**REPORT**_RAPPORT_

# SEN

Software Engineering

*Software ENgineering*

Decomposition Orders - another generalisation of the
fundamental theorem of arithmetic

S.P. Luttik, V. van Oostrom

# Decomposition Orders - another generalisation of the fundamental theorem of arithmetic

ABSTRACT

We discuss unique decomposition in partial commutative monoids. Inspired by a result from process theory, we propose the notion of decomposition order for partial commutative monoids, and prove that a partial commutative monoid has unique decomposition iff it can be endowed with a decomposition order. We apply our result to establish that the commutative monoid of weakly normed processes modulo bisimulation definable in ACP$^\varepsilon$ with linear communication, with parallel composition as binary operation, has unique decomposition. We also apply our result to establish that the partial commutative monoid associated with a well-founded commutative residual algebra has unique decomposition.

# Decomposition Orders
## another generalisation of the fundamental theorem of arithmetic

Bas Luttik[1,2]     Vincent van Oostrom[3]

*luttik@win.tue.nl      oostrom@phil.uu.nl*

[1]*Dept. of Math. and Comput. Sci., Eindhoven University of Technology,*

*P.O. Box 513, NL-5600 MB Eindhoven, The Netherlands*

[2]*CWI, P.O. Box 94079, NL-1090 GB Amsterdam, The Netherlands*

[3]*Dept. of Philosophy, Utrecht University,*

*Heidelberglaan 8, NL-3584 CS Utrecht, The Netherlands*

### Abstract

We discuss unique decomposition in partial commutative monoids. Inspired by a result from process theory, we propose the notion of *decomposition order* for partial commutative monoids, and prove that a partial commutative monoid has unique decomposition iff it can be endowed with a decomposition order. We apply our result to establish that the commutative monoid of weakly normed processes modulo bisimulation definable in $\mathsf{ACP}^\varepsilon$ with linear communication, with parallel composition as binary operation, has unique decomposition. We also apply our result to establish that the partial commutative monoid associated with a well-founded commutative residual algebra has unique decomposition.

## 1   Introduction

The fundamental theorem of arithmetic states that every positive natural number can be expressed as a product of prime numbers uniquely determined up to the order of the factors. Analogues of the fundamental theorem of arithmetic make sense for arbitrary *commutative monoids*, i.e., sets endowed with an associative and commutative multiplication for which the set contains an identity element. Call an element of a commutative monoid *indecomposable* if it is not the product of two elements that are both not the identity. A commutative monoid has *unique decomposition* if every element can be expressed as a product of indecomposable elements uniquely determined up to the order of the factors, i.e., if an analogue of the fundamental theorem of arithmetic holds in it.

From the proof of the fundamental theorem of arithmetic (see, e.g., Hardy and Wright's book [15]), a necessary and sufficient criterion can be inferred that characterises the class of commutative monoids with unique decomposition: a commutative monoid has unique decomposition iff it satisfies the following three conditions:

1. it has *cancellation* (i.e., $xy = xz$ implies $y = z$);

2. its divisibility relation | is *well-founded*; and

3. its indecomposable elements are *prime* with respect to divisibility (i.e., if $p$ is indecomposable and $p \mid xy$, then $p \mid x$ or $p \mid y$).

Hence, to prove that a commutative monoid has unique decomposition, it suffices to prove that it satisfies the above three conditions.

However, these conditions are not always easy to work with. The motivating examples for this paper are the commutative monoids of processes, with parallel composition as binary operation, that arise in process theory. For some of these commutative monoids, a unique decomposition result has been proved, but it is not known how to establish cancellation except as a *consequence* of unique decomposition. Also, proofs of unique decomposition results in process theory employ the order induced on processes by their operational semantics, rather than divisibility. Our main contribution is to provide another necessary and sufficient criterion for unique decomposition, inspired by unique decomposition results in process theory.

## 1.1 Process theory

In process theory, unique decomposition results are crucial, e.g., in the proofs that bisimulation is decidable for normed BPP [7] and normed PA [16]. They have also proved to be a useful tool in the analysis of axiom systems involving an operation for parallel composition [1, 11, 23]. Furthermore, inspired by unique decomposition results, a verification method for concurrent processes based on decomposition was proposed in [14], and a notion of parallelisation of concurrent processes was proposed in [8].

The first unique decomposition theorem in process theory, to the effect that the commutative monoid of finite processes definable in BCCS modulo bisimulation can be written as the parallel composition of parallel prime processes, was established by Milner and Moller [21]. The parallel operator they consider implements a simple form of interleaving, without communication between components. Their elegant proof still proceeds via a cancellation lemma; that processes are finite and interleaving is without communication seems to be essential in the proof of this lemma.

In [22], Moller presents an alternative proof of the result in [21], which he attributes to Milner; we shall henceforth refer to it as *Milner's technique.* A remarkable feature of Milner's technique is that it does not rely on cancellation. Moller explains that the reason for presenting Milner's technique is that it serves "as a model for the proof of the same result in more complicated languages which evade the simpler proof method" of [21]. He refines Milner's technique twice. First, he adds communication to the operational semantics of the parallel operator. Then, he turns to weak bisimulation semantics. Christensen [6] shows how Milner's technique can be further refined so that also certain infinite processes can be dealt with. He proves unique decomposition theorems for the commutative monoids of weakly normed BPP and of weakly normed $BPP_\tau$ expressions modulo (strong) bisimulation.

## 1.2 Decomposition order

Milner's technique hinges on some special properties of the operational semantics of parallel composition. In [18], the first author already placed these properties in the general algebraic context of commutative monoids, proving that they entail a unique decomposition theorem. In this paper we further improve and extend this result. Our main contribution is the notion of *decomposition order* on partial commutative monoids (multiplication is allowed to be a partial operation). We prove that the existence of such a decomposition order is a necessary and sufficient condition for a partial commutative monoid to have unique decomposition, and thus, we obtain an abstract algebraic characterisation of the class of partial commutative monoids with unique decomposition.

By our result, to prove that a partial commutative monoid has unique decomposition, it suffices to define a decomposition order on it. Frequently, this will be the decomposition

order naturally associated with the operation of the monoid, i.e., its divisibility relation. In fact, we shall prove that if a commutative monoid has unique decomposition, then its divisibility relation always is a decomposition order. However, part of the strength of our result is that it offers the flexibility to proceed via *another* decomposition order than the divisibility relation. For instance, Milner's technique for proving unique decomposition results in process theory is based on an order induced on processes by their operational semantics, which is *not* the divisibility relation associated with parallel composition. An interesting aspect of this order is that parallel prime processes need not be incomparable (cf. Remark 4.23), whereas with respect to the divisibility relation they always are.

## 1.3 Overview

In Section 2 we introduce partial commutative monoids, we define when a partial commutative monoid has unique decomposition, and we discuss a straightforward generalisation of the proof of the fundamental theorem of arithmetic as it appears, e.g., in [15] to partial commutative monoids. The section is meant to introduce our notations and illustrate the idea of generalising a concrete proof to an abstract algebraic setting. It also serves to put our alternative generalisation into context. Since our notations are fairly standard, readers with some knowledge of abstract algebra can skip this section.

In Section 3 we propose and study the notion of decomposition order, and we prove our main results:

1. a partial commutative monoid has unique decomposition iff it can be endowed with a decomposition order;

2. divisibility in a partial commutative monoid with unique decomposition is always a decomposition order; and

3. for divisibility in a partial commutative monoid to be a decomposition order it is enough that it satisfies only three of the five conditions;

4. in general the five conditions of a decomposition order are independent and they are all necessary for unique decomposition.

In Section 4 we illustrate how our result can be applied to obtain a unique decomposition result in the realm of the process theory $\mathsf{ACP}^\varepsilon$ [27]. Two features of $\mathsf{ACP}^\varepsilon$ make the extension of Milner's technique to $\mathsf{ACP}^\varepsilon$ a nontrivial exercise. Firstly, $\mathsf{ACP}^\varepsilon$ distinguishes successful and unsuccessful termination, and secondly, $\mathsf{ACP}^\varepsilon$ has a very general communication mechanism (an arbitrary number of parallel components may participate in a single communication, and communication does not necessarily result in $\tau$). We shall see that both features lead to counterexamples obstructing a general unique decomposition result (see Examples 4.4 and 4.8). To bar them, we introduce for $\mathsf{ACP}^\varepsilon$ an appropriate notion of weak normedness that takes into account the distinction between successful and unsuccessful termination, and we propose a mild restriction on the communication mechanism. If the communication mechanism satisfies the restriction, then the operational semantics of $\mathsf{ACP}^\varepsilon$ induces a decomposition order on the commutative monoid of weakly normed $\mathsf{ACP}^\varepsilon$ expressions modulo bisimulation, which then, by the result of Section 3, has unique decomposition.

In Section 5 we apply our result to obtain a representation theorem for the class of well-founded *commutative residual algebras* [24]. The theorem is obtained by showing that the partial commutative monoid naturally associated with a well-founded commutative residual algebra has unique decomposition. The operation of the associated monoid being partial in general was our motivation to generalise our unique decomposition theorem to the partial case as well.

# 2 Unique decomposition via divisibility

In this section we introduce the notion of partial commutative monoid, and we define the notion of decomposition of an element in a partial commutative monoid. We then proceed with presenting a straightforward generalisation of the proof of the fundamental theorem of arithmetic to a class of partial commutative monoids that is defined by three abstract conditions. The first abstract condition is the well-known cancellation law. The second abstract condition states that the divisibility relation associated with a partial commutative monoid is well-founded. The third abstract condition is an abstract formulation of Euclid's first theorem, which states that a prime number dividing a product divides one of the factors. That the proof of the fundamental theorem of arithmetic generalises to partial commutative monoids satisfying these three abstract conditions, shows that the conditions are sufficient for the partial commutative monoid to have unique decomposition. We shall also prove that they are necessary.

## 2.1 Partial commutative monoids

**Definition 2.1** A *partial commutative monoid* is a set $M$ with a distinguished element $e$ and a partial binary operation on $M$ such that for all $x, y, z \in M$:

$$x(yz) \simeq (xy)z \qquad \text{(associativity)};$$
$$xy \simeq yx \qquad \text{(commutativity)};$$
$$xe \simeq ex \simeq x \qquad \text{(identity)}.$$

(The meaning of the symbol $\simeq$ is explained in Remark 2.2 below.)

**Remark 2.2** 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. Thus, $x(yz)$ is defined only if $yz$ is defined, say $yz = u$, and moreover $xu$ is 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 instance, $x(yz) = (xy)z$ is true if the expressions $x(yz)$ and $(xy)z$ are both defined and their values are equal; otherwise it is false.

Note that the commutative law for a partial commutative monoid $M$ could have been formulated thus: for all $x, y \in M$, $xy$ is defined iff $yx$ is defined, and if both $xy$ and $yx$ are defined then $xy = yx$. For a more succinct formulation we used in Definition 2.1 the symbol $\simeq$ introduced by Kleene [17]: 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 few examples of partial commutative monoids that will serve to illustrate the theory of decomposition that we present in this paper.

**Example 2.3**    1. It is well-known that the set of natural numbers $\mathbf{N}$ is a commutative monoid[1] under addition. Each initial segment $\{0, \ldots, n\}$ of $\mathbf{N}$ is a partial commutative monoid with as partial binary operation the restriction of addition to $\{0, \ldots, n\}$. So addition in the partial commutative monoid $\{0, \ldots, n\}$ is defined for $k, l \in \{0, \ldots, n\}$ iff $k + l \leq n$.

2. The set of positive natural numbers $\mathbf{N}_{>0}$ is a commutative monoid under multiplication.

---

[1]When the binary operation is everywhere defined, the adjective 'partial' is of course dropped.

3. 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* $\square$ is the multiset that satisfies $\square(x) = 0$ for all $x \in X$. With these definitions, $\mathcal{M}(X)$ is a commutative monoid. If $x_1, \ldots, x_n$ is a sequence of elements of $X$, then $[x_1, \ldots, x_n]$ denotes the multiset $m$ such that $m(x)$ is the number of occurrences of $x$ in $x_1, \ldots, x_n$.

**Notation 2.4** Let $x_1, \ldots, x_n$ be a (possibly empty) sequence of elements of a monoid $M$; we define its *generalised product* $x_1 \cdots x_n$ inductively as follows:

(i) if $n = 0$, then $x_1 \cdots x_n \simeq e$, and

(ii) if $n > 0$, then $x_1 \cdots x_n \simeq (x_1 \cdots x_{n-1})x_n$.

Occasionally, we shall write $\prod_{i=1}^{n} x_i$ instead of $x_1 \cdots x_n$. Furthermore, we write $x^n$ for the $n$-fold composition of $x$, i.e.,

$$x^n \simeq \prod_{i=1}^{n} x_i \text{ with } x_i = x \text{ for all } 1 \leq i \leq n.$$

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

$$(x_1 \cdots x_k)(y_1 \cdots y_l) \simeq x_1 \cdots x_k y_1 \cdots y_l \ .$$

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

$$\text{if } i_1, \ldots, i_n \text{ is any permutation of } 1, \ldots, n, \text{ then } x_1 \cdots x_n \simeq x_{i_1} \cdots x_{i_n} \ .$$

## 2.2 Indecomposables and decompositions

An indecomposable element of a partial 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 2.5** An element $p$ of a partial commutative monoid $M$ is called *indecomposable* if $p \neq e$ and $p = xy$ implies $x = e$ or $y = e$.

**Example 2.6** 1. The number 1 is the only indecomposable element in $\mathbf{N}$ and all its non-trivial initial segments; the trivial initial segment $\{0\}$ has no indecomposable elements.

2. The prime numbers are the indecomposable elements of $\mathbf{N}_{>0}$.

3. The indecomposable elements of $\mathcal{M}(X)$ are the *singleton* multisets, i.e., the multisets $m$ for which it holds that $\sum_{x \in X} m(x) = 1$.

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 $[x_1, \ldots, x_k]$ and $[y_1, \ldots, y_l]$ are the same (extensionally) iff the sequence $y_1, \ldots, y_l$ can be obtained from the sequence $x_1, \ldots, x_k$ by a permutation of its elements.

**Definition 2.7** Let $x$ be an element of a partial commutative monoid $M$. A *decomposition* of $x$ in $M$ is a finite multiset $[p_1, \ldots, p_n]$ of indecomposable elements of $M$ such that $x = p_1 \cdots p_n$. If $x$ has a unique decomposition (up to multiset equivalence), then we shall denote it by $\partial x$. If every element of $M$ has a unique decomposition, then we say that $M$ has *unique decomposition*.

**Example 2.8**   1. Since 1 is the only indecomposable element of $\mathbf{N}$ and of any of its nontrivial initial segments, a decomposition in these partial commutative monoids is a multiset over the singleton set $\{1\}$. There is exactly one way in which a natural number $n$ can be written as a sum of 1s, so decompositions in $\mathbf{N}$ and its initial segments are unique.

2. According to the fundamental theorem of arithmetic every positive natural number has a unique decomposition in $\mathbf{N}_{>0}$.

3. 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 $[x]$.

Let $M$ be a partial commutative monoid, let $P$ be its set of indecomposable elements, and suppose that $M$ has unique decomposition. Then $\partial M$, the image of $M$ under the mapping $\partial : M \to \mathcal{M}(P)$ that associates with every element of $M$ its unique decomposition, is a division-closed isomorphic copy of $M$ within $\mathcal{M}(P)$, as formalised by the following definition and proposition.

**Definition 2.9** Let $M$ be a partial commutative monoid. The *divisibility* relation $\mid$ associated with $M$ is defined by

$x \mid y$ iff there exists $y'$ such that $xy' = y$ .

A subset $M'$ of $M$ is *division-closed* if for all $x, y \in M$:

if $x \mid y$ and $y \in M'$, then $x \in M'$ .

**Example 2.10**   1. The divisibility relation of $\mathbf{N}$ coincides with the usual less-than-or-equal relation $\leq$. The restriction of $\leq$ to the set $\{0, \ldots, n\}$ is the divisibility relation of the initial segment $\{0, \ldots, n\}$ of $\mathbf{N}$. Also note that each initial segment is a division-closed subset of $\mathbf{N}$.

2. The divisibility relation of $\mathbf{N}_{>0}$ is the usual divisibility relation on numbers.

3. The divisibility relation of $\mathcal{M}(X)$ coincides with the *submultiset relation* $\sqsubseteq$, defined by

$m \sqsubseteq m'$ iff $m(x) \leq m'(x)$ for all $x \in X$.

**Proposition 2.11** Let $M$ be a partial commutative monoid with unique decomposition, let $P$ be its set of indecomposable elements, and let $\partial : M \to \mathcal{M}(P)$ be the mapping that associates with every element of $M$ its unique decomposition. Then

(i) $\partial$ is injective;

(ii) $\partial$ preserves multiplication in the sense that for all $x, y, z \in M$:

$xy = z$ iff $\partial x \uplus \partial y = \partial z$ ;

(iii) $\partial$ preserves the identity in the sense that for all $x \in M$:

$$x = e \text{ iff } \partial x = \square \ ;$$

(iv) the image $\partial M$ of $M$ under $\partial$ is a division-closed subset of $\mathcal{M}(P)$, i.e., for all $x \in M$ and $m \in \mathcal{M}(P)$:

$$\text{if } m \sqsubseteq \partial x, \text{ then there exists } x' \in M \text{ such that } \partial x' = m \ ; \text{ and}$$

(v) $\partial$ preserves divisibility in the sense that for all $x, y, z \in M$:

$$x \mid y \text{ iff } \partial x \sqsubseteq \partial y \ .$$

*Proof.*

(i) Suppose that $\partial x = \partial y$. Let $\partial x = [p_1, \ldots, p_k]$ and let $\partial y = [q_1, \ldots, q_l]$. Then $[p_1, \ldots, p_k] = \partial x = \partial y = [q_1, \ldots, q_l]$, so the sequence $q_1, \ldots, q_l$ can be obtained from the sequence $p_1, \ldots, p_k$ by a permutation. Moreover, $x = p_1 \cdots p_k$ and $y = q_1 \cdots q_l$, so by the generalised commutative law

$$x = p_1 \cdots p_k = q_1 \cdots q_l = y \ .$$

It follows that $\partial$ is injective.

(ii) Let $x, y, z \in M$, let $\partial x = [p_1, \ldots, p_k]$ and let $\partial y = [q_1, \ldots, q_l]$.

If $xy = z$, then by the generalised associative law

$$z = xy = (p_1 \cdots p_k)(q_1 \cdots q_l) = p_1 \cdots p_k q_1 \cdots q_l \ ,$$

so $[p_1, \ldots, p_k, q_1, \ldots, q_l]$ is the unique decomposition of $z$, and hence

$$\partial z = [p_1, \ldots, p_k, q_1, \ldots, q_l] = [p_1, \ldots, p_k] \uplus [q_1, \ldots, q_l] = \partial x \uplus \partial y \ .$$

On the other hand, if $\partial x \uplus \partial y = \partial z$, then

$$\partial z = [p_1, \ldots, p_k, q_1, \ldots, q_l] \ ,$$

so by the generalised associative law

$$z = p_1 \cdots p_k q_1 \cdots q_l = (p_1 \cdots p_k)(q_1 \cdots q_l) = xy \ .$$

It follows that $\partial$ preserves multiplication.

(iii) If $x = e$, then according to the identity law $xx = x$, so by (ii) $\partial x$ is an element of $\mathcal{M}(P)$ that satisfies $\partial x \uplus \partial x = \partial x$; clearly, the empty multiset $\square$ is the only element of $\mathcal{M}(P)$ with this property. On the other hand, if $x \neq e$, then by (i) $\partial x \neq \partial e$, so $\partial x \neq \square$. It follows that $\partial$ preserves the identity.

(iv) Let $x \in M$, say with unique decomposition $\partial x = [p_1, \ldots, p_n]$, and let $m \in \mathcal{M}(P)$; we need to prove that $m \sqsubseteq \partial x$ implies the existence of an element $x' \in M$ such that $\partial x' = m$. Suppose that $m \sqsubseteq \partial x$; then without loss of generality we may assume that $m = [p_1, \ldots, p_k]$ $(0 \le k \le n)$. If $k = n$, then $m = \partial x$, so the implication holds with $x' = x$. Otherwise, since $p_1 \cdots p_n$ is defined, it follows by the generalised associative law that $(p_1 \cdots p_k)(p_{k+1} \cdots p_n)$ is defined, and hence that $p_1 \cdots p_k$ is defined, so the implication holds with $x' = p_1 \cdots p_k$. It follows that $\partial M$ is a division-closed subset of $\mathcal{M}(P)$.

(v) Recall that $\sqsubseteq$ is the divisibility relation of $\mathcal{M}(P)$. Hence, that $x \mid y$ implies $\partial x \sqsubseteq \partial y$ for all $x, y \in M$ is a straightforward consequence of (ii), and the converse is a straightforward consequence of (ii) and (iv). It follows that $\partial$ preserves divisibility. $\square$

**Remark 2.12** It follows from Proposition 2.11 that if $M$ has unique decomposition, then the $\partial M$, with multiset sum restricted to it, is an isomorphic copy of $M$ within $\mathcal{M}(P)$, i.e., the mapping $\partial$ is an *embedding* (cf. [13, Chapter 2]).

## 2.3   The proof of the fundamental theorem of arithmetic

We proceed with presenting three abstract conditions on partial commutative monoids that facilitate an abstract version of the proof of the fundamental theorem of arithmetic (see, e.g., [15]). The first condition is directly expressible as a property of multiplication.

**Definition 2.13** A partial commutative monoid $M$ has *cancellation* if for all $x, y, z \in M$:

$$xy = xz \text{ implies } y = z \ .$$

Consider a partial commutative monoid $M$ with cancellation; we now derive a sufficient condition on $M$ that ensures that every element of $M$ has a decomposition. First note that the identity element $e$ of $M$ has the empty multiset as a decomposition, and that every indecomposable element $p$ of $M$ has the singleton multiset $[p]$ as decomposition. If $x \in M$ is not the identity element, nor indecomposable, then there exist $y, z \in M$, both not the identity, such that $x = yz$. If $y$ and $z$ both have decompositions, then $x$ has a decomposition too, viz. the multiset sum of the decompositions of $y$ and $z$. So, if $x$ has no decomposition, then we can assume without loss of generality that $y$ has no decomposition. From $z \neq e$ it then follows by cancellation that $x \neq y$; for if $x = y$, then $xz = yz = x = xe$, so by cancellation $z = e$. It has now been established that if $M$ is a partial commutative monoid with cancellation and $x$ is an element of $M$ without a decomposition, then there exists another element $y$ in $M$, also without a decomposition, that properly divides $x$, i.e., such that $y \mid x$ and $y \neq x$.

An element $x$ is called a $\mid$-*minimal* element of a subset $M'$ of $M$ if $x \in M'$ and, for all $y \in M'$, $y \mid x$ implies $y = x$. From what have just seen it follows that the subset of all elements of $M$ without a decomposition cannot have a $\mid$-minimal element. Therefore, to ensure that in a partial commutative monoid $M$ with cancellation every element has a decomposition, it suffices to require that its divisibility relation is *well-founded*, i.e., that every nonempty subset of $M$ has a $\mid$-minimal element. The following lemma is a direct consequence of the preceding observations.

**Lemma 2.14** If $M$ is a partial commutative monoid with cancellation and a well-founded divisibility relation, then every element of $M$ has a decomposition.

It easily follows from the definition of divisibility that it is reflexive and transitive, and hence a quasi-order. A well-founded divisibility relation is, moreover, antisymmetric, and consequently a partial order, with the identity as its least element.

**Lemma 2.15** If the divisibility relation of a partial commutative monoid is well-founded, then it is a partial order with the identity as its least element.

*Proof.*    Let $M$ be a partial commutative monoid and let $\mid$ be its divisibility relation. Any well-founded relation, and *a fortiori* a well-founded divisibility relation of a partial commutative monoid, is antisymmetric; for, if $x \mid y$ and $y \mid x$, then the set $\{x, y\}$ has no minimal element unless $x = y$. Since $\mid$ is also reflexive and transitive, it is a partial order.

To see that the identity $e$ of $M$ is the least element of $M$ with respect to $\mid$, note that $e \mid x$ by the identity law for partial commutative monoids, so if $x \mid e$, then $x = e$ by antisymmetry. $\qquad\square$

Our last requirement is to ensure that decompositions in a partial commutative monoid with cancellation and a well-founded divisibility relation are unique. Call an element $p$ of a partial commutative monoid $M$ *prime* with respect to $\mid$ if for all $x, y \in M$:

$$p \mid xy \text{ implies } p \mid x \text{ or } p \mid y \ .$$

**Lemma 2.16** Let $M$ be a partial commutative monoid and let $p, p_1, \ldots, p_n$ be indecomposable elements of $M$. If $p$ is prime with respect to divisibility in $M$, then $p \mid p_1 \cdots p_n$ implies $p = p_i$ for some $1 \leq i \leq n$.

*Proof.* We proceed by induction on $n$.

If $n = 0$, then $p_1 \cdots p_n = e$. Since $p \nmid e$, the implication of the lemma vacuously holds in this case.

Suppose $n > 0$ and $p \mid p_1 \cdots p_n$. Then, since $p$ is prime with respect to divisibility, $p \mid p_1 \cdots p_{n-1}$ or $p \mid p_n$. In the first case the lemma is immediate by the induction hypothesis. For the second case note that according to the definition of divisibility there exists an element $x$ such that $px = p_n$. Since $p_n$ is indecomposable it follows that $x = e$, and hence $p = p_n$ as required by the statement of the lemma. $\square$

We are now in a position to prove that the three abstract conditions on partial commutative monoids just introduced ensure uniqueness of decompositions.

**Theorem 2.17** Let $M$ be a partial commutative monoid and suppose that

(i) $M$ has cancellation;

(ii) divisibility in $M$ is well-founded; and

(iii) every indecomposable element is prime with respect to divisibility in $M$.

Then $M$ has unique decomposition.

*Proof.* By Lemma 2.14 every element of $M$ has a decomposition. For uniqueness consider an element $a$ of $M$ and sequences of indecomposable elements $p_1, \ldots, p_k$ and $q_1, \ldots, q_l$ such that

$$a = p_1 \cdots p_k = q_1 \cdots q_l \ .$$

We show by induction on $k$ that $[p_1, \ldots, p_k] = [q_1, \ldots, q_l]$.

If $k = 0$, then the multiset $[p_1, \ldots, p_k]$ is empty, so we need to show that $[q_1, \ldots, q_l]$ is empty too. Note that from $a = p_1 \cdots p_k$ it follows that $a$ is the identity, so by Lemma 2.15 $a$ is the least element with respect to divisibility, i.e., it has no proper divisors. On the other hand, from $a = q_1 \cdots q_l$ it follows by the generalised associative and commutative laws that every element of $[q_1, \ldots, q_l]$ divides $a$. Since elements of $[q_1, \ldots, q_l]$ are by assumption indecomposable, whence not the identity, it follows that $[q_1, \ldots, q_l]$ indeed contains no elements.

Suppose that $k > 0$. Then by the generalised associative and commutative laws $p_k \mid a$ and since $a = q_1 \cdots q_l$, it follows by Lemma 2.16 that $p_k = q_i$ for some $1 \leq i \leq n$. By cancellation

$$p_1 \cdots p_{k-1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_l \ ,$$

so by the induction hypothesis $[p_1, \ldots, p_{k-1}] = [q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_l]$. It now follows that $[p_1, \ldots, p_k] = [q_1, \ldots, q_l]$, so the proof of the theorem is complete. $\square$

To establish that a partial commutative monoid has unique decomposition it now suffices to establish the conditions of the preceding theorem. This is illustrated in the next example.

**Example 2.18** 1. It is straightforward to show that the commutative monoid $\mathbf{N}$ and each of its initial segments satisfy the conditions of Theorem 2.17, and hence have unique decomposition.

2. To get the fundamental theorem of arithmetic as a corollary to Theorem 2.17, we prove that the commutative monoid of positive natural numbers $\mathbf{N}_{>0}$ with multiplication satisfies the three conditions of the theorem. To see that $\mathbf{N}_{>0}$ has cancellation, suppose that $km = kn$ for some positive natural number $k$. Then $k(m - n) = 0$, so $m - n = 0$ and hence $m = n$. To see that divisibility is well-founded, note that if $k \mid l$ then $k \leq l$. To see that every indecomposable positive natural number $k$ is prime, suppose $k \mid mn$. If $k \mid m$ then we are done. Otherwise, the greatest common divisor of $k$ and $m$ is 1, so there exist integers $x$ and $y$ such that

$$1 = xk + ym \ .$$

Then $n = nxk + ymn$ and since $k \mid mn$ it follows that $k \mid n$.

3. That, for any set $X$, the commutative monoid $\mathcal{M}(X)$ of all multisets over $X$ satisfies the three conditions of Theorem 2.17 is a straightforward consequence from the fact that $\mathbf{N}$ satisfies them.

That $\mathcal{M}(P)$ satisfies the conditions of Theorem 2.17 (cf. Example 2.18) can now be used to show that they are not only sufficient, but also necessary.

**Corollary 2.19** A partial commutative monoid $M$ has unique decomposition iff the following three conditions hold:

(i) $M$ has cancellation;

(ii) divisibility in $M$ is well-founded; and

(iii) every indecomposable element is prime with respect to divisibility in $M$.

*Proof.* The implication from right to left has already been proved as Theorem 2.17; it remains to prove the implication from left to right. Let $P$ be the set of indecomposable elements of $M$. According to Example 2.18, the partial commutative monoid $\mathcal{M}(P)$ satisfies the conditions in the statement of the corollary; we use the properties of the mapping $\partial : M \to \mathcal{M}(P)$ properties established in Proposition 2.11 to show that $M$ then also satisfies them.

If $xy = xz$, then $\partial x \uplus \partial y = \partial(xy) = \partial(xz) = \partial x \uplus \partial z$. Since $\mathcal{M}(P)$ has cancellation, it follows that $\partial y = \partial z$, and hence $y = z$. So $M$ has cancellation.

To prove that $\mid$ is well-founded, consider a nonempty subset $M'$ of $M$; we need to show that $M'$ has a $\mid$-minimal element. Since $\sqsubseteq$ is well-founded, the image $\partial M'$ of $M'$ under $\partial$ has a $\sqsubseteq$-minimal element, say $\partial x$. Consider $x' \in M'$ such that $x' \mid x$; then $\partial x' \sqsubseteq \partial x$. Since $\partial x$ is a minimal element of $\partial M'$, it follows that $\partial x' = \partial x$, and hence $x' = x$. So $x$ is a minimal element of $M'$.

Suppose that $p \mid xy$; then $\partial p \sqsubseteq \partial x \uplus \partial y$. Note that $\partial p = [p]$, so $\partial p$ is an indecomposable element of $\mathcal{M}(P)$. Since indecomposable elements of $\mathcal{M}(P)$ are prime with respect to $\sqsubseteq$, it follows that either $\partial p \sqsubseteq \partial x$ or $\partial p \sqsubseteq \partial y$. In the first case $p \mid x$ and in the second case $p \mid y$. So $p$ is prime with respect to divisibility in $M$. $\square$

# 3   Unique decomposition via a decomposition order

The conditions of Corollary 2.19 of the previous section constitute a complete abstract algebraic characterisation of the class of partial commutative monoids with unique decomposition; it was obtained by a generalisation of the proof of the fundamental theorem of arithmetic. In this section we propose an alternative characterisation, which is inspired by Milner's technique for proving unique decomposition in process theory. The crucial notion in our characterisation is the notion of decomposition order.

**Definition 3.1** 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 $x, y, z \in M$

> if $x \prec y$ and $yz$ is defined, then $xz \prec yz$;

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

> $x \preccurlyeq yz$ implies $x = y'z'$ for some $y' \preccurlyeq y$ and $z' \preccurlyeq z$; and

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

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

**Remark 3.2**  1. As far as we know, the notion of decomposition order is new, but the requirements that constitute a decomposition order are well-known. Only the fourth condition, which was termed 'precompositionality' in [18], is slightly nonstandard. It appears in the literature also with the name *(Riesz) decomposition property* (see, e.g., [9, 10, 19]). Algebraic structures equipped with an ordering are studied extensively in the books by Birkhoff [5] and Fuchs [12].

2. Note that if a partial order $\preccurlyeq$ on a partial commutative monoid $M$ is strictly compatible, then it is also *compatible*, i.e., for all $x, y, z \in M$:

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

We shall use the notion of decomposition order to obtain an alternative characterisation of the class of partial commutative monoids with unique decomposition. Let us compare the three conditions in Corollary 2.19 with the conditions in Definition 3.1, considering divisibility as the candidate order. Then it can be readily observed that well-foundedness, the second condition of Corollary 2.19, also occurs in Definition 3.1, and that the precompositionality condition of Definition 3.1 generalises the third condition of Corollary 2.19 that indecomposables be prime with respect to divisibility.

Cancellation, the first condition of Corollary 2.19, is conspicuously absent from Definition 3.1. Note that (the contrapositive of) strict compatibility, the third condition of Definition 3.1, does imply a weak form of cancellation: if $xy = xz$, then it follows by strict compatibility that either $y = z$, or $y$ and $z$ are incomparable. It will turn out that the existence of a decomposition order on a partial commutative monoid implies cancellation, but only *after* unique decomposition has been established.

The divisibility relations are decomposition orders on the partial commutative monoids that we considered in the previous section.

**Example 3.3**    1. The usual less-than-or-equal relation $\leq$ on $\mathbf{N}$ and its restrictions to the initial segments of $\mathbf{N}$ are (total) decomposition orders. They are well-known to be well-founded, with 0 as least element, strictly compatible, and Archimedean. It is easy to see that they are also precompositional.

2. The divisibility relation $\mid$ on $\mathbf{N}_{>0}$ is a (partial) decomposition order. Note that $k \mid l$ and $k \neq l$ implies $k < l$. Hence it follows that $\mid$ is well-founded, that 1 is the least element of $\mathbf{N}_{>0}$ with respect to $\mid$, that $\mid$ is strictly compatible and, since $k^n < k^{n+1}$ unless $k = 1$, that $\mid$ is Archimedean. To show that it is also precompositional, we use that every indecomposable natural number $p$ is prime, i.e.,

$$\text{if } p \mid kl, \text{ then } p \mid k \text{ or } p \mid l \qquad \text{(cf. Example 2.18(2))}.$$

Suppose that $m \mid kl$ and proceed by induction on $m$. If $m = 1$, then we can take $k' = 1$ and $l' = 1$. If $m > 1$, then there exists a prime number $p$ such that $p \mid m$, whence by transitivity $p \mid kl$. Using the above mentioned property, assume without loss of generality that $p \mid k$, which means that there exist $m', k' \in \mathbf{N}_{>0}$ such that $m = m'p$ and $k = k'p$, and thus $m' \mid k'l$. The induction hypothesis now yields $k'', l' \in \mathbf{N}_{>0}$ such that $k'' \mid k'$ and $l' \mid l$ and $m' = k''l'$. It follows that $m = m'p = (k''p)l'$, $(k''p) \mid (k'p) = k$ and $l' \mid l$.

3. That the submultiset relation $\sqsubseteq$ is a decomposition order on $\mathcal{M}(X)$ is a straightforward consequence of the fact that $\leq$ is a decomposition order on $\mathbf{N}$.

Our main result is that the existence of a decomposition order on a partial commutative monoid implies that it has unique decomposition; it will be proved as Theorem 3.13 in Section 3.1. Note that that in every case of Example 3.3 we have proved that the divisibility relation is a decomposition order. This is no coincidence, for in Section 3.2 we shall prove that whenever a partial commutative monoid has unique decomposition, then its divisibility relation is a decomposition order, which is called the *natural* (or: *algebraic*) decomposition order. As a corollary the converse of our main result is obtained: if a partial commutative monoid has unique decomposition, then it can be endowed with a decomposition order. Hence, our notion of decomposition order provides an alternative abstract algebraic characterisation of the class of partial commutative monoids with unique decomposition.

Recall that every well-founded divisibility relation of a partial commutative monoid is a partial order with the identity as its least element (Lemma 2.15). In Section 3.2 we shall moreover prove that whenever the divisibility relation of a partial commutative monoid is well-founded, strictly compatible and precompositional, then it is also Archimedean. So for divisibility relations the second and fifth condition of Definition 3.1 are redundant; to prove that the divisibility relation of a partial commutative monoid is a decomposition order, it actually suffices to prove that it is a well-founded, strictly compatible and precompositional partial order. In Section 3.3 we show that in the general case none of the five conditions of Definition 3.1 are redundant in the sense that none of them is implied by the other four, and that each of them is necessary for the unique decomposition result.

It is important to note that our main result requires only the *existence* of a decomposition order on a partial commutative monoid to have unique decomposition. Although it is both necessary and sufficient that its divisibility relation be a decomposition order, the existential quantification offers a useful extra degree of freedom. When applying our result in process theory it is usually convenient to consider a partial order different from the natural one (cf. also Remark 4.23), viz. the one induced on processes by an operational semantics.

## 3.1 Unique decomposition

First, we establish that the existence of a decomposition order on a partial commutative monoid implies that every element has a decomposition. Then, we proceed to prove uniqueness. A crucial tool for that will be a *subtraction property* (Corollary 3.7) that formalises the upward proliferation of cancellation along a partial order.

**Proposition 3.4** In a partial commutative monoid $M$ with a decomposition order $\preccurlyeq$ every element has a decomposition.

*Proof.*    Since $\preccurlyeq$ is well-founded, we may proceed by $\preccurlyeq$-induction.

Consider an element $x$ of $M$, and suppose, by way of induction hypothesis, that all $\preccurlyeq$-predecessors of $x$ have a decomposition.

If $x = e$, then the empty multiset is a decomposition of $x$.

If $x$ is indecomposable, then the singleton multiset containing $x$ is a decomposition of $x$.

In the case that remains there exist $y, z \neq e$ such that $x = yz$. From $e \prec y, z$, it follows by strict compatibility that $y$ and $z$ are predecessors of $x$ (e.g., $y = ye \prec yz = x$), so by the induction hypothesis $y$ and $z$ have decompositions, say $[p_1, \ldots, p_m]$ and $[q_1, \ldots, q_n]$. Since $x = yz = p_1 \cdots p_m q_1 \cdots q_n$, it follows that $[p_1, \ldots, p_m, q_1, \ldots, q_n]$ is a decomposition of $x$. □

Next, we proceed to consider uniqueness. We begin with the simple observation that if a composition has a unique decomposition, then its components have unique decompositions too.

**Lemma 3.5** Let $M$ be a partial commutative monoid with a decomposition order and let $x$ and $y$ be elements of $M$. If $xy$ has a unique decomposition, then $x$ and $y$ have unique decompositions too.

*Proof.*    By Proposition 3.4 $x$ and $y$ have decompositions. Since the multiset sum of decompositions of $x$ and $y$ is a decomposition of $xy$, distinct decompositions of $x$ or of $y$ would give rise to distinct decompositions of $xy$. It follows that the decompositions of $x$ and $y$ are unique.                    □

Recall that one of the conditions of the unique decomposition theorem of the previous section (Theorem 2.17) is that the partial commutative monoid has cancellation. One of the reasons for introducing the notion of decomposition order is to eliminate cancellation as a condition. We shall now prove that the conditions of our notion of decomposition order do imply a weak form of cancellation that is not with respect to equality, but with respect to the partial order and its strict version. This weak form of cancellation we refer to as *subtraction*. We need the following lemma.

**Lemma 3.6** Let $M$ be a partial commutative monoid with a decomposition order $\preccurlyeq$; let $x$, $y$ and $z$ be arbitrary elements of $M$, and let $p$ be an indecomposable element of $M$. If $px$ has a unique decomposition and $y \preccurlyeq p$, then $px \preccurlyeq yz$ implies $x \preccurlyeq z$.

*Proof.*    By precompositionality, $px \preccurlyeq yz$ implies that $px = y'z'$ for some $y' \preccurlyeq y$ and $z' \preccurlyeq z$. Since $px$ has a unique decomposition, it follows by Lemma 3.5 that $x$, $y'$ and $z'$ have unique decompositions too. Note that

$$[p] \uplus \partial x = \partial(px) = \partial(y'z') = \partial y' \uplus \partial z' \ .$$

It follows that the indecomposable $p$ is either in the unique decomposition $\partial y'$ of $y'$ or it is in the unique decomposition $\partial z'$ of $z'$. If $p$ is in $\partial y'$, then $p \preccurlyeq y'$, and since also $y' \preccurlyeq y \preccurlyeq p$ it follows that $y' = p$, so $x = z' \preccurlyeq z$. On the other hand, if $p$ is in $\partial z'$, then there exists $z''$ such that $z' = pz''$, so $x = y'z'' \preccurlyeq pz'' = z$ by compatibility.                    □

**Corollary 3.7 (Subtraction)** Let $M$ be a partial commutative monoid with a decomposition order $\preccurlyeq$, and let $x, y, z \in M$. If $xy$ has a unique decomposition, then

$$xy \preccurlyeq xz \text{ implies } y \preccurlyeq z; \text{ and} \tag{1}$$

$$xy \prec xz \text{ implies } y \prec z. \tag{2}$$

*Proof.* By Lemma 3.5 $x$ has a unique decomposition; the proof of (1) is by induction on the cardinality of the unique decomposition $\partial x$ of $x$.

If $\partial x$ is empty, then $x = e$, so $y = xy \preccurlyeq xz = z$.

Otherwise, let $p$ be an element of $\partial x$ and let $x' \in M$ be such that $x = px'$. Then $px'y = xy \preccurlyeq xz = px'z$, so by Lemma 3.6 $x'y \preccurlyeq x'z$. By Lemma 3.5 $x'$ has a unique decomposition too, and since $\partial x' \sqsubset [p] \uplus \partial x' = \partial x$ it follows by the induction hypothesis that $y \preccurlyeq z$.

For the proof of (2), note that $xy \prec xz$ implies $y \preccurlyeq z$ by (1). It follows that $y \prec z$, for $y = z$ would imply $xy = xz$ quod non. $\qquad\square$

**Corollary 3.8** Let $M$ be a partial commutative monoid with a decomposition order $\preccurlyeq$ and let $x$, $y$ and $z$ be arbitrary elements of $M$. If $a = xy = xz$ and all predecessors of $a$ have a unique decomposition, then every predecessor of $y$ is a predecessor of $z$.

*Proof.* If $y' \prec y$, then, by strict compatibility, $xy' \prec xy = xz$, and hence, by Corollary 3.7, $y' \prec z$. $\qquad\square$

**Remark 3.9** Note that our results about partial commutative monoids with decomposition orders so far do not rely on the fifth condition of Definition 3.1. Hence, in particular, Corollary 3.7 remains true if $\preccurlyeq$ is assumed to be a well-founded, strictly compatible and precompositional partial order with the identity as its least element, rather than a decomposition order.

Another condition of the unique decomposition theorem of the previous section (Theorem 2.17) is that indecomposables are prime with respect to the divisibility relation. According to the following lemma, the precompositionality condition of a decomposition order implies that indecomposables are prime with respect to it.

**Lemma 3.10** In a partial commutative monoid $M$ with a precompositional order $\preccurlyeq$ every indecomposable element $p \in M$ is *prime* with respect to $\preccurlyeq$, i.e., for all $x, y \in M$

$$p \preccurlyeq xy \text{ implies } p \preccurlyeq x \text{ or } p \preccurlyeq y.$$

*Proof.* If $p \preccurlyeq xy$, then by precompositionality $p = x'y'$ for some $x' \preccurlyeq x$ and $y' \preccurlyeq y$. Since $p$ is indecomposable, it follows that $x' = e$ or $y' = e$, and hence $p = x'y' = y' \preccurlyeq y$ or $p = x'y' = x' \preccurlyeq x$. $\qquad\square$

Before embarking on the actual proof that the existence of a decomposition order implies uniqueness of decompositions, we provide some intuitions. The idea is to show that two decompositions of a given element $a$ can neither be *too far apart* nor *too close together*, hence must be the same. In particular, consider two decompositions of $a$:

$$p^k p_1^{k_1} \cdots p_n^{k_n} = a = p^l p_1^{l_1} \cdots p_n^{l_n}$$

that agree for all indecomposable $p_i$ larger than $p$, i.e. if $p \preccurlyeq p_i$ then $k_i = l_i$, and assume w.l.o.g. that $l \geq k$. In case $l = k$, then the decompositions agree for $p$ as well, and we conclude. Otherwise, the decompositions are said to be *too close together* if the right-hand side is of shape $p^{k+1}$ (case (2) in the proof), and *too far apart* (case (1) in the proof) otherwise. Let us illustrate these notions by means of an example.

**Example 3.11** Let $q \prec p \prec r$ be indecomposables.

1. The decompositions $qp^2r = p^3r$ are too far apart, since the right-hand side is not a power of $p$.

2. The decompositions $p^2 = p^4$ are too far apart, since although the right-hand side is a $p$-power, the respective multiplicities of $p$ on the left and on the right differ by more than 1.

3. The decompositions $pq^2 = p^2$ are too close together, since the right-hand side is a power of $p$, and its multiplicity is one more than its multiplicity on the left.

The proof idea in the case when two decompositions are too far apart, is that the difference $l - k$ between the factors of $p$ in the two decompositions can be exploited to unboundedly *pump up* the $p$-factors below $a$, by repeatedly *switching* between the two representations of $a$, deriving a contradiction with Archimedeanity. For instance, consider the right-hand side $p^3r$ in Example 3.11(1) and take the $p$-power $p^3$ which clearly is strictly below it. By switching to the left-hand side we obtain $p^3 \prec qp^2r$ as well. Using subtraction (Corollary 3.7) we find that the $q$ is irrelevant for this, and obtain $p^3 \prec p^2r$. But then, $p^3p \prec p^2rp$ holds by strict compatibility. That is, pumping up $p^3$ by the difference $p^{3-2}$ between the $p$-factors of the left- and right-hand sides, yields an element $p^4$ still strictly below $p^3r$. Continuing in this way would yield an infinite increasing sequence $p^3, p^4, p^5, \ldots$ of elements all strictly below $p^3r$, contradicting Archimedeanity.

The infinite process intuition of *pumping up* $p$-factors below $a$ is not actually present in in the proof of Theorem 3.13 below. Instead, we derive a contradiction with the following lemma, which is a direct consequence of Archimedeanity.

**Lemma 3.12** Let $M$ be a partial commutative monoid with a decomposition order $\preccurlyeq$, and let $x, y \in M$. If $x \neq e$, then $\{i : x^i \prec y\}$ is a finite set.

*Proof.* Since $\preccurlyeq$ is Archimedean and $x \neq e$, there exists $n > 0$ such that $x^n \not\prec y$. Since $e \preccurlyeq x^j$, it follows by strict compatibility that $x^n \preccurlyeq x^{n+j}$, so $x^{n+j} \not\prec y$ for all $j \geq 0$. It follows that $x^i \prec y$ implies $i < n$, so the set $\{i : x^i \prec y\}$ is finite. $\square$

The idea in the case when two decompositions are too close together is that the extra $p$-power on the right is compensated for on the left by a *remainder* $p_1^{k_1} \cdots p_n^{k_n}$ consisting of *fractions* of $p$, i.e. indecomposables below $p$. To keep matters concrete consider Example 3.11(3), where the extra $p$-factor of $p^2$ is compensated for in $pq^2$ by a remainder $q^2$. The proof idea is that removing a single fraction $q$ from the remainder would yield an element $q$ *just* below $p$. Therefore, replacing $p$ in $pq^2$ by $q$ yields an element $q^3$ strictly below $pq^2 = p^2$. But since $q$ was chosen *just* below $p$, the two $p$s of $p^2$ can only cover two of the $q$s of $q^3$. In order for the third to be covered as well, it should be *splittable* into smaller fractions. The splitting of fractions can be repeated ad infinitum, and thus it yields a nonempty set without a minimal element contradicting well-foundedness.

**Theorem 3.13 (Unique decomposition)** In a partial commutative monoid with a decomposition order every element has a unique decomposition.

*Proof.* Let $M$ be a partial commutative monoid with a decomposition order $\preccurlyeq$. By Proposition 3.4 every element of $M$ has a decomposition. To prove uniqueness, suppose, to the contrary, that the subset of elements of $M$ with two or more distinct decompositions is nonempty; since $\preccurlyeq$ is well-founded, this subset has a $\preccurlyeq$-minimal element $a$. For the remainder of this proof we fix two distinct decompositions of $a$, and an indecomposable element $p$ that is $\preccurlyeq$-maximal in both decompositions and that occurs more often in one of

the decompositions than in the other. To make this explicit we fix a sequence $p, p_1, \ldots, p_n$ of distinct indecomposable elements, and sequences $k, k_1, \ldots, k_n$ and $l, l_1, \ldots, l_n$ of natural numbers such that

(A) $a = p^k p_1^{k_1} \cdots p_n^{k_n}$ and $a = p^l p_1^{l_1} \cdots p_n^{l_n}$;

(B) $k < l$; and

(C) $p \prec p_i$ implies $k_i = l_i$ for all $1 \le i \le n$.

That $a$ is $\preccurlyeq$-minimal in the subset of elements of $M$ with two or more distinct decompositions, means that all predecessors of $a$ have a unique decomposition.

1. Suppose $l > k + 1$ or $l_i \ne 0$ for some $1 \le i \le n$. By Lemma 3.12 $\{i : p^i \prec a\}$, the set of multiplicities of $p$ in predecessors of $a$, is finite. Let $m = \max\{i : p^i \prec a\}$, so that $m$ denotes the maximum of the multiplicities of $p$ in the predecessors of $a$. From $a = p^l p_1^{l_1} \cdots p_n^{l_n}$ and the supposition, it follows that $k < m$; for if $l > k+1$, then, since $p^{l-1} \prec a$, $k < l - 1 \le m$, and if $l_i \ne 0$ for some $1 \le i \le n$, then $p^l \prec a$, so $k < l \le m$ by (B). From $p^m \prec a = p^k p_1^{k_1} \cdots p_n^{k_n}$ it follows by Corollary 3.7 that

$$p^{m-k} \prec p_1^{k_1} \cdots p_n^{k_n}.$$

Since $p^{m-k}$ is a predecessor of $a$, it has a unique decomposition consisting of $m - k$ copies of $p$. So, by precompositionality there exist $m_1, \ldots, m_n \ge 0$ such that

$$p^{m_i} \preccurlyeq p_i^{k_i} \text{ for all } 1 \le i \le n \text{ and } m_1 + \cdots + m_n = m - k.$$

If $m_i = 0$, then $p^{m_i} = e \preccurlyeq p_i^{l_i}$. If $m_i > 0$, then $p \preccurlyeq p_i^{k_i}$, so $p \preccurlyeq p_i$ by Lemma 3.10. Recall that $p$ and $p_i$ are distinct, so $p \prec p_i$. Hence $p^{m_i} \preccurlyeq p_i^{k_i} = p_i^{l_i}$ by condition (C). It follows that

$$p^{m_i} \preccurlyeq p_i^{l_i} \text{ for all } 1 \le i \le n.$$

By compatibility $p^{m-k} \preccurlyeq p_1^{l_1} \cdots p_n^{l_n}$. Moreover, $p^{m-k} \ne p_1^{l_1} \cdots p_n^{l_n}$, for the unique decomposition of $p^{m-k}$ contains $p$ (recall that $k < m$), whereas the unique decomposition of $p_1^{l_1} \cdots p_n^{l_n}$ does not ($p \ne p_i$ for $1 \le i \le n$). Hence,

$$p^{m-k} \prec p_1^{l_1} \cdots p_n^{l_n}.$$

By strict compatibility $p^{l+(m-k)} \prec a$. However, since $l > k$ according to condition (B), it holds that $l + (m - k) = m + (l - k) > m$, contradicting that $m$ is the maximum of the multiplicities of $p$ in the predecessors of $a$.

2. Suppose $l = k + 1$ and $l_i = 0$ for all $1 \le i \le n$. For the remainder of this proof, let

$$b = p_1^{k_1} \cdots p_n^{k_n}, \tag{3}$$

so that $p^k b = p^k p$. Clearly $b \ne p$, so $k > 0$ and hence $b \prec a$. Moreover, $p^k \prec p^k p = p^k b$ by strict compatibility, so $b \ne e$. So the decomposition of $b$ implied by (3) is unique and nonempty. Without loss of generality we may assume that $p_1$ is a $\preccurlyeq$-minimal element of the unique decomposition of $b$, i.e., $k_1 > 0$ and $p_i \prec p_1$ implies $k_i = 0$. Let $c$ be obtained by subtracting $p_1$ from $b$, i.e., let

$$c = p_1^{k_1 - 1} p_2^{k_2} \cdots p_n^{k_n}. \tag{4}$$

Since $c \prec b$, by Corollary 3.8 $c \prec p$, so by strict compatibility

$$p^{k-1}cb \prec p^{k-1}pb = p^{k-1}pp,$$

By Corollary 3.7, $bc \prec pp$, and hence, by precompositionality, there exist $d, d' \preccurlyeq p$ such that

$$bc = dd'. \tag{5}$$

Note that $d$ and $d'$ are predecessors of $a$ so they have unique decompositions. Moreover, the elements of their unique decompositions are elements of the set $\{p_1, \ldots, p_n\}$. In particular, $p$ is not an element of the decompositions of $d$ and $d'$, so $d, d' \prec p$, and hence, by Corollary 3.8, $d, d' \prec b$. From (3), (4) and (5) it follows that the unique decomposition of $dd'$ contains $2k_1 - 1$ copies of $p_1$. So we may assume without loss of generality that the unique decomposition of $d'$ contains at most $k_1 - 1$ copies of $p_1$. Since $d' \prec b = p_1^{k_1} \cdots p_n^{k_n}$, by precompositionality $d' = b_1 \cdots b_n$ with $b_i \preccurlyeq p_i^{k_i}$ for all $1 \le i \le n$. Again by precompositionality, $b_1 = b_{11} \cdots b_{1k_1}$ with $b_{1i} \preccurlyeq p_1$ for all $1 \le i \le n$. Since the elements of the unique decomposition of $b_1$ are elements of the set $\{p_1, \ldots, p_n\}$ and since $p_1$ is a $\preccurlyeq$-minimal element of this set, it follows that $b_{1i} = p_1$ or $b_{1i} = e$ for all $1 \le i \le k_1$. Recall that that the unique decomposition of $d'$ contains at most $k_1 - 1$ copies of $p_1$, so $b_1 \preccurlyeq p_1^{k_1-1}$. It follows by compatibility that $d' \preccurlyeq c$, and by strict compatibility that $dd' \prec bc$, a contradiction with (5). $\square$

## 3.2 The natural decomposition order

Recall that in Example 3.3 we proved that the divisibility relations associated with the commutative monoids $\mathbf{N}$, $\mathbf{N}_{>0}$ and $\mathcal{M}(X)$ are decomposition orders. We shall now first prove that the divisibility relation of a partial commutative monoid with unique decomposition is always a decomposition order; it is called the *natural* decomposition order. In order to prove that a partial commutative monoid has unique decomposition, it is good practice to first attempt to prove that its divisibility relation is a decomposition order. Recall that any well-founded divisibility relation is a partial order with the identity as its least element (cf. Lemma 2.15). To further reduce the task of showing that the divisibility relation is a decomposition order, we show that a well-founded, strictly compatible and precompositional divisibility relation is necessarily Archimedean. Hence, to show that a partial commutative monoid has unique decomposition, it suffices to verify that its divisibility relation is well-founded, strictly compatible and precompositional.

**Theorem 3.14** The divisibility relation associated with a partial commutative monoid $M$ with unique decomposition is a decomposition order, and it is minimal in the sense that it is included in any other decomposition order on $M$.

*Proof.* Let $M$ be a partial commutative monoid with unique decomposition and let $P$ be the set of indecomposable elements of $M$. According to Example 3.3(3), $\sqsubseteq$ is a decomposition order of the commutative monoid $\mathcal{M}(P)$ of multisets over $P$. We use the properties of the mapping $\partial : M \to \mathcal{M}(P)$ established in Proposition 2.11 to prove that the divisibility relation $|$ of $M$ is also a decomposition order.

According to Example 3.3(3) $\sqsubseteq$ is a decomposition order of the commutative monoid $\mathcal{M}(P)$ of multisets over $P$. We use the properties of the mapping $\partial : M \to \mathcal{M}(P)$ established in Proposition 2.11 to prove that the divisibility relation $|$ of $M$ is then also a decomposition order.

Since $\sqsubseteq$ on $\mathcal{M}(P)$ is a well-founded partial order with least element $\square$, and since $\partial$ preserves divisibility and the identity, it follows that $\mid$ is a well-founded partial order with least element $e$.

Since $\sqsubseteq$ is strictly compatible, and $\partial$ is injective and preserves the divisibility relation, it follows that $\mid$ is strictly compatible too.

To see that $\mid$ is Archimedean, let $x$ and $y$ be elements of $M$ such that $x^n \mid y$ and $x^n \neq y$ for all $n \in \mathbf{N}$. Since $\partial$ is injective and preserves divisibility and multiplication, $n\partial x \sqsubset \partial y$ for all $n \in \mathbf{N}$. Hence, since $\sqsubset$ is Archimedean, it follows that $\partial x = \square$, which implies that $x = e$ since $\partial$ preserves the identity. So $\mid$ is Archimedean.

To see that $\mid$ is precompositional, suppose that $x \mid yz$. Then, since $\mid$ preserves the divisibility relation and multiplication, $\partial x \sqsubseteq \partial y \uplus \partial z$. Since $\sqsubseteq$ is precompositional, it follows that there exist multisets $m \sqsubseteq \partial y$ and $m' \sqsubseteq \partial z$ such that $\partial x = m \uplus m'$. Since $\partial M$ is division-closed, there exist $y'$ and $z'$ such that $m = \partial y'$ and $m' = \partial z'$, so $\partial x = \partial y' \uplus \partial z'$. Hence, since $\partial$ preserves the divisibility relation $y' \mid y$ and $z' \mid z$, and since $\partial$ preserves multiplication $x = y'z'$. It follows that $\mid$ is precompositional.

It is now proved that the divisibility relation associated with a partial commutative monoid with unique decomposition is a decomposition order. It remains to prove that the divisibility relation is minimal, i.e., that it is contained in every other decomposition order on $M$. To this end, let $\preccurlyeq$ be an arbitrary decomposition order on $M$, and suppose that $x \mid y$. From $x \mid y$ it follows that $xy' = y$ for some element $y'$ of $M$. Since the identity $e$ is the least element of $M$ with respect to $\preccurlyeq$, and $\preccurlyeq$ is compatible, it follows that $x = xe \preccurlyeq xy' = y$. So if $x \mid y$, then $x \preccurlyeq y$.

Hence, if a partial commutative monoid has unique decomposition, then its divisibility relation is its minimal decomposition order. $\qquad\square$

According to Theorem 3.13, to prove that a partial commutative monoid has unique decomposition it suffices to show that it has a decomposition order. Moreover, according to Theorem 3.14, such a decomposition order always exists whenever the monoid has unique decomposition. It follows that our method is complete.

**Corollary 3.15** A partial commutative monoid has a unique decomposition iff it has a decomposition order.

We proceed to prove that any well-founded, strictly compatible and precompositional divisibility relation is in fact necessarily an Archimedean partial order with the identity as its least element, and hence a decomposition order. The essence of the proof is that the division-closed substructures of a partial commutative monoid inherit most of its properties.

**Lemma 3.16** Any nonempty division-closed subset $M'$ of a partial commutative monoid $M$ is a partial commutative monoid under the restriction of the multiplication of $M$ to $M'$. Moreover, divisibility in $M'$ is the restriction of divisibility in $M$ to $M'$.

*Proof.* In this proof we denote multiplication in $M$ by $\cdot$, and its restriction to $M'$ by $\cdot'$. Note that, since $M'$ is nonempty and division-closed, $e$ is an element of $M'$. We need to show that $(M', \cdot', e)$ is a partial commutative monoid again, i.e., that it satisfies the laws of Definition 2.1. We treat the associative law in detail; the proofs for the commutative and identity laws are similar.

Suppose that $x, y, z \in M'$ and that $x \cdot' (y \cdot' z)$ is defined. Then, since $\cdot'$ is the restriction of $\cdot$ to $M'$, $x \cdot (y \cdot z)$ is defined, and since $(M, \cdot, e)$ satisfies the associative law, it follows that $(x \cdot y) \cdot z$ is defined too and that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Note that from $(x \cdot y) \mid (x \cdot y) \cdot z = x \cdot (y \cdot z)$, it follows that $(x \cdot y)$ and $(x \cdot y) \cdot z$ are divisors of $x \cdot (y \cdot z)$. Hence, since $M'$ is division-closed, $(x \cdot y)$ and $(x \cdot y) \cdot z$ are elements of $M'$, and $(x \cdot' y)$ and $(x \cdot' y) \cdot' z = (x \cdot y) \cdot' z$ are defined.

Similarly, it can be established that $x \cdot' (y \cdot' z)$ is defined whenever $(x \cdot' y) \cdot' z$ is defined. Since $x \cdot' (y \cdot' z) = x \cdot (y \cdot z) = (x \cdot y) \cdot z = (x \cdot' y) \cdot' z$, it follows that $\cdot'$ is associative.

Next, we show that divisibility in $M'$ is the restriction of divisibility in $M$ to $M'$. Let $|$ denote divisibility in $M$ and let $|'$ denote divisibility in $M'$. If $x \mid' y$, then there exists $y' \in M'$ such that $x \cdot' y' = y$; since $\cdot'$ is the restriction of $\cdot$ to $M'$ it follows that $x \cdot y' = y$, and hence $x \mid y$. On the other hand, if $x$ and $y$ are elements of $M'$ such that $x \mid y$, then there exists $y'$ such that $x \cdot y' = y$. By the commutative law it follows that $y'$ is a divisor of $y$, so $y'$ is an element of $M'$. It follows that $x \cdot' y' = y$, so $x \mid' y$. Thereby it is proved that $|'$ is the restriction of $|$ to $M'$. $\qquad\square$

**Theorem 3.17** If the divisibility relation of a partial commutative monoid is well-founded, strictly compatible and precompositional, then it is a decomposition order.

*Proof.* Let $M$ be a partial commutative monoid with a well-founded, strictly compatible and precompositional divisibility relation $|$.

By Lemma 2.15 $|$ is a partial order on $M$ with the identity $e$ of $M$ as its least element. Hence, to prove the theorem, it remains to show that $|$ is Archimedean. Assume, to the contrary, that the set

$$\{y \in M : \text{there exists } x \neq e \text{ such that } x^n \mid y \ \& \ x^n \neq y \text{ for all } n \in \mathbf{N}\} \qquad (6)$$

is nonempty. Let $a$ be a $|$-minimal element of this set (which exists since $|$ is well-founded), and let $b \neq e$ be such that $b^n \mid a \ \& \ b^n \neq a$ for all $n \in \mathbf{N}$.

First, we establish that all proper divisors of $a$, i.e., the elements of the set

$$M' = \{x \in M : x \mid a \ \& \ x \neq a\},$$

have a unique decomposition in $M$. Note that $M'$ is nonempty since $e \mid a$ and $e \neq a$. To prove that $M'$ is division-closed, suppose $x \in M$ and $y \in M'$ such that $x \mid y$. Since $|$ is well-founded, it is by Lemma 2.15 a partial order; from $x \mid y$, $y \mid a$ and $y \neq a$, it follows by transitivity that $x \mid a$ and by antisymmetry that $x \neq a$, so $x \in M'$. Now, since $M'$ is a nonempty division-closed subset of $M$, it follows by Lemma 3.16 that $M'$ is a partial commutative monoid under the restriction of the multiplication of $M$ to $M'$, and that its divisibility relation is the restriction of divisibility in $M$ to $M'$. From this, it is straightforward to verify that divisibility in $M'$ is well-founded, strictly compatible and precompositional. Moreover, since the elements of $M'$ are proper divisors of $a$, divisibility in $M'$ is Archimedean. It follows that divisibility in $M'$ is a decomposition order on $M'$, and hence, by Theorem 3.13, $M'$ has unique decomposition. Since decompositions in $M$ of elements in $M'$ must entirely consist of proper divisors of $a$, whence of elements of $M'$, it follows that the elements of $M'$ have a unique decomposition in $M$ as well.

Now, in particular, we know that $b$ has a unique decomposition in $M$, which is nonempty since $b \neq e$. Let $p$ be an indecomposable element in the unique decomposition of $b$. Then $b = pb'$ for some $b' \in M'$ and, since $b$ is a proper divisor of $a$, it follows that $a = pa'$ for some proper divisor $a'$ of $a$. But then, since $pb'b^n = b^{n+1} \mid a = pa'$ and $pb'b^n = b^{n+1} \neq a = pa'$ for all $n \in \mathbf{N}$, it follows by Corollary 3.7 (cf. also Remark 3.9) that $b'b^n \mid a'$ and $b'b^n \neq a'$, and hence $b^n \mid a'$ and $b^n \neq a'$ for all $n \in \mathbf{N}$. This means that $a'$ is an element of the set in (6) whereas $a'$ is a proper divisor of $a$, contradicting our assumption that $a$ is a $|$-minimal element of that set. $\qquad\square$

**Corollary 3.18** A partial commutative monoid has unique decomposition iff its divisibility relation is well-founded, strictly compatible and precompositional.

**Remark 3.19** There is interesting analogy between the proofs of Corollary 2.19 and Theorem 3.14 on the one hand, and Theorem 3.17 on the other hand. Note that if $M$ has unique decomposition, then by Proposition 2.11 $\partial M$ is a nonempty division-closed subset of $\mathcal{M}(P)$, and hence, by Lemma 3.16, it is a partial commutative monoid under restricted multiset sum. In the proofs of Corollary 2.19 and Theorem 3.14 we have established that this particular relative subalgebra of $\mathcal{M}(P)$ (cf. [13] for a definition of *relative subalgebra*) inherits all relevant properties. In the proof of Theorem 3.17 it was also used that some division-closed relative subalgebra of a partial commutative monoid inherits all relevant properties.

Call a property of partial commutative monoids *division-persistent* if it is preserved under taking division-closed relative subalgebras. One may wonder if there is common reason for the conditions of Corollary 2.19 and of decomposition orders to be preserved under taking division-closed relative subalgebras. To that end, note that they all can be formalised by means of a formula in which all existential quantifications and definedness assumptions are 'division-bounded'. For instance, strict compatibility can be formalised by means of the formula

$$\forall x, y, z, u. \ (x \mid y \ \& \ x \neq y \ \& \ yz = u) \implies \exists v \mid u. \ v = xz \ \& \ v \neq u \ ;$$

the existential quantification is division-bounded since the existentially quantified $v$, used to express definedness of $xz$, is required to divide $u$.

## 3.3 Independence

In this section, examples are exhibited of partial orders on partial commutative monoids such that the latter do *not* have unique decomposition, and the former are decomposition orders *except* that in each example exactly *one* of the conditions in Definition 3.1 does not hold. This shows both the necessity and the independence of these conditions. The counterexamples against well-foundedness, strict compatibility and precompositionality employ the divisibility relation. The counterexamples against $e$ being the least element and the order being Archimedean by necessity employ an order different from the divisibility relation (cf. Theorem 3.17).

The nonnegative rationals do not have unique decomposition and the only difference with the natural numbers is that their natural order is not well-founded.

**Example 3.20** Consider the commutative monoid $(\mathbf{Q}_{\geq 0}, +, 0)$ of nonnegative rational numbers. It has no indecomposable elements (e.g., if $r$ is a positive rational number, then $r = \frac{r}{2} + \frac{r}{2}$ and $0 < \frac{r}{2} < r$), and hence only 0 has a decomposition in $(\mathbf{Q}_{\geq 0}, +, 0)$.

Let $\leq$ be the usual less-than-or-equal relation on $\mathbf{Q}_{\geq 0}$; it is not well-founded (e.g., the set $\{\frac{1}{n} : n \in \mathbf{N}_{>0}\}$ does not contain a minimal element). It is easily verified that 0 is the least element of $\mathbf{Q}_{\geq 0}$ with respect to $\leq$, that $\leq$ is strictly compatible, and that it is precompositional and Archimedean. So $\leq$ is not a decomposition order on $(\mathbf{Q}_{\geq 0}, +, 0)$ due only to the fact that it is not well-founded.

Taking the trivial order on the rationals instead of the natural order, 0 fails to be the least element.

**Example 3.21** Consider again the commutative monoid $(\mathbf{Q}_{\geq 0}, +, 0)$ of nonnegative rational numbers. The diagonal $\Delta = \{(r, r) : r \in \mathbf{Q}_{\geq 0}\}$ on $\mathbf{Q}_{\geq 0}$ is trivially a well-founded partial order that is strictly compatible, precompositional and Archimedean, but 0 is not the least element of $\mathbf{Q}_{\geq 0}$ with respect to $\Delta$ (e.g., $(0, 1) \notin \Delta$). So $\Delta$ is not a decomposition order on $(\mathbf{Q}_{\geq 0}, +, 0)$ due only to the fact that 0 is not the least of $\mathbf{Q}_{\geq 0}$ with respect to $\Delta$.

Taking maximum instead of addition as the operation on the natural numbers, unique decomposition does not hold and it is only strictness of compatibility that fails for the natural order. The failure actually already shows up in the initial segment of bits with maximum, which is isomorphic to Booleans with disjunction.

**Example 3.22** Consider the commutative monoid $(B, \vee, \bot)$ of Booleans $B = \{\bot, \top\}$ with disjunction. It has no indecomposable elements, for if $b \in B$ and $b \neq \bot$, then $b = \top$, and $\top = \top \vee \top$. The divisibility relation on $B$, which we denote by $\preccurlyeq$, is clearly well-founded, so by Lemma 2.15 it is a partial order with $\bot$ as least element. Note that $\bot \prec \top$ but $\bot \vee \top = \top \vee \top$, so $\preccurlyeq$ is not strictly compatible. That $\preccurlyeq$ is precompositional and Archimedean is, however, easily verified. So $\preccurlyeq$ is not a decomposition order on $(B, \vee, \bot)$ due only to the fact that it is not strictly compatible.

We obtain an example showing that precompositionality cannot be omitted from the definition of decomposition order by adjoining a copy $1'$ of $1$ to the commutative monoid of natural numbers.

**Example 3.23** Consider the commutative monoid $(\mathbf{N}', +', 0)$, where $\mathbf{N}' = \mathbf{N} \cup \{1'\}$ and $+'$ is defined by

$$0 +' x = x +' 0 = x \ ,$$
$$m +' 1' = 1' +' m = m + 1 \ , \text{ and}$$
$$m +' n = m + n$$

for $x$ in $\mathbf{N}'$ and $m, n$ in $\mathbf{N}_{>0}$. Checking that the natural order $\leq'$ is a well-founded partial order with $0$ as least element, and that it is strictly compatible and Archimedean, is as easy as it is for $(\mathbf{N}, +, 0)$. Hence, $\leq'$ is not a decomposition order due only to the fact that it is not precompositional, as witnessed by $1' \leq' 2 = 1 +' 1$.

We conclude this section with an example that shows that our requirement that a decomposition order be Archimedean cannot be omitted.

**Example 3.24** Let $M = (\mathbf{N} \times \mathbf{N} \times \{0\}) \cup (\mathbf{N}_{>0} \times \mathbf{N} \times \{1\})$ and define on $M$ a binary operation $\oplus$ by

$$(k, l, 0) \oplus (m, n, 0) = (k + m, l + n, 0) \ ,$$
$$(k, l, 1) \oplus (m, n, 1) = (k + m, l + n, 1) \ , \text{ and}$$
$$(k, l, 0) \oplus (m, n, 1) = (m, n, 1) \oplus (k, l, 0) = (m, k + l + n, 1) \ .$$

It is straightforward to verify that $M$ is a commutative monoid under $\oplus$, with $(0, 0, 0)$ as the identity. Note that $(1, 0, 0)$, $(0, 1, 0)$ and $(1, 0, 0)$ are indecomposable and that

$$(1, 0, 0) \oplus (1, 0, 1) = (1, 1, 1) = (0, 1, 0) \oplus (1, 0, 1) \ ,$$

so decomposition in $M$ is not unique.

Let $\sqsubseteq$ be the least relation on $M$ such that

$$(k, l, 0) \sqsubseteq (m, n, 0) \text{ iff } k \leq m \ \& \ l \leq n \ ,$$
$$(k, l, 1) \sqsubseteq (m, n, 1) \text{ iff } k \leq m \text{ or } (k = m \ \& \ l \leq n) \ ,$$
$$(k, l, 0) \sqsubseteq (m, n, 1) \text{ for all } k, l, m, n \geq 0 \ .$$

Then $\sqsubseteq$ is a well-founded partial order and $(0, 0, 0)$ is the least element of $M$ with respect to $\sqsubseteq$. That $\sqsubseteq$ is precompositional and strictly compatible is proved by distinguishing cases

according to the form of the elements. Let $n(1,0,0)$ denote the $n$-fold sum of $(1,0,0)$; then $n(1,0,0) = (n,0,0) \sqsubseteq (1,0,1)$ for all $n \in \mathbf{N}$ and $(1,0,0) \neq (0,0,0)$, so it follows that $\sqsubseteq$ is not Archimedean. So $\sqsubseteq$ is not a decomposition order on $M$ due only to the fact that it fails to be Archimedean.

**Remark 3.25** For people familiar with the multiset extension of an order (see e.g. [26, Definition A.6.2]): the partial order $\sqsubseteq$ of Example 3.24 is isomorphic to the multiset extension of the order $q, r \prec p$ on $\{p, q, r\}$, modulo $[p, q] = [p, r]$. The isomorphism is given by

$$(k, l, 0) \mapsto [\overbrace{q, \ldots, q}^{k}, \overbrace{r, \ldots, r}^{l}] \;,\; \text{and} \; (k, l, 1) \mapsto [\overbrace{p, \ldots, p}^{k}, \overbrace{r, \ldots, r}^{l}] \;.$$

(To see that the mapping is surjective, note that if $k > 0$, then modulo $[p, q] = [p, r]$ the multisets $[\overbrace{p, \ldots, p}^{k}, \overbrace{q, \ldots, q}^{l}, \overbrace{r, \ldots, r}^{m}]$ and $[\overbrace{p, \ldots, p}^{k}, \overbrace{r, \ldots, r}^{l+m}]$ are the same .)

# 4 An application in process theory

We shall now illustrate the application of our main theorem using it to establish a unique decomposition theorem for the process theory $\mathsf{ACP}^{\varepsilon}$, the extension of the theory $\mathsf{ACP}$ of Bergstra and Klop [4] with the *empty process* $\varepsilon$ (see, e.g., Vrancken [27]). We proceed as follows. First we introduce $\mathsf{ACP}^{\varepsilon}$ in full generality and we show that the set of $\mathsf{ACP}^{\varepsilon}$ expressions modulo bisimulation [20, 25] is a commutative monoid under parallel composition. Then, we discuss three examples that show that this commutative monoid does not have unique decomposition, and we propose requirements on $\mathsf{ACP}^{\varepsilon}$ that bar these examples. The commutative submonoid induced by these requirements has unique decomposition, for the operational semantics of $\mathsf{ACP}^{\varepsilon}$ induces a decomposition order on it. The interesting thing about this particular decomposition order is that it is *not* the natural decomposition order.

## 4.1 $\mathsf{ACP}^{\varepsilon}$

We fix two disjoint sets of symbols $\mathcal{A}$ and $\mathcal{V}$; the elements of $\mathcal{A}$ are called *actions* and the elements of $\mathcal{V}$ are called *process variables*. With $a \in \mathcal{A}$, $X \in \mathcal{V}$ and $\mathcal{H}$ ranging over finite subsets of $\mathcal{A}$, the set $\mathcal{P}$ of *process expressions* is generated by

$$P ::= \; \varepsilon \;\mid\; \delta \;\mid\; a \;\mid\; X \;\mid\; P \cdot P \;\mid\; P + P \;\mid\; \partial_{\mathcal{H}}(P) \;\mid\; P \,\|\!\!\llcorner\, P \;\mid\; P \mid P \;\mid\; P \,\|\, P.$$

If $X$ is a process variable and $P$ is a process expression, then the expression

$$X \stackrel{\text{def}}{=} P$$

is called a *process equation defining $X$*. A set of such expressions is called a *process specification* if it contains precisely one defining process equation for each $X \in \mathcal{V}$.

For the remainder of this paper we fix a *guarded* process specification $\mathcal{S}$: every occurrence of a process variable in the right-hand side $P$ of an equation in $\mathcal{S}$ occurs in a subexpression of $P$ of the form $a \cdot Q$ with $a \in \mathcal{A}$.

We also presuppose a *communication function*, i.e., a commutative and associative partial mapping

$$\gamma : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}$$

that specifies which actions may communicate. If $\gamma(a, b)$ is undefined, then the actions $a$ and $b$ cannot communicate, whereas if $\gamma(a, b) = c$ then they can communicate and the action $c$ stands for the communication event.

Table 1: The transition system specification for $\mathsf{ACP}^\varepsilon$.

$$\frac{}{\varepsilon\downarrow} \qquad \frac{P\downarrow,\ Q\downarrow}{(P\cdot Q)\downarrow} \qquad \frac{P\downarrow}{(P+Q)\downarrow,\ (Q+P)\downarrow} \qquad \frac{P\downarrow,\ Q\downarrow}{(P\parallel Q)\downarrow,\ (Q\parallel P)\downarrow} \qquad \frac{P\downarrow}{\partial_{\mathcal{H}}(P)\downarrow}$$

$$\frac{}{a\stackrel{a}{\longrightarrow}\varepsilon} \qquad \frac{P\stackrel{a}{\longrightarrow}P'}{P\cdot Q\stackrel{a}{\longrightarrow}P'\cdot Q} \qquad \frac{P\downarrow,\ Q\stackrel{a}{\longrightarrow}Q'}{P\cdot Q\stackrel{a}{\longrightarrow}Q'}$$

$$\frac{P\stackrel{a}{\longrightarrow}P'}{P+Q\stackrel{a}{\longrightarrow}P',\ Q+P\stackrel{a}{\longrightarrow}P'} \qquad \frac{P\stackrel{a}{\longrightarrow}P',\ (X\stackrel{\mathrm{def}}{=}P)\in\mathcal{S}}{X\stackrel{a}{\longrightarrow}P'}$$

$$\frac{P\stackrel{a}{\longrightarrow}P'}{P\parallel\!\!\!\;\underline{\phantom{}}\,Q\stackrel{a}{\longrightarrow}P'\parallel Q} \qquad \frac{P\stackrel{b}{\longrightarrow}P',\ Q\stackrel{c}{\longrightarrow}Q',\ a=\gamma(b,c)}{P\mid Q\stackrel{a}{\longrightarrow}P'\parallel Q'} \qquad \frac{P\stackrel{a}{\longrightarrow}P',\ a\notin\mathcal{H}}{\partial_{\mathcal{H}}(P)\stackrel{a}{\longrightarrow}\partial_{\mathcal{H}}(P')}$$

$$\frac{P\stackrel{a}{\longrightarrow}P'}{P\parallel Q\stackrel{a}{\longrightarrow}P'\parallel Q,\ Q\parallel P\stackrel{a}{\longrightarrow}Q\parallel P'} \qquad \frac{P\stackrel{b}{\longrightarrow}P',\ Q\stackrel{c}{\longrightarrow}Q',\ a=\gamma(b,c)}{P\parallel Q\stackrel{a}{\longrightarrow}P'\parallel Q'}$$

The transition system specification in Table 1 defines on the set $\mathcal{P}$ a unary predicate $\downarrow$ and binary relations $\stackrel{a}{\longrightarrow}$ $(a\in\mathcal{A})$.

**Definition 4.1** A *bisimulation* is a symmetric binary relation $\mathcal{R}$ on $\mathcal{P}$ such that $P\ \mathcal{R}\ Q$ implies

(i) if $P\downarrow$, then $Q\downarrow$; and

(ii) if $P\stackrel{a}{\longrightarrow}P'$, then there exists $Q'$ such that $Q\stackrel{a}{\longrightarrow}Q'$ and $P'\ \mathcal{R}\ Q'$.

Process expressions $P$ and $Q$ are said to be *bisimilar* (notation: $P\leftrightarrow Q$) if there exists a bisimulation $\mathcal{R}$ such that $P\ \mathcal{R}\ Q$.

Baeten and van Glabbeek [3] prove that $\leftrightarrow$ is a congruence for $\mathsf{ACP}^\varepsilon$, i.e., it is an equivalence relation with the substitution property for all the syntactic constructs. Let $\mathcal{P}/\!\!\leftrightarrow$ denote the quotient of $\mathcal{P}$ by $\leftrightarrow$, i.e., the set of equivalence classes of $\mathcal{P}$ with respect to $\leftrightarrow$. The equivalence class containing the process expression $P$ we denote by $[P]$. The equivalence class $[\varepsilon]$ is considered a distinguished element of $\mathcal{P}/\!\!\leftrightarrow$, and, since $\leftrightarrow$ has the substitution property for $\parallel$, we can define on $\mathcal{P}/\!\!\leftrightarrow$ a binary operation $\parallel$ by

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

(It is standard practice to use the same symbol for the binary operation on the quotient.) We have then have following proposition.

**Proposition 4.2** $\mathcal{P}/\!\!\leftrightarrow$ is a commutative monoid under $\parallel$ with identity $[\varepsilon]$.

*Proof.* It is easily verified that

$$P\parallel(Q\parallel R)\leftrightarrow(P\parallel Q)\parallel R$$
$$P\parallel Q\leftrightarrow Q\parallel P$$
$$P\parallel\varepsilon\leftrightarrow\varepsilon\parallel P\leftrightarrow P$$

and the proposition is an immediate consequence. $\qquad\qquad\square$

23

## 4.2 Weakly normed ACP$^\varepsilon$ with linear communication

In this section we present three counterexamples obstructing a general unique decomposition theorem for the commutative monoid $\mathcal{P}/\leftrightarrows$ defined in the previous section. They will guide us in identifying a submonoid which does admit a unique decomposition theorem, as we shall prove in the next section.

The first counterexample already appears in [21]; it shows that perpetual processes need not have a decomposition.

**Example 4.3** Let $a$ be an action, let $\gamma(a,a)$ be undefined and let $X \stackrel{\text{def}}{=} a \cdot X$. One can show that $X \leftrightarrows P_1 \| \cdots \| P_n$ implies $P_i \leftrightarrows X$ for some $1 \leq i \leq n$. Since $[X]$ is not an indecomposable element of $\mathcal{P}/\leftrightarrows$ (e.g., $X \leftrightarrows a \| X$), it follows that $[X]$ has no decomposition in $\mathcal{P}/\leftrightarrows$.

Let $w \in \mathcal{A}^*$, say $w = a_1 \cdots a_n$; we write $P \stackrel{w}{\longrightarrow} P'$ if there exist $P_0, \ldots, P_n$ such that

$$P = P_0 \stackrel{a_1}{\longrightarrow} \cdots \stackrel{a_n}{\longrightarrow} P_n = P' \ .$$

The perpetuality exploited in the above counterexample is sometimes excluded by restricting to process expressions $P$ that can terminate, i.e., for which there exist $w \in \mathcal{A}^*$ and a process expression $P'$ such that $P \stackrel{w}{\longrightarrow} P' \not\rightarrow$ (where $P' \not\rightarrow$ means that there exist no $a \in \mathcal{A}$ and process expression $P''$ such that $P' \stackrel{a}{\longrightarrow} P''$). The next counterexample, which employs the distinction between successful and unsuccessful termination characteristic of ACP-like theories, shows that in our setting this restriction is not enough.

**Example 4.4** Let $a$ be an action; then $a$, $[a + a \cdot \delta]$ and $[a \cdot \delta + \varepsilon]$ are indecomposable elements of $\mathcal{P}/\leftrightarrows$. Moreover, $a \not\leftrightarrows a + a \cdot \delta$ (the transition $a + a \cdot \delta \stackrel{a}{\longrightarrow} \delta$ cannot be simulated by $a$). However, it is easily verified that

$$a \| (a \cdot \delta + \varepsilon) \leftrightarrows (a + a \cdot \delta) \| (a \cdot \delta + \varepsilon) \ ,$$

so a decomposition in $\mathcal{P}/\leftrightarrows$ need not be unique.

To eliminate the obstructions to a unique decomposition theorem illustrated by Examples 4.3 and 4.4, we use the following definition.

**Definition 4.5** A process expression $P$ is *weakly normed* if there exist $w \in \mathcal{A}^*$ and a process expression $P'$ such that

$$P \stackrel{w}{\longrightarrow} P' \leftrightarrows \varepsilon \ .$$

The set of weakly normed process expressions is denoted by $\mathcal{P}_{wn}$.

Bisimulation respects the property of being weakly normed and $\|$ preserves it.

**Lemma 4.6** Let $P$ and $Q$ be process expressions;

(i) $P \| Q$ is weakly normed iff $P$ and $Q$ are weakly normed; and

(ii) if $P \leftrightarrows Q$ and $P$ is weakly normed, then also $Q$ is weakly normed.

*Proof.* If $P \| Q \stackrel{w}{\longrightarrow} R \leftrightarrows \varepsilon$, then with induction on the length of the sequence $w$ it can be shown that there exist $u$, $v$, $P'$ and $Q'$ such that $R = P' \| Q'$, $P \stackrel{u}{\longrightarrow} P'$ and $Q \stackrel{v}{\longrightarrow} Q'$ (cf. also Lemma 4.10 where a stronger property is proved); clearly, $P' \| Q' \leftrightarrows R \leftrightarrows \varepsilon$ implies that $P' \leftrightarrows \varepsilon$ and $Q' \leftrightarrows \varepsilon$. On the other hand, if $P \stackrel{v}{\longrightarrow} P' \leftrightarrows \varepsilon$ and $Q \stackrel{w}{\longrightarrow} Q' \leftrightarrows \varepsilon$, then $P \| Q \stackrel{vw}{\longrightarrow} P' \| Q' \leftrightarrows \varepsilon$. The proof of the first part of the lemma is complete. If $P \leftrightarrows Q$ and $P \stackrel{w}{\longrightarrow} P'$, then there exists $Q'$ such that $Q \stackrel{w}{\longrightarrow} Q'$ and $P' \leftrightarrows Q'$. It follows that if $P \stackrel{w}{\longrightarrow} P' \leftrightarrows \varepsilon$, then $Q \stackrel{w}{\longrightarrow} Q' \leftrightarrows \varepsilon$; this proves the second part. $\square$

The following proposition is an immediate consequence of the above lemma.

**Proposition 4.7** $\mathcal{P}_{wn}/\hspace{-0.3em}\leftrightarrow$ is a (commutative) submonoid of $\mathcal{P}/\hspace{-0.3em}\leftrightarrow$.

Christensen et al. [7] prove that every element of the commutative monoid of weakly normed BPP expressions[2] modulo bisimulation has a unique decomposition. Presupposing a communication function $\gamma$ that is everywhere undefined, the operational semantics for BPP expressions is as given in Table 1. So, in BPP there is no communication between parallel components. Christensen [6] extends this result to a unique decomposition theorem for the commutative monoid of weakly normed $\mathsf{BPP}_\tau$ expressions modulo bisimulation. His $\mathsf{BPP}_\tau$ is obtained by replacing the parallel operator of BPP by a parallel operator that allows a restricted form of handshaking communication. Our next example shows that the more general communication mechanism of $\mathsf{ACP}^\varepsilon$ gives rise to weakly normed process expressions without a decomposition.

**Example 4.8** Let $a$ be an action, suppose that $a = \gamma(a, a)$ and

$$X \stackrel{\text{def}}{=} a \cdot X + a.$$

Suppose that $X \leftrightarrow P_1 \parallel \cdots \parallel P_n$. Since $X \not\leftrightarrow \varepsilon$, there exists $i \in \{1, \ldots, n\}$ such that $P_i \not\leftrightarrow \varepsilon$. Hence, since $P \parallel \varepsilon \leftrightarrow \varepsilon \parallel P \leftrightarrow P$, we may assume without loss of generality that $P_i \not\leftrightarrow \varepsilon$ for all $1 \leq i \leq n$. Note that $X$ has two transitions: $X \xrightarrow{a} \varepsilon$ and $X \xrightarrow{a} X$. Since $P'_1 \parallel \cdots \parallel P'_n \leftrightarrow \varepsilon$ only if $P'_i \leftrightarrow \varepsilon$ for all $1 \leq i \leq n$, the transition $X \xrightarrow{a} \varepsilon$ can only be simulated by $P_1 \parallel \cdots \parallel P_n$ if there exist $a_1, \ldots, a_n \in \mathcal{A}$ and $P'_1, \ldots, P'_n$ such that $a = \gamma(a_1, \ldots, a_n)$ and $P_i \xrightarrow{a_i} P'_i \leftrightarrow \varepsilon$ for all $1 \leq i \leq n$. So

$$P_1 \parallel \cdots \parallel P_n \xrightarrow{a_1} P'_1 \parallel P_2 \parallel \cdots \parallel P_n \xrightarrow{a_2} \ldots \xrightarrow{a_{n-1}} P'_1 \parallel \cdots \parallel P'_{n-1} \parallel P_n,$$

and hence, by induction on $n \geq 1$, it follows that $P_i \parallel \cdots \parallel P_n \leftrightarrow X$ for all $1 \leq i \leq n$. In particular, we have now shown that $X \leftrightarrow P_1 \parallel \cdots \parallel P_n$ implies that $P_n \leftrightarrow X$, and by a similar argument as in Example 4.3 it follows that $[X]$ has no decomposition in $\mathcal{P}/\hspace{-0.3em}\leftrightarrow$.

The communication function in the above example allows an unbounded number of copies of the action $a$ to participate in a single communication. To exclude this phenomenon, we use the following definition.

**Definition 4.9** A communication function $\gamma$ is *linear* if every action can be assigned a *weight* $\geq 1$ in such a way that $a = \gamma(b, c)$ implies that the weight of $a$ is the sum of the weights of $b$ and $c$.

Note that, since $i \geq 1$ implies $i \neq i + i$, the communication function in Example 4.8 is not linear.

Henceforth, we shall assume that the presupposed communication function $\gamma$ is linear and that every action has a weight assigned to it (cf. Definition 4.9). We use it to define the *weighted length* $\ell(w)$ of $w \in \mathcal{A}^*$ inductively as follows:

(i) if $w$ is the empty sequence, then $\ell(w) = 0$; and

(ii) if $w = w'a$ and $a$ is an action of weight $i$, then $\ell(w) = \ell(w') + i$.

---

[2] BPP is the subtheory of $\mathsf{ACP}^\varepsilon$ in which process expressions are generated by the restricted syntax $P ::= \varepsilon \mid X \mid a \cdot P \mid P + P \mid P \parallel P$.

This definition takes into account that a communication stands for the simultaneous execution of multiple actions. It allows us to formulate the following crucial property of the operational semantics of $\mathsf{ACP}^\varepsilon$.

**Lemma 4.10** If $P$, $Q$ and $R$ are process expressions such that $P \parallel Q \xrightarrow{w} R$, then there exist $P', Q'$ and $u, v \in \mathcal{A}^*$ such that

$$R = P' \parallel Q', \ P \xrightarrow{u} P', \ Q \xrightarrow{v} Q' \text{ and } \ell(u) + \ell(v) = \ell(w).$$

*Proof.* We prove this lemma by induction on the weighted length of $w$.

If $\ell(w) = 0$, then $w$ is the empty sequence, whence $R = P \parallel Q$. It follows that $P \xrightarrow{w} P$, $Q \xrightarrow{w} Q$, and $\ell(w) + \ell(w) = \ell(w)$.

If $\ell(w) > 0$, then there exist $w' \in \mathcal{A}^*$, $a \in \mathcal{A}$ and $R^\dagger$ such that $w = w'a$ and

$$P \parallel Q \xrightarrow{w'} R^\dagger \xrightarrow{a} R.$$

Furthermore, by the induction hypothesis, there exist $P^\dagger, Q^\dagger$ and $u, v \in \mathcal{A}^*$ such that

$$R^\dagger = P^\dagger \parallel Q^\dagger, \ P \xrightarrow{u} P^\dagger, \ Q \xrightarrow{v} Q^\dagger \text{ and } \ell(u) + \ell(v) = \ell(w').$$

Now an inspection of the rules in Table 1 reveals that the transition $P^\dagger \parallel Q^\dagger \xrightarrow{a} R$ may come about in three ways:

1. If $R = P' \parallel Q^\dagger$ with $P^\dagger \xrightarrow{a} P'$, then $P \xrightarrow{ua} P'$ and, denoting by $i$ the weight of $a$,

   $$\ell(ua) + \ell(v) = \ell(u) + \ell(v) + i = \ell(w') + i = \ell(w).$$

2. If $R = P^\dagger \parallel Q'$ with $Q^\dagger \xrightarrow{a} Q'$, then $Q \xrightarrow{va} Q'$, and $\ell(u) + \ell(va) = \ell(w)$ is obtained as in the previous case.

3. Suppose that $R = P' \parallel Q'$ with $P^\dagger \xrightarrow{b} P'$, $Q^\dagger \xrightarrow{c} Q'$ and $a = \gamma(b, c)$. We then have that $P \xrightarrow{ub} P'$ and $Q \xrightarrow{vc} Q'$, so it remains to establish that $\ell(ub) + \ell(vc) = \ell(w)$. Let $i$, $j$ and $k$ be the weights of $a$, $b$ and $c$, respectively; then, since $i = j + k$,

   $$\ell(ub) + \ell(vc) = \ell(u) + \ell(v) + j + k = \ell(w') + i = \ell(w).$$

The proof of the lemma is now complete. $\qquad\qquad\square$

## 4.3 Unique decomposition in $\mathcal{P}_{wn}/\leftrightarrow$

We now prove that every element of the commutative monoid $\mathcal{P}_{wn}/\leftrightarrow$ of weakly normed process expressions modulo bisimulation has a unique decomposition, provided that the communication function is linear. We proceed by defining a reduction relation $\rightarrowtail$ on $\mathcal{P}_{wn}$, derived from the transition relation, that induces a decomposition order on $\mathcal{P}_{wn}/\leftrightarrow$. Then, it may be concluded from Theorem 3.13 that every element of $\mathcal{P}_{wn}/\leftrightarrow$ has a unique decomposition.

**Definition 4.11** The *norm* $|P|$ of a weakly normed process expression is the least natural number $n$ such that there exists $w \in \mathcal{A}^*$ of weighted length $n$ and a process expression $P'$ such that $P \xrightarrow{w} P' \leftrightarrow \varepsilon$, i.e.,

$$|P| = \min\{\ell(w) : \text{there exists } P' \text{ such that } P \xrightarrow{w} P' \leftrightarrow \varepsilon\}.$$

We define on $\mathcal{P}_{wn}$ a *reduction relation* $\rightarrowtail$ by

$$P \rightarrowtail Q \Longleftrightarrow \text{there exists } a \in \mathcal{A} \text{ of weight } i \text{ s.t. } P \xrightarrow{a} Q \text{ and } |P| = |Q| + i.$$

We denote by $\rightarrowtail^+$ the transitive closure of $\rightarrowtail$ and by $\rightarrowtail^*$ the reflexive-transitive closure of $\rightarrowtail$. Since $P \rightarrowtail Q$ implies $|P| > |Q|$, it follows that $\rightarrowtail^*$ is antisymmetric, so it is a partial order on $\mathcal{P}_{wn}$, and $\rightarrowtail^+$ is the associated strict partial order. We establish that the inverse of $\rightarrowtail^*$ has all the properties of a decomposition order up to bisimulation. To that end we first establish that it is a partial order.

**Lemma 4.12** If $P \leftrightarroweq Q$, then $|P| = |Q|$ for all $P, Q \in \mathcal{P}_{wn}$.

*Proof.*    If $P \leftrightarroweq Q$ and $P \xrightarrow{w} P'$, then there exists $Q'$ such that $Q \xrightarrow{w} Q'$ and $P' \leftrightarroweq Q'$. It follows that if $P \xrightarrow{w} P' \leftrightarroweq \varepsilon$, then $Q \xrightarrow{w} Q' \leftrightarroweq \varepsilon$, so $|Q| \leq |P|$. Similarly, $|P| \leq |Q|$.    □

**Lemma 4.13** If $P \rightarrowtail^* Q$, then for all $P' \leftrightarroweq P$ there exists $Q' \leftrightarroweq Q$ such that $P' \rightarrowtail^* Q'$.

*Proof.*    First consider the special case that $P \rightarrowtail Q$. Then there exists $a \in \mathcal{A}$ of weight $i$ such that $P \xrightarrow{a} Q$ and $|P| = |Q| + i$. If $P' \leftrightarroweq P$, then according to the definition of bisimulation (Definition 4.1) there exists $Q' \leftrightarroweq Q$ such that $P' \xrightarrow{a} Q'$. By Lemma 4.12 $|P'| = |P| = |Q| + i = |Q'| + i$, so $P' \rightarrowtail Q'$. Thereby, this special case of the lemma is proved, and the general follows easily with induction on the length of the reduction $P \rightarrowtail^* Q$.    □

**Definition 4.14** We denote by $\preccurlyeq$ the partial order on $\mathcal{P}_{wn}/\leftrightarroweq$ defined by

$$[P] \preccurlyeq [Q] \Longleftrightarrow \text{there exist } P' \text{ and } Q' \text{ such that } Q \leftrightarroweq Q' \rightarrowtail^* P' \leftrightarroweq P.$$

Using Lemma 4.13 for transitivity, it is straightforward to verify that $\preccurlyeq$ indeed is a partial order on weakly normed process expressions. After establishing a technical lemma, we proceed by verifying each of the conditions required for $\preccurlyeq$ to be a decomposition order on $\mathcal{P}_{wn}/\leftrightarroweq$. The verifications will be performed for $\rightarrowtail^*$ on process expressions, which will then be extended to process expressions up to bisimulation in the proof that $\preccurlyeq$ is a decomposition order (Theorem 4.21).

**Lemma 4.15** $|P \parallel Q| = |P| + |Q|$ for all $P, Q \in \mathcal{P}_{wn}$.

*Proof.*    Note that if $P \xrightarrow{v} P' \leftrightarroweq \varepsilon$ and $Q \xrightarrow{w} Q' \leftrightarroweq \varepsilon$, then $P \parallel Q \xrightarrow{vw} P' \parallel Q' \leftrightarroweq \varepsilon$; it follows that $|P \parallel Q| \leq |P| + |Q|$.

On the other hand, if $P \parallel Q \xrightarrow{w} R \leftrightarroweq \varepsilon$ and $|P \parallel Q| = \ell(w)$, then by Lemma 4.10 there exist $P', Q' \in \mathcal{P}_{wn}$ and $u, v \in \mathcal{A}^*$ such that $R = P' \parallel Q'$, $P \xrightarrow{u} P'$, $Q \xrightarrow{v} Q'$ and $\ell(u) + \ell(v) = \ell(w)$. Clearly, if $P' \parallel Q' \leftrightarroweq \varepsilon$, then both $P' \leftrightarroweq \varepsilon$ and $Q' \leftrightarroweq \varepsilon$, so $P \xrightarrow{u} P' \leftrightarroweq \varepsilon$ and $Q \xrightarrow{v} Q' \leftrightarroweq \varepsilon$. It follows that $|P| + |Q| \leq |P \parallel Q|$, so the proof of the lemma is complete.    □

**Proposition 4.16 (Well-founded)** The inverse of the relation $\rightarrowtail^*$ is well-founded.

*Proof.*    The elements of minimal norm in a nonempty subset of $\mathcal{P}_{wn}$ are $\rightarrowtail^*$-maximal.    □

**Proposition 4.17 (Least element)** For every $P$ there is a $P'$ such that $P \rightarrowtail^* P' \leftrightarroweq \varepsilon$.

*Proof.*    Note that if $P \in \mathcal{P}_{wn}$, then there exist $w \in \mathcal{A}^*$ and $P' \in \mathcal{P}_{wn}$ such that $P \xrightarrow{w} P' \leftrightarroweq \varepsilon$ and $|P| = \ell(w)$. We prove by induction on $\ell(w)$ that if $|P| = \ell(w)$ and $P \xrightarrow{w} P' \leftrightarroweq \varepsilon$, then $P \rightarrowtail^* P' \leftrightarroweq \varepsilon$.

If $\ell(w) = 0$, then $w$ is the empty sequence and hence $P = P' \leftrightarroweq \varepsilon$.

Suppose that $\ell(w) > 0$, then there exists $a \in \mathcal{A}$, say of weight $i$, such that $w = aw'$ and $P \xrightarrow{a} Q \xrightarrow{w'} P' \leftrightarroweq \varepsilon$. It follows from the definition of norm that $|Q| = \ell(w')$; for if $|Q| < \ell(w')$, then there exist $w'' \in \mathcal{A}^*$ and $Q' \in \mathcal{P}_{wn}$ such that $P \xrightarrow{a} Q \xrightarrow{w''} Q' \leftrightarroweq \varepsilon$ and $\ell(aw'') < \ell(w)$ contradicting $\ell(w) = |P|$. So by the induction hypothesis $Q \rightarrowtail^* P' \leftrightarroweq \varepsilon$. Moreover, $|P| = |Q| + i$, so $P \rightarrowtail Q$. Hence, $P \rightarrowtail^* P' \leftrightarroweq \varepsilon$. $\square$

**Proposition 4.18 (Strictly compatible)** If $P \rightarrowtail^+ Q$, then $P \parallel R \rightarrowtail^+ Q \parallel R$.

*Proof.*    First consider the special case that $P \rightarrowtail Q$. Then there exists $a$, say of weight $i$, such that $P \xrightarrow{a} Q$ and $|P| = |Q| + i$. From $P \xrightarrow{a} Q$ it follows that $P \parallel R \xrightarrow{a} Q \parallel R$, and by Lemma 4.15 $|P \parallel R| = |P| + |R| = |Q| + |R| + i = |Q \parallel R| + i$. So $P \parallel R \rightarrowtail Q \parallel R$. The general case now follows by induction on the length of the reduction $P \rightarrowtail^+ Q$. $\square$

**Proposition 4.19 (Precompositional)** If $P \parallel Q \rightarrowtail^* R$, then there exist $P'$ and $Q'$ such that

$$P \rightarrowtail^* P', \ Q \rightarrowtail^* Q' \text{ and } R = P' \parallel Q'.$$

*Proof.*    We prove the lemma by induction on $|P \parallel Q| - |R|$. If $P \parallel Q = R$, then the lemma holds trivially. Otherwise, there exists a process expression $R'$ such that $P \parallel Q \rightarrowtail^* R' \rightarrowtail R$ and $|R'| - |R| = \ell(a)$. Since $|R'| > |R|$, there exist by the induction hypothesis $P'$ and $Q'$ such that $P \rightarrowtail^* P'$, $Q \rightarrowtail^* Q'$ and $R' = P' \parallel Q'$. Furthermore, since $R' \rightarrowtail R$, there exists $a \in \mathcal{A}$ such that $|P' \parallel Q'| = |R| + \ell(a)$ and $P' \parallel Q' \xrightarrow{a} R$. Inspection of the rules in Table 1 reveals that the latter transition may come about in three ways:

1. $R = P'' \parallel Q'$ and $P' \xrightarrow{a} P''$: Then by Lemma 4.15

$$|P'| = |P' \parallel Q'| - |Q'| = |P'' \parallel Q'| - |Q'| + \ell(a) = |P''| + \ell(a),$$

   so $P' \rightarrowtail P''$.

2. $R = P' \parallel Q''$ and $Q' \xrightarrow{a} Q''$: Then by Lemma 4.15

$$|Q'| = |P' \parallel Q'| - |P'| = |P' \parallel Q''| - |P'| + \ell(a) = |Q''| + \ell(a),$$

   so $Q' \rightarrowtail Q''$.

3. $R = P'' \parallel Q''$, $P' \xrightarrow{b} P''$, $Q' \xrightarrow{c} Q''$ and $a = \gamma(b, c)$: Then by Lemma 4.15

$$|P'| + |Q'| = |P' \parallel Q'| = |P'' \parallel Q''| + \ell(a) = |P''| + \ell(b) + |Q''| + \ell(c).$$

   Furthermore, note that $|P'| \leq |P''| + \ell(b)$ and $|Q'| \leq |Q''| + \ell(c)$, so it follows that $|P'| = |P''| + \ell(b)$ and $|Q'| = |Q''| + \ell(c)$. Hence, $P' \rightarrowtail P''$ and $Q' \rightarrowtail Q''$.

The proof of the lemma is complete. $\square$

**Proposition 4.20 (Archimedean)** Let $P, Q \in \mathcal{P}_{wn}$ and let $Q_0, Q_1, Q_2, \ldots$ be a sequence of weakly normed process expressions such that $Q_0 \leftrightarrow \varepsilon$ and $Q_{n+1} \leftrightarrow Q_n \parallel Q$ for all $n \geq 0$ (i.e., each $Q_n$ is bisimilar to the parallel composition of $n$ copies of $Q$). If $P \rightarrowtail^+ Q_n$ for all $n \in \mathbf{N}$, then $Q \leftrightarrow \varepsilon$.

*Proof.* Note that by Lemma 4.15 and Lemma 4.12 $|Q_n| = n|Q|$. Since $P \rightarrowtail^+ Q_n$ for every $n \in \mathbf{N}$, it follows that $|P| > n|Q|$ for all $n \in \mathbf{N}$. So $|Q| = 0$, and hence $Q \leftrightarrow \varepsilon$. $\square$

**Theorem 4.21** The partial order $\preccurlyeq$ is a decomposition order on $\mathcal{P}_{wn}/\!\leftrightarrow$.

*Proof.* To see that $\preccurlyeq$ is well-founded, consider a nonempty subset $X$ of $\mathcal{P}_{wn}/\!\leftrightarrow$. By Proposition 4.16 $\bigcup X$ has a $\rightarrowtail^*$-maximal element $P$; we verify that $[P]$ is a $\preccurlyeq$-minimal element of $X$. For this it suffices to establish that $[Q] \preccurlyeq [P]$ implies $[P] = [Q]$ for all $Q$. If $[Q] \preccurlyeq [P]$, then there exist $P'$ and $Q'$ such that $P \leftrightarrow P' \rightarrowtail^* Q' \leftrightarrow Q$. Hence, by Lemma 4.13 there exists $Q''$ such that $P \rightarrowtail^* Q'' \leftrightarrow Q$, and since $P$ is $\rightarrowtail^*$-maximal it follows that $P = Q'' \leftrightarrow Q$, so $[P] = [Q]$.

That $[\varepsilon]$ is the least element of $\mathcal{P}_{wn}/\!\leftrightarrow$ with respect to $\preccurlyeq$ follows from Proposition 4.17.

To see that $\preccurlyeq$ is strictly compatible, suppose that $[P] \prec [Q]$; then there exist $P'$ and $Q'$ such that

$$Q \leftrightarrow Q' \rightarrowtail^+ P' \leftrightarrow P.$$

By Proposition 4.18 and since $\leftrightarrow$ is a congruence it follows that

$$Q \parallel R \leftrightarrow Q' \parallel R \rightarrowtail^+ P' \parallel R \leftrightarrow P \parallel R.$$

So $[P] \parallel [R] = [P \parallel R] \prec [Q \parallel R] = [Q] \parallel [R]$.

To see that $\preccurlyeq$ is precompositional, suppose that $[P] \preccurlyeq [Q] \parallel [R]$; then there exists a $P'$ such that

$$Q \parallel R \rightarrowtail^* P' \leftrightarrow P.$$

By Proposition 4.19 there exist $Q'$ and $R'$ such that $Q \rightarrowtail^* Q'$, $R \rightarrowtail^* R'$ and $P' = Q' \parallel R'$. Hence, $[P] = [P'] = [Q'] \parallel [R']$ with $[Q'] \preccurlyeq [Q]$ and $[R'] \preccurlyeq [R]$.

That $\preccurlyeq$ is Archimedean, is immediate by Proposition 4.20. $\square$

**Corollary 4.22** The commutative monoid $\mathcal{P}_{wn}/\!\leftrightarrow$ has unique decomposition, provided that the communication function $\gamma$ is linear.

**Remark 4.23** Note that the decomposition order $\preccurlyeq$ on $\mathcal{P}/\!\leftrightarrow$ is not the natural decomposition order associated with $\mathcal{P}/\!\leftrightarrow$. Whereas distinct indecomposable elements are always incomparable with respect to the natural decomposition order, they need not be incomparable with respect to $\preccurlyeq$. For instance, if $a$ and $b$ are distinct actions, then $[a \cdot b]$ and $[b]$ are distinct indecomposable elements of $\mathcal{P}/\!\leftrightarrow$ and $[b] \preccurlyeq [a \cdot b]$.

# 5  Commutative Residual Algebras

We shall now illustrate our main theorem by using it to establish a unique decomposition theorem for commutative residual algebras (CRAs). CRAs are designed to enable algebraic reasoning about multisets, and the unique decomposition result yields the satisfying situation that any well-founded CRA is isomorphic to a CRA having multisets as elements (Corollary 5.16), i.e., that elements of well-founded CRAs *are* multisets. We proceed as

follows. First we present CRAs and the natural order for them. Then, we show how to associate a partial commutative monoid to any CRA in a natural way. For a well-founded CRA its associated monoid has unique decomposition entailing that the CRA itself is isomorphic to a CRA of multisets.

**Remark 5.1** For the case of finite CRAs the isomorphism was due to Visser. Recently, we found that CRAs are equivalent to commutative BCK-algebras with relative cancellation,[3] and both isomorphisms are entailed by the representation theorem of [10] for the class of *all* CRAs. Nevertheless, the present section illustrates well how to apply our unique decomposition theorem to classes of algebras, by reasoning directly with the axioms of CRAs.

**Definition 5.2** A *commutative residual algebra* $(A, -, 0)$ consists of a set $A$ with a distinguished element 0 and a binary operation $- : A \times A \to A$ such that for all $x, y, z \in A$:

$$x - 0 = x \tag{cra1}$$
$$x - x = 0 \tag{cra2}$$
$$0 - x = 0 \tag{cra3}$$
$$(x - y) - (z - y) = (x - z) - (y - z) \tag{cra4}$$
$$(x - y) - x = 0 \tag{cra5}$$
$$x - (x - y) = y - (y - x). \tag{cra6}$$

Note that (cra2) and (cra3) are superfluous. To derive (cra2), first apply (cra5) with $y = 0$ to the right-hand side and then apply (cra1). To derive (cra3), first apply (cra5) with $y = x$ to the right-hand side and then apply (cra2) (alternatively, see [26, Remark 8.7.3]).

We present three examples of CRAs, which will be shown to give rise to the three partial commutative monoids of Example 2.3.

**Example 5.3**  1. Natural numbers with cut-off subtraction and zero constitute a CRA.

2. Positive natural numbers with cut-off division and one constitute a CRA, where cut-off division $\div$ is defined for positive natural numbers $m$ and $n$ by

$$m \div n = \frac{m}{\gcd(m, n)}$$

(where $\gcd(m, n)$ denotes the greatest common divisor of $m$ and $n$). For instance, $12 \div 15 = \frac{12}{3} = 4$ and $15 \div 12 = \frac{15}{3} = 5$.

3. Multisets with multiset difference and the empty multiset constitute a CRA.

For the remainder, we fix a commutative residual algebra $(A, -, 0)$. There is a natural partial order associated with it: let $\preccurlyeq$ be the binary relation on $A$ defined by

$$x \preccurlyeq y \text{ iff } x - y = 0. \tag{7}$$

**Lemma 5.4** $\preccurlyeq$ is a partial order.

---

[3]For more on the connexion, see [24].

*Proof.* That $\preccurlyeq$ is reflexive is immediate from (cra2).

To prove that $\preccurlyeq$ is transitive, suppose that $x \preccurlyeq y$ and $y \preccurlyeq z$. Then, from $y - z = 0$ it follows by (cra1) that $x - z = (x - z) - (y - z)$, and from $x - y = 0$ it follows by (cra3) that $0 = (x - y) - (z - y)$. Hence, by (cra4) $x - z = 0$, so $x \preccurlyeq z$.

To prove that $\preccurlyeq$ is antisymmetric, suppose that $x \preccurlyeq y$ and $y \preccurlyeq x$. Then $x - y = 0$ and $y - x = 0$. By (cra1) it follows that $x = x - (x - y)$ and $y = y - (y - x)$, and the right-hand sides are equated by (cra6), so $x = y$. $\square$

A CRA is said to be *well-founded* if its natural order is. The natural orders for the three CRAs of Example 5.3 are the less-than-or-equal relation, the divisibility relation, and the submultiset relation respectively, so all three CRAs are well-founded. Note that these orders correspond exactly to the decomposition orders for their associated partial commutative monoids, as presented in Example 3.3. This is no coincidence: to any CRA a partial commutative monoid can be associated such that the natural order of the former coincides with the divisibility relation of the latter. The *addition* $x + y$ of two elements of the CRA should obviously satisfy that $x$ is below it and that $y$ is the residual of it after $x$ (cf. [10]):

$$x \preccurlyeq x + y \tag{8}$$
$$(x + y) - x = y \ . \tag{9}$$

The following lemma entails that if an element $x + y$ satisfying (8) and (9) exists then it is unique, making $+$ into a partial binary operation on $A$, in other words, making $(A, +)$ into an *add* in the sense of [2].

**Lemma 5.5 (Relative cancellation)** If $x \preccurlyeq y, z$ and $y - x = z - x$, then $y = z$.

*Proof.* If $x \preccurlyeq y, z$, then $x - y = 0$ and $x - z = 0$.

From $x - z = 0$ it follows by (cra1) that $y - z = (y - z) - (x - z)$, and from $y - x = z - x$ it follows by (cra2) that $0 = (y - x) - (z - x)$. Hence, by (cra4) $y - z = 0$, so $y \preccurlyeq z$.

Similarly, from $x - y = 0$ and $z - x = y - x$ it follows that $z \preccurlyeq y$. Hence, by Lemma 5.4 $y = z$. $\square$

In order to establish that $(A, +, 0)$ is a partial commutative monoid, we need to verify that the associativity, commutativity, and identity axioms hold for it. We first establish the identity axiom.

**Lemma 5.6** $x + 0 \simeq 0 + x \simeq x$.

*Proof.* Note that $x \preccurlyeq x$ by Lemma 5.4 and $x - x = 0$ by (cra2), so $x$ satisfies the defining conditions (8) and (9) of $x + 0$, and hence $x + 0 = x$. On the other hand, note that $0 \preccurlyeq x$ by (cra3), and $x - 0 = x$ by (cra3), so $x$ also satisfies the defining conditions (8) and (9) of $0 + x$, and hence $0 + x = x$. $\square$

The associativity and commutativity axioms are entailed by two lemmas which are interesting in their own right. The first explains how subtraction distributes over addition. The second expresses commutativity of max defined by $x \max y = x + (y - x)$. For the CRAs of Example 5.3, max corresponds to maximum, least common multiple, and multiset union, respectively.

**Lemma 5.7 (Distributivity)** If $x + y$ is defined, then

$$z - (x + y) = (z - x) - y \tag{cra7}$$
$$(x + y) - z = (x - z) + (y - (z - x)). \tag{cra8}$$

*Proof.* If $x + y$ is defined, then (*) $x - (x + y) = 0$ and (**) $(x + y) - x = y$.
Then (cra7) is derived as follows:

$$\begin{aligned}
z - (x + y) &= (z - (x + y)) - 0 && \text{by (cra1)} \\
&= (z - (x + y)) - (x - (x + y)) && \text{by (*)} \\
&= (z - x) - ((x + y) - x) && \text{by (cra4)} \\
&= (z - x) - y && \text{by (**).}
\end{aligned}$$

For (cra8), we show that the right-hand side sum exists and is equal to the left-hand side by demonstrating that the left-hand side satisfies the defining conditions (8) and (9) for the right-hand side sum. Note that $x - z \preccurlyeq (x + y) - z$ is established by

$$\begin{aligned}
(x - z) - ((x + y) - z) &= (x - (x + y)) - (z - (x + y)) && \text{by (cra4)} \\
&= 0 - (z - (x + y)) && \text{by (*)} \\
&= 0 && \text{by (cra3),}
\end{aligned}$$

and that

$$\begin{aligned}
((x + y) - z) - (x - z) &= ((x + y) - x) - (z - x) && \text{by (cra4)} \\
&= y - (z - x) && \text{by (**).}
\end{aligned}$$

So (cra8) follows by Lemma 5.5. $\qquad\square$

**Lemma 5.8** (max-**commutativity**) $x + (y - x) \simeq y + (x - y)$.

*Proof.* Suppose that $x + (y - x)$ is defined; then on the one hand

$$\begin{aligned}
y - (x + (y - x)) &= (y - x) - (y - x) && \text{by (cra7)} \\
&= 0 && \text{by (cra2),}
\end{aligned}$$

and, on the other hand,

$$\begin{aligned}
(x + (y - x)) - y &= (x - y) + ((y - x) - (y - x)) && \text{by (cra8)} \\
&= (x - y) + 0 && \text{by (cra2)} \\
&= x - y && \text{by (cra2),}
\end{aligned}$$

so $y + (x - y)$ is also defined and $x + (y - x) = y + (x - y)$.

By a symmetric argument it can be established that if $y + (x - y)$ is defined, then $x + (y - x)$ is also defined and $x + (y - x) = y + (x - y)$. Thereby, the lemma is proved. $\qquad\square$

**Proposition 5.9** $(A, +, 0)$ is a partial commutative monoid.

*Proof.* Since we already know that $+$ is a partial binary operation on $A$, it remains to prove that $+$ is associative and commutative, and that $0$ is the identity element for $+$. These are established in reverse order.

By Lemma 5.6 $0$ is the identity element for $+$.

To prove that $+$ is commutative, suppose that $x + y$ is defined. Then by (cra7) and (cra5) $y - (x + y) = (y - x) - y = 0$, whence $y \preccurlyeq (x + y)$, and

$$\begin{aligned}
(x + y) - y &= (x - y) + (y - (y - x)) && \text{by (cra8)} \\
&= (x - y) + (x - (x - y)) && \text{by (cra6)} \\
&= x + ((x - y) - x) && \text{by Lemma 5.8} \\
&= x + 0 && \text{by (cra5)} \\
&= x
\end{aligned}$$

where the last equality holds by $0$ being the identity. The argument is symmetric in $x$ and $y$, so it follows that $+$ is commutative.

To prove that $+$ is associative, we first show that

$$\text{if } (x+y)+z \text{ is defined, then } (x+y)+z = x+(y+z). \tag{10}$$

Suppose that $(x+y)+z$ is defined. Then

$$
\begin{aligned}
x - ((x+y)+z) &= ((x-x)-y)-z &&\text{by (cra7) twice} \\
&= (0-y)-z &&\text{by (cra2)} \\
&= 0 &&\text{by (cra3),}
\end{aligned}
$$

whence $x \preccurlyeq (x+y)+z$ and, since $x+y$ is defined too, (*) $x-(x+y)=0$ and (**) $(x+y)-x=y$, so

$$
\begin{aligned}
((x+y)+z)-x &= ((x+y)-x)+(z-(x-(x+y))) &&\text{by (cra8)} \\
&= y+(z-0) &&\text{by (*), (**)} \\
&= y+z &&\text{by (cra1).}
\end{aligned}
$$

Next, suppose that $x+(y+z)$ is defined; apply the commutative law to both occurrences of $+$ in this term, then apply (10) and commute back; this yields $(x+y)+z$. $\square$

The partial commutative monoids associated with the CRAs of Example 5.3 are the ones of Example 2.3. Note that addition is in fact total for each of them. In general this need not be the case, as witnessed by undefinedness of $1+1$ in the partial commutative monoid associated with the CRA of bits with cut-off subtraction (which is isomorphic to the CRA $(B, \leftarrow, \top)$ of Booleans with reverse implication and true).

**Remark 5.10** An alternative route to establishing the above is to exploit the equivalence between CRAs and commutative BCK algebras with relative cancellation, and to go through the construction of the so-called *BCK-clan* of the latter; cf. [10, p. 161].

Except for commutativity, all of the above goes through for *residual algebras*, which are CRAs which need not be commutative, that is which need only satisfy axioms (cra1)–(cra4), and for their generalization to *residual systems*; cf. [26, Section 8.7.3].

Finally, we show that the partial commutative monoid associated with a well-founded CRA has unique decomposition, by first establishing that the natural order of the latter coincides with the divisibility relation of the former (cf. [26, Exercise 8.7.51]), which is then shown to be a decomposition order.

**Lemma 5.11** The partial order $\preccurlyeq$ is the divisibility relation of $(A, +, 0)$, i.e., for all $x, y \in A$:

$$x \preccurlyeq y \text{ iff there exists } y' \in A \text{ such that } x + y' = y.$$

*Proof.* Both implications are immediate from the definition of $+$, taking $y - x$ as witness for $y'$ for the implication from left to right. $\square$

**Theorem 5.12** If the partial order $\preccurlyeq$ is well-founded, then it is a decomposition order on $(A, +, 0)$.

*Proof.* By Corollary 3.18 it suffices to prove that $\preccurlyeq$ is strictly compatible and precompositional.

To show strict compatibility of $\preccurlyeq$, let $x \prec y$ and suppose $y + z$ exists. Then by Lemma 5.11, $x + y' = y$ for some $y'$, hence $y + z = (x + y') + z$ from which existence of $x + z$ follows using commutativity and associativity of $+$. Moreover, if $z + x$ and $z + y$ are defined then

$$(z + x) - (z + y) = (z - (z + y)) + (x - ((z + y) - z) = x - y,$$

so $x + z \prec y + z$ is equivalent to the assumption $x \prec y$, and we conclude.

If $x \preccurlyeq y + z$, then $x - (y + z) = 0$. Let $x' = (y + z) - x$, $y' = y - x'$ and $z' = z - (x' - y)$; we prove that $x = y' + z'$, $y' \preccurlyeq y$ and $z' \preccurlyeq z$. Note that the last two assertions are immediate by (cra5); the first assertion is proved by the following derivation:

$$
\begin{aligned}
x &= x - 0 && \text{by (cra1)} \\
&= x - (x - (y + z)) \\
&= (y + z) - x' && \text{by (cra6)} \\
&= y' + z' && \text{by (cra8).}
\end{aligned}
$$

This shows that $\preccurlyeq$ is precompositional. $\qquad\qquad\square$

**Remark 5.13** Note that (cra8) is the key fact employed to establish precompositionality; $x$ can be obtained by subtracting the difference $x'$ between $y + z$ and $x$ from the former, and by (cra8) this can be done by distributing $x'$ over the summands of $y + z$.

The theorem, together with our main result, Theorem 3.13, entails unique decomposition for partial commutative monoids associated with well-founded CRAs, and hence the desired representation theorem for the latter.

**Corollary 5.14** Let $(A, +, 0)$ be the partial commutative monoid associated with a commutative residual algebra. If its divisibility relation is well-founded, and in particular if $A$ is finite, then every element of $A$ has a unique decomposition in $(A, +, 0)$.

**Remark 5.15** Unique decomposition can also be shown via the abstract account of the proof of the fundamental theorem of arithmetic as presented in Section 2.3, by verifying the conditions of Theorem 2.17:

(i) cancellation follows from $(x + z) - (y + z) = x - y$ as established in the proof of Theorem 5.12.

(ii) divisibility is well-founded since it coincides with $\preccurlyeq$ by Lemma 5.11, and

(iii) by Lemma 3.10 that indecomposable elements are prime is implied by precompositionality of divisibility, which may be established as in the proof of Theorem 5.12.

This proof illustrates the exchange as noted in the beginning of Section 3 (p. 11), between the conditions of decomposition orders (Definition 3.1) and those of the proof of the fundamental theorem of arithmetic (Theorem 2.17), in particular between strict compatibility and cancellation and between precompositionality and indecomposables being prime.

An element $x$ is an *atom* if $0 \prec x$ and $0 \prec y \preccurlyeq x$ implies $y = x$ for all $y$. Since the atoms of a CRA correspond to the indecomposables of its associated partial commutative monoid, the representation theorem follows.

**Corollary 5.16** Every well-founded CRA is isomorphic to a downward closed subalgebra of the multiset CRA on its atoms.

## Acknowledgements

## References

[1] L. Aceto and M. Hennessy. Towards action-refinement in process algebras. *Inform. and Comput.*, 103(2):204–269, 1993.

[2] R. Baer. Free sums of groups and their generalizations. An analysis of the associative law. *American Journal of Mathematics*, 71:706–742, 1949.

[3] J. C. M. Baeten and R. J. van Glabbeek. Merge and termination in process algebra. In K. V. Nori, editor, *Proc. of FST TCS 1987*, LNCS 287, pages 153–172, 1987.

[4] J. A. Bergstra and J. W. Klop. Process algebra for synchronous communication. *Information and Control*, 60(1–3):109–137, 1984.

[5] G. Birkhoff. *Lattice theory*, volume XXV of *American Mathematical Society Colloquium Publications*. American Mathematical Society, third edition, 1967.

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

[7] S. Christensen, Y. Hirshfeld, and F. Moller. Decomposability, decidability and axiomatisability for bisimulation equivalence on basic parallel processes. In *Proc. of LICS 1993*, pages 386–396. IEEE Computer Society Press, 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. Danet. The Riesz decomposition property for the space of regular operators. *Proceedings of the American Mathematical Society*, 129:539–542, 2001.

[10] A. Dvurečenskij and M. G. Graziano. Commutative BCK-algebras and lattice ordered groups. *Math. Japonica*, 49(2):159–174, 1999.

[11] W. J. Fokkink and S. P. Luttik. An $\omega$-complete equational specification of interleaving. In U. Montanari, J. D. P. Rolim, and E. Welzl, editors, *Proc. of ICALP 2000*, LNCS 1853, pages 729–743, 2000.

[12] L. Fuchs. *Partially Ordered Algebraic Systems*, volume 28 of *International Series of Monographs on Pure and Applied Mathematics*. Pergamon Press, 1963.

[13] G. Grätzer. *Universal algebra*. Springer-Verlag, second edition, 1979.

[14] J. F. Groote and F. Moller. Verification of parallel systems via decomposition. In *Proc. of CONCUR 1992*, LNCS 630, pages 62–76, Berlin, 1992. Springer.

[15] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford University Press, Oxford, Great Britain, fifth edition, 1979.

[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, *Proc. of ICALP 1999*, LNCS 1644, pages 412–421, 1999.

[17] S. C. Kleene. *Introduction to Metamathematics*. D. Van Nostrand Co., Inc., New York, N. Y., 1952.

[18] B. Luttik. A unique decomposition theorem for ordered monoids with applications in process theory. In Branislav Rovan and Peter Vojtás, editors, *Proceedings of MFCS 2003*, volume 2747 of *Lecture Notes in Computer Science*, pages 562–571, Bratislava, Slovak Republic, 2003. Springer-Verlag Heidelberg.

[19] G. McCusker. A fully abstract relational model of syntactic control of interference. In Julian C. Bradfield, editor, *Proceedings of CSL 2002*, volume 2471 of *Lecture Notes in Computer Science*, pages 247–261, Edinburgh, Scotland, 2002. Springer-Verlag Heidelberg.

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

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

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

[23] F. Moller. The importance of the left merge operator in process algebras. In M. S. Paterson, editor, *Proc. of ICALP 1990*, LNCS 443, pages 752–764, 1990.

[24] V. van Oostrom and A. Visser. Residual algebras. Forthcoming.

[25] D. Park. Concurrency and automata on infinite sequences. In P. Deussen, editor, *Proc. of the 5th GI Conference*, LNCS 104, pages 167–183, Karlsruhe, Germany, 1981. Springer-Verlag.

[26] Terese. *Term Rewriting Systems*, volume 55 of *Cambridge Tracts in Theoret. Comput. Sci.* Cambridge University Press, 2003.

[27] J. L. M. Vrancken. The algebra of communicating processes with empty process. *Theoret. Comput. Sci.*, 177:287–328, 1997.