On the Completeness of the Equations for the Kleene Star in Bisimulation

Wan Fokkink

Utrecht University, Department of Philosophy
Heidelberglaan 8, 3584 CS Utrecht, The Netherlands
`fokkink@phil.ruu.nl`

Abstract. A classical result from Redko [20] says that there does not exist a complete finite equational axiomatization for the Kleene star modulo trace equivalence. Fokkink and Zantema [13] showed, by means of a term rewriting analysis, that there does exist a complete finite equational axiomatization for the Kleene star up to strong bisimulation equivalence. This paper presents a simpler and shorter completeness proof. Furthermore, the result is extended to open terms, i.e., to ω-completeness. Finally, it is shown that the three equations for the Kleene star are all essential for completeness.

1 Introduction

Kleene [15] defined a binary operator x^*y in the context of finite automata, which denotes the iterate of x on y. Intuitively, the expression x^*y can choose to execute either x, after which it evolves into x^*y again, or y, after which it terminates. An advantage of the Kleene star is that on the one hand it can express recursion, while on the other hand it can be captured in equational laws. Hence, one does not need meta-principles such as the Recursive Specification Principle from Bergstra and Klop [8]. Kleene formulated several equations for his operator, notably $x^*y = x(x^*y) + y$.

Redko [20] (see also Conway [10]) proved that there does not exist a complete finite equational axiomatization for the Kleene star in language theory. We observe that Redko's proof can be transposed to the binary Kleene star in Basic Process Algebra, denoted by BPA*, modulo trace equivalence. This observation is not immediate because Redko studies the Kleene star in the presence of the special constants 0 and 1 from language theory, which are not present in BPA*. However, Redko's proof does not use these constants; the basic idea is that x^*x is trace equivalent with $(x^n)^*(x + x^2 + \ldots + x^{n-1})$ for each $n \geq 2$, and this infinite number of equivalences cannot be expressed in finitely many equations. This reasoning is also valid in BPA* modulo trace equivalence.

Bergstra, Bethke and Ponse [7] studied BPA* modulo bisimulation equivalence, and they suggested a finite equational axiomatization for it. Fokkink and Zantema [13] proved that this axiomatization is complete, by means of a sophisticated term rewriting analysis. The completeness proof in [13] is deplorably long and complicated. Therefore, the completeness result itself was presented in

the recent handbook chapter of Baeten and Verhoef [6], but its proof was omitted because it was considered beyond the scope of that paper. Here, a simpler completeness proof is proposed, which is based on induction on the structure of process terms. This proof is better suited for presentation in a handbook, or at an advanced process algebra course. Also, the proof method employed here is a general strategy, which can be applied to other iteration constructs just as well, see [3, 2].

Following [17, 14, 3], the preliminaries and the completeness proof focus on open terms, so that we obtain not only completeness, but also ω-completeness of the axioms. This last result is new.

Finally, it is shown that the completeness result is lost if either one of the three equations for the Kleene star is removed from the axiomatization. The proof strategy is to find a model for the axioms minus one of the equations for the Kleene star.

Sewell [22] proved that if the deadlock δ is added to BPA*, then a complete finite equational axiomatization does not exist. Milner [16] formulated an axiomatization for BPA* together with the deadlock δ and the empty process ϵ, which includes a conditional axiom which stems from Salomaa [21] in the setting of language theory. He asked whether his axiomatization is complete with respect to bisimulation. The proof that is presented here stems from an, up to now unsuccessful, attempt to solve this problem. However, the proof in this paper may constitute a first step towards solving Milner's problem. For example, in the setting of BPA* with the deadlock δ, the cases that are not yet covered by this proof can all be reduced to the form $p^*\delta \underline{\leftrightarrow} q^*\delta$.

2 BPA with Binary Kleene Star

2.1 The Syntax

We assume a non-empty alphabet A of atomic actions, with typical elements a, b, c, and a countably infinite set $\mathtt{Var}$ of variables, with typical elements x, y, z. We shall use α, β to range over $A \cup \mathtt{Var}$. Furthermore, we have three binary operators: alternative composition $+$, sequential composition $\cdot$, and the Kleene star *. The language of Basic Process Algebra with the binary Kleene star, denoted by $\mathbb{T}(\mathrm{BPA}^*(A))$, with typical elements P, Q, R, S, T, U, V, consists of all the open terms that can be constructed from the atomic actions and the three binary operators. That is, the BNF grammar for the collection of process terms is as follows:
$$P \quad ::= \quad \alpha \mid P + P \mid P \cdot P \mid P^*P.$$
In the sequel the operator $\cdot$ will often be omitted, so PQ denotes $P \cdot Q$. As binding convention, * and $\cdot$ bind stronger than $+$.

$T(\mathrm{BPA}^*(A))$ denotes the subset of closed process terms in $\mathbb{T}(\mathrm{BPA}^*(A))$, that is, the process terms which do not contain any variables.

2.2 Operational Semantics

Table 1 presents an operational semantics for $\mathbb{T}(\mathrm{BPA}^*(A))$ in Plotkin style [19], where variables are taken to be atomic actions, that is, variable x can execute x and then terminate; the special symbol $\sqrt{}$ represents (successful) termination.

$$\alpha \xrightarrow{\alpha} \sqrt{}$$

$$\frac{P \xrightarrow{\alpha} \sqrt{}}{P+Q \xrightarrow{\alpha} \sqrt{} \xleftarrow{\alpha} Q+P} \qquad \frac{P \xrightarrow{\alpha} P'}{P+Q \xrightarrow{\alpha} P' \xleftarrow{\alpha} Q+P}$$

$$\frac{P \xrightarrow{\alpha} \sqrt{}}{P \cdot Q \xrightarrow{\alpha} Q} \qquad \frac{P \xrightarrow{\alpha} P'}{P \cdot Q \xrightarrow{\alpha} P' \cdot Q}$$

$$\frac{P \xrightarrow{\alpha} \sqrt{}}{P^*Q \xrightarrow{\alpha} P^*Q} \qquad \frac{P \xrightarrow{\alpha} P'}{P^*Q \xrightarrow{\alpha} P'(P^*Q)}$$

$$\frac{Q \xrightarrow{\alpha} \sqrt{}}{P^*Q \xrightarrow{\alpha} \sqrt{}} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P^*Q \xrightarrow{\alpha} Q'}$$

Table 1. Action rules for $\mathbb{T}(\mathrm{BPA}^*(A))$

Process terms are considered modulo bisimulation equivalence from Park [18]. Intuitively, process terms are bisimilar if they have the same branching structure.

Definition 1. Two processes P and Q are *bisimilar*, denoted by $P \underline{\leftrightarrow} Q$, if there is a symmetric binary relation B on processes which relates P and Q such that:

- if $R \ B \ S$ and $R \xrightarrow{\alpha} R'$, then there is a transition $S \xrightarrow{\alpha} S'$ such that $R' \ B \ S'$,
- if $R \ B \ S$ and $R \xrightarrow{\alpha} \sqrt{}$, then $S \xrightarrow{\alpha} \sqrt{}$.

The action rules in Table 1 are in the 'path' format of Baeten and Verhoef [5]. Hence, bisimulation equivalence is a congruence with respect to all the operators, which means that if $P \underline{\leftrightarrow} P'$ and $Q \underline{\leftrightarrow} Q'$, then $P+Q \underline{\leftrightarrow} P'+Q'$ and $PQ \underline{\leftrightarrow} P'Q'$ and $P^*Q \underline{\leftrightarrow} P'^*Q'$. See [5] for the definition of the path format, and for a proof of this congruence result. Their proof uses the extra assumption that the rules are well-founded; Fokkink and Van Glabbeek [12] showed that this requirement can be dropped.

Note that we give operational semantics to open terms, following [17, 14] for process algebra with abstraction, and [3] for process algebra with the prefix iteration operator from [11], which is a restricted version of the Kleene star. This approach deviates from the standard approach, which prescribes to give operational semantics to closed terms only, and to give meaning to open terms by defining $P \underline{\leftrightarrow} Q$ if $P\sigma \underline{\leftrightarrow} Q\sigma$ for all substitutions $\sigma : \mathtt{Var} \to T(\mathrm{BPA}^*(A))$. The next lemma implies that both approaches yield the same notion of bisimulation

equivalence on $\mathbb{T}(\mathrm{BPA}^*(A))$, that is, in our setting, two open terms are bisimilar if and only all their closed instantiations are bisimilar.

Lemma 2. $P \leftrightarrow Q$ *if and only if* $P\sigma \leftrightarrow Q\sigma$ *for all substitutions* $\sigma : \mathrm{Var} \to T(\mathrm{BPA}^*(A))$.

This lemma can be proved following the strategy that was employed in [3] for prefix iteration, although in the case of the binary Kleene star the technical details are considerably more complicated [1]. An easy way out is offered by Sewell [22][Theorems 4 and 5], where this type of result is proved in the more general setting of a simply typed lambda calculus, which captures iteration.

According to Lemma 2, if an axiomatization $\mathcal{E}$ for $\mathbb{T}(\mathrm{BPA}^*(A))$ is sound and complete modulo bisimulation, then it is ω-complete for $T(\mathrm{BPA}^*(A))$ modulo bisimulation. Namely, if $\mathcal{E} \vdash P\sigma = Q\sigma$ for all $\sigma : \mathrm{Var} \to T(\mathrm{BPA}^*(A))$, then soundness yields $P\sigma \leftrightarrow Q\sigma$ for all $\sigma : \mathrm{Var} \to T(\mathrm{BPA}^*(A))$, so Lemma 2 implies $P \leftrightarrow Q$. Then completeness yields $\mathcal{E} \vdash P = Q$.

2.3 The Axioms

Table 2 contains an axiom system for $\mathbb{T}(\mathrm{BPA}^*(A))$. It consists of the standard axioms A1-5 together with three axioms BKS1-3 for the binary Kleene star. The most advanced axiom BKS3 originates from Troeger [23]. In the sequel, $P = Q$ will mean that this equality can be derived from the axioms.

This axiomatization is sound for $\mathbb{T}(\mathrm{BPA}^*(A))$ with respect to bisimulation equivalence, i.e., if $P = Q$ then $P \leftrightarrow Q$. Since bisimulation equivalence is a congruence, this can be verified by checking soundness for each axiom separately, which is left to the reader. The purpose of this paper is to prove that the axiomatization is complete with respect to bisimulation, i.e., if $P \leftrightarrow Q$ then $P = Q$.

A1	$x + y = y + x$
A2	$(x + y) + z = x + (y + z)$
A3	$x + x = x$
A4	$(x + y)z = xz + yz$
A5	$(xy)z = x(yz)$
BKS1	$x(x^*y) + y = x^*y$
BKS2	$(x^*y)z = x^*(yz)$
BKS3	$x^*(y((x + y)^*z) + z) = (x + y)^*z$

Table 2. Axioms for $\mathbb{T}(\mathrm{BPA}^*(A))$

In the sequel, terms are considered modulo associativity and commutativity of the $+$, and we write $P =_{\mathrm{AC}} Q$ if P and Q can be equated by axioms A1,2. As usual, $\sum_{i=1}^{n} P_i$ represents $P_1 + \ldots + P_n$. In the sequel, we will take care to avoid empty sums (where $\sum_{i \in \emptyset} P_i + Q$ is not considered empty).

For each process term P, its collection of possible transitions is non-empty and finite, say $\{P \xrightarrow{\alpha_i} P_i \mid i = 1, ..., m\} \cup \{P \xrightarrow{\beta_j} \sqrt{} \mid j = 1, ..., n\}$. We call

$$\sum_{i=1}^{m} \alpha_i P_i + \sum_{j=1}^{n} \beta_j$$

the *expansion* of P. The terms $\alpha_i P_i$ and β_j are called the *summands* of P.

Lemma 3. *Each process term is provably equal to its expansion.*

Proof. Straightforward, by structural induction, using axioms A4,5 and BKS1.

3 A New Completeness Proof

In this section we present a new proof for the fact that the axioms A1-5+BKS1-3 completely axiomatize $\mathbb{T}(\text{BPA}^*(A))$ modulo bisimulation.

We start with determining a collection of normal forms such that for each infinite derivation $P_0 \xrightarrow{a_0} P_1 \xrightarrow{a_1} P_2 \xrightarrow{a_2} \cdots$ with P_0 a normal form, there is a normal form R^*S and a natural N such that each P_n for $n > N$ is of the form either R^*S or $R'(R^*S)$. Thus, the completeness proof boils down to checking the following three cases: $R^*S \underset{\leftrightarrow}{} T^*U$ and $R'(R^*S) \underset{\leftrightarrow}{} T^*U$ and $R'(R^*S) \underset{\leftrightarrow}{} T'(T^*U)$. Such pairs of bisimilar terms are shown to be provably equal by structural induction with respect to a subtle ordering on terms.

3.1 A Lemma for Normed Processes

Process terms in $\mathbb{T}(\text{BPA}^*(A))$ are *normed*, which means that they are able to terminate in finitely many transitions. The *norm* of a process yields the length of the shortest termination trace of this process; this notion stems from [4]. Norm can be defined inductively as follows.

$$|\alpha| = 1$$
$$|P + Q| = \min\{|P|, |Q|\}$$
$$|PQ| = |P| + |Q|$$
$$|P^*Q| = |Q|.$$

Note that bisimilar processes have the same norm.

Definition 4. P' is a *derivative* of P if P can evolve into P' by zero or more transitions. A derivative P' of P is *proper* if P can evolve into P' by one or more transitions.

The following lemma, which is due to Caucal [9], is typical for normed processes.

Lemma 5. *Let $PQ \underset{\leftrightarrow}{} RS$. By symmetry we may assume $|Q| \leq |S|$. We can distinguish two cases:*

- *either $P \leftrightarrow R$ and $Q \leftrightarrow S$,*
- *or there is a proper derivative P' of P such that $P \leftrightarrow RP'$ and $P'Q \leftrightarrow S$.*

Proof. We prove this lemma from the following facts A and B.

A. If $PQ \leftrightarrow RS$ and $|Q| \leq |S|$, then either $Q \leftrightarrow S$, or there is a proper derivative P' of P such that $P'Q \leftrightarrow S$.

   Proof. We apply induction on $|P|$. First, let $|P| = 1$. Then $P \xrightarrow{\alpha} \sqrt{}$ for some α, so $PQ \xrightarrow{\alpha} Q$. Since $PQ \leftrightarrow RS$, we have two options:
   - $R \xrightarrow{\alpha} \sqrt{}$ and $Q \leftrightarrow S$. Then we are done.
   - $R \xrightarrow{\alpha} R'$ and $Q \leftrightarrow R'S$. This leads to a contradiction: $|Q| \leq |S| < |R'S| = |Q|$.

   Next, suppose that we have proved the case for $|P| \leq n$, and let $|P| = n + 1$. Then there is a P' with $|P'| = n$ and $P \xrightarrow{\alpha} P'$, which implies $PQ \xrightarrow{\alpha} P'Q$. Since $PQ \leftrightarrow RS$, we have two options:
   - $R \xrightarrow{\alpha} \sqrt{}$ and $P'Q \leftrightarrow S$. Then we are done.
   - $R \xrightarrow{\alpha} R'$ and $P'Q \leftrightarrow R'S$. Since $|P'| = n$, induction yields either $Q \leftrightarrow S$ or $P''Q \leftrightarrow S$ for a proper derivative P'' of P'. Again, we are done.

B. If $PQ \leftrightarrow RQ$, then $P \leftrightarrow R$.

   Proof. Define a binary relation B on process terms by $T\ B\ U$ if $TQ \leftrightarrow UQ$. We show that B constitutes a bisimulation relation between P and R:
   - Since $\leftrightarrow$ is symmetric, so is B.
   - $PQ \leftrightarrow RQ$, so $P\ B\ R$.
   - Suppose that $T\ B\ U$ and $T \xrightarrow{\alpha} T'$. Then $TQ \xrightarrow{\alpha} T'Q$, so $TQ \leftrightarrow UQ$ implies that this transition can be mimicked by a transition from UQ. This cannot be a transition $UQ \xrightarrow{\alpha} Q$ because $|T'Q| > |Q|$, so apparently there is a transition $U \xrightarrow{\alpha} U'$ with $T'Q \leftrightarrow U'Q$. Hence, $T'\ B\ U'$.
   - Similarly, we find that if $T\ B\ U$ and $T \xrightarrow{\alpha} \sqrt{}$, then $U \xrightarrow{\alpha} \sqrt{}$.

Finally, we show that facts A and B together prove the lemma. Let $PQ \leftrightarrow RS$ with $|Q| \leq |S|$. According to fact A we can distinguish two cases:

- $Q \leftrightarrow S$. Then $PQ \leftrightarrow RS \leftrightarrow RQ$, so fact B yields $P \leftrightarrow R$.
- $P'Q \leftrightarrow S$ for some proper derivative P' of P. Then $PQ \leftrightarrow RS \leftrightarrow RP'Q$, so fact B yields $P \leftrightarrow RP'$. □

3.2 Basic Terms

We construct a set $\mathbb{B}$ of *basic* process terms, such that each process term is provably equal to a basic term. We will prove the completeness theorem by showing that bisimilar basic terms are provably equal.

Table 3 presents a rewrite system $\mathcal{R}$, which consists of directions of the axioms A4,5 and BKS2, pointing from left to right. The rules in $\mathcal{R}$ are to be interpreted modulo AC of the $+$. $\mathcal{R}$ is terminating, which means that there are no infinite

$$\begin{aligned}
(x+y)z &\longrightarrow xz + yz \\
(xy)z &\longrightarrow x(yz) \\
(x^*y)z &\longrightarrow x^*(yz)
\end{aligned}$$

Table 3. The rewrite system $\mathcal{R}$

reductions. This follows from the following weight function w in the natural numbers.

$$\begin{aligned}
w(\alpha) &= 2 \\
w(P+Q) &= w(P) + w(Q) \\
w(PQ) &= w(P)^2 w(Q) \\
w(P^*Q) &= w(P) + w(Q).
\end{aligned}$$

It is easy to see that if $\mathcal{R}$ reduces P to Q, then $w(P) > w(Q)$. Since the ordering on the natural numbers is well-founded, we can conclude that $\mathcal{R}$ is terminating. Let $\mathbb{G}$ denote the collection of *ground normal forms* of $\mathcal{R}$, i.e., the collection of process terms that cannot be reduced by rules in $\mathcal{R}$. Since $\mathcal{R}$ is terminating, and since its rules are directions of axioms, it follows that each process term is provably equal to a process term in $\mathbb{G}$. The elements in $\mathbb{G}$ are defined by:

$$P ::= \alpha \mid P + P \mid \alpha P \mid P^* P.$$

$\mathbb{G}$ is not yet our desired set of basic terms, due to the fact that there exist process terms in $\mathbb{G}$ which have a derivative outside $\mathbb{G}$. We give an example.

Example 1. Let $A = \{a, b, c\}$. Clearly, $(a^*b)^*c \in \mathbb{G}$, and

$$(a^*b)^*c \xrightarrow{a} (a^*b)((a^*b)^*c).$$

However, the derivative $(a^*b)((a^*b)^*c)$ is not in $\mathbb{G}$ because the third rule in $\mathcal{R}$ reduces this term to $a^*(b((a^*b)^*c))$.

In order to overcome this complication, we introduce the following collection of process terms:

$$\mathbb{H} = \{P^*Q,\ P'(P^*Q) \mid P^*Q \in \mathbb{G} \wedge P' \text{ proper derivative of } P\}.$$

We define an equivalence relation $\cong$ on $\mathbb{H}$ by putting $P'(P^*Q) \cong P^*Q$ for proper derivatives P' of P, and taking the reflexive, symmetric, transitive closure of $\cong$.

The set $\mathbb{B}$ of *basic* terms is the union of $\mathbb{G}$ and $\mathbb{H}$.

Lemma 6. *If $P \in \mathbb{B}$ and $P \xrightarrow{\alpha} P'$, then $P' \in \mathbb{B}$.*

Proof. We apply induction on the structure of P.

If $P \in \mathbb{H} \backslash \mathbb{G}$, then it is of the form $Q'(Q^*R)$ for some normal form Q^*R. So P' is of the form either Q^*R or $Q''(Q^*R)$ for some proper derivative Q'' of Q'. In both cases, $P' \in \mathbb{B}$.

If $P \in \mathbb{G}$, then it is of the form $\sum_i \alpha_i Q_i + \sum_j R_j^* S_j + \sum_k \beta_k$, where the Q_i and R_j and S_j are normal forms. So P' is of the form either Q_i or $R_j^* S_j$ or $R_j'(R_j^* S_j)$ or S_j', which are all basic terms (in the last case, this follows by structural induction). $\square$

3.3 An Ordering on Basic Terms

Norm does not constitute a nice ordering on process terms, because it does not respect term size, for example, $|aa + a| < |aa|$. L-value, from Fokkink and Zantema [13], induces an ordering which does not have this drawback. It is defined as follows:

$$L(P) = \max\{|P'| \mid P' \text{ proper derivative of } P\}.$$

Note that $L(P) < L(PQ)$ because for each proper derivative P' of P, $P'Q$ is a proper derivative of PQ. Likewise, $L(P) < L(P^*Q)$. Since norm is preserved under bisimulation, it follows that the same holds for L-value, that is, if $P \leftrightarrow Q$ then $L(P) = L(Q)$.

We define an ordering on $\mathbb{B}$ as follows:

- $P < Q$ if $L(P) < L(Q)$,
- $P < Q$ if P is a derivative of Q but Q is not a derivative of P,

and we take the transitive closure of $<$.

Note that if $P, Q \in \mathbb{H}$ with $P \cong Q$, then P and Q have the same proper derivatives, and so $L(P) = L(Q)$. These observations imply that the ordering $<$ on $\mathbb{B}$ respects the equivalence $\cong$ on $\mathbb{H}$, that is, if $P \cong Q < R \cong S$, then $P < S$.

Lemma 7. $<$ *is a well-founded ordering on* $\mathbb{B}$.

Proof. If P is a derivative of Q, then all proper derivatives of P are proper derivatives of Q, so $L(P) \le L(Q)$. Hence, if $P < Q$ then $L(P) \le L(Q)$.

Suppose that $<$ is not well-founded, so there exists an infinite chain $P_0 > P_1 > P_2 > \cdots$. Then $L(P_n) \ge L(P_{n+1})$ for all n, so there is an N such that $L(P_N) = L(P_n)$ for all $n > N$. Since $P_N > P_n$ for $n > N$, it follows that P_n is a derivative of P_N for $n > N$. Each process term has only finitely many derivatives, so there are $m, n > N$ with $m < n$ and $P_m =_{\text{AC}} P_n$. Then $P_m \not> P_n$, so we have found a contradiction. Hence, $<$ is well-founded. $\square$

In the next two lemmas, we need a weight function g in the natural numbers, which is defined inductively as follows:

$$
\begin{aligned}
g(\alpha) &= 0 \\
g(P + Q) &= \max\{g(P), g(Q)\} \\
g(PQ) &= \max\{g(P), g(Q)\} \\
g(P^*Q) &= \max\{g(P), g(Q) + 1\}
\end{aligned}
$$

It is not hard to see, by structural induction, that if $P \xrightarrow{\alpha} P'$, then $g(P) \ge g(P')$.

Lemma 8. *Let $P^*Q \in \mathbb{B}$. If Q' is a proper derivative of Q, then $Q' < P^*Q$.*

Proof. Since Q' is a derivative of Q, it follows that $g(Q') \leq g(Q)$. Hence, $g(Q') < g(P^*Q)$, so P^*Q cannot be a derivative of Q'. On the other hand, Q' is a derivative of P^*Q, so then $Q' < P^*Q$. $\square$

Lemma 9. *If $P \in \mathbb{B}$ and $P \xrightarrow{\alpha} P'$, then either $P' < P$, or $P, P' \in \mathbb{H}$ and $P \cong P'$.*

Proof. We will use the following two facts A and B.

A. If $P \in \mathbb{B}$ and $P' \notin \mathbb{H}$ and $P \xrightarrow{\alpha} P'$, then P' has smaller size than P.
   Proof. We apply induction on the structure of P. If $P \in \mathbb{H}\backslash\mathbb{G}$ then it follows that $P' \in \mathbb{H}$, so then we are done. Hence, we may assume that $P \in \mathbb{G}$:

$$P =_{\mathrm{AC}} \sum_i \alpha_i Q_i + \sum_j R_j^* S_j + \sum_k \beta_k.$$

   Since $P \xrightarrow{\alpha} P'$, we find that P' is of one of the following forms:
   - $P' =_{\mathrm{AC}} Q_i$ for some i. In this case we are done because the Q_i have smaller size than P.
   - $P' =_{\mathrm{AC}} R_j'(R_j^* S_j)$ or $P' =_{\mathrm{AC}} R_j^* S_j$ for some j. These cases contradict the assumption that $P' \notin \mathbb{H}$.
   - $S_j \xrightarrow{\alpha} P'$ for some j. In this last case, induction yields that P' has smaller size than S_j, and thus P' has smaller size than P.

B. If $P \in \mathbb{H}$ and $P \xrightarrow{\alpha} P'$, then either $g(P) > g(P')$, or $P' \in \mathbb{H}$ and $P \cong P'$.
   Proof. Since $P \in \mathbb{H}$, either $P =_{\mathrm{AC}} Q'(Q^*R)$ or $P =_{\mathrm{AC}} Q^*R$ for some Q and R. Hence, either $P' =_{\mathrm{AC}} Q''(Q^*R)$ or $P' =_{\mathrm{AC}} Q^*R$ or $P' =_{\mathrm{AC}} R'$ for a proper derivative R' of R. In the first two cases $P' \in \mathbb{H}$ and $P \cong P'$, and in the last case $g(P') = g(R') \leq g(R) < g(Q^*R) = g(P)$.

Now, we are ready to prove the lemma. Let $P \xrightarrow{\alpha} P'$ with $P' \nless P$; we prove that $P, P' \in \mathbb{H}$ and $P \cong P'$.

Since P' is a derivative of P and $P' \nless P$, apparently P is a derivative of P'. So there exists a derivation

$$P_0 \xrightarrow{\alpha_1} P_1 \xrightarrow{\alpha_2} \cdots \xrightarrow{\alpha_n} P_n =_{\mathrm{AC}} P_0, \qquad n \geq 1.$$

where $P_0 =_{\mathrm{AC}} P$ and $P_1 =_{\mathrm{AC}} P'$ and $P_n =_{\mathrm{AC}} P'$.

Suppose that $P_k \notin \mathbb{H}$ for all k. Then according to fact A, P_{k+1} has smaller size than P_k for $k = 0, ..., n-1$, so $P_n =_{\mathrm{AC}} P_0$ has smaller size than P_0; contradiction. Hence, $P_l \in \mathbb{H}$ for some l.

Since each P_k is a derivative of each $P_{k'}$, we have $g(P_k) \leq g(P_{k'})$ for k and k', so $g(P_k)$ must be the same for all k. Then it follows from fact B, together with $P_l \in \mathbb{H}$, that $P_k \in \mathbb{H}$ for all k and $P_0 \cong P_1 \cong \cdots \cong P_n$. $\square$

Elements of $\mathbb{B} \times \mathbb{B}$ are considered modulo commutativity. The well-founded ordering $<$ on $\mathbb{B}$ is extended to a well-founded ordering on $\mathbb{B} \times \mathbb{B}$ as expected: $(P, Q) < (R, S)$ if $P < R$ and $Q \cong S$.

3.4 The Main Theorem

Now we are ready to prove the desired completeness result.

Theorem 10. *If $P \leftrightarrow Q$, then* A1-5+BKS1-3 $\vdash P = Q$.

Proof. Each process term is provably equal to a basic term, so it is sufficient to show that bisimilar basic terms are provably equal. Assume $P, Q \in \mathbb{B}$ with $P \leftrightarrow Q$; we show that $P = Q$, by induction on the ordering $<$ on $\mathbb{B} \times \mathbb{B}$. So suppose that we have already dealt with pairs of bisimilar basic terms that are smaller than (P, Q).

First, assume that P or Q is not in $\mathbb{H}$, say $P \notin \mathbb{H}$. Since $P \leftrightarrow Q$, by using axiom A3 we can adapt the expansions of P and Q to the following forms:

$$P = \sum_{i=1}^{m} \alpha_i P_i + \sum_{j=1}^{n} \beta_j, \qquad Q = \sum_{i=1}^{m} \alpha_i Q_i + \sum_{j=1}^{n} \beta_j,$$

where $P_i \leftrightarrow Q_i$ for $i = 1, ..., m$. Since $P \notin \mathbb{H}$, Lemma 9 says that $P_i < P$ for $i = 1, ..., m$. Furthermore, Lemma 9 says that either $Q_i < Q$ or $Q_i \cong Q$ for $i = 1, ..., m$. Then $(P_i, Q_i) < (P, Q)$, so induction yields $P_i = Q_i$ for $i = 1, ..., m$. Hence, $P = Q$.

Next, assume $P, Q \in \mathbb{H}$. We distinguish three cases.

1. Let $P =_{\text{AC}} R^*S$ and $Q =_{\text{AC}} T^*U$. We prove $R^*S = T^*U$.
   We spell out the expansions of R and T:

   $$R = \sum_{i \in I} R_i, \qquad T = \sum_{j \in J} T_j,$$

   where the R_i and the T_j are of the form either αV or α.
   Clearly, the summands of T^*U are the summands of $T(T^*U)$ together with the summands of U. Hence, since $R^*S \leftrightarrow T^*U$, each term $R_i(R^*S)$ for $i \in I$ is bisimilar either to $T_j(T^*U)$ for a $j \in J$ or to a summand of U. We distinguish these two cases.
   (a) $R_i(R^*S) \leftrightarrow T_j(T^*U)$ for a $j \in J$. Then $R_i(R^*S) \leftrightarrow T_j(R^*S)$ because $R^*S \leftrightarrow T^*U$, so Lemma 5 implies $R_i \leftrightarrow T_j$.
   (b) $R_i(R^*S) \leftrightarrow \alpha U'$ for a $U \xrightarrow{\alpha} U'$.
   Thus, I can be divided into the following, not necessarily disjoint, subsets.

   $$I_0 = \{i \in I \mid \exists j \in J \ (R_i \leftrightarrow T_j)\}$$
   $$I_1 = \{i \in I \mid \exists U \xrightarrow{\alpha} U' \ (R_i(R^*S) \leftrightarrow \alpha U')\}$$

   Similarly, J can be divided:

   $$J_0 = \{j \in J \mid \exists i \in I \ (T_j \leftrightarrow R_i)\}$$
   $$J_1 = \{j \in J \mid \exists S \xrightarrow{\alpha} S' \ (T_j(T^*U) \leftrightarrow \alpha S')\}$$

   If both I_1 and J_1 are not empty, then $U' \leftrightarrow R^*S$ for a proper derivative U' of U and $S' \leftrightarrow T^*U$ for a proper derivative S' of S, and so $U' \leftrightarrow S'$. Then

induction yields $R^*S = U' = S' = T^*U$, and we are done. Hence, we may assume that either I_1 or J_1 is empty, say $J_1 = \emptyset$.

$$\sum_{i \in I_1} R_i(R^*S) + S = U. \tag{1}$$

In order to derive Equation 1, we show that each summand at the left-hand side of the equality sign is provably equal to a summand of U, and vice versa. By definition of I_1, for each $R_i(R^*S)$ with $i \in I_1$ there is a summand $\alpha U'$ of U such that $R_i(R^*S) \underline{\leftrightarrow} \alpha U'$. According to Lemma 8 $U' < T^*U$, so induction yields $R_i(R^*S) = \alpha U'$.
Consider a summand $\alpha S'$ of S. Since $R^*S \underline{\leftrightarrow} T^*U$, and $J_1 = \emptyset$, it follows that $\alpha S'$ is bisimilar with a summand $\alpha U'$ of U, so induction yields $\alpha S' = \alpha U'$. Finally, summands α of S correspond with summands α of U.
By the converse argument it follows that each summand of U is provably equal to a summand at the left-hand side of the equality sign.

We continue with the proof of $R^*S = T^*U$. Since $J_1 = \emptyset$, it follows that $J_0 \neq \emptyset$, so clearly also $I_0 \neq \emptyset$. Put $R_0 = \sum_{i \in I_0} R_i$.

$$R_0 = T. \tag{2}$$

In order to prove this equation, note that by definition of I_0 and $J_0 = J$, each R_i for $i \in I_0$ is bisimilar to a T_j with $j \in J$. Since $L(R_i) \leq L(R) < L(R^*S)$, induction yields $R_i = T_j$. Conversely, each T_j for $j \in J$ is provably equal to a R_i with $i \in I_0$. Hence, $R_0 = T$.

Since $I_0 \cup I_1 = I$, we have $R \stackrel{\mathrm{A3}}{=} R_0 + \sum_{i \in I_1} R_i$. Finally, we can derive $R^*S = T^*U$:

$$
\begin{aligned}
R^*S &\stackrel{\mathrm{A3}}{=} (R_0 + \sum_{i \in I_1} R_i)^*S \\
&\stackrel{\mathrm{BKS3}}{=} R_0^*(\sum_{i \in I_1} R_i((R_0 + \sum_{i \in I_1} R_i)^*S) + S) \\
&\stackrel{\mathrm{A3}}{=} R_0^*(\sum_{i \in I_1} R_i(R^*S) + S) \\
&\stackrel{\mathrm{Eq.1,2}}{=} T^*U.
\end{aligned}
$$

2. Let $P =_{\mathrm{AC}} R'(R^*S)$ and $Q =_{\mathrm{AC}} T^*U$. We prove $R'(R^*S) = T^*U$.
$|U| = |T^*U| = |R'(R^*S)| \geq 2$, so U does not have atomic summands, so its expansion is of the form $\sum_i \alpha_i U_i$. Since $R'(R^*S) \underline{\leftrightarrow} T^*U$, each U_i is bisimilar to R^*S or to a term $R''(R^*S)$. According to Lemma 8 $U_i < T^*U$, and $R^*S \cong R'(R^*S)$ or $R''(R^*S) \cong R'(R^*S)$, so induction yields $U_i = R^*S$ or $U_i = R''(R^*S)$ respectively. This holds for all i, so $U = \sum_i \alpha_i U_i = V(R^*S)$ for some term V. Then $R'(R^*S) \underline{\leftrightarrow} T^*U \underline{\leftrightarrow} (T^*V)(R^*S)$, so Lemma 5 implies $R' \underline{\leftrightarrow} T^*V$. Since $L(R') < L(R'(R^*S))$ and $L(T^*V) < L(T^*U)$, induction yields $R' = T^*V$. Hence, $R'(R^*S) = (T^*V)(R^*S) \stackrel{\mathrm{BKS2}}{=} T^*(V(R^*S)) = T^*U$.

3. Let $P =_{\mathrm{AC}} R'(R^*S)$ and $Q =_{\mathrm{AC}} T'(T^*U)$. We prove $R'(R^*S) = T'(T^*U)$.
By symmetry we may assume $|R^*S| \leq |T^*U|$. Lemma 5 distinguishes two possible cases.

Either $R' \leftrightarrow T'$ and $R^*S \leftrightarrow T^*U$. Since $L(R') < L(R'(R^*S))$, induction yields $R' = T'$, and Case 1 applied to $R^*S \leftrightarrow T^*U$ yields $R^*S = T^*U$.
Or $R' \leftrightarrow T'R''$ and $R''(R^*S) \leftrightarrow T^*U$ for a proper derivative R'' of R'. Since $L(R') < L(R'(R^*S))$, induction yields $R' = T'R''$. Furthermore, Case 1 applied to $R''(R^*S) \leftrightarrow T^*U$ yields $R''(R^*S) = T^*U$. Hence, $R'(R^*S) = (T'R'')(R^*S) \stackrel{\text{BKS2}}{=} T'(R''(R^*S)) = T'(T^*U)$. $\square$

Lemma 2 implies the following corollary.

Corollary 11. *The axiomatization* A1-5+BKS1-3 *is complete and ω-complete for* $T(\text{BPA}^*(A))$ *modulo bisimulation.*

3.5 An Example

We give an example as to how the construction in the completeness proof acts on a particular pair of bisimilar process terms.

Example 2. Let $A = \{a_1, b\}$, and consider the two bisimilar closed process terms:

$$a_1^*b \leftrightarrow a_1^*(a_1^*b).$$

We show how the construction in the proof of Theorem 10 applied to this pair produces a derivation of $a_1^*b = a_1^*(a_1^*b)$.

Clearly both terms are in $\mathbb{H}$, and we are dealing with the first of the three possible cases for bisimilar terms in $\mathbb{H}$ that were distinguished in the completeness proof. Following the notations that were introduced there, we have $I = I_0 = I_1 = \{1\}$ and $J = J_0 = \{1\}$ and $J_1 = \emptyset$. Hence, Equation 1 takes the form $a_1(a_1^*b) + b = a_1^*b$, which is an instantiation of BKS1, and Equation 2 takes the trivial form $a_1 = a_1$. Thus, the derivation at the end of the first case for pairs in $\mathbb{H}$ here takes the following form:

$$
\begin{aligned}
a_1^*b \;\;&\stackrel{\text{A3}}{=}\;\; (a_1 + a_1)^*b \\
&\stackrel{\text{BKS3}}{=}\;\; a_1^*(a_1((a_1 + a_1)^*b) + b) \\
&\stackrel{\text{A3}}{=}\;\; a_1^*(a_1(a_1^*b) + b) \\
&\stackrel{\text{BKS1}}{=}\;\; a_1^*(a_1^*b).
\end{aligned}
$$

3.6 A Comparison of Proof Strategies

We discuss the strategy of the original completeness proof for $T(\text{BPA}^*(A))$ from Fokkink and Zantema [13] . That proof is based on a standard rewriting technique, which means a quest for unique ground normal forms. It is noted that this strive cannot be fulfilled for the Kleene star, so this operator is replaced by $x^{\oplus}y$, which represents $x(x^*y)$, and the axioms BKS1-3 are adopted for this new operator. These axioms are turned into conditional rewrite rules, which are applied modulo AC of the $+$. Four rewrite rules are added to make the rewrite

system weakly confluent, that is, if there are one-step reductions from a term P to terms P' and P'', then both P' and P'' can be reduced to a term Q.

The next aim is to prove that the resulting conditional rewrite system is terminating, which means that there are no infinite reductions. In this particular case, deducing termination is a complicated matter, due to the occurrence of a rewrite rule where the left-hand side can be obtained from the right-hand side by the elimination of function symbols. Termination is obtained by means of the advanced technique of semantic labelling from Zantema [24]. Hence, each process term is provably equal to a ground normal form, which cannot be reduced by the conditional rewrite system.

Finally, a painstaking case analysis learns that if two ground normal forms are bisimilar, then they are the same modulo AC of the +. This observation yields the desired completeness result.

In this paper, we presented a completeness proof for $\mathbb{T}(\mathrm{BPA}^*(A))$, based on induction on term structure. This strategy turns out to be much more convenient than the term rewriting analysis sketched above. Moreover, this approach is more general, in the sense that it can be applied to variants of iteration, see for example [3, 2].

4   The Axioms BKS1-3 are Essential for Completeness

Experience learns that axiom systems can contain embarrassing redundancies; see [14] for an example in branching bisimulation. Therefore, we conclude this paper by addressing the issue of the relative independence of the equations for the Kleene star. That is, we show that each of the axioms BKS1-3 for the binary Kleene star is essential for the obtained completeness result.

Theorem 12. *If one of the axioms BKS1-3 is skipped from A1-5+BKS1-3, then this axiomatization is no longer complete for $T(\mathrm{BPA}^*(A))$ modulo bisimulation.*

Proof. We apply a standard technique for proving that an equation e cannot be derived from an equational theory $\mathcal{E}$, which prescribes to define a model for $\mathcal{E}$ in which e is not valid.

In order to show that BKS1 cannot be derived from A1-5+BKS2,3, we define the following interpretation function ϕ of open terms in the natural numbers. It captures the intuition that BKS1 is the only equality that enables to expand the Kleene star. Namely, it does not take into account terms that occur at the right-hand side of a multiplication.

$$\phi(\alpha) = 0$$
$$\phi(x) = 0$$
$$\phi(P + Q) = \max\{\phi(P), \phi(Q)\}$$
$$\phi(P \cdot Q) = \phi(P)$$
$$\phi(P^*Q) = \max\{\phi(P) + 1, \phi(Q) + 1\}$$

It is easy to see that this interpretation is a model for A1-5+BKS2,3. However, $\phi(a(a^*a)+a) = 0$, while $\phi(a^*a) = 1$. Hence, the equality $a(a^*a)+a = a^*a$ cannot be derived from A1-5+BKS2,3.

In order to show that BKS2 cannot be derived from A1-5+BKS1,3, we define the following interpretation function ψ of open terms in the natural numbers.

$$\psi(\alpha) = 0$$
$$\psi(x) = 0$$
$$\psi(P + Q) = \max\{\psi(P), \psi(Q)\}$$
$$\psi(P \cdot Q) = \psi(Q)$$
$$\psi(P^*Q) = \max\{\psi(P) + 1, \psi(Q)\}$$

It is easy to see that this interpretation is a model for A1-5+BKS1,3. However, $\psi((a^*a)a) = \psi(a) = 0$, while $\psi(a^*(aa)) = \max\{\psi(a) + 1, \psi(aa)\} = 1$. Hence, the equality $(a^*a)a = a^*(aa)$ cannot be derived from A1-5+BKS1,3.

In order to show that BKS3 cannot be derived from A1-5+BKS1,2, we define the following interpretation function η of open terms in sets of natural numbers. It captures the intuition that BKS3 is the only equality to change the interpretation at the left-hand side of a Kleene star. Namely, $\eta(P)$ collects the norms of subterms that occur as arguments at the left-hand side of a Kleene star.

$$\eta(\alpha) = \emptyset$$
$$\eta(x) = \emptyset$$
$$\eta(P + Q) = \eta(P) \cup \eta(Q)$$
$$\eta(P \cdot Q) = \eta(P) \cup \eta(Q)$$
$$\eta(P^*Q) = \eta(P) \cup \eta(Q) \cup \{|P|\}$$

It is easy to see that this interpretation is a model for A1-5+BKS1,2. However, $\eta((aa)^*(a((aa + a)^*a) + a)) = \{|aa|, |aa + a|\} = \{1, 2\}$ while $\eta((aa + a)^*a) = \{|aa + a|\} = \{1\}$. Hence, the equality $(aa)^*(a((aa + a)^*a) + a) = (aa + a)^*a$ cannot be derived from A1-5+BKS1,2. □

References

1. L. Aceto. Personal communication, December 1995.
2. L. Aceto and W.J. Fokkink. An equational axiomatization for multi-exit iteration. Report RS-96-22, BRICS, University of Aalborg, 1996.
3. L. Aceto, W.J. Fokkink, R.J. van Glabbeek, and A. Ingólfsdóttir. Axiomatizing prefix iteration with silent steps. Report RS-95-56, BRICS, University of Aalborg, 1995. To appear in *Information and Computation*.
4. J.C.M. Baeten, J.A. Bergstra, and J.W. Klop. Decidability of bisimulation equivalence for processes generating context-free languages. *Journal of the ACM*, 40(3):653–682, 1993.
5. J.C.M. Baeten and C. Verhoef. A congruence theorem for structured operational semantics with predicates. In E. Best, ed., *Proceedings CONCUR'93*, Hildesheim, LNCS 715, pp. 477–492. Springer, 1993.

6. J.C.M. Baeten and C. Verhoef. Concrete process algebra. In S. Abramsky, D.M. Gabbay, and T.S.E. Maibaum, eds., *Handbook of Logic in Computer Science, Volume IV*, pp. 149–268. Oxford University Press, 1995.

7. J.A. Bergstra, I. Bethke, and A. Ponse. Process algebra with iteration and nesting. *The Computer Journal*, 37(4):243–258, 1994.

8. J.A. Bergstra and J.W. Klop. Verification of an alternating bit protocol by means of process algebra. In W. Bibel and K.P. Jantke, eds., *Proceedings Mathematical Methods of Specification and Synthesis of Software Systems*, Wendisch-Rietz, LNCS 215, pp. 9–23. Springer, 1985.

9. D. Caucal. Graphes canoniques de graphes algébriques. *Theoretical Informatics and Applications*, 24(4):339–352, 1990.

10. J.H. Conway. *Regular algebra and finite machines*. Chapman and Hall, 1971.

11. W.J. Fokkink. A complete equational axiomatization for prefix iteration. *Information Processing Letters*, 52(6):333–337, 1994.

12. W.J. Fokkink and R.J. van Glabbeek. Ntyft/ntyxt rules reduce to ntree rules. *Information and Computation*, 126(1):1–10, 1996.

13. W.J. Fokkink and H. Zantema. Basic process algebra with iteration: completeness of its equational axioms. *The Computer Journal*, 37(4):259–267, 1994.

14. R.J. van Glabbeek. A complete axiomatization for branching bisimulation congruence of finite-state behaviours. In A.M. Borzyszkowski and S. Sokołowski, eds., *Proceedings MFCS'93*, Gdansk, LNCS 711, pp. 473–484. Springer, 1993.

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

16. R. Milner. A complete inference system for a class of regular behaviours. *Journal of Computer and System Sciences*, 28:439–466, 1984.

17. R. Milner. A complete axiomatisation for observational congruence of finite-state behaviors. *Information and Computation*, 81(2):227–247, 1989.

18. D.M.R. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, *Proceedings 5th GI Conference*, Karlsruhe, LNCS 104, pp. 167–183. Springer, 1981.

19. G.D. Plotkin. A structural approach to operational semantics. Report DAIMI FN-19, Aarhus University, 1981.

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

21. A. Salomaa. Two complete axiom systems for the algebra of regular events. *Journal of the ACM*, 13(1):158–169, 1966.

22. P. Sewell. Bisimulation is not finitely (first order) equationally axiomatisable. In *Proceedings LICS'94*, Paris, pp. 62–70. IEEE Computer Society Press, 1994.

23. D.R. Troeger. Step bisimulation is pomset equivalence on a parallel language without explicit internal choice. *Mathematical Structures in Computer Science*, 3(1):25–62, 1993.

24. H. Zantema. Termination of term rewriting by semantic labelling. *Fundamenta Informaticae*, 24(1,2):89–105, 1995.