag{17}$$

in terms of $Q_1, Q_2, \ldots, Q_q$ such that

$$Q = Q_1 \equiv u^T \cdot B^* \cdot v,$$

where $\mathcal{B} = (u, B, v)$ is the deterministic automaton associated to (17).
If $Q \in \Omega \cup \{0, 1\}$ it easy to see that it is true. For $+$, $\cdot$, $*$ it follows using Lemmas 4.4, 5.2, 5.3 and 5.4. It also follows that the complete deterministic automaton $\mathcal{A} = (u, A, v)$ associated to (17) is accessible.

Next, we see that $Q \equiv u^T \cdot A^* \cdot v$ follows from $u^T \cdot B^* \cdot v \equiv u^T \cdot A^* \cdot v$.
To prove the latter, it is enough to find X such that

$$u^T \cdot X \equiv u^T, \;\; X \cdot B \equiv A \cdot X, \;\; X \cdot v \equiv v. \tag{18}$$

Let $X \in \mathcal{M}_{q,q}(\{0,1\})$ such that $x_{i,j} = 1$ if and only if $i = j$ and $\sigma(Q_i) \neq \emptyset$. With this X it follows that the relations (18) are true. Then, using Lemma 5.1, we get that

$$u^T \cdot B^* \cdot v \equiv u^T \cdot A^* \cdot v. \qquad \square$$

Theorem 5.6 Let Q be a unambiguous regular expression, then $Q \equiv u^T \cdot A^* \cdot v$ where $\mathcal{A} = (u,\ A,\ v)$ is a minimal complete deterministic automaton which has $\sigma(Q)$ as its language.

Proof. We first recall from [10] the construction of a minimal automaton $\mathcal{A} = (u, A, v)$ pointing on the fact that $Q \equiv u^T \cdot A^* \cdot v$ can be proved without using the idempotency of $+$. Let $\mathcal{B} = (s,\ B,\ t)$ be a complete accesible deterministic automaton given by Theorem 5.5 such that $Q \equiv s^T \cdot B^* \cdot t$, where $B = (b_{k,l})_{k,l\in[q]}$ and $b_{k,l} = \sum\limits_{\substack{\alpha\in\Omega \\ h(\alpha,k)=l}} \alpha$.

In [9, 12] the unique minimal complete automaton is obtained as a qoutient by the equivalence relation $\approx$ of an accessible complete determinist automaton defined on the set of states by $k \approx l \Leftrightarrow \sigma(e_k^T \cdot A^* \cdot v) = \sigma(e_l^T \cdot A^* \cdot v)$ (the languages of the states k and l are the same) where e_k is the column vector which has 1 in row k and 0 elsewhere. It follows that if $k \approx l$ then

$$h(\alpha, k) \approx h(\alpha, l), \ \ \forall\alpha \in \Omega \text{ and } t_k = t_l \tag{19}$$

Let $\widehat{n}_1, \widehat{n}_2, \ldots \widehat{n}_p$ be the equivalence classes of the relation $\approx$ such that $1 \in \widehat{n}_1$.

Let $A = (a_{i,j})_{i,j\in[p]}$ be given by

$$a_{i,j} = \sum_{m\in\widehat{n}_j} b_{n_i,m}$$

and let $u = (1,\ 0,\ \ldots,\ 0)^T$ and $v = (t_{n_1},\ \ldots,\ t_{n_p})^T$.
If $l \approx k$, then we have

$$\sum_{m\in\widehat{n}_j} b_{l,m} \equiv \sum_{m\in\widehat{n}_j} b_{k,m}. \tag{20}$$

Because $\mathcal{B}$ is a complete deterministic automaton we have that any $b_{i,j}$ has the form $\sum\limits_{\alpha\in U} \alpha$ for an $U \subseteq \Omega$ and $\sum\limits_{m\in\widehat{n}_j} b_{l,m}$ is unambiguous. So, to prove (20) it is enough to show that

$$V = \sigma(\sum_{m\in\widehat{n}_j} b_{l,m}) = \sigma(\sum_{m\in\widehat{n}_j} b_{k,m}) = T.$$

If $\alpha \in V$, then there is $m \in \widehat{n}_j$ such that $h(\alpha, l) = m$. Because $l \approx k$ it follows $h(\alpha, l) \approx h(\alpha, k)$. But $\alpha \in \sigma(b_{k,h(\alpha,k)})$, implies $\alpha \in T$. The converse inclusion is proved similarly.

From (19) and (20) it follows that u, A and v are well defined. Also $(u,\ A,\ v)$ is a complete deterministic automaton.
We want to prove that $s^T \cdot B^* \cdot t \equiv u^T \cdot A^* \cdot v$. For this we find $X \in \mathcal{M}_{q,p}(\{0, 1\})$ such that

$$B \cdot X \equiv X \cdot A, \ u^T \equiv s^T \cdot X \text{ and } t \equiv X \cdot v.$$

Let $X = (X_1,\ X_2,\ \ldots,\ X_p)$ where X_l is the column vector $(x_{1,l},\ \ldots,\ x_{q,l})^T$ with $x_{k,l} = 1$ if and only if $k \in \widehat{n}_l$.

Let $B \cdot X = (\beta_{k,j})_{\substack{k\in[q] \\ j\in[p]}}$. Then $\beta_{k,j} \equiv \sum\limits_{m=1}^{q} b_{k,m} \cdot x_{m,j} \equiv \sum\limits_{m\in\widehat{n}_j} b_{k,m}$.

Let $X \cdot A = (\gamma_{k,j})_{\substack{k\in[q]\\ j\in[p]}}$. Then $\gamma_{k,j} \equiv \sum_{i=1}^{p} x_{k,i} \cdot a_{i,j} \equiv \sum_{\substack{i=1\\ k\in\widehat{n}_i}}^{p} a_{i,j} \equiv \sum_{m\in\widehat{n}_j} b_{n_i,m}$, where $i \in [p]$ is the unique number such that $k \in \widehat{n}_i$. Using (20), it follows that $B \cdot X \equiv X \cdot A$.

Also $u^T \equiv s^T \cdot X$ because $1 \in \widehat{n}_1$. Let $X \cdot v = (\beta_1, \ldots, \beta_q)^T$. We have

$$\beta_l \equiv \sum_{j=1}^{p} x_{l,j} \cdot v_j = \sum_{\substack{j=1\\ l\in\widehat{n}_j}} v_j \equiv t_{n_j}$$

where $j \in [p]$ is unique such that $l \in \widehat{n}_j$. Because $t_l = t_{n_j}$, we get $X \cdot v \equiv t$.

Therefore, it follows using Lemma 5.1, that $Q \equiv u^T \cdot A^* \cdot v$, and we also have that $\mathcal{A}$ is a minimal complete automaton. □

Theorem 5.7 Let Q and R be two unambiguous regular expressions such that $\sigma(Q) = \sigma(R)$. Then $Q \equiv R$.

Proof. By Theorem 5.6 we have $Q \equiv u^T \cdot A^* \cdot v$ and $R \equiv s^T \cdot B^* \cdot v$ where $\mathcal{A} = (u, A, v)$ is a minimal complete automaton which has as language $\sigma(Q)$ and $\mathcal{B} = (s, B, t)$ is a minimal complete automaton which has as language $\sigma(R)$. Because $\sigma(Q) = \sigma(R)$ and the automata are minimal complete deterministic, they are the same, up to a permutation of states. It follows from [10] that $u^T \cdot A^* \cdot v \equiv s^T \cdot B^* \cdot t$, hence

$$Q \equiv R.$$ □

Corollary 5.8 If two unambiguous regular expressions have the same language then:

1. they specify the same (up to isomorphism) abstract data type.
2. they are equal when are interpreted as real numbers.
3. they yield the same values when are interpreted in any algebraic structure (with operations $+$, $\cdot$, *, 0, 1) that satisfies Theorem 3.11 □

Acknowledgements. I am grateful to Professor Roland Backhouse for the guidance in this research, and valuable comments. I would also like to thank the anonymous referees for many useful comments that led to an improvement of this paper.

References

[1] A. Asperti and G. Longo. *Categories, Types, and Structures: An Introduction to Category Theory for the Working Computer Scientist.* The MIT Press, 1991.

[2] R. C. Backhouse, M. Bijsterveld, R. van Geldrop, and J.C.S.P. van der Woude. Categorical fixed point calculus. In D. Pitt, D.E. Rydeheard, and P. Johnstone, editors, *Category Theory and Computer Science, 6th International Conference*, volume 953 of *LNCS*, pages 159–179. Springer-Verlag, 1995.

[3] R. C. Backhouse, M. Bijsterveld, R. van Geldrop, and J.C.S.P. van der Woude. Category theory as coherently constructive lattice theory. Department of Mathematics and Computing Science, Eindhoven University of Technology. Working document. Available via World-Wide Web at `http://www.win.tue.nl/cs/wp/papers`, 1995.

[4] R. Balbes and P. Dwinger. *Distributive Lattices.* University of Missoury Press, 1974.

[5] M. Barr and C. Wells. *Category Theory for Computer Science.* Prentice Hall, 1995.

[6] A. Carboni, S. Leck, and R. F. C. Walters. Introduction to extensive and distributive categories. *Journal of Pure and Applied Algebra*, 84(2):155–158, 1993.

[7] J. R. B. Cockett. Introduction to distributive categories. *Mathematical Structure in Computer Science*, 3:277–307, 1993.

[8] J. H. Conway. *Regular Algebra and Finite Machines.* Chapman and Hall, London, 1971.

[9] J. E. Hopcroft and J. D. Ullman. *Introduction to Automata Theory, Languages, and Computation.* Addison–Wesley, Reading, Mass, 1979.

[10] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Information and Computation*, 110(2):366–390, 1 May 1994.

[11] J. Lambek and P.J. Scott. *Introduction to Higher Order Categorical Logic.* Cambridge University Press, 1986.

[12] H. Lewis and C. Papadimitriou. *Elements of the Theory of Computation.* Prentice Hall, Englewood, NJ, 1981.

[13] R. Loader. Equational theories for inductive types. *Annals of Pure and Applied Logic*, 84(3):175–217, 1997.

[14] S. MacLane. *Categories for the Working Mathematician.* Springer–Verlag New York, 1971.

[15] A. M. Pitts. Categorical logic. Technical Report 367, University of Cambridge Computer Laboratory, May 1995. 94 pages.

[16] R. E. Tarjan. A unified approach to path problems. *Journal of the ACM*, 28(3):577–593, July 1981.