Unique Parallel Decomposition in Branching and Weak Bisimulation Semantics

Bas Luttik

Abstract

We consider the property of unique parallel decomposition modulo branching and weak bisimilarity. First, we show that normed behaviours always have parallel decompositions, but that these are not necessarily unique. Then, we establish that finite behaviours have unique parallel decompositions. We derive the latter result from a general theorem about unique decompositions in partial commutative monoids.

1 Introduction

A recurring question in process theory is to what extent the behaviours definable in a certain process calculus admit a unique decomposition into indecomposable parallel components. Milner and Moller [22] were the first to address the question. They proved a unique parallel decomposition theorem for a simple process calculus, which allows the specification of finite behaviour up to strong bisimilarity and includes parallel composition in the form of pure interleaving without interaction between the components. They also presented counterexamples showing that unique parallel decomposition may fail in process calculi in which it is possible to specify infinite behaviour, or in which certain coarser notions of behavioural equivalence are used.

Moller proved several more unique parallel decomposition results in his dissertation [23], replacing interleaving parallel composition by CCS parallel composition, and then also considering weak bisimilarity. These results were established with subsequent refinements of an ingenious proof technique attributed to Milner. Christensen, in his dissertation [7], further refined the proof technique to make it work for the *normed* behaviours recursively definable modulo strong bisimilarity, and for *all* behaviours recursively definable modulo distributed bisimilarity.

With each successive refinement of Milner's proof technique, the technical details became more complicated, but the general idea of the proof remained the same. In [18] we made an attempt to isolate the deep insights from the technical details, by identifying a sufficient condition on partial commutative monoids that facilitates an abstract version of Milner's proof technique. To concisely present the sufficient condition, we have put forward the notion of *decomposition order*; it is established in [18], by means of an abstract version of Milner's technique, that if a partial commutative monoid can be endowed with a decomposition order, then it has unique decomposition.

Application of the general result of [18] in commutative monoids of behaviour is often straightforward: a well-founded order naturally induced on behaviour by (a terminating fragment of) the transition relation typically satisfies the properties of a decomposition order. All the aforementioned unique parallel decomposition results can be directly obtained in this way, except Moller's result that finite behaviours modulo weak bisimilarity have unique decomposition. It turns out that a decomposition order cannot straightforwardly be obtained from the transition relation if certain transitions are deemed unobservable by the behavioural equivalence under consideration.

In this article, we address the question of how to establish unique parallel decomposition in settings with a notion of unobservable behaviour. Our main contribution will be an adaptation of the general result in [18] to make it suitable for establishing unique parallel decomposition also in settings with a notion of unobservable behaviour. To illustrate the result, we shall apply it to establish unique parallel decomposition for finite behaviour modulo branching or weak bisimilarity. We shall also show, by means of a counterexample, that unique parallel decomposition fails for infinite behaviours modulo branching and weak bisimilarity, even if only a very limited form of infinite behaviour is considered (normed behaviour definable in a process calculus with prefix iteration).

A positive answer to the unique parallel decomposition question seems to be primarily of theoretical interest, as a tool for proving other theoretical properties about process calculi. For instance, Moller's proofs in [24, 25] that PA and CCS cannot be finitely axiomatised without auxiliary operations and Hirshfeld and Jerrum's proof in [16] that bisimilarity is decidable for normed PA both rely on unique parallel decomposition. When parallel composition cannot be eliminated from terms by means of axioms, then unique parallel decomposition is generally used to find appropriate normal forms in completeness proofs for equational axiomatisations [1, 2, 3, 11, 15]. In [17], a unique parallel decomposition result serves as a stepping stone for proving complete axiomatisation and decidability results in the context of a higher-order process calculus.

There is an intimate relationship between unique parallel decomposition and of cancellation with respect to parallel composition; the properties are in most circumstances equivalent. In [6], cancellation with respect parallel composition was first proved and exploited to prove the completeness of an axiomatisation of distributed bisimilarity.

Unique parallel decomposition could be of practical interest too, e.g., to devise methods for finding the maximally parallel implementation of a behaviour [8], or for improving verification methods [14]. In [10], unique parallel decomposition results are established for the Applied π-calculus, as a tool in the comparison of different security notions in the context of electronic voting.

This article is organised as follows. In Section 2 we introduce the process calculus that we shall use to illustrate our theory of unique decomposition. There, we also present counterexamples to the effect that infinite behaviours in general may not have a decomposition, and normed behaviours may have more than one decomposition. In Section 3 we recap the theory of decomposition put forward in [18] and discuss why it is not readily applicable to establish unique parallel decomposition for finite behaviours modulo branching and weak bisimilarity. In Section 4 we adapt the theory of [18] to make it suitable for proving unique parallel decomposition results in process calculi with a notion of unobservability. In Section 5 we apply the theorem from Section 4, showing that bounded behaviours have a unique parallel decomposition both modulo branching and weak bisimilarity. We end the article in Section 6 with a short conclusion.

An extended abstract of this article appeared as [19].

2 Processes up to branching and weak bisimilarity

We define a simple language of process expressions together with an operational semantics, and notions of branching and weak bisimilarity. We shall then investigate to what extent process expressions modulo branching or weak bisimilarity admit parallel decompositions. We shall present examples of process expressions without a

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

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

Table 1: The operational semantics.

decomposition, and of normed process expressions with two distinct decompositions.

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

$$P ::= \mathbf{0} \mid \alpha.P \mid P + P \mid P \parallel P \mid \alpha^* P \qquad (\alpha \in \mathcal{A}_\tau).$$

The language above is BCCS (the core of Milner's CCS [20]) extended with a construction $\_ \parallel \_$ to express interleaving parallelism and the prefix iteration construction $\alpha^*\_$ to specify a restricted form of infinite behaviour. We include only a very basic notion of parallel composition in our calculus, but note that this is just to simplify the presentation. Our unique decomposition theory extends straightforwardly to more intricate notions of parallel composition, e.g., modelling some form of communication between components. To be able to omit some parentheses when writing process expressions, we adopt the conventions that $\alpha.$ and α^* bind stronger, and that $+$ binds weaker than all the other operations.

Operational semantics and branching and weak bisimilarity We define on $\mathcal{P}$ binary relations $\xrightarrow{\alpha}$ $(\alpha \in \mathcal{A}_\tau)$ by means of the operational rules in Table 1. We denote by $\twoheadrightarrow$ the reflexive-transitive closure of $\xrightarrow{\tau}$, i.e., $P \twoheadrightarrow P'$ if there exist $P_0, \dots, P_n$ $(n \geq 0)$ such that $P = P_0 \xrightarrow{\tau} \cdots \xrightarrow{\tau} P_n = P'$. Furthermore, we shall write $P \xrightarrow{(\alpha)} P'$ if $P \xrightarrow{\alpha} P'$ or $\alpha = \tau$ and $P = P'$.

Definition 1 (Branching bisimilarity [13]). A symmetric binary relation $\mathcal{R}$ on $\mathcal{P}$ is a *branching bisimulation* if for all $P, Q \in \mathcal{P}$ such that $P \mathrel{\mathcal{R}} Q$ and for all $\alpha \in \mathcal{A}_\tau$ it holds that

> if $P \xrightarrow{\alpha} P'$ for some $P' \in \mathcal{P}$, then there exist $Q'', Q' \in \mathcal{P}$ such that $Q \twoheadrightarrow Q'' \xrightarrow{(\alpha)} Q'$ and $P \mathrel{\mathcal{R}} Q''$ and $P' \mathrel{\mathcal{R}} Q'$.

We write $P \leftrightarrow_{\mathrm{b}} Q$ if there exists a branching bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

The relation $\leftrightarrow_{\mathrm{b}}$ is an equivalence relation on $\mathcal{P}$ (this is not as trivial as one might expect; for a proof see [5]). It is also compatible with the construction of parallel composition in our syntax, which means that, for all $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$:

$$P_1 \leftrightarrow_{\mathrm{b}} Q_1 \text{ and } P_2 \leftrightarrow_{\mathrm{b}} Q_2 \text{ implies } P_1 \parallel P_2 \leftrightarrow_{\mathrm{b}} Q_1 \parallel Q_2 \ . \qquad (1)$$

(The relation $\leftrightarrow_{\mathrm{b}}$ is also compatible with $\alpha.$, but not with $+$ and α^*. In this article, we shall only rely on compatibility with $\parallel$.)

Definition 2 (Weak bisimilarity [21]). A symmetric binary relation $\mathcal{R}$ on $\mathcal{P}$ is a *weak bisimulation* if for all $P, Q \in \mathcal{P}$ such that $P \mathrel{\mathcal{R}} Q$ and for all $\alpha \in \mathcal{A}_\tau$ it holds that if $P \xrightarrow{\alpha} P'$ for some $P' \in \mathcal{P}$, then there exist $Q', Q'', Q''' \in \mathcal{P}$ such that $Q \twoheadrightarrow Q'' \xrightarrow{(\alpha)} Q''' \twoheadrightarrow Q'$ and $P' \mathrel{\mathcal{R}} Q'$.

We write $P \leftrightarroweq_{\mathrm{w}} Q$ if there exists a weak bisimulation $\mathcal{R}$ such that $P \mathrel{\mathcal{R}} Q$.

The relation $\leftrightarroweq_{\mathrm{w}}$ is an equivalence relation on $\mathcal{P}$. It is also compatible with parallel composition, i.e., for all $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$:

$$P_1 \leftrightarroweq_{\mathrm{w}} Q_1 \text{ and } P_2 \leftrightarroweq_{\mathrm{w}} Q_2 \text{ implies } P_1 \parallel P_2 \leftrightarroweq_{\mathrm{w}} Q_1 \parallel Q_2 \ . \qquad (2)$$

(Just like $\leftrightarroweq_{\mathrm{b}}$, the relation $\leftrightarroweq_{\mathrm{w}}$ is not compatible with $+$ and α^*.) Note that $\leftrightarroweq_{\mathrm{b}} \subseteq \leftrightarroweq_{\mathrm{w}}$; we shall often implicitly use this property below.

A process expression is *indecomposable* if it is not behaviourally equivalent to $\mathbf{0}$ or a non-trivial parallel composition (a parallel composition is trivial if one of its components is behaviourally equivalent to $\mathbf{0}$). We say that a process theory has *unique parallel decomposition* if every process expression is behaviourally equivalent to a unique (generalised) parallel composition of indecomposable process expressions. Uniqueness means that the indecomposables of any two decompositions of a process expression are pairwise behaviourally equivalent up to a permutation.

We should make the definitions of indecomposable and unique parallel decomposition more formal and concrete for the two behavioural equivalences considered in this article (viz. branching and weak bisimilarity). For reasons of generality and succinctness, however, it is convenient to postpone our formalisation until the next section, where we will discuss decomposition in the more abstract setting of commutative monoids. For now, we rely on the intuition of the reader and discuss informally and by means of examples to what extent the process theory introduced above might have the property of unique parallel decomposition. In our explanations we use branching bisimilarity as behavioural equivalence, but everything we say in the remainder of this section remains valid if branching bisimilarity is replaced by weak bisimilarity.

The first observation, already put forward by Milner and Moller in [22], is that there are process expressions that do not have a decomposition at all. (In [22], the following example is actually used to show that there exist infinite processes which do not have a decomposition modulo *strong* bisimilarity.)

Example 3. Consider the process expression $a^*\mathbf{0}$ (with $a \neq \tau$), and suppose that $a^*\mathbf{0}$ has a decomposition, say $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} P \parallel Q$ for some process expressions P and Q.

We first argue that either $P \leftrightarroweq_{\mathrm{b}} a^*\mathbf{0}$ or $Q \leftrightarroweq_{\mathrm{b}} a^*\mathbf{0}$. Note that it follows from $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} P \parallel Q$ that all process expressions reachable from $P \parallel Q$ are branching bisimilar to $a^*\mathbf{0}$, and hence for all process expressions R reachable from P we have that $R \xrightarrow{\alpha} R'$ implies $\alpha = a$. So if R is reachable from P, then either $R \leftrightarroweq_{\mathrm{b}} \mathbf{0}$ or there exists R' such that $R \xrightarrow{a} R'$. If, on the one hand, there exists a process expression R reachable from P such that $R \leftrightarroweq_{\mathrm{b}} \mathbf{0}$, then, since $R \parallel Q$ is reachable from $P \parallel Q$, it follows that $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} R \parallel Q \leftrightarroweq_{\mathrm{b}} Q$. If, on the other hand, there does not exist a process expression R reachable from P such that $R \leftrightarroweq_{\mathrm{b}} \mathbf{0}$, then, for all process expressions R reachable from P, on the one hand there exists R' such that $R \xrightarrow{a} R'$ and on the other hand for all R' and α such that $R \xrightarrow{\alpha} R'$ we have that $\alpha = a$. Therefore, the relation $\mathcal{R} = \{(a^*\mathbf{0}, R) \mid R \text{ is reachable from } P\}$ is a (branching) bisimulation relation, and hence $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} P$.

Now, since $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} P \parallel Q$ implies that either $P \leftrightarroweq_{\mathrm{b}} a^*\mathbf{0}$ or $Q \leftrightarroweq_{\mathrm{b}} a^*\mathbf{0}$, a decomposition of $a^*\mathbf{0}$ would necessarily include an indecomposable branching bisimilar to $a^*\mathbf{0}$. But, since $a^*\mathbf{0} \leftrightarroweq_{\mathrm{b}} a^*\mathbf{0} \parallel a^*\mathbf{0}$, there does not exist an indecomposable branching bisimilar to $a^*\mathbf{0}$. We conclude that $a^*\mathbf{0}$ fails to have a decomposition.

Note that the process expression $a^*\mathbf{0}$ does not admit terminating behaviour; it does not have a transition sequence to a process expression from which no further transitions are possible. We want to identify a conveniently large subset of process expressions that do have decompositions, and to exclude the counterexample against existence of decompositions, we confine our attention to process expressions with terminating behaviour.

For $a \in \mathcal{A}$ and process expressions P and Q we write $P \stackrel{a}{\longrightarrow\!\!\!\!\!\rightarrow} Q$ whenever there exist process expressions P' and Q' such that $P \longrightarrow\!\!\!\!\!\rightarrow P' \stackrel{a}{\longrightarrow} Q' \longrightarrow\!\!\!\!\!\rightarrow Q$. We say that P is *silent* and write $P\downarrow$ if there do not exist $a \in \mathcal{A}$ and Q such that $P \stackrel{a}{\longrightarrow\!\!\!\!\!\rightarrow} Q$.

Definition 4. A process expression P is *normed* if there exist a natural number $k \in \mathbf{N}$, process expressions $P_0, \dots, P_k \in \mathcal{P}$ and actions $a_1, \dots, a_k \in \mathcal{A}$ such that $P = P_0 \stackrel{a_1}{\longrightarrow\!\!\!\!\!\rightarrow} \cdots \stackrel{a_k}{\longrightarrow\!\!\!\!\!\rightarrow} P_k$ and $P_k\downarrow$. The *norm* $n(P)$ of a normed process expression P is defined by

$$n(P) = \min\{k : \exists P_0, \dots, P_k \in \mathcal{P}.\ \exists a_1, \dots, a_k \in \mathcal{A}.\ P = P_0 \stackrel{a_1}{\longrightarrow\!\!\!\!\!\rightarrow} \cdots \stackrel{a_k}{\longrightarrow\!\!\!\!\!\rightarrow} P_k\downarrow\}\ .$$

It is immediate from their definitions that both branching and weak bisimilarity preserve norm: if two process expressions are branching or weakly bisimilar, then they have equal norms. It is also easy to establish that a parallel composition is normed if, and only if, both parallel components are normed. In fact, norm is additive with respect to parallel composition: the norm of a parallel composition is the sum of the norms of its parallel components. Note that a process expression with norm 0 is behaviourally equivalent to $\mathbf{0}$.

With a straightforward induction on norm it can be established that normed process expressions have a decomposition. But sometimes even more than one, as is illustrated in the following example.

Example 5. Consider the process expressions $P = a^*\tau.b.\mathbf{0}$ and $Q = b.\mathbf{0}$. It is clear that P and Q are *not* branching bisimilar. Both P and Q have norm 1, and from this it immediately follows that they are both indecomposable. Note that, according to the operational semantics, $P \parallel P$ gives rise to the following three transitions:

1. $P \parallel P \stackrel{a}{\longrightarrow} P \parallel P$;
2. $P \parallel P \stackrel{\tau}{\longrightarrow} P \parallel Q$; and
3. $P \parallel P \stackrel{\tau}{\longrightarrow} Q \parallel P$.

Further note that $P \parallel Q \stackrel{a}{\longrightarrow} P \parallel Q$ and $Q \parallel P \stackrel{a}{\longrightarrow} Q \parallel P$. (The complete transition graph associated with $P \parallel P$ by the operational semantics is shown in Figure 1.) Using these facts it is straightforward to verify that the reflexive-symmetric closure of the binary relation

$$\mathcal{R} = \{(P \parallel P, P \parallel Q), (P \parallel P, Q \parallel P)\} \\ \cup \{(P \parallel Q, Q \parallel P), (P \parallel \mathbf{0}, \mathbf{0} \parallel P), (Q \parallel \mathbf{0}, \mathbf{0} \parallel Q)\}$$

is a branching bisimulation, and hence $P \parallel P \leftrightarrow_{\mathrm{b}} P \parallel Q$. It follows that $P \parallel P$ and $P \parallel Q$ are distinct decompositions of the same process up to branching bisimilarity.

Incidentally, the processes in the above counterexample also refute claims in [12] to the effect that processes definable with a normed BPP specification have a unique decomposition modulo branching bisimilarity and weak bisimilarity.

Apparently, more severe restrictions are needed.

Definition 6. Let $k \in \mathbf{N}$; a process expression P is *bounded* by k if for all $\ell \in \mathbf{N}$ the existence of $P_1, \dots, P_\ell \in \mathcal{P}$ and $a_1, \dots, a_\ell \in \mathcal{A}$ such that $P \stackrel{a_1}{\longrightarrow\!\!\!\!\!\rightarrow} \cdots \stackrel{a_\ell}{\longrightarrow\!\!\!\!\!\rightarrow} P_\ell$ implies that $\ell \leq k$. We say that P is *bounded* if P is bounded by k for some $k \in \mathbf{N}$.

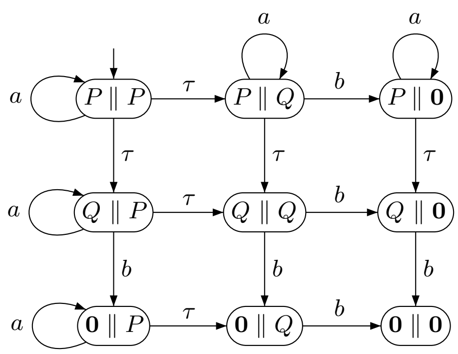

Figure 1: Transition graph associated with $P \parallel P$.

The *depth* $d(P)$ of a bounded process expression P is the length of its longest transition sequence not counting τ-transitions, i.e.,

$$d(P) = \max\{k : \exists P_0, \ldots, P_k.\ \exists a_1, \ldots, a_k.\ P = P_0 \xrightarrow{a_1}\!\!\!\!\rightarrow \cdots \xrightarrow{a_k}\!\!\!\!\rightarrow P_k\}\ .$$

Both branching and weak bisimilarity preserve depth: if two process expressions are branching or weakly bisimilar, then they have equal depth. Furthermore, depth is additive with respect to parallel composition: the depth of a parallel composition is the sum of the depths of its parallel components. A process expression with depth 0 is behaviourally equivalent to $\mathbf{0}$.

In the remainder of this article we shall establish that bounded process expressions have a unique parallel decomposition both modulo branching and weak bisimilarity. We shall derive these results from a more general result about unique decomposition in commutative monoids.

3 Partial commutative monoids and decomposition

In this section we recall the abstract algebraic notion of partial commutative monoid, and formulate the property of unique decomposition. We shall see that the process theories discussed in the previous section give rise to commutative monoids of processes with parallel composition as binary operation. The notion of unique decomposition associated with these commutative monoids coincides with the notion of unique parallel decomposition as discussed.

Then, we shall recall the notion of decomposition order on partial commutative monoids proposed in [18]. We shall investigate whether the notion of decomposition order can be employed to prove unique parallel decomposition of bounded process expressions modulo branching and weak bisimilarity.

Definition 7 ([18], Definition 1)**.** A *(partial) commutative monoid* is a set M with a distinguished element e and a (partial) binary operation on M (for clarity in this definition denoted by $\cdot$) such that for all $x, y, z \in M$:

$x \cdot (y \cdot z) \simeq (x \cdot y) \cdot z$	(associativity);
$x \cdot y \simeq y \cdot x$	(commutativity);
$x \cdot e \simeq e \cdot x \simeq x$	(identity).

(The symbol $\simeq$ expresses that either both sides of the equation are undefined or both sides are defined and designate the same element in M; see Remark 2 in [18] for further explanations.)

The symbol $\cdot$ will be omitted if this is unlikely to cause confusion. Also, we shall sometimes use other symbols ($\parallel$, $+$, ...) to denote the binary operation of a partial commutative monoid.

In [18], the key notions of the general theory of decomposition for commutative monoids are illustrated using three examples: the commutative monoid of natural numbers with addition, the commutative monoid of positive natural numbers with multiplication, and the commutative monoid of multisets over some set. Here we recap the latter example, because we need some of the definitions pertaining to multisets in the remainder of this article.

Example 8. Let X be any set. A *(finite) multiset* over X is a mapping $m : X \to \mathbf{N}$ such that $m(x) > 0$ for at most finitely many $x \in X$; the number $m(x)$ is called the *multiplicity* of x in m. The set of all multisets over X is denoted by $\mathcal{M}(X)$. If m and n are multisets, then their sum $m \uplus n$ is obtained by coordinatewise addition of multiplicities, i.e., $(m \uplus n)(x) = m(x) + n(x)$ for all $x \in X$. The *empty multiset* $\Box$ is the multiset that satisfies $\Box(x) = 0$ for all $x \in X$. With these definitions, $\mathcal{M}(X)$ is a commutative monoid. If $x_1, \ldots, x_k$ is a sequence of elements of X, then $\wr x_1, \ldots, x_k \int$ denotes the multiset m such that $m(x)$ is the number of occurrences of x in $x_1, \ldots, x_k$.

Process expressions modulo branching or weak bisimilarity also give rise to commutative monoids. Recall that $\leftrightarrow_{\mathrm{b}}$ and $\leftrightarrow_{\mathrm{w}}$ are equivalence relations on the set of process expressions. We denote the equivalence class of a process expression P modulo $\leftrightarrow_{\mathrm{b}}$ or $\leftrightarrow_{\mathrm{w}}$, respectively, by $[P]_b$ and $[P]_w$, i.e.,

$$[P]_b = \{Q \in \mathcal{P} : P \leftrightarrow_{\mathrm{b}} Q\} \ ; \text{ and}$$
$$[P]_w = \{Q \in \mathcal{P} : P \leftrightarrow_{\mathrm{w}} Q\} \ .$$

Then, we define

$$\mathbf{B} = \mathcal{P}/{\leftrightarrow_{\mathrm{b}}} = \{[P]_b : P \in \mathcal{P}\} \ ; \text{ and}$$
$$\mathbf{W} = \mathcal{P}/{\leftrightarrow_{\mathrm{w}}} = \{[P]_w : P \in \mathcal{P}\} \ .$$

In this article, the similarities between the commutative monoids $\mathbf{B}$ and $\mathbf{W}$ will be more important than the differences. It will often be necessary to define notions for both commutative monoids, in a very similar way. For succinctness of presentation, we allow ourselve a slight *abus de language* and most of the time deliberately omit the subscripts b and w from our notation for equivalence classes. Thus, we will be able to efficiently define notions and prove facts simultaneously for $\mathbf{B}$ and $\mathbf{W}$.

For example, since both $\leftrightarrow_{\mathrm{b}}$ and $\leftrightarrow_{\mathrm{w}}$ are compatible with $\parallel$ (see Equations (1) and (2)), we can define a binary operation $\parallel$ simultaneously on $\mathbf{B}$ and $\mathbf{W}$ simply by

$$[P] \parallel [Q] = [P \parallel Q] \ .$$

Also, we agree to write just $\mathbf{0}$ for $[\mathbf{0}]$. It is then straightforward to establish that the binary operation $\parallel$ is commutative and associative (both on $\mathbf{B}$ and $\mathbf{W}$), and that $\mathbf{0}$ is the identity element for $\parallel$.

Proposition 9. *The sets* $\mathbf{B}$ *and* $\mathbf{W}$ *are commutative monoids under* $\parallel$*, with* $\mathbf{0}$ *as identity element.*

Note that, since both branching and weak bisimilarity preserve depth (norm), whenever an equivalence class $[P]$ contains a bounded (normed) process expression, it consists entirely of bounded (normed) process expressions. We define subsets $\mathbf{B}_{fin} \subseteq \mathbf{B}_n \subseteq \mathbf{B}$ and $\mathbf{W}_{fin} \subseteq \mathbf{W}_n \subseteq \mathbf{W}$ by

$$\mathbf{B}_{fin} = \{[P]_b : P \in \mathcal{P} \ \&\ P \text{ is bounded}\} \ ;$$
$$\mathbf{B}_n = \{[P]_b : P \in \mathcal{P} \ \&\ P \text{ is normed}\} \ ;$$
$$\mathbf{W}_{fin} = \{[P]_w : P \in \mathcal{P} \ \&\ P \text{ is bounded}\} \ ; \text{ and}$$
$$\mathbf{W}_n = \{[P]_w : P \in \mathcal{P} \ \&\ P \text{ is normed}\} \ .$$

Since a parallel composition is bounded (normed) if, and only if, its parallel components are bounded (normed), $\mathbf{B}_{fin}$ and $\mathbf{B}_n$ are commutative submonoids of $\mathbf{B}$, and $\mathbf{W}_{fin}$ and $\mathbf{W}_n$ are commutative submonoids of $\mathbf{W}$.

Notation 10. Let $x_1, \dots, x_k$ be a (possibly empty) sequence of elements of a monoid M; we define its *generalised composition* $x_1 \cdots x_k$ as usual. Furthermore, we write x^n for the k-fold composition of x. For explicit definitions of these notations see Notation 4 of [18].

It is straightforward by induction to establish the following *generalised associative law*:

$$(x_1 \cdots x_k)(y_1 \cdots y_\ell) \simeq x_1 \cdots x_k y_1 \cdots y_\ell \ .$$

Also by induction, a *generalised commutative law* can be established, so

if $i_1, \dots, i_\ell$ is any permutation of $1, \dots, \ell$, then $x_1 \cdots x_\ell \simeq x_{i_1} \cdots x_{i_\ell}$.

An indecomposable element of a commutative monoid is an element that cannot be written as a product of two elements that are both not the identity element of the monoid.

Definition 11 ([18], Definition 5)**.** An element p of a commutative monoid M is called *indecomposable* if $p \neq e$ and $p = xy$ implies $x = e$ or $y = e$.

Example 12.

1. The indecomposable elements of $\mathcal{M}(X)$ are the *singleton* multisets, i.e., the multisets m for which it holds that $\sum_{x \in X} m(x) = 1$.
2. The indecomposable elements of $\mathbf{B}_{fin}$, $\mathbf{B}_n$, $\mathbf{B}$, $\mathbf{W}_{fin}$, $\mathbf{W}_n$, and $\mathbf{W}$ are the equivalence classes of process expressions that are not behaviourally equivalent to $\mathbf{0}$ or a non-trivial parallel composition.

We define a decomposition in a partial commutative monoid to be a finite multiset of indecomposable elements. Note that this gives the right notion of equivalence on decompositions, for two finite multisets $\wr x_1, \dots, x_k \int$ and $\wr y_1, \dots, y_\ell \int$ are equal iff the sequence $y_1, \dots, y_\ell$ can be obtained from the sequence $x_1, \dots, x_k$ by a permutation of its elements.

Definition 13 ([18], Definition 7)**.** Let M be a partial commutative monoid. A *decomposition* in M is a finite multiset $\wr p_1, \dots, p_k \int$ of indecomposable elements of M such that $p_1 \cdots p_k$ is defined. The element $p_1 \cdots p_k$ in M will be called the *composition* associated with the decomposition $\wr p_1, \dots, p_k \int$, and, conversely, we say that $\wr p_1, \dots, p_k \int$ is a decomposition of the element $p_1 \cdots p_k$ of M. Decompositions $d = \wr p_1, \dots, p_k \int$ and $d' = \wr p'_1, \dots, p'_\ell \int$ are *equivalent* in M (notation: $d \equiv d'$) if they have the same compositions, i.e., if

$$p_1 \cdots p_k = p'_1 \cdots p'_\ell \ .$$

A decomposition d in M is *unique* if $d \equiv d'$ implies $d = d'$ for all decompositions d' in M. We say that an element x of M has a unique decomposition if it has a decomposition and this decomposition is unique; we shall then denote the unique decomposition of x by ∂x. If every element of M has a unique decomposition, then we say that M has *unique decomposition*.

Example 14. Every finite multiset m over X has a unique decomposition in $\mathcal{M}(X)$, which contains for every $x \in X$ precisely $m(x)$ copies of the singleton multiset $\wr x \int$.

The general notion of unique decomposition for commutative monoids, when instantiated to one of the commutative monoids of processes considered in this article, indeed coincides with the notion of unique parallel decomposition as discussed in the preceding section. We have already seen that the commutative monoids $\mathbf{B}_n$, $\mathbf{B}$, $\mathbf{W}_n$ and $\mathbf{W}$ do not have unique decomposition. Our goal in the remainder of this article is to establish that the commutative monoids $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ do have unique decomposition.

Preferably, we would like to have a general sufficient condition on partial commutative monoids for unique decomposition that is easily seen to hold for $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$, and hopefully also for other commutative monoids of processes. We shall now first recall the sufficient criterion put forward in [18], which was specifically designed for commutative monoids of processes. Then, we shall explain that it cannot directly be applied to conclude that $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ have unique decomposition. In the next section, we shall subsequently modify the condition, so that it becomes applicable to the commutative monoids at hand.

Definition 15 ([18], Definition 20)**.** Let M be a partial commutative monoid; a partial order $\preccurlyeq$ on M is a *decomposition order* if

(i) it is *well-founded*, i.e., every non-empty subset of M has a $\preccurlyeq$-minimal element;

(ii) the identity element e of M is the *least element* of M with respect to $\preccurlyeq$, i.e., $e \preccurlyeq x$ for all x in M;

(iii) it is *strictly compatible*, i.e., for all $x, y, z \in M$

$$\text{if } x \prec y \text{ and } yz \text{ is defined, then } xz \prec yz;$$

(iv) it is *precompositional*, i.e., for all $x, y, z \in M$

$$x \preccurlyeq yz \text{ implies } x = y'z' \text{ for some } y' \preccurlyeq y \text{ and } z' \preccurlyeq z; \text{ and}$$

(v) it is *Archimedean*, i.e., for all $x, y \in M$

$$x^n \preccurlyeq y \text{ for all } n \in \mathbf{N} \text{ implies that } x = e.$$

Remark 16. In [18] a slightly weaker form of the Archimedean property (condition (v) of Definition 15) was used. In the context of strict compatibility the weaker form was enough to arrive at a sufficient condition for unique decomposition in partial commutative monoids. We include the stronger version here, because we will need to relax the requirement of strict compatibility to just compatibility to facilitate application of our result in the present setting of weak behavioural equivalences.

In [18] it was proved that the existence of a decomposition order on a partial commutative monoid is a necessary and sufficient condition for unique decomposition. The advantage of establishing unique decomposition via a decomposition order is that it circumvents first establishing cancellation, which in some cases is hard without knowing that the partial commutative monoid has unique decomposition. We refer to [18] for a more in-depth discussion.

In commutative monoids of processes, an obvious candidate decomposition order is the order induced on the commutative monoid by the transition relation. We define a binary relation $\longrightarrow$ on $\mathbf{B}$ and $\mathbf{W}$ by

$$[P] \longrightarrow [P'] \text{ if there exist } Q \in [P],\ Q' \in [P'] \text{ and } \alpha \in \mathcal{A}_\tau \text{ such that } Q \xrightarrow{\alpha} Q' \ .$$

We shall denote the inverse of the reflexive-transitive closure of $\longrightarrow$ (both on $\mathbf{B}$ and $\mathbf{W}$) by $\preccurlyeq$, i.e., $\preccurlyeq = (\longrightarrow^*)^{-1}$.

Lemma 17. *If P and Q are process expressions such that $[Q] \preccurlyeq [P]$, then for all $P' \in [P]$ there exist $Q' \in [Q]$, $k \geq 0$, $Q_0, \dots, Q_k \in \mathcal{P}$ and $\alpha_0, \dots, \alpha_k \in \mathcal{A}_\tau$ such that*

$$P' = Q_0 \xrightarrow{\alpha_0} \cdots \xrightarrow{\alpha_k} Q_k = Q' \ .$$

The following lemma implies that every set of process expressions has minimal elements with respect to the reflexive-transitive closure of the transition relation. Caution: the lemma holds true only thanks to the very limited facility for defining infinite behaviour in our calculus (see also Remark 20 below).

Lemma 18. *If $P_0, \dots, P_i, \dots$ $(i \in \mathbf{N})$ is an infinite sequence of process expressions, and $\alpha_0, \dots, \alpha_i, \dots$ $(i \in \mathbf{N})$ is an infinite sequence of elements in $\mathcal{A}_\tau$ such that $P_i \xrightarrow{\alpha_i} P_{i+1}$ for all $i \in \mathbf{N}$, then there exists $j \in \mathbf{N}$ such that $P_k = P_\ell$ for all $k, \ell \geq j$.*

Proof. Define the size $|P|$ of a process expression P as the number of symbols in P. It can then be shown with a straightforward induction on a derivation of the transition $P \xrightarrow{\alpha} P'$ according to the operational semantics in Table 1 that either $|P| > |P'|$ or $P = P'$. From this, the lemma clearly follows. □

Using Lemmas 17 and 18 it is straightforward to establish the following proposition.

Proposition 19. *The relation $\preccurlyeq$ is a well-founded precompositional partial order on each of the commutative monoids $\mathbf{B}$, $\mathbf{B}_n$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}$, $\mathbf{W}_n$, and $\mathbf{W}_{\mathit{fin}}$.*

Remark 20. That Lemma 18 holds true of our particular process calculus, and that, as a consequence (see the following proposition), $\preccurlyeq$ is well-founded on the unrestricted commutative monoids $\mathbf{B}$ and $\mathbf{W}$ is thanks to the very limited facility of defining infinite behaviour, by means of simple loops. In calculi with more expressive facilities to specify infinite behaviour (e.g., recursion, general iteration or replication) $\preccurlyeq$ as defined above is not well-founded (it is not even anti-symmetric). Note that the contribution of this article does not depend on the well-foundedness of $\mathbf{B}$ and $\mathbf{W}$, which is stated for completeness sake.

It is often possible to define a well-founded partial order on processes based on the transition relation in a setting with a more general form of infinite behaviour, at least for normed processes. See, e.g., [18] for an example of an anti-symmetric and well-founded order on normed processes definable in ACP with recursion, which is based on a restriction of the transition relation.

The ordering $\preccurlyeq$ defined on $\mathbf{B}_n$, $\mathbf{B}$, $\mathbf{W}_n$ and $\mathbf{W}$ is not a decomposition order: on $\mathbf{B}$ and $\mathbf{W}$ it does not satisfy conditions (ii), (iii) and (v) of Definition 15, and on $\mathbf{B}_n$ and $\mathbf{W}_n$ it does not satisfy condition (iii) of Definition 15.

Example 21.

1. Since $a^*\mathbf{0} \xrightarrow{a} a^*\mathbf{0}$ is the only transition from $a^*\mathbf{0}$, it follows that $[a^*\mathbf{0}]$ is a minimal element of $\mathbf{B}$ and $\mathbf{W}$ with respect to $\preccurlyeq$. It is also clear that $[a^*\mathbf{0}] \neq \mathbf{0}$, so we have that $\mathbf{0}$ is not the least element of $\preccurlyeq$ in $\mathbf{B}$ and $\mathbf{W}$.
2. In Example 3 we have argued that $a^*\mathbf{0} = a^*\mathbf{0} \parallel a^*\mathbf{0}$, from which it easily follows that $[a^*\mathbf{0}]^n = [a^*\mathbf{0}]$ for all $n \in \mathbf{N}$. Hence, $\preccurlyeq$ on $\mathbf{B}$ and $\mathbf{W}$ is not Archimedean.

Notice that in the above example, it is essential that $a^*\mathbf{0}$ is not normed. Using that both norm and depth are additive with respect to parallel composition, it follows that $\preccurlyeq$ is Archimedean on normed and bounded behaviour, and using that a process expression with a norm or depth equal to 0 is behaviourally equivalent to $\mathbf{0}$, it follows that $\mathbf{0}$ is the least element with respect to $\preccurlyeq$ on normed and bounded behaviour.

Proposition 22. *The partial order* $\preccurlyeq$ *on* $\mathbf{B}_n$*,* $\mathbf{B}_{\mathit{fin}}$*,* $\mathbf{W}_n$ *and* $\mathbf{W}_{\mathit{fin}}$ *is Archimedean and* $\mathbf{0}$ *is its least element.*

Example 23. Consider the process expressions $P = a^*\tau.b.\mathbf{0}$ and $Q = b.\mathbf{0}$ discussed in Example 5 (see also Figure 1). Then, since $P \xrightarrow{\tau} Q$ and $[P] \neq [Q]$, we have that $[Q] \prec [P]$, but also $[Q] \parallel [P] = [P] \parallel [P]$. It follows that $\preccurlyeq$ is not strictly compatible in $\mathbf{B}$, $\mathbf{B}_n$, $\mathbf{W}$, and $\mathbf{W}_n$.

We should now still ask ourselves the question whether $\preccurlyeq$ on $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ is strictly compatible. An important step towards proving the property for, e.g., $\mathbf{B}_{\mathit{fin}}$ would be to establish the following implication for all bounded process expressions P, Q and R:

$$P \xrightarrow{\tau} Q \;\&\; P \parallel R \leftrightarrow_{\mathrm{b}} Q \parallel R \Longrightarrow P \leftrightarrow_{\mathrm{b}} Q \ .$$

Example 23 illustrates that this implication does not hold for all normed processes, suggesting that the implication is perhaps hard to establish from first principles. In fact, all our attempts in this direction so far have failed. Note, however, that establishing the implication would be straightforward if we could use that $\parallel$ is cancellative (i.e., $P \parallel R \leftrightarrow_{\mathrm{b}} Q \parallel R$ implies $P \leftrightarrow_{\mathrm{b}} Q$), and this, in turn, would be easy if we could use that $\mathbf{B}_{\mathit{fin}}$ has unique decomposition.

The difficulty of establishing strict compatibility is really with strictness. Due to the shape of the operational rules for parallel composition (see Table 1) it is actually straightforward to establish the following non-strict variant. Let M be a partial commutative monoid; a partial order $\preccurlyeq$ on M is *compatible* if for all $x, y, z \in M$:

if $x \preccurlyeq y$ and yz is defined, then $xz \preccurlyeq yz$.

Proposition 24. *The partial order* $\preccurlyeq$ *on* $\mathbf{B}_n$*,* $\mathbf{B}_{\mathit{fin}}$*,* $\mathbf{W}_n$*, and* $\mathbf{W}_{\mathit{fin}}$ *is* compatible.

A partial order on a partial commutative monoid that has all the properties of a decomposition order except that it is compatible instead of strictly compatible, we shall henceforth call a *weak* decomposition order.

Definition 25. Let M be a partial commutative monoid; a partial order $\preccurlyeq$ on M is a *weak decomposition order* if it is well-founded, has the identity element $e \in M$ as least element, is compatible, precompositional and Archimedean.

The following corollary summarises Propositions 19, 22 and 24.

Corollary 26. *The partial order* $\preccurlyeq$ *on* $\mathbf{B}_n$*,* $\mathbf{B}_{\mathit{fin}}$*,* $\mathbf{W}_n$*, and* $\mathbf{W}_{\mathit{fin}}$ *is a weak decomposition order.*

In [18] it is proved that the existence of a decomposition order is a sufficient condition for a partial commutative monoid to have unique decomposition. Note that, since $\preccurlyeq$ is a weak decomposition order on $\mathbf{B}_n$ and $\mathbf{W}_n$, and since according to Example 5 these commutative monoids do not have unique decomposition, the existence of a *weak* decomposition order is *not* a sufficient condition for having unique decomposition; it should be supplemented with additional requirements to get a sufficient condition.

Strictness of compatibility—which is the only difference between the notion of decomposition order of [18] and the notion of weak decomposition order put forward here—is used in [18] both in the proof of *existence* of decompositions and in the proof that decompositions are *unique*. Thanks to the strengthening of the Archimedean property (cf. Remark 16), it is possible to establish the existence of decompositions in partial commutative monoids endowed with a weak decomposition order.

Proposition 27. *In every partial commutative monoid with a weak decomposition order, every element of M has a decomposition.*

Proof. Let M be a commutative monoid with a weak decomposition order $\preccurlyeq$; we prove with $\preccurlyeq$-induction that every element M has a decomposition. Let x be an element of M and suppose, by way of induction hypothesis, that all $\preccurlyeq$-predecessors of x have a decomposition; we distinguish two cases:

1. Suppose there exist $y, z \prec x$ such that $x = yz$. Then by the induction hypothesis y and z have decompositions d_y and d_z, respectively, and their sum $d_y \uplus d_z$ (see Example 8 for the definition of $\uplus$) is a decomposition of x.

2. Suppose there do not exist $y, z \prec x$ such that $x = yz$. Then, for all $y, z \in M$ such that $x = yz$ we have that $y = x$ or $z = x$, and hence $x = yx$ or $x = xz$.

   On the one hand, from $x = yx$ it follows that $x = y^n x$ for all $n \in \mathbf{N}$. Hence, since e is the least element of M with respect to $\preccurlyeq$ and $\preccurlyeq$ is compatible, we have $y^n = ey^n \preccurlyeq xy^n = y^n x = x$ for all $n \in \mathbf{N}$. So by the Archimedean property it follows that $y = e$. On the other hand, from $x = xz$ it follows by a similar argument that $z = e$.

   Thus, we have now established that $x = yz$ implies $y = e$ or $z = e$ for all $y, z \in M$. It follows that either $x = e$, in which case it has the empty multiset $\Box$ as decomposition, or x is indecomposable, in which case it has $\wr x \int$ as decomposition. $\Box$

It follows from Corollary 26 and Proposition 27 that in the monoids $\mathbf{B}_n$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}_n$, and $\mathbf{W}_{\mathit{fin}}$ every element has a decomposition. In the next section, we shall propose a general subsidiary property that will allow us to establish uniqueness of decompositions in commutative monoids with a weak decomposition order; in Section 5 we shall establish that this property holds in $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ and conclude that these monoids have unique decomposition.

4 Uniqueness

The failure of $\preccurlyeq$ on $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ to be strictly compatible prevents us from getting our unique decomposition results for those commutative monoids as an immediate consequence of the result in [18]. Nevertheless, many of the ideas in the proof of uniqueness of decompositions in [18] can be adapted and reused in the context of commutative monoids endowed with a weak decomposition order. Most importantly, the crucial *subtraction* property of decomposition orders holds for weak decomposition orders too, for its proof (see the proofs of Lemmas 24 and 25 and Corollary 16 in [18]) does not rely on strictness of compatibility.[1]

Lemma 28 (Subtraction)**.** *Let M be a partial commutative monoid with a weak decomposition order $\preccurlyeq$. Let $x, y, z \in M$, and suppose that xy has a unique decomposition. Then $xy \prec xz$ implies $y \prec z$.*

This section is devoted to eliminating the use of strictness of compatibility from most of the argument in [18] showing partial commutative monoids endowed with a decomposition order have unique decomposition, at the expense of more involved technical details.Thus, we shall push the use of strictness of compatibility to one corner case that can be settled if we replace strictness of compatibility by an alternative

[1]The proof of Lemma 24 in [18] does refer to Proposition 23 of [18] in which it is established that in a partial commutative monoid with a decomposition order every element has a decomposition using strict compatibility. But we have established in Proposition 27 that strictness of compatibility is not needed to conclude that every element has a decomposition.

requirement referred to as *power cancellation.* This will culminate in Theorem 34, the main result of this article, which states that a partial commutative monoid endowed with a weak decomposition order satisfying power cancellation has unique decomposition. In Section 5 we shall then establish that the weak decomposition orders that we have already defined on $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ satisfy power cancellation and conclude that these monoids both have unique decomposition.

Let us fix, for the remainder of this section, a partial commutative monoid M and a weak decomposition order $\preccurlyeq$ on M.

The uniqueness proof in [18] considers a minimal counterexample against unique decomposition, i.e., an element of the commutative monoid with at least two distinct decompositions, say d_1 and d_2, that is $\preccurlyeq$-minimal in the set of all such elements. Then, an important technique in the proof is to select a particular indecomposable in one of the two decompositions and replace it by predecessors with respect to the decomposition order. From minimality together with strict compatibility it is then concluded that the resulting decomposition is unique, which plays a crucial role in subsequent arguments towards a contradiction. To avoid the use of strictness of compatibility, we need a more sophisticated notion of minimality for the considered counterexample. The idea is to not just pick a $\preccurlyeq$-minimal element among the elements with two or more decompositions; we also choose the presupposed pair of distinct decompositions (d_1, d_2) in such a way that it is minimal with respect to a well-founded ordering induced by $\preccurlyeq$ on them.

The decomposition extension of $\preccurlyeq$ Let X be a set. In Example 8 we introduced the notion of multiset over X together with the binary operation $\uplus$ for multiset sum; we also need multiset difference: If m and n are multisets over X, then their multiset difference is the multiset $m - n$ that satisfies, for all $x \in X$,

$$m - n(x) = \begin{cases} m(x) - n(x) & \text{if } m(x) \geq n(x) \ ; \\ 0 & \text{otherwise} \ . \end{cases}$$

We define the *decomposition extension* $\lhd$ of $\prec$ by $d \lhd d'$ if, and only if, there exist, for some $k \geq 1$, a sequence of indecomposables $p_1, \dots, p_k \in M$, a sequence $x_1, \dots, x_k \in M$, and a sequence of decompositions $d_1, \dots, d_k$ such that

(i) $x_i \prec p_i$ $(1 \leq i \leq k)$;

(ii) each d_i is a decomposition of x_i $(1 \leq i \leq k)$; and

(iii) $d = (d' - \wr p_1, \dots, p_k \wr) \uplus (d_1 \uplus \cdots \uplus d_k)$.

We write $d \unlhd d'$ if $d = d'$ or $d \lhd d'$. Note that if $d \unlhd d'$, x is the composition of d, and y is the composition of d', then, by compatibility, $x \preccurlyeq y$.

The following two lemmas express general properties of the decomposition extension.

Lemma 29. *Let d_1 and d_2 be decompositions such that $d_1 \equiv d_2$. Then for every decomposition $d_1' \unlhd d_1$ there exists a decomposition $d_2' \unlhd d_2$ such that $d_1' \equiv d_2'$.*

Proof. Let $d_1' \unlhd d_1$. Clearly, if $d_1' = d_1$, then we can take $d_2' = d_2$ and immediately get $d_1' = d_1 \equiv d_2 = d_2'$. So suppose that $d_1' \lhd d_1$. Then there exist a decomposition d_1'' and, for some $k \geq 1$, sequences of indecomposables $p_1, \dots, p_k$ and of decompositions $d_{1,1}, \dots, d_{1,k}$ such that

(i) $d_1 = d_1'' \uplus \wr p_1, \dots, p_k \wr$;

(ii) each $d_{1,i}$ is a decomposition of a predecessor of p_i $(1 \leq i \leq k)$; and

(iii) $d_1' = d_1'' \uplus d_{1,1} \uplus \cdots \uplus d_{1,k}$.

Denote by x, x', x'', and x_i ($1 \leq i \leq k$) the compositions of the decompositions d_1, d_1', d_1'' and $d_{1,i}$ ($1 \leq i \leq k$), respectively. Then, for all $1 \leq i \leq k$, x_i is a $\preccurlyeq$-predecessor of p_i, so, by compatibility,

$$x' = x'' x_1 \cdots x_k \preccurlyeq x'' p_1 \cdots p_k = x \ .$$

If $x' = x$, then $d_1' \equiv d_2$, so we can take $d_2' = d_2$ and get $d_1' \equiv d_2'$.

It remains to consider the case that $x' \prec x$. Let $q_1, \ldots, q_\ell$ be such that $d_2 = \wr q_1, \ldots, q_\ell \int$. Then, since x is the composition of d_1 and $d_1 \equiv d_2$, $x = q_1 \cdots q_\ell$, and hence, by precompositionality, there exist $x_1', \ldots, x_\ell'$ such that $x' = x_1' \cdots x_\ell'$ and $x_i' \preccurlyeq q_i$ ($1 \leq i \leq \ell$). Note that, since $x' \neq x$, there is at least one $1 \leq i \leq \ell$ such that ${x_i}' \neq q_i$. We assume without loss of generality that the indecomposables $q_1, \ldots, q_\ell$ and their weak predecessors $x_1', \ldots, x_\ell'$ are ordered in such a way that there exists $1 \leq j \leq \ell$ such that $x_i' = q_i$ for all $1 \leq i < j$, and ${x_i}' \prec q_i$ for all $j \leq i \leq \ell$. Let $d_{2,j}', \ldots, d_{2,\ell}'$ be decompositions of $x_j', \ldots, x_\ell'$, and define $d_2' = \wr q_1, \ldots, q_{j-1} \int \uplus d_{2,j}' \uplus \cdots \uplus d_{2,\ell}'$. Then $d_2' \lhd d_2$, and since d_1' and d_2' both have x' as their composition, we have that $d_1' \equiv d_2'$. □

Lemma 30. *The relation $\unlhd$ is a well-founded partial order on decompositions.*

Proof. It is immediate from the definition of $\unlhd$ that it is reflexive and transitive. It remains to establish that $\unlhd$ is well-founded, for a well-founded reflexive and transitive relation is a partial order. To this end, note that $\unlhd$ is a subset of the standard multiset ordering associated with the well-founded partial order $\preccurlyeq$, which is proved to be well-founded by Dershowitz and Manna in [9]. □

We shall use the well-foundedness of both $\preccurlyeq$ and the Cartesian order $\unlhd_\times$ induced on pairs of decompositions by the well-founded partial order $\unlhd$. For two pairs of decompositions (d_1, d_2) and (d_1', d_2'), we write $(d_1, d_2) \unlhd_\times (d_1', d_2')$ if $d_1 \unlhd d_1'$ and $d_2 \unlhd d_2'$. A pair of decompositions (d_1, d_2) is said to be a *counterexample* against unique decomposition if d_1 and d_2 are distinct but equivalent, i.e., if $d_1 \equiv d_2$, but not $d_1 = d_2$. A counterexample (d_1, d_2) against unique decomposition is *minimal* if it is both minimal with respect to $\preccurlyeq$ and minimal with respect to $\unlhd_\times$. That is, a counterexample (d_1, d_2) against unique decomposition is *minimal* if

1. all $\preccurlyeq$-predecessors of the (common) composition of d_1 and d_2 have a unique decomposition; and
2. for all (d_1', d_2') such that $(d_1', d_2') \unlhd_\times (d_1, d_2)$ and $(d_1', d_2') \neq (d_1, d_2)$ it holds that $d_1' \equiv d_2'$ implies $d_1' = d_2'$.

Since both $\preccurlyeq$ and $\unlhd_\times$ are well-founded, if unique decomposition would fail, then there would exist a minimial counterexample. The general idea of the proof is that we derive a contradiction from the assumption that there exists a minimal counterexample (d_1, d_2) against unique decomposition. The decompositions d_1 and d_2 should be distinct, so the set of indecomposables that occur more often in one of the decompositions than in the other is non-empty. This set is clearly also finite, so it has $\preccurlyeq$-maximal elements. We declare p to be such a $\preccurlyeq$-maximal element, and assume, without loss of generality, that p occurs more often in d_1 than in d_2. Then we have that

(A) $d_1(p) > d_2(p)$; and

(B) $d_1(q) = d_2(q)$ for all indecomposables q such that $p \prec q$.

We shall distinguish two cases, based on how the difference between d_1 and d_2 manifests itself, and derive a contradiction in both cases:

1. $d_1(p) > d_2(p) + 1$ or $d_1(q) \neq 0$ for some indecomposable q distinct from p; we refer to this case by saying that d_1 and d_2 are *too far apart*.

2. $d_1(p) = d_2(p) + 1$ and $d_1(q) = 0$ for all q distinct from p; we refer to this case by saying that d_1 and d_2 are *too close together*.

Case 1: d_1 and d_2 are too far apart In this case, either the multiplicity of p in d_1 exceeds the multiplicity of p in d_2 by at least 2, or the difference in multiplicities is 1 but there is another indecomposable q, distinct from p, in d_1. We argue that d_1 has a predecessor d' in which p occurs more often than in any predecessor of d_2, while, on the other hand, the choice of a minimal counterexample implies that every predecessor of d_1 is also a predecessor of d_2. (The arguments leading to a contradiction in this case are analogous to the arguments in the proof in [18]; the only important difference is the use of the ordering $\trianglelefteq$ instead of $\preccurlyeq$.)

Using that $\preccurlyeq$ is compatible and Archimedean, it can be established that there is a bound on the multiplicity of p in the predecessors of d_1.

Lemma 31. *The set* $\{d_1'(p) : d_1' \lhd d_1\}$ *is finite.*

Proof. Denote by y the composition of d_1. Clearly, if d_1' is a predecessor of d_1, then, by compatibility, we have that $p^n \preccurlyeq y$ for all $n \leq d_1'(p)$. Hence, if the set $\{d_1'(p) : d_1' \lhd d_1\}$ would *not* be finite, then $p^n \preccurlyeq y$ for all $n \in \mathbf{N}$, from which, since $\preccurlyeq$ is Archimedean, it would follow that $p = e$. But $p = e$ is in contradiction with the assumption that p is indecomposable. □

Let m be the maximum of the multiplicities of p in predecessors of d_1, i.e.,

$$m := \max\{d_1'(p) : d_1' \lhd d_1\} \ . \tag{3}$$

On the one hand, if $d_1(p) > d_2(p)+1$, then $d_1 - \Lbag p \Rbag \lhd d_1$, so $m \geq d_1(p) - 1 > d_2(p)$. On the other hand, if $d_1(q) \neq 0$ for some indecomposable $q \neq p$, then $d_1 - \Lbag q \Rbag \lhd d_1$, so $m \geq d_1(p) > d_2(p)$. Hence

$$d_2(p) < m \ . \tag{4}$$

If $k \in \mathbf{N}$, then we write $k \cdot \Lbag p \Rbag$ for the decomposition consisting of k occurrences of p, i.e., the multiset for which it holds that

$$(k \cdot \Lbag p \Rbag)(q) = \begin{cases} k & \text{if } q = p \ ; \\ 0 & \text{otherwise} \ . \end{cases}$$

From (3) it is clear that $m \cdot \Lbag p \Rbag \lhd d_1$. Hence, by Lemma 29, there exists $d_2' \trianglelefteq d_2$ such that $m \cdot \Lbag p \Rbag \equiv d_2'$. Since (d_1, d_2) is a minimal counterexample, it follows that $m \cdot \Lbag p \Rbag = d_2'$, and hence $m \cdot \Lbag p \Rbag \trianglelefteq d_2$. Moreover, from (4), it is clear that $m \cdot \Lbag p \Rbag \neq d_2$, so $m \cdot \Lbag p \Rbag \lhd d_2$. Thus, we now have

$$m \cdot \Lbag p \Rbag \lhd d_1, d_2 \ . \tag{5}$$

We now proceed to argue that indecomposables distinct from p in d_2 can be used to *create* $m - d_2(p)$ additional occurrences of p in predecessors of d_2. Since those extra occurrences of p can only be created by occurrences in d_2 of indecomposables q such that $p \prec q$, it can be concluded by assumption (B) that d_1 must have the same potential for creating extra occurrences of p. We shall see that this reasoning will eventually lead to a contradiction with our definition of m as the maximal number of occurrences of p in predecessors of d_1.

In the remainder of our argument, it will be convenient to have notation for specific parts of d_1 and d_2: For $i = 1, 2$ we denote by $d_i^{\succ p}$ the multiset consisting of all indecomposables q in d_i such that $p \prec q$, i.e., $d_i^{\succ p}$ is defined by

$$d_i^{\succ p}(q) = \begin{cases} d_i(q) & \text{if } q \succ p \ ; \\ 0 & \text{otherwise} \ ; \end{cases}$$

we denote by $d_i^{=p}$ the multiset consisting of all occurrences of p in d_i, i.e., $d_i^{=p}$ is defined by

$$d_i^{=p}(q) = \begin{cases} d_i(q) & \text{if } q = p \ ; \\ 0 & \text{otherwise} \ ; \end{cases}$$

we denote by $d_i^{\not\succeq p}$ the multiset consisting of all occurrences of p in d_i, i.e., $d_i^{\not\succeq p}$ is defined by

$$d_i^{\not\succeq p}(q) = \begin{cases} d_i(q) & \text{if } q \not\succeq p \ ; \\ 0 & \text{otherwise} \ . \end{cases}$$

Then clearly we have

$$d_i = d_i^{\succ p} \uplus d_i^{=p} \uplus d_i^{\not\succeq p} \qquad (i = 1, 2) \ .$$

That the decompositions $d_i^{\succ p}$ $(i = 1, 2)$ both incorporate the potential of creating $m - d_2(p)$ occurrences of p is formalised by proving that $(m - d_2(p)) \cdot \wr p \int \lhd d_i^{\succ p}$ $(i = 1, 2)$. We shall first prove $(m - d_2(p)) \cdot \wr p \int \lhd d_2^{\succ p}$, and for this we need the following general lemma.

Let $x = p^{d_2(p)}$ and $y = p^{m - d_2(p)}$, and denote by z the composition of $d_2^{\succ p} \uplus d_2^{\not\succeq p}$. Then $xy = p^m$ and xz is equal to the composition of both d_1 and d_2. Note that from (5) and the minimality of the counterexample (d_1, d_2) it immediately follows that $p^m = xy \prec xz$. (For if $xy = xz$, then $p^m = xz$, so both $(m \cdot \wr p \int, d_2)$ and $(d_1, m \cdot \wr p \int)$ would constitute smaller counterexamples.) It follows that xy has a unique decomposition, so by Lemma 28 it follows that $y \prec z$.

Lemma 32. *If $y \prec z$ and d is a decomposition of z, then y has a decomposition d' such that $d' \lhd d$.*

Proof. Let $d = \wr p_1, \ldots, p_k \int$. Then $y \prec p_1 \cdots p_k$, so, by precompositionality, there exist $y_1, \ldots, y_k$ such that $y_i \preccurlyeq p_i$ for all $1 \leq i \leq k$. The y_i have decompositions, say $d_i{}'$, and clearly $d' = d_1{}' \uplus \cdots \uplus d_k{}'$ is a decomposition of y satisfying $d' \unlhd d$. Since $d' = d$ would imply $y = z$, it follows that $d' \lhd d$. □

By the preceding lemma, y has a decomposition, say d_2', such that $d_2' \lhd d_2^{\succ p} \uplus d_2^{\not\succeq p}$, and since y, in fact, has a unique decomposition, it follows that $(m - d_2(p)) \cdot \wr p \int \lhd d_2^{\succ p} \uplus d_2^{\not\succeq p}$. By definition of $d_2^{\not\succeq p}$, p does not occur in $d_2^{\not\succeq p}$, nor in any decomposition of a predecessor of an indecomposable in $d_2^{\not\succeq p}$, so $(m - d_2(p)) \cdot \wr p \int \lhd d_2^{\succ p}$. Since $d_2^{\succ p} = d_1^{\succ p}$ according to assumption (B), we have $(m - d_2(p)) \cdot \wr p \int \lhd d_1^{\succ p}$. It follows that

$$(m - d_2(p) + d_1(p)) \cdot \wr p \int \lhd d_1 \ , \tag{6}$$

and since $d_2(p) < d_1(p)$ according to assumption (A), we find $m - d_2(p) + d_1(p) > m$. Thus we have now derived a contradiction with our definition of m in (3) as the maximum of the multiplicities of p in the predecessors of d_1.

Case 2: d_1 and d_2 are too close together In this case d_1 contains no other indecomposables than p, while d_2 has $d_1(p)-1$ occurrences of p supplemented with a multiset d'_2 of other indecomposables.

In [18] it is proved, via a sophisticated argument, that the composition of d'_2 is a $\preccurlyeq$-predecessor of p. Hence, by strict compatibility, the composition of d_2 is an $\preccurlyeq$-predecessor of d_1, which is in contradiction with the assumption that the decompositions d_1 and d_2 are equivalent.

That $\preccurlyeq$ is not strictly compatible, but just compatible, leaves the possibility that d_1 and d_2 are equivalent even if the composition of d'_2 is a predecessor of p. For $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ this possibility can be ruled out by noting that the composition of d'_2 can be reached from p by τ-transitions, and proving that every transition of p can be simulated by a transition of the composition of d'_2. The following notion formalises this reason in the abstract setting of commutative monoids with a weak decomposition order.

Definition 33. Let M be a partial commutative monoid, and let $\preccurlyeq$ be a weak decomposition order on M. We say that $\preccurlyeq$ satisfies *power cancellation* if for all $x, y \in M$ and for every indecomposable $p \in M$ such that $p \not\prec x, y$ it holds that

$$p^k x = p^k y \text{ implies } x = y \text{ for all } k \in \mathbf{N}.$$

Suppose that $\preccurlyeq$ on M has power cancellation, let $k = d_2(p)$ and let x be the composition of d'_2. Then from $d_1 \equiv d_2$ it follows that

$$p^k p = p^k x \ .$$

Clearly, $p \not\prec p$ and, since d'_2 consists of indecomposables q such that $p \not\preccurlyeq q$, it follows by precompositionality that also $p \not\preccurlyeq x$. Hence, since $\preccurlyeq$ has power cancellation, $p = x$, so $d'_2 = \wr p \int$. It follows that $d_1 = d_2$, which contradicts that (d_1, d_2) is a counterexample against unique decomposition.

Theorem 34. *Every partial commutative monoid M with a weak decomposition order that satisfies power cancellation has unique decomposition.*

We conclude this section with the observation that a weak decomposition satisfying power cancellation is, in fact, strictly compatible, and hence a decomposition order. To see this, consider a partial commutative monoid M endowed with a weak decomposition order $\preccurlyeq$ that satisfies power cancellation. Since, by Theorem 34, M has unique decomposition, it also has *cancellation*: if $xz = yz$ implies $x = y$ for all $x, y \in M$ (see, e.g., Corollary 19 in [18]). Now, to establish that $\preccurlyeq$ is strictly compatible, let $x, y, z \in M$ and suppose that $x \prec y$ and yz is defined; then, by compatibility, $xz \preccurlyeq yz$. Since $x \neq y$ implies $xz \neq yz$ by cancellation, it follows that $xz \prec yz$.

Corollary 35. *A weak decomposition order satisfying power cancellation is a decomposition order.*

5 Bounded behaviour has unique parallel decomposition

In Section 3 we have already established that in the commutative monoids $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ every element has a decomposition and that $\preccurlyeq$ is a weak decomposition order on $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$. To be able to conclude from Theorem 34 at the end of Section 4 that $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$ have unique decomposition, it remains to establish that $\preccurlyeq$ on these commutative monoids satisfies power cancellation.

Proposition 36. *The weak decomposition order* $\preccurlyeq$ *on* $\mathbf{B}_{\mathit{fin}}$ *and* $\mathbf{W}_{\mathit{fin}}$ *satisfies power cancellation.*

Proof. We present the proof for $\mathbf{B}_{\mathit{fin}}$; the proof for $\mathbf{W}_{\mathit{fin}}$ is very similar except that some details are slightly simpler.

Let p be a indecomposable element in $\mathbf{B}_{\mathit{fin}}$, and let x, y and z be elements of $\mathbf{B}_{\mathit{fin}}$ such that $p \not\preccurlyeq x, y$, and, for some $k \in \mathbf{N}$,

$$z = p^k x = p^k y \ ; \tag{7}$$

we need to prove that $x = y$.

To this end, we first note that the ordering $\preccurlyeq$ on $\mathbf{B}_{\mathit{fin}} \times \mathbf{B}_{\mathit{fin}} \times \mathbf{B}_{\mathit{fin}}$ defined by

$$(u', v', w') \preccurlyeq (u, v, w) \text{ if } u' \preccurlyeq u \text{ and whenever } u' = u \text{ then also } v' \preccurlyeq v \text{ and } w' \preccurlyeq w$$

is well-founded. We proceed by $\preccurlyeq$-induction on (z, x, y), and suppose, by way of induction hypothesis, that whenever $(z', x', y') \prec (z, x, y)$ and, for some indecomposable element $p' \not\preccurlyeq x', y'$ of $\mathbf{B}_{\mathit{fin}}$, $z' = (p')^\ell x' = (p')^\ell y'$, then $x' = y'$.

Note that x and y are non-empty sets of process expressions, and that, to prove $x = y$, it suffices to show that there exist process expressions $Q \in x$ and $R \in y$ such that $Q \leftrightarroweq_{\mathrm{b}} R$. By Lemma 18, the non-empty sets of process expressions x and y have minimal elements with respect to the ordering induced on process expressions by $(\xrightarrow{\tau}{}^*)^{-1}$. Let Q and R be $(\xrightarrow{\tau}{}^*)^{-1}$-minimal elements in x and y, respectively; we prove that $Q \leftrightarroweq_{\mathrm{b}} R$ by establishing that the binary relation

$$\mathcal{R} = \{(Q, R), (R, Q)\} \cup \leftrightarroweq_{\mathrm{b}}$$

is a branching bisimulation.

To this end, we first suppose that $Q \xrightarrow{\alpha} Q'$ for some Q', and prove that there exist R'' and R' such that $R \twoheadrightarrow R'' \xrightarrow{(\alpha)} R'$, $Q \mathrel{\mathcal{R}} R''$, and $Q' \mathrel{\mathcal{R}} R'$.

Let P be an element of p, denote by $P^{\underline{k}}$ the k-fold parallel composition of P, and let $z' = [P^{\underline{k}} \parallel Q']_b$. Then $z' \preccurlyeq z$, so we can distinguish two cases:

Case 1: Suppose that $z' = z$. Then, since $P^{\underline{k}} \parallel Q$ is bounded, it follows that $\alpha = \tau$. Let $x' = [Q']_b$; since Q is a minimal element of x, we have that $x' \prec x$. Hence, $(z', x', y) \prec (z, x, y)$, so by the induction hypothesis $[Q']_b = x' = y = [R]_b$. It follows that $Q' \leftrightarroweq_{\mathrm{b}} R$, and we can take $R'' = R' = R$.

Case 2: Suppose that $z' \prec z$. Then, by the induction hypothesis, $\preccurlyeq$ on the partial commutative submonoid $\{z'' : z'' \preccurlyeq z'\}$ of $\mathbf{B}_{\mathit{fin}}$ satisfies power cancellation. By Theorem 34, it follows that z' has a unique decomposition in that submonoid, and hence in $\mathbf{B}_{\mathit{fin}}$ too. From $Q \xrightarrow{\alpha} Q'$ it follows that

$$P^{\underline{k}} \parallel Q \xrightarrow{\alpha} P^{\underline{k}} \parallel Q' \ ,$$

and hence, since $P^{\underline{k}} \parallel Q \leftrightarroweq_{\mathrm{b}} P^{\underline{k}} \parallel R$ according to (7), there exist R', R'', S', and S'' such that

$$P^{\underline{k}} \parallel R \twoheadrightarrow S'' \parallel R'' \xrightarrow{(\alpha)} S' \parallel R' \ ,$$

with $P^{\underline{k}} \parallel Q \leftrightarroweq_{\mathrm{b}} S'' \parallel R''$ and $P^{\underline{k}} \parallel Q' \leftrightarroweq_{\mathrm{b}} S' \parallel R'$. We have that

$$[R']_b \preccurlyeq [R'']_b \preccurlyeq [R]_b$$

and

$$[S']_b \preccurlyeq [S'']_b \preccurlyeq [P^k]_b \ ,$$

and, since $[S']_b \parallel [R']_b = z' \neq z = [P^{\underline{k}} \parallel R]_b$, it also holds that $[R']_b \neq [R]_b$, or $[S']_b \neq [P^{\underline{k}}]_b$. We distinguish two subcases:

CASE 2.1: Suppose $[R']_b \prec [R]_b$. Then, since $p \not\preccurlyeq x = [R]_b$, the unique decomposition of $[R']_b$ cannot have occurrences of p. Since z' has k occurrences of p, it follows that $p^k \preccurlyeq [S']_b \preccurlyeq [S'']_b \preccurlyeq [P^{\underline{k}}]_b = p^k$, so $[S']_b = [S'']_b = p^k$. Since $z' = p^k \parallel [Q']_b = p^k \parallel [R']_b$, by the induction hypothesis $[Q']_b = [R']_b$, and hence $Q' \mathcal{R} R'$.

It remains to establish that $Q \mathcal{R} R''$. If $R'' = R$, then, since $Q \mathcal{R} R$, this is immediate. If $R'' \neq R$, then since R is a $(\xrightarrow{\tau}{}^*)^{-1}$-minimal element of y, it follows that $[R'']_b \prec [R]_b$, so from $z = p^k \parallel [Q]_b = p^k \parallel [R'']_b$ it follows by the induction hypothesis that $[Q]_b = [R'']_b$, and hence $Q \mathcal{R} R''$.

CASE 2.2: Suppose $[S']_b \prec [P^k]_b$. Then the multiplicity of p in the unique decomposition of $[S']_b$ is at most $k-1$. Hence, since $[S']_b \parallel [R']_b = z' = p^k \parallel [Q']_b$, it follows that p must be an element of $[R']_b$. This means that $p \preccurlyeq [R']_b$, and since $p \not\preccurlyeq y = [R]_b$, it follows that $[P]_b = p = [R]_b$, and hence $P \leftrightarroweq_{\mathrm{b}} R$. Thus, we also get that the multiplicity of p in the decomposition of $[S']_b$ is, in fact, $k-1$, and therefore we can assume without loss of generality that there exist process expressions $P_1, P_2, \ldots, P_k, {P_1}'$ such that

$$
\begin{aligned}
&S'' = P_1 \parallel P_2 \parallel \cdots \parallel P_k \ , \\
&S' = {P_1}' \parallel P_2 \parallel \cdots \parallel P_k \ , \\
&P \twoheadrightarrow P_i \quad (1 \leq i \leq k) \ , \\
&P \leftrightarroweq_{\mathrm{b}} P_i \quad (2 \leq i \leq k) \ , \text{ and} \\
&P_1 \xrightarrow{(\alpha)} {P_1}' \ .
\end{aligned}
$$

From $P^{\underline{k}} \parallel Q' \leftrightarroweq_{\mathrm{b}} R \parallel P_2 \parallel \cdots P_k \parallel {P_1}'$, $P \leftrightarroweq_{\mathrm{b}} R$, and $P \leftrightarroweq_{\mathrm{b}} P_i$ $(2 \leq i \leq k)$ it follows that $Q' \leftrightarroweq_{\mathrm{b}} {P_1}'$. Hence, since $P \leftrightarroweq_{\mathrm{b}} R$, there exist R_1, ${R_1}'$ such that $R \twoheadrightarrow R_1 \xrightarrow{(\alpha)} {R_1}'$, $P_1 \leftrightarroweq_{\mathrm{b}} R_1$, and ${P_1}' \leftrightarroweq_{\mathrm{b}} {R_1}'$. From $Q' \leftrightarroweq_{\mathrm{b}} {P_1}' \leftrightarroweq_{\mathrm{b}} {R_1}'$ it follows that $Q' \mathcal{R} {R_1}'$.

It remains to establish that $Q \mathcal{R} R_1$. If $R_1 = R$, then, since $Q \mathcal{R} R$, this is immediate. If $R_1 \neq R$, then, since R is a $(\xrightarrow{\tau}{}^*)^{-1}$-minimal element of y, it follows that $[P_1]_b = [R_1]_b \prec [R]_b = [P]_b$. So from $z = p^k \parallel [Q]_b = p^k \parallel [P_1]_b$ it follows by the induction hypothesis that $Q \leftrightarroweq_{\mathrm{b}} P_1 \leftrightarroweq_{\mathrm{b}} R_1$, and hence $Q \mathcal{R} R_1$.

In a completely analogous manner, it can be established that whenever $R \xrightarrow{\alpha} R'$ for some process expression R', then there exist process expressions Q' and Q'' such that $Q \twoheadrightarrow Q'' \xrightarrow{(\alpha)} Q'$, $R \mathcal{R} Q''$, and $R' \mathcal{R} Q'$.

We conclude that $\mathcal{R}$ is a branching bisimulation, and hence $Q \leftrightarroweq_{\mathrm{b}} R$. □

By Corollaries 26 and 36, the commutative monoids $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ are endowed with a weak decomposition order $\preccurlyeq$ satisfying power cancellation. By Theorem 34 it follows that they have unique decomposition.

Corollary 37. *The commutative monoids $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ have unique decomposition.*

6 Concluding remarks

We have presented a general sufficient condition on partial commutative monoids that implies the property of unique decomposition, and is applicable to commutative monoids of behaviour incorporating a notion of unobservability. We have illustrated the application of our condition in the context of a very simple process calculus with an operation for pure interleaving as parallel compostion. The applicability is, however, not restricted to settings with this particular type of parallel composition. In fact, it is to be expected that our condition, similarly as in [18], can also be used to prove unique decomposition results in settings with more complicated notions of parallel composition operator allowing, e.g., synchronisation between components.

We leave for future investigations to what extent our theory of unique decomposition can be applied to variants of π-calculus. The article [10], in which unique parallel decomposition is established for a fragment of Applied π-calculus, will serve as a good starting point. A complication, illustrated in [10], is that parallel components may fuse into a single indecomposable process due to scope extrusion. As a consequence, precompositionality fails for the order induced on equivalence classes of π-terms by the transition relation. A solution may be to use a fragment of the transition relation that avoids scope extrusion.

In [4], Balabonski and Haucourt address the problem of unique parallel decomposition in the context of a concurrent programming language with a geometric semantics. It is less clear whether our general theory of unique decomposition is applicable there too; at least, the geometric semantics does not as naturally induce a candidate decomposition order on processes as in a process calculus with a transition system semantics. It would be interesting to compare the approaches.

Acknowledgement The author is grateful to both reviewers for their fine suggestions. In particular, one of the reviewers suggested Proposition 27 and its proof, which resulted in a stronger formulation of the main result and significant improvements in presentation.

References

[1] L. Aceto, W. J. Fokkink, A. Ingolfsdottir, and B. Luttik. CCS with Hennessy's merge has no finite equational axiomatization. *Theor. Comput. Sci.*, 330(3):377–405, 2005.

[2] L. Aceto, W. J. Fokkink, A. Ingólfsdóttir, and B. Luttik. A finite equational base for CCS with left merge and communication merge. *ACM Trans. Comput. Log.*, 10(1), 2009.

[3] L. Aceto, A. Ingólfsdóttir, B. Luttik, and P. van Tilburg. Finite equational bases for fragments of CCS with restriction and relabelling. In G. Ausiello, J. Karhumäki, G. Mauri, and C.-H. L. Ong, editors, *Fifth IFIP International Conference On Theoretical Computer Science - TCS 2008, IFIP 20th World Computer Congress, TC 1, Foundations of Computer Science, September 7-10, 2008, Milano, Italy*, volume 273 of *IFIP*, pages 317–332. Springer, 2008.

[4] T. Balabonski and E. Haucourt. A geometric approach to the problem of unique decomposition of processes. In P. Gastin and F. Laroussinie, editors, *CONCUR*, volume 6269 of *LNCS*, pages 132–146. Springer, 2010.

[5] T. Basten. Branching bisimilarity is an equivalence indeed! *Information Processing Letters*, 58(3):141–147, 1996.

[6] I. Castellani and M. Hennessy. Distributed bisimulations. *J. ACM*, 36(4):887–911, 1989.

[7] S. Christensen. *Decidability and Decomposition in Process Algebras.* PhD thesis, University of Edinburgh, 1993.

[8] F. Corradini, R. Gorrieri, and D. Marchignoli. Towards parallelization of concurrent systems. *RAIRO Inform. Théor. Appl.*, 32(4-6):99–125, 1998.

[9] N. Dershowitz and Z. Manna. Proving termination with multiset orderings. *Commun. ACM*, 22(8):465–476, 1979.

[10] J. Dreier, C. Ene, P. Lafourcade, and Y. Lakhnech. On unique decomposition of processes in the applied π-calculus. In Frank Pfenning, editor, *Proceedings of the 16th International Conference on Foundations of Software Science and Computation Structures (FOSSACS 2013)*, volume 7794 of *Lecture Notes in Computer Science*, pages 50–64. Springer, 2013.

[11] W. J. Fokkink and B. Luttik. An *omega*-complete equational specification of interleaving. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *Proceedings of the 27th International Colloquium on Automata, Languages and Programming (ICALP 2000)*, volume 1853 of *LNCS*, pages 729–743. Springer, 2000.

[12] S. B. Fröschle and S. Lasota. Normed processes, unique decomposition, and complexity of bisimulation equivalences. *Electr. Notes Theor. Comput. Sci.*, 239:17–42, 2009.

[13] R. J. van Glabbeek and W. P. Weijland. Branching time and abstraction in bisimulation semantics. *J. ACM*, 43(3):555–600, 1996.

[14] J. F. Groote and F. Moller. Verification of parallel systems via decomposition. In R. Cleaveland, editor, *Proceedings of the 3rd International Conference on Concurrency Theory (CONCUR'92)*, volume 630 of *LNCS*, pages 62–76. Springer, 1992.

[15] Daniel Hirschkoff and Damien Pous. A distribution law for CCS and a new congruence result for the p-calculus. *Logical Methods in Computer Science*, 4(2), 2008.

[16] Y. Hirshfeld and M. Jerrum. Bisimulation equivalence is decidable for normed process algebra. In J. Wiedermann, P. van Emde Boas, and M. Nielsen, editors, *Proceedings of 26th International Colloquium on Automata, Languages and Programming (ICALP'99)*, volume 1644 of *LNCS*, pages 412–421. Springer, 1999.

[17] Ivan Lanese, Jorge A. Pérez, Davide Sangiorgi, and Alan Schmitt. On the expressiveness and decidability of higher-order process calculi. *Inf. Comput.*, 209(2):198–226, 2011.

[18] B. Luttik and V. van Oostrom. Decomposition orders—another generalisation of the fundamental theorem of arithmetic. *Theor. Comput. Sci.*, 335(2-3):147–186, 2005.

[19] Bas Luttik. Unique parallel decomposition in branching and weak bisimulation semantics. In J. C. M. Baeten, T. Ball, and F. S. de Boer, editors, *Proceedings of the 7th IFIP TC 1/WG 2.2 International Conference on Theoretical Computer Science (TCS 2012)*, volume 7604 of *Lecture Notes in Computer Science*, pages 250–264. Springer, 2012.

[20] R. Milner. *Communication and Concurrency*. Prentice-Hall International, 1989.

[21] R. Milner. Operational and algebraic semantics of concurrent processes. In *Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics (B)*, pages 1201–1242. The MIT Press, 1990.

[22] R. Milner and F. Moller. Unique decomposition of processes. *Theoret. Comput. Sci.*, 107:357–363, January 1993.

[23] F. Moller. *Axioms for Concurrency.* PhD thesis, University of Edinburgh, 1989.

[24] Faron Moller. The importance of the left merge operator in process algebras. In Mike Paterson, editor, *Proceedings of the 17th International Colloquium on Automata, Languages and Programming (ICALP'90)*, volume 443 of *Lecture Notes in Computer Science*, pages 752–764. Springer, 1990.

[25] Faron Moller. The nonexistence of finite axiomatisations for CCS congruences. In *Proceedings of the Fifth Annual Symposium on Logic in Computer Science (LICS '90)*, pages 142–153. IEEE Computer Society, 1990.