CHURCH-ROSSER PROOFS IN KLEENE ALGEBRA AND ALLEGORIES

GEORG STRUTH

ABSTRACT. We prove Church-Rosser statements in Kleene algebra in the spirit of the point-free style of functional programming. Proofs of Church-Rosser theorems are simple and general, using only algebraic properties of the regular operations. They are fixed point-based, induction-free and often amenable to automata, hence suited to mechanization. In the strip lemma of the λ-calculus, the term and algebra part are cleanly separated. Relating Kleene algebras with allegories explains Church-Rosser diagrams categorially. Using allegoric techniques, we also prove algebraic variants of Newman's lemma and Church-Rosser statements modulo an equivalence relation, in which the well-foundedness assumptions are derived. Here, point-wise techniques are introduced via tabulations, but still the construction avoids the invention of complex induction orderings and measures. Our results can be read as a case study for the possibilities and limitations of point-free allegorial formal methods.

1. INTRODUCTION

Church-Rosser statements are usually proven either logically or in terms of diagrams. Logical proofs are rigorous, but often fail the appropriate level of abstraction and struggle with set-theoretic definitions and arguments. Proof by diagrams are usually abstract, intuitive and revealing, but sometimes not rigorous enough, in particular, when intended for a machine. Logical proofs can be made more abstract by proving lemmata about diagrams, proofs by diagrams more rigorous by translating them to logic, but this convergence requires mathematical insight.

Our main contribution is that Kleene algebra and allegories yield abstract rigorous Church-Rosser proofs. Allegories and Kleene algebras are useful formal methods for the specification and development of hard- and software systems. Intuitively, allegories are either (fragments of) typed relation algebras or categories with relations as arrows and some additional algebraic structure. Kleene algebras are (mono-typed) subalgebras of certain allegories, namely semirings with the additional operation of Kleene star satisfying least pre-fixed point axioms. Kleene algebra is essentially the algebra of regular events, but also the regular operations (union, composition, Kleene star) on set-theoretic relations form a Kleene algebra. Since Church-Rosser proofs use only the regular operations, Kleene algebra seems to be the minimal algebraic machinery to carry them out in a rigorous way. In particular, the Kleene star is introduced very abstractly as a fixed point and without connection to a sum of powers.

Kleene algebra and allegorial proofs are abstract; they deal with relations in a point-free style: relations are first-class citizens of the algebra and not set-theoretically defined via ordered pairs. In functional programming, the point-free style supports reasoning about programs with algebraic and category-theoretic

Key words and phrases. Kleene algebra, Allegory, Rewriting, Church-Rosser theorem, Newman's lemma, Formal Methods.

Research-Report No.146, January 2001, Institut für Informatik, Albert-Ludwigs-Universität Freiburg, Germany.

methods (c.f. [5]). The categorial abstraction from the internals of objects (variables, binders) allows highly structured and generic, but rigorous algebraic proofs that can be visualized by (commuting) diagrams. Generalizing categories to deal with relations leads to allegories [9], a point-free style of reasoning with relations similar to relational algebra and visualization by (semi-commuting) diagrams. Since Kleene algebras are special allegories, the arguments apply. An allegorial point-free style of specification is also implicit in Abrial's B-method [1].

Besides being rigorous and abstract, Kleene algebra pays computationally. One main result of this text are proofs of Church-Rosser theorems without induction via simple fixed point arguments. The proofs are completely arithmetic and not analytic, as in related semirings. They are usually simple, short and concise. The assumption $\leftarrow\rightarrow^* \subseteq \rightarrow^* \leftarrow^*$ instead of $\leftarrow^* \rightarrow^* \subseteq \rightarrow^* \leftarrow^*$, for instance, is almost suggested by the Church-Rosser proof itself. By a result of Kozen [14], large parts of the proof can even be done by automata.

Besides this result, we also prove Church-Rosser results for the Kleene plus, which are interesting for rewriting with non-symmetric transitive relations.

Our second main result concerns algebraic proofs of Newman's lemma and generalized variants of Church-Rosser theorems modulo an equivalence relation [11]. It includes allegorial techniques. To this end, not only the language of Kleene algebra must be extended, but also the point-free style comes to its limit. We therefore use tabulations of allegories as the standard allegorial way of mimicking point-wise reasoning. In particular our proofs for Church-Rosser theorems modulo show that our technique covers not only basic, but also quite advanced statements in the field of rewriting. We generalize the theorem to reasoning about non-symmetric transitive relations and give two proofs for this statements. One allegorial and the other, for a comparison, by proof transformation.

Besides its novelty, our approach has several further benefits. First, well-foundedness assumptions for Newman's lemma can be constructed and need not, as usually, be guessed. Second, the proofs are relatively simple and avoid the invention of complex proof measures. Third, the usual diagrams of rewrite theory are connected with the standard semi-commuting diagrams of allegory theory. Fourth, we demonstrate how allegorial methods are helpful in the strip lemma of the λ-calculus. Fifth, we re able to connect concepts of rewriting both with those of regular languages and with fixed point calculi.

Finally, we also argue that our proofs are well-suited for logical frameworks with integrated decision procedures. Since our approach seems interesting for program verification and specification in general, one can read the paper in several ways. First as a search for conceptual abstract and general Church-Rosser proofs, second as a fixed-point-based approach to mechanized proofs (as opposed to induction) and third and most generally as a case study in Kleene algebra and allegories as formal methods for the point-free specification of hard- and software systems, showing its possibilities and limitations. We have tried to include all important proofs into the paper.

The remainder is organized as follows. Section 2 includes the basics of traditional Church-Rosser statements. Section 3 and section 4 those of semirings and Kleene algebras. Section 5 and section 6 develops the elementary presuppositions for the Church-Rosser proofs of section 7 for the Kleene star of and section 8 for the Kleene plus. Section 9 introduces new structure to adapt the algebraic Church-Rosser statements to standard ones and to define functions. Section 10 introduces allegories. This yields diagrams, typed Kleene algebra terms and well-foundedness assumptions. Section 11 contains allegorial proofs of variants of Newman's lemma. Section 12 translates algebraic Church-Rosser statements to those of rewriting. Section 13 yields an algebraic reconstruction of generalizations of the Church-Rosser theorem modulo. Section 14 contains another proof of such a generalized statement by the traditional technique of proof transformation. Section 15 concerns the Church-Rosser theorem of the λ-calculus. Section 16 discusses the relevance of our approach to mechanized reasoning. Section 17 contains a conclusion.

2. Church-Rosser Basics

We briefly sketch the basic concepts concerning Church-Rosser statements. Let $(A, \to)$ be a *rewrite system* (or abstract reduction system or state transition system) of a set A and a binary set-theoretic relation $\to$ on A. We also speak of A instead of $(A, \to)$ and write $a \to b$ instead of $(a, b) \in \to$. We denote by $\leftarrow$ the converse, by $\to^+$ the transitive closure, by $\to^*$ the reflexive transitive closure and by $\leftrightarrow^*$ the reflexive symmetric transitive closure of $\to$. Juxtaposition of arrows denotes relational composition. The *diamond property* $\Diamond(x_1, x_2, x_3)$, the *weak diamond property* $\Diamond_w(x_1, x_2, x_3)$ and the *Church-Rosser property* $\bigtriangledown(x_1, x_2)$ are defined by the predicates

(1) $$\Diamond(x_1, x_2, x_3) \Leftrightarrow (x_1 \to^* x_2 \wedge x_1 \to^* x_3 \Rightarrow \exists x_4 . x_2 \to^* x_4 \wedge x_3 \to^* x_4),$$

(2) $$\Diamond_w(x_1, x_2, x_3) \Leftrightarrow (x_1 \to x_2 \wedge x_1 \to x_3 \Rightarrow \exists x_4 . x_2 \to^* x_4 \wedge x_3 \to^* x_4),$$

(3) $$\bigtriangledown(x_1, x_2) \Leftrightarrow (x_1 \leftrightarrow^* x_2 \Rightarrow \exists x_3 . x_1 \to^* x_3 \wedge x_2 \to^* x_3).$$

The rewrite system A *has the diamond property,* if $\forall x_1, x_2, x_3 \in A . \Diamond(x_1, x_2, x_3)$, the *weak diamond property* iff $\forall x_1, x_2, x_2 \in A . \Diamond_w(x_1, x_2, x_3)$ and the *Church-Rosser property,* iff $\forall x_1, x_2 \in A . \bigtriangledown (x_1, x_2)$.

Theorem 2.1 (Church-Rosser). *For all rewrite systems A,*

(4) $$\forall x_1, x_2 \in A . \bigtriangledown (x_1, x_2) \Leftrightarrow \forall x_1, x_2, x_3 \in A . \Diamond(x_1, x_2, x_3).$$

The Church-Rosser theorem is usually visualized by the following diagrams.

$$\begin{tikzcd} & x_1 \arrow[dl, "*"'] \arrow[dr, "*"] & \\ x_4 \arrow[dr, "*"'] & & x_3 \arrow[dl, "*"] \\ & x_2 & \end{tikzcd} \quad \Leftrightarrow \quad \begin{tikzcd} x_1 \arrow[rr, leftrightarrow, "*"] \arrow[dr, "*"'] & & x_2 \arrow[dl, "*"] \\ & x_3 & \end{tikzcd}$$

Often these diagrams are also decorated with universal or existential quantifiers or different kinds of arrows to point out the relation with (1) and (3).

Theorem 2.2 (Newman's lemma). *For every rewrite system $(A, \to)$ with well-founded* $\to$[1],

(5) $$\forall x_1, x_2 \in A . \bigtriangledown (x_1, x_2) \Leftrightarrow \forall x_1, x_2, x_3 \in A . \Diamond_w(x_1, x_2, x_3).$$

By he following example of Hindley, well-foundedness is necessary.

$$\begin{tikzcd} x_1 & x_2 \arrow[l] \arrow[r, bend left] & x_3 \arrow[l, bend left] \arrow[r] & x_4 \end{tikzcd}$$

Church-Rosser and diamond properties can be expressed purely relationally, hence in a more abstract point-free way.

Lemma 2.3. *Let A be a rewrite system.*

(6) $$\forall x_1, x_2 \in A . \bigtriangledown (x_1, x_2) \Leftrightarrow (\to \cup \leftarrow)^* \subseteq \to^* \leftarrow^*,$$

(7) $$\forall x_1, x_2, x_3 \in A . \Diamond(x_1, x_2, x_3) \Leftrightarrow \leftarrow^* \to^* \subseteq \to^* \leftarrow_*,$$

(8) $$\forall x_1, x_2, x_3 \in A . \Diamond_w(x_1, x_2, x_3) \Leftrightarrow \leftarrow \to \subseteq \to^* \leftarrow^* .$$

[1]There are no infinite $\to$-chains.

A proof of this lemma uses the defining properties of set-theoretic union, relational composition and the different closures involved. The loss of information in the abstraction is therefore compensated by the information content of the proof of these properties.

In the following sections we introduce an algebra to reason mathematically concisely about the algebraic properties of these relations.

3. Semirings

Kleene algebras are certain semirings with an additional operation—the Kleene star—that models iteration or fixed point computation. They have been pioneered by Conway [7] in the context the algebra of regular sets over a finite alphabet. Besides formal languages and automata, Kleene algebras or their substructures also arise, for instance, in the field of relational algebra (c.f. [19]) and logics of programs (c.f. [10]). We follow the definition of Kozen in [14].

A *semiring* is an algebra $(A, \cdot, +, 0, 1)$ of a set A, two binary operations of multiplication and addition and two constants 0 and 1 such that

(i) $(A, +, 0)$ is a commutative monoid,
(ii) $(A, \cdot, 1)$ is a monoid,
(iii) the distributive laws

$$a(b + c) = ab + ac, \qquad (a + b)c = ac + bc,$$

hold for all $a, b, c \in A$,
(iv) $0a = a0 = 0$ for every $a \in A$.

We often write A instead of $(A, \cdot, +, 0, 1)$ and express multiplication by juxtaposition. A semiring is *commutative*, if multiplication is commutative: $ab = ba$ for all $a, b \in A$. It is *idempotent*, if addition is idempotent: $a + a = a$ for all $a \in A$. A is *naturally ordered*, if its is partially ordered by the relation $\leq$ defined for all $a, b \in A$ by

$$a \leq b \Leftrightarrow a + c = b \tag{9}$$

for some $c \in A$.

Lemma 3.1. *Let A be a naturally ordered semiring with elements a, b, c.*

(i) $0 \leq a$,
(ii) $a \leq b \Rightarrow a + c \leq b + c$,
(iii) $a \leq b \Rightarrow ac \leq bc$,
(iv) $a \leq b \Rightarrow ca \leq cb$.

Proof. (ad i) $0 + a = a$, since 0 is a unit for addition. Then $0 \leq a$ follows from the definition of the ordering.

(ad ii) Let $a \leq b$. Then there exists some $x \in A$ with $a + x = b$. Substituting equals for equals there exists some $x \in A$ such that $a + x + c = b + c$. Hence $a + c \leq b + c$.

(ad iii) Under the same conditions as in (ii), substituting equals for equals and using distributivity yields that there is some $x \in A$ such that $c(a + x) = c = ca + cx = cb$. Thus there is some d, namely cx, such that $ca + d = cb$. Hence $ca \leq cb$.

(ad iv) Symmetric to (iii). □

Thus the zero is the least element in the ordering and addition and multiplication are monotonic.

Lemma 3.2. *For every idempotent semiring A, the relation $\leq$ defined by (9) is the only partial ordering on A that satisfies the conditions (i) to (iv) of lemma 3.1.*

Proof. We first show that $\leq$ is a partial ordering. Reflexivity is evident from $a+a=a$ by idempotence. Antisymmetry is evident from $a=a+b=b+a=b$ in case $a\leq b$ and $b\leq a$. We now show transitivity. Assume $a+b=b$ and $b+c=c$. We show $a+c=c$.

$$c=b+c=(a+b)+c=a+(b+c)=a+c.$$

It is also clear that $0\leq a$ since $a+0=a$ by definition. We now show monotonicity of addition. Assume $a+b=b$. We show $(a+c)+(b+c)=b+c$. $a+b=b$ implies $a+b+c=b+c$, replacing equals by equals. But by monotonicity, $b+b=b$ and therefore $(a+c)+(b+c)=b+c$. We now show (one part of) monotonicity of multiplication. Assume $a+b=b$. Then $ac+bc=bc$ follows immediately, replacing equals by equals and using distributivity.

We now show that $\leq$ is unique. Therefore assume that there is a partial ordering $\leq'$ on A that satisfies conditions (i) to (iv) of lemma 3.1. We must show that $\leq'=\leq$.

$\leq'\subseteq\leq$. Assume that $a\leq' b$. Then $a+b\leq' b+b=b$ Moreover we know that $0\leq' a$. Hence $b=0+b\leq' a+b$. We have thus shown that $a\leq' b$ implies $a+b=b$ and therefore $a\leq b$. Thus $\leq'\subseteq\leq$.

We now show $\leq\subseteq\leq'$. So assume that $a\leq b$; hence $a+b=b$. But this means that $a+b\leq' b$ and $b\leq' a+b$. But since $0\leq' b$ we also have $a=a+0\leq' a+b$. Hence $a\leq' b$ by transitivity. $\square$

Lemma 3.3. *Every idempotent semiring A is a semilattice with respect to addition (and least upper bounds). Thus for all $a,b,c\in A$,*

$$a+b\leq c\Leftrightarrow a\leq c\wedge b\leq c. \tag{10}$$

Proof. A semilattice is an algebra with an associative, commutative, idempotent operation. Addition in an idempotent semiring has these properties.

We now show that $a+b\leq c$ implies $a\leq c$ and $b\leq c$. By definition of the natural ordering, $a+b\leq c$ iff there is some $d\in A$ such that $a+b+d=c$, Hence there are elements $d_1,d_2\in A$, namely $d_1=b+d$ and $d_2=a+d$ such that $a+d_1\leq c$ and $b+d_2\leq c$. Thus $a\leq c$ and $b\leq c$.

We now show that $a\leq c$ and $b\leq c$ imply $a+b\leq c$. By monotonicity of addition, $a\leq c$ implies $a+b\leq c+b$ and $b\leq c$ implies $c+b\leq c+c$. Hence, by transitivity and idempotence, $a+b\leq c$. $\square$

In an idempotent semiring, monotonicity of multiplication is "almost" equivalent to the distributivity axiom.

Lemma 3.4. *Let A be an idempotent semiring with elements a,b,c. Then*

$$ab+ac\leq a(b+c)\Leftrightarrow(b\leq c\Rightarrow ab\leq ac).$$

Proof. $ab+ac\leq a(b+c)$ implies $b\leq c\Rightarrow ab\leq ac$. By definition of the ordering, $b\leq c$ iff $b+c=c$. Thus $a(b+c)=ab+ac=ac$ and therefore $ab\leq ac$.

$b\leq c\Rightarrow ab\leq ac$ implies $ab+ac\leq a(b+c)$. By definition of the supremum $b\leq b+c$ and $c\leq b+c$, hence $ab\leq a(b+c)$ and $ac\leq a(b+c)$ by monotonicity and therewith $ab+ac\leq a(b+c)$ again by definition of the supremum. $\square$

4. Kleene Algebras

The monotonicity and lattice properties make idempotent semirings an appropriate basis for defining fixed points and iteration via further completeness or continuity conditions. Kleene algebras specify least fixed points at least for chains of powers. *-continuous Kleene algebras identify these least fixed points and iteration. A hierarchy of related semirings is described in [7, 13, 15].

A *Kleene algebra* $(A, \cdot, +, ^*, 0, 1)$ is a set A with binary operations $\cdot$ and $+$, a unary operation * (*Kleene star*) and constants 0 and 1 such that $(A, \cdot, +, 0, 1)$ is an idempotent semiring and for all $a, b, c \in A$,

$$1 + aa^* \leq a^*, \tag{11}$$

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

$$ac + b \leq c \Rightarrow a^*b \leq c, \tag{13}$$

$$ca + b \leq c \Rightarrow ba^* \leq c. \tag{14}$$

Thus a^*b and ba^* are the least pre-fixed points of the monotonic mappings $\lambda x.b + ax$ and $\lambda x.b + xa$. a^* is also a least fixed point of the mappings $\lambda x.1 + ax$, $\lambda x.1 + xa$; the inequalities (11) and (12) can be strengthened to equations. Moreover, a^* is uniquely defined. (13) and (14) are special algebraic variants of induction principles that are sometimes called *Park induction*. We therefore call (11) and (12) *pre-fixed point axioms* and (13) and (14) *Park axioms*. The proofs of the following lemma depend on properties that we show in section 5. Nevertheless we present it here, since the properties it expresses are important for Kleene algebras in general. The reader may convince himself that this anticipation does not lead to circularities.

We define the power a^n of a by the recurrence $a^0 = 1$ and $a^{n+1} = aa^n$.

Lemma 4.1. *Let A be a Kleene algebra. Let $1 \leq a$ for some $a \in A$.*
(i) *The Kleene star is a monotonic operation.*
(ii) *$a^n \leq a^{n+1}$ for all $n \in \mathbb{N}$.*
(iii) *Every subset of the sequence $(a^i : i \in \mathbb{N})$ is a $\leq$-chain.*

Proof. (ad i) The leapfrog rule (34) of section 5 states that $ac = cb$ implies $a^*c = cb^*$, but as its proof shows, also $ac \leq bc$ implies $a^*c \leq cb^*$ and conversely. Setting $c = 1$ in this inequality immediately yields the result.

(ad ii) This is an immediate (inductive) consequence of $1 \leq a$ and monotonicity of multiplication.

(ad iii) Immediate from (ii). □

Lemma 4.2. *Let A be a Kleene algebra.*
(i) *$\sum_{i=0}^{n} a^i \leq \sum_{i=0}^{n+1} a^i$ for all $n \in \mathbb{N}$.*
(ii) *Every subset of the sequence $(\sum_{i=1}^{n} a^i : n \in \mathbb{N})$ is a $\leq -$chain.*

Proof. (ad i) This follows from general properties of suprema.

(ad ii) Immediate from (i). □

We call a chain as in lemma 4.1 a *chain of powers*. A Kleene algebra A is *-*continuous*, if for all $a, b, c \in A$,

$$ab^*c = \sum_{n \in \mathbb{N}} ab^nc \tag{15}$$

The sum notation denotes the supremum of the powers:

$$\sum_{i \in \mathbb{N}} a_i = \sup(a_i : i \in \mathbb{N}).$$

This connection of the Kleene star and supremum together with the definition of a supremum immediately yields the following equivalent (inductive) characterization of *-continuity. First, for all $i \in \mathbb{N}$,

$$ab^ic \leq ab^*c \tag{16}$$

and therefore in particular $a^i \leq a^*$ for all $i \in \mathbb{N}$. We will see in section 5 that (16) holds for arbitrary Kleene algebras. Second, for all $i \in \mathbb{N}$,

$$ab^ic \leq d \Rightarrow ab^*c \leq d. \tag{17}$$

Of course, (17) fails in arbitrary Kleene algebras. Setting $a = 1$ and $b = 1$ in (15) immediately yields that

$$b^* = \sum_{n\in\mathbb{N}} b^n. \tag{18}$$

Thus, in *-continuous Kleene algebras, the Kleene star is associated with a sum of powers, whereas in arbitrary Kleene algebras this is not necessarily so.

Lemma 4.3. *Let A be a *-continuous Kleene algebra.*

$$a(\sum_{n\in\mathbb{N}} b^n)c = \sum_{n\in\mathbb{N}}(ab^n c), \tag{19}$$

$$a + \sum_{n\in\mathbb{N}} b^n = \sum_{n\in\mathbb{N}}(a + b^n). \tag{20}$$

Proof. (19)) This is an immediate consequence of (15) and (18).

(20) This follows from general properties of suprema, the fact that addition is a supremum and idempotent. □

Thus addition and multiplication are continuous operations at sums of powers. (19) can also be read as an infinite distributivity law.

A poset is *-*complete*, if every countable chain of powers has a supremum. A simple adaption of a similar proof for ω-continuous semirings in [15] yields the following statement.

Lemma 4.4. *Let A be a *-continuous Kleene algebra.*

(i) *A is a *-complete poset.*
(ii) *Every countable chain of powers in A is of the form $(\sum_{i=0}^n a^i : n \in \mathbb{N})$.*
(iii) *For every $a \in A$, $a^* = \sup(\sum_{i=0}^n a^i : n \in \mathbb{N})$.*

Proof. (ad i) This follows immediately from the definition of *-continuity.

(ad ii) In a chain of powers $a^i \leq a^j$ for all $i, j \in \mathbb{N}$, $i \leq j$. Thus $a^n = \sum_{i=0}^n a^i$.

(ad iii) by *-continuity, lemma 4.2 (ii), and general properties of suprema, $\sum_{i=0}^n a^i \leq \sum_{i\in\mathbb{N}} a^i$ for all $n \in \mathbb{N}$. Hence $\sup(\sum_{i=0}^n a^i : n \in \mathbb{N}) \leq \sup(a^i : i \in \mathbb{N})$. For the converse direction, observe that $a^n \leq \sum_{i=0}^n a^i$ for all $n \in \mathbb{N}$ by definition of the natural ordering. Thus $\sup(a^n : n \in \mathbb{N}) \leq \sup(\sum_{i=0}^n a^i : n \in \mathbb{N})$ by general properties of the supremum. □

Lemma 4.5. *Let A be a *-continuous Kleene algebra. For all $n \in \mathbb{N}$*

$$\sum_{i=0}^n ab^i c \leq d \Rightarrow ab^* c \leq d. \tag{21}$$

Proof. By definition of the supremum, $ab^n c \leq \sum_{i=0}^n ab^i c \leq d$ for all $n \in \mathbb{N}$. Then (17) yields the result. □

Note the correspondence between (17) and (21). As a consequence of lemma 4.2 and lemma 4.4, the powers of the *-continuous mappings $\lambda x.1 + ax$ and $\lambda x.1 + xa$ evaluated at 0 yield an increasing chain. Its supremum exists (by *-continuity) and is equal to a^*. In a *-continuous Kleene algebra, the Kleene star is thus both least fixed point and limit of an iteration.

Lemma 4.6. *Every idempotent semiring extended with an *-operation that satisfies the *-continuity axiom is a Kleene algebra.*

Proof. We show the prefix axiom (11) and the Park axiom (13).

(11) $1 + aa^* \leq a^*$.

$$1 + aa^* = a^0 + a\sum_{n\in\mathbb{N}} a^n = a^0 + \sum_{n\in\mathbb{N}} aa^n = \sum_{n\in\mathbb{N}}(a^0 + a^{n+1}) = \sum_{n\in\mathbb{N}} a^n = a^*.$$

The proof uses (18) and continuity of addition (20) and multiplication (19).

(13) $ac + b \leq c \Rightarrow a^*b \leq c$. We assume that $ac + b \leq c$ and show $(\sum_{i=0}^{n} a^i)b \leq c$ for all $n \in \mathbb{N}$. The result then follows from lemma 4.5.

$$a^{n+1}c + (\sum_{i=0}^{n} a^i)b = a^n(ac+b) + \sum_{i=0}^{n-1}(a^ib) \leq a^nc + (\sum_{i=0}^{n-1} a^i)b \leq \cdots \leq ac + b \leq c.$$

Therefore also $(\sum_{i=0}^{n} a^i)b \leq c$ by (10). $\square$

In arbitrary Kleene algebras (not all of them are *-continuous [13]), there is no connection between the Kleene star and infinite sums and multiplication is not *-continuous. For most of our purposes plain Kleene algebras are sufficient. Therefore most of our proofs will be purely algebraic (or combinatorial). They do not involve analytic concepts like limits or induction over sequences of approximations. This makes them also well-suited for automation. Since relations satisfy infinite distributivity laws and the axiom of *-continuity (c.f. section 12), proofs in Kleene algebras are also more general than relational ones.

We define the *Kleene plus*

$$a^+ = aa^*. \tag{22}$$

Lemma 4.7. *Let A be a Kleene algebra. For every $a \in A$*

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

$$= a^+ + a^* \tag{24}$$

Proof. (23) The result is immediate, inserting the definition of a^+ into the prefix axiom $1 + aa^* \leq a^*$.

(24) By (23) and idempotence of addition, $a^* = 1 + a^+ + a^+ = a^* + a^+$. $\square$

There are pre-fixed point laws like (11) to (14).

Lemma 4.8. *let A be a Kleene algebra. Then for all $a, b, c \in A$*

$$a(a^+ + 1) \leq a^+, \tag{25}$$

$$(a + +1)a \leq a^+, \tag{26}$$

$$a(b + c) \leq c \Rightarrow a^+b \leq c, \tag{27}$$

$$(b + c)a \leq c \Rightarrow ba^+ \leq c. \tag{28}$$

Proof. We show (25) and (27). (26) and (28) are similar.

(25) The prefix axiom $1+aa^* \leq a^*$ and monotonicity of addition imply $a+aaa^* = a + aa^+ = a(1 + a^+) \leq aa^* = a^+$.

(27) Applying the Park axiom $ac + b \leq b \Rightarrow a^*b \leq c$ to $a(b + c) = ab + ac \leq c$ yields $a^*ab = a^+b \leq c$. $\square$

Lemma 4.9. *For every Kleene algebra A and $a, b \in A$. $a \leq b \Rightarrow a^+ \leq b^+$.*

Proof. $a \leq b$ implies $a^* \leq b^*$ by monotonicity of the Kleene star and $aa^* \leq ab^* \leq bb^*$ by monotonicity of multiplication. Thus $a^+ \leq b^+$ by definition of the Kleene plus. $\square$

Lemma 4.10. *Let A be a *-continuous Kleene algebra. Then for all $a, b, c \in A$,*

$$ab^+c = \sum_{n \in \mathbb{N}_+} ab^nc = \sup(ab^nc : n \in \mathbb{N}_+).$$

Proof.

$$ab^+c = abb^*c = \sum_{n \in \mathbb{N}} abb^nc = \sum_{n \in \mathbb{N}_+} ab^nc.$$

$\square$

Therefore all statements of this section for *-continuous Kleene algebras (lemma 4.3, lemma 4.4, lemma 4.5) also hold for the Kleene plus, replacing $\mathbb{N}$ with $\mathbb{N}_+$. We omit the proofs since they are obvious.

5. Simple Computations with the Kleene Star

We now present some simple properties of Kleene algebras. Most of them are simple induction-free computations that can be formalized using a complete deductive system built from universal Horn logic.

The first lemma presents general properties that are well-known for Kleene algebras, regular languages or automata (c.f. [7, 14]) or relation algebras (c.f [19]).

Lemma 5.1. *Let A be a Kleene algebra. For all $a, b, c \in A$,*

$$1 = 1^*, \tag{29}$$

$$1 \le a^*, \tag{30}$$

$$a^* a^* = a^*, \tag{31}$$

$$a \le a^*, \tag{32}$$

$$a^{**} = a^*, \tag{33}$$

$$ac = cb \Rightarrow a^* c = cb^*, \tag{34}$$

$$(ab)^* a = a(ba)^*, \tag{35}$$

$$a^* a = aa^*, \tag{36}$$

$$(a + b)^* = a^*(ba^*)^* = (a^* b)^* a^*. \tag{37}$$

Proof. (29) $1 \le 1^*$. Substituting 1 for a in the prefix axiom (11) yields $1 + 11^* \le 1^*$. Thus $1 \le 1^*$ by (10).

$1^* \le 1$. It suffices to show $1^* 1 \le 1$, since 1 is a unit for multiplication. By the Park axiom (13), it suffices to show $1 + 11 \le 1$, which is evident, since 1 is a unit for multiplication and addition is idempotent.

(30) By the prefix axiom, $1 + aa^a st \le a^*$. By (10) therefore $1 \le a^*$.

(31) $a^* \le a^* a^*$. $1 \le a^*$ by (30). Thus $a^* \le a^* a^*$ by monotonicity of multiplication.

$a^* a^* \le a^*$. By the Park axiom it suffices to show $aa^* + a^* \le a^*$. By (10) it suffices to show $aa^* \le a^*$. But this immediately follows from the prefix axiom and (10).

(32) $a = a1 \le aa^* \le a^*$. The first inequality follows from (30) by monotonicity of multiplication, the second one from the prefix axiom by (10).

(33) $a^* \le a^{**}$ follows from (32) by monotonicity of the Kleene star (lemma 4.1 (i)).

$a^{**} \le a^*$. By the Park axiom it suffices to show $1 + a^* a^* \le a^*$, thus $1 \le a^*$ and $a^* a^* \le a^*$ by (10). But the two inequalities hold by (30) and (31).

(34) We show that $ac \le cb$ implies $a^* c \le cb^*$. The proof of the implication with the converse inequalities is similar. By the Park axiom it suffices to show $acb^* + c \le cb^*$ and therefore $c \le cb^*$ and $acb^* \le cb^*$ by (10). The first inequality immediately follows from (30) by monotonicity of multiplication. For the second inequality, assume $ac \le cb$. Then $acb^* \le cbb^* \le cb^* b^* = cb^*$. The first inequality follows from monotonicity of multiplication. The second inequality follows from (32). The third inequality follows from (31).

(35) The simplest proof is by setting $a = ab, b = ba, c = a$ in (34). It is however not necessary to use any Horn expression beyond the definitions of Kleene algebra. We only show $(ab)^* a \le a(ba)^*$. The other direction is similar. By the Park axiom it suffices to show $aba(ba)^* + a \le a(ba)^*$ and therefore $a \le a(ba)^*$ and $aba(ba)^* \le a(ba)^*$ by (10). The first inequality, follows from $1 \le (ba)^*$, that is (30), and

monotonicity of composition. For the second inequality, $ba \le (ba)^*$ by (32), hence $aba \le a(ba)^*$ and $aba(ba)^* \le a(ba)^*(ba)^* = a(ba)^*$ by monotonicity of composition and (31).

(36) Set $b = 1$ in (35).

(37) We only show the first equality. The second then follows from (35).

$(a+b)^* \le a^*(ba^*)^*$. By the Park axiom it suffices to show that

$$(a+b)a^*(ba^*)^* + 1 \le a^*(ba^*)^*.$$

The proof is

$$\begin{aligned}
(a+b)a^*(ba^*)^* + 1 &= aa^*(ba^*)^* + (1 + ba^*(ba^*)^*) && \text{distributivity}\\
&\le aa^*(ba^*)^* + (ba^*)^* && \text{prefix axiom}\\
&= (aa^* + 1)(ba^*)^* && \text{distributivity}\\
&\le a^*(ba^*)^*. && \text{prefix axiom}
\end{aligned}$$

Monotonicity of multiplication has been used implicitly.

$a^*(ba^*)^* \le (a+b)^*$. By the Park axiom it suffices to show

$$(a+b)^*ba^* + a^* = ((a+b)^*b + 1)a^* \le (a+b)^*.$$

By the Park axiom again it suffices to show

$$(a+b)^*a + (a+b)^*b + 1 = (a+b)^*(a+b) + 1 \le (a+b)^*.$$

This last inequality holds by the prefix axiom. $\square$

Some expressions have names in the literature, others express distinguished algebraic properties. (30) and (31) express reflexivity and transitivity of a^*, (32) and (33) extensivity and idempotence of the Kleene star (which together with monotonicity of *—a consequence of (34)—defines the properties of a closure operation). (34) is called *leapfrog rule*, (35) *shift rule* and (37) *denesting rule*. As we have seen, the shift rule, (36) and monotonicity of the Kleene star immediately follow from the leapfrog rule, but can also be derived without that Horn rule.

In particular, the denesting rule (37) is important for one variant of our Church-Rosser proof. We therefore show the most important dependencies from other rules in the following diagram.

$$\begin{tikzcd}
(11) \arrow[rr] \arrow[dr] \arrow[drrr] \arrow[dddrr] & & (30) \arrow[dl] \arrow[dr] & & (13) \arrow[dl] \arrow[dddll] \\
& (32) \arrow[dr] & & (31) \arrow[dl] & \\
& & (35) \arrow[d] & & \\
& & (37) & &
\end{tikzcd}$$

The following statements are already specific to Church-Rosser properties.

Lemma 5.2. *Let A be a Kleene algebra. For all $a, b \in A$*

$$ba^* \le a^*b^* \Rightarrow (ba^*)^* \le a^*b^*, \tag{38}$$

$$ba^* \le a^*b^* \Rightarrow ba^*b^* \le a^*b^*, \tag{39}$$

$$ba^* \le a^*b^* \Leftrightarrow b^*a^* \le a^*b^*, \tag{40}$$

$$b^*a^* \le (a+b)^*. \tag{41}$$

Proof. (of 38) We assume $ba^* \leq a^*b^*$ and show $(ba^*)^* \leq a^*b^*$. By the Park axiom it suffices to show $ba^*a^*b^* + 1 \leq a^*b^*$, hence $1 \leq a^*b^*$ and $ba^*a^*b^* \leq a^*b^*$ by (10). The first inequality immediately follows from (30), monotonicity of multiplication and the fact that 1 is a unit of multiplication: $1 \leq a^* \Leftrightarrow a^*1 \leq a^*b^*$. The second one follows from (31) and the assumption: $ba^*a^*b^* = ba^*b^* \leq a^*b^*b^* = a^*b^*$.

(of 39) $ba^*b^* \leq a^*b^*b^* = a^*b^*$, by the assumption, (31) and monotonicity of multiplication.

(of 40) $ba^* \leq a^*b^* \Rightarrow b^*a^* \leq a^*b^*$. We assume $ba^* \leq a^*b^*$ and show $b^*a^* \leq a^*b^*$. By the Park axiom it suffices to show $ba^*b^* + a^* \leq a^*b^*$ and hence $a^* \leq a^*b^*$ and $ba^*b^* \leq a^*b^*$ by (10). The first inequality follows immediately from (30), monotonicity of multiplication and the fact that 1 is a unit for multiplication. The second one has been shown in the proof of (39).

$b^*a^* \leq a^*b^* \Rightarrow ba^* \leq a^*b^*$. By (32) and monotonicity of multiplication.

(of 41) By (37), it remains to show that $a^*b^* \leq a^*(ba^*)^*$. By (30), $1 \leq a^*$. By monotonicity of multiplication and the Kleene star, therefore $b \leq ba^*$, $b^* \leq (ba^*)^*$ and $a^*b^* \leq a^*(ba^*)^*$. □

(38), like denest (37), is important for one variant of our Church-Rosser proof. We therefore show the most important dependencies from other rules in the following diagram.

$$\begin{tikzcd}
 & (11) \arrow[dl] \arrow[dd] & \\
(30) \arrow[dr] \arrow[ddr] & & (13) \arrow[dl] \arrow[ddl] \\
 & (31) \arrow[d] & \\
 & (38) &
\end{tikzcd}$$

In all proofs of this text, inequational reasoning pays. The Park axioms are the working horses of Kleene algebra; also monotonicity and (10) are abundantly use. In particular, induction has not been used in any of the proofs of this section.

Lemma 5.1 yields are comparison of plain and *-continuous Kleene algebras.

Corollary 5.3. *Let A be a Kleene algebra. Then for all $a \in A$,*

(i) $a^i \leq a^*$ *for all* $i \in \mathbb{N}$.
(ii) $\sum_{i=0}^{n} a^i \leq a^*$ *for all* $n \in \mathbb{N}$.

Proof. (ad i) Reasoning inductively, (30) and (31) imply that

$$a^i \leq a^ia^* \leq a^{i-1}a^*a^* = a^{i-1}a^* \leq \cdots \leq aa^* \leq a^*a^* = a^*.$$

(ad ii) $\sum_{i=0}^{n} a^i \leq \sum_{i=0}^{n} a^* = a^*$ for all $n \in \mathbb{N}$ follows from (i) by monotonicity and idempotence of addition. □

Thus in a Kleene algebra, a^* is an upper, but not necessarily a least upper bound of the chain of powers of a, whereas *-continuous Kleene algebras have the latter property by lemma 4.4. Corollary 5.3, holds also for the Kleene plus and $\mathbb{N}_+$ for $\mathbb{N}$.

6. Simple Computations with the Kleene Plus

We now add some properties of the Kleene plus. Some of them can be found, for instance, in [8].

Lemma 6.1. *Let A be a Kleene algebra. For all $a, b, c \in A$*

$$a^+ \leq a^*, \tag{42}$$
$$1 = 1^+, \tag{43}$$
$$a^*a^+ = a^+a^* = a^+, \tag{44}$$
$$a^+a^+ = aa^+ = a^+a, \tag{45}$$
$$aa^+ \leq a^+, \tag{46}$$
$$a^+a^+ \leq a^+ \tag{47}$$
$$a \leq a^+, \tag{48}$$
$$a^{++} = a^+, \tag{49}$$
$$(a^*b)^+ = (a+b)^*b, \tag{50}$$
$$(ab)^+ = a(ba)^*b, \tag{51}$$
$$(ab)^+a = a(ba)^+, \tag{52}$$
(53)
$$(a+b)^+ = (a^*b)^+a^* + a^+ = a^*(ba^*)^+ + a^+ = (b^*a)^+b^* + b^+ = b^*(ab^*)^+ + b^*,$$
$$a^+b^* + a^*b^+ = a^+ + a^*b^+ = a^+b^* + b^+. \tag{54}$$

Proof. Like in lemma 5.1, we could prove all statements from the fixed point properties of the Kleene plus, as given in lemma 4.8. However it is sometimes easier to use the statements of lemma 5.1 together with the definition of the Kleene plus in (22) and lemma 4.7.

(42) This is immediate from (23) and (10).

(43) By (29) and the definition of the Kleene plus, $1 = 1^* = 11^* = 1^+$.

(44) First, $a^*a^+ = a^*aa^* = aa^*a^* = a^+a^*$, by the definition of the Kleene star and (36). Moreover, $aa^*a^* = aa^* = a^+$ by (31) and the definition of the Kleene star.

(45) By (44), monotonicity of multiplication, (36) and the definition of the Kleene plus,

$$aa^+ = aa^*a^+ = a^+a^+ = a^+aa^* = a^+a^*a = a^+a.$$

(46) By (30), 44) and monotonicity of multiplication, $aa^+ \leq a^*a^+ = a^+$.

(47) This follows immediately from (45) and (46).

(48) By (30), $1 \leq a^*$. Thus $a \leq aa^* = a^+$ by monotonicity of multiplication.

(49) $a^* \leq a^{**}$ follows immediately from monotonicity of the Kleene plus and (48).

$a^{**} \leq a^*$. By (27) it suffices to show that $a^+(1 + a^+) = a^+ + a^+a^+ \leq a^+$ and therefore $a^+a^+ \leq a^+$ by (10), which holds by (47).

(50) $(a+b)^*b = (a^*b)^*a^*b(a^*b)^+$ by (37), monotonicity of multiplication and definition of the Kleene plus.

(51) $a(ba)^*b = (ab)^*ab = (ab)^+$ by (35), monotonicity of multiplication and definition of the Kleene plus.

(52) $(ab)^+a = ab(ab)^*a = aba(ba)^* = a(ba)^+$ by (35) and the definition of the Kleene plus.

(53) We show $(a+b)^+ = a^+(a^*b)^+a^*$. The remaining cases follow by (52) or exchange of a and b.

$$\begin{aligned}
(a+b)^+ &= (a+b)(a+b)^* && \text{def. Kleene plus}\\
&= (a+b)a^*(ba^*)^* && (37)\\
&= aa^*(ba^*)^* + ba^*(ba^*)^* &&\\
&= a^+(ba^*)^* + (ba^*)^+ && \text{def. Kleene plus}\\
&= a^+(1+(ba^*)^+) + (ba^*)^+ && (23)\\
&= a^+ + (a^+ + 1)(ba^*)^+ &&\\
&= a^+ + a^*(ba^*)^+ && (23)
\end{aligned}$$

(54) $a^+b^* + a^*b^+ = a^+(b^+ + 1) + (a^+ + 1)b^+ = a^+ + a^+b^+ + b^+$, by (23), monotonicity of multiplication, distributivity and idempotence of addition. But

$$\begin{aligned}
a^+ + a^+b^+ + b^+ &= a^+ + (a^+ + 1)b^+ = a^+ + a^*b^+\\
&= a^+(1+b^+) + b^+ = a^+b^* + a^+.
\end{aligned}$$

by distributivity, monotonicity of multiplication and (23). □

The following properties are needed in the Church-Rosser proofs in section 8.

Lemma 6.2. *Let A be a Kleene algebra. For all $a, b \in A$*

$$ba^* \le a^*b^+ + a^+b^* \Rightarrow b(a^*b^+ + a^+b^*) \le a^*b^+ + a^+b^*, \tag{55}$$

$$ba^* \le a^*b^+ + a^+b^* \Leftrightarrow b^+a^* \le a^*b^+ + a^+b^*, \tag{56}$$

$$a^*b^+ + a^+b^* \le (a+b)^+. \tag{57}$$

Proof. (55) $b(a^*b^+ + a^+b^*) \le ba^*b^* \le (a^+b^* + a^*b^+)b^* = a^+b^* + a^*b^+$, by (42), the assumption, (31) and (44).

(56) $ba^* \le a^*b^+ + a^+b^* \Rightarrow b^+a^* \le a^*b^+ + a^+b^*$. We assume $ba^* \le a^*b^+ + a^+b^*$ and show $b^+a^* \le a^*b^+ + a^+b^*$. By (27) and (10) it suffices to show

$$ba^* \le a^+b^* + a^*b^+, \qquad b(a^+b^* + a^*b^+) \le a^+b^* + a^*b^+.$$

The first inequality is the assumption. The second one is (55).

$b^+a^* \le a^*b^+ + a^+b^* \Rightarrow ba^* \le a^*b^+ + a^+b^*$. By (48), $b \le b^+$. Then the result follows from monotonicity of multiplication.

(57) By (10) and (53) it suffices to show

$$\begin{aligned}
a^*b^+ &\le (a+b)^+ = a^*(ba^*)^+ + a^+,\\
a^+b^* &\le (a+b)^+ = (b^*a)^+b^* + b^+.
\end{aligned}$$

In the first inequality, (31), $1 \le a^*$ implies $a^*b^+ \le a^*(ba^*)^+ \le a^*(ba^*)^+ + a^+$ by monotonicity of multiplication, of the Kleene plus, of multiplication again and since addition defines a supremum.

In the second inequality, $1 \le b^*$ leads to $a^+b^* \le (b^*a)^+b^* + b^+$ by the same chain of reasoning. □

The following statement is similar to corollary 5.3. It is needed in the Church-Rosser proofs of section 8.

Corollary 6.3. *Let A be a Kleene algebra. Then for all $a \in A$,*

(i) $a^i \le a^+$ *for all* $i \in \mathbb{N}_+$.
(ii) $\sum_{i=1}^{n} a^i \le a^+$ *for all* $n \in \mathbb{N}_+$.

Proof. (ad i) Reasoning inductively, (42), $a^+ \leq$, (48), $a \leq a^+$ and the definition of the Kleene plus imply that

$$a^i \leq a^{i-1}a^+ \leq a^{n-1}a^* = a^{n-2}a^+ \leq \cdots \leq aa^+ \leq a^* = a^+.$$

(ad ii) The fact follows from (i) by monotonicity and idempotence of addition. □

Theorem 6.4. *Let K be a Kleene algebra whose carrier is a power set. Then the Kleene star and Kleene plus are closure operators.*

Proof. The defining properties of a closure operator are expressed by lemma 5.1 (iv) and (vi), lemma 6.1 (iii) and (vi) and lemma 4.9 (monotonicity). □

Proposition 6.5. *Let a and b be elements of a Kleene algebra and let $a \leq b$.*

(i) $bb \leq b \Rightarrow a^+ \leq b$.
(ii) $1 \leq b, bb \leq b \Rightarrow a^* \leq b$.

Proof. (ad i) $a \leq b$ implies $ab \leq bb \leq b$. Hence $a(b+1) = ab + a \leq b$ by (2) and therefore $a^+ \leq b$ by lemma 4.8.

(ad ii) $a \leq b$ implies $ab \leq bb \leq b$. Hence $ab + 1 \leq b$ and therefore $a^* \leq b$ by $(*iii)$. □

These lemma will later allow us to identify the Kleene plus and star with transitive and reflexive transitive closures of relations.

7. Church-Rosser Proofs with the Kleene Star

Let Σ^* be the free monoid over the alphabet Σ. A *semi-commutation relation* is an irreflexive relation S on Σ, a *commutation relation* a reflexive symmetric relation R on Σ. We associate with each P the rewrite system $S_P = \{ab \to ba : (a,b) \in P\}$. We write $v \to_P w$, if there exist words $v', v'', w', w'' \in \Sigma^*$ and $(a,b) \in P$ such that $v = v'abv''$ and $w = w'baw''$. The reflexive transitive closure of $\to_P$ is denoted by $\to_P^*$. Since it is the least quasi-ordering extending $v \to_P w$, we also write $v \preceq_P w$. $\preceq_P \cup \succeq_P$ is a congruence and its quotient with Σ^* the free partially commuting monoid generated by P. The concepts of semi-commutation and commutation are borrowed from trace theory [6], where they model priority or equivalence in execution sequences of concurrent processes.

$ba \leq ab$ and $ba \to ab$ mean the same in a Kleene algebra. But weaker concepts of semi-commutation for Church-Rosser statements are needed. Partially semi-commuting Kleene algebras are finitely presented Kleene algebras. We will always model them by universal Horn sentences. We now present a series of algebraic Church-Rosser statements.

Proposition 7.1. *Let A be a Kleene algebra. For all $a, b \in A$,*

(i) $ba^* \leq a^*b^* \Rightarrow (a+b)^* \leq a^*b^*$.
(ii) $ba \leq ab \Rightarrow (a+b)^* \leq a^*b^*$, *if A is *-continuous.*
(iii $b^*a^* \leq a^*b^* \Rightarrow (a+b)^* \leq a^*b^*$.

Proof. In all three proofs, we have to show $(a+b)^* \leq a^*b^*$ under the respective assumption. By the Park axiom it suffices to show $(a+b)a^*b^* + 1 \leq a^*b^*$ and therefore $1 \leq a^*b^*$, $aa^*b^* \leq a^*b^*$ and $ba^*b^* \leq a^*b^*$ by (10).

The first inequality follows immediately from (30): $1 \leq a^* = a^*1 \leq a^*b^*$.

The second inequality follows immediately from (32), (31) and monotonicity of multiplication: $a \leq a^*$ implies $aa^*b^* \leq a^*a^*b^* = a^*b^*$. Only the third inequality depends on the assumptions.

(ad i) The third inequality is identical to (39). It has been shown in lemma 5.2.

(ad ii) It suffices to show $ba \le ab \Rightarrow ba^* \le a^*b^*$. The result then follows from (i). We thus assume $ba \le ab$ and show $ba^* \le a^*b^*$. $ba \le ab$ implies $ba^i \le a^ib$ for all $i \in \mathbb{N}$ by a simple induction and therefore also

$$b\sum_{i=0}^{n} a^i = \sum_{i=0}^{n}(ba^i) \le \sum_{i=0}^{n}(a^ib) = (\sum_{i=0}^{n} a^i)b.$$

But $b \le b^*$ by (32) and $\sum_{i=0}^{n} a^i \le a^*$ by corollary 5.3. Thus $b\sum_{i=0}^{n} a^i \le a^*b^*$ for all $n \in \mathbb{N}$ and therefore $ba^* = \sum_{i\in\mathbb{N}}(ba^i) \le a^*b^*$ by lemma 4.5 and *-continuity.

(ad iii) By (40) (lemma 5.2), $ba^* \le a^*b^* \Leftrightarrow b^*a^* \le a^*b^*$. The result then follows from (i). □ □

There is an alternative proof of proposition 7.1 (i). Assuming $ba^* \le a^*b^*$, we show that $(a+b)^* \le a^*b^*$. By the denesting rule, it suffices to show $a^*(ba^*)^* \le a^*b^*$. By (38) (lemma 5.2) $(ba^*)^* \le a^*b^*$ follows from the assumption. Thus $a^*(ba^*)^* \le a^*a^*b^* = a^*b^*$ follows from monotonicity of multiplication and (31).

Theorem 7.2. *In proposition 7.1, the inequality $(a+b)^* \le a^*b^*$ can be strengthened to an equality.*

Proof. Combination of (41) in lemma 5.2 and proposition 7.1. □

With the exception of proposition 7.1 (ii), all statements relevant to our Church-Rosser statements were induction-free, but heavily dependent on the Park axioms. It seems that *-continuity cannot be avoided in proposition 7.1 (ii).

Proposition 7.1 and theorem 7.2 can be generalized to sums $\sum_{i=0}^{n} a_i$ and products $\prod_{i=0}^{n} a_i$ and products in more than two variables. The proofs use induction on the number of generators and proposition 7.1 as base cases. The induction is not difficult, but proofs become longer and require some bookkeeping.

Lemma 7.3. *Let A be a Kleene algebra with $a_0,\dots,a_n \in A$.*

(i) $1 \le \prod_{i=0}^{n} a_i^*$,

(ii) $a_ja_i^* \le a_i^*a_j^* \Rightarrow a_n(\prod_{i=0}^{n-1} a_i^*) \le \prod_{i=0}^{n} a_i^*$, *for all $i,j \in \mathbb{N}$, $i < j \le n$.*

Proof. (ad i) By induction on n. In the base case, $1 \le a_i^*$ holds by (30) for all i, $0 \le i \le n$. Using the base case for a_n, in the induction step,

$$1 \le \prod_{i=1}^{n-1} a_i^* = (\prod_{i=1}^{n-1} a_i^*)1 \le (\prod_{i=1}^{n-1} a_i^*)a_n^* = \prod_{i=1}^{n} a_i^*$$

follows from the induction hypothesis for $\prod_{i=1}^{n-1} a_i^*$ and monotonicity of multiplication.

(ad ii) By induction on n. The base case $a_1a_0^* \le a_0^*a_1^*$ is trivial. In the step case, we assume that $a_k(\prod_{i=0}^{n-2} a_i^*) \le (\prod_{i=0}^{n-2})a_k^*$ for all $k \ge n-1$. In fact we only need the hypothesis for $k = n$.

$$a_n(\prod_{i=0}^{n-1} a_i^*) = a_n(\prod_{i=0}^{n-2} a_i^*)a_{n-1}^* \le (\prod_{i=0}^{n-2} a_i^*)a_n^*a_{n-1}^* \le (\prod_{i=0}^{n-2} a_i^*)a_{n-1}^*a_n^* = \prod_{i=0}^{n} a_i^*$$

(40) has been used to apply the base case in the rightmost inequality step. □

Proposition 7.4. *Let A be a Kleene algebra. For all $a_0,\dots,a_n \in A$.*

(i) $a_j^*a_i^* \le a_i^*a_j^*$ *for all $0 \le i < j \le n$ implies $(\sum_{i=0}^{n} a_i)^* \le \prod_{i=1}^{n} a_i^*$.*

(ii) $a_ja_i \le a_ia_j$ *for all $0 \le i < j \le n$ implies $(\sum_{i=0}^{n} a_i)^* \le \prod_{i=1}^{n} a_i^*$, if A is ω-continuous.*

Proof. (ad i) The base case for $n = 2$ has been shown in proposition 7.1 (iii). For the induction step, it suffices to show by the prefix axiom that the assumption implies

$$(\sum_{i=0}^{n} a_i)(\prod_{i=0}^{n} a_i^*) + 1 \leq \prod_{i=0}^{n} a_i^*$$

and therefore

$$1 \leq \prod_{i=0}^{n} a_i^*, \qquad (\sum_{i=0}^{n} a_i)(\prod_{i=0}^{n} a_i^*) \leq \prod_{i=0}^{n} a_i^*,$$

by (10). The first inequality has already been shown in lemma 7.3 (i). The second inequality follows from a simple induction using lemma 7.3 (ii). We assume that $(\sum_{i=0}^{n-1} a_i)(\prod_{i=0}^{n-1} a_i^*) \leq \prod_{i=0}^{n-1} a_i^*$.

$$\begin{aligned}
(\sum_{i=0}^{n} a_i)(\prod_{i=0}^{n} a_i^*) &= ((\sum_{i=0}^{n-1} a_i) + a_n)(\prod_{i=0}^{n-1} a_i^*)a_n^* \\
&= (\sum_{i=0}^{n-1} a_i)(\prod_{i=0}^{n-1} a_i^*)a_n^* + a_n(\prod_{i=0}^{n-1} a_i^*)a_n^* \\
&\leq (\prod_{i=0}^{n-1} a_i^*)a_n^* + (\prod_{i=0}^{n} a_i^*)a_n^* && \text{Ind.Hyp., lemma 7.3 (ii)} \\
&= (\prod_{i=0}^{n} a_i^*) + (\prod_{i=0}^{n-1} a_i^*)a_n^* a_n^* \\
&= (\prod_{i=0}^{n} a_i^*) + (\prod_{i=0}^{n} a_i^*) && (31) \\
&= \prod_{i=0}^{n} a_i^*.
\end{aligned}$$

Monotonicity properties and the like have been left implicit. The assumption is needed to apply lemma 7.3 (ii).

(ad ii) It suffices to show that $a_j a_i \leq a_i a_j$ for all $0 \leq i < j \leq n$ implies $a_j^* a_i^* \leq a_i^* a_j^*$ for all $0 \leq i < j \leq n$. The result then follows from (i). In the proof of proposition 7.1 (ii), we have shown that $a_j a_i \leq a_i a_j$ implies $a_j a_i^* \leq a_i^* a_j^*$, using *-continuity. In lemma 5.2, (40), we have shown that $a_j a_i^* \leq a_i^* a_j^*$ if and only if $a_j^* a_i^* \leq a_i^* a_j^*$. This yields the result. $\square$

Proposition 7.4 (i) is loosely related to Church-Rosser theorems modulo [11], as we will see in section 12. Proposition 7.4 (ii) can be understood as an algebraic completeness proof of bubble sort.

8. Church-Rosser Proofs with the Kleene Plus

In this section we give some Church-Rosser statements for the Kleene plus. The proofs are more involved than those for the Kleene star.

Proposition 8.1. *Let A be a Kleene algebra. Then for all $a, b \in A$*

(i) $ba^* \leq a^*b^+ + a^+b^* \Rightarrow (a+b)^+ \leq a^*b^+ + a^+b^*$.
(ii) $ba \leq ab \Rightarrow (a+b)^+ \leq a^*b^+ + a^+b^*$, *if A is ω-continuous.*
(iii) $b^+a^* \leq a^*b^+ + a^+b^* \Rightarrow (a+b)^+ \leq a^*b^+ + a^+b^*$.

Proof. (ad i) By (42), $a^+ \leq a^*$. Thus $a^*b^+ + a^+b^* \leq a^*b^*$ and $ba^* \leq a^*b^+ + a^+b^*$ implies $ba^* \leq a^*b^*$. But then

$$(a+b)^+ = (a+b)(a+b)^* \leq (a+b)a^*b^* = aa^*b^* + ba^*b^*$$

by definition of the Kleene plus and proposition 7.1 (i), using the weakened assumption. Thus

$$\begin{aligned}
(a+b)^+ &= aa^*b^* + ba^*b^* \\
&\leq a^+b^* + (a^*b^+ + a^+b^*)b^* && \text{def. Kleene plus, Ass.} \\
&= a^+b^* + a^*b^+b^* + a^+b^*b^* \\
&= a^+b^* + a^*b^+ + a^+b^* && (44), (31) \\
&= a^+b^* + a^*b^+.
\end{aligned}$$

(ad ii) In analogy to the proof of proposition 7.1 (ii), it suffices to show that $ba \leq ab$ implies that $ba^* \leq a^*b^+ + a^+b^*$. Since $a \leq a^+$ by (48), the proof in proposition 7.1 (ii) can easily be adapted. We therefore do not carry it out explicitly. It essentially uses *-continuity.

(ad iii) This follows immediately from (i) and (56). □

Corollary 8.2. *In proposition 8.1, the inequality $(a+b)^* \leq a^+b^* + a^*b^+$ can be replaced by $(a+b)^* \leq a^+b^* + b^+$ or $(a+b)^* \leq a^+ + a^*b^+$.*

Proof. By (54), the righthand sides are equal. □

Theorem 8.3. *In proposition 8.1 and corollary 8.2, the inequalities $(a+b)^* \leq a^+b^* + a^*b^+$, $(a+b)^* \leq a^+ + a^*b^+$ and $(a+b)^* \leq a^+b^* + b^+$ can be strengthened to equalities.*

Proof. Combination of (57) and (54) respectively in lemma 6.2 and proposition 8.1 and corollary 8.2. □

With the exception of proposition 8.1 (ii), all statements relevant to our Church-Rosser statements were again induction-free. (57). Like in the proof of proposition 7.4, proposition 8.1 yields base cases for inductive proofs of Church-Rosser statements with more than two generators.

For this generalization, we introduce s function δ on a Kleene algebra, which is defined by $\delta_{ij} = 1$ iff $i \neq j$ and $\delta_{ij} = 0$ iff $i = j$ for all $i, j \in \mathbb{N}$. In generalization of $a^*b^+ + a^+b^*$, we now consider expressions of the form

$$\sum_{j=0}^{n} \prod_{i=0}^{n} (a_i^+(1 + a_i\delta_{ij})).$$

Since $a^* + a^+ = a^*$ by (23), this expression yields a sum of product, such that alternatingly one factor is a Kleene plus and the others are Kleene stars.

Lemma 8.4. *Let A be a Kleene algebra and $a_0, \ldots, a_n \in A$.*

(i) $\sum_{j=0}^{1} \prod_{i=0}^{1} a_i^+(1 + a_i\delta_{ij}) = a_0^+a_1^* + a_0^*a_1^+$.
(ii) $\sum_{j=0}^{n} \prod_{i=0}^{n} (a_i^+(1 + a_i\delta_{ij})) = (\sum_{j=0}^{n-1} \prod_{i=0}^{n-1} (a_i^+(1 + a_i\delta_{ij})))a_n^* + (\prod_{i=0}^{n-1} a_i^*)a_n^+$.

Proof. (ad i)

$$\begin{aligned}\sum_{j=0}^{1}\prod_{i=0}^{1} a_i^+(1+a_i\delta_{ij}) &= \sum_{j=0}^{1}(a_1^+(1+a_1\delta_{1j})a_2^+(1+a_2\delta_{2j}) \\ &= a_1^+(1+a_1\delta_{11})a_2^+(1+a_2\delta_{21}) + a_1^+(1+a_1\delta_{12})a_2^+(1+a_2\delta_{22}) \\ &= a_1^+(1+a_1 0)a_2^+(1+a_2 1) + a_1^+(1+a_1 1)a_2^+(1+a_2 0) \\ &= a_1^+(a_2^+ + a_2^*) + (a_1^+ + a_1^*)a_2^+ \\ &= a_1^+ a_2^* + a_1^* a_2^+.\end{aligned}$$

We used (23) in the last step.

(ad ii)

$$\begin{aligned}\sum_{j=0}^{n}\prod_{i=0}^{n}(a_i^+(1+a_i\delta_{ij})) &= \sum_{j=0}^{n}(\prod_{i=0}^{n-1}(a_i^+(1+a_i\delta_{ij}))a_n^+(1+a_n\delta_{nj})) \\ &= \sum_{j=0}^{n-1}(\prod_{i=0}^{n-1}(a_i^+(1+a_i\delta_{ij}))a_n^+(1+a_n\delta_{nj})) \\ &\quad + (\prod_{i=0}^{n-1} a_i^+(1+a_i\delta_{in})a_n^+(1+a_n\delta_{nn})) \\ &= (\sum_{j=0}^{n-1}\prod_{i=0}^{n-1}(a_i^+(1+a_i\delta_{ij})))a_n^* + (\prod_{i=0}^{n-1} a_i^*)a_n^+.\end{aligned}$$

□

Lemma 8.5. *Let A be a Kleene algebra with $a_0, \ldots, a_n \in A$. For all $0 \le k < l \le n$*

$$a_l^+ a_k^* \le a_k^+ a_l^* + a_k^* a_l^+ \Rightarrow a_n \prod_{i=0}^{n-1} a_i^* \le \sum_{j=0}^{n}\prod_{i=0}^{n} a_i^+(1+a_i\delta_{ij}). \tag{58}$$

Proof. By induction on n. The base case is given by the assumption, according to lemma 8.4 (i). For the induction step we assume that

$$a_n \prod_{i=0}^{n-2} a_i^* \le (\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))a_n^* + (\prod_{i=0}^{n-2} a_i^*)a_n^+$$

according to lemma 8.4 (ii). Thus

$$\begin{aligned}a_n \prod_{i=0}^{n-1} a_i^* &= a_n(\prod_{i=0}^{n-2} a_i^*)a_{n-1}^* \\ &\le (\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))a_n^* a_{n-1}^* + (\prod_{i=0}^{n-2} a_i^*)a_n^+ a_{n-1}^* \\ &= (\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))(1+a_n^+)a_{n-1}^* + (\prod_{i=0}^{n-2} a_i^*)a_n^+ a_{n-1}^* \\ &\le (\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))(a_{n-1}^* + a_{n-1}^* a_n^+ + a_{n-1}^+ a_n^*) \\ &\quad + (\prod_{i=0}^{n-2} a_i^*)(a_{n-1}^+ a_n^* + a_{n-1}^* a_n^+)\end{aligned}$$

$$
\begin{aligned}
&\leq (\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))(a_{n-1}^*a_n^*+a_{n-1}^*a_n^*+a_{n-1}^*a_n^*)\\
&\quad +(\prod_{i=0}^{n-2}a_i^*)(a_{n-1}^+a_n^*+a_{n-1}^*a_n^+)\\
&= [(\sum_{j=0}^{n-2}\prod_{i=0}^{n-2}(a_i^+(1+a_i\delta_{ij})))a_{n-1}^*+(\prod_{i=0}^{n-2}a_i^*)a_{n-1}^+]a_n^*+(\prod_{i=0}^{n-1}a_i^*)a_n^+\\
&= (\sum_{j=0}^{n-1}\prod_{i=0}^{n-1}(a_i^+(1+a_i\delta_{ij})))a_n^*+(\prod_{i=0}^{n-1}a_i^*)a_n^+\\
&= \sum_{j=0}^{n}\prod_{i=0}^{n}(a_i^+(1+a_i\delta_{ij})))
\end{aligned}
$$

We used (23) from the second to the third row, the assumption from the third to the fourth row, (30) and (42) from the fourth to the fifth row and lemma 8.4 (ii) at for the last two steps. ☐

Proposition 8.6. *Let A be a Kleene algebra. For all $a_0, \dots, a_n \in A$, for all $0 \leq k < l \leq n$,*

$$
a_l^+a_k^* \leq a_k^+a_l^* + a_k^*a_l^+ \Rightarrow (\sum_{i=0}^{n}a_i)^+ \leq \sum_{j=0}^{n}\prod_{i=0}^{n}a_i^+(1+a_i\delta_{ij}). \tag{59}
$$

Proof. Obviously, $a_l^+a_k^* = (1+a_l^*)a_k^*$ by (23) and thus $a_l^+a_k^* \leq a_k^+a_l^* + a_k^*a_l^+$ implies $a_l^*a_k^* \leq a_k^+a_l^* + a_k^*a_l^+ \leq a_k^*a_l^*$ by (42). Therefore

$$
(\sum_{i=0}^{n}a_i)^+ = (\sum_{i=0}^{n}a_i)(\sum_{i=0}^{n}a_i)^* \leq (\sum_{i=0}^{n}a_i)(\prod_{i=0}^{n}a_i^*) = \sum_{i=0}^{n}(a_i\prod_{j=0}^{n}a_i^*)
$$

by proposition 7.4 (i). For every k, $0 \leq k \leq n$ we now split

$$
a_k\prod_{j=0}^{n}a_i^* = a_k(\prod_{j=0}^{k-1}a_i^*)a_k^*(\prod_{j=k+1}^{n}a_i^*),
$$

where the last two factors are possibly empty. Applying lemma 8.5, using the assumption, yields

$$
\begin{aligned}
a_k\prod_{j=0}^{n}a_i^* &= \sum_{j=0}^{k}\prod_{i=0}^{k}a_i^+(1+a_i\delta_{ij})a_k^*(\prod_{j=k+1}^{n}a_i^*)\\
&= [(\sum_{j=0}^{k-1}\prod_{i=0}^{k-1}(a_i^+(1+a_i\delta_{ij})))a_k^*+(\prod_{i=0}^{k-1}a_i^*)a_k^+]a_k^*(\prod_{j=k+1}^{n}a_i^*)\\
&= [(\sum_{j=0}^{k-1}\prod_{i=0}^{k-1}(a_i^+(1+a_i\delta_{ij})))a_k^*a_k^*+(\prod_{i=0}^{k-1}a_i^*)a_k^+a_k^*](\prod_{j=k+1}^{n}a_i^*\\
&= [(\sum_{j=0}^{k-1}\prod_{i=0}^{k-1}(a_i^+(1+a_i\delta_{ij})))a_k^*+(\prod_{i=0}^{k-1}a_i^*)a_k^+](\prod_{j=k+1}^{n}a_i^*\\
&= (\sum_{j=0}^{k}\prod_{i=0}^{k}(a_i^+(1+a_i\delta_{ij})))(\prod_{j=k+1}^{n}a_i^*),
\end{aligned}
$$

using lemma 8.4 (ii), (31) and (44). But

$$(\sum_{j=0}^{k}\prod_{i=0}^{k}(a_i^+(1+a_i\delta_{ij})))(\prod_{j=k+1}^{n}a_i^*)\leq\sum_{j=0}^{n}\prod_{i=0}^{n}(a_i^+(1+a_i\delta_{ij})),$$

since the left-hand side lacks those elements of the sum, where all a_i for $0 \leq i \leq k$ carry a Kleene star and some a_j with $k < j \leq n$ a Kleene plus (maybe $k = n$). Concluding, putting the calculations together,

$$\begin{aligned}(\sum_{i=0}^{n}a_i)^+ &= \sum_{i=0}^{n}(a_i\prod_{j=0}^{n}a_i^*)\\ &\leq \sum_{i=0}^{n}\sum_{j=0}^{n}\prod_{k=0}^{n}(a_k^+(1+a_k\delta_{kj}))\\ &= \sum_{j=0}^{n}\prod_{i=0}^{n}(a_k^+(1+a_k\delta_{ij}))\end{aligned}$$

by idempotence of addition and renaming of the indices. □

9. Conversion and Functions

To present more traditional variants of the algebraic Church-Rosser statement of proposition 7.1, we add a *converse* operator. A *Kleene algebra with converse* is a tuple $(A, +, \cdot, ^*, ^\circ, 0, 1)$, where $(A, +, \cdot, ^*, 0, 1)$ is a Kleene algebra and the unary operation $^\circ$ is a contravariant involution that distributes with addition and the Kleene star:

$$a^{\circ\circ} = a, \qquad (a+b)^\circ = a^\circ + b^\circ, \qquad (ab)^\circ = b^\circ a^\circ, \qquad a^{*\circ} = a^{\circ *}.$$

Lemma 9.1. *Let A be a Kleene algebra with converse. For all $a, b \in A$.*

(i) $a \leq b \Leftrightarrow a^\circ \leq b^\circ$ *iff* $(a+b)^\circ = a^\circ + b^\circ$.
(ii) $1^\circ = 1$.
(iii) $0^\circ = 0$.

Proof. (ad i) $a \leq b \Leftrightarrow a^\circ \leq b^\circ$ implies $(a+b)^\circ = a^\circ + b^\circ$. We assume $a \leq b \Leftrightarrow a^\circ \leq b^\circ$ and show $(a+b)^\circ \leq a^\circ + b^\circ$ and $a^\circ + b^\circ \leq (a+b)^\circ$.

$(a+b)^\circ \leq a^\circ + b^\circ$. By definition of the supremum, $a^\circ \leq a^\circ + b^\circ$ and $b^\circ \leq a^\circ + b^\circ$. Hence $a = a^{\circ\circ} \leq (a^\circ + b^\circ)^\circ$ and $b \leq (a^\circ + b^\circ)^\circ$ and therefore $a + b \leq (a^\circ + b^\circ)^\circ$. By monotonicity of the converse operator therefore $(a+b)^\circ \leq (a^\circ + b^\circ)^{\circ\circ} = a^\circ + b^\circ$.

$a^\circ + b^\circ \leq (a+b)^\circ$. $a \leq a + b$ and $b \leq a + b$ imply $a^\circ \leq (a+b)^\circ$ and $b^\circ \leq (a+b)^\circ$ and therefore $a^\circ + b^\circ \leq (a+b)^\circ$.

$(a+b)^\circ = a^\circ + b^\circ$ implies $a \leq b \Rightarrow a^\circ \leq b^\circ$. We assume $(a+b)^\circ = a^\circ + b^\circ$ and show $a \leq b \Rightarrow a^\circ \leq b^\circ$. By definition of the ordering, $a \leq b$ iff $a + b = b$. Thus $b^\circ = (a+b)^\circ = a^\circ + b^\circ$ and therefore $a^\circ \leq b^\circ$ by definition of the ordering.

$(a+b)^\circ = a^\circ + b^\circ$ implies $a^\circ \leq b^\circ \Rightarrow a \leq b$. We assume $(a+b)^\circ = a^\circ + b^\circ$ and show $a^\circ \leq b^\circ \Rightarrow a \leq b$. By definition $a^\circ \leq b^\circ$ iff $a^\circ + b^\circ = b^\circ$. Thus

$$b = b^{\circ\circ} \leq (a^\circ + b^\circ)^\circ = a^{\circ\circ} + b^{\circ\circ} = a + b,$$

and therefore $a \leq b$ by definition of the ordering.

(ad ii) $1 = 1^{\circ\circ} = (11^\circ)^\circ = 1^{\circ\circ}1^\circ = 11^\circ = 1^\circ$.

(ad iii) $0 = 0^{**} = (0 + 0^*)^* = 0^* + 0^{**} = 0^* + 0 = 0^*$. □

Kleene algebras with converse allow the definition of partial and total functions, injections or surjections. We will need functions in section 10 and section 15. An element a of a Kleene algebra A is *total* or *entire*, if $1 \leq aa^\circ$, *functional* or *simple*, if $a^\circ a \leq 1$, *surjective*, if a° total, *injective*, if a° functional and a *mapping*, if it is total and functional. From these definitions one can derive many of the usual properties of functions. We need only two of them.

Lemma 9.2. *The properties simple, entire, map are preserved by composition.*

Lemma 9.3. *Let A be a Kleene algebra with converse. For all $a, b, f \in A$ and f a function,*

(i) $af \leq b \Leftrightarrow a \leq bf^\circ$.
(ii) $f^\circ a \leq b \Leftrightarrow a \leq fb$.

The following corollaries are the Church-Rosser statements.

Corollary 9.4. *For every element a of some Kleene algebra A with converse,*

$$a^\circ a^* \leq a^* a^{\circ *} \Rightarrow (a + a^\circ)^* \leq a^* a^{\circ *}.$$

Proof. Let $b = a^\circ$ in theorem 7.2 (i). □

Of course, $a^\circ a^* \leq a^* a^{\circ *} \Leftrightarrow a^{\circ *} a^* \leq a^* a^{\circ *}$ by (40). Moreover the right-hand-side of the implication can again be strengthened to an equality by (41).

Corollary 9.5. *For all elements a and e of some Kleene algebra A with converse,*

$$ea^* \leq a^* e^*, a^{\circ *} a^* \leq a^* a^{\circ *}, a^{\circ *} e^* \leq e^* a^{\circ *} \Rightarrow (a + e + a^\circ)^* \leq a^* e^* a^{\circ *}.$$

Proof. Let $n = 2$, $a_0 = a$, $a_1 = e$ and $a_2 = a^*$ in theorem 7.4 (i). □

Corollary 9.5 is a variant of a Church-Rosser theorem modulo. The transition from Church-Rosser statements without a converse to those with that operation did not use any algebraic properties of the converse. It worked by mere insertion. In this sense, corollary 9.4 and corollary 9.5 are simple instances of proposition 7.1 and 7.4. We will discuss this further in section 12, where we present the transition from Kleene algebras to rewrite relations.

10. Allegories

In this section, we discuss applications of allegories to algebraic Church-Rosser proofs. Allegories have been introduced by Freyd and Scedrov [9] as relational extensions of categories. They can also be seen as typed relation algebras and typed Kleene algebras. In our setting, allegories are interesting for three reasons. They allow us first to rigorously connect algebraic and diagrammatic reasoning, second to determine well-foundedness assumptions, like in Newman's lemma and third to introduce types for Kleene algebra expressions.

Briefly, an *allegory* is a category that besides the identity arrows and the partial operation of composition of arrows is also endowed with the total operation of conversion $^\circ$ and the partial associative, commutative and idempotent operation $\cap$ of intersection. The operations are partial, since they are constrained by source-target conditions on arrows. Finally, there are algebraic laws like distributivity of the converse over intersection,

$$(a \cap b)^\circ = a^\circ \cap b^\circ,$$

the semi-distributivity laws

$$a(b \cap c) \leq ab \cap ac, \qquad (a \cap b)c \leq ac \cap bc$$

and the modular law

$$ab \cap c \leq (a \cap cb^\circ)b.$$

For a formal definition, see [9].

As usually in categories we write $a : A \to B$ if a has source A and target B. Typical source-target or type constraints are that $a : A \to B$ implies $a^\circ : B \to A$

or $ab : A \to C$ is defined, if $a : A \to B$ and $b : B \to C$ for some object or type B. Categories encode source target information via commuting diagrams. In allegories, semi-commuting diagrams take their role. The diagram

$$\begin{tikzcd} & B \arrow[dr, "b"] \arrow[d, phantom, "\leq"] & \\ A \arrow[ur, "a"] \arrow[rr, "c"'] & {} & C \end{tikzcd}$$

semi-commutes, if $ab \leq c$. In case of one-object allegories, source-target information is irrelevant. Thus the concept of a semi-commuting diagram can be transferred to Kleene algebras and the Church-Rosser statements visualized as allegorical semi-commuting diagrams. The usual diagrams of rewriting theory can therefore be identified formally with the allegorial ones.

An allegory is *distributive* if it contains an operation of addition $+$ and a unit 0 that turns the allegory into a distributive lattice with zero with respect to intersection and a semiring with respect to composition. Moreover, conversion distributes over addition. An allegory is *locally complete*, if the underlying lattice is complete and composition and finite intersections distribute with arbitrary sums. Thus Kleene algebras are one-object allegories without intersection and converses, but with an explicit fixed point constructor. Of course, in an allegory, fixed points can be modeled as limits or colimits. This means that our algebraic Church-Rosser proofs can also be carried out in allegories.

In section 9, we defined functions in a Kleene algebra. This definition can be easily adapted to allegories by typing. Let $f : C \to A$ and $g : C \to B$ be functions and $a : A \to B$ an arrow of some allegory. The pair (f, g) is a *tabulation* of a, if

$$f^\circ g = a, \qquad ff^\circ \cap gg^\circ = 1.$$

An allegory is *tabular*, if every arrow has a tabulation. Since relations are thus reducible to functions, tabular allegories (with an additional assumption on units) are isomorphic with certain (regular) categories [9]. Tabular allegories can be used to simulate point-wise proofs (c.f. [5] for examples). On the other hand, the allegory of set-theoretic (binary) relations is tabular, since—in the above notation, C can be identified with a subset of the cartesian product $A \times B$ and f and g with the projection functions.

We now present proofs of a variant of Newman's lemma to show the extendibility and the limitations of our point-free approach to rewriting.

11. Algebraic Proofs of Newman's Lemma

There seem two directions for generalizing the Church-Rosser statements of section 7 and section 8. First, weakening the assumption $ba^* \leq a^*b^*$ to $ba \leq a^*b^*$ in proposition 7.1. Second, weakening the assumption $a_j a_i^* \leq a_i^* a_j^*$ to $a_j a_i^* \leq \prod_{i=o}^n a_i^*$ in proposition 7.4. Of course there are related directions dealing with the Kleene plus.

We call occurances of ba in a Kleene algebra term a *reversal* and those of a^*b^* or $a^+b^* + a^*b^+$ a *rearrangement*. In analogy to trace theory we say that *a semi-commutes* over b, if $ba \leq a^*b^*$ (or $ba \leq a^+b^* + a^*b^+$). We call chains of Kleene algebra terms, where reversals are successively replaced by rearrangements *rearrangement chains*. Of course, our above examples lead to infinite rearrangement chains. In the first case, consider the inequality $ba \leq aa + bb (\leq a^*b^*)$ on the word bba. We obtain the infinite rearrangement chain

$$bba \leq baa + bbb \leq aaa + bba + bbb \leq aaa + baa + bbb \leq aaa + bba + bbb \leq \dots$$

Obviously, $ba \leq a^*b^*$, but neither $ba^* \leq a^*b^*$, nor $(a + b)^* \leq a^*b^*$.

In the second case, consider the inequalities $ba \leq bc$, $cb \leq ab$ on the word bab. We obtain the infinite rearrangement chain

$$bab \leq bcb \leq bab \leq bcb \leq \ldots$$

Obviously, $ba^* + ca^* + cb^* \leq a^*b^*c^*$, but not $(a+b+c)^* \leq a^*b^*c^*$.

Both chains have in common that they do not become stationary after finitely many steps but alternate between two states.

Conversely, it is clear that the semi-commutation conditions in the Church-Rosser statements can be weakened in the above way, if all rearrangement chains are finite. The question is now how to replace this generic termination condition by a condition on Kleene algebra terms (like Newmans lemma depends on a well-foundedness assumption on relations). First it seems appropriate to introduce an ${}^\omega$-operation that formalizes greatest post-fixed points of chains of powers as greatest solution to the monotonic mapping $\lambda x.ax$. This allows us not only to describe infinite rearrangement chains, but also to connect Kleene algebra terms with well-foundedness: If a is a set-theoretic relation, then $a^\omega = 0$ iff a is well-founded. We use the following properties.

$$a^\omega \leq aa^\omega, \tag{60}$$

$$a^\omega \leq a^\omega a, \tag{61}$$

$$c \leq ac \Rightarrow c \leq a^\omega, \tag{62}$$

$$c \leq ca \Rightarrow c \leq a^\omega. \tag{63}$$

But it does not seem obvious to derive such a condition from chains like the aboves. Therefore it also seems necessary to introduce positions, where semi-commutations occur, as first-class citizens. This can be done by tabulations. The situation is very interesting, since a transition from Church-Rosser statements to variants of Newman's lemma seems to force a transition from the point-free to the point-wise style.

For our purposes we need the following properties.

Proposition 11.1 (Freyd, Scedrov, p.200, 2.143). *Let (f, g) be a tabulation of a; let x and y be functional. Then $x^\circ y \leq a$ iff there exists a (necessarily unique) functional arrow $h = xf^\circ \cap yg^\circ$ such that $x = hf$, $y = hg$, that is the following diagram semi-commutes.*

$$\begin{tikzcd}
& \cdot \arrow[dl, "x"'] \arrow[dr, "y"] \arrow[dd, "h"] & \\
\cdot & & \cdot \\
& \cdot \arrow[ul, "f"] \arrow[ur, "g"'] &
\end{tikzcd}$$

Corollary 11.2. *Tabulations of an arrow are unique up to isomorphism.*

We henceforth assume a tabular allegory.

Proposition 11.3 (Freyd, Scedrov, p.201 2.146). *Let x, y, f, g be maps. Then $x^\circ y \leq fg^\circ \Leftrightarrow xf = yg$.*

$$\begin{tikzcd}
& \cdot \arrow[dr, "y"] & \\
\cdot \arrow[ur, "x^\circ"] \arrow[dr, "f"'] \arrow[rr, phantom, "\leq"] & & \cdot \\
& \cdot \arrow[ur, "g^\circ"'] &
\end{tikzcd}
\quad \Leftrightarrow \quad
\begin{tikzcd}
& \cdot \arrow[dl, "x"'] \arrow[dr, "y"] & \\
\cdot \arrow[dr, "f"'] & & \cdot \arrow[dl, "g"] \\
& \cdot &
\end{tikzcd}$$

Lemma 11.4. *(f_a, g_a) is a tabulation of a iff (g_a, f_a) is a tabulation of a°.*

Proof. Let (f_a, g_a) be a tabulation of a. Then $a^\circ = (f_a^\circ g_a)^\circ = g_a^\circ f_a$. Moreover, $g_a g_a^\circ \cap f_a f_a^\circ = 1$, since (f_a, g_a) is a tabulation of a. Thus (g_a, f_a) is a tabulation of a°. The converse direction is similar. □

The following statement relates the tabulation of a product with the tabulations of the factors. We call a *subtabulation* of arrow a a pair of mappings (f, g) such that $f^\circ g = a$ (but not necessarily $ff^\circ \cap gg^\circ = 1$). We introduce this definition since we do not want to bother with the universality condition of tabulations.

Proposition 11.5. *Let (f_a, g_a) and (f_b, g_b) be tabulations of a and b. Let (f_c, g_c) be a tabulation of $c = g_a f_b^\circ$ and (f_{ab}, g_{ab}) a tabulation of ab.*

(i) *$(f_c f_a, g_c g_b)$ is a subtabulation of ab.*

$$\begin{tikzcd}
 & & \cdot \arrow[dl, "f_c"'] \arrow[dr, "g_c"] & & \\
 & \cdot \arrow[dl, "f_a"'] \arrow[dr, "g_a"] & & \cdot \arrow[dl, "f_b"'] \arrow[dr, "g_b"] & \\
\cdot & & \cdot & & \cdot
\end{tikzcd}$$

(ii) *There exists a unique mapping h such that $hf_{ab} = f_c f_a$ and $hg_{ab} = g_c g_b$.*

$$\begin{tikzcd}
 & & \cdot \arrow[ddll, "f_{ab}"'] \arrow[ddrr, "g_{ab}"] & & \\
 & & \cdot \arrow[u, "h"] \arrow[dl, "f_c"'] \arrow[dr, "g_c"] & & \\
\cdot & \cdot \arrow[l, "f_a"'] \arrow[r, "g_a"] & \cdot & \cdot \arrow[l, "f_b"'] \arrow[r, "g_b"] & \cdot
\end{tikzcd}$$

Proof. (ad i) First, $f_c f_a$ and $g_c g_a$ are mappings since this property is preserved by composition. We have to show that $ab = (f_c f_a)^\circ (g_c g_b)$

$$ab = f_a^\circ g_a f_b^\circ g_b = f_a^\circ c g_b = f_a^\circ f_c^\circ g_c g_b = (f_c f_a)^\circ (g_c g_b).$$

(ad ii) This is an immediate consequence of proposition 11.1. □

Note that the pair (f_c, g_c) is actually a pullback of (g_a, f_b).

Lemma 11.6. *Under the same conditions as in lemma 11.5, let $h_{ab} = f_c g_a$.*

(i) $f_c g_a = g_c b_f$.
(ii) $f_c f_a \leq h_{ab} a^\circ$, $g_c g_b \leq h_{ab} b$.
(iii) $ab = (h_{ab} a^\circ)^\circ (h_{ab} b)$.

Proof. (ad i) This is an immediate consequence of proposition 11.3.

(ad ii) We show only the equality for a°, the other being equal. From the diagram in lemma 11.5,

$$a = f_a^\circ g_a = f_a^\circ f_c^\circ f_c g_a = f_a^\circ f_c^\circ h_{ab},$$

hence in particular $(f_c f_a)^\circ h_{ab} \leq a$. Equivalently therefore $(f_c f_a)^\circ \leq a h_{ab}^\circ$ by lemma 9.3 and $f_c f_a \leq h_{ab} a^\circ$ by properties of the converse.

(ad iii) Using (ii), simplicity of h_{ab} and properties of converse we obtain

$$\begin{aligned}(h_{ab} a^\circ)^\circ (h_{ab} b) = a h_{ab}^\circ h_{ab} b \leq ab = (f_c f_a)^\circ (g_c g_b) \\ \leq (h_{ab} a^\circ)^\circ (g_c g_b) \leq (h_{ab} a^\circ)^\circ (h_{ab} b).\end{aligned}$$

□

Given a reversal ba, the intuition is that h_{ab} points at the vertex between b and a, whereas f_{ba} and g_{ba} point at the initial and final vertex. Writing ba as $(h_{ab}b^\circ)^\circ(h_{ab}a)$ uses b° and a to point at the initial and final vertex.

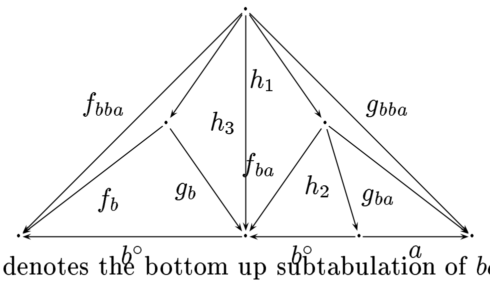
Lemma 11.6 generalizes to words $w = w_1w_2$, using subtabulations (f_{w_1}, g_{w_1}) and (f_{w_2}, g_{w_2}). Thus pointers to vertices of a word can be constructed recursively from the pointers of subwords, starting at some arbitrary subword. The recursion is defined as follows. We call a subtabulation of a word w *bottom up*, if it has been constructed from tabulations of its letters as in 11.6.

Corollary 11.7. *Let a, b be letters, w a word and (f_w, g_w) a bottom-up subtabulation of w. Then there exists some maps h (different in the following equations) such that*

$$h_{bw} = hf_w, \qquad h_{wa} = hg_w,$$
$$bw = (hf_wb^\circ)^\circ(hg_w), \qquad wa = (hf_w)^\circ(hg_wa).$$

Proof. For the first equality in the first row set $h = g_c$, for the second equality $h = f_c$ in the above diagram. For the first equality in the second row set $w = a$ and $h = g_c$, for the second equality set $w = b$ and $h = f_c$ in the above diagram. Then lemma 11.6 yields the result. □

For example, $bba = (hb^\circ b^\circ)^\circ(ha)$ using this corollary, setting $h = h_1h_2$ in the diagram



Thereby (f_{bba}, g_{bba}) denotes the bottom up subtabulation of ba and (f_ba, g_{ba}) that of ba. The computation is

$$\begin{aligned} bba = f_{bba}^\circ g_{bba} &\leq (h_3b^\circ)^\circ(h_1g_{ba} \\ &= (h_1f_{ba}b^\circ)^\circ(h_1h_2a) \\ &\leq (h_1h_2b^\circ b^\circ)^\circ(ha) \\ &= (hb^\circ b^\circ)^\circ(ha) \\ &= bbh^\circ ha \\ &\leq bba. \end{aligned}$$

Lemma 11.8. *Let v_0 be a reversal in a word w. Rearranging the reversal introduces at most two new reversals v_1 and v_2.*

(i) *In the allegorial setting, $h_{v_1} = hf_{v_0}$ and $h_{v_2} = kg_{v_0}$ for some mappings h and k.*

(ii) *With respect to rearrangement sequences, the new reversals occur at the beginning and the end of the rearrangement.*

Proof. (ad i) Set $w = bbaa$ and let ba be rearranged by ab. Then $w' = baba$ and there are two new reversals. By the construction of bottom up subtabulations, the f and g mapping of the initial reversals point to the centers of the new ones.

(ad ii) Obvious. □

We call two reversals v and v' in words w and w' *connected*, if w is a predecessor of w', v is rearranged and v' occurs at the beginning or the end of the respective rearrangement.

Lemma 11.9. *A rearrangement chain on words (without addition) terminates iff the chain contains only finitely many connected reversals.*

Proof. We construct a reversal tree as follows. Let the initial word w_0 contain reversals $v_1, \ldots, v_n$. Then we add to the root of the tree nodes labeled by 1 to n. When rearranging w_0 by w_1 at v_i introduces a reversal at the beginning (end) of the rearrangement, we index the reversal with $i0$ ($i1$) and add a vertex labeled with that index and an arc between the vertex labeled with i and the new one to the tree. We iterate the construction for each rewriting. Then by König's lemma, the tree has an infinite branch (an infinite chain of connected reversals), iff the rearrangement chain is infinite. $\square$

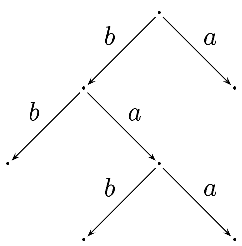
Lemma 11.10. *Let $a+b$ be a Kleene algebra term. There is an infinite rearrangement chain from $a+b$ iff there is such a chain from a or b.*

This lemma allows us to generalize lemma 11.9 from words to full Kleene algebra expressions, by constructing a forest instead of a tree, splitting for each addition. Then non-termination occurs iff there is a tree with an infinite branch in the forest. We therefore neglect addition henceforth without loss of generality.

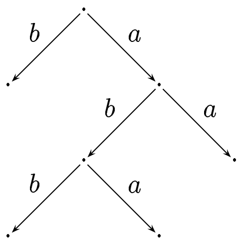
Theorem 11.11. *Let A be (the Kleene algebra fragment of) an one-object distributive tabular allegory. For all $a, b \in A$,*

$$ba \leq a^*b^*, (a + b^\circ)^\omega = 0 \Rightarrow (a + b)^* \leq a^*b^*.$$

Proof. By lemma 11.6 and corollary 11.7, we can construct a subtabulation and a characteristic word for each chain of reversals corresponding to a sequence of rewrites. The center of each initial reversal v_1 is identified by a map h_1. Hence these maps are in one-to-one correspondence with he successor nodes of the root of the reversal tree. When rewriting the initial word w_0 to w_1 at v_i introduces a reversal at the beginning (end) of the reduct, we add maps h_{i0} (or h_{i1}) that are constructed from the f_i (or g_i). We also obtain words h_ib° (or h_ia) in one-to-one correspondence with h_{i0} (or h_{i1}). We can therefore label the lowest arcs of the reversal tree with b° or a respectively. Iterating this construction for each semi-commutation we obtain a labeling of the arcs of the reversal tree in one-to-one correspondence with the set of characteristic words for chains of connected reversals. In the situation depicted in the diagram



for instance, one considers first the subtabulation for the highest reversal, which yields a characteristic word hb°. Since the lowest reversal occurs at the end of the middle one, the next subtabulation to construct is that of $a^\circ ba$ which leads to the word $h'b^\circ a^{\circ\circ} = h'b^\circ a$. On the other hand, a situation like



leads to the word hab° via the subtabulation of bab°. In general, forgetting the h-part, the construction of characteristic words can be described by $w_{i+1} = (a+b^\circ)w_i$, thus we look in general for solutions of the equation $x = (a + b^\circ)x$. Of course the associated rearrangement chain is not stationary after finitely many steps iff $(a + b^\circ)^\omega \neq 0$. Hence we have established a one-to-one correspondence between an infinite branch of the reversal tree and an infinite characteristic word. ☐

The construction immediately transfers to algebras with three or more letters.

Theorem 11.12. *Let A be (the Kleene algebra fragment of) an one-object distributive tabular allegory. For all $a, b, e \in A$,*

$$ba + ca + cb \leq a^*b^*c^*, (a + b + b^\circ + c^\circ)^\omega = 0 \Rightarrow (a + b + c)^* \leq a^*b^*c^*.$$

Proof. Similar to that of theorem 11.11. ☐

To encode the construction of characteristic words in theorem 11.12 algorithmically, we can use the rewrite rules $b|w|a \to |wb^\circ|c|wa|$, where $c \leq a^*b^*$, and start with $|w| = |1|$. For each word produced this way one can uniquely tell how it has been produced by rewriting. Given a word $w_0|xb^0|w_1|xa|w_2$, one knows that the immediate ancestor (up to independent non-interfering inferences) is $w_0b|x|wa$ etc. Projecting out the expressions between bars (reading is unique) one can thus reconstruct the original sequence (up to independent rewrites).

12. Set-Theoretic Relations and Rewrite Systems

We assume that the usual regular operations of addition, multiplication and Kleene star are defined on the category Rel of set-theoretic relations. In particular the Kleene star is identified with the reflexive transitive closure.

Theorem 12.1. *Rel is a *-continuous Kleene algebra.*

The axioms of the idempotent semiring are obvious. The natural ordering $\leq$ is given by set-theoretic inclusion $\subseteq$. According to lemma 4.6, idempotent semirings satisfying the *-continuity axiom are automatically Kleene algebras. The key to showing *-continuity are the infinite distributivity laws $S(\bigcup_{i\in\mathbb{N}} R_i) = \bigcup_{i\in\mathbb{N}}(SR_i)$ and $(\bigcup_{i\in\mathbb{N}} R_i)S = \bigcup_{i\in\mathbb{N}}(R_iS)$. Thus

$$RS^*T = R(\bigcup_{i\in\mathbb{N}} S^i)T = \bigcup_{i\in\mathbb{N}}(RS^iT) = \sup(RS^iT : i \in \mathbb{N}).$$

Of course set-theoretic relations have additional algebraic properties, but these are not needed for Church-Rosser proofs. Proposition 7.1, proposition 8.1 and corollary 9.4 together with theorem 12.1 immediately yield the following results.

Theorem 12.2 (Church-Rosser)**.** *Let R and S be binary relations on a set A.*

(i) $R^\circ R^* \subseteq R^*R^{\circ *} \Rightarrow (R \cup R^\circ)^* = R^*R^{\circ *}$.
(ii) $SR^* \subseteq R^*S^* \Rightarrow (R \cup S)^* = R^*S^*$.
(iii) $SR^+ \subseteq R^+S^* \cup R^*S^+ \Rightarrow (R \cup S)^+ = R^+S^* \cup R^*S^+$.

(i) expresses the standard equational Church-Rosser theorem, whereas (ii) and (iii) are those for quasi-orderings [16] and transitive relations [20], respectively. Our algebraic arguments show that the Church-Rosser theorem of equational rewriting is just a special case of the non-equational ones and that the theorems deal essentially with semi-commutation, a property similar to sorting. Of course they can also be stated allegorically via semi-commuting diagrams. Finally, on can also express the Church-Rosser statements logically. We have already argued in lemma 2.3 that the expressions $R^{\circ}R^* \subseteq R^*R^{\circ *}$ and

$$\forall w, x, y.((w,x) \in R \wedge (w,y) \in R^* \Rightarrow \exists z.(x,z) \in R^* \wedge (y,z) \in R^*)$$

are logically equivalent. The first is therefore a point-free relational abstraction of the logical $\forall\exists$-expression. According to the discussion in section 10, we can also translate relational variants Church-Rosser theorems modulo and Newmans lemma from the allegorial statements in theorem 11.11 and theorem 11.12. Note, however, that the usual Church-Rosser theorem modulo (c.f. [11]) differs from ours, it requires further reasoning with equivalence relations. We leave the exact reconstruction to the following section.

13. Reconstructing Church-Rosser Modulo

We now adapt our algebraic results to Church-Rosser theorems modulo a congruence relation in the spirit of [11]. More precisely, we study the more general case of two rewriting relations R and S modulo an equivalence relation E^*. According to this approach, E is incorporated in the well-foundedness assumption. Also, the commutations of the rewrite rules with the rules from E are studied to make computations effective. The main idea of rewriting modulo—in the term case—is that part of the E-steps is dealt with explicitly via semi-commutation, whereas others can be neglected at the abstract level and treated via E-unification at the term level. Intuitively, $R/E = E^*RE^*$ and $S/E = E^*SE^*$ model R- and S-rewrite steps on E-equivalence classes. To integrate E-unification, one uses rewrite relations R_E and S_E instead that are defined by $R \subseteq R_E \subseteq R/E$ and $S \subseteq S_E \subseteq S/E$. For a formal introduction consider [21]. Since R_E and S_E do not absorb all E-steps in expressions $(R \cup E \cup S)^*$, one not only must consider semi-commutations between R_E and S_E, but more generally those between R and S_E, between R_E and E, between R_E and S and between S_E and E. We will restrict our attention to the Kleene plus case and moreover to the case where at least one R or S-step occurs in $R \cup E \cup S$[2]. This means that we can deal with rearrangements of the form $R_E^+E^*S_E^* \cup R_E^*E^*S_E^+$.

Abstracting to the allegorial setting, we need to define an equivalence. In a Kleene algebra with converse an element a is *reflexive*, if $1 \leq a$, *transitive*, if $aa \leq a$ and *symmetric*, if $a \leq a^{\circ}$ and therefore $a = a^{\circ}$. We also follow the relational case to define $a/e = e^*ae^*$, $b/e = e^*be^*$[3] and a_e and b_e by $a \leq a_e \leq a/e$, $b \leq b_e \leq b/e$. To code $(a+e+b)^+$ excluding e^+, we write informally $(a+e+b)^*_{-e}$. More concisely, this can be expressed, for instance, by the Kleene algebra expression $((a+e+b)^*b+1)(a+e)^* + a^+$. We immediately obtain the following results from theorem 11.11 and theorem 11.12.

Corollary 13.1. *Let A be (the Kleene algebra fragment of) an one-object distributive tabular allegory. For all $a, b, e \in A$,*

$$(b/e)(a/e) \leq (a/e)^+e^*(b/e)^* + (a/e)^*e^*(b/e)^+, (a/e + e + b^+/e)^{\omega} = 0$$
$$\Rightarrow (a+e+b)^* \leq (a/e)^+e^*(b/e)^* + (a/e)^*e^*(b/e)^+.$$

[2]This restriction is justified by the application of this result to rewriting with a non-symmetric transitive relation. An explanation is beyond the scope of this text. For more information c.f. [21].

[3]Note that this has nothing to do with the definition of division in an allegory (c.f. [9]).

Note that $(a/e)e^* = (a/e)$, since $e^*e^* = e^*$ in every Kleene algebra (cf. my extended version).

Corollary 13.2. *Let A be (the Kleene algebra fragment of) an one-object distributive tabular allegory. For all $a, b, e \in A$,*

$$b_e a + b a_e + e a_e + b_e e \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+, (a_e + e + b_e^\circ)^\omega = 0$$
$$\Rightarrow (a + e + b)_{-e}^+ \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+.$$

The following lemmata state general properties of $^\omega$-expressions and greatest fixed points that we leave without proof.

Lemma 13.3. *Let A be a Kleene algebra with greatest fixed point operator $^\omega$ and let $a, b \in A$. Then $a \leq b$ and $b^\omega = 0$ implies $a^\omega = 0$.*

Lemma 13.4. *Let A be a Kleene algebra with greatest fixed point operator $^\omega$ and let $a \in A$ be a set-theoretic relation. Then $a^\omega = 0$ iff a is well-founded iff a^+ is well-founded.*

Therefore the assumption $(a_e + e + b_e^\circ)^\omega = 0$ in corollary 13.2 can be weakened to $(a/e + e + b^\circ/e)^\omega = 0$. Also the assumption $(a + e + b)^\omega = 0$ is weaker than $(a/e + e + b^\circ/e)^\omega = 0$.

Corollary 13.2 is already very similar to a standard Church-Rosser modulo theorem. The only difference is that in the relational version of the latter, a well-foundedness assumption corresponding to $(a/e + b^\circ/e)^\omega = 0$, but not $(a/e + e + b^\circ/e)^\omega = 0$ is used. We now argue how to get rid of the e. This does not follow from well-foundedness assumptions alone. Thus the semi-commutation relations and the arguments of section 11, in particular theorem 11.11 must be reconsidered.

Theorem 13.5. *Let A be (the Kleene algebra fragment of) an one-object distributive tabular allegory. For all $a, b, e \in A$,*

$$b_e a + b a_e + e a_e + b_e e \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+, (a_e + b_e^\circ)^\omega = 0$$
$$\Rightarrow (a + e + b)_{-e}^+ \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+.$$

Proof. Reconsider the reversal tree of lemma 11.9 and theorem 11.11. We must show that it does not contain any infinite e-branches. By definition of $(a+e+b)_{-e}$ we can assume that the initial chain contains at least one a_e or b_e. For our purposes we (exhaustively) classify two different types of infinite e-branches. Those who always connect left successor nodes with left successor nodes or right successor nodes with right successor nodes and those who at some stage connect a left successor node with a right one or vice versa. We say that the first kind of e-branch does not zig-zag, whereas the second kind does. Note that this classification is sound since the construction of reversal trees does not allow us to flip subtrees.

We first show that there is no infinite zig-zag e-branch. There are two kinds of reversals that can generate such branches, namely those of the form $e a_e \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+$ and $b_e e \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+$. Since the two situations are symmetric, we consider only the first one. By lemma 11.10, we can further split our consideration into two cases; one where the reversal is rearranged by the expression $a_e^+ e^* b_e^*$ and the other where this is done by $a_e^* e^* b_e^+$. The first case cannot lead to a zig-zag chain, since the zag-step after the zig-step e is of the form a_e. In the second case, assume that $a_e^* = 1$. This would lead to a bad zig-zag step. But the inequality $e a_e \leq e^* b_e^+$ is equivalent to $a_e \leq e^+ b_e^+$ by lemma 9.3. But since $a^+ \leq a^*$ holds for every element a of a Kleene algebra, $a_e \leq e^* b_e^+ \leq (b/e)^+$. Without loss of generality we may assume that $a_e \leq b/e$. (Note that $a \leq a^+$ in every Kleene algebra). Then $(a/e + b^\circ/e)^\omega = 0$ implies $(a/e + a_e^\circ)^\omega = 0$. Conversely, $(a/e + a^\circ/e)^\omega \neq 0$ implies

$(a/e + b^\circ/e)^\omega \neq 0$. But $(a/e + a^\circ/e)^\omega \neq 0$ cannot be in general excluded. Hence the above zig-zag branch leads to a violation of our well-foundedness assumption.

We now show that there is no infinite non-zig-zag e branch. We again restrict our attention to reversals of the form $ea_e \leq a_e^+ e^* b_e^* + a_e^* e^* b_e^+$, the other case being symmetric. Now by construction of the reversal tree, the infinite branch under consideration can only exist if at infinitely many steps of the construction of the reversal tree there exists a reversal immediately left of that under consideration that generates words of the form $a_e^+ e^+$. Thus this reversal must be of the form ea_e, otherwise the above argument for the zig-zag case applies. Then either this left-hand side reversal is connected with a zig-zag branch, such that there also is an infinite $(a/e + b^\circ/e)$-branch, or this is not the case. So consider the left-most non-zig-zag e-branch instead. Iterating this argument to the left-most infinite non-zig-zag e-branch, there cannot be any further reversal generating the necessary e-steps. Thus for every infinite non-zig-zag e-branch, there is also one of the form $(a/e + b^\circ/e)$ and we can in general use the well-foundedness assumption $(a/e + b^\circ/e)^\omega = 0$. □

14. Church-Rosser Modulo by Proof Transformation

To compare our reconstruction with the standard technique, we also give the proof of a variant of Church-Rosser modulo by proof transformation. The main idea of this technique (c.f. [2]), is to assign a complexity measure to individual R-S- and E-steps, to incorporate this measure into a well-founded ordering and to show that each rearrangement leads to a smaller proof. This means in particular that a certain monotonicity property must be satisfied: a local rearrangement must decrease the measure for arbitrary global proof contexts. By well-foundedness, obviously, each initial proof is transformed into a proof without any reversals after finitely many steps.

Consider a rewrite system (A, R, S, E) consisting of a set A and rewrite relations R, S and E, such that E^* is an equivalence. We define R/E, R_E, S/E and S_E as in section 13. For the sake of brevity, we set

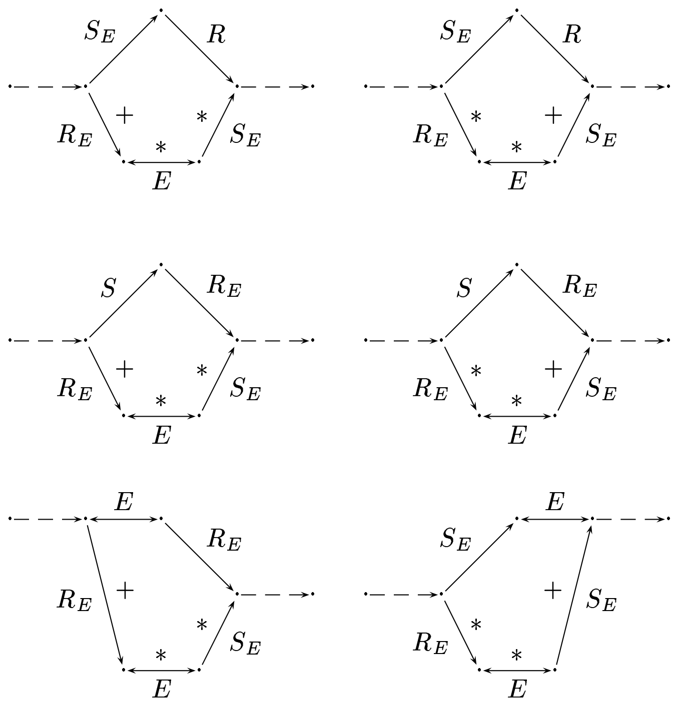
$$P\downarrow = R_E^+ E^* S_E^* \cup R_E^* E^* S_E^+.$$

We say that R *weakly commutes modulo* E over S_E, or R_E *weakly commutes modulo* E over S, if the corresponding reversal $S_E R$ or SR_E is contained in $P\downarrow$. An $R \cup S \cup E$-sequence can be *rearranged modulo* E, if it can be replaced by a sequence in $P\downarrow$. The rewrite system has the *rearrangement property* (modulo E), if all sequences, which are not of the form E^+, can be replaced by sequences in $P\downarrow$, We call the left E-steps of an R_E-step *left-covered* and the right E-steps of an S_E-step *right-covered*. The rewrite system *terminates*, if the relation $(R/E \cup S^{-1}/E)^+$ is well-founded.

Covering is used in the proof of theorem 14.2, since the identification of E-steps which occur within R_E-steps and S_E-steps and hence in a pictorial sense are covered, will be a means to to make the measure of the proof transformation steps anti-monotonic with respect to replacement of chains.

Lemma 14.1. *In a terminating rewrite system (A, R, S, E) each $P\downarrow$-sequence replacing an ER_E-sequence contains at least one R-step and each $P\downarrow$-sequence replacing a $S_E E$-sequence contains at least one S-step.*

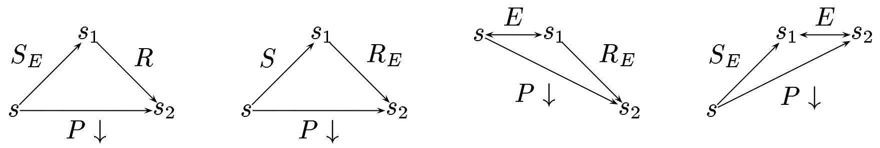
Proof. The semi-commutations to be considered for rearrangements are shown in the following diagrams.



It is easy to check for cycles in these diagrams, when the conditions in the lemma are not satisfied. $\square$

Note the correspondence of this statement with our argument against zig-zag-branches in section 13

Theorem 14.2. *A terminating rewrite system (A, R, S, E) has the rearrangement property modulo E, if the diagrams*



semi-commute.

Proof. The general scenario again consists in showing that the rearrangements corresponding to the semi-commuting diagrams decrease measures for proof with respect to the proof ordering defined below. More precisely, we associate an induction measure with each elementary reduction of a sequence and extend this measure to the whole sequence. An ordering will be constructed to compare the elementary reductions and the sequences according to our measure.

In case that the sequence consists solely of E-steps, there is nothing to rearrange. Hence we can concentrate on the case where sequences contain at least one elementary reduction different from E.

Since the ordering $\succ = (R/E \cup S^{-1}/E)^+$ is in principle an ordering on E-equivalence classes, and therefore E-compatible, one could imagine to simply measure terms by the individual steps in their E-equivalence classes. But this does not work. Consider the replacement

$$ER_E \longrightarrow R_E E = (EEER)E$$

of sequences. Clearly the measure associated with the right-hand sequence is bigger than the measure associated with the left-hand one. All E-steps belong to the same equivalence class and elementary reductions are extended to sequences by building multisets. One therefore must refine the ordering to distinguish E-steps occurring *inside* and *outside* an R_E-step or S_E-step, which amounts to include the distinction of left-covered and right-covered steps into our measure.

With the k-th elementary reduction of a sequence $\bar{t} = \langle t_0, \ldots, t_n \rangle$ we associate an elementary measure $\mu_k^{\bar{t}} \langle t_{\rho(k)}, \kappa_k^{\bar{t}} \rangle$, where

$$\rho(k) = \begin{cases} k-1 & \text{for } R\text{-steps and } E\text{-steps,} \\ k & \text{for } S\text{-steps.} \end{cases}$$

and the *cover number*

$$\kappa_k^{\bar{t}} = \begin{cases} 0 & \text{for } R\text{-steps and } S\text{-steps,} \\ 1 & \text{for left-covered and right-covered } E\text{-steps,} \\ 2 & \text{for left-covered, but not right-covered } E\text{-steps,} \\ 3 & \text{for right-covered, but not left-covered } E\text{-steps,} \\ 4 & \text{for non-covered } E\text{-steps.} \end{cases}$$

With the full sequence $\bar{t}$ we associate the measure

$$M(s) = \{\mu_1^{\bar{t}}, \ldots, \mu_n^{\bar{t}}\} = \{\langle t_{\rho(1)}, \kappa_1^{\bar{t}} \rangle, \ldots, \langle t_{\rho(n)}, \kappa_1^{\bar{t}} \rangle\}.$$

We define an induction ordering, also denoted by $\succ$,

$$\succ = ((\succ, >)_{lex})_{mul},$$

to compare sequences with respect to the associated measures. The elementary measures $\mu_i^{\bar{t}}$ are compared with respect to the lexicographic combination of $\succ$ and the standard ordering $>$ on $\mathbb{N}$; sequents are compared with respect to the multiset extension of the lexicographic combination.

Due to the construction of the ordering, sequences are compared with the help of transfinite ordinals and therefore the induction process is also transfinite.

In the following case analysis we show for all semi-commuting diagrams of the theorem, that the measure is globally anti-monotone with respect to each single replacement.

(Case i) Consider the diagram

$$\begin{tikzcd} & s_1 \arrow[dr, "R"] & \\ s \arrow[ur, "S_E"] \arrow[rr, "P\downarrow"'] & & s_2 \end{tikzcd}$$

Obviously the first component of μ_i^S associated to the S-reduction in the initial S_E-reduction of the reversal is equal to s_1 under $\succ$, since the ordering is E-compatible. If this reduction is not followed by an E-reduction, it majorizes the measure $M(sS_Es_1Rs_2)$, otherwise the succeeding E-reductions do, since they possess a bigger cover-number. The measure $M(P\downarrow)$ of the replacement is majorized either by the elementary measure associated with its initial or its final step, hence the first component of the elementary measure majorizing $P\downarrow$ is either equal to s or to s_2 with respect to $\succ$. But by well-foundedness of S and R, the elementary measure majorizing the reversal is greater than the elementary measure majorizing the replacement.

It remains to show monotonicity of the measure under context application, i.e.,

$$M(sS_Es_1Rs_2) \succ M(sP\downarrow s_2) \qquad \text{implies} \qquad M(\bar{t}[sS_Es_1Rs_2]) \succ M(\bar{t}[sP\downarrow s_2])$$

for an arbitrary sequence $\bar{t}$. This is not obvious since we must take into account the non-local effects of covering. Covering can change the size of measures, because covered step can become non-covered by the replacement and vice versa. But this only affects the second component of the elementary measures and the replacement is dominated by the first one. Therefore the anti-monotonicity of the measures corresponding to the rearrangement is preserved under context application and the above implication holds.

(Case ii) Consider the diagram

$$\begin{tikzcd} & s_1 \arrow[dr, "R_E"] & \\ s \arrow[ur, "S"] \arrow[rr, "P\downarrow"'] & & s_2 \end{tikzcd}$$

It is clearly symmetric to the first one, when reverting arrows and exchanging labels.

(Case iii) Consider the diagram

$$\begin{tikzcd} s \arrow[r, leftrightarrow, "E"] \arrow[drr, "P\downarrow"'] & s_1 \arrow[dr, "R_E"] & \\ & & s_2 \end{tikzcd}$$

By lemma 14.1 rearrangements $P\downarrow$ have to be of the form $R_E^{+}E^{*}S_E^{*}$, hence the diagram can be expanded as

$$\begin{tikzcd} s \arrow[r, leftrightarrow, "E"] \arrow[d, "R_E"', "+"] & s_1 \arrow[d, "R_E"] \\ \cdot \arrow[r, leftrightarrow, "*", "E"'] & \cdot \arrow[u, phantom] \end{tikzcd}$$

$$\begin{tikzcd} & s_1 \arrow[d, "R_E"] \\ & s_2 \\ \cdot \arrow[r, leftrightarrow, "*", "E"'] & \cdot \arrow[u, "*", "S_E"'] \end{tikzcd}$$

The first step of $P\downarrow$ can either be an E-step or and R-step, but then the first component of $\mu_1^{ER_E}$ and the first component of $\mu_1^{P\downarrow}$ are the same, namely s. Moreover s majorizes all first components in the reversal as well as in the rearrangement. Therefore we can entirely concentrate on the cover numbers.

If the first step in the rearrangement is an R-reduction, then $\kappa_1^{P\downarrow} = 0$. But $\kappa_1^{ER_E} > 0$ holds for the cover number of the initial reduction of the reversal. Since both initial reductions majorize their respective sequents, the measure of the reversal is greater than that of the rearrangement.

If the first step in the rearrangement is an E-reduction, then it is at least left-covered and therefore has $\kappa_1^{P\downarrow} \leq 2$. The E-reduction in the reversal is at least not left-covered, otherwise there would be no reversal to be replaced. Hence it is either right-covered or non-covered. In both cases $\kappa_1^{ER_E} \geq 3$. Again the measure of the reversal is greater than that of the rearrangement.

These cases are exhaustive for the diagram and therefore all reversals have bigger measures than the rearrangements. Finally we again have to consider the global impact of the rearrangement on the sequence. First observe that if the reversal is preceded by an E-sequence, then these outer E-reductions can never be covered by the R_E-reductions in the reversal, since otherwise the reversal under consideration needs not be replaced. But then there is always at least one more non-covered reduction in the sequence containing the reversal. Therefore this sequence always has a greater measure than the sequence with the rearrangement. Concluding,

$$M(ER_E) \succ M(P\downarrow) \qquad \text{implies} \qquad M(s[ER_E]) \succ M(s[P\downarrow]),$$

as desired.

(Case iv) Consider the diagram

$$\begin{tikzcd}
 & s_1 \arrow[r, leftrightarrow, "E"] & s_2 \\
s \arrow[ur, "S_E"] \arrow[urr, "P\downarrow"'] & &
\end{tikzcd}$$

with the associated $P\downarrow$ of the form $R_E^* E^* S_E^+$, as shown in the diagram

$$\begin{tikzcd}
 & s_1 \arrow[rr, leftrightarrow, "E"] & & s_2 \\
s \arrow[ur, "S_E"] \arrow[d, "R_E"', "*"] & & & \\
\cdot \arrow[rr, leftrightarrow, "E"', "*"] & & \cdot \arrow[uur, "S_E"', "+"] &
\end{tikzcd}$$

This case is almost symmetric to the above one, only the asymmetric definition of the cover number with respect to left-covering and right-covering breaks the symmetry. The bad case obviously occurs, when the final E-reduction of the cliff is left covered. Then its cover number would be smaller than the one associated to the final reduction of the rearrangement, if it is an E-reduction. But fortunately we can disregard this last case and analyze it as an ER_E-reversal.

This finishes the case analysis of the diagrams. The transformation process on sequences terminates and all minimal sequences are rearrangements, since otherwise, reversals had to exist leading to further rearrangements. □

15. The Church-Rosser Theorem of the λ-Calculus

In the Church-Rosser theorem of the λ-calculus, the antecedent of our Church-Rosser theorem is shown. Our Church-Rosser proofs lead almost automatically to a *strip lemma* of the form $R^\circ R^* \leq R^* R^{\circ *}$. We follow the proof in Barendregt [3]. It might be interesting to try our algebraic approach with other proofs. Some sublemmata of the strip lemma essentially deal with the term structure, hence are point-wise. Others can again be modeled purely algebraically.

Let Λ be the set of λ-terms on a set of variables X and let $\rightarrow_\beta$ be the associated reduction relation. We write $\rightarrow_\beta^*$ for the reflexive-transitive closure and $\leftarrow_\beta$ for the converse of $\rightarrow_\beta$. $s[t/x]$ denotes substitution of a term t for all occurances of the variable x in a term s.

The proof in Barendregt is based on redex-indexing to trace their behavior in reduction sequences. Intuitively, an indexed λ-term is obtained from a λ-term by indexing some of its redices $(\lambda x.s)t$ as $(\lambda x_i.s)t$ in $\mathbb{N}$. Λ' denotes the set of indexed λ-terms. Obviously $\Lambda \subseteq \Lambda'$. We extend $\rightarrow_\beta$ to $\rightarrow_{\beta'} = \rightarrow_{\beta_0} + \rightarrow_{\beta_1}$ on indexed lambda terms such that $\rightarrow_{\beta_0}$ acts on the indexed and $\rightarrow_{\beta_1}$ on the non-indexed part. We (recursively) define the mappings $\pi : \Lambda' \longrightarrow \Lambda$ that forgets all indices and $\sigma : \Lambda' \longrightarrow \Lambda$ that β-reduces all indexed redices in a term from inside out: $\sigma(x) = x$, $\sigma(\lambda x.s) = \lambda x.\sigma(s)$, $\sigma(st) = \sigma(s)$, if $s \neq \lambda_i x.s$ and $\sigma((\lambda_i x.s)t = \sigma(s)[\sigma(t)/x]$. We require that $\rightarrow_{\beta'}$ acts on Λ' exactly like $\rightarrow_\lambda$ on Λ, that σ performs all reduction on indexed redices and that σ leaves non-indexed redices untouched. This can be written algebraically as

$$\pi \to_\beta = \to_{\beta'} \pi, \tag{64}$$

$$\to_{\beta_0} \sigma = \sigma, \tag{65}$$

$$\to_{\beta_1} \sigma \leq \sigma \to_\beta, \tag{66}$$

$$\to_{\beta'} \sigma \leq \sigma \to_\beta . \tag{67}$$

It is easy to check that these expressions are well-typed. We can take (64), (65) and (66) as defining properties of $\to_{\beta'}$. In general, a term-based definition must be given and (64), (65) and (66) must be shown, using substitution properties and the defining properties λ-terms. Similarly one can show the following.

Lemma 15.1. *π and σ restricted to Λ are equal to 1_Λ.*

Lemma 15.2. *Let τ be one of π or σ.*

$$(\tau \to_\beta)^* = \tau \to_\beta^*, \tag{68}$$

$$(\to_{\beta'} \tau)^* = \to_{\beta'}^* \tau \tag{69}$$

Proof. We give proofs for π. Those for σ are similar.

(of 68) $(\pi \to_\beta)^* = (\pi \to_\beta)^* \pi = \pi(\to_\beta \pi)^* = \pi \to_\beta^*$, by lemma 15.1 and the shift rule (35).

(of 69)

$$\begin{aligned}((\to_{\beta'} \pi)^* &= 1 + (\to_{\beta'} \pi)(\to_{\beta'} \pi)^* = 1 + \to_{\beta'} (\pi \to_{\beta'})^* \pi) \\ &= 1 + \to_{\beta'} \to_{\beta'}^* \pi = \to_{\beta'}^* \pi,\end{aligned}$$

using the prefix axiom (11) (as equation) and (35). From the third to the fourth equality we implicitly use the fact that $\to_{\beta'}$ can be restricted to Λ (sub-typing). $\square$

Lemma 15.3.

$$\pi \to_\beta^* = \to_{\beta'}^* \pi, \tag{70}$$

$$\to_{\beta'}^* \sigma \leq \sigma \to_\beta^*, \tag{71}$$

$$\sigma^\circ \to_{\beta'}^* \sigma \leq \to_\beta . \tag{72}$$

Proof. (of 70) $\tau \to_\beta^* = (\tau \to_\beta)^* = (\to_{\beta'} \tau)^* = \to_{\beta'}^* \tau$, using (68), (64) or (67), and (69) together with monotonicity of the Kleene star.

(of 71)Similar to (70).

(of 72) The statement immediately follows from (70) by lemma 9.3. $\square$

A final property we need is $\sigma \leq \pi \to_\beta^*$, which can be shown by structural induction on Λ. We however use its variant (via lemma 9.3)

$$\pi \leq \sigma \leftarrow_\beta^* . \tag{73}$$

Proposition 15.4 (Strip Lemma). $\leftarrow_\beta \to_\beta^* \leq \to_\beta^* \leftarrow_\beta^*$.

Proof. Index the redex where the one-step reduction occurs. At this point, therefore, $\to_\beta = \pi^\circ \sigma$ (which is consistent with (73).

$$\leftarrow_\beta \to_\beta^* = (\pi^\circ \sigma)^\circ \to_\beta^* = \sigma^\circ \pi \to_\beta^* = \sigma^* \to_{\beta'}^* \pi \leq \sigma^* \to_{\beta'}^* \sigma \leftarrow_\beta^* \leq \to_\beta^* \leftarrow_\beta^*,$$

by the assumption, properties of the converse, (70), (73) and (72). $\square$

Corollary 15.5 (Church-Rosser). $(\to_\beta + \leftarrow_\beta)^* \leq \to_\beta^* \leftarrow_\beta^*$.

Proof. By the strip lemma (lemma 15.4) and the abstract Church-Rosser result of corollary 9.4, which itself is a corollary of proposition 7.1. $\square$

Again, the arguments can be visualized by semi-commuting allegorial diagrams.

16. Church-Rosser Machine Proofs

Our algebraic Church-Rosser proofs have two benefits. First, they are based on natural algebraic properties like fixed points, suprema, distributivity, reflexivity, transitivity, idempotence or monotonicity. This makes them simple, well-structured, revealing and easy to read and understand. Second, they are induction-free, based on fixed point considerations (Park induction) instead. This makes them computationally appealing and interesting for mechanization, since no induction measures and hypotheses had to be guessed. One might therefore say that the Church-Rosser theorems have been proved by calculation.

Both benefits seem interesting in the general context of program specification and verification. On the one hand, Kleene algebras are expressibly weak variants of relation algebras or allegories. Since they support point-free algebraic reasoning and the introduction of natural algebraic lemmata, they introduce a discipline of abstraction. On the other hand, Kleene algebras are computationally strong. Since they force us to circumvent induction, creativity is often replaced by computation. There is a deeper and more important reason why Kleene algebra (and allegories in general) are appropriate for mechanized reasoning. There is a strong connection between Kleene algebras and regular sets.

Theorem 16.1 ([14]). *There is a deductive system for the universal Horn theory of Kleene algebra such that an equation in the language of Kleene algebras is a logical consequence of the axioms if and only if the two expressions denote the same regular set.*

Completeness results for related systems have been given, for instance, in [7]; a similar statements relates a deductive system for certain allegories with the Horn theory of relations and sets [9]. Remember that the algebra of regular events cannot be be characterized by a finite set of equations [18]. Finally, Kleene algebra is not complete with respect to the Horn theory of regular events [13].

These statements separate the proofs of Church-Rosser theorems in this text into two classes. Those (the equational ones) that can be decided by automata and those that possibly require interaction (the Horn ones). Of course, the Church-Rosser statements are Horn, but most of their lemmata are equational. Also all statements, where assumptions about functions appear, are beyond automata. It seems therefore promising to carry out the proofs in a proof environment that combines a logical framework with automata-based decision tools, like for instance the system described in [4], which is based on the Isabelle-prover [17] and the Mona-tool [12].

17. Conclusion

We have shown how to carry out proofs of variants of Church-Rosser theorems and Newman's lemma in the purely algebraic setting of Kleene algebras and allegories. The Church-Rosser proofs were done in a point-free style, purely algebraically, without induction but via fixed-point reasoning. Proofs of Newman's lemmata, however, recurred to tabulations, that is mimicked point-wise proofs. As a main result we reconstructed a variant of the Church-Rosser theorem modulo an equivalence relation. Main benefits of the allegorial approach are that the well-foundedness assumptions in the respective theorems are constructed in the proofs and need not be guessed a priori. We thus obtain a very fine-grained procedural view on the properties under consideration. We could also connect the standard diagrams of term rewriting with allegorial ones and thus with categorial ones. We also saw that the standard Church-Rosser theorem modulo arises quite naturally as a special case of a more general Church-Rosser statement, that has been shown to be appropriate for rewriting with non-symmetric transitive relations in [21].

The proofs of Church-Rosser theorems should be well-suited for mechanization; those of Newman's lemma might need to be further formalized for this purpose. We believe that the techniques used in this paper are not only interesting in the given context, but also for point-free specification and verification in general. Here, allegorial reasoning (or reasoning with Kleene algebra) could lead to the same benefits in the context of relations that categorial reasoning has in the context of point-free functional programming; since point-freeness is often an excellent means of abstraction. Thus a mechanization of our Church-Rosser proofs might serve as a case study for an allegorial calculus for point-free specification and development of hard- and software systems in general.

References

[1] J.-R. Abrial. *The B-Book*. Cambridge University Press, 1996.

[2] L. Bachmair. *Canonical Equational Proofs*. Birkhäuser, 1991.

[3] H. Barendregt. *The Lambda Calculus*. Elsevier, 1984.

[4] D. Basin and S. Friedrich. Combining WS1S and HOL. In D.M. Gabbay and M. de Rijke, editors, *Frontiers of Combining Systems 2*, volume 7 of *Studies in Logic and Computation*, pages 39–56. Research Studies Press/Wiley, 2000.

[5] R. Bird and O. de Moor. *Algebra of Programming*. Prentice Hall, 1997.

[6] M. Clerbout, M. Latteux, and Y. Roos. Semi-Commutations. In V. Diekert and G. Rozenberg, editors, *The Book of Traces*, chapter 12, pages 488–574. World Scientific, 1995.

[7] J. H. Conway. *Regular Algebras and Finite State Machines*. Chapman and Hall, 1971.

[8] S. Eilenberg. *Automata, Languages and Machines*, volume A. Academic Press, 1974.

[9] P. J. Freyd and A. Scedrov. *Categories, Allegories*. North-Holland, 1990.

[10] D. Harel, D. Kozen, and J. Tiuryn. *Dynamic Logic*. MIT Press, 2000.

[11] J.-P. Jouannaud and H. Kirchner. Completion of a set of rules modulo a set of equations. *SIAM J. Comput.*, 15:1155–1194, 1986.

[12] N. Klarlund and A. Møller. *MONA Version 1.3 User Manual*. BRICS Notes Series NS-98-3 (2.revision), Department of Computer Science, University of Aarhus, 1998.

[13] D. Kozen. On Kleene algebras and closed semirings. In rovan, editor, *Proc. MFCS90*, volume 452 of *LNCS*, pages 26–47. Springer-Verlag, 1990.

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

[15] W. Kuich. Semirings and formal power series: Their relevance to formal languages and automata. In G. Rozenberg and A. Salomaa, editors, *Handbook of Formal Language Theory*, volume I, pages 609–677. Springer-Verlag, 1997.

[16] J. Levy and J. Agustí. Bi-rewrite systems. *J. Symbolic Computation*, 22:279–314, 1996.

[17] L. C. Paulson. *Isabelle : a generic theorem prover; with contributions by Tobias Nipkow*, volume 828 of *LNCS*. 1994.

[18] V. N. Redko. On defining relations for the algebra of regular events. *Ukrain. Mat. Z.*,, 16:120–126, 1964.

[19] G. W. Schmidt and T. Ströhlein. *Relations and Graphs: Discrete Mathematics for Computer Scientists*. EATCS Monographs on Theoretical Computer Science. Springer-Verlag, 1993.

[20] G. Struth. Non-Symmetric rewriting. Technical Report MPI-I-96-2-004, Max-Planck-Institut für Informatik, Saarbrücken, 1996.

[21] G. Struth. *Canonical Transformations in Algebra, Universal Algebra and Logic*. PhD thesis, Institut für Informatik, Universität des Saarlandes, 1998.

Institut für Informatik, Albert-Ludwigs-Universität Freiburg, Georges-Köhler-Allee, D-79110 Freiburg i. Br. Germany

E-mail address: `struth@informatik.uni-freiburg.de`