Bisimulation equivalence is decidable for normed Process Algebra

Yoram Hirshfeld*
School of Mathematical Sciences
Tel Aviv University
Israel

Mark Jerrum†
Department of Computer Science
University of Edinburgh
United Kingdom.

May, 1998

Abstract

We present a procedure for deciding whether two normed PA terms are bisimilar. The procedure is "elementary," having doubly exponential non-deterministic time complexity.

*The first author was supported in part by EPSRC Visiting Research Fellowships GR/K83243 and GR/M06468. Address for correspondence: School of Mathematical Sciences, The Raymond and Beverly Sackler Faculty of Exact Sciences, Tel Aviv University, Ramat Aviv, Tel Aviv 69978, Israel.

†The second author is supported in part by Esprit Working Group No. 21726, "RAND2." Address for correspondence: Department of Computer Science, University of Edinburgh, The King's Buildings, Edinburgh EH9 3JZ, United Kingdom.

1 Discussion

Let Atom be a finite set of *atomic processes* or *atoms*, Act a finite set of *actions*, and Π a collection of *productions* of the form $X \xrightarrow{a} Y$, where $X, Y \in$ Atom and $a \in$ Act. Regarding the atoms as states of a system, we can think of the production $X \xrightarrow{a} Y$ as specifying a possible evolution, or *derivation* of the system from state X to Y via action a. What we have is nothing more than a finite state automaton, familiar from formal language theory.

We can generalise this situation somewhat by allowing both the states and the right hand sides of productions to be terms constructed from atoms using an associative, non-commutative operator "$\cdot$" that we think of as "sequential composition." The productions specify the derivations available to atoms, and hence, by extension, to terms: the derivations available to a general term $P = X_1 \cdot \cdots \cdot X_n$ are precisely those of the form

$$P \xrightarrow{a} X_1' \cdot X_2 \cdot \cdots \cdot X_n,$$

where $X_1 \xrightarrow{a} X_1'$ is a derivation of the atom X_1. (Note that X_1' is not in general an atom, and may be ε, the empty term.) The non-commutativity of the sequential composition operator is reflected in the restriction that productions can be applied only to the leftmost atom.

By way of example, if Atom $= \{X\}$, Act $= \{a, b\}$, and the available productions are

$$X \xrightarrow{a} X \cdot X \quad \text{and} \quad X \xrightarrow{b} \varepsilon,$$

then the states reachable (by some sequence of derivations) from X are ε, X, $X \cdot X$, $X \cdot X \cdot X$, ..., and the available action-sequences from state X to itself are ε, ab, $abab$, $aabb$, $ababab$, ..., i.e., all "balanced parenthesis sequences."

In the field of concurrency theory, systems defined by sets of productions of the form just described are known as "context-free" or "Basic Process Algebra" (BPA) processes. (What we have been terming "states" are commonly referred to as *processes* in concurrency theory.) In language-theoretic terms, a BPA process is equivalent to a pushdown automaton with one state. However, concurrency theory is distinguished from formal language theory in having a different set of concerns: given two BPA processes P and Q we are interested not in whether the action-sequences available to the P and Q are equal as sets (a static notion), but in whether P and Q are "behaviourally equivalent" in a dynamical sense.

What is the "correct" notion of behavioural equivalence for concurrent processes? A popular and mathematically fruitful answer is the relation of bisimilarity: two processes are *bisimilar*, or *bisimulation equivalent*, if, roughly, they may evolve together in such a way that whenever the first process performs a certain action, the second process is able to respond by performing the same action, and *vice versa*. (Precise definitions of this and other terms appearing in this section will be given in Section 2.) The notion of bisimulation equivalence was introduced by Park [11] around 1980, and has been intensively studied since. Bisimilarity plays an important role in algebraic theories of concurrency, such as that based on Milner's CCS [9].

As we have already seen, a BPA process may have infinitely many states, so it is by no means clear, a priori, that there is an effective procedure for deciding whether two BPA processes P and Q are bisimilar. The first such procedure was presented by Christensen, Hüttel and Stirling [6], though no upper bound on complexity could be offered at the time. Subsequently, Burkart, Caucal and Steffen showed the decision problem to be "elementary," i.e., to have time-complexity bounded by some constant-height tower of exponentials [3].

With an eye to modelling concurrent systems, we may introduce an associative, commutative operator "$\mid$" representing "parallel composition." *Basic Parallel Process*es (BPP) are terms constructed from atoms using just this parallel composition operator. Derivations on atoms may be defined, as in BPA, by a finite set of productions, and then extended to terms in the natural way. The commutativity of the parallel composition operator expresses itself in the ability of a process $P \mid Q \mid R$, say, to evolve through any of P, Q or R undergoing a derivation. Bisimilarity of pairs of BPPs was shown to be decidable by Christensen, Hirshfeld and Moller [5], but is not known to be elementary.

Is is natural to consider processes built from atoms using both sequential and parallel composition operators. As before, derivations on atoms may be defined by a grammar, the productions of which have atoms on the left hand side, and arbitrary terms on the right. The derivation relation extends to terms in the natural way, respecting the commutativity of parallel composition; so that, for example, if $U, X, Y, Z \in \mathrm{Atom}$ and $U \xrightarrow{a} U'$, $X \xrightarrow{a} X'$, $Y \xrightarrow{a} Y'$ and $Z \xrightarrow{a} Z'$ are possible derivations, then (adopting the convention that "$\cdot$" binds more tightly than "$\mid$"), the process $(U \mid X) \cdot Y \mid Z$ has all of

$$(U' \mid X) \cdot Y \mid Z, \quad (U \mid X') \cdot Y \mid Z \quad \text{and} \quad (U \mid X) \cdot Y \mid Z'$$

as possible derivatives (via action a), but not $(U \mid X) \cdot Y' \mid Z$. This set-up can be viewed as a fragment of the process algebra ACP, the *Algebra of Communicating Processes* of Bergstra and Klop [2]; we refer to this fragment as *PA*. As a model for concurrent systems, PA still lacks the important element of synchronisation (the "C" in "ACP"), but at least it represents step towards the the kind of expressivity that would be required to describe realistic concurrent systems.

An open problem of some years' standing is whether bisimilarity of PA processes is decidable and, if so, how great is its computational complexity. We are not able to provide a complete answer to this question. However, we are able to present a decision procedure for the subclass of "normed" PA processes. The property of being normed applies to processes generally, independently of how they are described (in BPA, BPP, PA, or whatever). A process P is said to be *normed* if, for all P^* that can be reached from P via some sequence of derivations, there is a further sequence of derivations that reduces P^* to ε. For processes described in BPA, BPP or PA, a sufficient condition for being normed is that all atoms $X \in \mathrm{Atom}$ can be reduced to ε via some derivation sequence.

The assumption of normedness seems innocuous; nevertheless, experience suggests that normed processes are easier to cope with than arbitrary ones. For both BPA and BPP, bisimilarity was shown first shown to be decidable for normed processes: in the case of BPA by Baeten, Bergstra and Klop [1], and in the case of BPP by Christensen, Hirshfeld and Moller [4]. Furthermore, Hirshfeld, Jerrum and Moller have presented polynomial-time algorithms for deciding bisimilarity for both normed BPA [7] and normed BPP [8]. The same phenomenon now reappears in the context of PA.

At the core of the problem of deciding bisimilarity of PA processes lies the surprising complexity of interactions that can occur between sequential and parallel composition. In particular, there are situations in which the sequential composition of two processes $P_1 \cdot P_2$ may be equivalent to a parallel composition $Q_1 \mid Q_2$ of two other processes. A trivial example is given by $\mathrm{Atom} = \{X\}$, $\mathrm{Act} = \{a, b\}$ and productions

$$X \xrightarrow{a} X \mid X \quad \text{and} \quad X \xrightarrow{b} \varepsilon,$$

which system is equivalent to the example using sequential composition given earlier. But this is just the simplest case, and the equivalence $P_1 \cdot P_2 \sim Q_1 \mid Q_2$ in fact has an infinite set of solutions of apparently unbounded complexity.

The key to our approach is to develop a structure theory for PA that completely classifies the situations in which a sequential composition of two processes can be bisimilar to a parallel composition. Fortunately, the infinite collection of examples mentioned earlier can be covered using a small number of patterns (applied recursively). As a consequence of the classification we obtain a decision procedure for bisimilarity in normed PA. Unfortunately, the structure theory we develop relies crucially on unique decomposition of processes into sequential and parallel prime components, which in turn relies of normedness, so there seems little hope of a direct extension to the general (un-normed) case.

It is a chastening thought that we have absolutely no information concerning the complexity of deciding bisimilarity for general (un-normed) PA: the two extremes—that bisimilarity is in the class P, or that it is undecidable—are perfectly consistent with our current lack of knowledge.

2 Notation and Basic facts about PA

Here, we collect together many definitions that are standard in the area. Because they are numerous and routine, we shall not explicitly flag definitions as such in this section.

Recall that Atom is a finite set of *atomic processes* or *atoms*, and Act a finite set of *actions*. We let U, X, Y, Z stand for generic atoms, and a, b, c

Atoms, actions and processes.

for generic actions; other naming conventions will be introduced as and when convenient. The set Proc of *processes* contains all terms in the free algebra over Atom generated by the non-commutative associative operator "$\cdot$" of *sequential composition*, and the commutative associative operator "$|$" of *parallel composition.*

PA process, derivation, immediate derivative.

A PA process is defined by a finite set Π of *productions*, each of the form

$$X \xrightarrow{a} P, \tag{1}$$

where $X \in$ Atom, $a \in$ Act and $P \in$ Proc. A production such as (1) specifies a *derivation* available to X: atomic process X undergoes action a to become process P. The notion of derivation may be extended to arbitrary processes $P \in$ Proc in the natural way:

- if $P \xrightarrow{a} P'$ then $P \cdot Q \xrightarrow{a} P' \cdot Q$;
- if $P \xrightarrow{a} P'$ then $P \mid Q \xrightarrow{a} P' \mid Q$;
- if $Q \xrightarrow{a} Q'$ then $P \mid Q \xrightarrow{a} P \mid Q'$.

(The last rule adds nothing new, but is included to emphasise the commutative nature of parallel composition.) If $P \xrightarrow{a} Q$ for some action a we say that Q is an *immediate derivative* of P. We drop the label a from the derivation $P \xrightarrow{a} Q$ in cases where the associated action a is unimportant.

Derivative, labelled transition system.

We write $P \leadsto P^*$—and say that P^* is a *derivative* of P—if there is some sequence of processes $P_0, P_1, \ldots, P_l$ such that

$$P = P_0 \to P_1 \to \cdots \to P_{l-1} \to P_l = P^*;$$

the number l is the *length* of the derivation sequence. Note that an immediate derivative corresponds to the special case $l = 1$. We shall typically use P' to denote an immediate derivative of P, and P^* to denote a (general) derivative. The collection of all derivations defines a structure known as a *labelled transition system*: formally, this is just a labelled directed multigraph on vertex set Proc, in which there is an edge labelled a from P to P' precisely when $P \xrightarrow{a} P'$. Note that the finite set of productions Π may define an infinite labelled transition system.

Notational conventions.

When writing PA processes we adopt a couple of conventions: sequential composition binds more tightly than parallel composition, and exponentiation is used to denote a parallel composition of several copies of a process, thus

$$P^k = \underbrace{P \mid \ldots \mid P}_{k \text{ copies}}.$$

Norm, reduction, immediate reduct, reduct.

The norm $\|P\|$ of a process $P \in$ Proc is the length of a shortest derivation sequence $P \leadsto \varepsilon$ if such a sequence exists, and ∞ otherwise. A process P is said to be *normed* if every derivative P^* of P has finite norm. Note that if all atoms $X \in \mathrm{Act}$ have finite norm, than all processes $P \in \mathrm{Proc}$ will be normed. A *reduction* is a derivation $P \xrightarrow{a} P'$ that reduces norm, i.e., $\|P'\| < \|P\|$; we say that P' is an *immediate reduct* of P. Note that if $P \xrightarrow{a} P'$ is any reduction then $\|P'\| = \|P\| - 1$. A (general) *reduct* of P is any process P^* that can be reached from P via a sequence of reductions.

Observation 2.1 *If* P *and* Q *have finite norm, then* $\|P \cdot Q\| = \|P \mid Q\| = \|P\| + \|Q\|$.

A binary relation $\mathcal{R}$ on Proc is a *bisimulation* if the following conditions are satisfied:

Bisimulation relation, bisimilarity (or bisimulation equivalence).

- for all $P, Q, P' \in \mathrm{Proc}$ and $a \in \mathrm{Act}$ such that $P \mathrel{\mathcal{R}} Q$ and $P \xrightarrow{a} P'$, there exists $Q' \in \mathrm{Proc}$ such that $Q \xrightarrow{a} Q'$ and $P' \mathrel{\mathcal{R}} Q'$; and
- for all $P, Q, Q' \in \mathrm{Proc}$ and $a \in \mathrm{Act}$ such that $P \mathrel{\mathcal{R}} Q$ and $Q \xrightarrow{a} Q'$, there exists $P' \in \mathrm{Proc}$ such that $P \xrightarrow{a} P'$ and $P' \mathrel{\mathcal{R}} Q'$.

The property of being a bisimulation is closed under union, so there is a unique maximal bisimulation that we shall denote by "$\sim$". Two processes P, Q such that $P \sim Q$ are said to be *bisimilar* or *bisimulation equivalent*. Note that bisimilarity is well defined for PA, being invariant under rearrangement of terms, using associativity of sequential composition and associativity and commutativity of parallel composition.

By way of example, suppose $\mathrm{Atom} = \{H, K, X\}$, $\mathrm{Act} = \{a, b, c\}$, and Π is the set of productions

An example of a pair of bisimilar processes.

$$\begin{array}{lll} X \xrightarrow{a} X^2, & K \xrightarrow{c} X, & H \xrightarrow{c} K \mid X^2 \\ X \xrightarrow{b} \varepsilon, & K \xrightarrow{c} K \mid X, & H \xrightarrow{c} H \mid X \end{array}$$

Then

$$H \cdot X \sim K \cdot X \mid K \cdot X, \tag{2}$$

as can be verified by explicit construction of a bisimulation R containing the pair $\langle H \cdot X,\ K \cdot X \mid K \cdot X \rangle$:

$$\begin{aligned} R = {} & \{ \langle (H \mid X^{i+j}) \cdot X,\ (K \mid X^i) \cdot X \mid (K \mid X^j) \cdot X \rangle : i, j \in \mathbb{N} \} \\ & \cup \{ \langle (K \mid X^{i+j+1}) \cdot X,\ (K \mid X^i) \cdot X \mid X^j \cdot X \rangle : i, j \in \mathbb{N} \} \\ & \cup \{ \langle (K \mid X^{i+j}) \cdot X,\ (K \mid X^i) \cdot X \mid X^j \rangle : i, j \in \mathbb{N} \} \\ & \cup \{ \langle X^{i+j+1} \cdot X,\ X^i \cdot X \mid X^j \cdot X \rangle : i, j \in \mathbb{N} \} \\ & \cup \{ \langle X^{i+j} \cdot X,\ X^i \cdot X \mid X^j \rangle : i, j \in \mathbb{N} \} \\ & \cup \{ \langle X^i \cdot X,\ X^{i+1} \rangle : i \in \mathbb{N} \}. \end{aligned}$$

It is a routine exercise to check that R satisfies the definition of a bisimulation.

This relatively simple example hints at the technical difficulties that lie at the heart of the problem of deciding bisimilarity of PA processes: observe that an equation such as (2) may hold even though the l.h.s. is formally a sequential composition and the r.h.s. a parallel composition, and even though both sides are infinite state (i.e., the set of processes reachable from either side is infinite).

The bisimulation relation on PA processes possesses algebraic structure which is crucial to our decision procedure.

Bisimilarity is a congruence.

Observation 2.2 *Bisimulation equivalence is a congruence under sequential and parallel composition. That is,*

$$P \cdot R \sim Q \cdot R, \quad R \cdot P \sim R \cdot Q \quad \text{and} \quad P \mid R \sim Q \mid R,$$

for all P, Q, R *satisfying* $P \sim Q$.

Note that Observation 2.2 holds even if the some of the processes involved have infinite norm.

Sequential and parallel primes.

For normed processes the situation is even better. We say that a normed process P is a *sequential prime* (respectively a *parallel prime*) if it is not bisimilar to any process of the form $P_1 \cdot P_2$ (respectively $P_1 \mid P_2$) with $\|P_1\|, \|P_2\| > 0$. The use of the term "prime" here is justified by the following facts.

Unique sequential decomposition.

Proposition 2.3 *Suppose*

$$P_1 \cdot P_2 \cdot \cdots \cdot P_n \sim Q_1 \cdot Q_2 \cdot \cdots \cdot Q_m,$$

where the processes P_i *and* Q_j *are sequential primes of finite norm. Then* $n = m$, *and* $P_i \sim Q_i$, *for all* $1 \leq i \leq n$.

Proof. See, for example, Hirshfeld et al. [7]. □

Unique parallel decomposition.

Proposition 2.4 *Suppose*

$$P_1 \mid P_2 \mid \ldots \mid P_n \sim Q_1 \mid Q_2 \mid \ldots \mid Q_m,$$

where the processes P_i *and* Q_j *are parallel primes of finite norm. Then* $n = m$, *and there exists a permutation* π *of the integers* $\{1, 2, \ldots, n\}$ *such that* $P_i \sim Q_{\pi(i)}$, *for all* $1 \leq i \leq n$.

Proof. See, for example, Christensen et al. [4]. □

(The phenomenon of unique decomposability of processes was first noted by Milner and Moller [10].) Note that Propositions 2.3 and 2.4 require the component processes to have finite norm. It is because we make extensive use of unique decomposition that our decision procedure is restricted to normed processes.

Cancellation rules.

Note also that Propositions 2.3 and 2.4 imply a converse to Observation 2.2, which allows cancellation of like components. Thus, if P, Q, R are normed and $P \cdot R \sim Q \cdot R$, then $P \sim Q$. In fact, the cancelled processes do not need to be equal, merely bisimilar. Similar cancellation rules can be formulated for the other two cases in Observation 2.2. Cancellation fails for general (possibly infinite norm) processes.

3 Outline of the decidability proof

The full proof of decidability is long and technically involved, so we offer in this section a rough guide to its main features.

To motivate the approach, let us attempt to build a (non-deterministic) decision procedure directly from the definition of bisimilarity. Given a pair or processes $\langle P, Q \rangle$, we wish to decide whether $P \sim Q$. We try all derivations $P \xrightarrow{a} P'$ (note that there are finitely many) and for each one guess a matching derivation $Q \xrightarrow{a} Q'$. (By "matching" derivation we mean one for which $P' \sim Q'$.) Symmetrically, for each derivation $Q \xrightarrow{a} Q'$ we guess a matching derivation $P \xrightarrow{a} P'$. Let us call the process of generating all pairs $\langle P', Q' \rangle$ derived from $\langle P, Q \rangle$ an "expansion step." If there exists a derivation $P \xrightarrow{a} P'$ that is not matched by any derivation $Q \xrightarrow{a} Q'$ (i.e., Q is incapable of performing action a), we say the expansion step fails; in this case, we immediately halt and reject.

Otherwise we consider all the derived pairs of processes $\langle P', Q' \rangle$ and apply the expansion step to *them* to build a second level of derived processes, and then a third, and so on. If $P \sim Q$ then the nondeterministic choices can be made so that no expansion step fails. Conversely, if $P \not\sim Q$ then, eventually, some expansion step must fail, whatever nondeterministic choices are made.

The main (and only) objection to the above approach is that the derived processes can grow without limit, so that the procedure will not in general terminate in the case $P \sim Q$. We counter this objection by combining the expansion step with a complementary simplification step that cuts in when the norm of P and Q becomes larger than the norm of any atom. In this situation, P and Q must either be sequential or parallel compositions. If P and Q are of the same kind—both sequential or both parallel—the simplification step is straightforward. For example, if $P = P_1 \cdot P_2$ and $Q = Q_1 \cdot Q_2$ with $\|P_1\| \geq \|Q_1\|$, then we guess a process R with norm $\|R\| = \|P_1\| - \|Q_1\|$; then we replace the pair $\langle P, Q \rangle$ by the two smaller pairs $\langle P_1, Q_1 \cdot R \rangle$ and $\langle R \cdot P_2, Q_2 \rangle$. This is an appropriate action, since, by unique factorisation,

$$P \sim Q \iff \exists R \left[P_1 \sim Q_1 \cdot R \wedge R \cdot P_2 \sim Q_2 \right].$$

A similar simplification step is available when P and Q are both parallel compositions.

The difficult case for simplification is when (say) P is a sequential composition, and Q a parallel composition, leading to a so-called "mixed equation." For this case we develop a structure theory that classifies the situations when $P \sim Q$. The range of possible mixed equations is remarkably rich, and it is this fact that leads to the technical complexities of the proof. Nevertheless, the classification can be described with sufficient precision to allow the simplification step described above to be extended to mixed equations.

An overview of the structure theory is presented in Figure 1. For the few readers who wish to brave the full proof presented in later sections, we hope Fig-

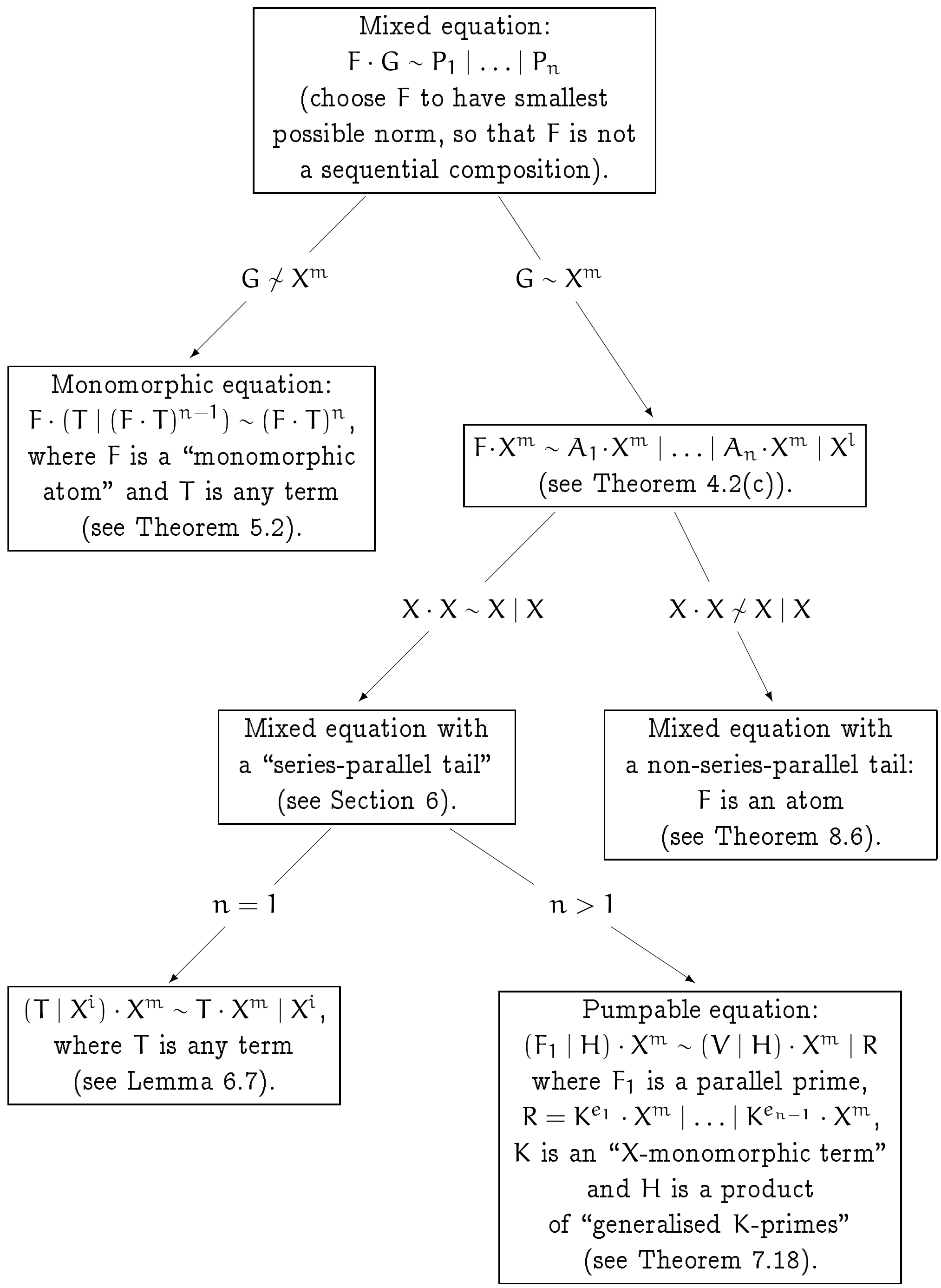

Figure 1: Outline of the structure theory for mixed equations

ure 1 will provide a useful map; for the majority, Figure 1, taken in conjunction with the referenced theorems and Section 9, will probably prove sufficient.

4 Mixed equations: preliminaries and normal form

Our procedure for deciding bisimilarity in PA relies on having a complete classification of the circumstances in which a sequential composition of two processes can be bisimilar to a parallel composition.

Definition 4.1 *A* mixed equation *is an equivalence of the form*

Mixed equation, minimal mixed equation, unit.

$$F \cdot G \sim P_1 \mid \cdots \mid P_n, \tag{3}$$

where $P_1, \ldots, P_n$ *are parallel primes, and* $n \geq 2$*. We say that (3) is a* minimal mixed equation *if* $\|F\| = 1$*; in this case,* F *is necessarily an atom of norm one, or* unit*. We reserve the letters* X*,* Y *and* Z *to stand for units.*

Our basic normal-form theorem for mixed equations follows after technical lemma.

Lemma 4.1 *Let* $T = P_1 \mid P_2 \mid \cdots \mid P_n$ *be a decomposition of a process* T *into parallel primes. If all the immediate reducts of* T *are bisimilar to each other then* $P_1 \sim P_2 \sim \cdots \sim P_n \sim P$*, i.e.,* $T \sim P^n$ *is a (parallel) power. Furthermore,* P *has a unique immediate reduct (up to bisimulation).*

Proof. Let T' be the unique immediate reduct on the l.h.s., so that $T \to T'$ with $\|T'\| < \|T\|$. Let P_i and P_j be two factors on the r.h.s., and $P \to P_i'$, $P \to P_j'$ be two immediate reducts. By assumption,

$$P_1 \mid \cdots \mid P_i' \mid \cdots \mid P_j \mid \cdots \mid P_n \sim P_1 \mid \cdots \mid P_i \mid \cdots \mid P_j' \mid \cdots \mid P_n,$$

and, by unique decomposition, $P_i' \mid P_j \sim P_i \mid P_j'$. The prime process P_i is either bisimilar to the prime P_j or to a component of P_i', and, since $\|P_i'\| < \|P_i\|$, we must conclude the former. The final part of the lemma is again an easy consequence of unique factorisation. □

Theorem 4.2 *(a) In a minimal mixed equation, all the components on the r.h.s. are bisimilar to each other:*

Normal-form theorem for mixed equations.

$$Y \cdot G \sim P^n \quad \text{and} \quad G \sim P' \mid P^{n-1}, \tag{4}$$

where P' *is the unique reduct of* P*.*

(b) Every mixed equation can be reduced to a minimal mixed equation, which is unique up to bisimilarity.

(c) *If* $||F|| > 1$ *then there is a unit* X *such that* $G \sim X^m$*, and each component* P_i *is bisimilar either to* X *or to a sequential composition of the form* $A \cdot X^m$ *(the same* m *as in the decomposition of* G*). Thus the normal form for mixed equations with* $||F|| > 1$ *is*

$$F \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l. \tag{5}$$

(d) *The minimal equation obtained by reducing equation (5) is*

$$Y \cdot X^m \sim X^{m+1}, \tag{6}$$

where Y *is a unit.*

(e) *Every immediate derivative of* X *is bisimilar either to some power of* X*, or to a sequential composition* $B \cdot X^m$ *(the same* m *as in the decomposition of* G*). In particular, if* $m \geq \max\{||X'|| : X \rightarrow X'\}$*, then every derivative of* X *is bisimilar to a power of* X*.*

Proof. If $||F|| = 1$ in equation (3) then $F \cdot G$ has a unique immediate reduct. By Lemma 4.1, the r.h.s. of equation (3) is a power. This gives part (a) of the lemma.

If $||F|| > 1$ then reduce the r.h.s. for $||F|| - 1$ steps, always selecting a component of largest norm. No component will disappear before they are all of norm 1, so that by the time the l.h.s. becomes $Y \cdot G$, with Y a unit, the r.h.s. is still a parallel composition. Since the only immediate reduct on the l.h.s. is G, we conclude from Lemma 4.1 that the r.h.s. is a power:

$$Y \cdot G \sim Q^n \quad \text{and} \quad G \sim Q' \mid Q^{n-1}. \tag{7}$$

If an alternative derivation sequence leads to $\widehat{Y} \cdot G$ on the l.h.s. and a parallel composition on the r.h.s., where $\widehat{Y}$ is a unit, then, for the same reasons,

$$\widehat{Y} \cdot G \sim \widehat{Q}^{\hat{n}} \quad \text{and} \quad G \sim \widehat{Q}' \mid \widehat{Q}^{\hat{n}-1}.$$

Comparing the two expressions for G we see that $Q \sim \widehat{Q}$ and $n = \hat{n}$, since Q and $\widehat{Q}$ are both parallel primes. But then $Y \sim \widehat{Y}$ also, by unique sequential decomposition of $Q^n \sim \widehat{Q}^{\hat{n}}$. This proves (b).

If $||F|| > 1$, then in reducing F to Y the final step was $F^* \rightarrow Y$, so that the original equation evolved into

$$F^* \cdot G \sim Q_1 \mid Q_2 \mid \cdots \mid Q_r, \tag{8}$$

where we assume that the r.h.s. is fully factorised. Note that $r \geq 2$, since the reduction was done in such a way as to preserve the parallel composition. By part (b), any reduction on the r.h.s. of (8) that retains its parallel form leads to minimal equation (7). Without loss of generality, we assume that $Q_1 \rightarrow Q_1'$ reduces (8) to the minimal equation, so that

$$Q_1' \mid Q_2 \mid \cdots \mid Q_r \sim Q^n.$$

Hence $Q_2 \sim Q$. We shall show that $\|Q\| = 1$. Assume to the contrary that $\|Q\| > 1$. Then reducing Q_2 in equation (8) also retains the parallel form on the r.h.s., so that also

$$Q_1 \mid Q_2' \mid \cdots \mid Q_r \sim Q^n,$$

which is impossible, since $\|Q_2'\| < \|Q\|$ and Q is a parallel prime. Thus Q is a unit and we denote it by X. Clearly, $G \sim X^m$, where $m = \|G\|$ and the original equation (3) becomes

$$F \cdot X^m \sim P_1 \mid \cdots \mid P_n.$$

For each P_i we may eliminate on the right all the components except P_i. If $\|P_i\| \leq m$ we end up with $X^k \sim P_i$, for some $k \leq m$; and if $\|P_i\| > m$ with $F^* \cdot X^m \sim P_i$. This proves (c), with the component X^l accumulating all the components P_i with $\|P_i\| \leq m$.

Part (d) is an easy exercise: reduce each A_i on the r.h.s. to ε, and then reduce X's as necessary.

Finally, starting with equation (6), we analyse the possible derivatives of X. Assume that $X \to X'$, so that $X^{m+1} \to X' \mid X^m$ on the r.h.s. of (6). The l.h.s. follows with $Y \cdot X^m \to Y' \cdot X^m$. Hence $Y' \cdot X^m \sim X' \mid X^m$. Now eliminate the X^m on the right to obtain either $Y^* \cdot X^m \sim X'$ or $X^k \sim X'$, for some $k \leq m$. This completes part (e), and the proof of the lemma. □

5 Monomorphic equations

The analysis of mixed equations of form (5), in which G is a power of a unit, requires considerable work, which we leave to later sections. In this section we analyse the complementary case, which turns out to be much more tractable. By Theorem 4.2(c), we already know that $\|F\| = 1$; however, more can be said.

Definition 5.1 *We say that an atom is* monomorphic *if* $Y \to Y'$ *implies* $Y' \sim Y$ *or* $Y' \sim \varepsilon$.

Monomorphic atom.

Since Y is normed, $\|Y\| = 1$, so that only units may have this property.

Observation 5.1 *It is easy to decide if an atom is monomorphic, and if two monomorphic atoms are bisimilar. For convenience, we may modify the productions, keeping only one atom from each equivalence class (under bisimilarity) of monomorphic atoms, so that the only derivatives of a monomorphic atom* Y *are* Y *and* ε.

If Y is monomorphic then, for every term T and every $n \geq 2$, the following mixed equation holds:

$$Y \cdot (T \mid (Y \cdot T)^{n-1}) \sim (Y \cdot T)^n. \tag{9}$$

Definition 5.2 *An equation of the form (9), with* Y *a monomorphic atom, is called a* monomorphic equation.

Monomorphic equation.

We shall see that this family includes all instances of mixed equations that are not of the form (5).

Sufficient condition for an equation to be monomorphic.

Theorem 5.2 *If* G *is not bisimilar to the power of a unit, then the mixed equation* $F \cdot G \sim P_1 \mid \cdots \mid P_n$ *must be monomorphic:* F *is a monomorphic atom,* $P_i \sim P \sim F \cdot T$ *for some fixed* T*, and* $G \sim T \mid (F \cdot T)^{n-1}$*.*

Proof. Since G is not the power of a unit, we know from Theorem 4.2(c) that $||F|| = 1$, and from Theorem 4.2(a) that the r.h.s. is a power of some parallel prime P, i.e., $F \cdot G \sim P^n$. Moreover, P has a unique reduction $P \longrightarrow P'$, leading to $G \sim P' \mid P^{n-1}$. Assume that $F \longrightarrow \widehat{F} \not\sim \varepsilon$, so that $F \cdot G \longrightarrow \widehat{F} \cdot G$. The r.h.s. of the mixed equation responds with $P \longrightarrow \widehat{P}$, leading to

$$\widehat{F} \cdot G \sim \widehat{P} \mid P^{n-1}.$$

Since this is again a mixed equation, and G is still not a power of an atom, we again conclude that $||\widehat{F}|| = 1$, and the r.h.s. is a power with $||\widehat{P}|| = ||P||$. Necessarily, $\widehat{P} \sim P$, so that the r.h.s., and hence the l.h.s., remains the same, up to bisimilarity. Thus $\widehat{F} \sim F$, and F is monomorphic. Note that our analysis also showed that if $F \longrightarrow F$ then $P \longrightarrow P$, and if $F \longrightarrow \varepsilon$ then $P \longrightarrow P'$; and since F has no other move, P has no other move. It is therefore easy to see that $P \sim F \cdot P'$. Thus every mixed equation is either of form (5) or (9). □

As a corollary, we have a result that helps us analyse the situation when F in equation (5) is a sequential composition. (The bulk of the structure theory is concerned with the case of a parallel composition.)

Structure of mixed equations with a sequential composition on the l.h.s.

Corollary 5.3 *Consider the mixed equation*

$$(F_1 \cdot F_2) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l, \tag{10}$$

where the r.h.s. is a non-trivial ($n + l \geq 2$) parallel prime decomposition. One of the following two situations obtains:

- $F_2 \cdot X^m \sim X^{m+k}$ *and* $A_i \cdot X^m \sim B_i \cdot X^{m+k}$ *(with appropriately chosen* B_i*), so equation (10) is equivalent to*

$$F_1 \cdot X^{m+k} \sim B_1 \cdot X^{m+k} \mid \cdots \mid B_n \cdot X^{m+k} \mid X^l;$$

- *equation (10) is monomorphic, i.e.,*

$$F_1 \cdot (F_2 \cdot X^m) \sim (A \cdot X^m)^n,$$

where F_1 *is a monomorphic atom,* $A \sim F_1 \cdot A'$ *(where* A' *is the unique reduct of* A*), and*

$$F_2 \cdot X^m \sim A' \cdot X^m \mid (A \cdot X^m)^{n-1}.$$

Proof. Setting $G = F_2 \cdot X^m$, equation (10) becomes

$$F_1 \cdot G \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l. \qquad (11)$$

If G is bisimilar to a power of a unit, say $G \sim Y^{m+k}$ where $k = \|F_2\|$, then after some reductions, we discover that $Y \sim X$. Starting with $F_1 \cdot X^{m+k}$ on the l.h.s. and eliminating all but $A_i \cdot X^m$ on the r.h.s., we get $F_1^* \cdot X^{m+k} \sim A_i \cdot X^m$. (Note that $\|F_1^*\| > 0$ since $A_i \cdot X^m$ is a parallel prime.) This deals with the first possibility.

If G is not bisimilar to a power of a unit, then equation (11) is a monomorphic equation by Theorem 5.2. Necessarily, $A_i \cdot X^m$ is the P of Theorem 5.2, and F_1 the F of that theorem. □

6 Mixed equations with a series-parallel tail

If X is monomorphic then $X \cdot X \sim X \mid X$. This equation may also arise when X is not monomorphic, e.g., if X is defined by the transition rules

$$X \xrightarrow{a} \varepsilon, \quad X \xrightarrow{b} X \cdot X, \quad \text{and} \quad X \xrightarrow{c} X \mid X.$$

This breeds some more mixed equations, such as

$$(A \mid X) \cdot X^3 \sim A \cdot X^3 \mid X,$$

where A is any term.

Before classifying such equations, we shall present some useful alternative formulations of the "series-parallel" property $X \cdot X \sim X \mid X$.

Definition 6.1 *For any atom X, an* X-term *is a term built from the atom X using the operations of sequential and parallel composition. An* extended X-term *is a term that is bisimilar to an X-term.*

X-term, extended X-term.

For any term T and action $a \in \text{Act}$, denote by $\delta_a(T)$ the set

$$\delta_a(T) = \{k : \text{there exists } T' \text{ such that } T \xrightarrow{a} T' \text{ and } \|T'\| - \|T\| = k\}. \qquad (12)$$

Lemma 6.1 *Let $T \neq \varepsilon$ be an extended X-term. Then:*

(a) $\delta_a(T) = \delta_a(X)$, for all $a \in \text{Act}$;

(b) if all the immediate derivatives of X are extended X-terms, then all the immediate derivatives of T are extended X-terms.

Proof. For T an X-term, the claims are proved by structural induction. For T an extended X-term, part (a) holds because bisimulation preserves norm, and part (b) follows immediately from the definition of extended X-term. □

Lemma 6.2 *Let X be an atom. The following are equivalent statements of the series-parallel property:*

(i) $X \cdot X \sim X \mid X$;

(ii) every derivative of X *is an extended* X*-term;*

(iii) two (extended) X*-terms are bisimilar iff they have the same norm;*

(iv) X *satisfies a mixed equation*

$$F \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l,$$

(n may be 0), where m is bigger than the norm of any immediate derivative of X.

Proof. The equivalence of (i)–(iv) follows from the sequence of entailments: (i) $\Rightarrow$ (ii), (ii) $\Rightarrow$ (iii), (iii) $\Rightarrow$ (i), (iii) $\Rightarrow$ (iv) and (iv) $\Rightarrow$ (ii).

(i) $\Rightarrow$ (ii): Assume to the contrary that $X \rightsquigarrow T$, where T is the derivative with smallest norm that is not an extended X-term. The sequence of moves $X \mid X \rightsquigarrow X \mid T$ on the r.h.s. is matched on the l.h.s. by a sequence of moves $X \rightsquigarrow S$ such that $S \cdot X \sim X \mid T$. (Note that the first X on the l.h.s. cannot disappear.) We now eliminate X to get $S' \cdot X \sim T$. Since $X \rightsquigarrow S'$ and $\|S'\| < \|T\|$ we conclude that S' is an extended X-term. But then so is $S' \cdot X$ and hence T, a contradiction.

(ii) $\Rightarrow$ (iii): Observe that, by Lemma 6.1, the relation

$$\{\langle T, S\rangle : \|T\| = \|S\|, \text{ and } T \text{ and } S \text{ are both extended } X\text{-terms}\}$$

is a bisimulation.

(iii) $\Rightarrow$ (i): This entailment is immediate.

(iii) $\Rightarrow$ (iv): This follows from the equation $X^m \cdot X^m \sim X^m \mid X^m$, which holds for arbitrarily high m.

(iv) $\Rightarrow$ (ii): This is just Theorem 4.2(e). □

Corollary 6.3 *Suppose X is a series-parallel atom, so that $X \cdot X \sim X \mid X$. Then:*

(a) if T is an extended X-term then $T \sim X^{\|T\|}$;

(b) every subterm of an extended X-term is an extended X-term.

Proof. Part (a) is a special case of the equivalence of (i) and (iii) in Lemma 6.2.

Suppose that T is a minimal counterexample to part (b). If $T = T_1 \cdot T_2$ then by the equivalence of (i) and (iii) in Lemma 6.2,

$$T \sim \underbrace{X \cdot X \cdot \ \cdots \ \cdot X}_{\|T\| \text{ copies}},$$

so by unique sequential decomposition,

$$T_1 \sim \underbrace{X \cdot X \cdot \ \cdots \ \cdot X}_{\|T_1\| \text{ copies}} \quad \text{and} \quad T_2 \sim \underbrace{X \cdot X \cdot \ \cdots \ \cdot X}_{\|T_2\| \text{ copies}}:$$

Step 1: Let $\mathcal{A}(X)$ be the set of all atoms occurring as subterms in derivatives of X. Compute $\mathcal{A}(X)$ by forming the transitive closure of the following binary relation on atoms:

$$\{\langle U, U' \rangle : U' \text{ is a subterm in an immediate derivative of } U\}.$$

Step 2: Test, for all atoms $U \in \mathcal{A}(X)$ and all actions $a \in \mathrm{Act}$, whether

$$\delta_a(U) = \delta_a(X), \quad (13)$$

where δ_a is as defined in (12); accept if equality (13) holds for all choices of U and a, and reject otherwise.

Figure 2: A procedure for deciding $X \cdot X \sim X \mid X$.

a contradiction to minimality. Similarly, if $T = T_1 \mid T_2$ then $T \sim X^{\|T\|}$ and hence, by unique parallel decomposition, $T_1 \sim X^{\|T_1\|}$ and $T_2 \sim X^{\|T_2\|}$: again a contradiction. □

In the light of Lemma 6.2 and Corollary 6.3, the series-parallel property ought to be easy to test. This is indeed so, and Figure 2 presents a decision procedure.

Lemma 6.4 *The algorithm in Figure 2 correctly decides* $X \cdot X \sim X \mid X$.

Proof. First suppose X is series-parallel, i.e., $X \cdot X \sim X \mid X$. For every $U \in \mathcal{A}(X)$ there is, by definition, some derivative T of X which contains U as a subterm. By the equivalence of (i) and (ii) in Lemma 6.2, T is an extended X-term, and hence, by Corollary 6.3, $U \sim X^{\|U\|}$. Thus equality (13) is satisfied for all $U \in \mathcal{A}(X)$ and $a \in \mathrm{Act}$, and the procedure accepts.

Conversely, suppose that the procedure accepts, so that equality (13) holds for all $U \in \mathcal{A}(X)$ and $a \in \mathrm{Act}$. It is easy to check that the relation

$$\{\langle T, X^{\|T\|} \rangle : T \text{ is a term such that } X \rightsquigarrow T\}$$

is a bisimulation. Thus X is series-parallel by the equivalence of (i) and (ii) in Lemma 6.2. □

Definition 6.2 *Let* T *be a term. The* X-norm $\|T\|_X$ of T *is the length of the shortest norm-reducing sequence* $T \rightsquigarrow S$*, where* S *is an extended* X*-term. (Note that every step in the sequence is required to reduce the usual norm.) An* (immediate) X-reduction *of a term* T *is an (immediate) derivation* $T \rightarrow S$ *that decreases both the (usual) norm and the* X*-norm, i.e.,* $\|S\| < \|T\|$ *and* $\|S\|_X < \|T\|_X$*. In this case, we say that* S *is an* (immediate) X-reduct *of* T. X-norm, X-reduction, X-reduct.

Note that if T is an extended X-term then $||\mathsf{T}||_X = 0$; otherwise, T has finite X-norm $||\mathsf{T}||_X \leq ||\mathsf{T}||$ and there is at least one X-reduction of T. (The X-reduction necessarily reduces both norms by 1.)

Properties of X-norm.

Observation 6.5 *The* X*-norm has similar properties to the norm:*

(a) if $\mathsf{T} \sim \mathsf{S}$ *then* $||\mathsf{T}||_X = ||\mathsf{S}||_X$*;*

(b) $||\mathsf{T} \mid \mathsf{S}||_X = ||\mathsf{T}||_X + ||\mathsf{S}||_X$*;*

(c) $||\mathsf{T} \cdot \mathsf{S}||_X \geq ||\mathsf{T}||_X + ||\mathsf{S}||_X$*;*

(d) $||\mathsf{T} \cdot \mathsf{S}||_X = ||\mathsf{T}||_X$ *if* S *is an* X*-term; in particular, in the equation*

$$\mathsf{F} \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l$$

we have $||\mathsf{F}||_X = ||A_1||_X + \cdots + ||A_n||_X$*.*

X-unit, X-free.

Definition 6.3 *If* $||\mathsf{K}||_X = 1$ *we say that* K *is an* X-unit*. A term* T *is* X-free *if its decomposition into parallel primes does not contain a component bisimilar to* X*, i.e.,* T *cannot be expressed in the form* $\mathsf{T} \sim \mathsf{S} \mid X$ *for some* S*. We reserve the letter* K *(possibly subscripted) to stand for an* X*-unit.*

Note that an X-unit may have norm greater than one, and is not in general an atom. The following lemma is a major tool in our analysis.

Lemma 6.6 *Suppose* X *is series-parallel, i.e.,* $X \cdot X \sim X \mid X$*.*

(a) If K *is an* X*-unit then it has a unique (up to bisimilarity)* X*-reduct* K'*; necessarily* K' *is an* X*-term and hence* $\mathsf{K}' \sim X^{||\mathsf{K}||-1}$*.*

(b) Suppose $\mathsf{T} \sim P_1 \mid P_2 \mid \cdots \mid P_n$ *is a decomposition of a process* T *into parallel primes. If* T *is* X*-free and has a unique* X*-reduction (up to bisimilarity) then* $P_1 \sim P_2 \sim \cdots \sim P_n$*.*

Proof. To see part (a), observe that all the X-reductions of K lead to an extended X-term with norm $||\mathsf{K}|| - 1$; by Corollary 6.3, all such terms are bisimilar to $X^{||\mathsf{K}||-1}$ and hence to each other.

For (b), note that each P_i has positive X-norm and a (unique) X-reduct P_i'. By assumption,

$$P_1' \mid \cdots \mid P_i \mid \cdots \mid P_n \sim P_1 \mid \cdots \mid P_i' \mid \cdots \mid P_n,$$

for all i. By unique decomposition, $P_1' \mid P_i \sim P_1 \mid P_i'$, and P_1 is a parallel component of $P_1' \mid P_i$. Since $||P_1|| > ||P_1'||$ and P_1 and P_i are prime, $P_1 \sim P_i$. □

The sample mixed equation that opened the section is a special case of a general pattern.

Lemma 6.7 *Suppose* X *is series-parallel. For every term* T*, and every* i *and* m*:*

$$(T \mid X^i) \cdot X^m \sim T \cdot X^m \mid X^i. \tag{14}$$

Proof. If S is an X-term then $S \cdot X^m \sim X^m \mid S$, by the equivalence of (i) and (iii) in Lemma 6.2. Hence the relation

$$\left\{ \left\langle (T \mid S) \cdot X^m, T \cdot X^m \mid S \right\rangle : S \text{ is an } X\text{-term and } T \text{ is an arbitrary term} \right\}$$

is a bisimulation. □

7 Pumpable equations

In this section we explore the series-parallel case further. Recall that, in the generic mixed equation (5), n stands for the number of components with positive X-norm on the r.h.s., and F denotes the first (sequential) component on the l.h.s. Lemma 6.7 gives a potentially infinite family of mixed equations with $n = 1$; as we shall see, there may be other infinite families of mixed equations with $n \geq 2$.

Since Corollary 5.3 enables us to handle the cases where F is a sequential composition, we concentrate in this section on classifying the situations in which F is a parallel composition. It turns out that equations of this kind—the "pumpable equations" of the section title—have a rich and interesting structure.

Definition 7.1 *Suppose* X *is series-parallel. A* pumpable equation *is a mixed equation of the form* (margin note: Pumpable equation.)

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l, \tag{15}$$

where $r \geq 2$*,* $n + l \geq 2$*, and* F_i *and* A_j *are* X*-free for* $1 \leq i \leq r$ *and* $1 \leq j \leq n$*.*

The appropriateness of the terminology "pumpable equation" will become apparent towards the end of the section. Note that the assumption that F_i and A_j are X-free is harmless: by Lemma 6.7, if $A_j \sim \widehat{A}_j \mid X$ then the factor X can be pulled out and incorporated into the X^l component. Similarly, if $F_i \sim \widehat{F}_i \mid X$ then, again by Lemma 6.7, X can be pulled out and cancelled with an X on the right (which must exist by unique decomposition).

In retrospect, the r.h.s. of (15) is a little too general, as X cannot in fact occur as a factor. For suppose $l > 0$; then we may apply the reduction $X \to \varepsilon$ to the r.h.s., which, without loss of generality, is matched by $F_1 \to F_1'$ on the l.h.s.:

$$(F_1' \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^{l-1},$$

Then (parallel) composing both sides with X, and applying Lemma 6.7:

$$((F_1' \mid X) \mid F_2 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l$$

By unique factorisation, $F_1 \sim F_1' \mid X$, contradicting X-freeness of F_1. We record this information for future reference.

Observation 7.1 *In a pumpable equation, n (the number of parallel components with positive X-norm on the r.h.s.) is at least two, and l (the number of occurrences of X as a factor) is zero.*

7.1 Basic facts

With the ultimate aim of brevity in mind, we slightly extend one of our earlier definitions.

X-simplification of a term or equation, minimal pumpable equation, X-valence of a term.

Definition 7.2 *Suppose T is an X-free term. We say that an X-free term S is an* X-simplification of T, *and write $T \rightarrow_X S$, if there is an X-reduction $T \rightarrow T' \sim S \mid X^i$ for some i (possibly zero). An* X-simplification *of an equation $T_1 \sim T_2$ is a second equation $S_1 \sim S_2$ obtained by applying bisimilarity-preserving X-simplifications $T_1 \rightarrow_X S_1$ and $T_2 \rightarrow_X S_2$ to the two sides. A pumpable equation is* minimal *if no X-simplification of it is a pumpable equation. The X-valence of a term T is the number of distinct (up to bisimulation equivalence) X-simplifications of T.*

In operational terms an X-simplification of a pumpable equation may be achieved in three steps: (i) apply X-reductions to both sides, (ii) pull any parallel X components to the outer level using Lemma 6.7, and (iii) cancel any parallel X components that are common to the two sides.

Lemma 7.2 *The form of pumpable equations is constrained as follows.*

(a) There are no pumpable equations with X-norm less than three.

(b) There are no pumpable equations with a product of X-units on the l.h.s., i.e., with $\|F_i\|_X = 1$, for all $1 \leq i \leq r$.

(c) Every pumpable equation may be transformed by a series of X-simplifications to a minimal pumpable equation of X-norm three. This minimal equation is necessarily of the form

$$(F \mid K) \cdot X^m \sim K^2 \cdot X^m \mid K \cdot X^m, \tag{16}$$

with $\|F\|_X = 2$ and $\|K\|_X = 1$.

Proof. A pumpable equation trivially has X-norm at least two. To achieve this value, the equation would need to have the form

$$(F_1 \mid F_2) \cdot X^m \sim A_1 \cdot X^m \mid A_2 \cdot X^m, \tag{17}$$

with $\|F_1\|_X = \|F_2\|_X = \|A_1\|_X = \|A_2\|_X = 1$. Suppose, without loss of generality, that the X-simplification of equation (17) annihilating F_1 on the l.h.s. also annihilates A_1 on the r.h.s., so that

$$F_2 \cdot X^m \sim A_2 \cdot X^m,$$

and hence

$$F_2 \sim A_2. \tag{18}$$

In a similar fashion, by employing an X-simplification annihilating F_2, we deduce

$$F_1 \sim A_1 \quad \text{or} \quad F_1 \sim A_2, \tag{19}$$

and by annihilating A_2,

$$F_1 \sim A_1 \quad \text{or} \quad F_2 \sim A_1. \tag{20}$$

It follows easily from assertions (18–20) that $F_1 \sim A_1$ and $F_2 \sim A_2$. But this is impossible, since the (usual) norm of the r.h.s. of equation (17) would then exceed that of the l.h.s. by $m > 0$. This deals with part (a).

Suppose, contrary to part (b) that

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m,$$

where $\|F_i\|_X = 1$ for $1 \leq i \leq r$. Perform $r - 2$ X-simplifications, taking care to maintain at least two components of positive X-norm on the r.h.s. Note that this procedure maintains pumpability, but the X-norm of the resulting equation is just two, contradicting part (a).

Finally to part (c). A minimum pumpable equation must have the form

$$(F \mid K) \cdot X^m \sim A_1 \cdot X^m \mid A_2 \cdot X^m, \tag{21}$$

with $\|K\|_X = \|A_2\|_X = 1$ and $\|F\|_X = \|A_1\|_X \geq 2$, otherwise an X-simplification would be available. (If either side had three parallel components with positive X-norm, or two components of X-norm at least two, then we could X-reduce the component of largest X-norm on the other side.) Moreover, again by minimality, X-simplifications of F must be answered by A_2, and hence there is only one such (up to bisimilarity); and X-simplifications of A_1 must be answered by K. We must show that $\|F\|_X = 2$, $A_1 \sim K^2$ and $A_2 \sim K$.

Applying the X-simplification that annihilates A_2 and reduces $F \to_X F'$ with $\|F'\|_X = \|F\|_X - 1$, we obtain

$$(F' \mid K) \cdot X^m \sim A_1 \cdot X^m,$$

and consequently $A_1 \sim F' \mid K$. Now A_1 has a unique X-simplification, so, by Lemma 6.6(b), $A_1 \sim K^t$ and $F' \sim K^{t-1}$; moreover, $t \geq 2$ by part (a) of this lemma.

Applying to equation (21) the X-simplification that annihilates K and reduces $A_1 \to_X K^{t-1}$, we obtain

$$F \cdot X^m \sim K^{t-1} \cdot X^m \mid A_2 \cdot X^m.$$

Now a further X-simplification, annihilating a K on the r.h.s. and reducing $F \to_X F' \sim K^{t-1}$ on the l.h.s., yields

$$K^{t-1} \cdot X^m \sim K^{t-2} \cdot X^m \mid A_2 \cdot X^m$$

if $t > 2$, and

$$K \cdot X^m \sim A_2 \cdot X^m$$

otherwise. By part (b) of this lemma, the former is impossible, and we must conclude that $\|F\|_X = \|A_1\|_X = t = 2$, $A_1 \sim K^2$ and $A_2 \sim K$. □

Uniqueness of X-units.

Lemma 7.3 *Let*

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m$$

be a pumpable equation. All the (X-free) X-units reachable by (iterated) X-simplification from $F_1, \ldots, F_r$ *and* $A_1, \ldots, A_n$ *are bisimilar to some fixed X-unit, say* K.

Proof. Throughout the proof, X-units will always be X-free. Suppose K is an X-unit reachable from some F_i. Perform repeated X-simplifications on the l.h.s. until only $K \cdot X^m$ remains; the r.h.s. must respond, so K must also reachable from some A_j. A similar argument applies in the other direction, so the set of X-units reachable from the l.h.s. is equal to the set reachable from the r.h.s. Call an equation *heterogeneous* if this set contains more than one element. We start by assuming that heterogeneous pumpable equations exist, and obtain a contradiction.

Consider a heterogeneous equation of minimum X-norm. Assume the F_i are ordered so that $\|F_1\|_X \geq \|F_2\|_X \geq \cdots \geq \|F_r\|_X$ and similarly for the A_j. Observe that $r = 2$ and $\|F_2\|_X = 1$, otherwise we can perform an X-simplification on the r.h.s. that preserves heterogeneity and automatically retains the parallel form of the l.h.s. By an exactly similar argument, $n = 2$ (we know by Observation 7.1 that $n \geq 2$) and $\|A_2\|_X = 1$. So, with some renaming, the minimal counterexample must look like

$$(F \mid K) \cdot X^m \sim A \cdot X^m \mid \widehat{K} \cdot X^m, \tag{22}$$

where K and $\widehat{K}$ are X-units, and $\|F\|_X = \|A\|_X \geq 2$ by Lemma 7.2(a).

Consider an X-simplification $F \to_X F'$ that preserves heterogeneity, i.e., $F' \rightsquigarrow \widetilde{K}$ where $\widetilde{K} \not\sim K$ is an X-unit. By minimality, this X-simplification must be matched on the r.h.s. by $\widehat{K}$, and hence F' is unique (up to bisimilarity). Now perform this X-simplification to obtain

$$(F' \mid K) \cdot X^m \sim A \cdot X^m,$$

and hence $A \sim F' \mid K$. Write $F' \sim H \mid K^i$ with i maximal (possibly zero), so that H does not contain K as a parallel component. Then

$$A \sim H \mid K^{i+1} \tag{23}$$

We distinguish two cases, depending on whether or not K is bisimilar to $\widehat{K}$.

If $K \not\sim \widehat{K}$, then any X-simplification $A \to_X A'$ that preserves parallel composition on the l.h.s. would contradict minimality, since preservation of heterogeneity is automatic. Thus there is a unique X-simplification to A', which is answered by K. If $H \neq \varepsilon$ then equation (23) would formally have at least two X-simplifications: to $H \mid K^i$ and to $H' \mid K^{i+1}$, where $H \to_X H'$ is any X-simplification of H. But these two are both bisimilar to A' and hence to each other, i.e.,

$$H \mid K^i \sim H' \mid K^{i+1},$$

which is impossible since H does not contain K as a factor. Thus we conclude that $H = \varepsilon$ and $F' \sim K^i$. But this is a contradiction, as F' was chosen to preserve heterogeneity.

Finally suppose $\widehat{K} \sim K$, so that equation (22) becomes

$$(F \mid K) \cdot X^m \sim A \cdot X^m \mid K \cdot X^m. \tag{24}$$

There must exist an X-simplification $A \to_X A'$ that preserves heterogeneity, i.e., $A' \rightsquigarrow \widetilde{K}$ with $\widetilde{K} \not\sim K$. Any such X-simplification that preserved the parallel form on the l.h.s. would contradict minimality, so there is a unique such reduction, which is matched by K on the l.h.s. Now return to equation (23). We know that $\|H\|_X \geq 1$, otherwise the only X-unit reachable from the r.h.s. is K, contradicting heterogeneity. If $\|H\|_X \geq 2$ then there is an X-simplification $H \to_X H' \rightsquigarrow \widetilde{K}$ of H preserving reachability of $\widetilde{K}$. In that case, the r.h.s. of equation (23) formally has at least two X-simplifications preserving reachability of $\widetilde{K}$, namely $H \mid K^i$ and to $H' \mid K^{i+1}$. These two are both bisimilar to A' and hence to each other, implying, as before, that H contains K as a parallel factor, contrary to its definition. The only remaining possibility is that $\|H\|_X = 1$, which is equivalent to $H \sim \widetilde{K}$. Equation (24) then specialises to

$$(F \mid K) \cdot X^m \sim (\widetilde{K} \mid K^{i+1}) \cdot X^m \mid K \cdot X^m. \tag{25}$$

The possibility $i = 0$ is ruled out by Lemma 7.2(c), so we may suppose $i \geq 1$. Observe that there are three distinct (up to bisimulation equivalence) X-simplifications on the r.h.s., induced by $\widetilde{K} \to_X \varepsilon$, $K^{i+1} \to_X K^i$ and $K \cdot X^m \to_X \varepsilon$. (In checking this observation, note that $K^{i+1} \cdot X^m$ and $(\widetilde{K} \mid K^i) \cdot X^m$ are both parallel primes by Lemma 7.2(b).) In other words, the r.h.s. of equation (25) has X-valence three, and so must the l.h.s. The X-simplification $K^{i+1} \to_X K^i$ applied to the r.h.s. of equation (25) preserves the X-valence of the r.h.s., and so cannot be matched by $K \to_X \varepsilon$ on the l.h.s., which reduces the X-valence from three to two. So we have an X-simplification that preserves heterogeneity, contradicting minimality of equation (22). □

Lemma 7.3 associates a privileged X-unit K with each pumpable equation. This X-unit plays an important role in the structure theory, and we need to examine its properties further.

X-monomorphic term.

Definition 7.3 *An X-unit K is* X-monomorphic *if all derivations of K are of one of the two forms* $K \to K \mid X^k$ *or* $K \to X^k$ *(where k may be zero).*

X-units do not grow.

Lemma 7.4 *Let K be the privileged X-unit associated with some pumpable equation. Then K has no X-norm-increasing moves. As an immediate consequence, K is X-monomorphic.*

Proof. Consider the minimal equation (16), which we choose to write

$$(K_{(2)} \mid K) \cdot X^m \sim K^2 \cdot X^m \mid K \cdot X^m. \tag{26}$$

We shall see in due course that the notation $K_{(2)}$ is an instance of a general naming convention for a potentially infinite sequence of terms derived from K; the notation is introduced here only for consistency with later proofs, and the nature of the convention itself need not concern us for the moment. Suppose that some X-norm-increasing immediate derivative $K \to H$ exists. There are two possible responses on the r.h.s. to applying $K \to H$ to the l.h.s. of (26):

$$(K_{(2)} \mid H) \cdot X^m \sim K^2 \cdot X^m \mid \widehat{H} \cdot X^m \tag{27}$$

and

$$(K_{(2)} \mid H) \cdot X^m \sim (K \mid \widehat{H}) \cdot X^m \mid K \cdot X^m. \tag{28}$$

We analyse these two possibilities in turn.

In case (27), apply the X-simplification $K_{(2)} \to_X K$ to the l.h.s., yielding a pumpable equation with $(K \mid H) \cdot X^m$ as its l.h.s. (Note that the r.h.s. must remain a parallel composition.) Now, by Lemma 8, the minimal form (26) may be regained by iterated X-simplification. The factor $K_{(2)}$ on the l.h.s. can only have come from H, so there must be a derivation $K \rightsquigarrow K_{(2)}$, and consequently

$$K \cdot X^m \rightsquigarrow K_{(2)} \cdot X^m \sim (K \cdot X^m)^2. \tag{29}$$

Therefore, for any n, starting with $K \cdot X^m$ and applying an appropriate sequence of derivations, we can get to a term that is syntactically of the form $F \cdot X^m$ but bisimilar to $(K \cdot X^m)^n$:

$$F \cdot X^m \sim (K \cdot X^m)^n. \tag{30}$$

If F is formally a sequential composition, then write $F \sim F_1 \cdot F_2$ with F_1 a sequential prime. By Corollary 5.3, $F_2 \sim X^k$ and $K \sim \widehat{K} \cdot X^k$ for some k, and we may reformulate equation (30) be redefining F to be F_1, K to be $\widehat{K}$, and m to be $m + k$. (Note that the second possibility allowed by Corollary 5.3—that equation (30) is monomorphic—can be ruled out, as it is inconsistent with the assumption that K has X-norm-increasing moves.) We can therefore proceed under the assumption that F is not a formal sequential composition.

Can F be a formal parallel composition? If so, it would have to be the power of a parallel prime, since the X-valence of the r.h.s. of (30) is clearly one. By Lemma 7.2(b), the prime in question must have X-norm at least two. But then there is no X-simplification of the l.h.s. of (30) that preserves the property of having X-valence one, a contradiction.

The only remaining possibility is that F is an atom, but this too can be ruled out by choosing n sufficiently large (larger than the X-norm of any atom). This completes the analysis of case (27).

In case (28), apply the X-simplification $K \mid \widehat{H} \rightarrow_X \widehat{H}$ to the r.h.s., to obtain a pumpable equation with r.h.s. $\widehat{H} \cdot X^m \mid K \cdot X^m$. (Note that the parallel product on the l.h.s. must survive.) By Lemma 7.2(c), this r.h.s. is reducible, via a series of X-simplifications, to $K^2 \cdot X^m \mid K \cdot X^m$. Since $K^2 \cdot X^m$ is a parallel prime, it must be possible to reduce $\widehat{H} \cdot X^m \rightsquigarrow K^2 \cdot X^m$, and hence $\widehat{H} \rightsquigarrow K^2$, again by a series of X-simplifications. Applying the pattern $K \rightarrow \widehat{H} \rightsquigarrow K^2$ of derivations repeatedly to the r.h.s. of equation (26) yields an equation of the form

$$F \cdot X^m \sim (K^n \cdot X^m)^2. \tag{31}$$

for arbitrarily large n. As before, by adjusting F, K and m as necessary, we may assume that F is not a formal sequential composition.

Can F be a formal parallel composition? Again, it would have to be the power of a parallel prime, since the X-valence of the r.h.s. of (31) is one. Moreover the power would have to be a square, as the r.h.s. of (31) is able to regain the property of having valence one after just two X-simplifications:

$$(K^n \cdot X^m)^2 \rightarrow_X K^n \cdot X^m \mid K^{n-1} \cdot X^m \rightarrow_X (K^{n-1} \cdot X^m)^2. \tag{32}$$

(Recall that by Lemma 7.2(b) the parallel prime of which the l.h.s. is a power has X-norm at least two.) By applying balanced X-simplifications of the form (32) repeatedly to the r.h.s. we arrive eventually at an equation of the form

$$P^2 \cdot X^m \sim (K^2 \cdot X^m)^2,$$

which in one further step yields

$$(P \mid K) \cdot X^m \sim K^2 \cdot X^m \mid K \cdot X^m,$$

which we recognise as the minimal equation (26). Thus $P \sim K_{(2)}$, and

$$K_{(2)}^2 \cdot X^m \sim (K^2 \cdot X^m)^2.$$

But this equation is incompatible with

$$K_{(2)} \cdot X^m \sim (K \cdot X^m)^2.$$

on (ordinary) norm grounds, as together they imply $m = 0$.

Finally, by taking n sufficiently large, we may rule out the remaining possibility, that F is an atom. This completes the analysis of case (28), and the proof. □

Starting with an X-monomorphic X-unit K, we identify a sequence $K_{(1)}, K_{(2)}, K_{(3)}, \ldots$ of terms of increasing X-norm, of which K itself is the first element. When K is the privileged X-unit associated with some pumpable equation, the associated sequence plays a key role in elucidating the structure the equation.

Generalised K-prime.

Definition 7.4 *Suppose* X *is a series-parallel atom,* K *an* X*-monomorphic term, and* m *a positive integer. A term* $K_{(j)}$ *of* X*-norm* j *is a* generalised K-prime *if it satisfies the equation*

$$K_{(j)} \cdot X^m \sim (K \cdot X^m)^j. \tag{33}$$

Note that for sufficiently large j *the term* $K_{(j)}$ *may not be expressible in our language of terms; however, if* $K_{(j)}$ *is expressible then it is unique (up to bisimilarity) by unique factorisation. Thus we may speak of "the"* j*th generalised* K*-prime* $K_{(j)}$*.*

Our notation for generalised K-primes omits reference to m, since this number will always be clear from the context. We shall turn to the question of expressibility (or constructibility) of generalised K-primes after reviewing some of their elementary properties.

Observation 7.5 *Let* K *be an* X*-monomorphic term, and* $K_{(j)}$ *an associated generalised* K*-prime satisfying (33). Then:*

(a) the unique X*-simplification of* $K_{(j)}$ *is* $K_{(j)} \rightarrow_X K_{(j-1)}$*;*

(b) $K_{(j)}$ *is a parallel prime.*

Proof. Glancing at (33), we see that the unique X-simplification of $K_{(j)} \cdot X^m$ is

$$K_{(j)} \cdot X^m \rightarrow_X (K_{(j)})' \cdot X^m \sim (K \cdot X^m)^{j-1} \sim K_{(j-1)} \cdot X^m.$$

By unique factorisation, $(K_{(j)})' \sim K_{(j-1)}$, establishing (a).

Suppose $K_{(j)}$ is not a parallel prime. Then, since $K_{(j)}$ and $K_{(j-1)}$ both have unique X-simplifications, $K_{(j)}$ must be the power of some X-unit, say $K_{(j)} \sim \widehat{K}^j$. Indeed, by performing $j-1$ X-simplifications starting from (33) we find that $\widehat{K} \sim K_{(1)} = K$ and, one step before that, $K^2 \cdot X^m \sim (K \cdot X^m)^2$. But this is not possible on (ordinary) norm grounds, establishing (b). □

Observation 7.5(b) justifies to some extent our chosen terminology. Concerning expressibility of generalised K-primes, Observation 7.5(a) allows two apparent possibilities: for a given X-monomorphic term K, either all generalised K-primes $K_{(j)}$ are expressible, or there exists a k such that $K_{(j)}$ is expressible if $j \leq k$, and not otherwise. Both possibilities can in fact occur.

Lemma 7.6 *Let* K *be an* X*-monomorphic term.*

(a) If $K \sim Y \cdot X^i$ *for some monomorphic atom* Y *and integer* i, *then all generalised* K*-primes may be explicitly expressed using the recurrence* $K_{(1)} = Y \cdot X^i$, *and* $K_{(j)} = Y \cdot (K_{(j-1)} \mid X^{i+m})$ *for all* $j \geq 2$.

(b) Otherwise, there is a maximum integer j *for which* $K_{(j)}$ *is expressible. This maximum* j *is bounded by the maximum norm of any atom.*

Proof. Consider equation (33). If $K_{(j)}$ is a formal sequential composition, then, by Corollary 5.3, either equation (33) is monomorphic, or $K_{(j)} = F_1 \cdot F_2$, where $F_2 \sim X^i$. Part (a) of the lemma covers the former case, and part (b) the latter.

In the monomorphic case, K has only the derivations $K \to K$ and $K \to X^i$, where $i = \|K\| - 1$, and hence $K \sim Y \cdot X^i$ for some monomorphic Y. The claimed expressions for $K_{(j)}$ in terms of Y and X may be verified by explicit construction of the bisimulation relation: simply take all pairs

$$\left\{ \left\langle K_{(j)} \cdot X^m \mid X^l,\ (K \cdot X^m)^j \mid X^l \right\rangle : j, l \in \mathbb{N} \right\}$$

and all pairs that can be derived from these by applying Lemma 6.7. This deals with part (a).

In the non-monomorphic case, we may, by taking F_1 as small as possible, assume that F_1 is not a sequential composition. By Corollary 5.3, $F_2 \sim X^i$ where $i = \|F_2\|$, and F_1 is a generalised $\widehat{K}$-prime satisfying

$$F_1 \cdot X^{\widehat{m}} \sim (\widehat{K} \cdot X^{\widehat{m}})^j,$$

where $\widehat{K} \cdot X^i \sim K$ and $\widehat{m} = i + m$. Now F_1 is not a sequential composition by construction, and not a parallel composition by Observation 7.5. Hence F_1 is an atom, and its X-norm (and hence the X-norm of $K_{(j)}$) is bounded by the largest X-norm (and hence the largest norm) of any atom. This deals with part (b). □

When we turn to algorithmic issues, we shall sidestep the question of expressibility of generalised K-primes by explicitly constructing them; that is, we shall add new atoms to represent the terms $K_{(j)}$, and new productions to represent their derivations. Lemma 7.6 assures that the number of new atoms we need to add is bounded.

Definition 7.5 *Suppose* X *is a series-parallel atom and* K *an* X*-monomorphic term. Let* j *be such that* $K_{(j)}$ *is expressible. Then*

Generalised K-term (of degree j).

$$\Pi K_{(\leq j)} = \left\{ K_{(j)}^{e_j} \mid K_{(j-1)}^{e_{j-1}} \mid \cdots \mid K_{(1)}^{e_1} : (e_j, \ldots, e_1) \in \mathbb{N}^j \text{ and } e_j \geq 1 \right\},$$

is the set of generalised K-terms of degree j, *and*

$$\Pi K_{(*)} = \bigcup_j \Pi K_{(\leq j)}$$

where the union is over j *for which* $K_{(j)}$ *is expressible, is the set of* generalised K-terms.

7.2 The left-hand side

The goal of this subsection is to show (Theorem 7.9) that the l.h.s. of a pumpable equation is necessarily of a certain form. In rough terms, the l.h.s. is of the form $F \cdot X^m$, where F is "nearly" a generalised K-term. Our approach is via the study of equations in which F is *precisely* a generalised K-term, which are characterised in Lemma 7.8. First of all, though, a technical lemma.

Lemma 7.7 *Let* K *be the privileged* X*-unit associated with some pumpable equation, and let* $K_{(1)} (= K), K_{(2)}, K_{(3)}, \ldots$ *be as in Definition 7.4. Suppose* H *is an* X*-free term that does not contain* $K_{(j')}$ *as a parallel component for any* $j' < j$*. If* $(H \mid K_{(j)}) \cdot X^m$ *is a parallel composite (i.e., non-prime), then so is* $(H \mid K_{(j-1)}) \cdot X^m$*. (Interpret* $K_{(0)}$ *as* ε *here.)*

Proof. Consider the prime decomposition $\prod_{i=1}^{n} A_i \cdot X^m$ of $(H \mid K_{(j)}) \cdot X^m$, ordered so that $\|A_1\|_X \geq \|A_2\|_X \geq \cdots \geq \|A_n\|_X$. For $(H \mid K_{(j-1)}) \cdot X^m$ to be a parallel prime, we must have $n = 2$ and $\|A_2\|_X = 1$, i.e., $A_2 \sim K$. Thus

$$(H \mid K_{(j)}) \cdot X^m \sim A_1 \cdot X^m \mid K \cdot X^m, \tag{34}$$

and the X-simplification $K \to_X \varepsilon$ on the r.h.s. is matched by $K_{(j)} \to_X K_{(j-1)}$ on the l.h.s. So $A_1 \sim H \mid K_{(j-1)}$, and by substitution into equation (34),

$$(H \mid K_{(j)}) \cdot X^m \sim (H \mid K_{(j-1)}) \cdot X^m \mid K \cdot X^m. \tag{35}$$

On (ordinary) norm grounds, $j = 1$ is not possible, so we may assume $j \geq 2$. Since H does not contain $K_{(j-1)}$ as a factor, the X-valence of $(H \mid K_{(j-1)})$ is at least as large as that of $(H \mid K_{(j)})$. So the X-simplification that annihilates the factor $K \cdot X^m$ on the r.h.s. of equation (35) must be a duplicate; i.e., a term bisimulation equivalent to $(H \mid K_{(j-1)}) \cdot X^m$ can be obtained by two formally distinct X-simplifications on the r.h.s. of (35), and one of these is an explicit parallel composition. But $(H \mid K_{(j-1)}) \cdot X^m \sim A_1 \cdot X^m$, which is supposed to be a parallel prime. □

So provided we reduce the $K_{(j)}$ factors on the l.h.s. of a pumpable equation in the correct order (smallest first), we guarantee to preserve parallel compositeness of the r.h.s.

Lemma 7.8 *Let* K *be the privileged* X*-unit associated with some pumpable equation, and let* $\Pi K_{(*)} = \bigcup_j \Pi K_{(\leq j)}$ *be the corresponding set of generalised* K*-terms. Suppose* $F \in \Pi K_{(\leq j)}$*, and write* $F = K_{(j)}^e \mid H$*, where* $e \geq 1$*,* $H \in \Pi K_{(\leq h)}$ *and* $h < j$*.*

(a) If $e \geq 2$ *then* $F \cdot X^m$ *is a parallel prime.*

(b) If $e = 1$ *then*

$$F \cdot X^m = (K_{(j)} \mid H) \cdot X^m \sim (K_{(j-1)} \mid H) \cdot X^m \mid K \cdot X^m.$$

(Note that if $h < j - 1$*, the r.h.s. will factorise further.)*

Proof. We start with the easier part (b). It is routine to verify that if we add the set of pairs

$$\Big\{\big\langle (K_{(j)} \mid H \mid X^l)\cdot X^m,\ (K_{(j-1)} \mid H)\cdot X^m \mid K\cdot X^m \mid X^l\big\rangle : H \in \Pi K_{(\le h)} \text{ and } h < j\Big\},$$

to the maximum bisimulation relation, the result is still a bisimulation (obviously the maximum one). The only interesting case is when $K_{(j-1)} \to K_{(j-2)} \mid X^k$ on the r.h.s. If $h < j-1$ then there is a valid response on the l.h.s., namely $K_{(j)} \to K_{(j-1)} \mid X^k$; otherwise, we finesse by instead applying the derivation $K_{(j-1)} \to K_{(j-2)} \mid X^k$ to one of the copies of $K_{(j-1)}$ that we know to exist within H (instead of the explicit $K_{(j-1)}$ component), and matching that derivation by a similar one in the H on the l.h.s. This deals with part (b).

Part (a) is proved by contradiction. Suppose $F = K^e_{(j)} \mid H$ provides a minimum (X-norm) counterexample, so that $F\cdot X^m$ is composite and $e \ge 2$. In the light of Lemma 7.7, minimality of F implies $H = \varepsilon$ and $e = 2$. So we must have

$$K^2_{(j)}\cdot X^m \sim \prod_{i=1}^{n} A_i \cdot X^m,$$

where $n \ge 2$. The X-valence of the l.h.s. is one, so the r.h.s. is a prime-power:

$$K^2_{(j)}\cdot X^m \sim (A\cdot X^m)^n. \tag{36}$$

Letting $A \to_X A'$ be the unique X-simplification of A, we have

$$(K_{(j)} \mid K_{(j-1)})\cdot X^m \sim \begin{cases} (A\cdot X^m)^{n-1}, & \text{if } \|A\|_X = 1;\\ (A\cdot X^m)^{n-1} \mid A'\cdot X^m, & \text{otherwise.}\end{cases}$$

By minimality, $K^2_{(j-1)}\cdot X^m$ is a parallel prime, so either $\|A\|_X = 1$ and $n \le 3$, or $\|A\|_X = 2$ and $n = 2$. Equation (36) must be of one of two forms:

$$K^2\cdot X^m \sim (A\cdot X^m)^2$$

which is impossible by Lemma 7.2(b), or

$$K^2_{(2)}\cdot X^m \sim (A\cdot X^m)^2, \tag{37}$$

which leads after one X-simplification to

$$(K_{(2)} \mid K)\cdot X^m \sim A\cdot X^m \mid A'\cdot X^m,$$

and after another to

$$K^2\cdot X^m \sim A\cdot X^m. \tag{38}$$

($K_{(2)} \to_X K$ on the l.h.s. must be matched by $A' \to_X \varepsilon$ on the r.h.s., since we know that $K^2\cdot X^m$ is a parallel prime.) Substituting (38) into (37) yields

$$K^2_{(2)}\cdot X^m \sim (K^2\cdot X^m)^2,$$

which, as we saw in the proof of Lemma 7.4, is impossible on (ordinary) norm grounds. □

We are now in a position to state and prove the main theorem of the section, which gives rather precise information about the form of the l.h.s. of any pumpable equation.

General form of the l.h.s. of a pumpable equation.

Theorem 7.9 *Suppose*

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m$$

is a pumpable equation. Let K *be the privileged* X*-unit associated with the equation, and let* $\Pi K_{(*)} = \bigcup_j \Pi K_{(\leq j)}$ *be the corresponding set of generalised* K*-terms, as in Definition 7.4. Assume that both sides of the equation are completely factored (so that, in particular, each* F_i *is a parallel prime) and that the factors are listed in order of non-increasing* X*-norm,* $\|F_1\|_X \geq \|F_2\|_X \geq \cdots \geq \|F_r\|_X$*. Then* $\|F_1\|_X > \|F_2\|_X$ *(i.e.,* F_1 *is the unique factor on the l.h.s. of largest* X*-norm), and* $F_2 \mid \cdots \mid F_r \sim H \in \Pi K_{(*)}$ *(i.e., each factor with the possible exception of the largest is bisimilar to* $K_{(j)}$ *for some* j *).*

Exceptional factor, l.h.s.

Proof. Call a factor F_i *exceptional* if it is not bisimilar to $K_{(j)}$ for some j. The proof is in two stages: (i) show that there can be at most one exceptional factor on the l.h.s., and then (ii) show that the exceptional factor, if it exists, must have strictly larger X-norm than all the others. This is enough to establish the theorem, since the case where all factors F_i are non-exceptional is covered by Lemma 7.8(b).

To prove first claim—that there can be at most one exceptional factor—we postulate a minimum X-norm counterexample and derive a contradiction. Minimality implies that the counterexample must have the form

$$(F_1 \mid F_2) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m, \tag{39}$$

i.e., there are precisely two factors (both exceptional) on the l.h.s. (If there are additional exceptional factors, perform any X-simplification on the r.h.s. that preserves the parallel composition; if there are additional factors of the form $K_{(j)}$, apply an X-simplification to the smallest of them and appeal to Lemma 7.7.) We distinguish three cases.

Case I. Assume $n \geq 3$, or $n = 2$ and $\|A_1\|_X, \|A_2\|_X \geq 2$. In this case, any X-simplification on the l.h.s. of (39) preserves the parallel product on the r.h.s., and thus must destroy one of the exceptional factors on the l.h.s. Without loss of generality, assume that $F_1 \to_X F_1' \in \Pi K_{(\leq j_1)}$ and $F_2 \to_X F_2' \in \Pi K_{(\leq j_2)}$, where $j_1 \geq j_2$. (Reverse the roles of F_1 and F_2 if necessary to obtain the inequality.) As we have observed, $(F_1' \mid F_2) \cdot X^m$ is a (parallel) composite, and the same must be true of $(K_{(j_2)} \mid F_2) \cdot X^m$ by Lemma 7.7. In contrast, we know from Lemma 7.8(a) that $(K_{(j_2)} \mid F_2') \cdot X^m$ is a parallel prime, since $K_{(j_2)}$ occurs with exponent at least two. We conclude that

$$(K_{(j_2)} \mid F_2) \cdot X^m \sim (K_{(j_2)} \mid F_2') \cdot X^m \mid K \cdot X^m,$$

and further, by Lemma 7.8(b) and unique factorisation,

$$K_{(j_2)} \mid F_2 \sim K_{(j_2+1)} \mid F_2'.$$

But the last equation contradicts the assumption that F_2 is exceptional.

Case II. Assume that $n = 2$ and $A_2 \sim K$. (Note that this is the complement to Case I.) The form of the counterexample is now

$$(F_1 \mid F_2) \cdot X^m \sim A \cdot X^m \mid K \cdot X^m. \tag{40}$$

We consider two complementary subcases.

Case IIa. To the Case II assumptions, add the further assumption $F_1 \sim F_2 \sim F$. Applying an X-simplification to A on the r.h.s. of (40) yields

$$(F \mid F') \cdot X^m \sim A' \cdot X^m \mid K \cdot X^m,$$

where, by minimality, $F' \in \Pi K_{(\leq j)}$ for some j. In contrast, by Lemma 7.8(a), $(F' \mid F') \cdot X^m$ is a parallel prime. We conclude that

$$(F \mid F') \cdot X^m \sim (F' \mid F') \cdot X^m \mid K \cdot X^m.$$

In the light of Lemma 7.8(b) and unique factorisation, the last equation contradicts the assumption that F_2 is exceptional, just as in Case I.

Case IIb. To the Case II assumptions, add the further assumption $F_1 \not\sim F_2$. Apply an X-simplification to the factor $K \cdot X^m$ on the r.h.s. of (40), and suppose, without loss of generality, that the response on the l.h.s. is $F_1 \to_X F_1'$, yielding

$$(F_1' \mid F_2) \cdot X^m \sim A \cdot X^m. \tag{41}$$

Note that any X-simplification $F_2 \to_X F_2'$ on the l.h.s. of (40) is matched on the r.h.s. by A, and hence the parallel composition on the r.h.s. is preserved. Minimality then implies $F_2' \in \Pi K_{(\leq j_2)}$ for some integer j_2.

If F_1 has some other X-simplification $F_1 \to_X F_1^\dagger$ with $F_1^\dagger \not\sim F_1'$, then the r.h.s. must respond with an X-simplification of A, again preserving the parallel composition on the r.h.s. Minimality then implies $F_1^\dagger \in \Pi K_{(\leq j_1)}$ for some j_1, a situation we already ruled out in Case I. We conclude that the X-simplification $F_1 \to_X F_1'$ is unique, up to bisimilarity.

Between equations (40) and (41) the X-valence of the r.h.s. (and hence of the l.h.s.) has decreased. This observation, combined with the fact that F_1 has a unique X-simplification, implies $F_1' \sim F_2^k$ for some $k \geq 1$. Thus, noting (41) and substituting for A in (40),

$$(F_1 \mid F_2) \cdot X^m \sim F_2^{k+1} \cdot X^m \mid K \cdot X^m,$$

which leads after one X-simplification to

$$(F_1 \mid F_2') \cdot X^m \sim (F_2^k \mid F_2^\dagger) \cdot X^m \mid K \cdot X^m, \tag{42}$$

where $F_2^\dagger \in \Pi K_{(*)}$. (Recall that *every* X-simplification of F_2 leads to a generalised K-term.) In k X-simplifications, the r.h.s. of (42) becomes

$$(F_2^\dagger)^{k+1} \cdot X^m \mid K \cdot X^m,$$

which by Lemma 7.8(b) is bisimilar to $H \cdot X^m$ with $H \in \Pi K_{(*)}$. But the l.h.s. of (42) requires a sequence of at least $k+1$ X-simplifications to achieve the same form. This contradiction eliminates the final case (Case IIb).

We have established that the l.h.s. of any pumpable equation contains at most one exceptional factor. In the second stage of the proof, we must show that the unique exceptional factor, if it exists, has larger X-norm than all the others. As in the first stage, we consider a minimum X-norm counterexample and obtain a contradiction. By Lemma 7.7 we know the minimum counterexample is of the form

$$(F \mid K_{(j)}) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m, \tag{43}$$

where F is a parallel prime that is not bisimilar to any $K_{(j')}$, and has X-norm at most j. We distinguish two cases.

First, suppose that there is an X-simplification of F, say $F \to_X F'$, that preserves the parallel composition on the r.h.s. of (43). Minimality entails $F' \in \Pi K_{(\leq j')}$ for some $j' < j$. Now reduce $K_{(j)}$ to $K_{(j')}$ by a series of X-simplifications; by Lemma 7.7, the parallel composition on the r.h.s. of (43) is preserved. On the other hand, one further X-simplification, that of $F \to_X F'$, destroys the parallel composition on the r.h.s., by Lemma 7.8(a). Therefore, we must have

$$(F \mid K_{(j')}) \cdot X^m \sim A \cdot X^m \mid K \cdot X^m, \tag{44}$$

reducing in one X-simplification to

$$(F' \mid K_{(j')}) \cdot X^m \sim A \cdot X^m.$$

By unique factorisation, $A \sim F' \mid K_{(j')}$, and we may substitute for A in equation (44) to obtain

$$(F \mid K_{(j')}) \cdot X^m \sim (F' \mid K_{(j')}) \cdot X^m \mid K \cdot X^m.$$

But this would imply, in the light of Lemma 7.8(b), that $F \in \Pi K_{(*)}$, a contradiction.

Finally suppose that there is no X-simplification of F that preserves the parallel composition on the r.h.s. of (43). Then F has a unique X-simplification, say $F \to_X F'$, and we must have

$$(F \mid K_{(j)}) \cdot X^m \sim A \cdot X^m \mid K \cdot X^m,$$

reducing in one X-simplification to

$$(F' \mid K_{(j)}) \cdot X^m \sim A \cdot X^m.$$

Thus, $A \sim F' \mid K_{(j)}$ and

$$(F \mid K_{(j)}) \cdot X^m \sim (K_{(j)} \mid F') \cdot X^m \mid K \cdot X^m. \tag{45}$$

The l.h.s. of (45) has X-valence two, whereas the r.h.s. has X-valence at least three, a contradiction. To verify the latter claim, note that, by Lemma 7.8(b), $F' \not\sim K_{(j)}$, so that there must be at least two distinct X-simplifications of $K_{(j)} \mid F'$. The X-simplification of K on the r.h.s. of (45) leads to an outcome clearly distinct from either of these, since it leaves the r.h.s. as a parallel prime. □

7.3 The right-hand side

The goal of this subsection is to show (Theorem 7.12) that the r.h.s. of a pumpable equation is necessarily of a certain form. In rough terms, the r.h.s. is "nearly" a parallel composition of terms of the form $K^t \cdot X^m$. The approach is similar that adopted in the previous section: namely, we initially aim to characterise (in Lemma 7.11) those equations in which the r.h.s. is *precisely* a product of such terms. We start with a technical lemma. Call a component $A \cdot X^m$ on the r.h.s. of a pumpable equation *exceptional* if $A \notin \Pi K_{(\leq 1)}$, i.e., if it is not of the form $K^t \cdot X^m$ for some t.

Exceptional factor, r.h.s.

Lemma 7.10 *Let*

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_{n-1} \cdot X^m \mid K^t \cdot X^m$$

be a pumpable equation which has $K^t \cdot X^m$ as its smallest non-exceptional component on the r.h.s. (I.e., every $A_i \cdot X^m$ is either exceptional or is bisimilar to $K^s \cdot X^m$ with $s \geq t$.) Suppose that the X-simplification $K^t \to_X K^{t-1}$ is applied to the r.h.s. The response on the l.h.s. satisfies the following condition: if the l.h.s. had a component F_i bisimilar to K before the X-simplification then it continues to have one after. As a consequence: (a) the parallel composition on the l.h.s. is preserved, that is, the new l.h.s. is of the form $(F'_1 \mid \cdots \mid F'_{r'}) \cdot X^m$ with $r' \geq 2$, and (b) at least one of the new prime components $F'_1 \mid \cdots \mid F'_{r'}$ is bisimilar to $K_{(j)}$ for some positive j. (Note that (b) holds even if $n = 2$ and $t = 1$ so that the parallel composition on the r.h.s. is destroyed).

Proof. If there are at least two components F_i bisimilar to K then the result is immediate. So suppose that $F_r \sim K$ and $\|F_{r-1}\|_X \geq 2$. (Assume that the components F_i are listed in order of non-increasing X-norm.) The X-simplification $K^t \to_X K^{t-1}$ on the r.h.s. cannot be matched by $K \to \varepsilon$ on the l.h.s.: on the one hand, if $t \geq 2$, the X-valence of the r.h.s. does not decrease, whereas the

X-valence of the l.h.s. certainly does; on the other hand, if $t = 1$, the (ordinary) norm of the r.h.s. decreases by more (in fact an additive term m) than the norm of the l.h.s.

Rider (a) is immediate, since the destruction of the parallel composition on the l.h.s. would necessitate the annihilation of a unique factor bisimilar to K. Rider (b) is almost as easy. By Theorem 7.9 we know that the l.h.s. of the initial equation has at least one component bisimilar to $K_{(j)}$ for some j. If $j \geq 2$ then there is a component $K_{(j)}$ or $K_{(j-1)}$ after X-simplification; if $j = 1$ then at least one component bisimilar to $K_{(1)} \sim K$ must survive. □

Lemma 7.11 *Suppose*

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim \prod_{i=1}^{n} K^{e_i} \cdot X^m \tag{46}$$

is a pumpable equation in which both sides are fully factored (i.e., $F_1, \ldots, F_r$ *are all parallel primes), the* F_k *are in listed in order of non-increasing X-norm* $\|F_1\|_X \geq \|F_2\|_X \geq \cdots \geq \|F_r\|_X$*, and the exponents* e_i *are also in non-increasing order* $e_1 \geq e_2 \geq \cdots \geq e_n$*. Then* $r = e_1 - e_2 + 1$ *(in particular,* $e_1 > e_2$*),*

$$F_1 \cdot X^m \sim (K^{e_2} \cdot X^m)^2 \mid K^{e_3} \cdot X^m \mid \cdots \mid K^{e_n} \cdot X^m.$$

and $F_2 \sim F_3 \sim \cdots \sim F_r \sim K$*. Moreover, for all* $e > e_2$ *(and not just for* $e = e_1$*) it is the case that*

$$(F_1 \mid K^{e-e_2}) \cdot X^m \sim K^e \cdot X^m \mid K^{e_2} \cdot X^m \mid K^{e_3} \cdot X^m \mid \cdots \mid K^{e_n} \cdot X^m.$$

Proof. Consider the equation obtained from (46) by applying a sequence of $e_1 - e_2$ X-simplifications to the largest component K^{e_1} on the l.h.s.:

$$\widehat{F} \cdot X^m \sim (K^{e_2} \cdot X^m)^2 \mid K^{e_3} \cdot X^m \mid \cdots \mid K^{e_n} \cdot X^m. \tag{47}$$

We claim that $\widehat{F}$ is a parallel prime. (Later we shall argue that $\widehat{F}$ is in fact F_1.) Suppose to the contrary that $\widehat{F}$ is a (parallel) composite. Then, by repeated application of Lemma 7.10,

$$\widetilde{F} \cdot X^m \sim (K^{e_2} \cdot X^m)^2,$$

where $\widetilde{F}$ is still a composite. The X-valence of the r.h.s. is one, so $\widetilde{F} \sim F^s$ for some parallel prime F and some exponent $s \geq 2$. Furthermore, by Theorem 7.9, $F \sim K_{(j)}$ for some j. But this is impossible by Lemma 7.8(a).

Denote by $\mathcal{F}$ the finite set of all non-increasing sequences of positive numbers $f_1 \geq f_2 \geq \cdots \geq f_\nu$ such that

$$K^{f_1} \cdot X^m \mid K^{f_2} \cdot X^m \mid \cdots \mid K^{f_\nu} \cdot X^m$$

is reachable from the r.h.s. of (47) via some sequence of X-simplifications. For all $(f_1, \ldots, f_\nu) \in \mathcal{F}$ denote by $F[f_1, \ldots, f_\nu]$ the term satisfying

$$F[f_1, \ldots, f_\nu] \cdot X^m \sim K^{f_1} \cdot X^m \mid K^{f_2} \cdot X^m \mid \cdots \mid K^{f_\nu} \cdot X^m.$$

(c.f., equation (47)). Note that $F[f_1, \ldots, f_\nu]$ is well defined (up to bisimilarity) for any sequence $(f_1, \ldots, f_\nu) \in \mathcal{F}$. It is routine to verify—recall Lemma 7.4 at this point—that if we add the set of pairs

$$\Big\{\big\langle (F[f_1, \ldots, f_\nu] \mid K^s) \cdot X^m,\ K^{f_1+s} \cdot X^m \mid K^{f_2} \cdot X^m \mid \cdots \mid K^{f_n} \cdot X^m \big\rangle : \\ s \in \mathbb{N} \text{ and } (f_1, \ldots, f_\nu) \in \mathcal{F}\Big\}$$

to the maximum bisimulation relation, the result is still a bisimulation (obviously the maximum one). Now set $\nu = n$, $s = e_1 - e_2$, $f_1 = e_2$, and $f_2 = e_2, \ldots, f_n = e_n$. □

Now for the main result of the section, which provides a rather precise characterisation of the general form of the r.h.s. of a pumpable equation.

Theorem 7.12 *Suppose*

General form of the r.h.s. of a pumpable equation.

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m$$

is a pumpable equation, and let K *be the privileged* X*-unit associated with the equation. Assume that both sides of the equation are completely factored (so that, in particular, each* $A_i \cdot X^m$ *is a parallel prime) and that the factors are listed in order of non-increasing* X*-norm,* $\|A_1\|_X \geq \|A_2\|_X \geq \cdots \geq \|A_n\|_X$*. Then* $\|A_1\|_X > \|A_2\|_X$ *(i.e.,* $A_1 \cdot X^m$ *is the unique factor on the r.h.s. of largest* X*-norm), and* $A_2, \ldots, A_n \in \Pi K_{(\leq 1)}$ *(i.e., each factor with the possible exception of the largest is bisimilar to* $K^t \cdot X^m$ *for some* t*).*

Proof. As with Theorem 7.9, the proof is in two stages. In the first stage, we prove by contradiction that the r.h.s. of a pumpable equation contains at most one exceptional factor. Consider a minimal (X-norm) counterexample to this claim. The number of exceptional factors cannot be greater than two, otherwise we could perform an X-simplification on the l.h.s. and obtain a smaller counterexample. Furthermore, there cannot be any non-exceptional factors by Lemma 7.10. So the minimum counterexample has the form

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A \cdot X^m \mid B \cdot X^m \tag{48}$$

where $A \cdot X^m$ and $B \cdot X^m$ are parallel primes, and $A, B \notin \Pi K_{(\leq 1)}$. Note in particular that $\|A\|_X, \|B\|_X \geq 2$.

Apply some X-simplification to the l.h.s. of (48) that preserves the parallel composition on the l.h.s. Without loss of generality, the r.h.s. responds with $A \rightarrow_X A'$. By minimality, one of the exceptional components on the r.h.s. must disappear, and so

$$A' \cdot X^m \sim \prod_i K^{e_i} \cdot X^m \tag{49}$$

for some finite sequence (e_i) of positive integers (possibly of length one). By Lemma 7.7, we may reduce $A' \cdot X^m \rightsquigarrow \varepsilon$ via some sequence of X-simplifications that preserves the parallel composition on the l.h.s. Referring to equation (48), we have annihilated the component $A \cdot X^m$ on the r.h.s. while retaining the parallel composition on the l.h.s.; it follows by unique factorisation that B is a (parallel) composite. We distinguish three cases.

Case I. Assume $r \geq 3$, or $r = 2$ and $\|F_r\|_X \geq 2$. In this case, any X-simplification of $B \rightarrow_X B'$ on the r.h.s. of (48) preserves the parallel product on the l.h.s., and by minimality must destroy one of the exceptional factors on the r.h.s. Thus

$$B' \cdot X^m \sim \prod_i K^{f_i} \cdot X^m \tag{50}$$

for some sequence (f_i). By Lemma 7.11,

$$B' \sim \widehat{B} \mid K^t \quad \text{or} \quad B' \sim K^t \tag{51}$$

where $\widehat{B}$ is a parallel prime with $\|\widehat{B}\|_X \geq 2$.

Consider the (parallel) prime decomposition of B. (Recall that B is composite.) If the prime decomposition of B contains K as a factor, then it can contain at most one non-K factor, otherwise the X-simplification of B induced by $K \rightarrow_X \varepsilon$ will lead to a term B' that is not of the form (51). Furthermore, if the prime decomposition of B does not contain K as a factor, then it must contain exactly two prime factors by similar reasoning. In this case, at least one of the two factors must be bisimilar to $K_{(2)}$, by Lemma 7.10. (There must be a factor bisimilar to $K_{(j)}$, for some j; and j must be two, otherwise there exists an X-simplification $B \rightarrow_X B'$ with B' not of the form (51)). These considerations reduce the possibilities for B to just two:

$$B \sim \widetilde{B} \mid K_{(2)} \tag{52}$$

and

$$B \sim \widetilde{B} \mid K^s, \tag{53}$$

where $s \geq 1$ and $\widetilde{B}$ is a parallel prime not bisimilar to K. (In the case of (52) this claim follows from primality of $B \cdot X^m$ and Lemma 7.8; in the case of (53) from the assumption that $B \cdot X^m$ is exceptional.)

The second possibility (53) is easy to rule out. Consider the X-simplification $B \sim \widetilde{B} \mid K^s \rightarrow_X \widetilde{B} \mid K^{s-1} \sim B'$. The term $B' \cdot X^m \sim (\widetilde{B} \mid K^{s-1}) \cdot X^m$ must factor (non-trivially) as specified in (50). But then, by Lemma 7.11, $(B' \mid K) \cdot X^m \sim (\widetilde{B} \mid K^s) \cdot X^m \sim B \cdot X^m$ would factor non-trivially. However, $B \cdot X^m$ is assumed to be a parallel prime.

With a little more work, the other possibility (52) may also be ruled out. Since any X-simplification $B \rightarrow_X B'$ of $B \sim \widetilde{B} \mid K_{(2)}$ must lead to a term B' of the form (51), it follows that there is a unique X-simplification of $\widetilde{B}$, which is of the form $\widetilde{B} \rightarrow_X K^u$ for some $u \geq 1$. Now consider the sequence of X-simplifications

$$B \cdot X^m \sim (\widetilde{B} \mid K_{(2)}) \cdot X^m \rightarrow_X (\widetilde{B} \mid K) \cdot X^m \sim B' \cdot X^m \tag{54}$$

$$\rightarrow_X (K^u \mid K) \cdot X^m \sim K^{u+1} \cdot X^m. \tag{55}$$

The outcome (54) of the first X-simplification is a (non-trivial) parallel composition as specified in (50), whereas the outcome (55) of the second is manifestly a parallel prime (recall Lemma 7.8(a)). The only way this can occur is for

$$(\widetilde{B} \mid K) \cdot X^m \sim B' \cdot X^m \sim K^{u+1} \cdot X^m \mid K \cdot X^m.$$

But, by Lemma 7.8,

$$K^{u+1} \cdot X^m \mid K \cdot X^m \sim (K_{(2)} \mid K^u) \cdot X^m,$$

which implies $\widetilde{B} \sim K_{(2)}$ and $u = 1$. Thus $B \sim K_{(2)}^2$. The same argument applies equally to A, yielding $A \sim K_{(2)}^2$. Substituting $A \sim B \sim K_{(2)}^2$ into (48), we obtain

$$F^k \cdot X^m \sim K_{(2)}^2 \cdot X^m \mid K_{(2)}^2 \cdot X^m,$$

where $\|F\|_X \geq 2$ (by Lemma 7.2(b)) and $k \geq 2$. (The r.h.s. has X-valence one, so all the components F_i on the l.h.s. must be bisimilar to each other.) But it is impossible for all F_i to have the same X-norm, by Theorem 7.9. This completes the analysis of Case I.

Case II. Assume that $n = 2$ and $F_2 \sim K$. (Note that this is the complement to Case I.) The form of the counterexample is now

$$(F \mid K) \cdot X^m \sim A \cdot X^m \mid B \cdot X^m, \tag{56}$$

where F a prime with $\|F\|_X \geq 2$. We consider two complementary subcases.

Case IIa. To the Case II assumptions, add the further assumption $A \sim B$, so that (56) becomes

$$(F \mid K) \cdot X^m \sim A \cdot X^m \mid A \cdot X^m.$$

The X-simplification $K \to_X \varepsilon$ reduces the X-valence of the l.h.s. but increases that of the r.h.s.

Case IIb. To the Case II assumptions, add the further assumption $A \not\sim B$. Without loss of generality assume that the X-simplification $K \to_X \varepsilon$ on the l.h.s. is matched by B on the r.h.s. Then there is an X-simplification $A \to_X A'$ (in fact any one will do) which when applied to the r.h.s. preserves the parallel composition on the l.h.s.. As we argued at the outset of the proof, this fact implies B is a parallel composition. (By minimality, the prime factorisation of $A' \cdot X^m$ contains no exceptional components; now annihilate these components one by one using Lemma 7.10.) But this time, we have a little more: by observation (b) in Lemma 7.10, B must contain K as a parallel component. Since $B \cdot X^m$ is exceptional, it must also contain a parallel component *not* bisimilar to K. So B has at least two X-simplifications, and one of these preserves the parallel composition on the l.h.s. So the argument we just applied to B applies equally to A: the (parallel) prime decomposition of A contains at least one component bisimilar to K, and at least one not bisimilar to K.

By minimality, every X-simplification $A \to_X A'$ yields an A' such that the prime decomposition of $A' \cdot X^m$ contains no exceptional factors. (We use the assumption $A \not\sim B$ here.) By Lemma 7.11, it follows that $A \sim \widetilde{A} \mid K^s$, where $s \geq 1$ and $\widetilde{A}$ is a parallel prime not bisimilar to K. Now consider the particular X-simplification

$$A \cdot X^m \sim (\widetilde{A} \mid K^s) \cdot X^m \to_X (\widetilde{A} \mid K^{s-1}) \cdot X^m \sim \prod_i K^{e_i} \cdot X^m,$$

where the product at the far right is non-trivial. By Lemma 7.11,

$$A \cdot X^m \sim (\widehat{A} \mid K^s) \cdot X^m \sim K^{e_1+1} \cdot X^m \mid \prod_{i \geq 2} K^{e_i} \cdot X^m,$$

contradicting the assumption that $A \cdot X^m$ is a parallel prime. This completes Case II, and the first stage of the proof: we now know that there is at most one exceptional component on the r.h.s.

Now to the second stage. If there are no exceptional factors on the r.h.s. then, by Lemma 7.11, $\|A_1 \cdot X^m\|_X > \|A_2 \cdot X^m\|_X$. We know from the first stage that there is at most one exceptional factor. So it only remains to show that the exceptional factor, if it exists, has strictly larger X-norm than all the others. As usual, we consider a minimal (X-norm) counterexample and derive a contradiction. By Lemma 7.10, a minimal counterexample is necessarily of the form

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim K^t \cdot X^m \mid A \cdot X^m, \tag{57}$$

where $A \notin \Pi K_{(\leq 1)}$, and $t = \|A\|_X$.

We distinguish two cases. First suppose that A has at least one X-simplification, say $A \to_X A'$ that preserves the parallel composition on the l.h.s. of (57). By minimality, $A' \cdot X^m$ is a parallel composition (possibly trivial) of non-exceptional components—refer to equation (49)—in which the highest power of K is $e_1 < t$. Using a sequence of X-simplifications, reduce $K^t \cdot X^m$ on the r.h.s. of equation (57) to $K^{e_1} \cdot X^m$. By Lemma 7.10, the response on the l.h.s. preserves the parallel composition. However, one further X-simplification on the l.h.s., namely $A \to_X A'$, destroys the parallel composition, by Lemma 7.11. Therefore, at the penultimate step we must have

$$(F \mid K) \cdot X^m \sim K^{e_1} \cdot X^m \mid A \cdot X^m, \tag{58}$$

reducing in the final X-simplification to

$$F \cdot X^m \sim (K^{e_1} \cdot X^m)^2 \mid \prod_{i \geq 2} K^{e_i} \cdot X^m.$$

But then, by Lemma 7.11,

$$(F \mid K) \cdot X^m \sim K^{e_1+1} \cdot X^m \mid K^{e_1} \cdot X^m \mid \prod_{i \geq 2} K^{e_i} \cdot X^m. \tag{59}$$

Comparing equations (58) and (59), we see that $A \cdot X^m$ is non-exceptional, counter to assumption.

The second case—all X-simplifications of A in (57) destroy the parallel composition on the l.h.s.—is simpler to handle. Note that the X-simplification $A \to_X A'$ is unique (up to bisimilarity). So the situation is

$$(F \mid K) \cdot X^m \sim K^t \cdot X^m \mid A \cdot X^m, \tag{60}$$

reducing in one X-simplification to

$$F \cdot X^m \sim K^t \cdot X^m \mid A' \cdot X^m. \tag{61}$$

The r.h.s. of equation (60) has X-valence two, which implies that the l.h.s. of (60) also has X-valence two, which in turn implies that the l.h.s. of (61) has X-valence one. This can only happen if the r.h.s. of (61) is a square, i.e., $A' \sim K^t$. But this is impossible on X-norm grounds, since $\|A'\|_X < \|A\|_X = t$. □

7.4 The left hand knows what the right is doing

The previous two sections provided considerable information about the l.h.s. and r.h.s. of pumpable equations, considered in isolation. We now consider how derivations on the two sides are coordinated. This will lead to an effective inductive classification of all pumpable equations.

Lemma 7.13 *Let*

The large component on the l.h.s. responds to the small ones on the r.h.s.

$$(F_1 \mid \cdots \mid F_r) \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \tag{62}$$

be any pumpable equation in completely factored form with components arranged in non-increasing order of X-norm. We know from Theorems 7.9 and 7.12 that F_1 and A_1 are the unique components of largest X-norm on the l.h.s. and r.h.s., respectively. Then any X-simplification of one of the $n-1$ smallest components $A_j \cdot X^m$ on the r.h.s. is matched by an X-simplification $F_1 \to_X F_1'$ of the largest component on the l.h.s. Moreover, provided $n \geq 3$ or $\|A_n\|_X \geq 2$, i.e., the parallel composition on the r.h.s. is preserved, the new largest component on the l.h.s. is to be found within the parallel components of F_1'.

Proof. First we demonstrate that the largest component F_1 on the l.h.s. always responds to an X-simplification of any of the $n-1$ smallest components $A_j \cdot X^m$ on the r.h.s. Recall (Theorem 7.12) that each A_j for $2 \leq j \leq n$ is bisimilar to K^t for some t. Consider a counterexample of smallest X-norm:

$$(F_1 \mid H) \cdot X^m \sim W \cdot X^m \mid K^t \cdot X^m, \tag{63}$$

where $H = F_2 \mid \cdots \mid F_r \in \Pi K_{(*)}$ and the X-simplification $K^t \to_X K^{t-1}$ on the r.h.s. is matched by $H \to_X H'$ on the l.h.s. (To see that it is possible to collect together the remaining $n-1$ components on the r.h.s. of 62 into the one term $W\cdot X^m$, simply annihilate $A_j \cdot X^m \sim K^t \cdot X^m$ on the r.h.s. via a sequence of X-simplifications, and observe the response on the l.h.s.) We distinguish two cases.

If $t = 1$ then equation (63) specialises to

$$(F_1 \mid H)\cdot X^m \sim W\cdot X^m \mid K\cdot X^m. \tag{64}$$

In one X-simplification we reach

$$(F_1 \mid H')\cdot X^m \sim W\cdot X^m$$

(H responds because (64) is a counterexample), implying $W \sim F_1 \mid H'$. Note that by Lemma 7.10(a) $||H'||_X \geq 1$, and hence $||H||_X \geq 2$; moreover, we have the option of applying a further X-simplification $H' \to_X H''$ to H'. Substituting for W in (64) yields

$$(F_1 \mid H)\cdot X^m \sim (F_1 \mid H')\cdot X^m \mid K\cdot X^m. \tag{65}$$

Now apply the sequence of X-simplifications

$$(F_1 \mid H')\cdot X^m \mid K\cdot X^m \to_X (F_1 \mid H'')\cdot X^m \mid K\cdot X^m \to_X (F_1 \mid H'')\cdot X^m$$

to the r.h.s. of (65). Since $||F_1||_X, ||H||_X \geq 2$, the l.h.s. after the first X-simplification is a parallel composition; moreover its largest component has X-norm at most $||F_1||_X$. By Lemma 7.10(a), the l.h.s. after the second X-simplification is also a parallel composition, and by minimality of the counterexample, its largest component has X-norm *strictly less* than $||F_1||_X$. But this is inconsistent with the r.h.s. being $(F_1 \mid H'')\cdot X^m$.

If $t \geq 2$, then write H as $\widehat{H} \mid K^s$ with s maximal (so that $\widehat{H}$ does not contain K as a parallel component). Because (63) is a counterexample, the X-simplification $K^t \to_X K^{t-1}$ on the r.h.s. is matched by $H \to_X H'$ on the l.h.s. By considering the change in ordinary norm, we see that it is K^s that responds and not $\widehat{H}$. (When $j \geq 2$, the X-simplification $K_{(j)} \to_X K_{(j-1)}$ reduces the ordinary norm by $||K|| + m$.) So starting at

$$(F_1 \mid \widehat{H} \mid K^s)\cdot X^m \sim W\cdot X^m \mid K^t\cdot X^m, \tag{66}$$

we reach, after one X-simplification,

$$(F_1 \mid \widehat{H} \mid K^{s-1})\cdot X^m \sim W\cdot X^m \mid K^{t-1}\cdot X^m. \tag{67}$$

By minimality of the counterexample, a further X-simplification yields

$$(F_1' \mid \widehat{H} \mid K^{s-1})\cdot X^m \sim W\cdot X^m \mid K^{t-2}\cdot X^m. \tag{68}$$

Consider what happens if the order of the X-simplifications on the l.h.s. is reversed, so that $F_1 \to_X F_1'$ is applied first and $K^s \to_X K^{s-1}$ second. The order of events on the l.h.s. is now

$$(F_1 \mid \widehat{H} \mid K^s)\cdot X^m \to_X (F_1' \mid \widehat{H} \mid K^s)\cdot X^m \to_X (F_1' \mid \widehat{H} \mid K^{s-1})\cdot X^m.$$

The end result is of course equation (68). Note, however, that the l.h.s. at the intermediate stage differs according to the order of the X-simplifications, since

$$F_1 \mid \widehat{H} \mid K^{s-1} \not\sim F_1' \mid \widehat{H} \mid K^s. \tag{69}$$

(The component F_1 on the l.h.s. has strictly greater X-norm than any appearing on the r.h.s.) Consider how the r.h.s. must respond. Since (68) has fewer copies of $K^t \cdot X^m$ on the r.h.s. than (66), at least one of the two X-simplifications on the r.h.s. in passing from (66) to (68) must be $K^t \cdot X^m \to_X K^{t-1} \cdot X^m$. It cannot be the first, by (69), nor the second, by minimality of the counterexample: a contradiction.

We have shown that in one X-simplification from equation (63) we reach

$$(F_1' \mid H) \cdot X^m \sim W \cdot X^m \mid K^{t-1} \cdot X^m; \tag{70}$$

it remains to show that F_1' continues to contain the largest component on the l.h.s., provided the parallel composition on the r.h.s. remains non-trivial. Assume that this is not the case, i.e., that H contains a component of strictly larger X-norm than any in F_1'. By Theorem 7.9, $F_1' \in \Pi K_{(*)}$, and hence $F_1' \mid H \in \Pi K_{(*)}$; thus equation (70) is covered by Lemma 7.8.

Suppose first that $t \geq 2$. Since the unique largest component is now contained within H, we have, after one further X-simplification,

$$(F_1' \mid H') \cdot X^m \sim W \cdot X^m \mid K^{t-2} \cdot X^m.$$

Consider what happens when the X-simplifications on the l.h.s. of (63) are performed in the reverse order

$$(F_1 \mid H) \cdot X^m \to_X (F_1 \mid H') \cdot X^m \to_X (F_1' \mid H') \cdot X^m.$$

As we observed earlier, the intermediate stage differs according to the order of X-simplifications, since $F_1 \mid H' \not\sim F_1' \mid H$. The r.h.s. cannot evolve in the same way as before, and the only alternative is that there is a component $K^{t-1} \cdot X^m$ on the r.h.s. of (63), and that $K^{t-1} \cdot X^m \to_X K^{t-2} \cdot X^m$ is performed first and then $K^t \cdot X^m \to_X K^{t-1} \cdot X^m$. But this is impossible, as the X-simplification $K^{t-1} \cdot X^m \to_X K^{t-2} \cdot X^m$ must be matched by F_1.

Finally suppose $t = 1$. Then $W \sim F_1' \mid H \in \Pi K_{(*)}$ and

$$(F_1 \mid H) \cdot X^m \sim W \cdot X^m \mid K \cdot X^m.$$

Matching this equation against Lemma 7.8 we see that $F_1 \mid H \in \Pi K_{(*)}$. In particular, F_1 is a generalised K-prime with a unique X-simplification $F_1 \to_X F_1'$ to another generalised K-prime F_1' whose X-norm is at least as large as any component of H, contradicting our assumption that the largest component has passed to H. □

To continue our investigations of the coordination of the two sides of a pumpable equation, it is convenient to work with a form of the equation in which the two sides of the equation are not necessarily fully factored:

$$(F \mid H)\cdot X^m \sim W\cdot X^m \mid R, \tag{71}$$

where

$$R = \prod_i K^{e_i}\cdot X^m. \tag{72}$$

and $H \in \Pi K_{(*)}$. The components F on the l.h.s. and $W\cdot X^m$ on the r.h.s. are in general parallel composites, but we insist that the factorisation of F contains the unique largest component on the l.h.s., and $W\cdot X^m$ the unique largest component on the r.h.s.

Lemma 7.14 *Consider any pumpable equation in partially factored form (71), where F and $W\cdot X^m$ contain, as factors, the unique largest components on the l.h.s. and r.h.s., respectively. Then W contains H as a factor, so that $W \sim V \mid H$ for some V, and equation (71) can be rewritten as*

$$(F \mid H)\cdot X^m \sim (V \mid H)\cdot X^m \mid R. \tag{73}$$

Proof. Apply any X-simplification to R on the r.h.s. of (71); by Lemma 7.13, it is F on the l.h.s. that responds. Furthermore, by the same lemma, the new largest component is contained in the derivative of F, provided R does not vanish. Repeating this argument $\|R\|_X$ times we see that H remains unscathed, giving $(F^* \mid H)\cdot X^m \sim W\cdot X^m$. □

Deflating a pumpable equation.

Lemma 7.15 *Consider a partially factored pumpable equation in the form (73). Let $H \to_X H'$ be any X-simplification of H. Then*

$$(F \mid H')\cdot X^m \sim (V \mid H')\cdot X^m \mid R. \tag{74}$$

Moreover, provided $\|H\|_X \geq 2$, the largest component on the r.h.s. remains in $(V \mid H')\cdot X^m$.

Proof. Recall (Theorem 7.9) that $H \in \Pi K_{(*)}$. We first show that any X-simplification $H \to_X H'$ applied to one side of (73) is matched by the same X-simplification on the other. Suppose (73) is a minimum X-norm counter-example: more precisely, there is a generalised K-prime $K_{(j)}$ occurring in H such that the X-simplifications $K_{(j)} \to_X K_{(j-1)}$ applied to H on the two sides of (73) do not match, as required by (74).

Re-express equation (74) as

$$(S \mid K_{(j)}^s)\cdot X^m \sim (T \mid K_{(j)}^t)\cdot X^m \mid R, \tag{75}$$

where $S \mid K_{(j)}^s \sim F \mid H$, $T \mid K_{(j)}^t \sim V \mid H$, and S and T do not contain $K_{(j)}$ as a factor. Note that $t \geq s$, by Lemma 7.14. In one X-simplification from (75) we arrive at

$$(S \mid K_{(j)}^{s-1} \mid K_{(j-1)})\cdot X^m \sim (T' \mid K_{(j)}^t)\cdot X^m \mid R$$

($K^t_{(j)}$ does not respond, since (75) is a counterexample, and R does not respond by Lemma 7.13), and in one further X-simplification we arrive at one of two possibilities:

$$(S \mid K^{s-2}_{(j)} \mid K^2_{(j-1)}) \cdot X^m \sim (T' \mid K^{t-1}_{(j)} \mid K_{(j-1)}) \cdot X^m \mid R \tag{76}$$

(the counterexample was minimal). Alternatively, starting at (75), we may arrive in one X-simplification at

$$(S' \mid K^s_{(j)}) \cdot X^m \sim (T \mid K^{t-1}_{(j)} \mid K_{(j-1)}) \cdot X^m \mid R \tag{77}$$

(again, because (75) is a counterexample), and in one further X-simplification at

$$\left.\begin{array}{r}(S'' \mid K^s_{(j)}) \cdot X^m \\ (S' \mid K^{s-1}_{(j)} \mid K_{(j-1)}) \cdot X^m\end{array}\right\} \sim (T' \mid K^{t-1}_{(j)} \mid K_{(j-1)}) \cdot X^m \mid R. \tag{78}$$

Now compare equations (76) and (78), and note that the r.h.s's are identical. However, whichever variant of equation (78) is taken, the l.h.s. of (78) has at least one more copy of $K_{(j)}$ than the l.h.s. of (76), a contradiction.

Finally, we need to show, under the assumption $\|H\|_X \geq 2$, that the largest component on the r.h.s. stays with $(V \mid H') \cdot X^m$ and does not pass to R. Suppose to the contrary that the largest (X-norm) component of $(V \mid H') \cdot X^m$ is no bigger than the largest component of R. Then, by Theorem 7.12, the r.h.s. of (74) consists only of non-exceptional factors, so that

$$(V \mid H') \cdot X^m \sim \prod_k K^{f_k} \cdot X^m,$$

for some non-increasing sequence (f_k), and R is as in (72) with (e_i) non-increasing. Note that $f_1 \leq e_1$. Starting with (73), apply a sequence of X-simplifications to R to yield a parallel composition R^* of non-exceptional factors, whose largest factor has X-norm f_1. By Lemma 7.13, it is F that responds on the l.h.s.:

$$(F^* \mid H) \cdot X^m \sim (V \mid H) \cdot X^m \mid R^*.$$

Now apply the X-simplification $H \to_X H'$ to the r.h.s.; the largest factor on the r.h.s. occurs to a power at least two, so, by Lemma 7.11, the l.h.s. is a parallel prime. But this is not possible, as $\|F^*\|_X, \|H\|_X \geq 2$. □

Lemma 7.16 *Consider a pumpable equation in the form (73), where* $H \in \Pi K_{(\leq h)}$ *Suppose* H^* *is any generalised* K*-term reachable via some sequence of* X*-simplifications from* H*. Then*

$$(F \mid H^*) \cdot X^m \sim (V \mid H^*) \cdot X^m \mid R;$$

in particular,

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R,$$

and

$$F \cdot X^m \sim V \cdot X^m \mid R.$$

Proof. Apply Lemma 7.15 repeatedly. □

7.5 The general form

We now show that Lemma 7.16 has a kind of converse; this will allow us to deduce that any pumpable equation, however complex, may be obtained from a relatively simple base equation by adding generalised K-primes evenly to the two sides. This construction justifies the choice of the name "pumpable" for this class of mixed equation.

Inflating a pumpable equation.

Lemma 7.17 *Consider a pumpable equation in the form (73), specialised to the case when* H *is a generalised* K*-prime:*

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R. \tag{79}$$

Note that the equation is not necessarily completely factored, but that the unique largest prime components on the l.h.s. and r.h.s. are contained in F *and* $(V \mid K_{(h)}) \cdot X^m$*, respectively. Then, for any* $H \in \Pi K_{(\leq h)}$*,*

$$(F \mid H) \cdot X^m \sim (V \mid H) \cdot X^m \mid R. \tag{80}$$

Furthermore, bisimulation preserving derivations of (80) are independent of H*: thus if* F *makes a derivation on the l.h.s. (or one of* V *or* H *makes a derivation on the r.h.s.) then the response on the other side is independent of* H*.*

Proof. Fix the X-monomorphic term K. We claim that if we add the set of pairs

$$\mathcal{P} = \Big\{ \big\langle (F \mid H) \cdot X^m,\ (V \mid H) \cdot X^m \mid R \big\rangle : h \in \mathbb{N}^+, H \in \Pi K_{(\leq h)}, \\ \text{and } F, V, R \text{ satisfy } (F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R \Big\}$$

to the maximum bisimulation relation, the result is still a bisimulation (obviously the maximum one). It is to be understood that the equation

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R$$

appearing in the definition of $\mathcal{P}$ is of the form (73); specifically, F and $(V \mid K_{(h)}) \cdot X^m$ satisfy the conditions placed upon them in the statement of the lemma. We need to check that for each pair $\langle P, Q \rangle \in \mathcal{P}$ and each derivation $P \to P'$ there is a derivation $Q \to Q'$ such that $(P', Q') \in \mathcal{P} \cup \sim$, and similarly with the roles of P and Q reversed.

Take a typical pair

$$\big\langle (F \mid H) \cdot X^m,\ (V \mid H) \cdot X^m \mid R \big\rangle \in \mathcal{P}, \tag{81}$$

corresponding to a bisimilar base pair

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R. \tag{82}$$

Case R. Consider first a derivation $R \to R'$ applied to the r.h.s. of (81). Recall that, by Theorem 7.12, R is a parallel composition of non-exceptional factors of the form $K^t \cdot X^m$. The only interesting derivations for us are X-norm decreasing ones (the others leave the r.h.s. unchanged modulo the creation or destruction of powers of X). Suppose, then that $R \to_X R'$ is some X-simplification of R. By Lemma 7.13, this X-simplification applied to the r.h.s. of (82) is matched on the l.h.s. by $F \to_X F'$:

$$(F' \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R'.$$

Then, by definition of $\mathcal{P}$,

$$\big\langle (F' \mid H) \cdot X^m,\ (V \mid H) \cdot X^m \mid R' \big\rangle \in \mathcal{P}.$$

Case H. Next consider a derivation $H \to H'$ applied to the r.h.s. of (81). Again, the only interesting case is the X-norm decreasing one. Suppose then that $H \to_X H'$ is some X-simplification of H. If $H' \in \Pi K_{(\le h)}$ then it is immediate from (82) and the definition of $\mathcal{P}$ that

$$\big\langle (F \mid H') \cdot X^m,\ (V \mid H') \cdot X^m \mid R \big\rangle \in \mathcal{P}. \tag{83}$$

Otherwise, $H' \in \Pi K_{(\le h-1)}$; but then, by Lemma 7.15, we have

$$(F \mid K_{(h-1)}) \cdot X^m \sim (V \mid K_{(h-1)}) \cdot X^m \mid R,$$

leading once more to (83).

Case V. Now consider a derivation $V \to V'$ applied to the r.h.s. of (81). Recall that V may be a parallel composite. If the derivation $V \to V'$ induces a reduction of an instance of $K_{(h)}$ in V, then finesse by using the copy of $K_{(h)}$ in H in place of the one in V. This reduces us to Case H. Otherwise, by Lemma 7.15, the derivation $V \to V'$ on the r.h.s. of (82) is matched by $F \to F'$ on the l.h.s., yielding

$$(F' \mid K_{(h)}) \cdot X^m \sim (V' \mid K_{(h)}) \cdot X^m \mid R. \tag{84}$$

Provided we can assure ourselves that the largest components on the l.h.s. and r.h.s. remain with F' and $(V' \mid K_{(h)}) \cdot X^m$,

$$\big\langle (F' \mid H) \cdot X^m,\ (V' \mid H) \cdot X^m \mid R \big\rangle \in \mathcal{P}$$

will follow from the definition of $\mathcal{P}$. It is easy to see that the largest component on the l.h.s. remains with F. For if not, the l.h.s. would be composed entirely of generalised K-primes (Theorem 7.9); but then (Lemma 7.8) the r.h.s. cannot contain an occurrence of $K_{(h)}$.

As for the r.h.s. suppose to the contrary that the largest (X-norm) component of $(V' \mid K_{(h)}) \cdot X^m$ is no bigger than the largest component of R. Then, by Theorem 7.12, the r.h.s. of (84) consists only of non-exceptional factors, so that

$$(V' \mid K_{(h)}) \cdot X^m \sim \prod_k K^{f_k} \cdot X^m,$$

for some non-increasing sequence (f_k), and R is as in (72) with (e_i) non-increasing. Note that $f_1 \leq e_1$. We proceed as in the proof of Lemma 7.15. Starting with (82), apply a sequence of X-simplifications to R to yield a parallel composition R^* of non-exceptional factors, whose largest factor has X-norm f_1. By Lemma 7.13, it is F that responds on the l.h.s.:

$$(F^* \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R^*;$$

moreover, $\|F^*\|_X > h \geq 1$. Now apply the X-simplification $V \rightarrow_X V'$ to the r.h.s.; as this is matched by F^*, which has norm at least two, the parallel composition on the l.h.s. is preserved. However, the largest factor on the r.h.s. occurs to a power at least two, so, by Lemma 7.11, the l.h.s. is a parallel prime, a contradiction.

Case F. The situations that occur as a result of the derivation $F \rightarrow F'$ have already been analysed under Case R and Case V.

Case F exhausts the possibilities and concludes the proof. □

Ideally we would like a stronger version of Lemma 7.17 in which the basis equation (79) is replaced by the the simpler equation

$$F_1 \cdot X^m \sim V \cdot X^m \mid R; \tag{85}$$

but such a strengthening would not be valid unless complex side conditions were placed on V. Nevertheless, the classification of pumpable equations that follows from Lemmas 7.16 and 7.17 will prove adequate, if we exercise care.

General form of a pumpable equation.

Theorem 7.18 *The general form of pumpable equation is*

$$(F \mid H) \cdot X^m \sim (V \mid H) \cdot X^m \mid R \tag{86}$$

where $H \in \Pi K_{(\leq h)}$ for some h, and R is a product (72) of non-exceptional components; furthermore, the largest parallel prime factor of F has norm greater than h and the other factors of F (if any) are generalised K-primes; finally, the term $(V \mid H) \cdot X^m$ contains the largest parallel prime factor on the r.h.s. The terms F, V and R satisfy

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R, \tag{87}$$

and equation (86) holds for all $H \in \Pi K_{(\leq h)}$. Furthermore, bisimulation preserving derivations of (80) are independent of H, as in Lemma 7.17.

Proof. Equations (87) follows from (86) by Lemma 7.16. Then equation (86) for general $H \in \Pi K_{(\leq h)}$ follows from (87) by Lemma 7.17. (Note that the largest factor on the r.h.s. of (87) remains with $(V \mid K_{(h)}) \cdot X^m$ by Lemma 7.15.) □

The key feature of Theorem 7.18 is that it allows us to represent the infinite family of equations of the form (86)—with F, V and R fixed, and H ranging over $\Pi K_{(\leq h)}$—by a single "schema" with "contexts" on either side into which an arbitrary term $H \in \Pi K_{(\leq h)}$ may be slotted. (Details will be supplied when we come to the decision procedure itself.) In general, the schema will be much more compact than the pumpable equation itself. However, will still be too large if the component F is.

We know that F is not a parallel composition (or more accurately need not be a parallel composition, otherwise we could absorb extra factors into H); furthermore, we are not too concerned if F is an atom, since the norm of the equation will then be bounded. However, it is important for us to be able to deal with the situation in which F is a sequential composition. Such an equation might be monomorphic, in which case its structure is simple enough to analyse using Theorem 5.2. Otherwise, Corollary 5.3 tells us that F factors as $F \sim \widehat{F} \cdot X^{m'}$, in which case (85) hides an underlying pumpable equation with "tail" $X^{m+m'}$. The final theorem shows that this underlying equation has a restricted form—all parallel factors of R have X-norm one—allowing further simplification to take place.

When one pumpable equation is built on top of another

Theorem 7.19 *Let*

$$(F \mid K_{(h)}) \cdot X^m \sim (V \mid K_{(h)}) \cdot X^m \mid R \tag{88}$$

be a pumpable equation in the usual not-fully-factored form (74), and suppose $F \sim \widehat{F} \cdot X^{m'}$ *for some* $\widehat{F}$ *and* $m' \geq 1$, *and suppose further that* $\widehat{F}$ *is a parallel composition. Then* R *is a power of* $K \cdot X^m$, *and* $h = 1$. *Moreover,* $V \sim \widehat{V} \cdot X^{m'}$ *and* $K \sim \widehat{K} \cdot X^{m'}$ *for some* $\widehat{V}$ *and* $\widehat{K}$, *yielding the new pumpable equation*

$$\widehat{F} \cdot X^{m+m'} \sim \widehat{V} \cdot X^{m+m'} \mid R. \tag{89}$$

Conversely, suppose K *is an* X*-unit and*

$$F \cdot X^m \sim V \cdot X^m \mid R \tag{90}$$

is an equation where R *is a power of* $K \cdot X^m$. *Suppose further that* V *has the property that* $V \rightsquigarrow V^*$ *and* $\|V^*\|_X = 1$ *entails* $V^* \sim K \mid X^j$ *for some* j. *Then*

$$(F \mid K) \cdot X^m \sim (V \mid K) \cdot X^m \mid R, \tag{91}$$

i.e., noting $h = 1$, *we recover (88).*

Proof. Annihilating $K_{(h)}$ from the two sides of (88), using Lemma 7.15, yields the new pumpable equation

$$\widehat{F} \cdot X^{m'} \cdot X^m \sim V \cdot X^m \mid R; \tag{92}$$

then, by Corollary 5.3, $V \sim \widehat{V} \cdot X^{m'}$ and (89) follows. Also by Corollary 5.3, every (parallel) prime factor in R is bisimilar to a term of the form $A \cdot X^{m+m'}$. Consider a typical prime factor $K^j \cdot X^m$ of R. Then $K^j \cdot X^m \sim A \cdot X^{m+m'} \sim A \cdot X^{m'} \cdot X^m$, entailing

$$A \cdot X^{m'} \sim K^j. \tag{93}$$

Now A cannot be a parallel composition, otherwise (93) would be a pumpable equation with only X-units on the r.h.s., which is impossible by Lemma 7.11. But $A \cdot X^{m+m'}$ is a factor on the r.h.s. of a pumpable equation, namely (89), and the only such factors for which A is a parallel prime are those of X-norm one. It follows that $j = 1$. Thus R is a power of $K \cdot X^m$. Note that $K \cdot X^m \sim \widehat{K} \cdot X^{m+m'}$ by Corollary 5.3.

We now show that $h = 1$. Suppose to the contrary that $h \geq 2$. Construct a generalised $\widehat{K}$-prime $\widehat{K}_{(h)}$ satisfying

$$\widehat{K}_{(h)} \cdot X^{m+m'} \sim (\widehat{K} \cdot X^{m+m'})^h \sim (K \cdot X^m)^h \sim K_{(h)} \cdot X^m,$$

and note that $K \sim \widehat{K} \cdot X^{m'}$. Since $\widehat{V} \cdot X^{m+m'}$ contains the largest factor on the r.h.s. of a pumpable equation, $\widehat{V}$ is a parallel composition. Thus, it is possible to reduce $\widehat{V} \cdot X^{m'}$ to ε in such a way that at any intermediate stage

$$\widehat{V} \cdot X^{m'} \rightsquigarrow \widehat{V}^* \cdot X^{m'} \rightsquigarrow \varepsilon, \tag{94}$$

with $\|\widehat{V}^*\|_X \geq 2$, we have that $\widehat{V}^*$ is a parallel composition. Consider any such intermediate term. Certainly $\widehat{V}^* \cdot X^{m'} \not\sim \widehat{K}_{(h)} \cdot X^{m'}$, since $\widehat{K}_{(h)}$ is a parallel prime (Observation 7.5). Neither can $\widehat{V}^* \cdot X^{m'}$ contain $\widehat{K}_{(h)} \cdot X^{m'}$ as a (proper, parallel) factor, for then we would obtain a pumpable equation of the form

$$\widehat{V}^* \cdot X^{m'} \sim \widehat{K}_{(h)} \cdot X^{m'} \mid S,$$

which again contradicts primality of $\widehat{K}_{(h)}$. So at no intermediate step in the reduction sequence (94) does $\widehat{V}^* \cdot X^{m'}$ contain $\widehat{K}_{(h)} \cdot X^{m'}$ as a factor.

Now rewrite (88) as

$$(\widehat{F} \cdot X^{m'} \mid \widehat{K}_{(h)} \cdot X^{m'}) \cdot X^m \sim (\widehat{V} \cdot X^{m'} \mid \widehat{K}_{(h)} \cdot X^{m'}) \cdot X^m \mid R,$$

and annihilate $\widehat{V} \cdot X^{m'}$ using a sequence of the type just described. Note that the response on the l.h.s. is always by $\widehat{F}$, so we end up with a pumpable equation of the form

$$(\widehat{F}^* \cdot X^{m'} \mid \widehat{K}_{(h)} \cdot X^{m'}) \cdot X^m \sim \widehat{K}_{(h)} \cdot X^{m'} \cdot X^m \mid R \sim (K \cdot X^m)^n$$

for some n, again contradicting Lemma 7.11. We must conclude that $h = 1$, and $K_{(h)} = K$.

Finally, starting with (90) we need to deduce (91). By assumption, any (X-free) X-unit reachable from V is bisimilar to K. Armed with this fact, we may effectively construct a bisimulation relation containing (91) by mimicking the assumed bisimulation relation containing (90), as in Lemma 7.17. The only misfortune that can befall us is if V reaches ε before K^i does: but this need not occur because in a previous step some reduct of V would be bisimilar to K, and we could have selected the explicit K instead. □

8 Mixed equations with a non-series-parallel tail

Theorem 7.18 provides an effective characterisation of pumpable equations, i.e., mixed equations whose "tail" is the power of a unit X that satisfies $X \cdot X \sim X \mid X$. We now need to characterise equations in which $X \cdot X \not\sim X \mid X$. Fortunately, this turns out to be an easier task.

Suppose we have a mixed equation

$$F \cdot X^m \sim A_1 \cdot X^m \mid \cdots \mid A_n \cdot X^m \mid X^l, \tag{95}$$

where the unit X satisfies $X \cdot X \not\sim X \mid X$. By Theorem 4.2(e), the exponent m is bounded by the maximum norm of an immediate derivative of X, and, by Lemma 6.2, there is at least one immediate derivation $X \to A \cdot X^m$, for which $A \cdot X^m$ is not bisimilar to a power of X. We shall show, eventually, that $m = 1$, X is finite state, and F is not a parallel composition. Theorem 8.6 will summarise the remaining possibilities, which almost amount to F being atomic.

Definition 8.1 *For a term* T*, the* internal parallelism $\mathrm{IP}(T)$ *of* T *is the maximum, over all subterms of* T *with the form* $S \cdot (T_1 \mid T_2)$*, of the norm* $\|T_1 \mid T_2\|$ *of* $T_1 \mid T_2$*. Here,* S *is assumed to be non-trivial. If there are no subterms of the prescribed form,* $\mathrm{IP}(T) = 0$*.*

Internal parallelism of a term.

Lemma 8.1 *Let*

$$d = \max\left\{\|S\| : Y \to S \textit{ and } Y \textit{ is an atom}\right\}.$$

If $T \to T'$ *then* $\mathrm{IP}(T') \le \max\{\mathrm{IP}(T), d\}$*.*

Proof. Structural induction on terms. □

Lemma 8.2 *For any mixed equation (95) with* $X \cdot X \not\sim X \mid X$*:*

The tail contains just one X.

(a) $m = 1$*;*

(b) if $X \rightsquigarrow T$ *then* $T \not\sim X^2$*.*

Proof. If $m > 1$ then, by Lemma 6.2, $X \to A \cdot X^m \rightsquigarrow X^2$. Hence (a) follows from (b). We shall assume that (b) is false, i.e., $X \rightsquigarrow X^2$, and obtain a contradiction.

We assume that m is as large as possible—the maximum of m is well defined by Theorem 4.2(e)—and start with the corresponding minimal mixed equation

$$Y \cdot X^m \sim X^{m+1}. \tag{96}$$

(Refer to Theorem 4.2(d).) Since $X \rightsquigarrow X^2 \rightsquigarrow X^3 \rightsquigarrow \ldots$, an equation of the form

$$F \cdot X^m \sim X^n \tag{97}$$

holds for arbitrary $n > m$. For sufficiently large n, the component F is not atomic. Can F be a sequential composition? By Corollary 5.3, equation (97) would have to be monomorphic, otherwise F could be factored to yield a mixed equation with a higher power of X on the l.h.s., contradicting maximality of m. But equation (97) cannot be monomorphic, since X, and hence F, has norm-increasing derivations.

The only remaining possibility is that F is a parallel composition; since the r.h.s. of (97) has valence one, F must be a prime power. By the same reasoning, the unique reduct F' of F is also a power. It follows that F is a power of units, and, in light of (96),

$$Y^{n-m} \cdot X^m \sim X^n, \tag{98}$$

for arbitrarily large n, and hence (by reduction) for all $n > m$.

Let A be a term such that (i) $X \rightsquigarrow A \cdot X^m$, (ii) $A \cdot X^m$ is not itself a power of X, but (iii) any reduct of $A \cdot X^m$ is a power of X. Starting with (97) and n a large prime number, transform the r.h.s. to $(A \cdot X^m)^n$. The l.h.s. responds with $F \rightsquigarrow F^*$, giving

$$F^* \cdot X^m \sim (A \cdot X^m)^n. \tag{99}$$

The term F^* is too big to be an atom. We shall see that F^* cannot be a sequential composition. Suppose to the contrary that it is; then, by Corollary 5.3 and maximality of m, equation (99) is monomorphic, so that $F^* \sim Z \cdot F^\dagger$, where Z is a monomorphic atom. Again, $F^\dagger$ is too large to be an atom, and cannot be a sequential composition, by maximality of m. If $F^\dagger$ is a parallel composition, then $\mathrm{IP}(F^*) \geq \|F^\dagger\| = \|F^*\| - 1$, which is inconsistent with Lemma 8.1 when n is sufficiently large. We a forced to conclude that F^* is a parallel composition.

The r.h.s. of (99) has valence one (all reducts of $A \cdot X^m$ are bisimilar to a certain power of X), so the term F^* is in fact a power, say

$$E^k \cdot X^m \sim (A \cdot X^m)^n, \tag{100}$$

where $k \geq 2$. In the light of (98), the length of a shortest sequence of reductions that transforms the r.h.s. of (100) to (a term bisimilar to) a power of X is equal to that of the shortest such sequence that transforms the l.h.s. to a power of Y. On the r.h.s. that minimum length is n, and on the l.h.s. it is a multiple of k. Since $k \geq 2$ and n is prime, $n = k$. But then in (100) the norm of the l.h.s. is congruent to m (mod n), while the norm of the r.h.s. is congruent to zero. □

Lemma 8.3 *Suppose* $X \rightsquigarrow A \cdot X$ *and*

$$(F_1 \mid F_2 \mid \ldots \mid F_r) \cdot X \sim (A \cdot X)^2, \tag{101}$$

where F_i *are parallel primes, and* $X \cdot X \not\sim X \mid X$*. Suppose also that the two reductions* $A \cdot X \to A' \cdot X$ *applied in sequence on the r.h.s. are answered by different components on the l.h.s.:*

$$(F_1' \mid F_2' \mid \ldots \mid F_r) \cdot X \sim (A' \cdot X)^2. \tag{102}$$

Then $F_1 \sim F_2$ *and* $F_1' \sim F_2'$*.*

Proof. Suppose $F_1 \to F_1'$ is the response to the first reduction $A \cdot X \to A' \cdot X$:

$$(F_1' \mid F_2 \mid \ldots \mid F_r) \cdot X \sim A' \cdot X \mid A \cdot X, \tag{103}$$

and $F_2 \to F_2'$ the response to the second. Consider what happens if the order of the two reductions is reversed, i.e., the reduction $F_2 \to F_2'$ is performed first and $F_1 \to F_1'$ second. We shall show that the first reduction $F_2 \to F_2'$ on the l.h.s. must be matched by $A \cdot X \to A' \cdot X$ on the r.h.s., just as before. Assume to the contrary that $F_2 \to F_2'$ is matched by $A \cdot X \to A_1 \cdot X$, with $A_1 \not\sim A'$:

$$(F_1 \mid F_2' \mid \ldots \mid F_r) \cdot X \sim A_1 \cdot X \mid A \cdot X. \tag{104}$$

Now apply the reduction $F_1 \to F_1'$ to the l.h.s.; the response on the r.h.s. is either of the form $A \cdot X \to A_2 \cdot X$ or $A_1 \cdot X \to A_1' \cdot X$. Since the end result is still (102), we have

$$(A' \cdot X)^2 \sim \begin{cases} A_1 \cdot X \mid A_2 \cdot X, & \text{or} \\ A_1' \cdot X \mid A \cdot X. \end{cases}$$

In either case we see that $A' \cdot X$ cannot be parallel prime (in the first because of our assumption that $A' \cdot X \not\sim A_1 \cdot X$; in the second because $\|A_1' \cdot X\| < \|A' \cdot X\|$). So $A' \cdot X$ is the l.h.s. of some mixed equation

$$A' \cdot X \sim \prod_i B_i \cdot X,$$

and

$$X \rightsquigarrow A \cdot X \to A' \cdot X \sim \prod_i B_i \cdot X \rightsquigarrow X^2,$$

in contradiction to Lemma 8.2. Hence our initial assumption that $A_1 \not\sim A'$ was incorrect, and the r.h.s's of (103) and (104) are in fact bisimilar, entailing $F_1' \mid F_2 \sim F_1 \mid F_2'$. Since $\|F_1'\| < \|F_1\|$, and F_1 and F_2 are primes, $F_1 \sim F_2$; but then $F_1' \sim F_2'$. □

Lemma 8.4 *Suppose* $X \rightsquigarrow A \cdot X$, $X \cdot X \not\sim X \mid X$ *and* $F \cdot X \sim (A \cdot X)^2$*. Then*

(a) F *is not a parallel composition;*

(b) X *is finite state.*

Proof. To prove (a), we assume that equation (101) is a minimal counterexample and obtain a contradiction. Suppose first that $||A|| \geq 2$, so that $||F|| \geq 5$ where $F = F_1 \mid \ldots \mid F_r$. We could then obtain a smaller counterexample: perform a reduction $F_1 \rightarrow F_1'$ (to the largest prime) on the l.h.s., which is matched by $A \rightarrow A'$ on the r.h.s.; and then a further reduction $A \rightarrow A'$ on the r.h.s. that is answered by the l.h.s. (If $r \geq 3$, or $r = 2$ and $F_1 \sim F_2$, then is is clear that the l.h.s. remains a parallel composition; if $r = 2$ and $F_1 \not\sim F_2$, then F_1 cannot be annihilated in two steps because it has norm at least three, and F_2 cannot be touched by Lemma 8.3.)

We are left with the case $||A|| = 1$. The r.h.s. $(A \cdot X)^2$ has valence one (since A has a unique reduction) and so must the l.h.s. It follows that F must be a power $F \sim E^k$, and since $||F \cdot X|| = 4$ we must have $E^3 \cdot X \sim (A \cdot X)^2$ and $||E|| = 1$. Annihilating $A \cdot X$ on the r.h.s. we obtain $E \cdot X \sim A \cdot X$, while annihilating two As we obtain $E \cdot X \sim X \mid X$. Hence $X \rightsquigarrow A \cdot X \sim X^2$, which is not possible by Lemma 8.2. This establishes (a).

For (b), start with the minimal equation $Y \cdot X \sim X \mid X$. If X is infinite state then it has arbitrarily large derivatives; in particular we may find an arbitrarily large term A such that $X \rightsquigarrow A \cdot X$ and A has a norm-increasing immediate derivation. Applying this sequence of derivations to the l.h.s. of the minimal equation, the r.h.s. is forced to follow:

$$F \cdot X \sim (A \cdot X)^2, \tag{105}$$

with $||F||$ arbitrarily large. The term F is too big to be atomic, and equation (105) cannot be monomorphic since A has a norm-increasing derivative. Thus, by Corollary 5.3, F cannot be a sequential composition. Finally, F is not a parallel composition by part (a). □

L.h.s. is not a parallel composition.

Lemma 8.5 *Suppose*

$$F \cdot X \sim A_1 \cdot X \mid \ldots \mid A_n \cdot X \mid X^l, \tag{106}$$

is a mixed equation with $X \cdot X \not\sim X \mid X$*; then the term* F *is not a parallel composition.*

Proof. We assume that (106) is a minimal counterexample and obtain a contradiction. Suppose first that the counterexample has norm three (the smallest possible). If the r.h.s. is X^3 then the l.h.s. has valence one, and must be of the form $Y^2 \cdot X$. Thus

$$Y^2 \cdot X \sim X^3 \quad \text{leading to} \quad Y \cdot X \sim X^2; \tag{107}$$

and X, and hence Y, is finite state by Lemma 8.4. Let x and y denote the lengths of the longest sequences of norm-increasing derivations available to X and Y, respectively. Then equations (107) give $2y = 3x$ and $y = 2x$ which imply $x = 0$. However, we know that X has at least one norm-increasing derivation.

Staying with norm three, the other possibility is

$$(A \mid Y) \cdot X \sim A \cdot X \mid X \quad \text{leading to} \quad Y \cdot X \sim X^2. \tag{108}$$

Again, X and Y are finite state. First, suppose A is finite state, and let a denote the length of the longest sequence of norm-increasing derivations available to A. Then equations (108) give $a + y = a + x$ and $y = 2x$, again entailing $x = 0$. Next, suppose that $A \rightsquigarrow A^*$ where $A^* \neq \varepsilon$ is finite state. Choose A^* firstly to minimise the number of derivations required to reach A^* from A, and secondly to maximise the length a^* of a sequence of norm-increasing transitions starting at A^*. Then, applying $A \rightsquigarrow A^*$ on the l.h.s., using a minimum-length sequence of derivations, we reach

$$(A^* \mid Y) \cdot X \sim \widehat{A} \cdot X \mid X,$$

where $\widehat{A}$ is finite state. Thus $a^* + y = \hat{a} + x \leq a^* + x$, where $\hat{a}$ is the length of a longest sequence of norm-increasing derivations available to $\widehat{A}$. Thus $y \leq x$, which together with $y = 2x$ entails $x = 0$, a contradiction. Finally, suppose that the only finite state term reachable from A is ε. Starting with the left equation in (108), apply norm-increasing derivations to Y until A responds for the first time:

$$(A \mid Y^*) \cdot X \sim A' \cdot X \mid X^*.$$

(A must eventually respond because $y = 2x$ and $x > 0$.) Now reduce $A \rightsquigarrow \varepsilon$ on the l.h.s. via a sequence of $\|A\| < \|A'\|$ reductions; the l.h.s. is now finite state, whereas the r.h.s. is still infinite state. This eliminates the possibility of a norm-three counterexample.

A minimum counterexample of norm greater than three must, as we have seen on previous occasions, have the form

$$(F \mid Z) \cdot X \sim A \cdot X \mid X, \tag{109}$$

with $\|Z\| = 1$. (If either side had more than two components, or had no components of norm one, we could easily obtain a smaller-norm counterexample.) Moreover, again by minimality, F has a unique reduction $F \rightarrow F'$ matching $X \rightarrow \varepsilon$ and A has a unique reduction $A \rightarrow A'$ matching $Z \rightarrow \varepsilon$. Reducing X, we obtain $(F' \mid Z) \cdot X \sim A \cdot X$, and hence $F' \mid Z \sim A$. Since A has a unique reduction, $A \sim Z^t$ and $F' \sim Z^{t-1}$ where $t \geq 2$. Substituting for A, equation (109) may be rewritten as

$$(F \mid Z) \cdot X \sim Z^t \cdot X \mid X. \tag{110}$$

On the other hand, applying the reduction $Z^t \rightarrow Z^{t-1}$ to the r.h.s. of (110) yields

$$F \cdot X \sim Z^{t-1} \cdot X \mid X,$$

and since the l.h.s. has a unique reduction,

$$Z^{t-1} \cdot X \sim X^t. \tag{111}$$

Since X has a norm-increasing derivation, so must Z; let $Z \rightarrow \widehat{Z}$ be one such. Applying this derivation to the l.h.s. of (110) leads to one of two equations:

$$(F \mid \widehat{Z}) \cdot X \sim \begin{cases} (\widetilde{Z} \mid Z^{t-1}) \cdot X \mid X, & \text{or} \\ Z^t \cdot X \mid \widehat{B} \cdot X. \end{cases} \tag{112}$$

where $Z \rightarrow \widetilde{Z}$ and $X \rightarrow \widehat{B} \cdot X$ are norm-increasing derivations. In the former instance, let $X \rightarrow \widetilde{B} \cdot X$ be the norm-increasing derivation induced when $Z \rightarrow \widetilde{Z}$ is applied to the l.h.s. of (111), yielding

$$(\widetilde{Z} \mid Z^{t-2}) \cdot X \sim \widetilde{B} \cdot X \mid X^{t-1}. \tag{113}$$

Applying the reduction $Z \rightarrow \varepsilon$ to the r.h.s's of (112) preserves the parallel composition on the l.h.s.—note that $\|F\|, \|\widehat{Z}\| \geq 2$—and leads to

$$(\text{parallel composition}) \cdot X \sim \begin{cases} (\widetilde{Z} \mid Z^{t-2}) \cdot X \mid X, & \text{or} \\ Z^{t-1} \cdot X \mid \widehat{B} \cdot X. \end{cases}$$

Comparing with (111) and (113), we see that both possibilities have the form

$$(\text{parallel composition}) \cdot X \sim B \cdot X \mid X^t,$$

where B stands for either $\widehat{B}$ or $\widetilde{B}$. (Note that in either case, $X \rightarrow B \cdot X$ is a possible derivation.) Now reduce the r.h.s. from $B \cdot X \mid X^t$ to $B \cdot X \mid X$, via a sequence of $t-1$ reductions; the valence of the r.h.s. remains constant during this process, and hence the parallel composition on the l.h.s. is still preserved:

$$(\text{parallel composition}) \cdot X \sim B \cdot X \mid X.$$

Finally apply the norm-increasing derivation $X \rightarrow B \cdot X$ to the r.h.s. and appeal to Lemma 8.4 to obtain the desired contradiction. □

General form of a mixed equation with $X \cdot X \not\sim X \mid X$.

Theorem 8.6 *The general form of a mixed equation which is neither monomorphic nor pumpable is*

$$F \cdot X \sim A_1 \cdot X \mid \ldots \mid A_n \cdot X \mid X^l$$

where F *is an atom, and* X *is a unit satisfying* $X \cdot X \not\sim X \mid X$*; moreover* X *is finite state.*

Proof. The term F is not a sequential composition by Corollary 5.3 and Lemma 8.2, and is not a parallel composition by Lemma 8.5. The unit X occurs to the power one on the l.h.s. by Lemma 8.2. Finally, by first reducing to the minimal mixed equation $Y \cdot X \sim X \mid X$, and then applying matched norm-increasing derivations $X \rightarrow A \cdot X$ to the r.h.s. we place ourselves in the situation of Lemma 8.2; hence X is finite state. □

9 The decision procedure

Subsection 9.1 will provide a high-level description of the Decision Procedure; Subsections 9.2 and 9.3 will present its main component procedures—expansion and simplification—along with an informal commentary; finally, Subsection 9.4 will justify correctness.

9.1 Overview

Figure 3 presents a high-level view of the proposed procedure for deciding whether a given terms P_0 and Q_0 of terms is bisimilar. The procedure maintains two sets, $\mathcal{B}$ and $\mathcal{P}$, whose elements are pairs of terms; $\mathcal{B}$ initially contains just the pair $\langle P_0, Q_0\rangle$, while $\mathcal{P}$ is empty. Roughly, our strategy is to augment the set $\mathcal{B}$ until either (a) $\mathcal{B}$ becomes a finite basis (in some sense) for a bisimulation that includes the pair $\langle P_0, Q_0\rangle$, or (b) some inconsistency is detected. The set $\mathcal{P}$, which at all times satisfies the inclusion $\mathcal{P} \subseteq \mathcal{B}$, may be interpreted as the set of "processed" pairs.

The computation proceeds via a sequence of nondeterministic steps, in which a pair $\langle P, Q\rangle \in \mathcal{B} \setminus \mathcal{P}$ is selected, processed, and added to $\mathcal{P}$. The type of processing—"expansion" or "simplification"— depends on whether $\|P\|$ exceeds some bound b. This bound must be chosen sufficiently large; it suffices to take b to be twice the largest norm of any atom. As a result of processing $\langle P, Q\rangle$, a number of new pairs may be added to $\mathcal{B}$; however, we are able to bound the norm of these processes, and hence deduce that the procedure must eventually halt. If $P_0 \sim Q_0$, the nondeterministic choices can be made so that only bisimilar pairs are ever added to $\mathcal{B}$; in this case, the Step 3 always succeeds, and the procedure accepts when all pairs in $\mathcal{B}$ have been processed. Conversely, if $P_0 \not\sim Q_0$, then every nondeterministic branch will arrive at an inconsistency, which will manifest itself in Step 3 failing during an "expansion." Note that, even if $P_0 \sim Q_0$, many nondeterministic branches will fail; the point is that at least one must succeed.

The elements of the set $\mathcal{B}$ are, in fact, slightly more general than has so far been admitted. In addition to simple pairs of terms, we also allow *schemas* of the form

Definition of schema; norm of a schema.

$$\big\langle (F \mid [\,]_h) \cdot X^m,\ (V \mid [\,]_h) \cdot X^m \mid R \big\rangle, \tag{114}$$

where R is an explicit parallel composition of terms of the form $K^j \cdot X^m$ (i.e., non-exceptional factors). The notation $[\,]_h$ stands for a *context* into which can be substituted any generalised K-term $H \in \Pi K_{(\leq h)}$ (the same term H on the two sides of the schema). The schema (114) is intended to stand for the infinite set of pairs of processes that can be obtained by such substitutions. So the set $\mathcal{B}$, though itself finite, represents a potentially infinite set of putatively bisimilar pairs of processes. The *norm* of a schema is the norm of the l.h.s. (which should be equal to the norm of the r.h.s.) with the context erased.

The input is a pair of terms $\langle P_0, Q_0\rangle$; we are required to decide if $P_0 \sim Q_0$.

STEP 1: If $||P_0|| \neq ||Q_0||$ then reject.

STEP 2: Set $\mathcal{B} := \{\langle P_0, Q_0\rangle\}$ and $\mathcal{P} := \emptyset$. (The set $\mathcal{B}$ is used to accumulate basis pairs; the set $\mathcal{P} \subseteq \mathcal{B}$ is the set of basis pairs that have been "processed.")

STEP 3: While $\mathcal{P} \subset \mathcal{B}$ choose a pair $\langle P, Q\rangle \in \mathcal{B} \setminus \mathcal{P}$, and process $\langle P, Q\rangle$ as follows.

- If $||P|| = ||Q|| \leq b$ then attempt to expand $\langle P, Q\rangle$ (refer to Figure 4 and Section 9.2); if the expansion fails then reject.
- Otherwise ($||P|| = ||Q|| > b$) apply the simplification step (refer to Figure 5 and Section 9.3) to $\langle P, Q\rangle$.

STEP 4: Accept. (At this point, $\mathcal{P} = \mathcal{B}$, and $\mathcal{B}$ is a basis for a bisimulation containing $\langle P, Q\rangle$.)

Figure 3: A high-level view of the Decision Procedure.

In order to understand the decision procedure in greater depth, it is necessary to introduce the notion of finite approximation (from above) to the maximum bisimulation relation $\sim$.

Finite approximants $\sim_k$ to the maximum bisimulation $\sim$.

Definition 9.1 *The sequence of binary relations* ($\sim_k$: $k \in \mathbb{N}$) *on* Proc *is defined as follows. For all* $P, Q \in \text{Proc}$*: (i)* $P \sim_0 Q$*, and (ii)* $P \sim_{k+1} Q$ *iff*

- *for all* $P' \in \text{Proc}$ *and* $a \in \text{Act}$ *such that* $P \xrightarrow{a} P'$*, there exists* $Q' \in \text{Proc}$ *such that* $Q \xrightarrow{a} Q'$ *and* $P' \sim_k Q'$*;* and
- *for all* $Q' \in \text{Proc}$ *and* $a \in \text{Act}$ *such that* $Q \xrightarrow{a} Q'$*, there exists* $P' \in \text{Proc}$ *such that* $P \xrightarrow{a} P'$ *and* $P' \sim_k Q'$*.*

$\sim$ is a limit of the sequence $(\sim_k)$.

Proposition 9.1 $P \sim Q$ *iff* $P \sim_k Q$ *for all* $k \in \mathbb{N}$*.*

Proof. Since $\sim \subseteq \sim_k$, for all k, the forward implication is immediate. For the reverse implication, take any pair $P, Q \in \text{Proc}$ satisfying $P \sim_k Q$ for all k. For any derivation $P \xrightarrow{a} P'$ there is a sequence of responses $Q \xrightarrow{a} Q'_k$ such that $P' \sim_k Q'_k$ for all k. But the sequence (Q'_k) contains only finitely many distinct processes—this is the "image-finiteness" property of PA—so some process Q' must occur infinitely often. This process has the property that $P' \sim_k Q'$ for all k. Thus the binary relation $\bigcap_k \sim_k$ satisfies the condition for a bisimulation relation, and hence is contained in $\sim$. $\square$

The input is a pair of terms or a schema $\langle P, Q\rangle$ to be expanded. If $\langle P, Q\rangle$ is a pair of simple terms, go to Case TT; if it is a schema, go to Case Sa.

CASE TT: For each derivation $P \overset{a}{\to} P'$ nondeterministically guess a derivation $Q \overset{a}{\to} Q'$ and set $\mathcal{B} := \mathcal{B} + \langle P', Q'\rangle$; if no derivation $Q \overset{a}{\to} Q'$ exists, halt and report failure. Repeat this procedure with the roles of P and Q reversed. If responses were proposed for all possible derivations, then halt and report success.

CASE Sa: (Refer to Theorem 7.18.) Suppose $P = (F \mid [\,]_h) \cdot X^m$ and $Q = (V \mid [\,]_h) \cdot X^m \mid R$.

(a) For each derivation $F \overset{a}{\to} F'$ nondeterministically guess a derivation $V \overset{a}{\to} V'$ or $R \overset{a}{\to} R'$ and set

$$\mathcal{B} := \mathcal{B} + \big\langle (F' \mid [\,]_h) \cdot X^m,\ (V' \mid [\,]_h) \cdot X^m \mid R\big\rangle, \text{ or} \quad (115)$$
$$\mathcal{B} := \mathcal{B} + \big\langle (F' \mid [\,]_h) \cdot X^m,\ (V \mid [\,]_h) \cdot X^m \mid R'\big\rangle, \quad (116)$$

as appropriate. If no such derivation can be found, halt and report failure.

(b) For each derivation $R \overset{a}{\to} R'$, nondeterministically guess a derivation $F \overset{a}{\to} F'$ and perform assignment (116). If no such derivation can be found, halt and report failure.

(c) For each derivation $V \overset{a}{\to} V'$, *either*

- nondeterministically guess a derivation $F \overset{a}{\to} F'$ and perform assignment (115), *or*
- provided $K_h \overset{a}{\to} K_{h-1} \mid X^i$,

$$\mathcal{B} := \mathcal{B} + \big\langle (\widehat{F} \mid [\,]_h) \cdot X^m,\ (\widehat{V} \mid [\,]_h) \cdot X^m \mid R\big\rangle, \text{ and} \quad (117)$$
$$\mathcal{B} := \mathcal{B} + \big\langle (\widehat{F} \mid [\,]_{h-1}) \cdot X^m,\ (\widehat{V} \mid [\,]_{h-1}) \cdot X^m \mid R\big\rangle, \quad (118)$$

where $\widehat{F} = F \mid K_{h-1} \mid X^i$ and $\widehat{V} = V' \mid K_h$. If there is no reduction of K_h via action a, halt and report failure.

(d) Set $\mathcal{B} := \mathcal{B} + \big\langle (F \mid [\,]_{h-1}) \cdot X^m,\ (V \mid [\,]_{h-1}) \cdot X^m \mid R\big\rangle$. (If $h = 1$, the result is no longer a schema, just a pair of processes.)

If responses were proposed for all possible derivations, then halt and report success.

Figure 4: The Expansion Procedure.

9.2 Expansion

The Expansion Procedure is presented in Figure 4. In certain steps of this and subsequent procedures the reader is referred Theorems or Lemmas which justify those steps. The proof of correctness is an inductive argument that uses the cited results to provide the inductive steps. The Expansion Procedure is easy to appreciate at an abstract level. Given a pair $\langle P, Q\rangle \in \mathcal{B} \setminus \mathcal{P}$ we would like to test whether $P \sim Q$. Since $\langle P, Q\rangle$ may be a schema, we have to make clear what we mean by bisimilarity in this case. For a schema $\langle P, Q\rangle$ we write $P \sim Q$ (respectively $P \sim_k Q$) if the two side of the schema are bisimilar (respectively, bisimilar up to k steps) for all valid substitutions into the context.

If indeed it is the case that $P \sim Q$, then for each derivation $P \xrightarrow{a} P'$ there will be a matching derivation $Q \xrightarrow{a} Q'$ with $P' \sim Q'$ (and vice versa). (What is meant by derivation in the case of a schema is made explicit in Figure 4; note the importance here of uniformity of bisimulation-preserving derivations, as assured by Theorem 7.18.) Provided the Expansion Procedure makes the correct nondeterministic choices at every step, only bisimilar pairs will ever be added to $\mathcal{B}$. On the other hand, if $P \not\sim Q$ then there is an integer k such that $P \not\sim_k Q$; consider the minimal such k. Whatever non-deterministic choices are made by the Expansion Procedure, it will be forced at some point to add a pair $\langle P', Q'\rangle$ to $\mathcal{B}$ for which $P' \not\sim_{k-1} Q'$.

Consider the set $\overline{\mathcal{B}}$ of bisimilar pairs $\langle P, Q\rangle$ reachable from $\langle P_0, Q_0\rangle$ by some sequence of expansion steps. If we knew an a priori upper bound b on the norm of (pairs of) processes contained in $\overline{\mathcal{B}}$, we would be done. For suppose $P_0 \sim Q_0$. Then, provided the correct nondeterministic choices are always made, only bisimilar pairs will be added to $\mathcal{B}$. Eventually $\mathcal{B} = \overline{\mathcal{B}}$, at which point the Decision Procedure halts and accepts. On the other hand, suppose $P_0 \not\sim Q_0$. The the Decision Procedure is doomed to add pairs $\langle P, Q\rangle$ to $\mathcal{B}$ such that $P \not\sim_k Q$ for smaller and smaller values of k. Eventually, a pair will be added such that $P \not\sim_0 Q$; when this pair is processed the expansion step will fail, and the Decision Procedure will halt and reject.

In reality, of course, there is no such bound b, so we must somehow control the norm of (pairs of) processes entering $\mathcal{B}$: this is the role of the Simplification Procedure, described in the following subsection. Although the details of the Expansion Procedure are mostly routine, the assignments (117) and (118) and the circumstances in which they are invoked may appear mystifying. At first sight, this step of the procedure may appear unnecessary, since Lemma 7.16 assures us that derivations involving generalised K-primes on the r.h.s. are matched by similar derivations on the l.h.s. However, we must remember that V may contain K_h as a factor when F does not; in this case, as in the Proof of Lemma 7.17, we may need to "steal" a K_h from the generalised K-term sitting in the context $[\,]_h$. After stealing from $[\,]_h$ there may or may not be any K_h remaining, leading to the two possibilities represented by (117) and (118).

The input is a pair $\langle P, Q \rangle$. Go to Case Sa if $\langle P, Q \rangle$ is a schema; otherwise, go to Case SS if P and Q are both (formal) sequential compositions, Case PP if they are both parallel, and case SP if (after possible relabelling) P is sequential and Q is parallel.

Case SS: (Refer to Lemma 9.2.) Let $P = P_1 \cdot P_2$ and $Q = Q_1 \cdot Q_2$, and assume, without loss of generality, that $\|P_1\| > \|Q_1\|$. Nondeterministically guess R with $\|R\| = \|P_1\| - \|Q_1\|$, and set

$$\mathcal{B} := \mathcal{B} + \langle P_1,\, Q_1 \cdot R \rangle + \langle R \cdot P_2,\, Q_2 \rangle.$$

Case PP: (Refer to Lemma 9.2.) Let $P = P_1 \mid P_2$ and $Q = Q_1 \mid Q_2$. Nondeterministically guess R_1, S_1, R_2, S_2 with $\|R_1\| + \|S_1\| = \|P_1\|$ and $\|R_2\| + \|S_2\| = \|P_2\|$. Then

$$\mathcal{B} := \mathcal{B} + \langle P_1,\, R_1 \mid S_1 \rangle + \langle P_2,\, R_2 \mid S_2 \rangle + \langle R_2 \mid S_1,\, Q_1 \rangle + \langle R_1 \mid S_2,\, Q_2 \rangle.$$

Case SP: Refer to Figure 6.

Case Sa: Refer to Figure 7.

Finally set $\mathcal{P} := \mathcal{P} + \langle P, Q \rangle$, recording the processing of the pair $\langle P, Q \rangle$.

Figure 5: The Simplification Procedure.

9.3 Simplification

The Simplification Procedure presented in Figures 5, 6 and 7 is invoked whenever a pair $\langle P, Q \rangle$ is processed whose constituent processes exceed, in norm, a certain bound b. The bound b is set larger than the norm of any atom, so we are guaranteed that P and Q are (explicit) sequential or parallel compositions. If P and Q are either both sequential (Case SS) or both parallel (Case PP) compositions, then the simplification step is straightforward: the unique sequential (respectively, parallel) decomposition theorem allows $\langle P, Q \rangle$ to be replaced by two (respectively, four) equivalent pairs of strictly smaller norm. In Case SS, for example, $P = P_1 \cdot P_2 \sim Q_1 \cdot Q_2 = Q$ if and only if there exists a term R, of the appropriate norm, such that both $P_1 \sim Q_1 \cdot R$ and $R \cdot P_2 \sim Q_2$.

Next, Case SP covers the situation where P or Q is a sequential composition and the other is parallel; suppose, without loss of generality that it is P that is sequential. We use the structure theory developed in Sections 4–8 to replace the pair $\langle P, Q \rangle$ by a number of equivalent pairs of lesser or equal norm. Note that this time the norm does not necessarily decrease; however, if the norm remains that same, the new pair will be of sequential-sequential or parallel-

Case SP: Let $P = P_1 \cdot P_2$ and $Q = Q_1 \mid Q_2$. Nondeterministically select and perform one of options (a)–(c) below.

(a) (Refer to Theorem 5.2.) Nondeterministically guess a monomorphic atom Y, a term T and a positive integer n satisfying $n(\|T\| + 1) = \|P\|$; then set

$$\mathcal{B} := \mathcal{B} + \langle P_1 \cdot P_2,\ Y \cdot (T \mid (Y \cdot T)^{n-1})\rangle + \langle Q_1 \mid Q_2,\ (Y \cdot T)^n\rangle.$$

(b) (Refer to Lemma 6.7.) Nondeterministically guess a series-parallel atom X, a term T and positive integers m and i such that $\|T\| + m + i = \|P\|$; then set

$$\mathcal{B} := \mathcal{B} + \langle P_1 \cdot P_2,\ (T \mid X^i) \cdot X^m\rangle + \langle Q_1 \mid Q_2,\ T \cdot X^m \mid X^i\rangle.$$

(c) (Refer to Theorem 7.18 and Lemma 7.6.) Nondeterministically guess a series-parallel unit X, an X-monomorphic X-unit K, positive integers h and m, and a system of generalised K-primes $K = K_{(1)}, K_{(2)}, \ldots, K_{(h)}$. Now guess terms F and V, a generalised K-term $H \in \Pi K_{(\leq h)}$, and a parallel product R of non-exceptional factors (terms of the form $K^j \cdot X^m$), all subject to the constraint

$$\|F\| + \|H\| + m\,\|X\| = \|V\| + \|H\| + m + \|R\| = \|P\| = \|Q\|.$$

Then set

$$\begin{aligned}\mathcal{B} := \mathcal{B}\ &+\ \langle P_1 \cdot P_2,\ (F \mid H) \cdot X^m\rangle \\ &+\ \langle Q_1 \mid Q_2,\ (V \mid H) \cdot X^m \mid R\rangle \\ &+\ \langle (F \mid [\,]_h) \cdot X^m,\ (V \mid [\,]_h) \cdot X^m \mid R\rangle.\end{aligned}$$

Figure 6: The Simplification Procedure (continued).

CASE Sa: The input is a schema $\big\langle (F \mid [\,]_h) \cdot X^m,\ (V \mid [\,]_h) \cdot X^m \mid R \big\rangle$ whose norm exceeds the bound b. There are two possibilities: F is either a parallel (SubCase P) or sequential (SubCase S) composition (its norm is too large for it to be an atom).

SUBCASE P: (Refer to Theorem 7.18.) Nondeterministically guess a number h' in the range $1 \le h' \le h$, and terms $\widehat{F}$, $\widehat{V}$, and $H \in \Pi K_{(\le h')}$, satisfying the norm conditions $\|\widehat{F}\| + \|H\| = \|F\|$ and $\|\widehat{V}\| + \|H\| = \|V\|$. Then set

$$\mathcal{B} := \mathcal{B} + \langle F, \widehat{F} \mid H \rangle + \langle V, \widehat{V} \mid H \rangle + \big\langle (\widehat{F} \mid [\,]_h) \cdot X^m,\ (\widehat{V} \mid [\,]_h) \cdot X^m \mid R \big\rangle.$$

SUBCASE S: (Refer to Theorem 7.19 and Lemma 9.3.) Verify that $h = 1$, $R = (K \cdot X^m)^i$ for some $i \ge 1$, and V has the property that $V \rightsquigarrow V^*$ and $\|V^*\|_X = 1$ entails $V^* \sim K \mid X^j$ for some j. (For a procedure to check the latter last condition, see Figure 8.) If any of these three conditions fail, halt and reject. Otherwise, set

$$\mathcal{B} := \mathcal{B} + \langle F \cdot X^m, V \cdot X^m \mid R \rangle.$$

Figure 7: The Simplification Procedure (concluded).

parallel type, so its norm will be decreased at a subsequent simplification step. The generalised K-primes used here are constructed using Lemma 7.6.

By setting the bound b larger than the norm of any atom, we avoid matching $\langle P, Q \rangle$ against a mixed equation with a non-series-parallel tail; for by Theorem 8.6, such an equation has l.h.s. $F \cdot X$ where F is atomic. This leaves three possibilities (assuming $P \sim Q$):

(a) The pair $\langle P, Q \rangle$ matches (its components are bisimilar to the two sides of) a monomorphic equation (see Theorem 5.2).

(b) The pair $\langle P, Q \rangle$ matches a trivial mixed equation of the form described in Theorem 6.7.

(c) The pair $\langle P, Q \rangle$ matches a pumpable equation (see Theorem 7.18).

These four possibilities are picked up by the correspondingly labelled options in Case SP of the simplification procedure (refer to Figure 6).

Finally, Case Sa deals with the possibility that $\langle P, Q \rangle$ is a schema. The term F is too large in norm to be an atom, so it must be either a parallel or sequential composition. In the former case, F must have accumulated some generalised K-factors which must now be shipped into the context, where they belong. In the latter case, the schema must hide a pumpable equation with a longer tail (higher

Search$(T \cdot X^i)$:

This recursive procedure takes a term T, explicitly given in the form $T \cdot X^i$. It searches systematically through all derivatives $T \leadsto T^*$ with $\|T^*\|_X = 1$, and verifies that all such T^* satisfy $T^* \cdot X^i \sim K \mid X^j$, for some j. The top level call to the procedure has $i = 0$.

(a) Has the parameter $T \cdot X^i$ been processed before by this procedure? If so, return immediately.

(b) Is T a formal parallel composition $T = T_1 \mid T_2$? If so, perform the following:
- if $\|T_1\|_X > 0$, call *Search*$(T_1 \cdot X^i)$;
- if $\|T_2\|_X > 0$, call *Search*$(T_2 \cdot X^i)$;

and return.

(c) Is T a formal sequential composition $T = T_1 \cdot T_2$? If so, perform the following:
- if $\|T_2\|_X > 0$, call *Search*$(T_2 \cdot X^i)$ and return; else
- $[\, \|T_2\|_X = 0 \,]$ if $\|T_2\| + i \geq \|K\|$, halt and reject; else
- $[\, \|T_2\|_X = 0$ and $i' = \|T_2\| + i < \|K\| \,]$ call *Search*$(T_1 \cdot X^{i'})$, and return.

(d) Otherwise T is an atom.
- If $\|T\|_X > 1$ then, for all derivations $T \to T'$, call *Search*$(T' \cdot X^i)$; else
- $[\, \|T\|_X = 1 \,]$ if T does not satisfy $T \cdot X^i \sim K \mid X^j$ for some i, halt and reject. (Refer to Figure 9 for a procedure to decide the latter condition.)

Figure 8: Searching derivatives of X-norm one.

value of m), which must now be revealed. This is the situation described in Theorem 7.19. The one algorithmically non-trivial premise of Theorem 7.19 is handled by procedure *Search* of Figure 8, and its attendant procedure K-*Bisim* of Figure 9. Both are conceptually quite straightforward: the former is just a closure operation, while the later only has to deal with bisimilarity of X-units.

9.4 Correctness

Recall that $\langle P_0, Q_0 \rangle$ is the input to the Decision Procedure, the pair of processes we wish to test for bisimilarity. We show separately that: if $P_0 \sim Q_0$ then the procedure halts and accepts its input, and if $P_0 \not\sim Q_0$, it halts and rejects. The former implication is the easier: we just need to check that the procedure

K-*Bisim*$(T \cdot X^i, K \mid X^j)$:

This non-deterministic, recursive procedure tests bisimilarity of two X-units.

(a) Have these parameters been processed before by this procedure? If so, return immediately.

(b) Is T a formal parallel composition $T = T_1 \mid T_2$? If so, perform the following (without loss of generality assume $\|T_2\|_X = 0$):
- if $j' = j - \|T_2\| < 0$, halt and reject; else,
- call K-*Bisim*$(T_1 \cdot X^i, K \mid X^{j'})$.

(c) Is T a formal sequential composition $T = T_1 \cdot T_2$? If so, perform the following:
- if $\|T_2\|_X > 0$, halt and reject; else,
- $[\,\|T_2\|_X = 0\,]$ if $\|T_2\| + i \geq \|K\|$, halt and reject; else
- $[\,\|T_2\|_X = 0$ and $i' = \|T_2\| + i < \|K\|\,]$ call K-*Bisim*$(T_1 \cdot X^{i'}, K \mid X^j)$ and return.

(d) Otherwise T is an atom. For all derivations $T \rightarrow T'$, so the following: derivation $K \rightarrow K \mid X^{j'}$ or $K \rightarrow X^{j'}$. Then:
- if $\|T'\|_X = 0$, verify that there is a matching derivation $K \rightarrow X^{j'}$ with $\|T' \cdot X^i\| = \|X^{j'}\|$ (halt and reject if none exist); else
- if $\|T'\|_X = 1$, non-deterministically guess a matching derivation $K \rightarrow K \mid X^{j'}$ with matching norm (halt and reject if none exist), and call K-*Bisim*$(T' \cdot X^i, K \mid X^{j'})$; else
- $[\,\|T'\|_X > 1\,]$ halt and reject.

Figure 9: Testing whether an X-unit is bisimilar to K.

is always able to keep the set $\mathcal{B}$ free from non-bisimilar pairs. For the latter implication, we rely on the following simple fact.

Lemma 9.2 *For all* k*, the relation* $\sim_k$ *is a congruence with respect to sequential and parallel composition; that is,* $\sim_k$ *is an equivalence relation on terms that satisfies*

$$P \cdot Q \sim_k \widehat{P} \cdot \widehat{Q} \quad \text{and} \quad P \mid Q \sim_k \widehat{P} \mid \widehat{Q},$$

for any terms $P, \widehat{P}, Q$ *and* $\widehat{Q}$*, with* $P \sim_k \widehat{P}$ *and* $Q \sim_k \widehat{Q}$*.*

This fact will be applied in the contrapositive form: e.g., if $P \mid Q \not\sim_k \widehat{P} \mid \widehat{Q}$ then either $P \not\sim_k \widehat{P}$ or $Q \not\sim_k \widehat{Q}$. We also need a level-k approximation version of the "lifting" part of Theorem 7.19.

Lemma 9.3 *Let* K *be an* X*-unit, and suppose*

$$F \cdot X^m \sim_k V \cdot X^m \mid R,$$

where R *is a power of* $K \cdot X^m$*. Suppose further that* V *has the property that* $V \rightsquigarrow V^*$ *and* $\|V^*\|_X = 1$ *entails* $V^* \sim K \mid X^j$ *for some* j*. Then*

$$(F \mid K^i) \cdot X^m \sim_k (V \mid K^i) \cdot X^m \mid R,$$

for all i*.*

All the machinery is in place for the main result.

Theorem 9.4 *The procedure presented in Figure 3 correctly decides bisimilarity of PA terms in doubly exponential nondeterministic time.*

Proof. The Simplification Procedure never produces terms whose norm is larger than the norm of its input. The Expansion Procedure can only produce terms reachable in one derivation from a term of norm at most b. Thus the set $\mathcal{B}$ contains only terms whose norm is bounded by $B = \max\{\|P_0\|, b + i\}$, where i is the maximum of $\|Z'\| - \|Z\|$ over all atoms Z and derivations $Z \rightarrow Z'$. Since there are only a finite number of terms with norm bounded by B, the procedure must terminate.

It is straightforward to check that if $P_0 \sim Q_0$ then there is some sequence of non-deterministic choices that causes the procedure to accept its input $\langle P_0, Q_0 \rangle$. Specifically, one checks that whenever a new pair $\langle P, Q \rangle$ is added to $\mathcal{B}$, the procedure has the flexibility to choose processes P and Q with $P \sim Q$. Thus the set $\mathcal{B}$ only contains bisimilar pairs, and the procedure terminates only when $\mathcal{P} = \mathcal{B}$.

Finally suppose $P_0 \not\sim Q_0$. We need to verify that the procedure rejects its input $\langle P_0, Q_0 \rangle$ whatever non-deterministic choices are made. For terms P, Q define $\kappa(P, Q)$ to be

$$\kappa(P, Q) = \begin{cases} \min\{k : P \not\sim_k Q\} & \text{if } P \not\sim Q; \\ \infty & \text{otherwise.} \end{cases}$$

Note that κ is well defined by the "image finiteness" property of PA, viz, that any PA term has only finitely many (immediate) derivatives. Image finiteness implies $P \sim Q$ iff $P \sim_k Q$ for all k. Applying the Expansion Procedure to any pair $\langle P, Q \rangle$ with $\kappa(P, Q) = k < \infty$ is bound to produce at least one pair $\langle P', Q' \rangle$ for which $\kappa(P', Q')$. If we can prove that applying the Simplification Procedure to any pair $\langle P, Q \rangle$ with $\kappa(P, Q) = k < \infty$ will produce at least one pair $\langle \widetilde{P}, \widetilde{Q} \rangle$ with $\kappa(P, Q) \leq k$ and $\|\widetilde{P}\| < \|P\|$, then we are done: the Decision Procedure will halt and reject by induction on lexicographic ordering on pairs $(\kappa(P, Q), \|P\|)$. (Actually, this situation does not quite obtain: one may have $\|\widetilde{P}\| = \|P\|$, but in that case the original simplification step is immediately followed by another that *does* reduce the norm.)

To verify that the Simplification Procedure satisfies this property, it is necessary to assess each of the cases in the light of Lemma 9.2 (or for SubCase S of Figure 7, in the light of Lemma 9.3). Take, as an example, the Case SS of the Figure 5, i.e., the first case. If $\kappa(P_1, Q_1 \cdot R) \geq k$ and $\kappa(R \cdot P_2, Q_2) \geq k$, then $P_1 \sim_k Q_1 \cdot R$ and $R \cdot P_2, \sim_k Q_2$. Then, by Lemma 9.2, $P_1 \cdot P_2 \sim_k Q_1 \cdot R \cdot P_2 \sim_k Q_1 \cdot Q_2$, and hence $\kappa(P_1 \cdot P_2, Q_1 \cdot Q_2) \geq k$. Equivalently, if $\kappa(P_1 \cdot P_2, Q_1 \cdot Q_2) = k$ then either $\kappa(P_1, Q_1 \cdot R) \leq k$ or $\kappa(R \cdot P_2, Q_2) \leq k$. Either way, the norm is reduced. The other cases may be argued similarly.

The (syntactic) size of processes in $\mathcal{B}$ is bounded by B, which in turn is exponential in the size of the (syntactic description) of the set of productions describing derivations, which we take to be the input size. Thus the cardinality of $\mathcal{B}$ is doubly exponential in the input size. The non-deterministic time-complexity of the decision procedure is thus doubly exponential. □

Acknowledgement

The authors thank Colin Stirling for useful discussions on the structure of mixed equations.

References

[1] 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 (1993), 653–682.

[2] J. A. Bergstra and J. W. Klop, Algebra of communicating processes with abstraction. *Theoretical Computer Science* 37(1), 77–121.

[3] Olaf Burkart, Didier Caucal and Bernhard Steffen, An elementary bisimulation decision procedure for arbitrary context-free processes. Proceedings of MFCS '95: 20th International Symposium on Mathematical Foundations of Computer Science, *Lecture Notes in Computer Science* 969, Springer-Verlag, 1995, 423–433.

[4] Søren Christensen, Yoram Hirshfeld, and Faron Moller, Decomposability, decidability and axiomatisability for bisimulation equivalence on basic parallel processes. *Proceedings of the Eighth Annual IEEE Symposium on Logic in Computer Science* (LICS 93), IEEE Computer Society Press, 1993, 386-396.

[5] Søren Christensen, Yoram Hirshfeld, and Faron Moller, Bisimulation equivalence is decidable for basic parallel processes. Proceedings of CONCUR 93: Fourth International Conference on Concurrency Theory, *Lecture Notes in Computer Science* 715 Springer-Verlag, 1993, 143–157.

[6] Søren CHRISTENSEN, Hans HÜTTEL and Colin STIRLING, Bisimulation equivalence is decidable for all context-free processes, *Information and Computation* 121 (1995), 143–148.

[7] Yoram HIRSHFELD, Mark JERRUM and Faron MOLLER, A polynomial algorithm for deciding bisimilarity of normed context-free processes, *Theoretical Computer Science* 158 (1996), 143–159.

[8] Yoram HIRSHFELD, Mark JERRUM and Faron MOLLER, A polynomial algorithm for deciding bisimulation equivalence of normed Basic Parallel Processes, *Mathematical Structures in Computer Science* 6 (1996), 251–259.

[9] Robin MILNER, *Communication and Concurrency*, Prentice Hall, 1989.

[10] Robin MILNER and Faron MOLLER, Unique decomposition of processes, *Theoretical Computer Science* 107 (1993), 357–363.

[11] D. M. R. PARK, Concurrency and Automata on Infinite Sequences. Theoretical Computer Science: Fifth GI-Conference, *Lecture Notes in Computer Science* 104, Springer Verlag, 1981, 167–183.