Unique Parallel Decomposition in Branching and Weak Bisimulation Semantics

Bas Luttik

Unique Parallel Decomposition in Branching and Weak Bisimulation Semantics

Bas Luttik

Eindhoven University of Technology

Abstract. We consider the property of unique parallel decomposition modulo branching and weak bisimilarity. First, we show that totally 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 [18] 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, in [19], proved several more unique parallel decomposition results, 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 [5], 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 [15] 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 [15], 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 [15] 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 paper, 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 [15] 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 (totally 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 of interest about process calculi. For instance, Moller's proofs in [20, 21] that PA and CCS cannot be finitely axiomatised without auxiliary operations, Hirshfeld and Jerrum's proof in [12] that bisimilarity is decidable for normed PA, and the completeness proofs for the equational axiomatisations of PA and CCS with auxiliary operations in [8] and [1], all rely on unique parallel decomposition. 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 [4], 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 [6], or for improving verification methods [11].

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 totally normed behaviours may have more than one decomposition. In Section 3 we recap the theory of decomposition put forward in [15] 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 [15] to make it suitable for proving unique parallel decomposition results in process calculi with a notion of unobservability. We end the paper in Section 5 with a short conclusion.

This article is an extended abstract of [14], which includes additional examples and detailed explanations, and more elaborate proofs.

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 decomposition, and of totally 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 [16]) 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.

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

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

Table 1. The operational semantics.

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 shall henceforth write $P \longrightarrow\!\!\!\!\!\rightarrow P'$ if there exist $P_0, \ldots, P_n$ ($n \geq 0$) 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 [10]) *A symmetric binary relation $\mathcal{R}$ on $\mathcal{P}$ is a* branching bisimulation *if for all $P, Q \in \mathcal{P}$ such that $P \mathcal{R} Q$ 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* $Q \longrightarrow\!\!\!\!\!\rightarrow Q'' \xrightarrow{(\alpha)} Q'$ *and* $P \mathcal{R} Q''$ *and* $P' \mathcal{R} Q'$*.*

We write $P \leftrightarrows_b Q$ *if there exists a branching bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$*.*

The relation $\leftrightarrows_{\rm b}$ is an equivalence relation on $\mathcal{P}$ (this is not as trivial as one might expect; for a proof see [3]). It is also compatible with the construction of parallel composition in our syntax, which means that, for all $P_1, P_2, Q_1, Q_2 \in \mathcal{P}$:

$$P_1 \leftrightarrows_{\rm b} Q_1 \text{ and } P_2 \leftrightarrows_{\rm b} Q_2 \text{ implies } P_1 \parallel P_2 \leftrightarrows_{\rm b} Q_1 \parallel Q_2 \ . \tag{1}$$

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

Definition 2 (Weak bisimilarity [17]) *A symmetric binary relation* $\mathcal{R}$ *on* $\mathcal{P}$ *is a* weak bisimulation *if for all* $P, Q \in \mathcal{P}$ *such that* $P \mathcal{R} Q$ *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* $Q \longrightarrow\!\!\!\!\!\rightarrow Q'' \xrightarrow{(\alpha)} Q''' \longrightarrow\!\!\!\!\!\rightarrow Q'$ *and* $P' \mathcal{R} Q'$*.*

We write $P \leftrightarrows_w Q$ *if there exists a weak bisimulation* $\mathcal{R}$ *such that* $P \mathcal{R} Q$*.*

Like $\leftrightarrows_{\rm b}$, the relation $\leftrightarrows_{\rm w}$ is an equivalence relation on $\mathcal{P}$, and compatible with parallel composition. Note that $\leftrightarrows_{\rm b} \subseteq \leftrightarrows_{\rm w}$; 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.

Milner and Moller in [18] already observed that there exist infinite behaviours without a decomposition modulo strong bisimilarity; their example $a^*\mathbf{0}$ also does not have a decomposition modulo branching and weak bisimilarity. To exclude such examples of infinite behaviours with decompositions, we need to confine our attention to process expressions with terminating behaviour. (A formalisation of aforementioned notions pertaining to unique decomposition is postponed until the next section.)

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

Definition 3 *A process expression* P *is* totally normed *if there exist a natural number* $k \in \mathbf{N}$*, process expressions* $P_0, \ldots, P_k \in \mathcal{P}$ *and actions* $a_1, \ldots, a_k \in \mathcal{A}$

such that $P = P_0 \stackrel{a_1}{\longrightarrow\!\!\!\!\!\rightarrow} \cdots \stackrel{a_k}{\longrightarrow\!\!\!\!\!\rightarrow} P_k$ *and* $P_k{\downarrow}$. *The* weak norm $wn(P)$ *of a totally normed process expression* P *is defined by*

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

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

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

Example 4 *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 weak 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 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 $P \parallel P \leftrightarrows_b P \parallel Q$. *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 [9] to the effect that processes definable with a totally normed BPP specification have a unique decomposition modulo branching bisimilarity and weak bisimilarity.

Apparently, more severe restrictions are needed.

Definition 5 *Let* $k \in \mathbf{N}$; *a process expression* P *is* weakly bounded *by* k *if for all* $\ell \in \mathbf{N}$ *the existence of* $P_1, \ldots, P_\ell \in \mathcal{P}$ *and* $a_1, \ldots, a_\ell \in \mathcal{A}$ *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* weakly bounded *if* P *is bounded by* k *for some* $k \in \mathbf{N}$.

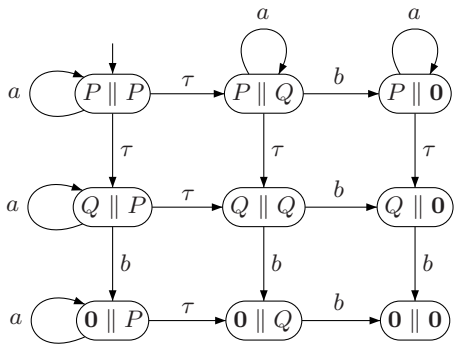

Fig. 1. Transition graph associated with $P \parallel P$.

Lemma 6 *Let P and Q be process expressions such that $P \leftrightarrows_w Q$. Then P is weakly bounded if, and only if, Q is weakly bounded.*

In the remainder of this paper we shall establish that weakly 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 [15]. We shall investigate whether the notion of decomposition order can be employed to prove unique parallel decomposition of weakly bounded process expressions modulo branching and weak bisimilarity.

Definition 7 *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 $\cdot$ 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.

Remark 8 *We adopt the convention that an expression designating an element of a partial commutative monoid M is defined only if all its subexpressions are defined. Furthermore, if t_1 and t_2 are expressions and $\mathcal{R}$ is a binary relation on M (e.g., equality or a partial order), then $t_1 \mathcal{R} t_2$ holds only if both t_1 and t_2 are defined and their values are related in $\mathcal{R}$. For a more succinct formulation we used in Definition 7 the symbol $\simeq$ introduced by Kleene [13]: if t_1 and t_2 are expressions designating elements of M, then $t_1 \simeq t_2$ means that either t_1 and t_2 are both defined and have the same value, or t_1 and t_2 are both undefined.*

We mention a key example of a commutative monoid that will serve to illustrate the theory of decomposition that we present in this paper.

Example 9 *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 $\wr x_1, \ldots, x_k \wr$ 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 $\leftrightarrows_{\mathrm{b}}$ and $\leftrightarrows_{\mathrm{w}}$ are equivalence relations on the set of process expressions. We denote the equivalence class of a process expression P modulo $\leftrightarrows_{\mathrm{b}}$ or $\leftrightarrows_{\mathrm{w}}$, respectively, by $[P]_b$ and $[P]_w$. Then, we define

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

In this paper, 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 ourselves 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 $\leftrightarrows_{\mathrm{b}}$ and $\leftrightarrows_{\mathrm{w}}$ are compatible with $\parallel$, we can define a binary operation $\parallel$ simultaneously on $\mathbf{B}$ and $\mathbf{W}$ simply by $[P] \parallel [Q] = [P \parallel Q]$, by which we then mean to define a binary operation $\parallel$ on $\mathbf{B}$ and a binary relation $\parallel$ on $\mathbf{W}$, respectively, by $[P]_b \parallel [Q]_b = [P \parallel Q]_b$ and $[P]_w \parallel [Q]_w = [P \parallel Q]_w$. Henceforth, we leave it to the reader to specialise notions, and also statements about these notions and their proofs, to $\mathbf{B}$ and $\mathbf{W}$ (or one of its submonoids to be introduced below).

We agree to write just $\mathbf{0}$ for $[\mathbf{0}]$. It is 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 10 $\mathbf{B}$ *and* $\mathbf{W}$ *are commutative monoids under* $\parallel$.

Note that, by Lemma 6, whenever an equivalence class $[P]$ contains a weakly bounded process expression, it consists entirely of weakly bounded process expressions. We define subsets $\mathbf{B}_{fin} \subseteq \mathbf{B}_{tn} \subseteq \mathbf{B}$ and $\mathbf{W}_{fin} \subseteq \mathbf{W}_{tn} \subseteq \mathbf{W}$ by

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

Corollary 11 *The sets $\mathbf{B}_{fin}$ and $\mathbf{B}_{tn}$ are commutative submonoids of $\mathbf{B}$, and the sets $\mathbf{W}_{fin}$ and $\mathbf{W}_{tn}$ are commutative submonoids of $\mathbf{W}$.*

Notation 12 *Let $x_1, \ldots, x_k$ be a (possibly empty) sequence of elements of a monoid M; we define its* generalised product *$x_1 \cdots x_k$ inductively as follows: (1) if $n = 0$, then $x_1 \cdots x_k \simeq e$, and (2) if $n > 0$, then $x_1 \cdots x_k \simeq (x_1 \cdots x_{k-1})x_k$. Occasionally, we shall write $\prod_{i=1}^{k} x_i$ instead of $x_1 \cdots x_k$. Furthermore, we write x^n for the k-fold composition of x, i.e., $x^k \simeq \prod_{i=1}^{k} x_i$ with $x_i = x$ for all $1 \leq i \leq k$.*

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 13 *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 14 *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 $\mathbf{B}_{fin}$, $\mathbf{B}_{tn}$, $\mathbf{B}$, $\mathbf{W}_{fin}$, $\mathbf{W}_{tn}$, 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 $\wr x_1, \ldots, x_k \int$ and $\wr y_1, \ldots, y_\ell \int$ are the equal iff the sequence $y_1, \ldots, y_\ell$ can be obtained from the sequence $x_1, \ldots, x_k$ by a permutation of its elements.

Definition 15 *Let M be a partial commutative monoid. A* decomposition *in M is a finite multiset $\wr p_1, \ldots, p_k \int$ 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 $\wr p_1, \ldots, p_k \int$, and, conversely, we say that $\wr p_1, \ldots, p_k \int$ is a decomposition of the element $p_1 \cdots p_k$ of M. Decompositions $d = \wr p_1, \ldots, p_k \int$ and $d' = \wr p'_1, \ldots, p'_\ell \int$ 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. If every element of M has a unique decomposition, then we say that M has unique decomposition.

Example 16 *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 paper, indeed coincides with the notion of unique parallel decomposition as discussed in the preceding section. We have already seen that the commutative monoids $\mathbf{B}_{tn}$, $\mathbf{B}$, $\mathbf{W}_{tn}$ and $\mathbf{W}$ do not have unique decomposition. Our goal in the remainder of this paper is to establish that the commutative monoids $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ 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 $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$, and hopefully also for other commutative monoids of processes. We shall now first recall the sufficient criterion put forward in [15], which was specifically designed for commutative monoids of processes. Then, we shall explain that it cannot directly be applied to conclude that $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ 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 17 *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 nonempty 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 $x, y \in M$*

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

In [15] 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 [15] 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 18 *If P and Q are process expressions such that $[Q] \preccurlyeq [P]$, then there exists $Q' \in [Q]$ such that $P \longrightarrow^* Q'$.*

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: it holds true of our process calculus only thanks to the very limited facility of defining infinite behaviour, by means of simple loops.

Lemma 19 *If $P_0, \ldots, P_i, \ldots$ $(i \in \mathbf{N})$ is an infinite sequence of process expressions, and $\alpha_0, \ldots, \alpha_i, \ldots$ $(i \in \mathbf{N})$ 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 $k, \ell \geq j$.*

Proposition 20 *$\preccurlyeq$ is a well-founded precompositional partial order on each of the commutative monoids $\mathbf{B}$, $\mathbf{B}_{tn}$, $\mathbf{B}_{fin}$, $\mathbf{W}$, $\mathbf{W}_{tn}$, and $\mathbf{W}_{fin}$.*

Note that if the iteration prefix in our process calculus is replaced by any of the familiar more general forms of iteration or recursion, then $\preccurlyeq$ as defined above will not be anti-symmetric, nor well-founded. Nevertheless, it is sometimes possible to define an anti-symmetric and 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 totally normed processes. (See, e.g., [15] for an example of an anti-symmetric and well-founded order on normed processes definable in ACP with recursion, which is based on the restriction of the transition relation.)

The ordering $\preccurlyeq$ defined on $\mathbf{B}_{tn}$, $\mathbf{B}$, $\mathbf{W}_{tn}$ 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 17, and on $\mathbf{B}_{tn}$ and $\mathbf{W}_{tn}$ it does not satisfy condition (iii) of Definition 17. (The latter is illustrated in Example 4.)

Proposition 21 *$\preccurlyeq$ on $\mathbf{B}_{tn}$, $\mathbf{B}_{fin}$, $\mathbf{W}_{tn}$ and $\mathbf{W}_{fin}$ is Archimedean and $\mathbf{0}$ is its least element.*

We should now still ask ourselves the question whether $\preccurlyeq$ on $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ is strictly compatible. An important step towards proving the property for, e.g., $\mathbf{B}_{fin}$ would be to establish, for all weakly bounded process expressions P, Q and R, the following implication: $P \xrightarrow{\tau} Q \ \&\ P \parallel R \leftrightarrows_{\mathrm{b}} Q \parallel R \Longrightarrow P \leftrightarrows_{\mathrm{b}} Q$. Example 4 illustrates that this implication does not hold for all totally 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., $P \parallel R \leftrightarrows_{\mathrm{b}} Q \parallel R$ implies $P \leftrightarrows_{\mathrm{b}} Q$), 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; it is 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 22 *$\preccurlyeq$ on $\mathbf{B}_{tn}$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}_{tn}$, 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 but not strictly compatible, we shall henceforth call a *weak* decomposition order.

Definition 23 *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 20, 21 and 22.

Corollary 24 *$\preccurlyeq$ on $\mathbf{B}_{tn}$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}_{tn}$, and $\mathbf{W}_{\mathit{fin}}$ is a weak decomposition order.*

In [15] 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 $\mathbf{B}_{tn}$ and $\mathbf{W}_{tn}$, and according to Example 4 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 [15] and the notion of weak decomposition order put forward here— is used both in the proof of *existence* of decompositions and in the proof that decompositions are *unique*. We shall now first establish the existence of decompositions in $\mathbf{B}_{tn}$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}_{tn}$, and $\mathbf{W}_{\mathit{fin}}$ separately. In the next section, we shall discuss uniqueness of decompositions in $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$. We shall propose a general subsidiary property that will allow us to establish uniqueness of decompositions in commutative monoids with a weak decomposition order, and establish that it holds in $\mathbf{B}_{\mathit{fin}}$ and $\mathbf{W}_{\mathit{fin}}$.

Proposition 25 *In the commutative monoids $\mathbf{B}_{tn}$, $\mathbf{B}_{\mathit{fin}}$, $\mathbf{W}_{tn}$, and $\mathbf{W}_{\mathit{fin}}$ every element has a 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 as an immediate consequence of the

result in [15]. Nevertheless, most of the ideas in the proof of uniqueness of decompositions in [15] can be adapted and reused in the context of commutative monoids endowed with a weak decomposition order, albeit with the technical details more involved. There is one special case in the unique decomposition proof that cannot be settled for commutative monoids with a weak decomposition order in general; this special case can be settled with an additional requirement on $\preccurlyeq$ that is satisfied both in $\mathbf{B}_{fin}$ and in $\mathbf{W}_{fin}$.

For the remainder of this paper, let M be a partial commutative monoid in which every element has a decomposition, and let $\preccurlyeq$ be a weak decomposition order on M.

The decomposition extension of $\preccurlyeq$ The uniqueness proof in [15] 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 strict 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 pairs of decompositions.

Let X be a set. If m and n are multisets over X, then we write $m - n$ for the multiset difference of m and n. 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 $p_1, \ldots, p_k \in M$, a sequence $x_1, \ldots, x_k \in M$, and a sequence of decompositions $d_1, \ldots, d_k$ 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) $d = (d' - \lbag p_1, \ldots, p_k \rbag) \uplus (d_1 \uplus \cdots \uplus d_k)$.

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

Lemma 26 *The partial order $\trianglelefteq$ on decompositions is well-founded.*

In our uniqueness proof, we shall use the well-foundedness of both $\preccurlyeq$ and the Cartesian order $\trianglelefteq_\times$ induced on pairs of decompositions by $\trianglelefteq$. For two pairs of decompositions (d_1, d_2) and (d_1', d_2'), we write $(d_1, d_2) \trianglelefteq_\times (d_1', d_2')$ if $d_1 \trianglelefteq d_1'$ and $d_2 \trianglelefteq d_2'$. 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 $\trianglelefteq_\times$. If

unique decomposition would fail then there would exist a minimal counterexample. For the subset of processes with two or more decompositions is nonempty, and therefore, by well-foundedness of $\preccurlyeq$, it has a $\preccurlyeq$-minimal element, say x. Then, by well-foundedness of $\trianglelefteq_\times$ on pairs of decompositions, the nonempty set of pairs of distinct decompositions with x as their composition has a minimal element, say (d_1, d_2).

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 nonempty. 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 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 [15]; the only important difference is the use of the ordering $\trianglelefteq$ instead of $\preccurlyeq$.

Case 2: d_1 and d_2 are too close together In [15] 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 $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ 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 27 *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 $x, y \in M$, for every indecomposable $p \in M$ such that $p \not\preccurlyeq x, y$, and for all $k \in \mathbf{N}$ it holds that $p^k x = p^k y$, then $x = y$.*

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, $p \not\preccurlyeq p$ and, since d_2' consists of indecomposables q such that $p \not\preccurlyeq q$, it follows that also $p \not\preccurlyeq x$. Hence, since $\preccurlyeq$ has power cancellation, $p = x$, so $d_2' = \lceil p \rfloor$. It follows that $d_1 = d_2$, which contradicts that (d_1, d_2) is a counterexample against unique decomposition.

Theorem 28 *Let M be a commutative monoid with a weak decomposition order that satisfies power cancellation. If every element of M has a decomposition, then M has unique decomposition.*

In the previous section we have already established that in the commutative monoids $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ every element has a decomposition and that $\preccurlyeq$ is a weak decomposition order on $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$. To be able to conclude from Theorem 28 that $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ have unique decomposition, it remains to establish that $\preccurlyeq$ on these commutative monoids satisfies power cancellation.

Proposition 29 *$\preccurlyeq$ on $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ satisfies power cancellation.*

By Corollary 24 and Propositions 25 and 29, the commutative monoids $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ are endowed with a weak decomposition order $\preccurlyeq$ satisfying power cancellation, and, moreover, all elements of $\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ have at least one decomposition. Hence, by Theorem 28, we obtain the following corollary.

Corollary 30 *$\mathbf{B}_{fin}$ and $\mathbf{W}_{fin}$ have unique decomposition.*

5 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 composition. 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 [15], 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 report [7], in which unique parallel decomposition is established for a fragment of Applied π-calculus, will serve as a starting point.

In [2], 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.

References

1. 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.
2. 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.
3. T. Basten. Branching bisimilarity is an equivalence indeed! *Information Processing Letters*, 58(3):141–147, 1996.
4. I. Castellani and M. Hennessy. Distributed bisimulations. *J. ACM*, 36(4):887–911, 1989.
5. S. Christensen. *Decidability and Decomposition in Process Algebras.* PhD thesis, University of Edinburgh, 1993.
6. F. Corradini, R. Gorrieri, and D. Marchignoli. Towards parallelization of concurrent systems. *RAIRO Inform. Théor. Appl.*, 32(4-6):99–125, 1998.
7. J. Dreier, C. Ene, P. Lafourcade, and Y. Lakhnech. On unique decomposition of processes in the applied π-calculus. Technical Report TR-2012-3, Verimag Research Report, 2011.
8. W. J. Fokkink and B. Luttik. An *omega*-complete equational specification of interleaving. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *ICALP*, volume 1853 of *LNCS*, pages 729–743. Springer, 2000.
9. S. Fröschle and S. Lasota. Normed processes, unique decomposition, and complexity of bisimulation equivalences. *ENTCS*, 239:17–42, 2009.
10. R. J. van Glabbeek and W. P. Weijland. Branching time and abstraction in bisimulation semantics. *J. ACM*, 43(3):555–600, 1996.
11. J. F. Groote and F. Moller. Verification of parallel systems via decomposition. In R. Cleaveland, editor, *CONCUR*, volume 630 of *LNCS*, pages 62–76. Springer, 1992.
12. Y. Hirshfeld and M. Jerrum. Bisimulation equivalence is decidable for normed process algebra. In J. Wiedermann, P. van Emde Boas, and M. Nielsen, editors, *ICALP*, volume 1644 of *LNCS*, pages 412–421. Springer, 1999.
13. S. C. Kleene. *Introduction to Metamathematics.* D. Van Nostrand Co., Inc., New York, N. Y., 1952.
14. B. Luttik. Unique parallel decomposition in branching and weak bisimulation semantics. *CoRR*, abs/1205.2117, 2012.
15. 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.
16. R. Milner. *Communication and Concurrency.* Prentice-Hall International, 1989.
17. 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.
18. R. Milner and F. Moller. Unique decomposition of processes. *Theoret. Comput. Sci.*, 107:357–363, January 1993.
19. F. Moller. *Axioms for Concurrency.* PhD thesis, University of Edinburgh, 1989.
20. F. Moller. The importance of the left merge operator in process algebras. In Mike Paterson, editor, *ICALP*, volume 443 of *LNCS*, pages 752–764. Springer, 1990.
21. F. Moller. The nonexistence of finite axiomatisations for CCS congruences. In *Proceedings of LICS'90*, pages 142–153. IEEE Computer Society Press, 1990.