Left-Handed Completeness via Cyclic Proofs

Anupam Das[1], Amina Doumane[2], and Damien Pous[2]

[1] University of Copenhagen
[2] CNRS, Plume team, LIP, ENS de Lyon, France

Abstract

We give a new proof that the axioms of left-handed Kleene algebra are complete with respect to language containments. This proof is significantly simpler than both the proof of Boffa (which relies on Krob's completeness result), and the more recent proof of Kozen and Silva. Our proof builds on a recent non-wellfounded sequent calculus which makes it possible to explicitly compute the invariants required for left-handed Kleene algebra.

1 Introduction

Kleene algebra is a finitely axiomatised quasi-equational theory over regular expressions [12], which admits *formal languages* and *binary relations* as free models: every equation which is universally valid in one of those models, or equivalently, whose members denote the same rational language, is provable from the axioms of Kleene algebra [7, 26, 19, 8]. This theorem is important in practice since it shows that the equational theory of Kleene algebra is decidable, and actually PSPACE-complete: it reduces to the problem of comparing rational languages. Thanks to the model of binary relations, Kleene algebra and its extensions have been used to reason abstractly about program correctness [21, 22, 3, 16, 2]. The aforementioned decidability result actually made it possible to automatise reasoning steps in proof assistants [9, 25, 27].

Several axiomatisations have been studied in the literature, and the existing completeness proofs are all technically involved. Redko first proved that every purely equational axiomatisation must be infinite [28]. Conway then conjectured completeness of fourteen 'classical' equations, plus a family of axioms indexed by finite semigroups [12, page 116]; Krob proved this result twenty years later, in a 137 pages long paper [26]. At the same time, Kozen proved completeness of a finite quasi-equational axiomatisation (what is called Kleene Algebra nowadays), using an ingenious and reasonably short proof [20] where automata computations are replayed algebraically, using matrices. This axiomatisation comprises two implications to characterise Kleene star.

(L) $z + yx \leq x$ implies $y^*z \leq x$

(R) $z + xy \leq x$ implies $zy^* \leq x$

By removing the second one, one obtains so-called *left-handed* Kleene algebras, which are the structures we consider in the present paper, and whose completeness with respect to rational language inclusions was stated without proof by Conway [12, Chap. 12, Thm. 5]. Such structures are important because there are models where one of the implications of Kleene algebra is not satisfied [18, 24] (see also Ex. 1 below).

Boffa proved [7, 8] that completeness of left-handed Kleene algebra follows from completeness of Conway's axioms, thus requiring Krob's extensive proof [26, Cor. 15.15]. Kozen and Silva recently gave a shorter but still highly technical proof [23], by relying on the coalgebraic semantics of regular expressions: Brzozowski's derivatives [11]. We give a new proof here.

Removing the second implication above disqualifies Kozen's technique for proving completeness [20]: both implications are needed to replay automata algorithms algebraically. In fact, the

key difficulty for left-handed completeness consists in finding *invariants* to exploit the remaining implication (L). A key feature of our proof is that we compute those invariants explicitly: we do not need to compute decompositions and solve linear systems of equations, as in [23].

Our completeness proof builds on a sequent-style calculus, HKA, which was proposed recently [14]. This system admits 'cyclic' proofs, where proofs are finite graphs with cycles rather than trees or dags, and soundness and completeness for rational language inclusions holds under a simple correctness criterion. These cyclic proofs make it possible to represent computations on automata in a structured way, which we exploit here to compute invariants and to obtain completeness. In the end, this results in a simple and direct proof, where the constructed derivations in left-handed Kleene algebra closely follow the computations on automata.

2 Regular expressions and their proof systems

2.1 Regular expressions and Kleene Algebras

We consider *regular expressions* over a finite *alphabet* A:

$$e, f \ ::= \ e \cdot e \mid e + e \mid e^* \mid 1 \mid 0 \mid a \in A$$

The set of regular expressions is denoted Exp_A, and we often write ef for $e \cdot f$. Each expression e denotes a rational language $\mathcal{L}(e) \subseteq A^*$, defined in the usual way [17].

A *left-handed Kleene algebra* is a tuple $(K, 0, 1, +, \cdot, *)$ where $(K, 0, 1, +, \cdot)$ is an idempotent semiring (see App. A) and, if we write $x \leq y$ as a shorthand for $x + y = y$, we have that:

(ℓ) $1 + xx^* \leq x^*$;

(L) if $z + yx \leq x$ then $y^*z \leq x$.

Given two regular expressions e, f, we write $\ell\mathrm{KA} \vdash e \leq f$ when $e \leq f$ is derivable from the axioms of left-handed Kleene algebra.

Together with the idempotent semiring axioms, Axioms (ℓ) and (L) amount to asking that y^*z is the least fixpoint of $x \mapsto z + yx$. These axioms admit several equivalent formulations (e.g. rules 'P1l', 'P2l' and 'P3l' in [12, page 103]). Also note that a few additional axioms are included in [23], which are all derivable from the ones used here. The point of *left-handed* Kleene algebra is that the right-handed versions of axioms (ℓ) and (L), characterising zy^* as the least fixpoint of $x \mapsto z + xy$, are omitted. This makes it possible to capture natural models as the one below.

Example 1. *Given a complete lattice $\langle X, \leq, \bigvee \rangle$, monotone functions $f : X \to X$ such that $f(x \vee y) = f(x) \vee f(y)$ and $f(\bot) = \bot$ form a left-handed Kleene algebra (where $\bot = \bigvee \varnothing$.). Addition is computed pointwise: $(f + g)(x) = f(x) \vee g(x)$; product is composition of functions: $(f \cdot g)(x) = f(g(x))$; Kleene star is obtained by iteration: $f^*(x) = \bigvee_{n \in \mathbb{N}} f^n(x)$ where $f^0(x) = x$ and $f^{n+1}(x) = f(f^n(x))$. Such models do not, in general, satisfy the implication (R) from the introduction (see App. E). Also note that we must restrict to functions that distribute over finite suprema to obtain a semiring: otherwise we only have semi-distributivity on the right [18].*

Left-handed completeness states that language inclusion implies derivability in ℓKA:

Theorem 2 (Left-handed completeness [12, 8, 23])**.** *If $\mathcal{L}(e) \subseteq \mathcal{L}(f)$ then $\ell\mathrm{KA} \vdash e \leq f$.*

(The converse implication holds by an easy inspection of ℓKA axioms.) We reprove this theorem in the remainder of this paper. The difficulties occur when the expression on the left, e, contains starred sub-expressions. When such a sub-expression occurs immediately on the left at toplevel, we shall rely on the following variant of Axiom (L):

Lemma 3 (Invariant lemma)**.** *For all regular expressions* e, Γ, X, I*,*

$$\textit{if} \quad \begin{cases} \ell\mathrm{KA} \vdash \Gamma \leq I \\ \ell\mathrm{KA} \vdash eI \leq I \\ \ell\mathrm{KA} \vdash I \leq X \end{cases} \qquad \textit{then} \qquad \ell\mathrm{KA} \vdash e^*\Gamma \leq X \ .$$

The reason for the choice of notation Γ and X becomes apparent in the next section when we deal with proof systems. The expression I in the above lemma is *invariant for* e *on the left* (second assumption of the lemma); it has to be guessed in order to apply the lemma and derive the inequality $e^*\Gamma \leq X$. The difficulty is that, in general neither Γ nor X can be chosen for I: some intermediate expression must be used. Most of the work in the present paper consists in computing such invariants and showing that they fulfil the requirements of the above lemma.

2.2 The system HKA of cyclic proofs

The sequent-style system HKA was introduced in [14]. It is a 'cut-free' proof system for inequalities between regular expressions and is well-suited for proof search; indeed it admits a PSPACE proof search procedure, which is optimal. HKA works with a form of *hypersequents*, which record slightly more structure than plain sequents, and proofs over this system may contain cycles. Both these features are critical for cut-free completeness. We recall this system below.

Notation 4 (Lists and multisets)**.** We denote lists (resp. finite multisets) by $x_1, \ldots, x_n$ (resp. $x_1; \ldots; x_n\}$), where $\{x_i\}_{i\in[1,n]}$ are the elements. We also use comma (resp. semicolon) to denote list concatenation (resp. multiset union). We write ε for the empty list. We let Γ, Δ range over lists of regular expressions, and X, Y range over multisets of such lists. We implicitly interpret such lists and multisets as regular expressions by converting lists into products and multisets into sums. For instance, the multiset $a, b; c$ is interpreted as the regular expression $ab + c$.

A *hypersequent* (or simply a sequent) is an expression $\Gamma \to X$; its general form is thus:

$$e_1, \ldots, e_l \to f_{11}, \ldots, f_{1n_1}; \cdots; f_{m1}, \ldots, f_{mn_m} \ .$$

A hypersequent $\Gamma \to X$ is *valid* if $\mathcal{L}(\Gamma) \subseteq \mathcal{L}(X)$.

The rules of HKA are given in Fig. 1. In the modal rule (a), we use the following notation: if $X = \Delta_1; \ldots; \Delta_n$, we write $e.X$ for the multiset $e, \Delta_1; \ldots; e, \Delta_n$. The rules presented in [14] are slightly more permissive: here we restrict to *leftmost* proofs, where logical rules only apply to regular expressions in head position of a list. Here we impose this condition syntactically since we do not need the more general setting of [14].

Definition 5 (HKA proofs)**.** A *preproof* is a potentially infinite derivation built using the rules of Fig. 1. A *proof* is a preproof that is *fair* for $*$-l, i.e. where every infinite branch contains infinitely many $*$-l steps. A proof is *regular* if it has finitely many distinct subtrees. We write $\mathsf{HKA} \vdash^{\omega} \Gamma \to X$ if $\Gamma \to X$ admits a regular proof.

We only work with regular proofs and we require them to be *uniform*: every two occurrences of the same sequent conclude identical subproofs. (Every proof can be transformed into a uniform one.) We moreover exploit the following concrete representation of such proofs.

Lemma 6. *Every regular and uniform proof can be represented as a finite tree with back-pointers to* $*$*-*l *steps: a finite derivation using the rules from Fig. 1 where leaves are either axioms (*0*-*l*, id) or pointers to one of their proper ancestors corresponding to a* $*$*-*l *step.*

Left logical rules:

$$\frac{}{0, \Delta \to}\ 0\text{-}l \qquad \frac{\Delta \to X}{1, \Delta \to X}\ 1\text{-}l \qquad \frac{e, f, \Delta \to X}{e \cdot f, \Delta \to X}\ \cdot\text{-}l \qquad \frac{e, \Delta \to X \quad f, \Delta \to X}{e + f, \Delta \to X}\ +\text{-}l \qquad \frac{\Delta \to X \quad e, e^*, \Delta \to X}{e^*, \Delta \to X}\ *\text{-}l$$

Right logical rules:

$$\frac{\Gamma \to \Sigma; X}{\Gamma \to 1, \Sigma; X}\ 1\text{-}r \qquad \frac{\Gamma \to e, f, \Sigma; X}{\Gamma \to e \cdot f, \Sigma; X}\ \cdot\text{-}r \qquad \frac{\Gamma \to e, \Sigma; f, \Sigma; X}{\Gamma \to e + f, \Sigma; X}\ +\text{-}r \qquad \frac{\Gamma \to \Sigma; e, e^*, \Sigma; X}{\Gamma \to e^*, \Sigma; X}\ *\text{-}r$$

Identity, modal and structural rules:

$$\frac{}{\to \varepsilon}\ id \qquad \frac{\Gamma \to X}{a, \Gamma \to a.X}\ (a) \qquad \frac{\Gamma \to X}{\Gamma \to \Delta; X}\ wk \qquad \frac{\Gamma \to \Delta; \Delta; X}{\Gamma \to \Delta; X}\ cntr$$

Figure 1: The rules of leftmost HKA.

Proof. Along each infinite branch, fairness gives infinitely many $*$-l steps, which occur on finitely many sequents by regularity; cut the branch using a back-pointer on the first such sequent visited twice. Now each branch is finite so that we have a finite tree (with back-pointers) by Knig's lemma. This tree faithfully represents the starting proof, by uniformity. □

Example 7. *The following derivation represents a regular and uniform proof, where $\bullet$ is used for back-pointers. We use it as a running example in the rest of the paper. We denote it by Π_0.*

$$\dfrac{\dfrac{}{\to (ab^*a)^*; a, (aa)^*}\ id}{\to (ab^*a)^*; a, (aa)^*}\ *\text{-}r, wk \qquad \dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to b^*a, (ab^*a)^*; (aa)^*}\ *\text{-}r, wk \qquad \dfrac{\dfrac{}{a^* \to (ab^*a)^*; a, (aa)^* \quad (\bullet)}\ (a)}{a, a^* \to a, (ab^*a)^*; a, a, (aa)^*}\ \cdot\text{-}r, *\text{-}r, *\text{-}r, \cdot\text{-}r, wk}{a^* \to b^*a, (ab^*a)^*; (aa)^*}\ *\text{-}l}{a, a^* \to (ab^*a)^*; a, (aa)^*}\ *\text{-}r, \cdot\text{-}r, wk$$

$$a^* \to (ab^*a)^*; a, (aa)^* \quad (\bullet)\ *\text{-}l$$

This proof intuitively corresponds to a computation where the language of the antecedent (a^*) is explored and matched with the language of the succedent $((ab^*a)^* + a(aa)^*)$, using an automata construction reminiscent from partial derivatives [4]. Now introduce the following notations:

$$X_0 \triangleq (ab^*a)^*; a, (aa)^* \qquad X_1 \triangleq b^*a, (ab^*a)^*; (aa)^*$$

$$R \triangleq *\text{-}r, wk \qquad R_0 \triangleq *\text{-}r, \cdot\text{-}r, wk \qquad R_1 \triangleq \cdot\text{-}r, *\text{-}r, *\text{-}r, \cdot\text{-}r, wk$$

we can write Π_0 and its subproof Π_1 rooted at $a^* \to X_1$ as follows:

$$\Pi_0 = \dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to X_0}\ R \qquad \dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to X_1}\ R \qquad \dfrac{\dfrac{}{a^* \to X_0 \quad (\bullet)}\ (a)}{a, a^* \to a.X_0}\ R_1}{a, a^* \to X_1}\ *\text{-}l}{a^* \to X_1}\ (a) \qquad \dfrac{}{a, a^* \to a.X_1}\ R_0}{a, a^* \to X_0}\ *\text{-}l$$

$$a^* \to X_0 \quad (\bullet)$$

$$\Pi_1 = \dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to X_0}\ R \qquad \dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to X_1}\ R \qquad \dfrac{\dfrac{}{a^* \to X_1 \quad (\bullet\bullet)}\ (a)}{a, a^* \to a.X_1}\ R_0}{a, a^* \to X_0}\ *\text{-}l}{a^* \to X_0}\ (a) \qquad \dfrac{}{a, a^* \to a.X_0}\ R_1}{a, a^* \to X_1}\ *\text{-}l$$

$$a^* \to X_1 \quad (\bullet\bullet)$$

We give other examples of HKA proofs in App. B. Our starting point is the following result: HKA is complete for rational language inclusions:

Theorem 8 (Completeness of HKA [14]). *If* $\mathcal{L}(\Gamma) \subseteq \mathcal{L}(X)$ *then* $\mathsf{HKA} \vdash^{\omega} \Gamma \to X$.

The proof of this theorem is not difficult: logical rules of HKA are invertible so that we may apply them eagerly; when a normal form is reached, we use a weakening (wk) followed by a modal step (a), as usual in proof search for modal logics. We obtain regular proofs since the number of sequents appearing is bounded, by appealing to an order on the occurring expressions.

Damien: amina: a
ble ok?
Amina: Yes!
Anupam: j'ai refor
paragraphe un peu

3 Proof of completeness

To prove completeness of left-handed Kleene algebra, it suffices by Thm. 8 to translate (regular) proofs of HKA into ℓKA derivations:

Theorem 9 (Translation theorem). *If* $\mathsf{HKA} \vdash^{\omega} \Gamma \to X$ *then* $\ell\mathrm{KA} \vdash \Gamma \leq X$.

The rest of the paper is dedicated to the proof of this theorem. We first observe the following:

Proposition 10. *If the premisses of a* HKA *rule are derivable in* ℓKA*, so is its conclusion.*

This means that every finite proof of HKA can be translated; the difficulty consists in handling cyclic—and thus infinite—proofs. To show Thm. 9, we need to slightly generalise it (Thm. 14 below), to deal with a certain form of *hypotheses*, which we define below.

Definition 11 (Hypotheses). A *hypothesis* is an expression $x \leq e$ where $x \in A$ and $e \in \mathrm{Exp}_A$. Let $\mathcal{H}$ be a set of hypotheses. We denote by $\ell\mathrm{KA}{+}\mathcal{H}$ the union of ℓKA axioms and $\mathcal{H}$. We write $\mathsf{HKA}{+}\mathcal{H}$ for the system obtained from HKA by adding, for every $(x \leq e) \in \mathcal{H}$, the following rule:

$$\frac{}{x \to e}\ \mathcal{H}$$

A straightforward induction yields the following lemma.

Lemma 12. *Suppose* $x \in \mathcal{L}(e)$ *for a letter* x*. Then* $\mathsf{HKA} \vdash^{\omega} x \to e$ *and* $\ell\mathrm{KA} \vdash x \leq e$.

Proviso 13. Let $\mathcal{H}_0 \triangleq \{x \leq e \mid x \in \mathcal{L}(e)\}$. We assume that all sets of hypotheses contain $\mathcal{H}_0$ and that in HKA proofs, the modal rule (a) is applied only when $\Gamma \neq \varnothing$: instances of this rule breaking this assumption can be removed using hypotheses from $\mathcal{H}_0$.

Our goal is now to prove the following generalisation of Thm. 9:

Theorem 14. *If* $\mathsf{HKA}, \mathcal{H} \vdash^{\omega} \Gamma \to X$*, then* $\ell\mathrm{KA}, \mathcal{H} \vdash \Gamma \leq X$.

Thm. 8 follows by taking $\mathcal{H} = \mathcal{H}_0$; note that while Thm. 9 actually yields an equivalence, the converse of Thm. 14 does not hold—see App. D.

We prove Thm. 14 by lexicographic induction on $\langle \#\Gamma, \#\pi \rangle$, where $\#\Gamma$ is the number of the $*$-subexpressions occurring in Γ, and $\#\pi$ is the number of (distinct) nodes in the starting regular proof π. We proceed by analysing the last rule ρ applied in π.

If ρ is the $\mathcal{H}$ rule, the result is immediate. Suppose that ρ is a HKA rule which is not $*$-l, and let $\{\pi_i\}_i$ be the sub-proofs of π rooted at the premisses of ρ. Let $\Gamma_i \to X_i$ be the conclusion sequent of π_i. Observe that $\#\Gamma_i \leq \#\Gamma$. Since ρ is not a $*$-l, there is no back-pointer from π_i to the conclusion of π, thus $\#\pi_i < \#\pi$. We have $\langle \#\Gamma_i, \#\pi_i \rangle <_{lex} \langle \#\Gamma, \#\pi \rangle$, and we can apply the induction hypothesis to π_i. We conclude using Prop. 10.

Suppose now that ρ is $*$-l, so that π is of the following form:

$$\dfrac{\dfrac{\pi_1}{\Gamma \to X} \qquad \dfrac{\pi_2}{e, e^*, \Gamma \to X}}{e^*, \Gamma \to X}\ *\text{-}l$$

We cannot in general apply the induction hypothesis to π_2: we have $\#(e, e^*, \Gamma) \geq \#(e^*, \Gamma)$ and since π_2 might have back-pointers to the conclusion of π, we might have $\#\pi_2 = \#\pi$.

Instead, to find a derivation of $e^*, \Gamma \leq X$ in $\ell\mathrm{KA}{+}\mathcal{H}$, we use the invariant lemma (Lem. 3). A naive idea is to use X as invariant, which implies showing that $\ell\mathrm{KA}, \mathcal{H} \vdash \Gamma \leq X$ and $\ell\mathrm{KA}, \mathcal{H} \vdash eX \leq X$. The first inequality can be obtained by applying the induction hypothesis to π_1 (since $\#\Gamma < \#(e^*, \Gamma)$). Let us show the second inequality in the simple case where π has the following property:

$$\text{whenever a sequent } e^*, \Gamma \to Y \text{ appears in } \pi, \text{ we have } Y = X. \tag{$\star$}$$

In this case, if we replace e^*, Γ by X in all the antecedents of sequents in π_2, we can close all the back-pointers to $e^*, \Gamma \to X$ by an identity rule as shown below.

$$\dfrac{\dfrac{\vdots}{e^*, \Gamma \to X}}{\dfrac{\vdots\,\pi_2}{e, e^*, \Gamma \to X}} \quad \rightsquigarrow \quad \dfrac{\dfrac{}{X \to X}\ id}{\dfrac{\vdots\,\pi_2[(e^*, \Gamma)/X]}{e, X \to X}}$$

We conclude by applying the induction hypothesis to $\pi_2[(e^*, \Gamma)/X]$, since $\#(e, X) < \#(e^*, \Gamma)$.

Unfortunately, π may contain sequents of the form $e^*, \Gamma \to X'$ where $X' \neq X$ (e.g. as in Ex. 7). In such a case, when we replace e^*, Γ by X in π_2, we get stuck with sequents of the form $X \to X'$, for which we potentially do not even have $\mathcal{L}(X) \subseteq \mathcal{L}(X')$:

$$\dfrac{\dfrac{\vdots}{e^*, \Gamma \to X'} \qquad \dfrac{\vdots}{e^*, \Gamma \to X}}{\dfrac{\vdots\,\pi_2}{e, e^*, \Gamma \to X}} \quad \rightsquigarrow \quad \dfrac{\dfrac{?}{X \to X'} \qquad \dfrac{}{X \to X}\ id}{\dfrac{\vdots\,\pi_2[(e^*, \Gamma)/X]}{e, X \to X}}$$

If we had an intersection operator in our syntax, we could choose $X \cap X'$ as invariant. Since we do not have such an operator, the challenge is to find an expression which will play the role of the intersection and for which we can derive the tree inequalities required for an invariant. (Blindly computing a regular expression for the rational language $\mathcal{L}(X) \cap \mathcal{L}(X')$ does not work since we would not know how to derive those three inequalities.)

We handle this case in the next two sections: let us fix a regular proof $\underline{\pi}$ of $\underline{e}^*, \underline{\Gamma} \to \underline{X}_1$ and ending with a $*$-l step. Let $\underline{X}_1, \ldots, \underline{X}_n$ be an enumeration of the multisets such that $\underline{e}^*, \underline{\Gamma} \to \underline{X}_i$ is a conclusion of a $*$-l step in π. In the following sections, we compute an expression $\underline{\mathcal{I}}$, the invariant, which intuitively corresponds to the intersection of $\underline{e}^*\underline{\Gamma}$ and $\underline{X}_1, \ldots, \underline{X}_n$ (Sect. 4), and we derive the following inequalities (resp. in Sect. 5.1, 5.2 and 5.3):

$$\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\Gamma} \to \underline{\mathcal{I}} \qquad \ell\mathrm{KA}, \mathcal{H} \vdash \underline{e}, \underline{\mathcal{I}} \to \underline{\mathcal{I}} \qquad \ell\mathrm{KA}, \mathcal{H} \vdash \underline{\mathcal{I}} \to \underline{X}_1$$

We underlined π, e, Γ, X_i and $\mathcal{I}$, to distinguish these global variables of the external induction from the local variables we will use in the subsequent lemmas and propositions.

Left rules:

$$\frac{\{\Gamma_i \Rightarrow \mathcal{X}\}_{i\in I}}{\Gamma \Rightarrow \mathcal{X}}\ l \qquad \text{If the following is a left } \mathsf{HKA} \text{ rule:} \qquad \frac{\{\Gamma_i \to X\}_{i\in I}}{\Gamma \to X}\ l$$

Right rules: (including weakening and contraction rules)

$$\frac{\Gamma \Rightarrow \mathcal{X}, X, \mathcal{Y}}{\Gamma \Rightarrow \mathcal{X}, Y, \mathcal{Y}}\ r \qquad \text{If the following is a right } \mathsf{HKA} \text{ rule:} \qquad \frac{\Gamma \to X}{\Gamma \to Y}\ r$$

Identity, hypothesis, and modal rules:

$$\frac{}{\Rightarrow \varepsilon, \dots, \varepsilon}\ id \qquad \frac{}{x \Rightarrow e_1, \dots, e_n}\ \mathcal{H} \qquad \frac{\Gamma \Rightarrow X_1, \dots, X_n}{a, \Gamma \Rightarrow a.X_1, \dots, a.X_n}\ (a)$$

Figure 2: The rules of synchronised HKA; the rule $\mathcal{H}$ applies only when the hypothesis $x \leq e_i$ belongs to $\mathcal{H}$ for every $i \in [1, n]$.

4 Computing the invariant

For every $i \in [1, n]$, let $\underline{\pi}_i$ be the subproof of $\underline{\pi}$ rooted at $\underline{e}^*, \underline{\Gamma} \to \underline{X}_i$. To construct the invariant, we proceed in three steps:

1. First, we synchronise the proofs $\{\underline{\pi}_i\}_i$ by taking their product. This product is a structure that we call a *synchronised proof*.
2. Second, we convert this synchronised proof into a non-deterministic automaton (NFA).
3. Third, we extract the invariant $\mathcal{I}$ from this NFA.

Several standard algorithms make it possible to extract regular expressions from finite automata (e.g. state removal from Kleene's theorem). We however need to design our own algorithm to retain control on the produced expressions, and derive the three inequalities of an invariant.

4.1 Synchronised proofs

We let $\mathcal{X}, \mathcal{Y}$ range over n-uples of multisets (of lists of regular expressions).

Definition 15 (Synchronised proof system)**.** A *synchronised sequent* is an expression of the form $\Gamma \Rightarrow \mathcal{X}$. A *synchronised proof* is a (potentially infinite yet regular) derivation built using the rules of Fig. 2, which is fair for $*$-l. As for HKA, we implicitly work with finite representations of synchronous proofs as trees with back-pointers.

Intuitively, a synchronised proof of $\Gamma \Rightarrow X_1, \dots, X_n$ is just a product of proofs for the sequents $\Gamma \to X_i$. Left logical rules are applied synchronously: at most one left logical rule applies for a given antecedent Γ; right logical rules are applied independently.

If $\Gamma \Rightarrow X_1, \dots, X_n$ is a synchronised sequent, we call the sequent $\Gamma \to X_i$ its i^{th} projection. When we replace the synchronised sequents of a synchronised proof π by their i^{th}-projection and remove irrelevant right steps, we get an $\mathsf{HKA}{+}\mathcal{H}$ proof, which we call the i^{th} projection of π.

Conversely, one can construct synchronous proofs from independent ones:

Definition 16. Let $\{\pi_i\}_{i\in[1,n]}$ be a collection of $\mathsf{HKA}{+}\mathcal{H}$ regular proofs, such that $\Gamma \to Y_i$ is the conclusion of π_i and let ρ_i be the last rule applied in π_i (note that all π_i have the same antecedent Γ). We let $\prod_{i\in[1,n]} \pi_i$ be the synchronous proof defined coinductively as follows:

- If some rule ρ_k, where $k \in [1,n]$ is a right rule r, whose premiss is $\Gamma \to Z_k$, we set θ_k to be the sub-proof of π_k rooted at $\Gamma \to Z_k$, and set:

$$\prod_{i\in[1,n]} \pi_i \quad \triangleq \quad \dfrac{\dfrac{\prod_{i\in[1,k-1]} \pi_i \times \theta_k \times \prod_{i\in[k+1,n]} \pi_i}{\Gamma \Rightarrow Y_1, \dots, Y_{k-1}, Z_k, Y_{k+1}, \dots, Y_n}}{\Gamma \Rightarrow Y_1, \dots, Y_{k-1}, Y_k, Y_{k+1}, \dots, Y_n}\ r$$

- If all the rules ρ_i are left logical rules, they are necessarily the same HKA rule l. Let $\{\Gamma_j\}_{j\in J}$ be the antecedents of the premisses of l, and let θ_{ij} be the sub-proof of π_i rooted at $\Gamma_j \to Y_i$. We set:

$$\prod_{i\in[1,n]} \pi_i \quad \triangleq \quad \dfrac{\left\{ \dfrac{\prod_{i\in[1,n]} \theta_{ij}}{\Gamma_j \Rightarrow Y_1, \dots, Y_n} \right\}_{j\in J}}{\Gamma \Rightarrow Y_1, \dots, Y_n}\ l$$

- If all the rules ρ_i are the modal rule (a), let $\Delta \to Z_i$ be the premiss of ρ_i in π_i and θ_i be the sub-proof of π_i rooted in $\Delta \to Z_i$. We set:

$$\prod_{i\in[1,n]} \pi_i \quad \triangleq \quad \dfrac{\dfrac{\prod_{i\in[1,n]} \theta_i}{\Delta \Rightarrow Z_1, \dots, Z_n}}{\Gamma \Rightarrow Y_1, \dots, Y_n}\ (a)$$

- If all the rules ρ_i are the hypothesis rule $\mathcal{H}$, we use the synchronised hypothesis rule.
- If all the rules ρ_i are the identity rule, we use the synchronised identity rule.

Thanks to Proviso 13, if Γ is of the form $\Gamma = a, \Delta$, the rules ρ_i are either all hypothesis rules (if $\Delta = \varnothing$) or all modal rules (otherwise). Our definition thus covers all the possible cases.

Remark 17. *Note that the i^{th} projection of $\prod_{i\in I} \pi_i$ is an unfolding of π_i. The above product of proofs can be seen as a way to find a 'common unfolding' for them, as illustrated by Ex. 18. Also note that the product is not uniquely defined, but we can fix one arbitrarily.*

Example 18. *The product of the proofs Π_0 and Π_1 of Ex. 7 is the following synchronised proof.*

$$\Pi_0 \times \Pi_1 = \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Rightarrow \varepsilon, \varepsilon}\ id}{\Rightarrow \varepsilon, X_0}\ R}{\Rightarrow X_1, X_0}\ R \qquad \dfrac{\dfrac{\dfrac{}{a^* \Rightarrow X_0, X_1}\ (\bullet)}{a, a^* \Rightarrow a.X_0, a.X_1}\ (a)}{a, a^* \Rightarrow a.X_0, X_0}\ R_0}{a, a^* \Rightarrow X_1, X_0}\ R_1}{a^* \Rightarrow X_1, X_0}\ *\text{-}l \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{\Rightarrow \varepsilon, \varepsilon}\ id}{\Rightarrow \varepsilon, X_1}\ R}{\Rightarrow X_0, X_1}\ R \qquad \dfrac{\dfrac{}{a, a^* \Rightarrow a.X_1, a.X_0}\ (a)}{a, a^* \Rightarrow a.X_1, X_1}\ R_1}{a, a^* \Rightarrow X_0, X_1}\ R_0}{a^* \Rightarrow X_0, X_1 \quad (\bullet)}\ *\text{-}l$$

4.2 Automata of synchronised proofs

Definition 19 (Automaton of a synchronised proof)**.** Let π be a synchronised proof. The automaton of π is the NFA $\mathcal{A}(\pi) = \langle Q, T, \iota, F \rangle$, where the set of states is $Q = S \uplus F$, S being the set of synchronised sequent occurrences of π and F being a copy of the conclusions of $\mathcal{H}$ and id steps, the initial state ι is the root of π, and the transition table $T \subseteq Q \times A \cup \{1\} \times Q$ is defined as follows. $(p, l, q) \in T$ if either:

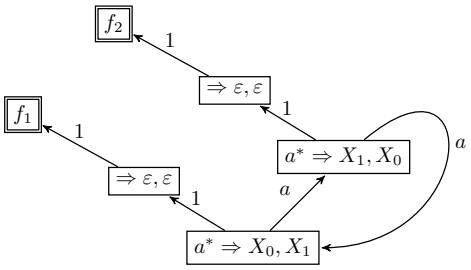


Figure 3: Automaton of the synchronised proof $\Pi_0 \times \Pi_1$ from Ex. 18.

- q is a premiss of p, the applied rule is not a modal rule, and $l = 1$.
- q is a premiss of p, the applied rule is a modal rule (a), and $l = a$.
- $p = (x \Rightarrow \mathcal{X})$ (resp. $p = (\Rightarrow \mathcal{X})$) is the conclusion of a $\mathcal{H}$ (resp. id) rule, $q \in F$ is its copy, and $l = x$ (resp. $l = 1$).

Proviso 20. Since synchronised proofs are represented as finite trees with back-pointers, their automata also have this shape. We call the tree structure underlying automata of this shape simply *their trees*. In the sequel we suppose that all our NFA have this shape, and that their trees are rooted in the initial state[1].

Example 21. *The automaton $\mathcal{A}$ of the synchronised proof $\Pi_0 \times \Pi_1$ of Ex. 18 is given in Fig. 3. The accepting states are f_1 and f_2, which are the copies of the two occurrences of $\Rightarrow \varepsilon, \varepsilon$. The initial state is $a^* \Rightarrow X_0, X_1$, the root of $\Pi_0 \times \Pi_1$. We omitted states and epsilon transitions for the sake of readability. This automaton recognises the language a^*, which is the intersection of the languages of X_0 and X_1. Note that if we had started with the multiset $X_0; a^*c$ in the right-hand side of the sequent from Ex. 7, we would have obtained a similar automaton, not an automaton for a^*c: in general, the constructed automaton recognises the intersection of $\underline{e}^*\underline{\Gamma}$ and the $\underline{X}_1, \dots, \underline{X}_n$.*

We will use some graph theoretic terminology for NFA; we introduce it below.

Definition 22 (Paths, labels, proper loops)**.** Let $\mathcal{A} = \langle Q, T, \iota, F \rangle$ be a NFA and let $l : Q \to \mathrm{Exp}_A$ be a labelling of the states of $\mathcal{A}$.

A *path* is a sequence $p = q_1, a_1, \dots, q_{k-1}, a_{k_1}, q_k$ where $q_i \in Q$ and $\langle q_i, a_i, q_{i+1} \rangle \in T$. It is *simple* if $q_i \neq q_j$ when $i \neq j$. We denote by $\mathsf{Simpl}(p, q)$ the set of simple paths from p to q. The *label of* p, denoted $l(p)$ is the sequence $l(q_1), a_1, \dots, l(q_{k-1}), a_{k_1}, l(q_k)$.

A *proper loop* of q is a sequence a, q', b s.t. q, a, q' and q', b, q are simple paths and all states of q' are descendants of q in the tree of $\mathcal{A}$. We write $\mathsf{Loop}(q)$ for the set of proper loops of q.

Remark 23. *There are two differences between proper loops and what is usually called a loop: they are not paths in the sense of the previous definition because they do not begin and do not finish by a node. (For that one can complete them by adding nodes to both extremities.) The second difference, more fundamental, is that we do not have the right to visit nodes which are ancestors (in the tree of the automaton) of the node on which we loop.*

[1] Note that every NFA can be put into this form.

4.3 Extracting regular expressions from automata

Definition 24 (Expression of a NFA)**.** Let $\mathcal{A} = \langle Q, T, \iota, F\rangle$ be a NFA. We define a state labelling function $l : Q \to \mathrm{Exp}_A$ recursively on the tree of $\mathcal{A}$, starting from the leaves. Suppose that we are processing the node n, we set:

$$l(n) = \left(\sum_{p \in \mathsf{Loop}(n)} l(p)\right)^*$$

(Since leaves cannot have proper loops, they are labelled with 0^*, which is equivalent to 1 in ℓKA; the map l is well defined: thanks to the definition of $\mathsf{Loop}(n)$, we use only the descendants of n in the tree of $\mathcal{A}$ to compute $l(n)$.) The *expression of* $\mathcal{A}$, $\mathcal{I}(\mathcal{A})$, is defined as follows[2]:

$$\mathcal{I}(\mathcal{A}) = \{l(p) \mid f \in F,\ p \in \mathsf{Simple}(\iota, f)\}$$

Example 25. *Let us compute the expression of the automaton $\mathcal{A}$ of Ex. 21. First, we need to compute its state labelling l. The only state having a proper loop is the initial state. Thus, modulo ℓ*KA *axioms, we get:*

$$l : q \mapsto \begin{cases} (aa)^* & \text{if } q \text{ is } a^* \Rightarrow X_0, X_1 \\ 1 & \text{otherwise} \end{cases}$$

*There are two paths from the initial state to final states: one going to f_1 and the other to f_2. The expression corresponding to the automaton $\mathcal{A}$ is then $\mathcal{I}(\mathcal{A}) = (aa)^*; (aa)^*, a$. (Again, modulo ℓ*KA*.) Of course, there are many other expressions recognising the language of $\mathcal{A}$; $\mathcal{I}(\mathcal{A})$ is convenient because it is closely related to both X_0 and X_1.*

Remark 26. *We do not state the Kleene theorem ($\mathcal{L}(\mathcal{A}) = \mathcal{L}(\mathcal{I}(\mathcal{A}))$) for this construction as we do not need it in the sequel. Know however that it holds.*

We set $\underline{\mathcal{I}} \triangleq \mathcal{I}(\underline{\mathcal{A}})$ where $\underline{\mathcal{A}}$ is the automaton of the synchronous proof $\prod_{i \in [1,n]} \pi_i$.

4.4 Regular expressions for arbitrary nodes

The computation of $\mathcal{I}(\mathcal{A})$ relies on the precise tree structure of $\mathcal{A}$. We will also need to compute the expression of $\mathcal{A}$ considering another state n of $\mathcal{A}$ as the initial state, which we will denote by $[\![n]\!]$. One could reorganise $\mathcal{A}$ as a tree rooted in n, but this would be very tedious. Another way to proceed is to use the labelling l of $\mathcal{A}$ (with ι as the root of $\mathcal{A}$), and generalise the computation of $\mathcal{I}(\mathcal{A})$ to arbitrary nodes. To do so, we need to generalise the notion of simple path:

Definition 27 (Forward path, expression of an arbitrary node)**.** A path $p = n_1, a_1, \ldots, a_{k-1}, n_k$ in a NFA $\mathcal{A}$ is *forward* if for every $i < j$ such that $n_i = n_j$, there is o such that $i < o < j$, $n_o \neq n_i$ and n_o is an ancestor of n_i in the tree of $\mathcal{A}$. For every state n, we write $\mathsf{Forward}(n)$ for the set of forward paths from n to a final state, and

$$[\![n]\!]_{\mathcal{A}} \triangleq \{l(p) \mid p \in \mathsf{Forward}(n)\} \ .$$

We write $[\![n]\!]$ instead of $[\![n]\!]_{\mathcal{A}}$ when the automaton is clear from the context or when $\mathcal{A} = \underline{\mathcal{A}}$.

We compute forward paths in a concrete graph in App. C; note that they are finitely many: a forward path may visit a given node at most twice.

[2]Formally, $\mathcal{I}(\mathcal{A})$ is a multiset; we however interpret it as a single regular expression, as usual in this paper.

Remark 28. *If ι is the initial state of $\mathcal{A}$, then a path starting from ι is forward if and only if it is simple, since ι is the root of the tree of $\mathcal{A}$. Thus we have that $\mathcal{I}(\mathcal{A}) = [\![\iota]\!]_{\mathcal{A}}$.*

Remark 29. *If π is a synchronised proof and $\mathcal{A} = \mathcal{A}(\pi)$, then $[\![x \Rightarrow \mathcal{X}]\!] = x$ (resp. $[\![\Rightarrow \mathcal{X}]\!] = 1$) if $x \Rightarrow \mathcal{X}$ (resp. $\Rightarrow \mathcal{X}$) is the conclusion of a $\mathcal{H}$ (resp. id) rule.*

We do not need to show that $[\![n]\!]$ is indeed the expression of $\mathcal{A}$ when n is the initial state. Instead, we just need to relate $[\![n]\!]$ and $[\![m]\!]$ of two close nodes n and m.

Lemma 30. *Let $\mathcal{A} = \langle Q, T, \iota, F\rangle$ be a NFA, $q \in Q$, and $\{q_i\}_{i\in[1,k]}$, $\{a_i\}_{i\in[1,k]}$ be sequences such that $\langle q, a_i, q_i\rangle \in T$ $\forall i \in [1,k]$. We have $\ell\mathrm{KA}, \mathcal{H} \vdash a_1[\![q_1]\!] + \cdots + a_k[\![q_k]\!] \leq [\![q]\!]$, and the following rule is derivable in $\mathsf{HKA}{+}\mathcal{H}$:*

$$\frac{\Gamma \to a_1.[\![q_1]\!]; \ldots; a_k.[\![q_k]\!]}{\Gamma \to [\![q]\!]}$$

Damien: I'm quit fident that we ca a slightly simpler without using c tion...

Proof. The inequality of $\ell\mathrm{KA}{+}\mathcal{H}$ follows from derivability of the rule by taking Γ to be $a_1[\![q_1]\!] + \cdots + a_k[\![q_k]\!]$, using Prop. 10 and distributivity. Let us show that the rule is derivable in $\mathsf{HKA}{+}\mathcal{H}$. For every $i \in [1,k]$, we set $\mathcal{F}_i = \{q_i, p | q, a_i, q_i, p \in \mathsf{Forward}(q)\}$ the set of paths starting from q_i which can be prolongated into forward paths of q by going through a_i; and we set $L_i = \{q_i, p | a_i, q_i, p \in \mathsf{Loop}(()q)\}$. First, let us show that:

$$\mathsf{Forward}(q_i) \subseteq \mathcal{F}_i \cup L_i, \mathsf{Forward}(q)$$

Let $p \in \mathsf{Forward}(q_i)$. There are three cases to distinguish:

- The path p does not visit q. In this case $q, a_i, p \in \mathsf{Forward}(q)$ thus $p \in \mathcal{F}_i$.
- p is of the form q_i, s, q, t where s does not contain q but contains an ancestor of q. In this case $q, a_i, p \in \mathsf{Forward}(q)$ thus $p \in \mathcal{F}_i$.
- p is of the form q_i, s, q, t where s does not contain q and contains only descendents of q. Note that a_i, q_i, s is a proper loop of q, hence $q_i, s \in L_i$ moreover $q, t \in \mathsf{Forward}(q)$ since the suffixe of a forward path is a forward path. We have then $p \in L_i, \mathsf{Forward}(q)$.

Let us now find our derivation.

$$\dfrac{\dfrac{\Gamma \to \{a_i, l(p) \mid i \in [1,k], p \in \mathcal{F}_i\} \cup \{a_j, l(r), l(q), a_i, l(p) \mid i,j \in [1,k], p \in \mathcal{F}_i, r \in L_j\}}{\Gamma \to \{l(q), a_i, l(p) \mid i \in [1,k], p \in \mathcal{F}_i\}}\ wk}{\Gamma \to [\![q]\!]}\ *\text{-}r, +\text{-}r, wk$$

We have that:

$$\begin{array}{lcl} \{a_i, l(p) \mid i \in [1,k], p \in \mathcal{F}_i\} & = & \cup_{i\in[1,k]} a_i, \mathcal{F}_i \\ \{a_j, l(r), l(q), a_i, l(p) \mid i,j \in [1,k], p \in \mathcal{F}_i, r \in L_j\} & = & \cup_{i\in[1,k]} a_i, L_i, \mathsf{Forward}(q) \end{array}$$

We can conclude using some weakenings. □

4.5 A minorant lemma

We end up this section by a generic lemma which we use twice in the proofs of the next section. This lemma states that the expression of a node n, $[\![n]\!]_{\mathcal{A}}$, is provably smaller (in $\ell\mathrm{KA}{+}\mathcal{H}$) than the value of any *compatible* function at n. Let us define first this notion of compatibility.

Definition 31. Let $\mathcal{A} = \langle Q, T, \iota, F\rangle$ be a NFA and $f : Q \to \mathrm{Exp}_A$ a function from states to expressions. We say that f is *compatible* with $\mathcal{A}$ if $\ell\mathrm{KA}, \mathcal{H} \vdash 1 \leq f(n)$ whenever n is a leaf of $\mathcal{A}$ and for all transitions $\langle n, a, m\rangle \in T$, we have $\ell\mathrm{KA}, \mathcal{H} \vdash af(m) \leq f(n)$.

For instance, the function $[\![\cdot]\!]_{\mathcal{A}} : n \mapsto [\![n]\!]_{\mathcal{A}}$ is compatible with $\mathcal{A}$ thanks to Lem. 30.

Lemma 32 (Minorant lemma)**.** *Let f be compatible with a NFA $\mathcal{A}$; for all state n, we have:*

$$\ell\mathrm{KA}, \mathcal{H} \vdash [\![n]\!]_{\mathcal{A}} \leq f(n)$$

Proof. Since $[\![n]\!]_{\mathcal{A}} = \sum_{p\in\mathsf{Forward}(n)} l(p)$, we should show that for all path $p \in \mathsf{Forward}(n)$, $\ell\mathrm{KA}, \mathcal{H} \vdash l(p) \leq f(n)$. We proceed by induction on the length of the path p. Let $p \in \mathsf{Forward}(n)$. We can write $p = n, a, m, r$ where m is a child of n in $\mathcal{A}$. Since $l(p) = l(n)al(mr)$, it is enough to show that $\ell\mathrm{KA}, \mathcal{H} \vdash l(n)f(n) \leq f(n)$ and $\ell\mathrm{KA}, \mathcal{H} \vdash al(mr) \leq f(n)$. Let us show the second inequality first; we will show the first inequality afterwards, out of the induction. Note that $mr \in \mathsf{Forward}(m)$ thus $l(mr) \leq f(m)$ by induction, and then $al(mr) \leq af(m)$. By compatibility of f we have that $af(m) \leq f(n)$ which concludes the proof.

Now, let us show now that $\ell\mathrm{KA}, \mathcal{H} \vdash l(n)f(n) \leq f(n)$. We proceed by induction on n, starting from the leaves of the tree of $\mathcal{A}$. Recall that $l(n) = S^*$ where $S = \sum_{p\in\mathsf{Loop}(n)} l(p)$. By the implication (L) of $\ell\mathrm{KA}$, it suffices to show that $\ell\mathrm{KA}, \mathcal{H} \vdash Sf(n) \leq f(n)$, or equivalently that for all path $p \in \mathsf{Loop}(n)$, $\ell\mathrm{KA}, \mathcal{H} \vdash l(p)f(n) \leq f(n)$.

Let $p = a_0, n_1, \ldots, n_k, a_k \in \mathsf{Loop}(n)$. We set $n_0 \triangleq n$ and $n_{k+1} \triangleq n$. For every $i \in [1, k]$, we set $s_i \triangleq a_i, n_{i+1} \ldots n_k, a_k$ and $t_i \triangleq n_i, a_i \ldots n_k, a_k$. We have that:

$$l(s_i) = a_i l(t_{i+1}) \qquad \text{and} \qquad l(t_{i+1}) = l(n_{i+1})l(s_{i+1})$$

We show by an internal induction on the length of s_i that:

$$\ell\mathrm{KA}, \mathcal{H} \vdash l(s_i)f(n) \leq f(n_i)$$

By compatibility of f, we have that $\ell\mathrm{KA}, \mathcal{H} \vdash a_i f(n_{i+1}) \leq f(n_i)$, so it is enough to show that $l(s_i)f(n) \leq a_i f(n_{i+1})$, or simplifying a_i from both sides, that $l(t_{i+1})f(n) \leq f(n_{i+1})$. For that, we show that $l(n_{i+1})f(n_{i+1}) \leq f(n_{i+1})$ and $l(s_{i+1})f(n) \leq f(n_{i+1})$. The first holds thanks to the external induction on n, while the second one comes from the internal induction. □

5 Deriving the inequalities for the invariant

5.1 Deriving $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\Gamma} \leq \underline{\mathcal{I}}$

Let us show the first inequality that should be satisfied by the invariant:

Theorem 33. $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\Gamma} \leq \underline{\mathcal{I}}$

Since $\#\underline{\Gamma} < \#(\underline{e}^*, \underline{\Gamma})$, this follows from the global induction hypothesis and:

Proposition 34. $\mathsf{HKA}, \mathcal{H} \vdash^{\omega} \underline{\Gamma} \to \underline{\mathcal{I}}$.

We generalise the statement into the following lemma.

Lemma 35. *Let π be a synchronised proof of $\Gamma \Rightarrow \mathcal{X}$. We have $\mathsf{HKA}, \mathcal{H} \vdash^{\omega} \Gamma \to [\![\Gamma \Rightarrow \mathcal{X}]\!]_{\mathcal{A}(\pi)}$.*

Prop. 34 follows from Lem. 35 by considering $\underline{\pi}$ and by remembering that $\underline{\mathcal{I}} = [\![\underline{\Gamma} \Rightarrow \underline{X}_1, \ldots, \underline{X}_n]\!]$ as noticed in Rmk. 28.

Proof of Lem. 35. Let $\mathcal{A} = \mathcal{A}(\pi)$; we build the desired proof $\theta(\pi)$ coinductively, by case analysis on the last rule ρ applied in π.

- ρ is a left rule:

$$\text{If} \quad \pi = \dfrac{\left\{ \dfrac{\pi_i}{\Gamma_i \Rightarrow \mathcal{X}} \right\}_{i\in I}}{\Gamma \Rightarrow \mathcal{X}}\ \mathrm{l} \qquad \text{then} \qquad \theta(\pi) = \dfrac{\left\{ \dfrac{\dfrac{\theta(\pi_i)}{\Gamma_i \to [\![\Gamma_i \Rightarrow \mathcal{X}]\!]_{\mathcal{A}}}}{\Gamma_i \to \bigcup_{j\in I} [\![\Gamma_j \Rightarrow \mathcal{X}]\!]_{\mathcal{A}}}\ wk \right\}_{i\in I}}{\dfrac{\Gamma \to \bigcup_{j\in I} [\![\Gamma_j \Rightarrow \mathcal{X}]\!]_{\mathcal{A}}}{\Gamma \to [\![\Gamma \Rightarrow \mathcal{X}]\!]_{\mathcal{A}}}\ (\text{Lem. } 30^{\dagger})}\ \mathrm{l}$$

  (†) $\{\Gamma_i \Rightarrow \mathcal{X}\}_{i\in I}$ are the children of $\Gamma \Rightarrow \mathcal{X}$ in $\mathcal{A}$; the transitions from the latter to the former are labelled with 1.

- ρ is a right rule:

$$\text{If} \quad \pi = \dfrac{\dfrac{\pi'}{\Gamma \Rightarrow \mathcal{X}, Z, \mathcal{Y}}}{\Gamma \Rightarrow \mathcal{X}, Y, \mathcal{Y}}\ \mathrm{r} \qquad \text{then} \qquad \theta(\pi) = \dfrac{\dfrac{\theta(\pi')}{\Gamma \to [\![\Gamma \Rightarrow \mathcal{X}, Z, \mathcal{Y}]\!]_{\mathcal{A}}}}{\Gamma \to [\![\Gamma \Rightarrow \mathcal{X}, Y, \mathcal{Y}]\!]_{\mathcal{A}}}\ (\text{Lem. } 30)$$

- ρ is the hypothesis rule.

$$\text{If} \quad \pi = \dfrac{}{x \Rightarrow \mathcal{X}}\ \mathcal{H} \qquad \text{then} \qquad \theta(\pi) = \dfrac{}{x \to [\![x \Rightarrow \mathcal{X}]\!]_{\mathcal{A}}}\ \mathcal{H}$$

  This is because $[\![x \Rightarrow \mathcal{X}]\!]_{\mathcal{A}} = x$ as noticed in Rmk 29.

- Similarly when ρ is the identity rule.

- ρ is the modal rule.

$$\text{If} \quad \pi = \dfrac{\dfrac{\pi'}{\Gamma \Rightarrow Y_1, \dots, Y_n}\ (a)}{a, \Gamma \Rightarrow a.Y_1, \dots, a.Y_n}\ (a) \qquad \text{then} \qquad \theta(\pi) = \dfrac{\dfrac{\dfrac{\theta(\pi')}{\Gamma \to [\![\Gamma \Rightarrow Y_1, \dots, Y_n]\!]_{\mathcal{A}}}\ (a)}{a, \Gamma \to a.[\![\Gamma \Rightarrow Y_1, \dots, Y_n]\!]_{\mathcal{A}}}\ (a)}{a, \Gamma \to [\![a, \Gamma \Rightarrow a.Y_1, \dots, a.Y_n]\!]_{\mathcal{A}}}\ (\text{Lem. } 30)$$

The obtained $\mathsf{HKA}{+}\mathcal{H}$ preproof is clearly regular and fair for $*$-l. □

5.2 Deriving $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{e}, \underline{\mathcal{I}} \leq \underline{\mathcal{I}}$

We now show that $\mathcal{I}$ is stable by composition with e on the left. This is the part of the proof that justifies the introduction of hypotheses.

Theorem 36. $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{e}, \underline{\mathcal{I}} \leq \underline{\mathcal{I}}$.

Notation 37. If $\mathcal{Y} = Y_1, \dots, Y_n$ and $\sigma : [1, n] \to [1, n]$ we write $\mathcal{Y}_\sigma$ for the n-uple $Y_{\sigma(1)}, \dots, Y_{\sigma(n)}$.

Let $\underline{x}$ be a fresh letter (not appearing in $\underline{e}$, $\underline{\mathcal{I}}$ nor in $\mathcal{H}$), and let $\mathcal{H}_{\underline{x}}$ be the following set of hypotheses, where $\underline{\mathcal{X}} \triangleq \underline{X}_1, \dots, \underline{X}_n$:

$$\mathcal{H}_{\underline{x}} \triangleq \{\underline{x} \leq [\![\underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}_\sigma]\!] \mid \ \sigma : [1, n] \to [1, n]\}$$

To prove Thm. 36, we first show that under these new hypotheses about $\underline{x}$, the sequent $\underline{e}, \underline{x} \to \underline{\mathcal{I}}$ is provable in $\mathsf{HKA}{+}\mathcal{H}{+}\mathcal{H}_{\underline{x}}$ (Prop. 38 below). Intuitively, we do so by mimicking the proof of $\underline{e}, \underline{e}^*, \underline{\Gamma} \to \underline{X}_1$: when we reach a sequent of the form $\underline{e}^*, \underline{\Gamma} \to \underline{X}_i$ in the latter, we reach a sequent of the form $\underline{x} \to [\![\underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}_\sigma]\!]$ in the former, which can be closed using a hypothesis from $\mathcal{H}_{\underline{x}}$.

Damien: slight ab
notation since $\mathcal{X}$,
shorter than expec
low
Amina: I do not ge
point Damien
Damien: this is not
tant: variables $\mathcal{X}$,
reserved for n-upl
used here for m- a
uples with $n = m+$

Once we get this $\mathsf{HKA}{+}\mathcal{H}{+}\mathcal{H}_{\underline{x}}$ proof of $\underline{e}, \underline{x} \to \underline{\mathcal{I}}$, we translate it into a $\ell\mathrm{KA}{+}\mathcal{H}{+}\mathcal{H}_{\underline{x}}$ proof using the induction hypothesis, since $\#(\underline{e}, \underline{x}) < \#(\underline{e}, \underline{e}^*, \underline{\Gamma})$. To get rid of the variable $\underline{x}$ and the hypotheses about it, we show that $\underline{\mathcal{I}}$ satisfies all the hypotheses about $\underline{x}$ (Prop. 40 below), thus $\underline{x}$ can be safely replaced by $\underline{\mathcal{I}}$, and the hypotheses $\mathcal{H}_{\underline{x}}$ that were introduced to characterise $\underline{x}$ are not needed anymore. Since $\underline{x}$ does not appear in $\underline{e}$, $\underline{\Gamma}$, and $\underline{\mathcal{I}}$, we obtain Thm. 36.

We now show Props. 38 and 40. As before, we first need to generalise their statements.

Proposition 38. $\mathsf{HKA}, \mathcal{H}, \mathcal{H}_{\underline{x}} \vdash^{\omega} \underline{e}, \underline{x} \to \underline{\mathcal{I}}$.

Lemma 39. *Let δ be a subproof of $\underline{\pi}$ rooted at $\Delta, \underline{e}^*, \underline{\Gamma} \Rightarrow \mathcal{Y}$. We have $\mathsf{HKA}, \mathcal{H}, \mathcal{H}_{\underline{x}} \vdash^{\omega} \Delta, \underline{x} \to [\![\Delta, \underline{e}^*, \underline{\Gamma} \Rightarrow \mathcal{Y}]\!]$.*

Proof. We proceed in the exact same way as for Lem. 35, that is by building the desired proof $\theta(\delta)$ coinductively, by case analysis of the last rule applied in δ and by mimicking this rule in $\mathsf{HKA}{+}\mathcal{H}{+}\mathcal{H}_{\underline{x}}$ using Lem. 30. The only new case is when the conclusion of δ is $\underline{e}^*, \underline{\Gamma} \Rightarrow \mathcal{Y}$ (that is, $\Delta = \varnothing$). By construction of $\underline{\pi}$, we know that $\mathcal{Y} = \underline{\mathcal{X}}_\sigma$ for some $\sigma : [1, n] \to [1, n]$. The proof $\theta(\delta)$ in this case is just an application of a hypothesis from $\mathcal{H}_{\underline{x}}$. □

Prop. 38 follows: since every $\underline{\pi}_i$ ends with an application of $*$-l rule to $\underline{e}^*, \underline{\Gamma} \to \underline{X}_i$, we have that $\underline{\pi}$ has the form on the left below. Recall that $\underline{\mathcal{I}} = [\![\underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}]\!]$; we get the $\mathsf{HKA}{+}\mathcal{H}{+}\mathcal{H}_{\underline{x}}$ proof on the right.

$$\dfrac{\dfrac{\sigma}{\underline{\Gamma} \Rightarrow \underline{\mathcal{X}}} \qquad \dfrac{\delta}{\underline{e}, \underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}}}{\underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}}\ {*}\text{-}l \qquad\qquad \dfrac{\dfrac{\dfrac{\theta(\delta)}{\underline{e}, \underline{x} \to [\![\underline{e}, \underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}]\!]_{\mathcal{A}}}\ wk}{\underline{e}, \underline{x} \to [\![\underline{\Gamma} \Rightarrow \underline{\mathcal{X}}]\!]; [\![\underline{e}, \underline{e}^*, \underline{\Gamma} \Rightarrow \underline{\mathcal{X}}]\!]}}{\underline{e}, \underline{x} \to \underline{\mathcal{I}}}\ (\text{Lem. 30})$$

Proposition 40. *For every $\sigma : [1, n] \to [1, n]$, we have:*

$$\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\mathcal{I}} \leq [\![\underline{e}^*, \underline{\Gamma} \leq \underline{\mathcal{X}}_\sigma]\!]$$

Proof. If $n = (\Delta \Rightarrow \mathcal{Y})$ is a state of $\underline{\mathcal{A}}$, we write n_σ for the state $\Delta \Rightarrow \mathcal{Y}_\sigma$.

Using this notation, and remembering that $\underline{\mathcal{I}} = [\![\underline{\iota}]\!]$, we can rephrase the statement as $\ell\mathrm{KA}, \mathcal{H} \vdash [\![\underline{\iota}]\!] \leq [\![\underline{\iota}_\sigma]\!]$. To prove this statement we generalise it into the following one. For every state n of $\underline{\mathcal{A}}$ we have:

$$\ell\mathrm{KA}, \mathcal{H} \vdash [\![n]\!] \leq [\![n_\sigma]\!]$$

This is a consequence of Lem. 32, when we consider the function $f : n \mapsto [\![n_\sigma]\!]$. Indeed, f is compatible, since when $\langle n, a, m \rangle \in \underline{T}$, we have also that $\langle n_\sigma, a, m_\sigma \rangle \in \underline{T}$, thus by Lem. 30 we have that $\ell\mathrm{KA}, \mathcal{H} \vdash a[\![m_\sigma]\!] \leq [\![n_\sigma]\!]$, which concludes the proof. □

5.3 Deriving $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\mathcal{I}} \leq X_1$

We finally prove the third requirement for the invariant:

Theorem 41. $\ell\mathrm{KA}, \mathcal{H} \vdash \underline{\mathcal{I}} \leq \underline{X}_1$.

Proof. Given a state n of a NFA $\mathcal{A}$, if $n = \Delta \Rightarrow Y_1, \ldots, Y_n$ we set $\pi_1(n) = Y_1$; if n is a final state, we set $\pi_1(n) = 1$. We can write Thm. 41 using this notation as $\ell\mathrm{KA}, \mathcal{H} \vdash [\![\underline{\iota}]\!] \leq \pi_1(\underline{\iota})$. To show this statement, we generalise it into the following one. For every state n of $\underline{\mathcal{A}}$, we have:

$$\ell\mathrm{KA}, \mathcal{H} \vdash [\![n]\!] \leq \pi_1(n)$$

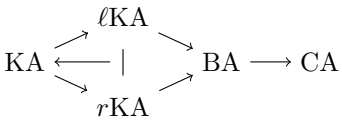


Figure 4: Relationships between complete axiomatisations.

This is a consequence of Lem. 32, when we consider the function $f : n \mapsto \pi_1(n)$. Indeed, by analysing all the synchronised rules, it is easy to show that $\ell\mathrm{KA}, \mathcal{H} \vdash a\pi_1(m) \leq \pi_1(n)$, whenever $\langle n, a, m\rangle$ is a transition of $\underline{\mathcal{A}}$, thus f is compatible. □

This concludes our proof of left-handed completeness (Thm. 2).

6 Conclusion

We have given a new and direct proof of completeness for left-handed Kleene algebra with respect to rational language inclusions. The left-handed derivations we construct closely follow the cyclic proofs of HKA, whose structure in turn corresponds to standard coinductive algorithms for comparing regular expressions. We use the implication of ℓKA (L) at two places: when a starred sub-expression of the left-hand side is unfolded, through the invariant lemma (Lem. 3), and to prove the the minorant lemma (Lem. 32, which is used twice to show that the constructed invariants fulfil the requirements of the invariant lemma).

Unlike Krob[26], Boffa [7], or Silva and Kozen [23], we do not need to exploit any specific laws about Kleene star, like Conway's axioms C11 and C12 ('sumstar' and 'productstar'). Our proof actually implies that those already follow from the characterisation of y^*z as the least fixpoint of $x \mapsto z + yx$ (axioms (ℓ) and (L)).

From a metalogical perspective, this work constitutes an example of translating cyclic proofs to ones that are 'inductive', a matter of considerable interest recently, cf. [29, 15, 1, 6, 13]. While the converse direction is, in general, routine (see, e.g., [10]), the technicalities encountered in this work contribute to our understanding of when the two proof-theoretic phenomena are equipotent. We point out that, despite the aforementioned recent breakthroughs in simulating cyclicity via induction, there are several settings where they do not coincide, e.g. [5].

We conclude with a summary of the complete axiomatisations known so far in Fig. 4. There, KA stands for Kleene algebra, rKA stands for right-handed Kleene algebra (the dual of left-handed Kleene algebra), CA stands for 'Conway algebra', those algebra satisfying Conway's axioms, proven complete by Krob [26], and BA stands for 'Boffa algebra' [8], which is a symmetrical axiomatisation where the only implication is $ee = e \Rightarrow e^* = 1 + e$.

Every left (or right) handed Kleene algebra is a Boffa algebra [8], and every Boffa algebra is a Conway algebra [7]. The converse implications do not hold. There is a Conway algebra which is not even a Boffa algebra [23] (even a finite one); Ex. 1 shows that there are left-handed Kleene algebras which are not right-handed (and vice-versa by symmetry); and one can find Boffa algebras which are neither left nor right handed—see App. F. Note however that the four classes on the left coincide on finite structures: every finite Boffa algebra is a Kleene algebra—App. G.

Krob's completeness result [26] ensures once and for all that the five notions are complete for rational language inclusions. Much simpler proofs have been given for KA [20] and ℓKA [23][present work], and thus rKA by symmetry. Whether relying on Krob's extensive proof

can be avoided for BA remains open: the techniques developed in the present paper do not seem to apply to such structures.

References

[1] B. Afshari and G. E. Leigh. Cut-free completeness for modal mu-calculus. In *Proc. LiCS*, pages 1–12, 2017.

[2] C. J. Anderson, N. Foster, A. Guha, J.-B. Jeannin, D. Kozen, C. Schlesinger, and D. Walker. NetKAT: semantic foundations for networks. In *Proc. POPL*, pages 113–126. ACM, 2014.

[3] A. Angus and D. Kozen. Kleene algebra with tests and program schematology. Technical Report TR2001-1844, CS Dpt., Cornell University, July 2001.

[4] V. M. Antimirov. Partial derivatives of regular expressions and finite automaton constructions. *TCS*, 155(2):291–319, 1996.

[5] S. Berardi and M. Tatsuta. Classical system of martin-löf's inductive definitions is not equivalent to cyclic proof system. In *Proc. FoSSaCS*, pages 301–317, 2017.

[6] S. Berardi and M. Tatsuta. Equivalence of inductive definitions and cyclic proofs under arithmetic. In *Proc. LiCS*, pages 1–12, 2017.

[7] M. Boffa. Une remarque sur les systèmes complets d'identités rationnelles. *Informatique Thorique et Applications*, 24:419–428, 1990.

[8] M. Boffa. Une condition impliquant toutes les identités rationnelles. *Informatique Thorique et Applications*, 29(6):515–518, 1995.

[9] T. Braibant and D. Pous. An efficient Coq tactic for deciding Kleene algebras. In *Proc. 1st ITP*, volume 6172 of *LNCS*, pages 163–178. Springer, 2010.

[10] J. Brotherston and A. Simpson. Sequent calculi for induction and infinite descent. *J. Log. and Comp.*, 21(6):1177–1216, 2011.

[11] J. A. Brzozowski. Derivatives of regular expressions. *J. ACM*, 11(4):481–494, 1964.

[12] J. H. Conway. *Regular algebra and finite machines*. Chapman and Hall, 1971.

[13] A. Das. On the logical complexity of cyclic arithmetic. *ArXiv e-prints*, 2018.

[14] A. Das and D. Pous. A cut-free cyclic proof system for Kleene algebra. In *Proc. TABLEAUX*, volume 10501 of *LNCS*, pages 261–277. Springer, 2017.

[15] A. Doumane. Constructive completeness for the linear-time μ-calculus. In *Proc. LiCS*, pages 1–12, 2017.

[16] C. A. R. Hoare, B. Möller, G. Struth, and I. Wehrman. Concurrent Kleene Algebra. In *Proc. CONCUR*, volume 5710 of *LNCS*, pages 399–414. Springer, 2009.

[17] S. C. Kleene. Representation of events in nerve nets and finite automata. In *Automata Studies*, pages 3–41. Princeton University Press, 1956.

[18] L. Kot and D. Kozen. Kleene algebra and bytecode verification. *ENTCS*, 141(1):221–236, 2005.

[19] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. In *Proc. LICS*, pages 214–225. IEEE, 1991.

[20] D. Kozen. A completeness theorem for Kleene algebras and the algebra of regular events. *Inf. and Comp.*, 110(2):366–390, 1994.

[21] D. Kozen. On Hoare logic and Kleene algebra with tests. *ACM Trans. Comput. Log.*, 1(1):60–76, 2000.

[22] D. Kozen and M.-C. Patron. Certification of compiler optimizations using Kleene algebra with tests. In *Proc. CL2000*, volume 1861 of *LNAI*, pages 568–582. Springer, 2000.

[23] D. Kozen and A. Silva. Left-handed completeness. In *Proc. RAMiCS*, volume 7560 of *LNCS*, pages 162–178. Springer, 2012.

[24] D. Kozen and J. Tiuryn. Substructural logic and partial correctness. *ACM Trans. Comput. Log.*, 4(3):355–378, 2003.

[25] A. Krauss and T. Nipkow. Proof pearl: Regular expression equivalence and relation algebra. *JAR*, 49(1):95–106, 2012.

[26] D. Krob. Complete systems of B-rational identities. *TCS*, 89(2):207–343, 1991.

[27] D. Pous. Kleene Algebra with Tests and Coq tools for while programs. In *Proc. ITP*, volume 7998 of *LNCS*, pages 180–196. Springer, 2013.

[28] V. N. Redko. On defining relations for the algebra of regular events. *Ukrainskii Matematicheskii Zhurnal*, 16:120–126, 1964.

[29] A. Simpson. Cyclic arithmetic is equivalent to peano arithmetic. In *Proc. FoSSaCS*, pages 283–300, 2017.

A Idempotent semirings

We list here the axioms of idempotent semirings, for the sake of self-containedness.

$$e + (f + g) = (e + f) + g \qquad e + f = f + e \qquad e + e = e \qquad e + 0 = e$$

$$e \cdot (f \cdot g) = (e \cdot f) \cdot g \qquad e \cdot 1 = e = 1 \cdot e$$

$$e{\cdot}(f + g) = e{\cdot}f + e{\cdot}g \qquad (e + f){\cdot}g = e{\cdot}g + f{\cdot}g \qquad e{\cdot}0 = 0 = 0{\cdot}e$$

We also recall that in such semirings, one gets a partial order by setting $x \leq y$ if $x + y = y$. Sum acts as a supremum operation for this partial order: $x + y \leq z$ iff $x \leq z$ and $y \leq z$, 0 is a bottom element, and product is monotone.

B More HKA proofs

In order to illustrate the sequent system HKA, we give proofs of Conway's axioms C11 and C12 [12, p. 25]:

$$(C11)\quad (a+b)^* = a^*(ba^*)^* \qquad\qquad (C22)\quad (ab)^* = 1 + a(ba)^*b$$

(C11) left to right:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\to \varepsilon}\,id}{\to \varepsilon; ba^*, (ba^*)^*; a, a^*, (ba^*)^*}\,wk}{\to (ba^*)^*; a, a^*, (ba^*)^*}\,{*}\text{-}r}{\to a^*, (ba^*)^*}\,{*}\text{-}r \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{(a+b)^* \to a^*, (ba^*)^* \quad (\bullet)}\,(a)}{a, (a+b)^* \to a, a^*, (ba^*)^*}\,wk}{a, (a+b)^* \to (ba^*)^*; a, a^*, (ba^*)^*}\,{*}\text{-}r}{a, (a+b)^* \to a^*, (ba^*)^*} \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(a+b)^* \to a^*, (ba^*)^* \quad (\bullet)}\,(b)}{b, (a+b)^* \to b, a^*, (ba^*)^*}\,wk}{b, (a+b)^* \to \varepsilon; b, a^*, (ba^*)^*}\,{\cdot}\text{-}r}{b, (a+b)^* \to \varepsilon; ba^*, (ba^*)^*}\,{*}\text{-}r}{b, (a+b)^* \to (ba^*)^*}\,wk}{b, (a+b)^* \to a^*, (ba^*)^*}\,{*}\text{-}r$$

$$\dfrac{\dfrac{a + b, (a+b)^* \to a^*, (ba^*)^*}{(a+b)^* \to a^*, (ba^*)^* \quad (\bullet)}\,{*}\text{-}l}{(a+b)^* \to a^*(ba^*)^*}\,{\cdot}\text{-}r$$

(C11) right to left:

$$\dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to \varepsilon; a+b, (a+b)^*}\ wk}{\to (a+b)^*}\ {*}\text{-}r \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{a^*, (ba^*)^* \to (a+b)^* \quad (\bullet)}\ (b)}{b, a^*, (ba^*)^* \to b, (a+b)^*}\ wk}{b, a^*, (ba^*)^* \to a+b, (a+b)^*}\ {+}\text{-}r}{b, a^*, (ba^*)^* \to (a+b)^*}\ {*}\text{-}r}{ba^*, (ba^*)^* \to (a+b)^*}\ {\cdot}\text{-}l \qquad \dfrac{\dfrac{\dfrac{\dfrac{}{a^*, (ba^*)^* \to (a+b)^* \quad (\bullet)}\ (a)}{a, a^*, (ba^*)^* \to a, (a+b)^*}\ wk}{a, a^*, (ba^*)^* \to \varepsilon; a, (a+b)^*; b, (a+b)^*}\ {+}\text{-}r}{a, a^*, (ba^*)^* \to \varepsilon; a+b, (a+b)^*}\ {*}\text{-}r}{a, a^*, (ba^*)^* \to (a+b)^*}\ {*}\text{-}l$$

$$\dfrac{(ba^*)^* \to (a+b)^*}{a^*, (ba^*)^* \to (a+b)^* \quad (\bullet)}\ {*}\text{-}l$$

$$\dfrac{a^*, (ba^*)^* \to (a+b)^* \quad (\bullet)}{a^*(ba^*)^* \to (a+b)^*}\ {\cdot}\text{-}l$$

(C12) left to right:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to \varepsilon; a, (ba)^*, b}\ wk \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(ab)^* \to \varepsilon; a, (ba)^*, b \quad (\bullet)}\ (b)}{b, (ab)^* \to b; b, a, (ba)^*, b}\ {\cdot}\text{-}r}{b, (ab)^* \to b; ba, (ba)^*, b}\ {*}\text{-}r}{b, (ab)^* \to (ba)^*, b}\ (a)}{a, b, (ab)^* \to a, (ba)^*, b}\ wk}{a, b, (ab)^* \to \varepsilon; a, (ba)^*, b}\ {\cdot}\text{-}l}{ab, (ab)^* \to \varepsilon; a, (ba)^*, b}\ {*}\text{-}l}{(ab)^* \to \varepsilon; a, (ba)^*, b \quad (\bullet)}\ 1\text{-}r$$

$$\dfrac{(ab)^* \to 1; a, (ba)^*, b}{(ab)^* \to 1; a(ba)^*b}\ {\cdot}\text{-}r, {\cdot}\text{-}r$$

$$\dfrac{(ab)^* \to 1; a(ba)^*b}{(ab)^* \to 1 + a(ba)^*b}\ {+}\text{-}r$$

(C12) right to left:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\to \varepsilon}\ id}{\to \varepsilon; ab, (ab)^*}\ wk}{\to (ab)^*}\ {*}\text{-}r}{1 \to (ab)^*}\ 1\text{-}l \qquad \dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{(ba)^*, b \to b, (ab)^* \quad (\bullet)}\ (a)}{a, (ba)^*, b \to a, b, (ab)^*}\ {\cdot}\text{-}r}{a, (ba)^*, b \to ab, (ab)^*}\ {*}\text{-}r, wk}{a, (ba)^*, b \to (ab)^*}\ (b)}{b, a, (ba)^*, b \to b, (ab)^*}\ {\cdot}\text{-}l}{ba, (ba)^*, b \to b, (ab)^*}\ {*}\text{-}l}{(ba)^*, b \to b, (ab)^* \quad (\bullet)}\ (a)}{a, (ba)^*, b \to a, b, (ab)^*}\ {\cdot}\text{-}r}{a, (ba)^*, b \to ab, (ab)^*}\ {*}\text{-}r, wk}{a, (ba)^*, b \to (ab)^*}\ {\cdot}\text{-}l, {\cdot}\text{-}l}{a(ba)^*b \to (ab)^*}\ {+}\text{-}l$$

$$\dfrac{}{b \to b, (ab)^*}\ {*}\text{-}r, wk, id \quad (b)$$

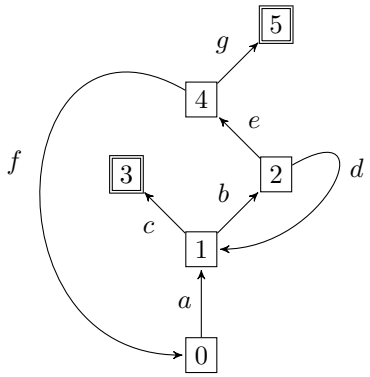
$$\dfrac{1 + a(ba)^*b \to (ab)^*}{}$$

(Note that we could use a back-pointer earlier, right after the top-right modal (b)-step, but this back-pointer would not point to a $*$-l step.)

Unlike the proof from Ex. 7, those four proofs are easy to translate to ℓKA: all their $*$-l steps satisfy the simplifying assumption ($\star$) from Sect. 3 so that we do not need to compute complicated invariants: their (unique) succedent does the job.

C Examples and non-examples of forward paths

We compute $l(\cdot)$ (Def. 24) and forward paths (Def. 27) in the following graph:



n	$l(n)$
0	$(a(bd)^*bef)^*$
1	$(bd)^*$
2	1
3	1
4	1
5	1

n	$\mathsf{Forward}(n)$
0	$0a1c3,\ 0a1b2e4g5$
1	$1c3,\ 1b2e4f\underline{0}a1c3,\ 1b2e4g5,\ 1b2e4f\underline{0}a1b2e4g5$
2	$2d1c3,\ 2e4f0a1c3,\ 2d\underline{1}b2e4f\underline{0}a1c3,\ 2e4g5,\ 2e4f\underline{0}a1b2e4g5$
3	3
4	$4f0a1c3,\ 4g5,\ 4f\underline{0}a1b2e4g5$
5	5

We did underline the nodes that permit loops in forward paths: in the path $1b2e4f\underline{0}a1c3$, the node 0 makes it possible to visit 1 twice; in the path $2d\underline{1}b2e4f\underline{0}a1c3$, the node 1 makes it possible to visit 2 twice, and the node 0 makes it possible to visit 1 twice.

The paths $1b2d1b2e4g5$ and $2e4f0a1b2d1c3$ are not forward: there is no node permitting to visit 1 twice. (Intuitively, these paths are already covered by the labels of the forward paths $1b2e4g5$ and $2e4f0a1c3$, since $l(1) = (bd)^*$.)

D Counter-example to the converse of Thm. 14

It suffices to consider a hypothesis $a \leq b$, and the sequent $ac \to bc$. We immediately get $\ell\mathsf{KA}, a \leq b \vdash ac \leq bc$, but $\mathsf{HKA}, a \leq b \not\vdash^{\mathcal{G}} ac \to bc$. Whether one can find a cut-free variant of $\mathsf{HKA}{+}\mathcal{H}$ to capture derivability in $\ell\mathsf{KA}{+}\mathcal{H}$ remains open—decidability is also open.

E A left-but-not-right handed Kleene algebra

Here we show that the construction from Ex. 1 may yield left-handed Kleene algebra which are not right handed. Consider the complete lattice of extended natural numbers, $\mathbb{N} \cup \{\infty\}$. This

lattice is totally ordered so that every monotone function preserves finite suprema. Take the following monotone functions:

$$\begin{cases} g(i) = 0 & i < \infty \\ g(\infty) = \infty \end{cases} \qquad \begin{cases} f(i) = i + 1 & i < \infty \\ f(\infty) = \infty \end{cases}$$

We have $g + g \cdot f \leq g$, but $g \cdot f^* \not\leq g$: $(g \cdot f^*)(0) = g(f^*(0)) = g(\infty) = \infty$, while $g(0) = 0$.

F A Boffa algebra which is neither left nor right handed

We take natural numbers ordered in the usual sense, completed with three elements $\bot$, ω and $\top$ such that $\bot < i < \omega < \top$ for all $i \in \mathbb{N}$. We define a commutative Boffa algebra as follows; the bottom element (0) of the algebra is $\bot$ and the identity element (1) is 0.

$+$	$\bot$	j	ω	$\top$
$\bot$	$\bot$	j	ω	$\top$
i	i	$\max i\, j$	ω	$\top$
ω	ω	ω	ω	$\top$
$\top$	$\top$	$\top$	$\top$	$\top$

$\cdot$	$\bot$	j	ω	$\top$
$\bot$	$\bot$	$\bot$	$\bot$	$\bot$
i	$\bot$	$i + j$	ω	$\top$
ω	$\bot$	ω	$\top$	$\top$
$\top$	$\bot$	$\top$	$\top$	$\top$

$\cdot^*$	
$\bot$	0
0	0
$i > 0$	ω
ω	$\top$
$\top$	$\top$

The idempotent elements are $\bot$ 0 and $\top$; ω is not idempotent so that the equality $\omega^* = \top$ does not break Boffa's implication. This algebra is however not left-handed (and thus not right-handed since it is commutative): for $x = z = \omega$ and $y = 1$, we have $z + yx = \omega = x$ but $y^* z = \top \not\leq x$.

G Every finite Boffa algebra is a Kleene algebra

Let x be an element of a finite Boffa algebra; we show that that $x^* = x'$, where x' is the (necessarily finite) sum of all powers of x: $x' = \Sigma_i x^i$. First, x^* is above all powers of x, so that $x' \leq x^*$. Then, by distributivity, we have $x'x' = x'$, so that $x'^* = 1 + x' = x'$ by Boffa's implication. Since $x \leq x'$, we conclude $x^* \leq x'^* = x'$ by monotonicity.

The two implications of Kleene algebra follow from distributivity and this characterisation of Kleene star.