A Unique Decomposition Theorem for Ordered Monoids with Applications in Process Theory
(Extended Abstract)

Bas Luttik

Dept. of Theoretical Computer Science, Vrije Universiteit Amsterdam
De Boelelaan 1081a, NL-1081 HV Amsterdam, The Netherlands
luttik@cs.vu.nl, http://www.cs.vu.nl/~luttik

Abstract. We prove a unique decomposition theorem for a class of ordered commutative monoids. Then, we use our theorem to establish that every weakly normed process definable in ACP^ε with bounded communication can be expressed as the parallel composition of a multiset of weakly normed parallel prime processes in exactly one way.

1   Introduction

The Fundamental Theorem of Arithmetic states that every element of the commutative monoid of positive natural numbers under multiplication has a unique decomposition (i.e., can be expressed as a product of prime numbers uniquely determined up to the order of the primes). It has been an invaluable tool in number theory ever since the days of Euclid. In the realm of process theory, unique decomposability with respect to parallel composition is crucial in the proofs that bisimulation is decidable for normed BPP [5] and normed PA [8]. It also plays an important rôle in the analysis of axiom systems involving an operation for parallel composition [1,6,12].

Milner and Moller [10] were the first to establish the unique decomposition property for a commutative monoid of finite processes with a simple operation for parallel composition. In [11], Moller presents an alternative proof of this result which he attributes to Milner; we shall henceforth refer to it as *Milner's technique*. 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 [10]. He refines Milner's technique twice. First, he adds communication to the operational semantics of the parallel operator. Then, he turns from strong bisimulation semantics to weak bisimulation semantics. Christensen [4] 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_τ expressions modulo strong bisimulation.

Milner's technique hinges on some special properties of the operational semantics of parallel composition. The main contribution of this paper is to place these properties in a general algebraic context. Milner's technique employs a well-founded subrelation of the transition relation induced on processes by the

operational semantics. We consider commutative monoids equipped with a well-founded partial order (rather than an arbitrary well-founded relation) to tie in with the theory of ordered monoids as put forward, e.g., in [3,7]. In Section 2 we propose a few simple conditions on ordered commutative monoids, and we prove that they imply the unique decomposition property (Theorem 13).

Then, to prove that a commutative monoid has the unique decomposition property, it suffices to define a partial order and establish that it satisfies our conditions. From Section 3 onwards, we illustrate this technique, discussing unique decomposability for the process theory ACP^ε [13]. ACP^ε is more expressive than any of the process theories for which unique decomposition was investigated previously. Firstly, it distinguishes two forms of termination (successful and unsuccessful). Secondly, it has a more general communication mechanism (an arbitrary number of parallel components may participate in a single communication, and communication not necessarily results in τ). These two features make the extension of Milner's technique to ACP^ε nontrivial; in fact, they both lead to counterexamples obstructing a general unique decomposition result (see Examples 16 and 19).

In Section 4 we introduce for ACP^ε an appropriate notion of weak normedness that takes into account the distinction between successful and unsuccessful termination, and we propose a requirement on the communication mechanism. In Section 5 we prove that if the communication mechanism meets the requirement, then the commutative monoid of weakly normed ACP^ε expressions modulo bisimulation satisfies the abstract specification of Section 2, and hence admits a unique decomposition theorem.

Whether or not a commutative monoid satisfies the conditions put forward in Section 2 is independent of the nature of its elements (be it natural numbers, bisimulation equivalence classes of process expressions, or objects of any other kind). Thus, in particular, our unique decomposition theorem for ordered monoids is independent of a syntax for specifying processes. We think that it will turn out to be a convenient tool for establishing unique decomposability results in a wide range of process theories, and for a wide range of process semantics. For instance, we intend to investigate next whether our theorem can be applied to establish unique decomposition results for commutative monoids of processes definable in ACP^ε modulo weak- and branching bisimulation, and of processes definable in the π-calculus modulo observation equivalence.

2   Unique Decomposition in Commutative p.o. Monoids

A *positively ordered monoid* (a *p.o. monoid*) is a nonempty set M endowed with:

(i) an associative binary operation $\otimes$ on M with an identity element $\iota \in M$; the operation $\otimes$ stands for *composition* and ι represents the *empty composition*;

(ii) a partial order $\preccurlyeq$ on M that is *compatible* with $\otimes$, i.e.,

$$x \preccurlyeq y \text{ implies } x \otimes z \preccurlyeq y \otimes z \text{ and } z \otimes x \preccurlyeq z \otimes y \text{ for all } x, y, z \in M,$$

and for which the identity ι is the *least element*, i.e., $\iota \preccurlyeq x$ for all $x \in M$.

A p.o. monoid is *commutative* if its composition is commutative.

An example of a commutative p.o. monoid is the set $\mathbf{N}$ of natural numbers with addition $(+)$ as binary operation, 0 as identity element and the less-than-or-equal relation $(\leq)$ as (total) order; we call it the *additive p.o. monoid of natural numbers*. Another example is the set $\mathbf{N}^*$ of positive natural numbers with multiplication $(\cdot)$ as binary operation, 1 as identity element and the divisibility relation $(|)$ as (partial) order; we call it the *multiplicative p.o. monoid of positive natural numbers*.

In the remainder of this section we shall use $\mathbf{N}$ and $\mathbf{N}^*$ to illustrate the theory of decomposition in commutative p.o. monoids that we are about to develop. However, they are not meant to motivate it; the motivating examples stem from process theory. In particular, note that $\mathbf{N}$ and $\mathbf{N}^*$ are so-called *divisibility monoids* [3] in which $x \preccurlyeq y$ is equivalent to $\exists z(x \otimes z = y)$. The p.o. monoids arising from process theory generally do not have this property.

Definition 1. An element p of a monoid M is called *prime* if $p \neq \iota$ and $p = x \otimes y$ implies $x = \iota$ or $y = \iota$.

Example 2. The natural number 1 is the only prime element of $\mathbf{N}$. The prime elements of $\mathbf{N}^*$ are the prime numbers.

Let $x_1, \ldots, x_n$ be a (possibly empty) sequence of elements of a monoid M; we formally define its composition $x_1 \otimes \cdots \otimes x_n$ by the following recursion:

(i) if $n = 0$, then $x_1 \otimes \cdots \otimes x_n = \iota$; and
(ii) if $n > 0$, then $x_1 \otimes \cdots \otimes x_n = (x_1 \otimes \cdots \otimes x_{n-1}) \otimes x_n$.

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

Definition 3. If x is an element of a monoid M and $p_1, \ldots, p_n$ is a sequence of prime elements of M such that $x = p_1 \otimes \cdots \otimes p_n$, then we call the expression $p_1 \otimes \cdots \otimes p_n$ a *decomposition* of x in M. Two decompositions $p_1 \otimes \cdots \otimes p_m$ and $q_1 \otimes \cdots \otimes q_n$ of x are *equivalent* if there is a bijection $\sigma : \{1, \ldots, m\} \rightarrow \{1, \ldots, n\}$ such that $p_i = q_{\sigma(i)}$ for all $1 \leq i \leq m$; otherwise, they are *distinct*.

The identity element ι has the composition of the empty sequence of prime elements as a decomposition, and every prime element has itself as a decomposition.

We now proceed to discuss the existence and uniqueness of decompositions in commutative p.o. monoids. We shall present two conditions that together guarantee that every element of a commutative p.o. monoid has a unique decomposition.

Definition 4. Let M be a commutative p.o. monoid; by a *stratification* of M we understand a mapping $|\_| : M \rightarrow \mathbf{N}$ from M into the additive p.o. monoid $\mathbf{N}$ of natural numbers that is a strict homomorphism, i.e.,

(i) $|x \otimes y| = |x| + |y|$, and
(ii) $x \prec y$ implies $|x| < |y|$ (where $\prec$ and $<$ are the *strict* relations corresponding to $\preccurlyeq$ and $\leq$, respectively).

A commutative p.o. monoid M together with a stratification $|\_| : M \to \mathbf{N}$ we call a *stratified* p.o. monoid; the number $|x|$ thus associated with every $x \in M$ is called the *norm* of x.

Observe that $|x| = 0$ iff $x = \iota$ (since $|\iota| + |\iota| \leq |\iota \otimes \iota| = |\iota|$ by the first condition in Definition 4, it follows that $|\iota| = 0$, and if $x \neq \iota$, then $\iota \prec x$, whence $0 = |\iota| < |x|$ by the second condition in Definition 4).

Example 5. The additive p.o. monoid $\mathbf{N}$ is stratified with the identity mapping $\mathrm{id}_{\mathbf{N}}$ on $\mathbf{N}$ as stratification. The multiplicative p.o. monoid $\mathbf{N}^*$ is stratified with $|\_| : \mathbf{N}^* \to \mathbf{N}$ defined by

$$|k| = \max\{n \geq 0 : \exists k_0 < k_1 < \cdots < k_n (1 = k_0 \mid k_1 \mid \cdots \mid k_n = k)\}.$$

Proposition 6. In a stratified commutative p.o. monoid every element has a decomposition.

Proof. Straightforward by induction on the norm.

The next two propositions are straightforward consequences of the definition of stratification; we need them later on.

Proposition 7. If M is a stratified commutative p.o. monoid, then M is *strict*:

$$x \prec y \text{ implies } x \otimes z \prec y \otimes z \text{ and } z \otimes x \prec z \otimes y \text{ for all } x, y, z \in M.$$

Proposition 8. The order $\preccurlyeq$ of a stratified p.o. monoid M is *well-founded*: every nonempty subset of M has a $\preccurlyeq$-minimal element.

Definition 9. We call a p.o. monoid M *precompositional* if for all $x, y, z \in M$:

$$x \preccurlyeq y \otimes z \text{ implies that there exist } y' \preccurlyeq y \text{ and } z' \preccurlyeq z \text{ such that } x = y' \otimes z'.$$

Example 10. That $\mathbf{N}^*$ is precompositional can be shown using the well-known property that if p is a prime number such that $p \mid k \cdot l$, then $p \mid k$ or $p \mid l$ (see, e.g., [9, p. 11]).

If $x \prec y$, then x is called a *predecessor* of y, and y a *successor* of x. If there is no $z \in M$ such that $x \prec z \prec y$, then x is an *immediate* predecessor of y, and y is an *immediate* successor of x. The following two lemmas establish a crucial relationship between the immediate predecessors of a composition and certain immediate predecessors of its components.

Lemma 11. Let M be a precompositional stratified commutative p.o. monoid, and let x, y and z be elements of M. If x is a predecessor of y of maximal norm, then $x \otimes z$ is an immediate predecessor of $y \otimes z$.

Lemma 12. Suppose that $x = x_1 \otimes \ldots \otimes x_n$ and y are elements of a precompositional stratified commutative p.o. monoid M. If y is an immediate predecessor of x, then there exist $i \in \{1, \ldots, n\}$ and an immediate predecessor y_i of x_i such that $y = x_1 \otimes \cdots \otimes x_{i-1} \otimes y_i \otimes x_{i+1} \otimes \cdots \otimes x_n$.

Theorem 13 (Unique Decomposition). In a stratified and precompositional commutative p.o. monoid every element has a unique decomposition.

Proof. Let M be a stratified and precompositional commutative p.o. monoid. By Proposition 6, 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 by Proposition 8, this subset has a $\preccurlyeq$-minimal element a. That a has at least two distinct decompositions means that there must be a sequence $p, p_1, \ldots, p_n$ of distinct primes, and sequences $k, k_1, \ldots, k_n$ and $l, l_1, \ldots, l_n$ of natural numbers such that

(A) $a = p^k \otimes p_1^{k_1} \otimes \cdots \otimes p_n^{k_n}$ and $a = p^l \otimes p_1^{l_1} \otimes \cdots \otimes p_n^{l_n}$;
(B) $k < l$; and
(C) $|p| < |p_i|$ implies $k_i = l_i$ for all $1 \le i \le n$.

That a is $\preccurlyeq$-minimal means that the predecessors of a, i.e., the elements of the initial segment $I(a) = \{x \in M : x \prec a\}$ of M determined by a, all have a unique decomposition. Let x be an element of $I(a)$. We define $\#_p(x)$, the *multiplicity* of p in x, as the number of occurrences of the prime p in the unique decomposition of x. The *index* of p in x, denoted by $[x\!:\!p]$, is the maximum of the multiplicities of p in the weak predecessors of x, i.e., $[x\!:\!p] = \max\{\#_p(y) : y \preccurlyeq x\}$.

We now use that $a = p^k \otimes p_1^{k_1} \otimes \cdots \otimes p_n^{k_n}$ to give an upper bound for the multiplicity of p in an element x of $I(a)$. Since M is precompositional there exist $y_1, \ldots, y_k \preccurlyeq p$ and $z_{11}, \ldots, z_{ik_i} \preccurlyeq p_i$ $(1 \le i \le n)$ such that

$$x = \left(\bigotimes_{i=1}^{k} y_i\right) \otimes \left(\bigotimes_{i=1}^{n} \bigotimes_{j=1}^{k_i} z_{ij}\right).$$

From $y_i \preccurlyeq p$ it follows that $\#_p(y_i) \le [p\!:\!p] = 1$, and from $z_{ij} \preccurlyeq p_i$ it follows that $\#_p(z_{ij}) \le [p_i\!:\!p]$, so for all $x \in I(a)$

$$\#_p(x) = \sum_{i=1}^{k} \#_p(y_i) + \sum_{i=1}^{n} \sum_{j=1}^{k_i} \#_p(z_{ij}) \le k + \sum_{i=1}^{n} k_i \cdot [p_i\!:\!p]. \tag{1}$$

We shall now distinguish two cases, according to the contribution of the second term to the right-hand side of the above inequality, and show that either case leads inevitably to a contradiction with condition (B) above.

First, suppose that $\sum_{i=1}^{n} k_i \cdot [p_i\!:\!p] > 0$; then $[p_j\!:\!p] > 0$ for some $1 \le j \le n$. Let $x_1, \ldots, x_n$ be such that $x_i \preccurlyeq p_i$ and $\#_p(x_i) = [p_i\!:\!p]$ for all $1 \le i \le n$, and

$$x = p^l \otimes x_1^{l_1} \otimes \cdots \otimes x_n^{l_n}.$$

Since $\#_p(p_i) = 0$, if $\#_p(x_i) > 0$ then $x_i \prec p_i$. In particular, since $\#_p(x_j) = [p_j\!:\!p] > 0$, this means that x is an element of $I(a)$ (use that $a = p^l \otimes p_1^{l_1} \otimes \cdots \otimes p_n^{l_n}$ and apply Proposition 7), and hence, that $\#_p(x)$ is defined, by

$$\#_p(x) = l + \sum_{i=1}^{n} l_i \cdot [p_i\!:\!p].$$

We combine this definition with the inequality in (1), to conclude that

$$l + \sum_{i=1}^{n} l_i \cdot [p_i : p] \leq k + \sum_{i=1}^{n} k_i \cdot [p_i : p].$$

To arrive at a contradiction with condition (B), it therefore suffices to prove that $k_i \cdot [p_i : p] = l_i \cdot [p_i : p]$ for all $1 \leq i \leq n$. If $[p_i : p] = 0$, then this is clear at once. If $[p_i : p] > 0$, then, since $\#_p(p_i) = 0$, there exists $x \prec p_i$ such that $\#_p(x) = [p_i : p] > 0$. Every occurrence of p in the decomposition of x contributes $|p|$ to the norm of x, so $|p| \leq |x| < |p_i|$, from which it follows by condition (C) that $k_i \cdot [p_i : p] = l_i \cdot [p_i : p]$. This settles the case that $\sum_{i=1}^{n} k_i \cdot [p_i : p] > 0$.

We continue with the hypothesis that $\sum_{i=1}^{n} k_i \cdot [p_i : p] = 0$. First, assume $l_i > 0$ for some $1 \leq i \leq n$; then, by Proposition 7, p^l is a predecessor of a, but that implies $l = \#_p(p^l) \leq k$, a contradiction with (B). In the case that remains, we may assume that $l_i = 0$ for all $1 \leq i \leq n$, and consequently, since $a = p^l$ cannot be prime, that $l > 1$. Clearly, p^{l-1} is a predecessor of a, so $0 < l - 1 = \#_p(p^{l-1}) \leq k$; it follows that $k > 0$. Now, let y be a predecessor of p of maximal norm; by Lemma 11, it gives rise to an immediate a-predecessor

$$x = y \otimes p^{k-1} \otimes p_1^{k_1} \otimes \cdots \otimes p_n^{k_n}.$$

Then, since $a = p^l$, it follows by Lemma 12 that there exists an immediate predecessor z of p such that $x = z \otimes p^{l-1}$. We conclude that $k - 1 = \#_p(x) = l - 1$, again a contradiction with condition (B). □

3   ACP$^\varepsilon$

We fix two disjoint sets of constant symbols $\mathcal{A}$ and $\mathcal{V}$; the elements of $\mathcal{A}$ we call *actions*; the elements of $\mathcal{V}$ we call *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

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

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 a 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*, a commutative and associative partial mapping $\gamma : \mathcal{A} \times \mathcal{A} \rightharpoonup \mathcal{A}$. It 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 and c stands for the event that they do.

The transition system specification in Table 1 defines on the set $\mathcal{P}$ a unary predicate $\downarrow$ and binary relations $\xrightarrow{a}$ ($a \in \mathcal{A}$). 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 $P \xrightarrow{a} P'$, then there exists Q' such that $Q \xrightarrow{a} Q'$ and $P' \mathcal{R} Q'$.

Table 1. The transition system specification for ACP^ε.

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

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

$$\frac{P \xrightarrow{a} P'}{P+Q \xrightarrow{a} P',\ Q+P \xrightarrow{a} P'} \qquad \frac{P \xrightarrow{a} P',\ (X \overset{\text{def}}{=} P)\in\mathcal S}{X \xrightarrow{a} P'}$$

$$\frac{P \xrightarrow{a} P'}{P\parallel\!\!\!\perp Q \xrightarrow{a} P'\parallel Q} \qquad \frac{P \xrightarrow{b} P',\ Q \xrightarrow{c} Q',\ a=\gamma(b,c)}{P\mid Q \xrightarrow{a} P'\parallel Q'} \qquad \frac{P \xrightarrow{a} P',\ a\notin\mathcal H}{\partial_{\mathcal H}(P) \xrightarrow{a} \partial_{\mathcal H}(P')}$$

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

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

The relation $\leftrightarrow$ is an equivalence relation; we write $[P]$ for the equivalence class of process expressions bisimilar to P, and we denote by $\mathcal P/\!\leftrightarrow$ the set of all such equivalence classes. Baeten and van Glabbeek [2] prove that $\leftrightarrow$ has the substitution property with respect to $\parallel$, and that $P \parallel (Q \parallel R) \leftrightarrow (P \parallel Q) \parallel R$, $P \parallel \varepsilon \leftrightarrow \varepsilon \parallel P \leftrightarrow P$ and $P \parallel Q \leftrightarrow Q \parallel P$. Hence, we have the following proposition.

Proposition 14. The set $\mathcal P/\!\leftrightarrow$ with $\otimes$ and ι defined by $[P]\otimes[Q]=[P\parallel Q]$ and $\iota=[\varepsilon]$ is a commutative monoid.

4   Weakly Normed ACP^ε with Bounded Communication

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

The first counterexample already appears in [10]; it shows that perpetual processes need not have a decomposition.

Example 15. Let a be an action, let $\gamma(a,a)$ be undefined and let $X \overset{\text{def}}{=} a\cdot X$. One can show that $X \leftrightarrow P_1 \parallel \cdots \parallel P_n$ implies $P_i \leftrightarrow X$ for some $1 \le i \le n$. It follows that $[X]$ has no decomposition in $\mathcal P/\!\leftrightarrow$. For suppose that $[X]=[P_1]\otimes\cdots\otimes[P_n]$; then $[P_i]=[X]$, whereas $[X]$ is not a prime element of $\mathcal P/\!\leftrightarrow$ (e.g., $X \leftrightarrow a \parallel X$).

The second counterexample employs the distinction between successful and unsuccessful termination characteristic of ACP-like process theories.

Example 16. Let a be an action; then $[a]$, $[a+a\cdot\delta]$ and $[a\cdot\delta+\varepsilon]$ are prime elements of $\mathcal P/\!\leftrightarrow$. Moreover, $a \not\leftrightarrow a+a\cdot\delta$ (the transition $a+a\cdot\delta \xrightarrow{a} \delta$ cannot be

simulated by a). However, it is easily verified that $a \| (a \cdot \delta + \varepsilon) \leftrightarrow (a + a \cdot \delta) \| (a \cdot \delta + \varepsilon)$, so a decomposition in $\mathcal{P}/\leftrightarrow$ need not be unique.

Let $w \in \mathcal{A}^*$, say $w = a_1 \cdots a_n$; we write $P \xrightarrow{w} P'$ if there exist $P_0, \ldots, P_n$ such that $P = P_0 \xrightarrow{a_1} \cdots \xrightarrow{a_n} P_n = P'$. To exclude the problems mentioned in Examples 15 and 16 above we use the following definition.

Definition 17. A process expression P is *weakly normed* if there exist $w \in \mathcal{A}^*$ and a process expression P' such that $P \xrightarrow{w} P' \leftrightarrow \varepsilon$. The set of weakly normed process expressions is denoted by $\mathcal{P}^\varepsilon$.

It is straightforward to show that bisimulation respects the property of being weakly normed, and that a parallel composition is weakly normed iff its parallel components are. Hence, we have the following proposition.

Proposition 18. The set $\mathcal{P}^\varepsilon/\leftrightarrow$ is a submonoid of $\mathcal{P}/\leftrightarrow$. Moreover, if $[P \| Q] \in \mathcal{P}^\varepsilon/\leftrightarrow$, then $[P] \in \mathcal{P}^\varepsilon/\leftrightarrow$ and $[Q] \in \mathcal{P}^\varepsilon/\leftrightarrow$.

Christensen et al. [5] prove that every element of the commutative monoid of weakly normed BPP expressions modulo bisimulation has a unique decomposition. Presupposing a communication function γ 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 [4] extends this result to a unique decomposition theorem for the commutative monoid of weakly normed BPP_τ expressions modulo bisimulation. His BPP_τ 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 ACP^ε gives rise to weakly normed process expressions without a decomposition.

Example 19. Let a be an action, suppose that $a = \gamma(a, a)$ and $X \stackrel{\text{def}}{=} a \cdot X + a$. Then one can show that $X \leftrightarrow P_1 \| \cdots \| P_n$ implies that $P_i \leftrightarrow X$ for some $1 \leq i \leq n$, from which it follows by a similar argument as in Example 15 that $[X]$ has no decomposition in $\mathcal{P}/\leftrightarrow$.

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 20. A communication function γ is *bounded* if every action can be assigned a *weight* ≥ 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.

5 Unique Decomposition in $\mathcal{P}^\varepsilon/\leftrightarrow$

We now prove that every element of the commutative monoid $\mathcal{P}^\varepsilon/\leftrightarrow$ of weakly normed process expressions modulo bisimulation has a unique decomposition, provided that the communication function is bounded. We proceed by defining on $\mathcal{P}^\varepsilon/\leftrightarrow$ a partial order $\preccurlyeq$ and a stratification $|\_| : \mathcal{P}^\varepsilon/\leftrightarrow \to \mathbf{N}$ turning it into

a precompositional stratified commutative p.o. monoid. That every element of $\mathcal{P}^\varepsilon/\!\leftrightarrow$ has a unique decomposition then follows from the theorem of Section 2. Throughout this section we assume that the presupposed communication function γ is bounded so that every action has a unique weight assigned to it (cf. Definition 20). We use it to define the *weighted length* $\ell(w)$ of $w \in \mathcal{A}^*$ inductively as follows: if w is the empty sequence, then $\ell(w) = 0$; and if $w = w'a$ and a is an action of weight i, then $\ell(w) = \ell(w') + i$. 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 ACP^ε.

Lemma 21. If P, Q and R are process expressions such that $P \,\|\, Q \xrightarrow{w} R$, then there exist $P', Q' \in \mathcal{P}^\varepsilon$ and $u, v \in \mathcal{A}^*$ such that $R = P' \,\|\, Q'$, $P \xrightarrow{u} P'$, $Q \xrightarrow{v} Q'$ and $\ell(u) + \ell(v) = \ell(w)$.

Definition 22. 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 $P \xrightarrow{w} P' \leftrightarrow \varepsilon$.

Lemma 23. If $P \leftrightarrow Q$, then $|P| = |Q|$ for all $P, Q \in \mathcal{P}^\varepsilon$.

Lemma 24. $|P \,\|\, Q| = |P| + |Q|$ for all $P, Q \in \mathcal{P}^\varepsilon$.

We define on $\mathcal{P}^\varepsilon$ binary relations $\rightarrowtail_i$ $(i \geq 1)$ and $\rightarrowtail$ by

$$P \rightarrowtail_i Q \iff \text{there exists } a \in \mathcal{A} \text{ of weight } i \text{ s.t. } P \xrightarrow{a} Q \text{ and } |P| = |Q| + i.$$
$$P \rightarrowtail Q \iff P \rightarrowtail_i Q \text{ for some } i \geq 1.$$

The reflexive-transitive closure $\rightarrowtail^*$ of $\rightarrowtail$ is a partial order on $\mathcal{P}^\varepsilon$.

Definition 25. We write $[P] \preccurlyeq [Q]$ iff there exist $P' \in [P]$ and $Q' \in [Q]$ such that $Q' \rightarrowtail^* P'$.

It is straightforward to verify that $\preccurlyeq$ is a partial order on $\mathcal{P}^\varepsilon/\!\leftrightarrow$. Furthermore, that $\preccurlyeq$ is compatible with $\otimes$ can be established by means of Lemma 24, and that ι is its least element essentially follows from weak normedness. Hence, we get the following proposition.

Proposition 26. The set $\mathcal{P}^\varepsilon/\!\leftrightarrow$ is a commutative p.o. monoid.

By Lemmas 23 and 24, the mapping $|\_| : (\mathcal{P}^\varepsilon/\!\leftrightarrow) \to \mathbf{N}$ defined by $[P] \mapsto |P|$ is a strict homomorphism.

Proposition 27. The mapping $|\_| : (\mathcal{P}^\varepsilon/\!\leftrightarrow) \to \mathbf{N}$ is a stratification of $\mathcal{P}^\varepsilon/\!\leftrightarrow$.

Lemma 28. If $P \,\|\, Q \rightarrowtail^* R$, then there exist P' and Q' such that $P \rightarrowtail^* P'$, $Q \rightarrowtail^* Q'$ and $R = P' \,\|\, Q'$.

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

Proposition 29. The p.o. monoid $\mathcal{P}^\varepsilon/\underline{\leftrightarrow}$ is precompositional.

According to Propositions 26, 27 and 29, $\mathcal{P}^\varepsilon/\underline{\leftrightarrow}$ is a stratified and precompositional commutative p.o. monoid, so by Theorem 13 we get the following result.

Theorem 30. In the p.o. monoid $\mathcal{P}^\varepsilon/\underline{\leftrightarrow}$ of weakly normed processes expressions modulo bisimulation every element has a unique decomposition, provided that the communication function is bounded.

Acknowledgment

References

1. L. Aceto and M. Hennessy. Towards action-refinement in process algebras. *Inform. and Comput.*, 103(2):204–269, 1993.
2. 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.
3. G. Birkhoff. *Lattice theory*, volume XXV of *American Mathematical Society Colloquium Publications*. American Mathematical Society, third edition, 1967.
4. S. Christensen. *Decidability and Decomposition in Process Algebras*. PhD thesis, University of Edingburgh, 1993.
5. 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.
6. W. J. Fokkink and S. P. Luttik. An ω-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.
7. L. Fuchs. *Partially Ordered Algebraic Systems*, volume 28 of *International Series of Monographs on Pure and Applied Mathematics*. Pergamon Press, 1963.
8. 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.
9. T. W. Hungerford. *Algebra*, volume 73 of *GTM*. Springer, 1974.
10. R. Milner and F. Moller. Unique decomposition of processes. *Theoret. Comput. Sci.*, 107:357–363, January 1993.
11. F. Moller. *Axioms for Concurrency*. PhD thesis, University of Edinburgh, 1989.
12. 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.
13. J. L. M. Vrancken. The algebra of communicating processes with empty process. *Theoret. Comput. Sci.*, 177:287–328, 1997.