Basic Research in Computer Science

A Finite Equational Base for CCS with Left Merge and Communication Merge

Luca Aceto
Willem Jan Fokkink
Anna Ingólfsdóttir
Bas Luttik

BRICS Report Series **RS-06-6**

ISSN 0909-0878 **March 2006**

**See back inner page for a list of recent BRICS Report Series publications.
Copies may be obtained by contacting:**

**BRICS
Department of Computer Science
University of Aarhus
IT-parken, Aabogade 34
DK–8200 Aarhus N
Denmark**

**Telephone: +45 8942 9300
Telefax: +45 8942 5601
Internet: BRICS@brics.dk**

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/06/6/`

A finite equational base for CCS with left merge and communication merge

Luca Aceto[1,4], Wan Fokkink[2,5], Anna Ingolfsdottir[1,4], and Bas Luttik[3,5]

[1] Department of Computer Science, Reykjavík University, Iceland, luca@ru.is,annai@ru.is
[2] Department of Computer Science, Vrije Universiteit Amsterdam, The Netherlands, wanf@cs.vu.nl
[3] Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, The Netherlands, s.p.luttik@tue.nl
[4] **BRICS**, Department of Computer Science, Aalborg University, Denmark
[5] Department of Software Engineering, CWI, The Netherlands

Abstract. Using the left merge and communication merge from ACP, we present an equational base for the fragment of CCS without restriction and relabelling. Our equational base is finite if the set of actions is finite.

1 Introduction

One of the first detailed studies of the equational theory of a process algebra was performed by Hennessy and Milner [9]. They considered the equational theory of the process algebra that arises from the recursion-free fragment of CCS (see [11]), and presented a set of equational axioms that is complete in the sense that all valid *closed* equations (i.e., equations in which no variables occur) are derivable from it in equational logic [15]. For the elimination of parallel composition from closed terms, Hennessy and Milner proposed the well-known *Expansion Law*, an axiom schema that generates infinitely many axioms. Thus, the question arose whether a finite complete set of axioms exists. With their axiom system ACP, Bergstra and Klop demonstrated in [3] that it does exist if two auxiliary operators are used: the left merge and the communication merge. It was later proved by Moller [13] that without using at least one auxiliary operator a finite complete set of axioms does not exist.

The aforementioned results pertain to the closed fragments of the equational theories discussed, i.e., to the subsets consisting of the closed valid equations only. Many valid equations such as, e.g., the equation $(x \parallel y) \parallel z \approx x \parallel (y \parallel z)$ expressing that parallel composition is associative, are not derivable (by means of equational logic) from the axioms in [3] or [9]. In this paper we shall not neglect the variables and contribute to the study of full equational theories of process algebras. We take the fragment of CCS without recursion, restriction and relabelling, and consider the full equational theory of the process algebra that is obtained by taking the syntax modulo bisimilarity [14]. Our goal is then to present an *equational base* (i.e., a set of valid equations from which every other valid equation can be derived) for it, which is finite if the set of actions is finite. Obviously, Moller's result about the unavoidability of the use of auxiliary operations in a finite complete axiomatisation of the closed fragment of the equational theory of CCS a fortiori implies that auxiliary operations

are needed to achieve our goal. So we add left merge and communication merge from the start.

Moller [12] considers the equational theory of the same fragment of CCS, except that his parallel operator implements pure interleaving instead of CCS-communication and the communication merge is omitted. He presents a set of valid axiom schemata and proves that it generates an equational base if the set of actions is infinite. Groote [6] does consider the fragment including communication merge, but, instead of the CCS-communication mechanism, he assumes an uninterpreted communication function. His axiom schemata also generate an equational base provided that the set of actions is infinite. We improve on these results by considering the communication mechanism present in CCS, and by proving that our axiom schemata generate an equational base also if the set of actions is finite. Moreover, our axiom schemata generate a finite equational base if the set of actions is finite.

Our equational base consists of axioms that are mostly well-known. For parallel composition ($\|$), left merge ($\between$) and communication merge ($|$) we adapt the axioms of ACP, adding from Bergstra and Tucker [4] a selection of the axioms for *standard concurrency* and the axiom $(x \mid y) \mid z \approx \mathbf{0}$, which expresses that the communication mechanism is a form of *handshaking communication*.

Our proof follows the classic two-step approach: first identify a set of normal forms such that every process term has a provably equal normal form, and then demonstrate that for distinct normal forms there is a distinguishing valuation that proves that they should not be equated. (We refer to the survey [2] for a discussion of proof techniques and an overview of results and open problems in the area. We remark in passing that one of our main results in this paper, viz. Corollary 34, solves the open problem mentioned in [2, p. 362].) Since both associating a normal form with a process term and determining a distinguishing valuation for two distinct normal forms are easily seen to be computable, as a corollary to our proof we get the decidability of the equational theory. Another consequence of our result is that our equational base is complete for the set of valid closed equations as well as ω-complete [7].

The positive result that we obtain in Corollary 34 of this paper stands in contrast with the negative result that we have obtained in [1]. In that article we proved that there does not exist a finite equational base for CCS if the auxiliary operation $\between$ of Hennessy [8] is added instead of Bergstra and Klop's left merge and communication merge. Furthermore, we conjecture that a finite equational base fails to exist if the unary action prefixes are replaced by binary sequential composition. (We refer to [2] for an infinite family of valid equations that we believe cannot all be derivable from a single finite set of valid equations.)

The paper is organised as follows. In Sect. 2 we introduce a class of algebras of processes arising from a process calculus à la CCS, present a set of equations that is valid in all of them, and establish a few general properties needed in the remainder of the paper. Our class of process algebras is parametrised by a communication function. It is beneficial to proceed in this generality, because it allows us to first consider the simpler case of a process algebra with pure interleaving (i.e., no communication at all) instead of CCS-like parallel composition. In Sect. 3 we prove

that an equational base for the process algebra with pure interleaving is obtained by simply adding the axiom $x \mid y \approx \mathbf{0}$ to the set of equations introduced in Sect. 2. The proof in Sect. 3 extends nicely to a proof that for the more complicated case of CCS-communication it is enough to replace $x \mid y \approx \mathbf{0}$ by $x \mid (y \mid z) \approx \mathbf{0}$; this is discussed in Sect. 4.

2 Algebras of processes

We fix a set $\mathcal{A}$ of *actions*, and declare a special action τ that we assume is not in $\mathcal{A}$. We denote by $\mathcal{A}_\tau$ the set $\mathcal{A} \cup \{\tau\}$. Generally, we let a and b range over $\mathcal{A}$ and α over $\mathcal{A}_\tau$. We also fix a countably infinite set $\mathcal{V}$ of *variables*. The set $\mathcal{P}$ of *process terms* is generated by the following grammar:

$$P ::= \; x \;\mid\; \mathbf{0} \;\mid\; \alpha.P \;\mid\; P + P \;\mid\; P \between P \;\mid\; P \mid P \;\mid\; P \parallel P \;,$$

with $x \in \mathcal{V}$, and $\alpha \in \mathcal{A}_\tau$. We shall frequently simply write α instead of $\alpha.\mathbf{0}$. Furthermore, to be able to omit some parentheses when writing terms, we adopt the convention that $\alpha.$ binds stronger, and $+$ binds weaker, than all the other operations.

Table 1. The operational semantics.

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

$$\frac{P \xrightarrow{\alpha} P'}{P \between Q \xrightarrow{\alpha} P' \parallel Q} \qquad \frac{P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q} \qquad \frac{Q \xrightarrow{\alpha} Q'}{P \parallel Q \xrightarrow{\alpha} P \parallel Q'}$$

$$\frac{P \xrightarrow{a} P',\ Q \xrightarrow{b} Q',\ \gamma(a,b)\!\downarrow}{P \mid Q \xrightarrow{\gamma(a,b)} P' \parallel Q'} \qquad \frac{P \xrightarrow{a} P',\ Q \xrightarrow{b} Q',\ \gamma(a,b)\!\downarrow}{P \parallel Q \xrightarrow{\gamma(a,b)} P' \parallel Q'}$$

A process term is *closed* if it does not contain variables; we denote the set of all closed process terms by $\mathcal{P}_0$. We define on $\mathcal{P}_0$ binary relations $\xrightarrow{\alpha}$ ($\alpha \in \mathcal{A}_\tau$) by means of the transition system specification in Table 1. The last two rules in Table 1 refer to a *communication function* γ, i.e., a commutative and associative partial binary function $\gamma : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}_\tau$. We shall abbreviate the statement '$\gamma(a,b)$ is defined' by $\gamma(a,b)\!\downarrow$ and the statement '$\gamma(a,b)$ is undefined' by $\gamma(a,b)\!\uparrow$. In the remainder of this paper we shall in particular consider the following communication functions:

1. The *trivial communication function* is the partial function $f : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}_\tau$ such that $f(a,b)\!\uparrow$ for all $a, b \in \mathcal{A}$.
2. The CCS *communication function* $h : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}_\tau$ presupposes a bijection $\bar{\cdot}$ on $\mathcal{A}$ such that $\overline{\overline{a}} = a$ and $\overline{a} \neq a$ for all $a \in \mathcal{A}$, and is then defined by $h(a,b) = \tau$ if $\overline{a} = b$ and undefined otherwise.

Definition 1. A *bisimulation* is a symmetric binary relation $\mathcal{R}$ on $\mathcal{P}_0$ such that $P\ \mathcal{R}\ Q$ implies

$$\text{if } P \xrightarrow{\alpha} P', \text{ then there exists } Q' \in \mathcal{P}_0 \text{ such that } Q \xrightarrow{\alpha} Q' \text{ and } P'\ \mathcal{R}\ Q'. \tag{1}$$

Closed process terms $P, Q \in \mathcal{P}_0$ are said to be *bisimilar* (notation: $P \leftrightarrows_\gamma Q$) if there exists a bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.

The relation $\leftrightarrows_\gamma$ is an equivalence relation on $\mathcal{P}_0$; we denote the equivalence class containing P by $[P]$, i.e.,

$$[P] = \{Q \in \mathcal{P}_0 : P \leftrightarrows_\gamma Q\}\ .$$

The rules in Table 1 are all in de Simone's format [5] if P, P', Q and Q' are treated as variables ranging over closed process terms, and if the last two rules are treated as rule schemata generating a rule for every a, b such that $\gamma(a,b)\downarrow$. Hence, $\leftrightarrows_\gamma$ has the substitution property for the syntactic constructs of our language of closed process terms, and therefore the constructs induce an algebraic structure on $\mathcal{P}_0/\leftrightarrows_\gamma$, with a constant $\mathbf{0}$, unary operations $\alpha.\ (\alpha \in \mathcal{A}_\tau)$ and four binary operations $+$, $\between$, $|$ and $\|$ defined by

$$\begin{array}{ll} \mathbf{0} = [\mathbf{0}] & [P] \between [Q] = [P \between Q] \\ \alpha.[P] = [\alpha.P] & [P] \mid [Q] = [P \mid Q] \\ [P] + [Q] = [P + Q] & [P] \| [Q] = [P \| Q]\ . \end{array}$$

Henceforth, we denote by $\mathbf{P}_\gamma$ (for γ an arbitrary communication function) the algebra obtained by dividing out $\leftrightarrows_\gamma$ on $\mathcal{P}_0$ with constant $\mathbf{0}$ and operations $\alpha.\ (\alpha \in \mathcal{A}_\tau)$, $+$, $\between$, $|$, and $\|$ as defined above. The elements of $\mathbf{P}_\gamma$ are called *processes*, and will be ranged over by p, q and r.

2.1 Equational reasoning

We can use the full language of process expressions to reason about the elements of $\mathbf{P}_\gamma$. A *valuation* is a mapping $\nu : \mathcal{V} \to \mathbf{P}_\gamma$; it induces an *evaluation mapping*

$$[\![\_]\!]_\nu : \mathcal{P} \to \mathbf{P}_\gamma$$

inductively defined by

$$\begin{array}{ll} [\![x]\!]_\nu = \nu(x) & [\![P \between Q]\!]_\nu = [\![P]\!]_\nu \between [\![Q]\!]_\nu \\ [\![\mathbf{0}]\!]_\nu = \mathbf{0} & [\![P \mid Q]\!]_\nu = [\![P]\!]_\nu \mid [\![Q]\!]_\nu \\ [\![\alpha.P]\!]_\nu = \alpha.[\![P]\!]_\nu & [\![P \| Q]\!]_\nu = [\![P]\!]_\nu \| [\![Q]\!]_\nu \\ [\![P + Q]\!]_\nu = [\![P]\!]_\nu + [\![Q]\!]_\nu. & \end{array}$$

A *process equation* is a formula $P \approx Q$ with P and Q process terms; it is said to be *valid* (in $\mathbf{P}_\gamma$) if $[\![P]\!]_\nu = [\![Q]\!]_\nu$ for all $\nu : \mathcal{V} \to \mathbf{P}_\gamma$. If $P \approx Q$ is valid in $\mathbf{P}_\gamma$, then

we shall also write $P \leftrightarrows_\gamma Q$. The *equational theory* of the algebra $\mathbf{P}_\gamma$ is the set of all valid process equations, i.e.,

$$EqTh(\mathbf{P}_\gamma) = \{P \approx Q : [\![P]\!]_\nu = [\![Q]\!]_\nu \text{ for all } \nu : \mathcal{V} \to \mathbf{P}_\gamma\} \ .$$

The precise contents of the set $EqTh(\mathbf{P}_\gamma)$ depend to some extent on the choice of γ. For instance, the process equation $x \mid y \approx \mathbf{0}$ is only valid in $\mathbf{P}_\gamma$ if γ is the trivial communication function f; if γ is the CCS communication function h, then $\mathbf{P}_\gamma$ satisfies the weaker equation $x \mid (y \mid z) \approx \mathbf{0}$.

Table 2. Process equations valid in every $\mathbf{P}_\gamma$.

A1	$x + y$	$\approx y + x$	C1	$\mathbf{0} \mid x$	$\approx \mathbf{0}$	
A2	$(x + y) + z$	$\approx x + (y + z)$	C2	$a.x \mid b.y$	$\approx \gamma(a,b).(x \parallel y)$	if $\gamma(a,b)\downarrow$
A3	$x + x$	$\approx x$	C3	$a.x \mid b.y$	$\approx \mathbf{0}$	if $\gamma(a,b)\uparrow$
A4	$x + \mathbf{0}$	$\approx x$	C4	$(x + y) \mid z$	$\approx x \mid z + y \mid z$	
			C5	$x \mid y$	$\approx y \mid x$	
L1	$\mathbf{0} \between x$	$\approx \mathbf{0}$	C6	$(x \mid y) \mid z$	$\approx x \mid (y \mid z)$	
L2	$\alpha.x \between y$	$\approx \alpha.(x \parallel y)$	C7	$(x \between y) \mid z$	$\approx (x \mid z) \between y$	
L3	$(x + y) \between z$	$\approx x \between z + y \between z$				
L4	$(x \between y) \between z$	$\approx x \between (y \parallel z)$	P1	$x \parallel y$	$\approx (x \between y + y \between x) + x \mid y$	
L5	$x \between \mathbf{0}$	$\approx x$				

Table 2 lists process equations that are valid in $\mathbf{P}_\gamma$ independently of the choice of γ. (The equations L2, C2 and C3 are actually axiom schemata; they generate an axiom for all $a, b \in \mathcal{A}$. Note that if $\mathcal{A}$ is finite, then these axiom schemata generate finitely many axioms.) Henceforth whenever we write an equation $P \approx Q$, we shall mean that it is derivable from the axioms in Table 2 by means of equational logic. It is well-known that the rules of equational logic preserve validity. We therefore obtain the following result.

Proposition 2. For all process terms P and Q, if $P \approx Q$, then $P \leftrightarrows_\gamma Q$.

In the following lemma we give an example of a valid equation that can be derived from Table 2 using the rules of equational logic.

Lemma 3. The following equation is derivable from the axioms in Table 2:

C8 $\quad (x \between y) \mid (z \between u) \approx (x \mid z) \between (y \parallel u)$.

Proof. The lemma is proved with the derivation:

$$\begin{aligned}
(x \between y) \mid (z \between u) &\approx (z \between u) \mid (x \between y) && \text{(by C5)}\\
&\approx (z \mid (x \between y)) \between u && \text{(by C7)}\\
&\approx ((x \between y) \mid z) \between u && \text{(by C5)}\\
&\approx ((x \mid z) \between y) \between u && \text{(by C7)}\\
&\approx (x \mid z) \between (y \parallel u) && \text{(by L4).}
\end{aligned}$$

□

A set of valid process equations is an *equational base* for $\mathbf{P}_\gamma$ if all other valid process equations are derivable from it by means of equational logic. Clearly, $\mathbf{P}_\gamma$ has $EqTh(\mathbf{P}_\gamma)$ as an equational base, but it is infinite, and offers little insight into the nature of the equations valid in $\mathbf{P}_\gamma$. The purpose of this paper is to prove that if we add to the equations in Table 2 the equation $x \mid y \approx \mathbf{0}$ we obtain an equational base for $\mathbf{P}_f$, and if, instead, we add $x \mid (y \mid z) \approx \mathbf{0}$ we obtain an equational base for $\mathbf{P}_h$. Both these equational bases are finite, if the set of actions $\mathcal{A}$ is finite.

Definition 4. Let P be a process term. We define the *height* of a process term P, denoted $h(P)$, inductively as follows:

$$\begin{array}{ll} h(\mathbf{0}) = 0 \ , & h(P \between Q) = h(P) + h(Q) \ , \\ h(x) = 1 \ , & h(P \mid Q) = h(P) + h(Q) \ , \\ h(\alpha.P) = h(P) + 1 \ , & h(P \parallel Q) = h(P) + h(Q) \ , \\ h(P + Q) = \max(h(P), h(Q)) \ . & \end{array}$$

Definition 5. We call a process term *simple* if it is not $\mathbf{0}$ and not an alternative composition.

Lemma 6. For every process term P there exists a sequence of simple process terms $S_1, \ldots, S_n$ $(n \geq 0)$ such that $h(P) \geq h(S_i)$ for all $i = 1, \ldots, n$ and

$$P \approx \sum_{i=1}^{n} S_i \qquad \text{(by A1, A2 and A4).}$$

We postulate that the summation of an empty sequence of terms denotes $\mathbf{0}$. The terms S_i will be called *syntactic summands* of P.

2.2 General properties of $\mathbf{P}_\gamma$

We collect some general properties of the algebras $\mathbf{P}_\gamma$ that we shall need in the remainder of the paper.

The binary transition relations $\xrightarrow{\alpha}$ $(\alpha \in \mathcal{A}_\tau)$ on $\mathcal{P}_0$, which were used to associate an operational semantics with closed process terms, will play an important rôle in the remainder of the paper. They induce binary relations on $\mathbf{P}_\gamma$, also denoted by $\xrightarrow{\alpha}$, and defined as the least relations such that $P \xrightarrow{\alpha} P'$ implies $[P] \xrightarrow{\alpha} [P']$. Note that we then get, directly from the definition of bisimulation, that for all $P, P' \in \mathcal{P}_0$:

$[P] \xrightarrow{\alpha} [P']$ iff for all $Q \in [P]$ there exists $Q' \in [P']$ such that $Q \xrightarrow{\alpha} Q'$.

Proposition 7. For all $p, q, r \in \mathbf{P}_\gamma$:

(a) $p = \mathbf{0}$ iff there do not exist $p' \in \mathbf{P}_\gamma$ and $\alpha \in \mathcal{A}_\tau$ such that $p \xrightarrow{\alpha} p'$;
(b) $\alpha.p \xrightarrow{\beta} r$ iff $\alpha = \beta$ and $r = p$;
(c) $p + q \xrightarrow{\alpha} r$ iff $p \xrightarrow{\alpha} r$ or $q \xrightarrow{\alpha} r$;
(d) $p \between q \xrightarrow{\alpha} r$ iff there exists $p' \in \mathbf{P}_\gamma$ such that $p \xrightarrow{\alpha} p'$ and $r = p' \parallel q$; and
(e) $p \mid q \xrightarrow{\alpha} r$ iff there exist actions $a, b \in \mathcal{A}$ and processes $p', q' \in \mathbf{P}_\gamma$ such that $\alpha = \gamma(a, b)$, $p \xrightarrow{a} p'$, $q \xrightarrow{b} q'$, and $r = p' \parallel q'$; and

(f) $p \parallel q \xrightarrow{\alpha} r$ iff $p \between q \xrightarrow{\alpha} r$ or $q \between p \xrightarrow{\alpha} r$ or $p \mid q \xrightarrow{\alpha} r$.

Let $p, p' \in \mathbf{P}_\gamma$; we write $p \to p'$ if $p \xrightarrow{\alpha} p'$ for some $\alpha \in \mathcal{A}_\tau$. We denote by $\to^*$ the reflexive-transitive closure of $\to$. If p and p' are processes such that $p \to p'$, then we call p' a *residual* of p.

It is easy to see from Table 1 that if $P \xrightarrow{\alpha} P'$, then P' has fewer symbols than P. Consequently, the length of a transition sequence starting with a process $[P]$ is bounded from above by the number of symbols in P.

Definition 8. The *depth* $|p|$ of an element $p \in \mathbf{P}_\gamma$ is defined as

$$|p| = \max\{n \geq 0 : \ \exists p_n, \ldots, p_0 \in \mathbf{P}_\gamma \text{ s.t. } p = p_n \to \cdots \to p_0\}.$$

The *branching degree* $bdeg(p)$ of an element $p \in \mathbf{P}_\gamma$ is defined as

$$bdeg(p) = |\{(\alpha, p') : p \xrightarrow{\alpha} p'\}| \ .$$

For the remainder of this section, we focus on properties of parallel composition on $\mathbf{P}_\gamma$. The depth of a parallel composition is the sum of the depths of its components.

Lemma 9. For all $p, q \in \mathbf{P}_\gamma$, $|p \parallel q| = |p| + |q|$.

Proof. If $p = p_m \to \cdots \to p_0$ and $q = q_n \to \cdots \to q_0$, then

$$p \parallel q = p_m \parallel q \to \cdots \to p_0 \parallel q = p_0 \parallel q_n \to \cdots \to p_0 \parallel q_0 \ ,$$

so clearly $|p \parallel q| \geq |p| + |q|$.

It remains to prove that $|p| + |q| \geq |p \parallel q|$. We proceed by induction on the depth of $p \parallel q$. If $|p \parallel q| = 0$, then $(p \parallel q)\not\to$, so $p\not\to$ and $q\not\to$; hence $|p| = 0$ and $|q| = 0$, and it follows that $|p \parallel q| = |p| + |q|$. Suppose that $|p \parallel q| = n + 1$. Then there exist $r_{n+1}, \ldots, r_0 \in \mathbf{P}_\gamma$ such that

$$p \parallel q = r_{n+1} \to r_n \to \cdots \to r_0 \ .$$

Note that $|r_i| = i$ for all $0 \leq i \leq n + 1$. Further note that the transition $r_{n+1} \to r_n$ cannot be the result $r_{n+1} \xrightarrow{\gamma(a,b)} r_n$ of communication between a transition $p \xrightarrow{a} p'$ and a transition $q \xrightarrow{b} q'$; for then there would exist a longer transition sequence from $p \parallel q$, obtained by replacing the single transition $r_{n+1} \to r_n$ by two transitions $r_{n+1} = p \parallel q \to p' \parallel q \to p' \parallel q' = r_n$, contradicting our assumption that $|p \parallel q| = n + 1$. Hence, either $r_n = p' \parallel q$ with $p \to p'$, or $r_n = p \parallel q'$ with $q \to q'$. In the first case it follows by the induction hypothesis that $|p'| + |q| \geq |p' \parallel q| = n$, so $|p| + |q| \geq |p'| + |q| + 1 \geq n + 1 = |p \parallel q|$. In the second case the proof is similar. □

According to the following lemma and Proposition 2, $\mathbf{P}_\gamma$ is a commutative monoid with respect to $\parallel$, with $\mathbf{0}$ as the identity element.

Lemma 10. The following equations are derivable from the axioms in Table 2:

P2	$(x \parallel y) \parallel z$	$\approx x \parallel (y \parallel z)$
P3	$x \parallel y$	$\approx y \parallel x$
P4	$x \parallel \mathbf{0}$	$\approx x$.

An element $p \in \mathbf{P}_\gamma$ is *parallel prime* if $p \neq \mathbf{0}$, and $p = q \parallel r$ implies $q = \mathbf{0}$ or $r = \mathbf{0}$. Suppose that p is an arbitrary element of $\mathbf{P}_\gamma$; a *parallel decomposition* of p is a finite multiset $[p_1, \ldots, p_n]$ of parallel primes such that $p = p_1 \parallel \cdots \parallel p_n$. (The process $\mathbf{0}$ has as decomposition the empty multiset, and a parallel prime process p has as decomposition the singleton multiset $[p]$.) The following theorem is a straightforward consequence of the main result in [10].

Theorem 11. Every element of $\mathbf{P}_\gamma$ has a unique parallel decomposition.

Proof. In a similar way as in [10, Sect. 4] it can be established that the inverse of $\rightarrow^*$ is a decomposition order on the commutative monoid $\mathbf{P}_\gamma$ with respect to parallel composition; it then follows from [10, Theorem 32] that this commutative monoid has unique decomposition. □

The following corollary is a straightforward consequence of the above unique decomposition result.

Corollary 12 (Cancellation). Let $p, q, r \in \mathbf{P}_\gamma$. If $p \parallel q = p \parallel r$, then $q = r$.

The branching degree of a parallel composition is at least the branching degree of its components.

Lemma 13. For all $p, q \in \mathbf{P}_\gamma$, $bdeg(p \parallel q) \geq bdeg(p), bdeg(q)$.

Proof. First we prove that $bdeg(p \parallel q) \geq bdeg(q)$. By Proposition 7, if $q \xrightarrow{\alpha} q'$, then $p \parallel q \xrightarrow{\alpha} p \parallel q'$. Suppose that q_1 and q_2 are distinct processes such that $q \xrightarrow{\alpha} q_1$ and $q \xrightarrow{\alpha} q_2$. Then $p \parallel q \xrightarrow{\alpha} p \parallel q_1$ and $p \parallel q \xrightarrow{\alpha} p \parallel q_2$. Since $p \parallel q_1 = p \parallel q_2$ would imply $q_1 = q_2$ by Corollary 12, it follows that $p \parallel q'$ and $p \parallel q''$ are distinct. Hence $bdeg(p \parallel q) \geq bdeg(q)$.

By commutativity of $\parallel$, it also follows that $bdeg(p \parallel q) \geq bdeg(p)$. □

We define a sequence of parallel prime processes with special properties that make them very suitable as tools in our proofs in the remainder of the paper:

$$\varphi_i = \tau.\mathbf{0} + \cdots + \tau^i.\mathbf{0} \qquad (i \geq 1) \tag{2}$$

(with $\tau^i.\mathbf{0}$ recursively defined by $\tau^i.\mathbf{0} = \mathbf{0}$ if $i = 0$, and $\tau.\tau^{i-1}.\mathbf{0}$ if $i > 0$).

Lemma 14. (i) For all $i \geq 1$, the processes φ_i are parallel prime.
(ii) The processes φ_i are all distinct, i.e., $\varphi_k = \varphi_l$ implies that $k = l$.
(iii) For all $i \geq 1$, the process φ_i has branching degree i.

Proof. (i) Clearly $\varphi_i \neq \mathbf{0}$. Suppose $\varphi_i = p \parallel q$; to prove that φ_i is parallel prime, we need to establish that either $p = \mathbf{0}$ or $q = \mathbf{0}$. Note that $p \parallel q \xrightarrow{\tau} \mathbf{0}$. There do not exist actions a and b and processes p' and q' such that $\gamma(a, b) = \tau$ and $p' \parallel q'$, for then also $p \parallel q \xrightarrow{a} p' \parallel q$, quod non. Therefore, according to Proposition 7, there are only two cases to consider:

(a) If there exists p' such that $p \xrightarrow{\tau} p'$ and $p' \parallel q = \mathbf{0}$, then it follows by Lemma 9 that $|q| = 0$, and hence $q = \mathbf{0}$.

(b) If there exists q' such that $q \xrightarrow{\tau} q'$ and $p \parallel q' = \mathbf{0}$, then it follows by Lemma 9 that $|p| = 0$, and hence $p = \mathbf{0}$.

(ii) If $\varphi_k = \varphi_l$, then $k = |\varphi_k| = |\varphi_l| = l$.

(iii) On the one hand, $\varphi_i \xrightarrow{\tau} \tau^j.\mathbf{0}$ for all $0 \leq j < i$ and $\tau^k.\mathbf{0} = \tau^l.\mathbf{0}$ implies $k = l$ for all $0 \leq k, l < i$, so $bdeg(\varphi_i)$ is at least i. On the other hand, if $\varphi_i \xrightarrow{\alpha} p$, then $\alpha = \tau$ and $p = \tau^j.\mathbf{0}$ for some $0 \leq j < i$, so $bdeg(\varphi_i)$ is at most i. □

3 An equational base for $\mathbf{P}_f$

In this section, we prove that an equational base for $\mathbf{P}_f$ is obtained if we add the axiom

$$\text{F} \quad x \mid y \;\approx\; \mathbf{0}$$

to the set of axioms generated by the axiom schemata in Table 2. The resulting equational base is finite if $\mathcal{A}$ is finite.

Henceforth, whenever we write $P \approx_{\text{F}} Q$, we shall mean that the equation $P \approx Q$ is derivable from the axioms in Table 2 and the axiom F.

Proposition 15. For all process terms P and Q, if $P \approx_{\text{F}} Q$, then $P \leftrightarrows_f Q$.

To prove that adding F to the axioms in Table 2 suffices to obtain an equational base for $\mathbf{P}_f$, we need to establish that $P \leftrightarrows_f Q$ implies $P \approx_{\text{F}} Q$ for all process terms P and Q. We adopt the classic two step approach [2]:

1. In the first step we identify a set of normal forms $\mathcal{N}_{\text{F}}$, and prove that every process term P can be rewritten to a normal form by means of the axioms.
2. In the second step we prove that bisimilar normal forms are identical modulo applications of the axioms A1–A4. This is done by associating with every pair of normal forms a so-called distinguishing valuation, i.e., a valuation that proves that the normal forms are not bisimilar unless they are provably equal modulo the axioms A1–A4.

Definition 16. The set $\mathcal{N}_{\text{F}}$ of F-*normal forms* is generated by the following grammar:

$$N \;::=\; \mathbf{0} \;\mid\; N + N \;\mid\; \alpha.N \;\mid\; x \mathbin{\underline{\parallel}} N \;,$$

with $x \in \mathcal{V}$, and $\alpha \in \mathcal{A}_\tau$.

Note that the set of simple F-normal forms (see Definition 5) is generated by the grammar

$$S \ ::= \ \alpha.N \ \mid \ x \between N \ ,$$

with $x \in \mathcal{V}$, $\alpha \in \mathcal{A}_\tau$, and $N \in \mathcal{N}_{\mathrm{F}}$.

Lemma 17. For every process term P there is an F-normal form N such that $P \approx_{\mathrm{F}} N$ and $h(P) \geq h(N)$.

Proof. Recall that $h(P)$ denotes the height of P (see Definition 4). In this proof we also use another syntactic measure on P: the *length* of P, denoted $\ell(P)$, is the number of symbols occurring in P. Define a partial order $\prec$ on process terms by $P \prec Q$ if the pair $(h(P), \ell(P))$ is less than the pair $(h(Q), \ell(Q))$ in the lexicographical order on $\omega \times \omega$; i.e., $P \prec Q$ if $h(P) < h(Q)$ or $h(P) = h(Q)$ and $\ell(P) < \ell(Q)$. It is well-known that the lexicographical order on $\omega \times \omega$, and hence the order $\prec$ on process terms, is well-founded; so we may use $\prec$-induction.

The remainder of the proof consists of a case distinction on the syntactic forms that P may take.

1. If P is a variable, say $P = x$, then $P \approx x \between \mathbf{0}$ by L5; the process term $x \between \mathbf{0}$ is an F-normal form and $h(P) = h(x) = h(x) + 0 = h(x \between \mathbf{0})$.
2. If $P = \mathbf{0}$, then P is an F-normal form.
3. If $P = \alpha.P'$, then, since $h(P') < h(P)$, it holds that $P' \prec P$, and hence by the induction hypothesis there exists an F-normal form N such that $P' \approx_{\mathrm{F}} N$ and $h(P') \geq h(N)$. Then $\alpha.N$ is an F-normal form such that $P \approx_{\mathrm{F}} \alpha.N$ and $h(P) \geq h(\alpha.N)$.
4. If $P = P_1 + P_2$, then, since $h(P_1), h(P_2) \leq h(P)$ and $\ell(P_1), \ell(P_2) < \ell(P)$, it holds that $P_1, P_2 \prec P$, and hence by the induction hypothesis there exist F-normal forms N_1 and N_2 such that $P_1 \approx_{\mathrm{F}} N_1$, $P_2 \approx_{\mathrm{F}} N_2$, $h(P_1) \geq h(N_1)$ and $h(P_2) \geq h(N_2)$. Then $N_1 + N_2$ is an F-normal form such that $P \approx_{\mathrm{F}} N_1 + N_2$ and $h(P) \geq h(N_1 + N_2)$.
5. If $P = Q \between R$, then, since $h(Q) \leq h(P)$ and $\ell(Q) < \ell(P)$, it holds that $Q \prec P$, and hence by the induction hypothesis and Lemma 6 there exists a sequence $S_1, \ldots, S_n$ of simple F-normal forms such that $Q \approx_{\mathrm{F}} \sum_{i=1}^{n} S_i$ and $h(Q) \geq h(S_i)$ for all $i = 1, \ldots, n$. If $n = 0$, then $P \approx_{\mathrm{F}} \mathbf{0} \between R \approx \mathbf{0}$ by L1, and clearly $h(P) \geq h(\mathbf{0})$. Otherwise, by L3

   $$P \approx_{\mathrm{F}} \sum_{i=1}^{n} (S_i \between R) \ .$$

   So it remains to show, for all $i = 1, \ldots, n$, that $S_i \between R$ is provably equal to an appropriate F-normal form. We distinguish cases according to the syntactic form of S_i:

   (a) If $S_i = \alpha.N_i'$, with N_i' an F-normal form, then by L2

   $$S_i \between R \approx \alpha.(N_i' \parallel R) \ .$$

Since $h(N_i') < h(S_i) \leq h(Q)$, it holds that $N_i' \parallel R \prec P$ and hence by the induction hypothesis there exists an F-normal form N_i such that $N_i' \parallel R \approx_{\mathrm{F}} N_i$ and $h(N_i' \parallel R) \geq h(N_i)$. Clearly, $\alpha.N_i$ is an F-normal form such that $S_i \between R \approx_{\mathrm{F}} \alpha.N_i$ and $h(S_i \between R) \geq h(\alpha.N_i)$.

(b) If $S_i = x \between N_i'$, with N_i' an F-normal form, then by L4

$$(x \between N_i') \between R \approx x \between (N_i' \parallel R) \ .$$

Note that $h(x) = 1$, so $h(N_i') < h(S_i) \leq h(Q)$. It follows that $N_i' \parallel R \prec P$, and hence by the induction hypothesis there exists an F-normal form N_i such that $N_i' \parallel R \approx_{\mathrm{F}} N_i$ and $h(N_i' \parallel R) \geq h(N_i)$. Clearly, $x \between N_i$ is an F-normal form such that $S_i \between R \approx_{\mathrm{F}} x \between N_i$ and $h(S_i \between R) \geq h(x \between N_i)$.

6. If $P = Q \mid R$, then $P \approx_{\mathrm{F}} \mathbf{0}$ according to the axiom F and clearly $h(P) \geq h(\mathbf{0})$.
7. If $P = Q \parallel R$, then $P \approx (Q \between R + R \between Q) + Q \mid R \approx_{\mathrm{F}} Q \between R + R \between Q$ by the axioms P1, F and A4. We can now proceed as in case 5 to show that for $Q \between R$ and $R \between Q$ there exist F-normal forms N_1 and N_2, respectively, such that $Q \between R \approx_{\mathrm{F}} N_1$, $R \between Q \approx_{\mathrm{F}} N_2$, $h(Q \between R) \geq h(N_1)$ and $h(R \between Q) \geq h(N_2)$. Then $N_1 + N_2$ is an F-normal form such that $P \approx_{\mathrm{F}} N_1 + N_2$ and $h(P) \geq h(N_1 + N_2)$. □

It remains to prove that for every two F-normal forms N_1 and N_2 there exists a *distinguishing valuation*, i.e., a valuation $*$ such that if N_1 and N_2 are *not* provably equal, then the $*$-interpretations of N_1 and N_2 are distinct. Stating it contrapositively, for every two F-normal forms N_1 and N_2, it suffices to establish the existence of a valuation $* : \mathcal{V} \to \mathbf{P}_\gamma$ such that

$$\text{if } [\![N_1]\!]_* = [\![N_2]\!]_*, \text{ then } N_1 \approx_{\mathrm{F}} N_2. \tag{3}$$

The valuation $* : \mathcal{V} \to \mathbf{P}_f$ that we are going to define below will depend on N_1 and N_2. The idea is that $*$ assigns processes to variables in such a way that much of the original syntactic structure of N_1 and N_2 can be recovered by analysing the behaviour of $[\![N_1]\!]_*$ and $[\![N_2]\!]_*$. To recognize variables, we shall use the special processes φ_i ($i \geq 1$) defined in Eqn. (2) on p. 8. Recall that the processes φ_i have branching degree i. We are going to assign to every variable a distinct process φ_i. By choosing i larger than the maximal 'branching degrees' occurring in N_1 and N_2, the behaviour contributed by an instantiated variable is distinguished from behaviour already present in the F-normal forms themselves.

Definition 18. We define the *width* $w(N)$ of an F-normal form N as follows:

(i) if $N = \mathbf{0}$, then $w(N) = 0$;
(ii) if $N = N_1 + N_2$, then $w(N) = w(N_1) + w(N_2)$;
(iii) if $N = \alpha.N'$, then $w(N) = \max(w(N'), 1)$;
(iv) if $N = x \between N'$, then $w(N) = \max(w(N'), 1)$.

We now fix a natural number W and use it to define a valuation $*$ that satisfies Eqn. (3) for all F-normal forms N_1 and N_2 such that $w(N_1), w(N_2) \leq W$ (as we shall prove in Theorem 22 below). Note that, since we are allowed to choose a different W

for each pair of F-normal forms N_1 and N_2, it follows that for each such pair there indeed exists a distinguishing valuation.

Let $\ulcorner\_\urcorner$ denote an *injective* function

$$\ulcorner\_\urcorner : \mathcal{V} \to \{n \in \omega : n > W\}$$

that associates with every variable a unique natural number greater than W. We define the valuation $* : \mathcal{V} \to \mathbf{P}_\gamma$ for all $x \in \mathcal{V}$ by

$$*(x) = \tau.\varphi_{\ulcorner x \urcorner} \ .$$

The τ-prefix is to ensure the following property for *all* normal forms (not just N_1 and N_2).

Lemma 19. For every F-normal form N, the branching degree of $[\![N]\!]_*$ is at most $w(N)$.

Proof. Structural induction on N. □

Lemma 20. Let S be a simple F-normal form, let $\alpha \in \mathcal{A}_\tau$, and let p be a process such that $[\![S]\!]_* \xrightarrow{\alpha} p$. Then the following statements hold:

(i) if $S = \beta.N$, then $\alpha = \beta$ and $p = [\![N]\!]_*$;
(ii) if $S = x \mathbin{\underline{\|}} N$, then $\alpha = \tau$ and $p = \varphi_{\ulcorner x \urcorner} \parallel [\![N]\!]_*$.

An important property of $*$ is that it allows us to distinguish the different types of simple F-normal forms by classifying their residuals according to the number of parallel components with a branching degree that exceeds W. Let us say that a process p is of *type* n ($n \geq 0$) if its unique parallel decomposition contains precisely n parallel prime components with a branching degree $> W$.

Corollary 21. Let S be a simple F-normal form such that $w(S) \leq W$.

(i) If $S = \alpha.N$, then the unique residual $[\![N]\!]_*$ of $[\![S]\!]_*$ is of type 0.
(ii) If $S = x \mathbin{\underline{\|}} N$, then the unique residual $\varphi_{\ulcorner x \urcorner} \parallel [\![N]\!]_*$ of $[\![S]\!]_*$ is of type 1.

Proof. On the one hand, by Lemma 19, in both cases $[\![N]\!]_*$ has a branching degree of at most $w(N) \leq w(S) \leq W$, and hence, by Lemma 13, its unique parallel decomposition cannot contain parallel prime components with a branching degree that exceeds W. On the other hand, by Lemmas 14(i) and 14(iii), the process $\varphi_{\ulcorner x \urcorner}$ is parallel prime and has a branching degree that exceeds W. So $[\![N]\!]_*$ is of type 0, and $\varphi_{\ulcorner x \urcorner} \parallel [\![N]\!]_*$ is of type 1. □

Theorem 22. For every two F-normal forms N_1, N_2 such that $w(N_1), w(N_2) \leq W$ it holds that $[\![N_1]\!]_* = [\![N_2]\!]_*$ only if $N_1 \approx N_2$ modulo A1–A4.

Proof. By Lemma 6 we may assume that N_1 and N_2 are summations of sequences of simple F-normal forms. We assume $[\![N_1]\!]_* = [\![N_2]\!]_*$ and prove that then $N_1 \approx N_2$ modulo A1–A4, by induction on the sum of the heights of N_1 and N_2.

We first prove that for every syntactic summand S_1 of N_1 there is a syntactic summand S_2 of N_2 such that $S_1 \approx S_2$ modulo A1–A4. To this end, let S_1 be an arbitrary syntactic summand of N_1; we distinguish cases according to the syntactic form of S_1.

1. Suppose $S_1 = \alpha.N_1'$; then $[\![S_1]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a syntactic summand S_2 of N_2 such that $[\![S_2]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$. By Lemma 19 the branching degree of $[\![N_1']\!]_*$ does not exceed W, so $[\![S_2]\!]_*$ has a residual of type 0, and therefore, by Corollary 21, there exist $\beta \in \mathcal{A}_\tau$ and a normal form N_2' such that $S_2 = \beta.N_2'$. Moreover, since $[\![S_2]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$, it follows by Lemma 20(i) that $\alpha = \beta$ and $[\![N_1']\!]_* = [\![N_2']\!]_*$. Hence, by the induction hypothesis, we conclude that $N_1' \approx N_2'$ modulo A1–A4, so $S_1 = \alpha.N_1' \approx \beta.N_2' = S_2$.
2. Suppose $S_1 = x \between N_1'$; then $[\![S_1]\!]_* \xrightarrow{\tau} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a summand S_2 of N_2 such that $[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$. Since S_2 has a residual of type 1, by Corollary 21 there exist a variable y and a normal form N_2' such that $S_2 = y \between N_2'$. Now, since $[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$, it follows by Lemma 20(ii) that

$$\varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_* = \varphi_{\ulcorner y \urcorner} \parallel [\![N_2']\!]_* \ . \tag{4}$$

   Since $[\![N_1']\!]_*$ and $[\![N_2']\!]_*$ are of type 0, we have that the unique decomposition of $[\![N_1']\!]_*$ (see Theorem 11) does not contain $\varphi_{\ulcorner y \urcorner}$ and the unique decomposition of $[\![N_2']\!]_*$ does not contain $\varphi_{\ulcorner x \urcorner}$. Hence, from (4) it follows that $\varphi_{\ulcorner x \urcorner} = \varphi_{\ulcorner y \urcorner}$ and $[\![N_1']\!]_* = [\![N_2']\!]_*$. From the former we conclude, by Lemma 14(ii) and the injectivity of $\ulcorner \cdot \urcorner$, that $x = y$ and from the latter we conclude by the induction hypothesis that $N_1' \approx N_2'$ modulo A1–A4. So $S_1 = x \between N_1' \approx y \between N_2' = S_2$.

We have established that every syntactic summand of N_1 is provably equal to a syntactic summand of N_2. Similarly, it follows that every syntactic summand of N_2 is provably equal to a syntactic summand of N_2. Hence, modulo A1–A4, $N_1 \approx N_1 + N_2 \approx N_2$, so the proof of the theorem is complete. □

Corollary 23. For all process terms P and Q, $P \approx_{\mathrm{F}} Q$ if, and only if, $P \leftrightarrows_f Q$, and hence the axioms generated by the schemata in Table 2 together with the axiom F consitute an equational base for $\mathbf{P}_f$.

Proof. The implication from left to right is Proposition 15. To prove the implication from right to left, suppose $P \leftrightarrows_f Q$. Then, by Lemma 17 there exist normal forms N_1 and N_2 such that $P \approx_{\mathrm{F}} N_1$ and $Q \approx_{\mathrm{F}} N_2$; from $P \leftrightarrows_f Q$ we conclude by Proposition 15 that $N_1 \leftrightarrows_f N_2$. Now choose W large enough such that $w(N_1), w(N_2) \leq W$. From $N_1 \leftrightarrows_f N_2$ it follows that $[\![N_1]\!]_* = [\![N_2]\!]_*$, and hence, by Theorem 22 $N_1 \approx N_2$. We may therefore conclude that $P \approx_{\mathrm{F}} N_1 \approx N_2 \approx_{\mathrm{F}} Q$. □

Corollary 24. The equational theory of $\mathbf{P}_f$ is decidable.

Proof. From the proof of Lemma 17 it is easy to see that there exists an effective procedure that associates with every process term a provably equivalent F-normal. Furthermore, from Definition 18 it is clear that every F-normal form has an effectively computable width. We now sketch an effective procedure that decides whether a process equation $P \approx Q$ is valid:

1. Compute F-normal forms N_1 and N_2 such that $P \approx_{\mathrm{F}} N_1$ and $Q \approx_{\mathrm{F}} N_2$.
2. Compute $w(N_1)$ and $w(N_2)$ and define W as their maximum.

3. Determine the (finite) set $\mathcal{V}'$ of variables occurring in N_1 and N_2; define an injection $\ulcorner\urcorner : \mathcal{V}' \to \{n \in \omega : n > W\}$, and a substitution $* : \mathcal{V}' \to \mathcal{P}_0$ that assigns to a variable x in $\mathcal{V}'$ the closed process term $\tau.\varphi_{\ulcorner x \urcorner}$. (We may interpret Eqn. 2 as defining a sequence of closed process terms instead of a sequence of processes.)
4. Let N_1^* and N_2^* be the results from applying $*$ to N_1 and N_2, respectively.
5. Determine if the closed process terms N_1^* and N_2^* are bisimilar; if they are, then the process equation $P \approx Q$ is valid in $\mathbf{P}_f$, and otherwise it is not. □

4 An equational base for $\mathbf{P}_h$

We now consider the algebra $\mathbf{P}_h$. Note that if $\mathcal{A}$ happens to be the empty set, then $\mathbf{P}_h$ satisfies the axiom F, and it is clear from the proof in the previous section that the axioms generated by the axiom schemata in Table 2 together with F in fact constitute a finite equational base for $\mathbf{P}_h$. We therefore proceed with the assumption that $\mathcal{A}$ is nonempty, and prove that an equational base for $\mathbf{P}_h$ is then obtained if we add the axiom

$$\text{H} \quad x \mid (y \mid z) \approx \mathbf{0}$$

to the set of axioms generated by the axiom schemata in Table 2. Again, the resulting equational base is finite if the set $\mathcal{A}$ is finite.

Henceforth, whenever we write $P \approx_{\text{H}} Q$, we shall mean that the equation $P \approx Q$ is derivable from the axioms in Table 2 and the axiom H.

Proposition 25. For all process terms P and Q, if $P \approx_{\text{H}} Q$, then $P \leftrightarrows_h Q$.

We proceed to adapt the proof presented in the previous section to establish the converse of Proposition 25. Naturally, with H instead of F not every occurrence of $\mid$ can be eliminated from process terms; we therefore need to adapt the notion of normal form.

Definition 26. The set $\mathcal{N}_{\text{H}}$ of H-*normal forms* is generated by the following grammar:

$$N \ ::= \ \mathbf{0} \ \mid \ N + N \ \mid \ \alpha.N \ \mid \ x \between N \ \mid \ (x \mid a) \between N \ \mid (x \mid y) \between N \ ,$$

with $x, y \in \mathcal{V}$, $\alpha \in \mathcal{A}_\tau$ and $a \in \mathcal{A}$.

Note that the set of simple H-normal forms (see Definition 5) is generated by the grammar

$$S \ ::= \ \alpha.N \ \mid \ x \between N \ \mid \ (x \mid a) \between N \ \mid (x \mid y) \between N \ ,$$

with $x, y \in \mathcal{V}$, $\alpha \in \mathcal{A}_\tau$, $a \in \mathcal{A}$, and N ranging over H-normal forms.

In the proof that every process term is provably equal to an H-normal form, we use the following derivable equation.

Lemma 27. The following equation is derivable from the axioms in Table 2 and the axiom H:

C9 $\quad \tau.x \mid y \approx_{\mathrm{H}} \mathbf{0}$.

Proof. Let $a \in \mathcal{A}$; then

$$\begin{aligned} \tau.x \mid y &\approx_{\mathrm{H}} \tau.(x \parallel \mathbf{0}) \mid y && \text{by P4 (see Lemma 10)} \\ &\approx_{\mathrm{H}} (a.x \mid \overline{a}.\mathbf{0}) \mid y && \text{by C2} \\ &\approx_{\mathrm{H}} \mathbf{0} && \text{by H.} \end{aligned}$$

□

Lemma 28. For every process term P there exists an H-normal form N such that $P \approx_{\mathrm{H}} N$ and $h(P) \geq h(N)$.

Proof. As in the proof of Lemma 17 we proceed by $\prec$-induction and do a case distinction on the syntactic form of P. For the first four cases (P is a variable, $P = \mathbf{0}$, $P = \alpha.P'$ and $P = P_1 + P_2$) the proofs are identical to those in Lemma 17, so they are omitted.

5. If $P = Q \between R$, then, since $h(Q) \leq h(P)$ and $\ell(Q) < \ell(P)$, it holds that $Q \prec P$, and hence by the induction hypothesis and Lemma 6 there exists a sequence $S_1, \ldots, S_n$ of simple H-normal forms such that $Q \approx_{\mathrm{H}} \sum_{i=1}^{n} S_i$ and $h(Q) \geq h(S_i)$ for all $i = 1, \ldots, n$. If $n = 0$, then $P \approx_{\mathrm{H}} \mathbf{0} \between R \approx \mathbf{0}$ by L1, and clearly $h(P) \geq h(\mathbf{0})$. Otherwise, by L3

$$P \approx_{\mathrm{H}} \sum_{i=1}^{n} (S_i \between R) \ ,$$

so it remains to show, for all $i = 1, \ldots, n$, that $S_i \between R$ is provably equal to an appropriate H-normal form. We distinguish cases according to the syntactic form of S_i:

(a) If $S_i = \alpha.N_i'$ (with N_i' an H-normal form), then by L2

$$S_i \between R \approx_{\mathrm{H}} \alpha.(N_i' \parallel R) \ .$$

Since $h(N_i') < h(S_i) \leq h(Q)$, it holds that $N_i' \parallel R \prec P$ and hence by the induction hypothesis there exists an H-normal form N such that $N_i' \parallel R \approx_{\mathrm{H}} N$ and $h(N_i' \parallel R) \geq h(N)$. Clearly, $\alpha.N$ is an H-normal form such that $S_i \between R \approx_{\mathrm{H}} \alpha.N$ and $h(S_i \between R) \geq h(\alpha.N)$.

(b) If $S_i = S_i' \between N_i''$ with $S_i' = x$, $S_i' = (x \mid a)$ or $S_i' = (x \mid y)$, and N_i'' an H-normal form, then by L4

$$S_i \between R \approx_{\mathrm{H}} S_i' \between (N_i'' \parallel R) \ .$$

Note that $h(S_i') > 0$, so $h(N_i'') < h(S_i) \leq h(Q)$. It follows that $N_i'' \parallel R \prec P$, and hence by the induction hypothesis there exists an H-normal form N such that $N_i'' \parallel R \approx_{\mathrm{H}} N$ and $h(N_i'' \parallel R) \geq h(N)$. Clearly, $S_i' \between N$ is an H-normal form such that $S_i \between R \approx_{\mathrm{H}} S_i' \between N$ and $h(S_i \between R) \geq h(S_i' \between N)$.

6. If $P = Q \,|\, R$, then, since $h(Q) \leq h(P)$ and $\ell(Q) < \ell(P)$, it holds that $Q \prec P$, and, for similar reasons, $R \prec P$. Hence, by the induction hypothesis and Lemma 6 there exist sequences $S_1, \ldots, S_m$ and $T_1, \ldots, T_n$ of simple H-normal forms such that $Q \approx_{\mathrm{H}} \sum_{i=1}^{m} S_i$, $R \approx_{\mathrm{H}} \sum_{j=1}^{n} T_j$, $h(Q) \geq h(S_i)$ for all $i = 1, \ldots, m$, and $h(R) \geq h(T_j)$ for all $j = 1, \ldots, n$. Note that if $m = 0$, then $P \approx_{\mathrm{H}} \mathbf{0} \mid R \approx \mathbf{0}$ by C1, and if $n = 0$, then $P \approx_{\mathrm{H}} Q \mid \mathbf{0} \approx_{\mathrm{H}} \mathbf{0} \mid Q \approx_{\mathrm{H}} \mathbf{0}$ by C5 and C1, and clearly $h(P) \geq h(\mathbf{0})$. Otherwise, by C4 and C5

$$P \approx_{\mathrm{H}} \sum_{i=1}^{m} \sum_{j=1}^{n} (S_i \mid T_j) \ ,$$

and it remains to show, for all $i = 1, \ldots, m$ and $j = 1, \ldots, n$, that $S_i \mid T_j$ is provably equal to an appropriate H-normal form. We distinguish cases according to the syntactic forms that S_i and T_j may take:

(a) Suppose $S_i = \tau.S_i'$; then $S_i \,|\, T_j \approx_{\mathrm{H}} \mathbf{0}$ by Lemma 27, and clearly $h(S_i \,|\, T_j) \geq 0$.

(b) Suppose $T_j = \tau.T_j'$; then we apply C5 and proceed as in the previous case.

(c) Suppose $S_i = S_i' \between S_i''$ with $S_i' = x \mid a$ or $S_i' = x \mid y$; then by C7, C6, H, and L1

$$S_i \mid T_j \approx (S_i' \mid T_j) \between S_i'' \approx_{\mathrm{H}} \mathbf{0} \between S_i'' \approx \mathbf{0} \ ,$$

and clearly $h(S_i \mid T_j) \geq h(\mathbf{0})$.

(d) Suppose $T_j = T_j' \between T_j''$ with $T_j' = x \mid a$ or $T_j' = x \mid y$; then $S_i \mid T_j \approx T_j \mid S_i$ by C5 and we can proceed as in the previous case.

(e) Suppose $S_i = a.S_i'$ and $T_j = b.T_j'$.
If $b \neq \overline{a}$, then $S_i \mid T_j \approx \mathbf{0}$ by C3 and $h(S_i \mid T_j) \geq h(\mathbf{0})$.
On the other hand, if $b = \overline{a}$, then $S_i \mid T_j \approx \tau.(S_i' \parallel T_j')$, and, since $h(S_i') < h(S_i) \leq h(Q)$ and $h(T_j') < h(T_i) \leq h(R)$, it follows that $S_i' \parallel T_j' \prec P$. So, by the induction hypothesis there exists an H-normal form N such that $S_i' \parallel T_j' \approx_{\mathrm{H}} N$ and $h(S_i' \parallel T_j') \geq h(N)$. Then clearly $\tau.N$ is an H-normal form such that $S_i \mid T_j \approx_{\mathrm{H}} \tau.N$ and $h(S_i \mid T_j) \geq h(\tau.N)$.

(f) Suppose $S_i = a.S_i'$ and $T_j = x \between T_j'$. Then

$$\begin{aligned} a.S_i' \mid (x \between T_j') &\approx a.(\mathbf{0} \parallel S_i') \mid (x \between T_j') && \text{(by P4, P3 in Lemma 10)} \\ &\approx (a \between S_i') \mid (x \between T_j') && \text{(by L2)} \\ &\approx (x \mid a) \between (S_i' \parallel T_j') && \text{(by Lemma 3 and C5).} \end{aligned}$$

Since $h(S_i') < h(S_i) \leq h(Q)$ and $h(T_j') < h(T_i) \leq h(R)$, it follows that $S_i' \parallel T_j' \prec P$, and hence by the induction hypothesis there exists an H-normal form N such that $S_i' \parallel T_j' \approx_{\mathrm{H}} N$ and $h(S_i' \parallel T_j') \geq h(N)$. Then clearly $(x \,|\, a) \between N$ is an H-normal form such that $S_i \mid T_j \approx_{\mathrm{H}} (x \mid a) \between N$ and $h(S_i \mid T_j) \geq h((x \mid a) \between N)$.

(g) If $S_i = x \between S_i'$ and $T_j = a.T_j'$, then the proof is analogous to the previous case.

(h) Suppose $S_i = x \mathbin{\underline{\|}} S_i'$ and $T_j = y \mathbin{\underline{\|}} T_j'$. Then, by the derived equation C8 (see Lemma 3)

$$S_i \mid T_j \approx (x \mid y) \mathbin{\underline{\|}} (S_i' \parallel T_j') \ .$$

Since $h(S_i') < h(S_i) \leq h(Q)$ and $h(T_j') < h(T_i) \leq h(R)$, it follows that $S_i' \parallel T_j' \prec P$, and hence by the induction hypothesis there exists an H-normal form N such that $S_i' \parallel T_j' \approx_{\mathrm{H}} N$ and $h(S_i' \parallel T_j') \geq h(N)$. Then clearly $(x \mid y) \mathbin{\underline{\|}} N$ is an H-normal form such that $S_i \mid T_j \approx_{\mathrm{H}} (x \mid y) \mathbin{\underline{\|}} N$ and $h(S_i \mid T_j) \geq h((x \mid y) \mathbin{\underline{\|}} N)$.

7. If $P = Q \parallel R$, then $P \approx Q \mathbin{\underline{\|}} R + R \mathbin{\underline{\|}} Q + Q \mid R$. We can now proceed as in case 5 to show that for $Q \mathbin{\underline{\|}} R$ and $R \mathbin{\underline{\|}} Q$ there exist H-normal forms N_1 and N_2, respectively, such that $Q \mathbin{\underline{\|}} R \approx_{\mathrm{H}} N_1$, $R \mathbin{\underline{\|}} Q \approx_{\mathrm{H}} N_2$, $h(Q \mathbin{\underline{\|}} R) \geq h(N_1)$ and $h(R \mathbin{\underline{\|}} Q) \geq h(N_2)$. Furthermore, we can proceed as in case 6 to show that for $Q \mid R$ there exists an H-normal form N_3 such that $Q \mid R \approx_{\mathrm{H}} N_3$ and $h(Q \mid R) \geq h(N_3)$. Then $N_1 + N_2 + N_3$ is an H-normal form such that $P \approx_{\mathrm{H}} N_1 + N_2 + N_3$ and $h(P) \geq h(N_1 + N_2 + N_3)$. □

We proceed to establish that for every two H-normal forms N_1 and N_2 there exists a valuation $* : \mathcal{V} \to \mathbf{P}_\gamma$ such that

$$\text{if } [\![N_1]\!]_* = [\![N_2]\!]_*, \text{ then } N_1 \approx_{\mathrm{H}} N_2. \tag{5}$$

The distinguishing valuations $*$ will have a slightly more complicated definition than before, because of the more complicated notion of normal form.

As in the previous section, for the definition of $*$ we fix a natural number W. Since $\mid$ may occur in H-normal forms, we now also need to make sure that whatever process $*$ assigns to variables has sufficient communication abilities. To achieve this, we fix a finite subset $\mathcal{A}' = \{a_1, \ldots, a_n\}$ of $\mathcal{A}$ that is closed under the bijection $\bar{\ }$ on $\mathcal{A}$. (Note that every finite subset of $\mathcal{A}$ has a finite superset with the aforementioned property.) Based on W and $\mathcal{A}'$ we define the valuation $* : \mathcal{V} \to \mathbf{P}_\gamma$ by

$$*(x) = a_1.\varphi_{(1 \cdot \ulcorner x \urcorner)} + \cdots + a_n.\varphi_{(n \cdot \ulcorner x \urcorner)} \ .$$

We shall prove that $*$ satisfies Eqn. (5) provided that the actions occurring in N_1 and N_2 are in $\mathcal{A}' \cup \{\tau\}$ and the width of N_1 and N_2, defined below, does not exceed W. We must also be careful to define the injection $\ulcorner \_ \urcorner$ in such a way that the extra factors $1, \ldots, n$ in the definition of $*$ do not interfere with the numbers assigned to variables; we let $\ulcorner \_ \urcorner$ denote an injection

$$\ulcorner \_ \urcorner : \mathcal{V} \to \{m : m \text{ a prime number such that } m > n \text{ and } m > W\}$$

that associates with every variable a prime number greater than the cardinality of $\mathcal{A}'$ and greater than W.

The definition of width also needs to take into account the cardinality of $\mathcal{A}'$ to maintain the property that the branching degree of $[\![N]\!]_*$ does not exceed $w(N)$.

Definition 29. We define the *width* $w(N)$ of an H-normal form N as follows:

(i) if $N = \mathbf{0}$, then $w(N) = 0$;
(ii) if $N = N_1 + N_2$, then $w(N) = w(N_1) + w(N_2)$;
(iii) if $N = \alpha.N'$, then $w(N) = \max(w(N'), 1)$;
(iv) if $N = x \between N'$, then $w(N) = \max(w(N'), |\mathcal{A}'|)$;
(v) if $N = (x \mid \alpha) \between N'$, then $w(N) = \max(w(N'), 1)$; and
(vi) if $N = (x \mid y) \between N'$, then $w(N) = \max(w(N'), |\mathcal{A}'|)$.

Lemma 30. For every H-normal form N, the branching degree of $[\![N]\!]_*$ is at most $w(N)$.

Proof. Structural induction on N. □

Lemma 31. Let S be a simple H-normal form, let $\alpha \in \mathcal{A}_\tau$, and let p be a process such that $[\![S]\!]_* \xrightarrow{\alpha} p$. Then the following statements hold:

(i) if $S = \beta.N$, then $\alpha = \beta$ and $p = [\![N]\!]_*$;
(ii) if $S = x \between N$, then $\alpha = a_i$ and $p = \varphi_{i\cdot\ulcorner x\urcorner} \parallel [\![N]\!]_*$ for some $i \in \{1, \ldots, n\}$;
(iii) if $S = (x \mid a) \between N$, then $\alpha = \tau$ and $p = \varphi_{i\cdot\ulcorner x\urcorner} \parallel [\![N]\!]_*$ for the unique $i \in \{1, \ldots, n\}$ such that $\overline{a} = a_i$; and
(iv) if $S = (x \mid y) \between N$, then $\alpha = \tau$ and $p = \varphi_{i\cdot\ulcorner x\urcorner} \parallel \varphi_{j\cdot\ulcorner y\urcorner} \parallel [\![N]\!]_*$ for some $i, j \in \{1, \ldots, n\}$ such that $\overline{a_i} = a_j$.

As in the previous section, we distinguish H-normal forms by classifying their residuals according to the number of parallel components with a branching degree that exceeds W. Again, we say that a process p is of *type* n ($n \geq 0$) if its unique parallel decomposition contains precisely n parallel prime components with a branching degree $> W$.

Corollary 32. Let S be a simple H-normal form such that $w(S) \leq W$ and such that the actions occurring in S are included in $\mathcal{A}' \cup \{\tau\}$.

(i) If $S = \alpha.N$, then the unique residual of $[\![S]\!]_*$ is of type 0.
(ii) If $S = x \between N$, then all residuals of $[\![S]\!]_*$ are of type 1.
(iii) If $S = (x \mid a) \between N$, then the unique residual of $[\![S]\!]_*$ is of type 1.
(iv) If $S = (x \mid y) \between N$, then all residuals of $[\![S]\!]_*$ are of type 2.

Proof. On the one hand, by Lemma 30, in each case $[\![N]\!]_*$ has a branching degree of at most $w(N) \leq w(S) \leq W$, and hence, by Lemma 13, its unique parallel decomposition cannot contain parallel prime components with a branching degree that exceeds W. On the other hand, by Lemmas 14(i) and 14(iii), the processes $\varphi_{i\cdot\ulcorner x\urcorner}$ and $\varphi_{j\cdot\ulcorner y\urcorner}$ are parallel prime and have a branching degree that exceeds W. Using these observations it is straightforward to establish the corollary as a consequence of Lemma 31. □

Theorem 33. For every two H-normal forms N_1, N_2 such that $w(N_1), w(N_2) \leq W$ and such that the actions occurring in N_1 and N_2 are included in $\mathcal{A}' \cup \{\tau\}$ it holds that $[\![N_1]\!]_* = [\![N_2]\!]_*$ only if $N_1 \approx N_2$ modulo A1–A4, C5.

Proof. By Lemma 6 we may assume that N_1 and N_2 are summations of sequences of simple H-normal forms. We assume $[\![N_1]\!]_* = [\![N_2]\!]_*$ and prove that then $N_1 \approx N_2$ modulo A1–A4, C5, by induction on the sum of the heights of N_1 and N_2.

We first prove that for every syntactic summand S_1 of N_1 there is a syntactic summand S_2 of N_2 such that $S_1 \approx S_2$ modulo A1–A4, C5. To this end, let S_1 be an arbitrary syntactic summand of N_1; we distinguish cases according to the syntactic form of S_1.

1. Suppose $S_1 = \alpha.N_1'$; then $[\![S_1]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a syntactic summand S_2 of N_2 such that $[\![S_2]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$. By Lemma 30 the branching degree of $[\![N_1']\!]_*$ does not exceed W, so $[\![S_2]\!]_*$ has a residual of type 0, and therefore, by Corollary 32, there exist $\beta \in \mathcal{A}_\tau$ and an H-normal form N_2' such that $S_2 = \beta.N_2'$. Moreover, since $[\![S_2]\!]_* \xrightarrow{\alpha} [\![N_1']\!]_*$ it follows by Lemma 31(i) that $\alpha = \beta$ and $[\![N_1']\!]_* = [\![N_2']\!]_*$. Hence, by the induction hypothesis, we conclude that $N_1' \approx N_2'$ modulo A1–A4, C5. So $S_1 = \alpha.N_1' \approx \beta.N_2' = S_2$.
2. Suppose $S_1 = x \between N_1'$; then $[\![S_1]\!]_* \xrightarrow{a_1} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a summand S_2 of N_2 such that $[\![S_2]\!]_* \xrightarrow{a_1} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$. Since S_2 has a residual of type 1, by Corollary 32(i, iv) it is not of the form $\alpha.N_2'$ for some $\alpha \in \mathcal{A}_\tau$ and H-normal form N_2', or of the form $(y \mid z) \between N_2'$ for some $y, z \in \mathcal{V}$ and H-normal form N_2'. Moreover, S_2 cannot be of the form $(y \mid a) \between N_2'$ for some $y \in \mathcal{V}$ and $a \in \mathcal{A}$, for then by Lemma 31(iii) $[\![S_2]\!]_* \xrightarrow{\alpha} p$ would imply $\alpha = \tau \neq a_1$. So, there exists a variable y and an H-normal form N_2' such that $S_2 = y \between N_2'$. Now, since $[\![S_2]\!]_* \xrightarrow{a_1} \varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_*$, it follows by Lemma 31(ii) that

$$\varphi_{\ulcorner x \urcorner} \parallel [\![N_1']\!]_* = \varphi_{\ulcorner y \urcorner} \parallel [\![N_2']\!]_* \ . \tag{6}$$

   Since $[\![N_1']\!]_*$ and $[\![N_2']\!]_*$ are of type 0, we conclude that the unique decomposition of $[\![N_1']\!]_*$ does not contain $\varphi_{\ulcorner y \urcorner}$ and the unique decomposition of $[\![N_2']\!]_*$ does not contain $\varphi_{\ulcorner x \urcorner}$. Hence, from (6) it follows that $\varphi_{\ulcorner x \urcorner} = \varphi_{\ulcorner y \urcorner}$ and $[\![N_1']\!]_* = [\![N_2']\!]_*$. From the former we conclude by the injectivity of $\ulcorner . \urcorner$ that $x = y$, and from the latter we conclude by the induction hypothesis that $N_1' \approx N_2'$ modulo A1–A4, C5. So $S_1 = x \between N_1' \approx y \between N_2' = S_2$.
3. Suppose $S_1 = (x \mid a) \between N_1'$, and let i be such that $\overline{a} = a_i$. Then $[\![S_1]\!]_* \xrightarrow{\tau} \varphi_{i \cdot \ulcorner x \urcorner} \parallel [\![N_1']\!]_*$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a summand S_2 of N_2 such that

$$[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{i \cdot \ulcorner x \urcorner} \parallel [\![N_1']\!]_* \ .$$

   Since S_2 has a residual of type 1, by Corollary 32(i, iv) it is not of the form $\alpha.N_2'$ for some $\alpha \in \mathcal{A}_\tau$ and H-normal form N_2', or of the form $(y \mid z) \between N_2'$ for some $y, z \in \mathcal{V}$ and H-normal form N_2'. Moreover, S_2 cannot be of the form $y \between N_2'$ for some $y \in \mathcal{V}$, for then by Lemma 31(ii) $[\![S_2]\!]_* \xrightarrow{\alpha} p$ would imply $\alpha = a_k \neq \tau$ for some $k \in \{1, \ldots, n\}$. So, there exist a variable y, action $b \in \mathcal{A}'$ and an H-normal form N_2' such that $S_2 = (y \mid b) \between N_2'$. Now, since $[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{i \cdot \ulcorner x \urcorner} \parallel [\![N_1']\!]_*$, it follows by Lemma 31(iii) that

$$\varphi_{i \cdot \ulcorner x \urcorner} \parallel [\![N_1']\!]_* = \varphi_{j \cdot \ulcorner y \urcorner} \parallel [\![N_2']\!]_* \ , \tag{7}$$

with $j \in \{1,\ldots,n\}$ such that $\overline{b} = a_j$. By Lemma 14(i, iii) the processes $\varphi_{i\cdot\ulcorner x\urcorner}$ and $\varphi_{j\cdot\ulcorner y\urcorner}$ are parallel prime and have branching degrees that, since $\ulcorner x\urcorner > W$ and $\ulcorner y\urcorner > W$, exceed W. Therefore, since $[\![N_1']\!]_*$ and $[\![N_2']\!]_*$ are of type 0, it follows that the unique decomposition of $[\![N_1']\!]_*$ does not contain $\varphi_{j\cdot\ulcorner y\urcorner}$ and the unique decomposition of $[\![N_2']\!]_*$ does not contain $\varphi_{i\cdot\ulcorner x\urcorner}$. Hence, by (7) we have that $\varphi_{i\cdot\ulcorner x\urcorner} = \varphi_{j\cdot\ulcorner y\urcorner}$ and $[\![N_1']\!]_* = [\![N_2']\!]_*$. From $\varphi_{i\cdot\ulcorner x\urcorner} = \varphi_{j\cdot\ulcorner y\urcorner}$, by Lemma 14(ii) we infer that $i \cdot \ulcorner x\urcorner = j \cdot \ulcorner y\urcorner$. Since $\ulcorner x\urcorner$ and $\ulcorner y\urcorner$ are prime numbers greater than i and j, it follows that $i = j$, whence $a = b$, and $\ulcorner x\urcorner = \ulcorner y\urcorner$, whence $x = y$ by the injectivity of $\ulcorner\cdot\urcorner$. From $[\![N_1']\!]_* = [\![N_2']\!]_*$ we conclude by the induction hypothesis that $N_1' \approx N_2'$ modulo A1–A4, C5. So $S_1 = (x \mid a) \between N_1' \approx (y \mid b) \between N_2' = S_2$.

4. Suppose $S_1 = (x|y) \between N_1'$. Then $[\![S_1]\!]_* \xrightarrow{\tau} \varphi_{i\cdot\ulcorner x\urcorner} \| \varphi_{j\cdot\ulcorner y\urcorner} \| [\![N_1']\!]_*$ with $i, j \in \{1,\ldots,n\}$ such that $\overline{a_i} = a_j$. Hence, since $[\![N_1]\!]_* = [\![N_2]\!]_*$, there exists a summand S_2 of N_2 such that

$$[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{i\cdot\ulcorner x\urcorner} \| \varphi_{j\cdot\ulcorner y\urcorner} \| [\![N_1']\!]_* \ .$$

Since S_2 has a residual of type 2, by Corollary 32 there exist $x', y' \in \mathcal{V}$ and an H-normal form N_2' such that $S_2 = (x' \mid y') \between N_2'$. Now, since $[\![S_2]\!]_* \xrightarrow{\tau} \varphi_{i\cdot\ulcorner x\urcorner} \| \varphi_{j\cdot\ulcorner y\urcorner} \| [\![N_1']\!]_*$ it follows by Lemma 31(iv) that for some $k, l \in \{1,\ldots,n\}$ such that $\overline{a_k} = a_l$

$$\varphi_{i\cdot\ulcorner x\urcorner} \| \varphi_{j\cdot\ulcorner y\urcorner} \| [\![N_1']\!]_* = \varphi_{k\cdot\ulcorner x'\urcorner} \| \varphi_{l\cdot\ulcorner y'\urcorner} \| [\![N_2']\!]_* \ . \tag{8}$$

By Lemma 14(i, iii) the processes $\varphi_{i\cdot\ulcorner x\urcorner}$, $\varphi_{j\cdot\ulcorner y\urcorner}$, $\varphi_{k\cdot\ulcorner x'\urcorner}$ and $\varphi_{l\cdot\ulcorner y'\urcorner}$ are parallel prime and have branching degrees that exceed W. Therefore, since $[\![N_1']\!]_*$ and $[\![N_2']\!]_*$ are of type 0, it follows that the unique decomposition of $[\![N_1']\!]_*$ does not contain $\varphi_{k\cdot\ulcorner x'\urcorner}$ and $\varphi_{l\cdot\ulcorner y'\urcorner}$, and the unique decomposition of $[\![N_2']\!]_*$ does not contain $\varphi_{i\cdot\ulcorner x\urcorner}$ and $\varphi_{j\cdot\ulcorner y\urcorner}$. Hence, from (8) we infer that $[\![N_1']\!]_* = [\![N_2']\!]_*$ and either $\varphi_{i\cdot\ulcorner x\urcorner} = \varphi_{k\cdot\ulcorner x'\urcorner}$ and $\varphi_{j\cdot\ulcorner y\urcorner} = \varphi_{l\cdot\ulcorner y'\urcorner}$, or $\varphi_{i\cdot\ulcorner x\urcorner} = \varphi_{l\cdot\ulcorner y'\urcorner}$ and $\varphi_{j\cdot\ulcorner y\urcorner} = \varphi_{k\cdot\ulcorner x'\urcorner}$. From the former we conclude by the induction hypothesis that $N_1' \approx N_2'$ modulo A1–A4, C5; from the latter it follows reasoning as in case 3 that either $x = x'$ and $y = y'$, or $x = y'$ and $y = x'$. In both cases, $S_1 = (x \mid y) \between N_1' \approx (x' \mid y') \between N_2' = S_2$.

We have established that every syntactic summand of N_1 is provably equal to a syntactic summand of N_2. Similarly, it follows that every syntactic summand of N_2 is provably equal to a syntactic summand of N_2. Hence, modulo A1–A4, C5 $N_1 \approx N_1 + N_2 \approx N_2$, and the proof of the theorem is complete. □

Corollary 34. For all process terms P and Q, $P \approx_{\mathrm{H}} Q$ if, and only if, $P \leftrightarrows_h Q$, and hence the axioms generated by the schemata in Table 2 together with the axiom H consitute an equational base for $\mathbf{P}_h$.

Proof. The implication from left to right is Proposition 25. To prove the implication from right to left, suppose $P \leftrightarrows_h Q$. Then, by Lemma 28 there exist H-normal forms N_1 and N_2 such that $P \approx_{\mathrm{H}} N_1$ and $Q \approx_{\mathrm{H}} N_2$; from $P \leftrightarrows_h Q$ we conclude by Proposition 25 that $N_1 \leftrightarrows_h N_2$. Now choose W large enough such that $w(N_1), w(N_2) \leq W$, and pick a finite set $\mathcal{A}'$ that is closed under $\bar{\cdot}$ and includes all of the actions occurring in N_1 and N_2. From $N_1 \leftrightarrows_h N_2$ it follows that $[\![N_1]\!]_* = [\![N_2]\!]_*$, and hence, by Theorem 33 $N_1 \approx N_2$. We can therefore conclude $P \approx_{\mathrm{H}} N_1 \approx N_2 \approx_{\mathrm{H}} Q$. □

Corollary 35. The equational theory of $\mathbf{P}_h$ is decidable.

Proof. From the proof of Lemma 28 it is easy to see that there exists an effective procedure that associates with every process term a provably equivalent H-normal. Furthermore, from Definition 29 it is clear that, given a set $\mathcal{A}'$, every H-normal form has a effectively computable width. We now sketch an effective procedure that decides whether a process equation $P \approx Q$ is valid:

1. Compute H-normal forms N_1 and N_2 such that $P \approx_{\mathrm{H}} N_1$ and $Q \approx_{\mathrm{H}} N_2$.
2. Determine the least set $\mathcal{A}' = \{a_1, \ldots, a_n\}$ of actions that is closed under $\bar{\cdot}$ and contains the actions in $\mathcal{A}$ occurring in N_1 and N_2.
3. Compute $w(N_1)$ and $w(N_2)$ given $\mathcal{A}'$ and define W as their maximum.
4. Determine the (finite) set $\mathcal{V}'$ of variables occurring in N_1 and N_2; define an injection

   $$\ulcorner\urcorner : \mathcal{V}' \to \{m \in \omega : m \text{ a prime number such that } m > n \text{ and } m > W\} \ ,$$

   and a substitution $* : \mathcal{V}' \to \mathcal{P}_0$ that assigns to a variable x in $\mathcal{V}'$ the closed process term

   $$a_1.\varphi_{1.\ulcorner x \urcorner} + \cdots + a_n.\varphi_{n.\ulcorner x \urcorner} \ .$$

   (Again, we interpret Eqn. 2 as defining a sequence of closed process terms instead of a sequence of processes.)
5. Let N_1^* and N_2^* be the results from applying $*$ to N_1 and N_2, respectively.
6. Determine if the closed process terms N_1^* and N_2^* are bisimilar; if they are, then the process equation $P \approx Q$ is valid in $\mathbf{P}_h$, and otherwise it is not. □

References

1. L. Aceto, W. J. Fokkink, A. Ingolfsdottir, and B. Luttik. CCS with Hennessy's merge has no finite equational axiomatization. *Theor. Comput. Sci.*, 330(3):377–405, 2005.
2. L. Aceto, W. J. Fokkink, A. Ingolfsdottir, and B. Luttik. Finite equational bases in process algebra: Results and open questions. In A. Middeldorp, V. van Oostrom, F. van Raamsdonk, and R. C. de Vrijer, editors, *Processes, Terms and Cycles: Steps on the Road to Infinity*, LNCS 3838, pages 338–367. Springer, 2005.
3. J. A. Bergstra and J. W. Klop. Process algebra for synchronous communication. *Inform. and Control*, 60(1-3):109–137, 1984.
4. J. A. Bergstra and J. V. Tucker. Top-down design and the algebra of communicating processes. *Sci. Comput. Programming*, 5(2):171–199, 1985.
5. R. de Simone. Higher-level synchronising devices in Meije-SCCS. *Theor. Comput. Sci.*, 37:245–267, 1985.
6. J. F. Groote. A new strategy for proving omega-completeness applied to process algebra. In J. C. M. Baeten and J. W. Klop, editors, *Proceedings of CONCUR'90*, LNCS 458, pages 314–331. Springer, 1990.
7. J. Heering. Partial evaluation and ω-completeness of algebraic specifications. *Theoret. Comput. Sci.*, 43(2-3):149–167, 1986.
8. M. Hennessy. Axiomatising finite concurrent processes. *SIAM J. Comput.*, 17(5):997–1017, 1988.
9. M. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *J. ACM*, 32(1):137–161, January 1985.

10. B. Luttik and V. van Oostrom. Decomposition orders—another proof of the fundamental theorem of arithmetic. *Theor. Comput. Sci.*, 335(2–3):147–186, 2005.
11. R. Milner. *Communication and Concurrency*. Prentice-Hall International, 1989.
12. F. Moller. *Axioms for Concurrency*. PhD thesis, University of Edinburgh, 1989.
13. F. Moller. The nonexistence of finite axiomatisations for CCS congruences. In *Proceedings of LICS'90*, pages 142–153. IEEE Computer Society Press, 1990.
14. D. M. R. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, 5^{th} *GI Conference*, LNCS 104, pages 167–183. Springer, 1981.
15. W. Taylor. Equational logic. *Houston J. Math.*, (Survey), 1979.

Recent BRICS Report Series Publications

RS-06-6 **Luca Aceto, Willem Jan Fokkink, Anna Ingólfsdóttir, and Bas Luttik.** ***A Finite Equational Base for CCS with Left Merge and Communication Merge*****. March 2006. 22 pp.**

RS-06-5 **Kristian Støvring.** ***Extending the Extensional Lambda Calculus with Surjective Pairing is Conservative*****. March 2006. 18 pp. To appear in** ***Logical Methods in Computer Science*****. Supersedes RS-05-35.**

RS-06-4 **Olivier Danvy and Kevin Millikin.** ***A Rational Deconstruction of Landin's J Operator*****. 2006.**

RS-06-3 **Małgorzata Biernacka and Olivier Danvy.** ***A Concrete Framework for Environment Machines*****. February 2006. ii+29 pp. To appear in the** ***ACM Transactions on Computational Logic*****. Supersedes BRICS RS-05-15.**

RS-06-2 **Mikkel Baun Kjærgaard and Jonathan Bunde-Pedersen.** ***A Formal Model for Context-Awareness*****. February 2006. 26 pp.**

RS-06-1 **Luca Aceto, Taolue Chen, Willem Jan Fokkink, and Anna Ingólfsdóttir.** ***On the Axiomatizability of Priority*****. January 2006. 25 pp.**

RS-05-38 **Małgorzata Biernacka and Olivier Danvy.** ***A Syntactic Correspondence between Context-Sensitive Calculi and Abstract Machines*****. December 2005. iii+39 pp. Revised version of BRICS RS-05-22.**

RS-05-37 **Gerth Stølting Brodal, Kanela Kaligosi, Irit Katriel, and Martin Kutz.** ***Faster Algorithms for Computing Longest Common Increasing Subsequences*****. December 2005. 16 pp.**

RS-05-36 **Dariusz Biernacki, Olivier Danvy, and Chung-chieh Shan.** ***On the Static and Dynamic Extents of Delimited Continuations*****. December 2005. ii+33 pp. To appear in the journal** ***Science of Computer Programming*****. Supersedes BRICS RS-05-13.**

RS-05-35 **Kristian Støvring.** ***Extending the Extensional Lambda Calculus with Surjective Pairing is Conservative*****. November 2005. 19 pp.**

RS-05-34 **Henning Korsholm Rohde.** ***Formal Aspects of Polyvariant Specialization*****. November 2005. 27 pp.**