A note on commutative Kleene algebra

Paul Brunet

University College London
paul.brunet-zamansky.fr
paul@brunet-zamansky.fr

Abstract. In this paper we present a detailed proof of an important result of algebraic logic: namely that the free commutative Kleene algebra is the space of semilinear sets. The first proof of this result was proposed by Redko in 1964, and simplified and corrected by Pilling in his 1970 thesis. However, we feel that a new account of this proof is needed now. This result has acquired a particular importance in recent years, since it is a key component in the completeness proofs of several algebraic models of concurrent computations (bi-Kleene algebra, concurrent Kleene algebra...). To that effect, we present a new proof of this result.

Keywords: commutative Kleene algebra· completeness theorem· algebraic logic· semilinear sets· Parikh vectors.

1 Introduction

In this paper we present a detailed proof of an important result of algebraic logic: namely that the free commutative Kleene algebra is the space of semilinear sets. This theorem is of central importance, in particular because it is necessary to obtain the completeness of concurrent variants of Kleene algebra, e.g. bi-Kleene algebras [7], concurrent Kleene algebras [2,4], and the recently introduced "concurrent Kleene algebras with observations" [3].

According to Daniel Krob [6]: "a theorem of Redko from 1964 (see [9]), whose proof was simplified and corrected by Pilling (see [8]), gives a complete identities system for the commutative rational expressions". An account of Pilling's proof was also included in Conway's 1971 book [1, Chapter 11].

However we feel that an accessible proof of this result is missing from this picture. To our knowledge, Redko's original proof, published in Russian, has not been translated to English. Pilling and Conway's proofs suffer from another drawback: these were done and published before the theory of Kleene algebra was settled. Since then, basic definitions and notations have diverged enough to render their text difficult to read by contemporary mathematicians.

In particular the axiomatisation that both Redko and Pilling prove complete differ from the one used in e.g. [7,4]. Indeed, they both rely on infinite axiom schemes, namely for each $k > 0$ they include an identity:

$$e^\star \equiv \left(\mathbf{1} + e^1 + \cdots + e^{(k-1)}\right) \cdot \left(e^k\right)^\star. \qquad (\star)$$

This principle may be understood as a limited form of counting modulo k: every natural number may be written as the addition of a number below k and a factor of k. By contrast, we avoid the need for an infinite axiomatisation by relying on an inference rule, in the style of e.g. [5,7,4]:

$$e \cdot x \leqq x \Rightarrow e^\star \cdot x \leqq x.$$

We do need the family of identities $(\star)$ in the proof. However, instead of postulating theses as axioms, we show that they may be derived from our finitary axiomatisation.

Besides showing that the axiomatisation used by Redko and Pilling can be derived from the more "standard" forms found in the literature, we give a step-by-step description of the proof, highlighting the techniques used and the key intermediary results that are needed for this proof. We strive to use standard definitions as much as possible, and to emphasise the relative difficulty of the various proof steps. In our opinion, this proof could be used as a template for formalisation in proof assistants, e.g. Coq or Isabelle.

The proof we present here loosely follows the strategy from Pilling's PhD thesis, although we simplify some arguments and prove others in more details.

The rest of the paper is organised as follows. In Section 2, we lay down some definitions, and provide an overview of the proof, identifying three main proof obligations. We then devote some pages in Section 3 to prove some preliminary results. Finally, in Sections 4, 5, and 6 we discharge the three remaining proof obligations, thus finishing the proof of the main result.

2   Definitions and overview of the proof

2.1   Semi-linear sets

A *Parikh vector* is a Σ-indexed vector of natural numbers. It can also be understood as a *multiset* (i.e. a set with multiplicity), or a *commutative word* (i.e. a sequence without order). The space of Parikh vectors is written $\mathbb{N}^\Sigma$. The vector with uniformly 0 coordinate is written ε. Given a letter $a \in \Sigma$, we write $\{\!|a|\!\}$ for the vector with 1 in coordinate a and 0 on every other coordinate. The addition of two vectors $u, v \in \mathbb{N}^\Sigma$, and the scalar multiplication of a number $n \in \mathbb{N}$ with a vector u are defined coordinate-wise as usual:

$$u \oplus v := \langle u_a + v_a \rangle_{a \in \Sigma} \qquad\qquad u^n := \langle n \times u_a \rangle_{a \in \Sigma}.$$

Let $\mathcal{B} = \{v_1, \cdots, v_n\} \subseteq \mathbb{N}^\Sigma$ be a finite set of vectors, we call a $\mathcal{B}$-point a vector $\alpha \in \mathbb{P}\langle\mathcal{B}\rangle := \mathbb{N}^n$. Such points can be interpreted as vectors by the function $\langle\!|{\_}|\!\rangle_\mathcal{B} : \mathbb{P}\langle\mathcal{B}\rangle \to \mathbb{N}^\Sigma$ defined by $\langle\!|\alpha|\!\rangle_\mathcal{B} := \bigoplus_{1 \leqslant i \leqslant n} v_i^{\alpha_i}$.

We now define the *regular operators* on sets of vectors:

$$\mathcal{U} \oplus \mathcal{V} := \{u \oplus v \mid u \in \mathcal{U},\ v \in \mathcal{V}\} \qquad \mathcal{U} \cup \mathcal{V} := \{u \mid u \in \mathcal{U} \text{ or } v \in \mathcal{V}\}$$

$$\mathcal{U}^\star := \left\{ \bigoplus_{b \in \mathcal{U}} b^{\alpha_b} \ \middle|\ \forall b \in \mathcal{U},\ \alpha_b \in \mathbb{N} \right\}.$$

$$e \cdot (f \cdot g) \equiv (e \cdot f) \cdot g \quad \text{(A1)} \qquad\qquad \mathbf{0} + e \equiv e \quad \text{(A7)}$$
$$e \cdot f \equiv f \cdot e \quad \text{(A2)} \qquad\qquad \mathbf{0} \cdot e \equiv \mathbf{0} \quad \text{(A8)}$$
$$\mathbf{1} \cdot e \equiv e \quad \text{(A3)} \qquad e \cdot (f + g) \equiv (e \cdot f) + (e \cdot g) \quad \text{(A9)}$$
$$e + (f + g) \equiv (e + f) + g \quad \text{(A4)} \qquad \mathbf{1} + e \cdot e^{\star} \leqq e^{\star} \quad \text{(A10)}$$
$$e + f \equiv f + e \quad \text{(A5)} \qquad e \cdot f \leqq f \Rightarrow e^{\star} \cdot f \leqq f \quad \text{(A11)}$$
$$e + e \equiv e \quad \text{(A6)}$$

Table 1. Axioms of commutative Kleene algebra

Notice in particular that for a finite set $\mathcal{B}$ we have $\mathcal{B}^{\star} = \{ \langle\!|\alpha|\!\rangle_{\mathcal{B}} \mid \alpha \in \mathbb{P}\langle \mathcal{B} \rangle \}$.

The *linear set generated by the vector u and the finite set $\mathcal{B} \subseteq \mathbb{N}^{\Sigma}$* is defined by the following expression:

$$\{u\} \oplus \mathcal{B}^{\star} = \left\{ u \oplus \bigoplus_{b \in \mathcal{B}} b^{\alpha_b} \;\middle|\; \forall b \in \mathcal{B}, \alpha_b \in \mathbb{N} \right\}.$$

A *semilinear set* is a finite union of linear sets.

A finite set of vectors $\mathcal{B}$ is called *independent* if every vector in $\mathbb{N}^{\Sigma}$ has at most one decomposition in terms of the vectors in $\mathcal{B}$. In other words $\mathcal{B}$ is independent iff $\langle\!|\_|\!\rangle_{\mathcal{B}}$ is injective.

2.2 Terms & axioms

Let $a, b, \cdots \in \Sigma$ be a finite alphabet. A *regular expression* is a term generated by the following grammar:

$$e, f \in \mathrm{Reg}_{\Sigma} ::= \mathbf{0} \mid \mathbf{1} \mid a \mid e \cdot f \mid e + f \mid e^{\star}.$$

Expressions may be immediately interpreted as sets of vectors:

$$\llbracket \mathbf{0} \rrbracket := \emptyset \qquad\qquad \llbracket \mathbf{1} \rrbracket := \{\varepsilon\} \qquad\qquad \llbracket a \rrbracket := \{\langle\!|a|\!\rangle\}$$
$$\llbracket e^{\star} \rrbracket := \llbracket e \rrbracket^{\star} \qquad \llbracket e \cdot f \rrbracket := \llbracket e \rrbracket \oplus \llbracket f \rrbracket \qquad \llbracket e + f \rrbracket := \llbracket e \rrbracket \cup \llbracket f \rrbracket$$

Notice that for any vector $v \in \mathbb{N}^{\Sigma}$, we may build an expression $[v]_{e} \in \mathrm{Reg}_{\Sigma}$ such that $\llbracket [v]_{e} \rrbracket = \{v\}$:

$$[v]_{e} := \prod_{a \in \Sigma} \left(\prod_{1 \leqslant j \leqslant v_a} a \right) = \underbrace{a \cdot \ldots \cdot a}_{\times v_a} \cdot \ldots \cdot \underbrace{z \cdot \ldots \cdot z}_{\times v_z}.$$

Therefore, any semi-linear set may be represented as the semantics of some regular expression.

We consider the *axiomatic equivalence relation* $\equiv$, defined as the smallest congruence on expressions containing the axioms listed in Table 1. If $e \equiv f$ we

say that e is provably equal to f. We use the convention that $e \leqq f$ means $e + f \equiv f$. It is a simple exercise to check that each of these axioms is sound, meaning that we have:

$$\forall e, f \in \mathrm{Reg}_{\overline{\Sigma}},\ e \equiv f \Rightarrow [\![e]\!] = [\![f]\!]. \tag{2.1}$$

As we will prove in Section 3.1, for finitary expressions, i.e. expressions that do not use the operator $\_^\star$, we also have completeness:

$$\forall e, f \in \mathrm{Reg}_{\overline{\Sigma}}^{fin},\ e \equiv f \Leftrightarrow [\![e]\!] = [\![f]\!]. \tag{2.2}$$

For this reason, we may (and will) dispense with the $[\_]_e$ notation, and identify the vector u and the expression $[u]_e$. We also identify a finite set E of expressions (or a finite set of vectors) with the expression $\sum_{e \in E} e$. This does not introduce ambiguity, thanks to the properties of $+$, in particular associativity (A4), commutativity (A5), and idempotency (A6).

A *linear* expression is a term $e \in \mathrm{Reg}_{\overline{\Sigma}}$ of the form $e = u \cdot \mathcal{B}^\star$, for some vector $u \in \mathbb{N}^{\Sigma}$ and finite set $\mathcal{B} \subseteq \mathbb{N}^{\Sigma}$. A *semilinear* expression is a finite sum of linear expressions. A linear expression $u \cdot \mathcal{B}^\star$ is said to be *unambiguous* when $\mathcal{B}$ is independent.

The *dimension* of a linear expression $u \cdot \mathcal{B}^\star$ is the cardinal of $\mathcal{B}$. The dimension of a semilinear expression e, written $\dim(e)$, is the maximum of the dimensions of the linear expressions composing it:

$$\dim\left(\sum_{i \in I} u_i \cdot \mathcal{B}_i^{\star}\right) := \max\left\{\#\mathcal{B}_i \mid i \in I\right\}.$$

2.3   Overview of the completeness proof

In this section we provide an overview of the proof that two expressions that share the same semantics are provably equal. Since $\leqq$ is antisymmetric with respect to $\equiv$, it is enough to show that if the semantics of e is contained in that of f, then the inequality $e \leqq f$ is derivable from (A1)-(A11).

The first step of the proof is the following proposition:

Proposition 1. *Every regular expression is provably equal to a finite sum of unambiguous linear expressions.*

Proof (Sketch). To prove this result, we will need two steps, first splitting expressions into finite sums of linear expressions (i.e. semilinear expressions), and then splitting single linear expressions into finite sums of unambiguous expressions. This later step more technically involved, and relies on an induction on the dimension of semilinear terms.   □

Remark 1. This entails that the sets of vectors generated by regular expressions are exactly the semilinear sets. Another consequence is that any semilinear set can be built as a finite union of linear sets generated by *independent* families.

We then discharge the case where e and f are both linear (unambiguity does not play a role here). This proof is fairly straightforward.

Proposition 2. *Given two linear expressions e, f, if $[\![e]\!] \subseteq [\![f]\!]$ then $e \leqq f$.*

Using Proposition 1, together with the fact that $+$ is a join operator with respect to $\leqq$, we may extend this seamlessly to the containment of an arbitrary expression inside a single linear expression.

Corollary 4. *For any terms e, f such that f is linear and $[\![e]\!] \subseteq [\![f]\!]$, then $e \leqq f$.*

We then arrive to the most subtle part of the proof:

Proposition 3. *Let f be an unambiguous linear expression. For any expression e there are expressions $[e \wedge f], [e \setminus f]$ such that (i) $e \equiv [e \wedge f] + [e \setminus f]$, (ii) $[\![[e \wedge f]]\!] \subseteq [\![f]\!]$, and (iii) $[\![[e \setminus f]]\!] \subseteq [\![e]\!] \setminus [\![f]\!]$.*

Proof (Sketch). To prove this proposition, we first discharge the case where $e = u \cdot \mathcal{A}^\star$ and $f = v \cdot \mathcal{B}^\star$ are such that $\mathcal{A} \subseteq \mathcal{B}^\star$. We call this situation "e is compatible with f", and prove it by induction on the cardinality of $\mathcal{A}$.

Given a fixed unambiguous linear expression $f = v \cdot \mathcal{B}^\star$, we then show that any expression e can be split into a sum $e' + e''$, where e' is a sum of compatible expressions, and $[\![e'']\!] \subseteq [\![e]\!] \setminus [\![f]\!]$. For this task, we consider $\mathbb{N}^\Sigma$ as a subset of $\mathbb{Q}^\Sigma$, and use this point of view to extend the independent family $\mathcal{B}$ into a basis $\mathbf{B}$ of the space $\mathbb{Q}^\Sigma$. This allows to to have a bijection between $\mathbb{Q}^\Sigma$ and the rational $\mathbf{B}$-points, meaning in particular that every vector $u \in \mathbb{N}^\Sigma$ has unique "coordinates" with respect to the vectors $\mathcal{b} \in \mathbf{B}$. We may now obtain a characterisation of $\mathcal{B}^\star$ in terms of these coordinates: $u \in \mathcal{B}^\star$ iff u has positive integer coordinates for each $\mathcal{b} \in \mathcal{B}$, and 0 coordinates for each $\mathcal{b} \in \mathbf{B} \setminus \mathcal{B}$. Thanks to the properties of $\mathbb{N}$ inside $\mathbb{Q}$, we know that for any vector $u \in \mathcal{B}$, there is a number $n \in \mathbb{N}$ such that u^n has integer coordinates for each $\mathcal{b} \in \mathbf{B}$. Therefore the crux of the argument revolves around the *sign* of the coordinates.

The most challenging lemma of this development tackles this very question. It states that every expression may be rewritten as a sum $\sum_i u_i \cdot \mathcal{A}_i^\star$ where each $\mathcal{A}_i$ is *homogeneous*. A family of vectors $\mathcal{A}$ is called homogeneous if for each $\mathcal{b} \in \mathbf{B}$, either every vector in $\mathcal{A}$ has uniformly positive $\mathcal{b}$-coordinates, or uniformly negative ones. In the first case of positive $\mathcal{B}$-coordinates and null $(\mathbf{B} \setminus \mathcal{B})$-coordinates, the expression may be massaged into a compatible form. In the other cases, we may rewrite the expression into the sum of an expression contained in $[\![e]\!] \setminus [\![f]\!]$, and one of strictly smaller dimension. We may therefore conclude the proof of Proposition 3 by an induction on the dimension. $\square$

Using these results, we may conclude our development:

Theorem 1 (Completeness of commutative Kleene algebra).
The axioms (A1)-(A11) are sound and complete for the equational theory of semi-linear sets.

Proof. Since soundness is straightforward, we will only focus on completeness. As we noticed earlier, we may restrict our attention to *inclusion* rather that *equivalence*, relying on antisymmetry to conclude.

Let $e, f \in \mathrm{Reg}_{\Sigma}$ be two expressions such that the semantics of e is contained in that of f. Using Proposition 1 we may rewrite f as a finite sum of unambiguous expressions $\sum_{1 \leqslant i \leqslant n} f_i$. We then leverage Proposition 3, to decompose e in terms of the f_i as follows:

$$g_0 := e \qquad\qquad g_{i+1} := [g_i \setminus f_{i+1}] \qquad\qquad e_{i+1} := [g_i \wedge f_{i+1}].$$

By construction, observe that we have

$$g_i \equiv e_{i+1} + g_{i+1} \qquad\qquad [\![e_{i+1}]\!] \subseteq [\![f_{i+1}]\!] \qquad\qquad [\![g_{i+1}]\!] \subseteq [\![g_i]\!] \setminus [\![f_{i+1}]\!].$$

Therefore we obtain that $e \equiv g_0 \equiv e_1 + g_1 \equiv \cdots \equiv e_1 + \cdots + e_n + g_n$ and:

$$[\![g_n]\!] \subseteq [\![e]\!] \setminus [\![f_1]\!] \setminus [\![f_2]\!] \cdots \setminus [\![f_n]\!] = [\![e]\!] \setminus [\![f]\!].$$

Since we assumed $[\![e]\!] \subseteq [\![f]\!]$, we know that $[\![g_n]\!] \subseteq [\![e]\!] \setminus [\![f]\!] = \emptyset$. We may prove by induction on g_n that $g_n \equiv \mathbf{0}$ (a proof is provided in Appendix A).

To conclude, we use Proposition 2 to show that for each i, $e_i \leqq f_i$, thus showing that

$$e \equiv \sum_i e_i + g_n \leqq \sum_i f_i + \mathbf{0} \equiv f. \qquad\qquad \square$$

3 Preliminary results

3.1 Completeness in the finite case

In this section we prove the obvious. The point is to make explicit the techniques and steps that are necessary, or at least useful, to establish statements that are instrumental for the main proof of this paper.

Lemma 1. $\forall u, v \in \mathbb{N}^{\Sigma}, [u \oplus v]_e \equiv [u]_e \cdot [v]_e.$

Proof. By induction on Σ:

▶ $\Sigma = \{a\}$**:** in this case, we only need to use associativity of $\cdot$, i.e. axiom (A₁), to prove that $[a^{(n+m)}]_e \equiv [a^n]_e \cdot [a^m]_e$.

▶ $\Sigma = \{a\} \uplus \Sigma'$**:** in this case, we have:

$$[u]_e = a^{u_a} \cdot [u']_e \qquad\qquad [v]_e = a^{v_a} \cdot [v']_e \qquad\qquad [u \oplus v]_e = a^{(u_a + v_a)} \cdot [u' \oplus v']_e$$

where $u', v' \in \mathbb{N}^{\Sigma'}$. By induction we get $[u' \oplus v']_e \equiv [u']_e \cdot [v']_e$.

$$\begin{aligned}
[u \oplus v]_e = a^{(u_a + v_a)} \cdot [u' \oplus v']_e &\equiv a^{(u_a + v_a)} \cdot [u']_e \cdot [v']_e && \text{(by I.H.)} \\
&\equiv a^{u_a} \cdot [u']_e \cdot a^{v_a} \cdot [v']_e && \text{(by A₁,A₂)} \\
&= [u]_e \cdot [v]_e. && \square
\end{aligned}$$

Lemma 2. *For every expression in* $\mathrm{Reg}_\Sigma^{fin}$, *it holds that* $e \equiv \sum_{v \in [\![e]\!]} [v]_e$.

The proof of this lemma proceeds by a straightforward induction on expressions. We make this explicit in Appendix B

Lemma 3. *For any vector* $u \in \mathbb{N}^\Sigma$ *and any expression* $e \in \mathrm{Reg}_\Sigma$, *we have:*

$$u \in [\![e]\!] \Rightarrow [u]_e \leqq e.$$

Proof. By induction on e:

▶ $\mathbf{0}$, $\mathbf{1}$, a: these cases hold trivially.
▶ $f + g$: $u \in [\![f + g]\!] = [\![f]\!] \cup [\![g]\!]$ implies that either $u \in [\![f]\!]$, in which case we have $[u]_e \leqq f \leqq f + g$, or $u \in [\![g]\!]$, in which case we have $[u]_e \leqq g \leqq f + g$
▶ $f \cdot g$: $u \in [\![f \cdot g]\!] = [\![f]\!] \oplus [\![g]\!]$ implies that there are vectors v, w such that $u = v \oplus w$, $v \in [\![f]\!]$, and $w \in [\![g]\!]$. We conclude this case:

$$\begin{aligned} [u]_e = [v \oplus w]_e &\equiv [v]_e \cdot [w]_e && \text{(By Lemma 1)} \\ &\leqq f \cdot g && \text{(By I.H.)} \end{aligned}$$

▶ $f^\star$: since, $u \in [\![f^\star]\!] = [\![f]\!]^\star$, u may be decomposed as $u = u_1 \oplus \cdots \oplus u_n$, with $\forall i, u_i \in [\![f]\!]$. We conclude this proof:

$$\begin{aligned} [u]_e = [u_1 \oplus \cdots \oplus u_n]_e &\equiv [u_1]_e \cdot \cdots \cdot [u_n]_e && \text{(By Lemma 1)} \\ &\leqq f \cdot \cdots \cdot f && \text{(By I.H.)} \\ &\leqq f^\star && \square \end{aligned}$$

Corollary 1. $\forall e \in \mathrm{Reg}_\Sigma^{fin}, \forall f \in \mathrm{Reg}_\Sigma, [\![e]\!] \subseteq [\![f]\!] \Rightarrow e \leqq f$.

Proof. Thanks to Lemma 2, we know that: $e \equiv \sum_{v \in [\![e]\!]} [v]_e$. Since $[\![e]\!] \subseteq [\![f]\!]$, by Lemma 3 we know that for all $v \in [\![e]\!]$, we can derive $[v]_e \leqq f$. Therefore, we get the following proof:

$$e \equiv \sum_{v \in [\![e]\!]} [v]_e \leqq \sum_{v \in [\![e]\!]} f \equiv f \qquad\qquad \square$$

Corollary 2. $\forall e, f \in \mathrm{Reg}_\Sigma^{fin}, e \equiv f \Leftrightarrow [\![e]\!] = [\![f]\!]$.

Proof. The left to right implication is soundness, which we already stated to hold for any expressions. For the converse direction, notice that $e \equiv f \Leftrightarrow e \leqq f \wedge f \leqq e$, so we obtain the desired entailment by two applications of Corollary 1. $\square$

3.2   Laws of commutative Kleene algebra

Omitted proofs from this section are provided in Appendix C.

The following are laws of Kleene algebra. Since a commutative Kleene algebra is in particular a Kleene algebra, these hold here as well.

$$e^\star \cdot e^\star \equiv e^\star \equiv (e^\star)^\star \tag{E$_1$}$$

$$(e \cdot f^\star)^\star \equiv \mathbf{1} + e \cdot (e + f)^\star \tag{E$_2$}$$

$$e^\star \equiv e^{<n} + e^n \cdot e^\star \tag{E$_3$}$$

Here the notation $e^{<n}$ refers to the expression $e^{<n} := (e + \mathbf{1})^{(n-1)}$, with the convention that $e^{<0} = \mathbf{0}$. Clearly if $n > 0$ we have $\mathbf{1} \leqq e^{<n} \leqq e^\star$. Note also that for any $k \in \mathbb{N}$ we have $e^{<k+1} \equiv e^k + e^{<k}$.

We show the proof of the following principle of Kleene algebra. This was used as an infinitary axiom scheme in both Redko and Pilling's proofs.

Lemma 4. *For any expression $e \in \mathrm{Reg}_\Sigma$ and any positive number $n > 0$ the following holds:*

$$e^\star \equiv e^{<n} \cdot (e^n)^\star. \tag{E4}$$

Proof. We prove both inequalities, relying on antisymmetry of $\leqq$ to conclude.

($\geqq$)**:** clearly if $n > 0$, we have: $e^n \leqq e^{\star n} \equiv e^\star$. Also notice that

$$e^{<n} = (e + \mathbf{1})^{(n-1)} \leqq e^{\star (n-1)} \leqq e^\star$$

Therefore we have the following: $e^{<n} \cdot (e^n)^\star \leqq e^\star \cdot (e^\star)^\star \equiv e^\star$.
($\leqq$)**:** since $n > 0$, we have $\mathbf{1} \leqq e^{<n} \equiv e^{(n-1)} + e^{<n-1}$, hence:

$$
\begin{aligned}
e \cdot e^{<n} \cdot (e^n)^\star &\equiv e \cdot \left(e^{(n-1)} + e^{<n-1} \right) \cdot (e^n)^\star \\
&\equiv e \cdot e^{(n-1)} \cdot (e^n)^\star + e \cdot e^{<n-1} \cdot (e^n)^\star \\
&\equiv e^n \cdot (e^n)^\star + e \cdot e^{<n-1} \cdot (e^n)^\star \\
&\leqq (e^n)^\star + (e + \mathbf{1}) \cdot e^{<n-1} \cdot (e^n)^\star \\
&\equiv \mathbf{1} \cdot (e^n)^\star + e^{<n} \cdot (e^n)^\star \\
&\leqq e^{<n} \cdot (e^n)^\star.
\end{aligned}
$$

By (A11), this entails $e^\star \cdot e^{<n} \cdot (e^n)^\star \leqq e^{<n} \cdot (e^n)^\star$, so we can now conclude since: $e^\star \equiv e^\star \cdot \mathbf{1} \leqq e^\star \cdot e^{<n} \cdot (e^n)^\star \leqq e^{<n} \cdot (e^n)^\star$. □

We will also use the following law of commutative Kleene algebra.

$$(e + f)^\star \equiv e^\star \cdot f^\star \tag{E5}$$

Lemma 5. *Given a finite set $\mathcal{B} = \{u_1, \ldots, u_n\}$ and a point $p \in \mathbb{P}\langle \mathcal{B} \rangle \setminus \varepsilon$, the following holds:*

$$\mathcal{B}^\star \equiv \langle\!\langle p \rangle\!\rangle_{\mathcal{B}}^\star \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^\star \right).$$

Due to the length of this proof, we are unable to reproduce it here. The interested reader may find on extended versions of this abstract. As a corollary, we get the following statement:

Corollary 3. *Given a finite set of vectors $\mathcal{B}$ and a vector $w \in \mathcal{B}^\star$, there exists a semilinear expression e such that (i) $\mathcal{B}^\star \equiv w^\star \cdot e$, and (ii) $\dim(e) < \#\mathcal{B}$.*

Remark 2 (On Pilling's axiomatisation). The axiomatisation proved complete by Pilling differs from ours in several ways. It does not include (A11) or (A10), but is instead entirely composed of identity axioms. It is however infinite, including the identities from Lemma 4 for each value of n. Besides those, it includes our axioms (A1)-(A9), together with (E5) and the following laws, all of which are derivable from (A1)-(A11):

$$\mathbf{1}^\star \equiv \mathbf{1} \qquad (e \cdot f^\star)^\star \equiv \mathbf{1} + e \cdot e^\star \cdot f^\star \qquad (e + f)^\star \equiv (e \cdot f)^\star \cdot (e^\star + f^\star)^\star.$$

3.3 Rational vector spaces

We will use in our development two facts about $\mathbb{Q}$-vector spaces[(\star)].

Remark 3. Any finite set of Parikh vectors $\mathcal{B} \subseteq \mathbb{N}^\Sigma$ is independent according to our definition if and only if it is linearly independent inside the space $\mathbb{Q}^\Sigma$.

Remark 4. Let $\mathcal{B} \subseteq \mathbb{N}^\Sigma$ be a finite independent set of vectors. There exists another finite set $\mathcal{B}' \subseteq \mathbb{N}^\Sigma$ such that (i) $\mathcal{B}$ and $\mathcal{B}'$ are disjoint, (ii) $\mathcal{B} \cup \mathcal{B}'$ is independent, and (iii) $\mathcal{B} \cup \mathcal{B}'$ is a basis of $\mathbb{Q}^\Sigma$.

Proof. This is an instance of the *incomplete basis theorem*:

Let E be a vector space, G a spanning family of E and L a linearly independent set. Then there exists $F \subset G \setminus L$ such that $L \cup F$ is a basis of E.

In our case, we may choose the family G to be the canonical basis on $\mathbb{Q}^\Sigma$, i.e. $\{\langle\!\langle a \rangle\!\rangle_\mathcal{B} \mid a \in \Sigma\} \subseteq \mathbb{N}^\Sigma$. □

4 Decomposition into linear expressions

In this section, we prove the first statement in the proof, i.e. Proposition 1, that states that every expression is provably equal to as a finite sum of unambiguous expressions.

First, we split expressions into finite sums of linear expressions, i.e. semilinear expressions. This first step already entails that every commutative regular language has star-height at most one.

Lemma 6. *Any expression e is provably equal to some semilinear expression.*

Proof. We will show this by induction on expressions.

▶ $\mathbf{0}, \mathbf{1}, a, e + f$**:** these all hold trivially with $\mathbf{0}$ as an empty sum, $\mathbf{1} \equiv \mathbf{1} \cdot \mathbf{0}^\star$ and $a \equiv a \cdot \mathbf{0}^\star$. For $e + f$, since a semilinear expression is defined as a sum, we can simply take the sum of the semilinear expressions computed inductively for e and f.

[(\star)] We provide a detailed proof of Remark 3 in Appendix D.

► $e \cdot f$: we simply make the following computation:

$$e \cdot f \equiv \sum_{1 \leqslant i \leqslant n} u_i \cdot \mathcal{B}_i^\star \cdot \sum_{1 \leqslant i \leqslant m} u_i' \cdot \mathcal{B}_i'^\star$$

$$\equiv \sum_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} u_i \cdot \mathcal{B}_i^\star \cdot u_i' \cdot \mathcal{B}_i'^\star$$

$$\equiv \sum_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m} u_i \cdot v_j \cdot \left(\mathcal{B}_i \cup \mathcal{B}_j'\right)^\star. \qquad \text{(by E5)}$$

► $e^\star$: we perform a similar computation, relying on (E5) and (E2):

$$e^\star \equiv \left(\sum_{1 \leqslant i \leqslant n} u_i \cdot \mathcal{B}_i^\star\right)^\star \equiv \prod_{1 \leqslant i \leqslant n} \left(u_i \cdot \mathcal{B}_i^\star\right)^\star \qquad \text{(by E5)}$$

$$\equiv \prod_{1 \leqslant i \leqslant n} \left(\mathbf{1} + u_i \cdot \left(u_i + \mathcal{B}_i\right)^\star\right) \qquad \text{(by E2)}$$

$$\equiv \sum_{I \subseteq \{1,\ldots,n\}} \left(\prod_{i \in I} u_i\right) \cdot \left(\sum_{i \in I} \left(u_i + \mathcal{B}_i\right)\right)^\star \qquad \square$$

The second step consists in splitting individual linear expressions into sums of unambiguous ones. We will do the decomposition by induction on the dimension of the expressions. In an attempt to clarify the argument, we prove separately the following lemma.

Lemma 7. *Let $\mathcal{B}$ be a finite set of vectors. If $\mathcal{B}$ is not independent, there exists a semilinear expression e such that (i) $\mathcal{B}^\star \equiv e$, and (ii) $dim(e) < \#\mathcal{B}$.*

Proof. If $\mathcal{B}$ is not independent, there is a pair of $\mathcal{B}$-points $\alpha, \beta \in \mathbb{P}\langle\mathcal{B}\rangle$ such that $\alpha \neq \beta$ and $\langle\!\langle\alpha\rangle\!\rangle_\mathcal{B} = \langle\!\langle\beta\rangle\!\rangle_\mathcal{B}$. We define the $\mathcal{B}$-points γ, μ, and ν by

$$\gamma_i := \min\left(\alpha_i, \beta_i\right), \qquad \mu_i := \alpha_i - \gamma_i, \qquad \nu_i := \beta_i - \gamma_i.$$

Observe that by construction μ and ν denote the same $\mathcal{B}$-point, and that for every coordinate either μ_i or ν_i equals 0. We split $\mathcal{B}$ according to μ and ν:

$$\mathcal{B}_\mu := \{u \in \mathcal{B} \mid \mu_u > 0\} \qquad \mathcal{B}_\nu := \{u \in \mathcal{B} \mid \nu_u > 0\}$$

$$\mathcal{B}_0 := \{u \in \mathcal{B} \mid \mu_u = \nu_u = 0\}.$$

Notice that since $\mathcal{B} = \mathcal{B}_\mu \uplus \mathcal{B}_\nu \uplus \mathcal{B}_0$, and thanks to (E5), we have:

$$\mathcal{B}^\star \equiv \left(\mathcal{B}_\mu + \mathcal{B}_\nu + \mathcal{B}_0\right)^\star \equiv \mathcal{B}_\mu^\star \cdot \mathcal{B}_\nu^\star \cdot \mathcal{B}_0^\star$$

Let $w := \langle\!\langle\mu\rangle\!\rangle_\mathcal{B} = \langle\!\langle\nu\rangle\!\rangle_\mathcal{B}$. Since this word is both in $\mathcal{B}_\mu^\star$ and in $\mathcal{B}_\nu^\star$, by Corollary 3 there are semilinear expressions e_μ and e_ν such that:

$$\mathcal{B}_\mu^\star \equiv w^\star \cdot e_\mu \qquad \mathcal{B}_\nu^\star \equiv w^\star \cdot e_\nu \qquad dim(e_\mu) < \#\mathcal{B}_\mu \qquad dim(e_\nu) < \#\mathcal{B}_\nu.$$

Combining these facts together we obtain:

$$\mathcal{B}^\star \equiv w^\star \cdot e_\mu \cdot w^\star \cdot e_\nu \cdot \mathcal{B}_0{}^\star \equiv w^\star \cdot e_\mu \cdot e_\nu \cdot \mathcal{B}_0{}^\star.$$

By distributivity, this expression may be rewritten as a semilinear expression e, the dimension of which is the sum of the dimensions of its terms, i.e.:

$$\begin{aligned}
\dim(e) &= \dim(w^\star) + \dim(e_\mu) + \dim(e_\nu) + \dim(\mathcal{B}_0{}^\star) \\
&= 1 + \dim(e_\mu) + \dim(e_\nu) + \#\mathcal{B}_0 \\
&\leqslant 1 + (\#\mathcal{B}_\mu - 1) + (\#\mathcal{B}_\nu - 1) + \#\mathcal{B}_0 \\
&= (\#\mathcal{B}_\mu + \#\mathcal{B}_\nu + \#\mathcal{B}_0) - 1 = \#\mathcal{B} - 1 < \#\mathcal{B}. \qquad \square
\end{aligned}$$

We may now use this lemma in an induction on the dimension of semilinear expressions to obtain the desired result.

Proposition 1. *Every regular expression is provably equal to a finite sum of unambiguous linear expressions.*

Proof. Let e be a commutative regular expression. By Lemma 6, we can compute a semilinear expression f such that $e \equiv f$. We prove by induction on $\dim(f)$ that f can be written as a sum of unambiguous linear expressions. If f is already a sum of unambiguous linear expressions, then the statement holds. Otherwise, let $u \cdot \mathcal{B}^\star$ be a term in f such that $\mathcal{B}$ is not independent. Notice that by definition of the dimension of an expression, we have $\#\mathcal{B} \leqslant \dim(f)$. Thanks to Lemma 7, we can obtain a semilinear expression f' such that: $\mathcal{B}^\star \equiv f'$ and $\dim(f') < \#\mathcal{B}$. By induction, f' can be rewritten as a sum of unambiguous linear expressions, and by distributivity so can $u \cdot f'$. We repeat this argument for every term in f, and take the sum of the resulting decompositions to obtain a sum of unambiguous linear expressions that is provably equal to f, and so to e. $\qquad \square$

5   Inclusion of linear terms

This step is the easiest in this development. We prove it directly.

Proposition 2. *Given two linear expressions e, f, if $[\![e]\!] \subseteq [\![f]\!]$ then $e \leqq f$.*

Proof. Let $e = u \cdot \mathcal{A}^\star$ and $f = v \cdot \mathcal{B}^\star$. Recall that the pointwise ordering of vectors of natural numbers is a well-quasi ordering, meaning in particular that every infinite set contains at least one ordered pair.

Let $a \in \mathcal{A}$. We now show that $\exists k_a \geqslant 1 : a^k \in \mathcal{B}^\star$. Consider the set $V_a := \{p \in \mathbb{P}\langle \mathcal{B}\rangle \mid v \oplus \langle\!| p |\!\rangle_\mathcal{B} \in u \oplus a^\star\}$. Since $u \oplus a^\star \subseteq [\![e]\!] \subseteq [\![f]\!]$, we know that this set is infinite. Therefore, there are two points $p, q \in V_a$ that are pointwise ordered, which implies that there exists a third point $r \in \mathbb{P}\langle \mathcal{B}\rangle \setminus \varepsilon$ such that $p \oplus r = q$. Since $p, q \in V_a$, there are numbers $n, m \in \mathbb{N}$ such that $v \oplus \langle\!| p |\!\rangle_\mathcal{B} = u \oplus a^n$ and $v \oplus \langle\!| q |\!\rangle_\mathcal{B} = u \oplus a^m$. Since p is pointwise smaller than q, it follows that $n < m$, i.e. $1 \leqslant m - n$. Coincidentally, since $p \oplus r = q$, we get that $\langle\!| r |\!\rangle_\mathcal{B} = \langle\!| q |\!\rangle_\mathcal{B} - \langle\!| p |\!\rangle_\mathcal{B}$, i.e.

$\langle r \rangle_{\mathcal{B}} = a^{(m-n)}$. Therefore, $k_a := m - n$ satisfies the required properties, namely $k_a \geqslant 1$ and $a^{k_a} = \langle r \rangle_{\mathcal{B}} \in \mathcal{B}^\star$.

This is enough to complete the proof:

$$e = u \cdot \mathcal{A}^\star \equiv u \cdot \prod_{a \in \mathcal{A}} \left(a^{<k_a} \cdot \left(a^{k_a} \right)^\star \right) \qquad \text{(by E5,E4)}$$

$$\leqq u \cdot \prod_{a \in \mathcal{A}} \left(a^{<k_a} \cdot (\mathcal{B}^\star)^\star \right) \qquad \text{(by Lemma 3)}$$

$$\equiv \left(u \cdot \prod_{a \in \mathcal{A}} a^{<k_a} \right) \cdot \mathcal{B}^\star$$

$$\leqq v \cdot \mathcal{B}^\star \cdot \mathcal{B}^\star \equiv v \cdot \mathcal{B}^\star = f. \qquad \text{(by Corollary 1)}$$

$\square$

Corollary 4. *For any terms e, f such that f is linear and $[\![e]\!] \subseteq [\![f]\!]$, then $e \leqq f$.*

Proof. By Proposition 1 we can write $e \equiv E$, with E a finite set of (unambiguous) linear expressions. To obtain $e \leqq f$, we only need to show for each $g \in E$ that $g \leqq f$. Since $g \leqq E \equiv e$, by soundness we have $[\![g]\!] \subseteq [\![e]\!]$. Therefore we have g, f linear and $[\![g]\!] \subseteq [\![e]\!] \subseteq [\![f]\!]$: by Proposition 2 we get $g \leqq f$. $\square$

6   Intersection and difference

We fix for the remainder of this section an unambiguous linear term $f := v \cdot \mathcal{B}^\star$. A *decomposition* of an expression e is a pair of terms $\langle x, y \rangle$ such that (i) $e \equiv x + y$, (ii) $[\![x]\!] \subseteq [\![f]\!]$, and (iii) $[\![y]\!] \subseteq [\![e]\!] \setminus [\![f]\!]$.

Remark 5. It is useful to keep in mind that the operations $\_ \cap X$ and $\_ \setminus X$ commute with unions. Because of this, showing that every expression can be decomposed is equivalent to proving that every *linear* expression is decomposable. Indeed, using Lemma 5, we may write any e as a finite sum of linear expressions $e_1, \ldots, e_n$. If we have decompositions $\langle x_i, y_i \rangle$ of each of those terms, then the pair $\langle \sum_i x_i, \sum_i y_i \rangle$ is a decomposition of e.

Now we show that linear expressions that are in some sense "compatible" with f can be decomposed.

Lemma 8. *A linear expression $e = u \cdot \mathcal{A}^\star$ such that $\mathcal{A}^\star \subseteq \mathcal{B}^\star$ can be decomposed.*

Proof. By induction on $\#\mathcal{A}$. If $\#\mathcal{A} = 0$, the statement holds trivially, with $\langle x, y \rangle \in \{\langle e, \mathbf{0} \rangle, \langle \mathbf{0}, e \rangle\}$ depending on whether $u \in [\![f]\!]$. Otherwise, if $[\![e]\!] \cap [\![f]\!] = \emptyset$, then again, the statement holds trivially, with $x = \mathbf{0}$ and $y = e$.

Therefore we only need to consider the case where $\#\mathcal{A} > 0$ and we have a vector $w \in [\![e]\!] \cap [\![f]\!]$. Since $w \in [\![e]\!]$, there is a point $\alpha \in \mathbb{P}\langle \mathcal{A} \rangle$ such that $w = u \cdot \langle \alpha \rangle_{\mathcal{A}}$. We make the following transformation on e, using (E5) and (E3):

$$e = u \cdot \mathcal{A}^\star \equiv u \cdot \prod_{a \in \mathcal{A}} a^\star \equiv u \cdot \prod_{a \in \mathcal{A}} \left(a^{<\alpha(a)} + \left(a^{\alpha(a)} \cdot a^\star \right) \right).$$

For $A \subseteq \mathcal{A}$, we define: $U_A := u \cdot \prod_{a \notin A} a^{<\alpha(a)} \cdot \prod_{a \in A} a^{\alpha(a)}$. Notice that $[\![U_A]\!]$ is finite, and that for $A = \mathcal{A}$, we get $U_\mathcal{A} = u \cdot \prod_{a \in \mathcal{A}} a^{\alpha(a)} = w$. By distributivity, we get from the previous identity:

$$e \equiv \sum_{A \subseteq \mathcal{A}} \sum_{t \in U_A} t \cdot A^\star \equiv (w \cdot \mathcal{A}^\star) + \sum_{A \subsetneq \mathcal{A}} \sum_{t \in U_A} t \cdot A^\star.$$

For each $A \subsetneq \mathcal{A}$, we have (i) $\#A < \#\mathcal{A}$ (ii) $A^\star \subseteq \mathcal{A}^\star \subseteq \mathcal{B}^\star$. Therefore we may use our induction hypothesis to get for each $A \subsetneq \mathcal{A}$ and $t \in U_A$ a pair of terms $x_{t,A}$ and $y_{t,A}$ such that: (i) $t \cdot A^\star \equiv x_{t,A} + y_{t,A}$, (ii) $[\![x_{t,A}]\!] \subseteq [\![f]\!]$, and (iii) $[\![y_{t,A}]\!] \subseteq [\![t \cdot A^\star]\!] \setminus [\![f]\!]$. Finally, we conclude by setting

$$x := (w \cdot \mathcal{A}^\star) + \sum_{A \subsetneq \mathcal{A}} \sum_{t \in U_A} x_{t,A} \qquad\qquad y := \sum_{A \subsetneq \mathcal{A}} \sum_{t \in U_A} y_{t,A}.$$

Clearly, $e \equiv x + y$. Since $w \in [\![f]\!]$, $\mathcal{A}^\star \subseteq \mathcal{B}^\star$ and $f \equiv f \cdot \mathcal{B}^\star$, we know that $[\![w \cdot \mathcal{A}^\star]\!] \subseteq [\![f]\!] \cdot \mathcal{B}^\star = [\![f]\!]$. Therefore we get $[\![x]\!] \subseteq [\![f]\!]$. Finally, we know that

$$[\![y]\!] = \bigcup_{A \subseteq \mathcal{A}} \bigcup_{t \in U_A} [\![y_{t,A}]\!] \subseteq \bigcup_{A \subseteq \mathcal{A}} \bigcup_{t \in U_A} [\![t \cdot A^\star]\!] \setminus [\![f]\!] \subseteq [\![e]\!] \setminus [\![f]\!]. \qquad \square$$

Using Remark 4, we extend $\mathcal{B}$ with $\bar{\mathcal{B}} \subseteq \mathbb{N}^\Sigma$ such that $\mathbf{B} := \mathcal{B} \uplus \bar{\mathcal{B}}$ is a basis of $\mathbb{Q}^\Sigma$. As such, $\langle\!\langle \_ \rangle\!\rangle_\mathbf{B}$ may be seen as a bijection between the rational $\mathbf{B}$-points $\mathbb{Q}^\mathbf{B}$ and the vector space $\mathbb{Q}^\Sigma$. We write $[\_]^\mathbf{B}$ for the inverse bijection. A linear expression $u \cdot \mathcal{A}^\star$ is called *homogeneous* if:

$$\forall \mathscr{b} \in \mathbf{B}, \forall \chi, y \in \mathcal{A}, \, [\chi]_\mathscr{b}^\mathbf{B} > 0 \Rightarrow [y]_\mathscr{b}^\mathbf{B} \geqslant 0.$$

Lemma 9. *Every expression is provably equal to a finite sum of homogeneous expressions.*

Proof. This proof works by double induction. Thanks to Lemma 1, we may write any expression as a finite sum of linear expressions. Therefore, it suffices to show that the statement holds for linear expressions. Let $e := u \cdot \mathcal{A}^\star$. We introduce two more definitions:

– *partial homogeneity*: for a subset $B \subseteq \mathbf{B}$, e is B-homogeneous if:

$$\forall \mathscr{b} \in B, \forall \chi, y \in \mathcal{A}, \, [\chi]_\mathscr{b}^\mathbf{B} > 0 \Rightarrow [y]_\mathscr{b}^\mathbf{B} \geqslant 0.$$

– *$\mathscr{b}$-score*: for $\mathscr{b} \in \mathbf{B}$, the $\mathscr{b}$-score of e is the number $\#\left\{ \chi \in \mathcal{A} \,\middle|\, [\chi]_\mathscr{b}^\mathbf{B} \neq 0 \right\}$.

We now prove by induction on $\#B$ that $\forall B \subseteq \mathbf{B}$, any linear expression $u \cdot \mathcal{A}^\star$ is provably equal to a finite sum of B-homogeneous expressions.

▶ $B = \emptyset$**:** the claim holds trivially, since any linear expression is $\emptyset$-homogeneous.

▶ $\mathscr{b} \uplus B$**:** by induction, any expression is provably equal to a finite sum of B-homogeneous expressions, so what remains to show is the following: any B-homogeneous linear expression is provably equal to a finite sum of $(\mathscr{b} \uplus B)$-homogeneous expressions. (Notice that being $(\mathscr{b} \uplus B)$-homogeneous means being

both B-homogeneous and b-homogeneous.) This we prove by induction on the b-score of the expressions.

▷ **b-score $= 0$:** in this case the expression is already b-homogeneous, and since by assumption it was B-homogeneous, the statement holds.

▷ **otherwise:** if $u \cdot \mathcal{A}^\star$ is already b-homogeneous the statement already holds. Otherwise, there are $x, y \in \mathcal{A}$ such that $[x]_b^{\mathbf{B}} > 0$ and $[y]_b^{\mathbf{B}} < 0$. By the properties of $\mathbb{Q}$, there are two natural numbers $n, m > 0$ such that

$$\left[x^n \oplus y^m\right]_b^{\mathbf{B}} = \left[x^n\right]_b^{\mathbf{B}} + \left[y^m\right]_b^{\mathbf{B}} = n \times \left[x\right]_b^{\mathbf{B}} + m \times \left[y\right]_b^{\mathbf{B}} = 0.$$

Since $x^n \oplus y^m \in \mathcal{A}^\star$, we have by Lemma 5:

$$\mathcal{A}^\star \equiv \left(x^n \oplus y^m\right)^\star \cdot \sum_{v \in \mathcal{A}} \left(v^{<p_v} \cdot \prod_{w \neq v} w^\star\right) \qquad \text{with } p_v := \begin{cases} n & \text{if } v = x \\ m & \text{if } v = y \\ 0 & \text{otherwise} \end{cases}.$$

We may simplify this expression, since if $v \neq x, y$ we have $p_v = 0$, so:

$$v^{<p_v} \cdot \prod_{w \neq v} w^\star = v^{<0} \cdot \prod_{w \neq v} w^\star = \mathbf{0} \cdot \prod_{w \neq v} w^\star \equiv \mathbf{0}.$$

$$\Rightarrow \mathcal{A}^\star \equiv \left(x^n \oplus y^m\right)^\star \cdot \left(x^{<n} \cdot \prod_{w \neq x} w^\star + y^{<m} \cdot \prod_{w \neq y} w^\star\right).$$

Therefore we split $e = u \cdot \mathcal{A}^\star$ into two finite families of linear expressions:

$$e \equiv \left(\sum_{v \in u \cdot x^{<n}} v \cdot \mathcal{A}_1^\star\right) + \left(\sum_{v \in u \cdot y^{<m}} v \cdot \mathcal{A}_1^\star\right)$$
$$\text{where } \mathcal{A}_1 := \left\{x^n \oplus y^m\right\} \cup \left(\mathcal{A} \setminus \{x\}\right)$$
$$\mathcal{A}_2 := \left\{x^n \oplus y^m\right\} \cup \left(\mathcal{A} \setminus \{y\}\right).$$

We want to conclude by apply the induction hypothesis. To do so we must check that each of the linear expressions in the decomposition of e are still B-homogeneous, and that their b-score has decreased strictly. For the first check, just notice that for $a \in B$ since the sign of the a-coordinates of x and y is the same, the sign of $x^n \oplus y^m$ is the same again. Therefore both $\mathcal{A}_1$ and $\mathcal{A}_2$ are B-homogeneous. For the second check, it follows immediately from the definitions that the b-score of both $\mathcal{A}_1$ and $\mathcal{A}_2$ is one less than that of $\mathcal{A}$. We may thus conclude the proof by applying the induction hypothesis to each.   □

Finally, we show the main result of this section, namely:

Proposition 3. *Let f be an unambiguous linear expression. For any expression e there are expressions $[e \wedge f], [e \setminus f]$ such that (i) $e \equiv [e \wedge f] + [e \setminus f]$, (ii) $\llbracket[e \wedge f]\rrbracket \subseteq \llbracket f \rrbracket$, and (iii) $\llbracket[e \setminus f]\rrbracket \subseteq \llbracket e \rrbracket \setminus \llbracket f \rrbracket$.*

Proof. Thanks to Lemma 9 and Remark 5, it is enough to show that every homogeneous expression can be decomposed. We do so by induction on the dimension of the expression.

Let $e = u \cdot \mathcal{A}^\star$ be a homogeneous expression. We distinguish two cases:

1. either $\forall a \in \mathcal{A}$ we have $[a]_b^{\mathbf{B}}$ is non-negative for every $b \in \mathcal{B}$ and 0 otherwise,
2. or there exists $\mathfrak{d} \in \mathcal{A}$ and $b \in \mathbf{B}$ such that either (a) $b \in \mathcal{B}$ and $[\mathfrak{d}]_b^{\mathbf{B}} < 0$, or (b) $b \in \bar{\mathcal{B}}$ and $[\mathfrak{d}]_b^{\mathbf{B}} < 0$, or (c) $b \in \bar{\mathcal{B}}$ and $[\mathfrak{d}]_b^{\mathbf{B}} > 0$.

Let us deal with each case in turn.

1. in this case, we show that e can be written as a finite sum of expressions satisfying the premise of Lemma 8, which allows us to conclude. To do that, notice that for every vector $a \in \mathbb{N}^{\Sigma}$, there is a natural number $n_a > 0$ such that every coordinate of $[a^{n_a}]^{\mathbf{B}}$ is an integer. Furthermore, if $a \in \mathcal{A}$, then the $\bar{\mathcal{B}}$ coordinates of $[a^{n_a}]^{\mathbf{B}}$ are equal to naught, and the $\mathcal{B}$ coordinates of $[a^{n_a}]^{\mathbf{B}}$ are natural numbers. This entails that $a^{n_a} \in \mathcal{B}^\star$. We may thus conclude this case using (E4):

$$u \cdot \mathcal{A}^\star \equiv u \cdot \prod_{a \in \mathcal{A}} a^\star \equiv u \cdot \prod_{a \in \mathcal{A}} \left(a^{<n_a} \cdot a^{n_a \star} \right) \equiv \left(u \cdot \prod_{a \in \mathcal{A}} a^{<n_a} \right) \cdot \left(\sum_{a \in \mathcal{A}} a^{n_a} \right)^\star$$

2. this case as three sub-cases. Since all three can be dispatched in the same way, we only detail the proof in case (a), where we have $\mathfrak{d} \in \mathcal{A}$ and $b \in \mathcal{B}$ such that $[\mathfrak{d}]_b^{\mathbf{B}} < 0$. Let $N = \left\lceil [u]_b^{\mathbf{B}} \right\rceil + 1$, and $u' := u \cdot \mathfrak{d}^N$. We rewrite e as follows:

$$\begin{aligned}
e = u \cdot \mathcal{A}^\star &\equiv u \cdot \mathfrak{d}^\star \cdot (\mathcal{A} \setminus \mathfrak{d})^\star \\
&\equiv u \cdot \left(\mathfrak{d}^{<N} + \mathfrak{d}^N \cdot \mathfrak{d}^\star \right) \cdot (\mathcal{A} \setminus \mathfrak{d})^\star \\
&\equiv u \cdot \mathfrak{d}^{<N} \cdot (\mathcal{A} \setminus \mathfrak{d})^\star + u \cdot \mathfrak{d}^N \cdot \mathfrak{d}^\star \cdot (\mathcal{A} \setminus \mathfrak{d})^\star \\
&\equiv \Big(\underbrace{u \cdot \mathfrak{d}^{<N} \cdot (\mathcal{A} \setminus \mathfrak{d})^\star}_{e'} \Big) + \Big(\underbrace{u' \cdot \mathcal{A}^\star}_{y} \Big).
\end{aligned}$$

The expression e' has dimension strictly smaller than $\#\mathcal{A}$, so we can decompose it using the induction hypothesis. We now show that y does not intersect $\mathcal{B}^\star$, hence $\langle \mathbf{0}, y \rangle$ is a decomposition of y. Let $v \in u' \oplus \mathcal{A}^\star$. Since e is homogeneous, and $[\mathfrak{d}]_b^{\mathbf{B}} < 0$, every vector in $\mathcal{A}$ has non-positive b-coordinates. It then follows that every vector in $\mathcal{A}^\star$ has non-positive b-coordinates. Therefore:

$$\begin{aligned}
[v]_b^{\mathbf{B}} = [v - u']_b^{\mathbf{B}} + [u']_b^{\mathbf{B}} &\leqslant 0 + [u']_b^{\mathbf{B}} \qquad\qquad (v - u' \in \mathcal{A}^\star) \\
&= [u]_b^{\mathbf{B}} + N \times [\mathfrak{d}]_b^{\mathbf{B}} \\
&\leqslant [u]_b^{\mathbf{B}} + N \times (-1) = [u]_b^{\mathbf{B}} - N.
\end{aligned}$$

We know that $[u]_{\mathit{b}}^{\mathbf{B}} < \left\lceil [u]_{\mathit{b}}^{\mathbf{B}} \right\rceil + 1 = N$, so $[u]_{\mathit{b}}^{\mathbf{B}} - N < 0$, meaning $[v]_{\mathit{b}}^{\mathbf{B}} < 0$. If v were in $\mathcal{B}^{\star}$, then there would be a point $p \in \mathbb{P}\langle\mathcal{B}\rangle$ such that $\langle\!\langle p\rangle\!\rangle_{\mathcal{B}} = v$. By definition of $[\_]^{\mathbf{B}}$ we have that $[v]_{\mathit{b}}^{\mathbf{B}} = [\langle\!\langle p\rangle\!\rangle_{\mathcal{B}}]_{\mathit{b}}^{\mathbf{B}} = p(\mathit{b}) \in \mathbb{N}$. Since we have just showed that $[v]_{\mathit{b}}^{\mathbf{B}} < 0$, this is impossible so $v \notin \mathcal{B}^{\star}$. $\qquad\square$

Acknowledgements

References

1. Conway, J.H.: Regular Algebra and Finite Machines. Chapman and Hall (1971)
2. Hoare, C.T., Möller, B., Struth, G., Wehrman, I.: Concurrent Kleene Algebra. In: CONCUR (2009). https://doi.org/10.1007/978-3-642-04081-8_27
3. Kappé, T., Brunet, P., Silva, A., Wagemaker, J., Zanasi, F.: Concurrent Kleene Algebra with Observations: From Hypotheses to Completeness. In: FoSSaCS (2020), submitted
4. Kappé, T., Brunet, P., Silva, A., Zanasi, F.: Concurrent Kleene Algebra: Free Model and Completeness. In: ESOP (2018). https://doi.org/10.1007/978-3-319-89884-1_30
5. Kozen, D.: A Completeness Theorem for Kleene Algebras and the Algebra of Regular Events. Information and Computation **110**(2) (1994). https://doi.org/10.1006/inco.1994.1037
6. Krob, D.: A complete system of B-rational identities. In: ICALP. pp. 60–73 (1990)
7. Laurence, M.R., Struth, G.: Completeness Theorems for Bi-Kleene Algebras and Series-Parallel Rational Pomset Languages. In: RAMiCS (2014). https://doi.org/10.1007/978-3-319-06251-8_5
8. Pilling, D.L.: The Algebra of Operators for Regular Events. Ph.D. thesis, Cambridge University (1970)
9. Redko, V.N.: On the algebra of commutative events. Ukrainskij matematicheskij zhurnal **16**(02), 185–195 (Apr 1964)

A   Omitted proofs of Section 2.3

Lemma 10. *For any $e \in \mathrm{Reg}_\Sigma$ if $[\![e]\!] = \emptyset$, then $e \equiv \mathbf{0}$.*

Proof. We show by induction on $e \in \mathrm{Reg}_\Sigma$ that either $\exists v \in [\![e]\!]$ or $e \equiv \mathbf{0}$:

▶ $e = \mathbf{0}, \mathbf{1}, a$: trivial.
▶ $e = e_1 \cdot e_2$: if e_1 or e_2 is provably equal to $\mathbf{0}$, then by (A8) we get $e \equiv \mathbf{0}$; otherwise we have $v_1 \in [\![e_1]\!]$ and $v_2 \in [\![e_2]\!]$, hence $v_1 \oplus v_2 \in [\![e]\!]$.
▶ $e = e_1 + e_2$: if both e_1 and e_2 are provably equal to $\mathbf{0}$, then thanks to (A6) $e \equiv \mathbf{0}$; otherwise we have either $v \in [\![e_1]\!]$ or $v \in [\![e_2]\!]$, and in both cases we get $v \in [\![e]\!]$;
▶ $e = f^\star$: we have $\varepsilon \in [\![e]\!]$.   □

B   Omitted proofs of Section 3.1

Lemma 2. *For every expression in $\mathrm{Reg}_\Sigma^{fin}$, it holds that $e \equiv \sum_{v \in [\![e]\!]} [v]_e$.*

Proof. By induction on e:

▶ $\mathbf{0}, \mathbf{1}, a$: In each of those case, we have $e = \sum_{v \in [\![e]\!]} [v]_e$, therefore the lemma holds by reflexivity.
▶ $f + g$:

$$f + g \equiv \sum_{v \in [\![f]\!]} [v]_e + \sum_{v \in [\![g]\!]} [v]_e \qquad \text{(by I.H.)}$$

$$\equiv \sum_{v \in [\![f]\!] \cup [\![g]\!]} [v]_e . \qquad \text{(by A4)}$$

▶ $f \cdot g$:

$$f \cdot g \equiv \sum_{u \in [\![f]\!]} [u]_e \cdot \sum_{v \in [\![g]\!]} [v]_e \qquad \text{(by I.H.)}$$

$$\equiv \sum_{u \in [\![f]\!], v \in [\![g]\!]} [u]_e \cdot [v]_e \qquad \text{(by A9,A2)}$$

$$\equiv \sum_{u \in [\![f]\!], v \in [\![g]\!]} [u \oplus v]_e \qquad \text{(by Lemma 1)}$$

$$\equiv \sum_{w \in [\![f \cdot g]\!]} [w]_e \qquad\qquad \square$$

C   Omitted proofs of Section 3.2

Lemma 11. *For any $k \in \mathbb{N}$ we have $e^{<k+1} \equiv e^k + e^{<k}$.*

Proof. First, notice that the right to left inequality holds directly:

$$e^k + e^{<k} = e^k + (e+\mathbf{1})^{(k-1)} \equiv e^k + (e+\mathbf{1})^{(k-1)} \cdot \mathbf{1}$$
$$\leqq (e+\mathbf{1})^k + (e+\mathbf{1})^{(k-1)} \cdot (e+\mathbf{1})$$
$$\equiv (e+\mathbf{1})^k = e^{<k+1}.$$

We now prove the conversion inequality by induction on k.

case $k = 0$: we have

$$e^{<k+1} = (e+\mathbf{1})^0 = \mathbf{1} \leqq \mathbf{1} + e^{<0} = e^0 + e^{<0}.$$

case $k + 1$: in this case, we have

$$e^{<k+2} = (e+\mathbf{1})^{(k+1)} = (e+\mathbf{1}) \cdot e^{<k+1}$$
$$\equiv e \cdot e^{<k+1} + e^{<k+1}$$
$$\leqq e \cdot \left(e^k + e^{<k}\right) + e^{<k+1} \qquad \text{(by I.H.)}$$
$$\equiv e^{(k+1)} + e \cdot e^{<k} + e^{<k+1}$$
$$\leqq e^{(k+1)} + (e+\mathbf{1}) \cdot e^{<k} + e^{<k+1}$$
$$\equiv e^{(k+1)} + e^{<k+1} + e^{<k+1} \equiv e^{(k+1)} + e^{<k+1}. \qquad \square$$

Lemma 12.

$$(e+f)^\star \equiv e^\star \cdot f^\star \qquad \text{(E5)}$$

Proof. Since $e \leqq e + f$ and $f \leqq e + f$, and since $\leqq$ is a precongruence, we get $e^\star \leqq (e+f)^\star$ and $f^\star \leqq (e+f)^\star$, hence:

$$e^\star \cdot f^\star \leqq (e+f)^\star \cdot (e+f)^\star \equiv (e+f)^\star.$$

For the converse direction, we start by showing the following inequality:

$$(e+f) \cdot (e^\star \cdot f^\star) \leqq e^\star \cdot f^\star. \qquad (\star\star)$$

$$(e+f) \cdot e^\star \cdot f^\star \equiv e \cdot e^\star \cdot f^\star + f \cdot e^\star \cdot f^\star$$
$$\equiv e \cdot e^\star \cdot f^\star + e^\star \cdot f \cdot f^\star$$
$$\leqq e^\star \cdot f^\star + e^\star \cdot f^\star \equiv e^\star \cdot f^\star.$$

By (A11), the inequality $(\star\star)$ entails that $(e+f)^\star \cdot (e^\star \cdot f^\star) \leqq e^\star \cdot f^\star$. We may thus conclude, because since $\mathbf{1} \leqq e^\star \cdot f^\star$ we have:

$$(e+f)^\star \equiv (e+f)^\star \cdot \mathbf{1} \leqq (e+f)^\star \cdot e^\star \cdot f^\star \leqq e^\star \cdot f^\star.$$

We have therefore proved both inequalities, we may conclude by antisymmetry.
$$\square$$

Lemma 5. *Given a finite set $\mathcal{B} = \{u_1, \ldots, u_n\}$ and a point $p \in \mathbb{P}\langle\mathcal{B}\rangle \setminus \varepsilon$, the following holds:*

$$\mathcal{B}^{\star} \equiv \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \right).$$

Proof. The inclusion from right to left is trivial, so we focus on the other one. By (A11), and given$^{(\star\star)}$ that the right-hand side is provably larger than $\mathbf{1}$, this amounts to proving:

$$\mathcal{B} \cdot \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \right) \leqq \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \right)$$

$$\Leftrightarrow \forall i, k : u_k \cdot \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \leqq \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \right)$$

We consider two cases, depending on $i \overset{?}{=} k$:

▶ $i \neq k$**:** In this case, we have $u_k \in \{u_j \mid j \neq i\}$, hence $u_k \cdot \prod_{i \neq j} u_j^{\star} \leqq \prod_{i \neq j} u_j^{\star}$, so we obtain:

$$u_k \cdot \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \leqq \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star}$$

$$\leqq \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot \sum_i \left(u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \right).$$

▶ $i = k$**:** In this case, we observe that since $u_i \cdot u_i^{<n} \leqq u_i^{<n} + u_i^{n}$, we have:

$$u_i \cdot \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} \leqq \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{<p_i} \cdot \prod_{i \neq j} u_j^{\star} + \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{i \neq j} u_j^{\star}$$

Since the first term is smaller than our goal, we focus on the second one:

$$\langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{i \neq j} u_j^{\star} \equiv \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{i \neq j} \left(u_j^{<p_j} + u_j^{p_j} \cdot u_j^{\star} \right) \qquad \text{(by E3)}$$

$$\equiv \sum_{I \subseteq \{1,\ldots,n\}\setminus i} \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{\substack{j \neq i \\ j \notin I}} u_j^{<p_j} \cdot \prod_{j \in I} \left(u_j^{p_j} \cdot u_j^{\star} \right)$$

$$\equiv \sum_{I \subsetneq \{1,\ldots,n\}\setminus i} \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{\substack{j \neq i \\ j \notin I}} u_j^{<p_j} \cdot \prod_{j \in I} u_j^{p_j} \cdot \prod_{j \in I} u_j^{\star}$$

$$+ \langle\!\langle p\rangle\!\rangle_{\mathcal{B}}^{\star} \cdot u_i^{p_i} \cdot \prod_{i \neq j} u_j^{p_j} \cdot \prod_{i \neq j} u_j^{\star}$$

We consider those two terms separately:

$^{(\star\star)}$ For this to hold it is necessary to check that $p \neq \varepsilon$, i.e. $\exists i, p_i \neq 0$.

– For the first term, consider $I \subsetneq \{1, \ldots, n\} \setminus i$. Since $I \neq \{1, \ldots, n\} \setminus i$, there is an index k such that $k \neq i$ and $k \notin I$. Observe that we get:

$$\forall j \in I,\ u_j \leqq \prod_{j \neq k} u_j{}^\star \qquad\qquad u_i{}^{p_i} \leqq \prod_{j \neq k} u_j{}^\star$$

$$\prod_{\substack{j \neq i \\ j \notin I}} u_j{}^{<p_j} \equiv u_k{}^{<p_k} \cdot \prod_{\substack{j \neq i,k \\ j \notin I}} u_j{}^{<p_j} \leqq u_k{}^{<p_k} \cdot \prod_{j \neq k} u_j{}^\star.$$

Therefore we obtain

$$\langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot u_i{}^{p_i} \cdot \prod_{\substack{j \neq i \\ j \notin I}} u_j{}^{<p_j} \cdot \prod_{j \in I} u_j{}^{p_j} \cdot \prod_{j \in I} u_j{}^\star$$

$$\leqq\ \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot \prod_{k \neq j} u_j{}^\star \cdot u_k{}^{<p_k} \cdot \prod_{k \neq j} u_j{}^\star \cdot \prod_{k \neq j} u_j{}^\star \cdot \prod_{k \neq j} u_j{}^\star$$

$$\equiv\ \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot u_k{}^{<p_k} \cdot \prod_{k \neq j} u_j{}^\star \leqq \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot \sum_k \left(u_k{}^{<p_k} \cdot \prod_{k \neq j} u_j{}^\star \right).$$

– for the second term, i.e. $\langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot u_i{}^{p_i} \cdot \prod_{i \neq j} u_j{}^{p_j} \cdot \prod_{i \neq j} u_j{}^\star$, first we notice:

$$u_i{}^{p_i} \cdot \prod_{i \neq j} u_j{}^{p_j} \equiv \prod_j u_j{}^{p_j} \equiv \langle\!| p |\!\rangle_{\mathcal{B}}.$$

Therefore we have

$$\langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot u_i{}^{p_i} \cdot \prod_{i \neq j} u_j{}^{p_j} \cdot \prod_{i \neq j} u_j{}^\star \leqq \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot \langle\!| p |\!\rangle_{\mathcal{B}} \cdot \prod_{i \neq j} u_j{}^\star$$

$$\leqq\ \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot \prod_{i \neq j} u_j{}^\star \leqq \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot u_i{}^{<p_i} \cdot \prod_{i \neq j} u_j{}^\star$$

$$\leqq\ \langle\!| p |\!\rangle_{\mathcal{B}}{}^\star \cdot \sum_k \left(u_k{}^{<p_k} \cdot \prod_{k \neq j} u_j{}^\star \right). \qquad\qquad \square$$

D   Omitted proofs of Section 3.3

Remark 3. Any finite set of Parikh vectors $\mathcal{B} \subseteq \mathbb{N}^\Sigma$ is independent according to our definition if and only if it is linearly independent inside the space $\mathbb{Q}^\Sigma$.

Proof. ($\Rightarrow$) Suppose $\mathcal{B}$ is independent. By our definition this means that $\langle\!|_- |\!\rangle_{\mathcal{B}}$ is injective, i.e. for any pair of $\mathcal{B}$-points $\alpha, \beta \in \mathbb{P}\langle \mathcal{B} \rangle$, $\langle\!| \alpha |\!\rangle_{\mathcal{B}} = \langle\!| \beta |\!\rangle_{\mathcal{B}} \Rightarrow \alpha = \beta$. Let $p \in \mathbb{Q}^{\mathcal{B}}$ be a rational $\mathcal{B}$-point such that

$$\bigoplus_{u \in \mathcal{B}} u^{p(u)} = \varepsilon.$$

First, we use the fact that since $\{p(u) \mid u \in \mathcal{B}\}$ is a finite set of rational numbers, there exists a natural number N such that for any $u \in \mathcal{B}$ the number $N \times p(u)$ is an integer. We now define two points $\alpha, \beta \in \mathbb{P}\langle\mathcal{B}\rangle$:

$$\alpha := \left[u \mapsto \begin{cases} N \times p(u) & \text{if } p(u) > 0 \\ 0 & \text{otherwise} \end{cases}\right]$$

$$\beta := \left[u \mapsto \begin{cases} -N \times p(u) & \text{if } p(u) \leqslant 0 \\ 0 & \text{otherwise} \end{cases}\right]$$

It is now a simple exercise to check that $\langle\!\langle\alpha\rangle\!\rangle_{\mathcal{B}} = \langle\!\langle\beta\rangle\!\rangle_{\mathcal{B}}$, which means that $\alpha = \beta$. By unfolding the definitions, this implies that $\alpha = \beta = p = \varepsilon$.

($\Leftarrow$) Now assume that $\mathcal{B}$ is linearly independent, and let $\alpha, \beta \in \mathbb{P}\langle\mathcal{B}\rangle$ such that $\langle\!\langle\alpha\rangle\!\rangle_{\mathcal{B}} = \langle\!\langle\beta\rangle\!\rangle_{\mathcal{B}}$. Now, if we define $p = \alpha - \beta$, we get that:

$$\bigoplus_{u \in \mathcal{B}} u^{p(u)} = \bigoplus_{u \in \mathcal{B}} u^{\alpha(u)} - \bigoplus_{u \in \mathcal{B}} u^{\beta(u)} = \langle\!\langle\alpha\rangle\!\rangle_{\mathcal{B}} - \langle\!\langle\beta\rangle\!\rangle_{\mathcal{B}} = \varepsilon.$$

Since $\mathcal{B}$ is linearly independent, p must be uniformly zero, i.e. $\alpha = \beta$. $\square$