Enhancing Partial-Order Reduction via Process Clustering

T. Basten and D. Bošnački

00/11

ISSN 0926-4515

All rights reserved
editors: prof.dr. J.C.M. Baeten
         prof.dr. P.A.J. Hilbers

Reports are available at:
http://www.win.tue.nl/win/cs

Computing Science Reports 00/11
Eindhoven, March 2000
Enhancing Partial-Order Reduction via Process Clustering

Twan Basten\textsuperscript{1} and Dragan Bošnački\textsuperscript{2}

\textsuperscript{1} Dept. of Electrical Eng., Eindhoven University of Technology, PO Box 513, NL-5600 MB Eindhoven, The Netherlands
\textsuperscript{2} Dept. of Computing Science, Eindhoven University of Technology PO Box 513, NL-5600 MB Eindhoven, The Netherlands

e-mail: a.a.basten@tue.nl
e-mail: dragan@win.tue.nl

Abstract

Partial-order reduction is a well-known technique to cope with the state-space-explosion problem in the verification of concurrent systems. Using the hierarchical structure of concurrent systems, we present an enhancement of the partial-order-reduction scheme of \cite{Hollmann12, Peled19}. A prototype of the new algorithm has been implemented on top of the verification tool SPIN. The first experimental results are encouraging.

Key words: concurrency - state explosion - formal verification - partial-order reduction - (LTL) model checking - SPIN

1 Introduction

Over the last decades, the complexity of computer systems has been increasing rapidly, with a tendency towards distribution and concurrency. The correct functioning of these complex concurrent systems is becoming an ever larger problem. Many verification and proof techniques have been invented to solve this problem. An important class of techniques are those based on a fully automatic, exhaustive traversal of the state space of a concurrent system. Well-known representatives are the various model-checking techniques.

An infamous problem complicating an exhaustive traversal of the state space of a concurrent system is the state explosion, caused by the arbitrary interleaving of independent actions of the various components of the system. Several techniques have been developed to cope with this problem. Partial-order reduction is a very prominent one (see, for example, \cite{Basten12, Peled19, Holzmann12, Peled18, Holzmann19, Peled20, Holzmann21, Peled22}). It exploits the independence of actions to reduce the state space of a system while preserving properties of interest. During the generation of a state space, in each state, a subset of the enabled actions satisfying certain criteria is chosen for further exploration. Following \cite{Hollmann12, Peled19}, we call these sets ample sets.

The traditional approach to partial-order reduction (see, for example, \cite{Hollmann12, Peled19}) deals with systems seen as an unstructured collection of sequential processes running in parallel. However, many systems have inherent hierarchical structure, imposed either explicitly by the language used for the system specification that groups processes in blocks or similar constructs (e.g., SDL, UML), or implicitly by the interconnections among processes. In this paper, we present a partial-order-reduction algorithm that exploits the hierarchical structure of a system.

As our starting point, we take the partial-order algorithm of Holzmann and Peled \cite{Hollmann12, Peled19}. This algorithm is implemented in the verification tool SPIN \cite{Holzmann19} and has proven to be successful in coping with the state-space explosion. It is also sufficiently flexible to allow extensions (see for instance the extensions for timed systems in \cite{Holzmann14, Peled17}). The algorithm uses a notion of safety to
select ample sets. The safety requirement is imposed via syntactical criteria to avoid expensive
computations during the state-space traversal. These criteria yield ample sets consisting of either
all enabled actions of a single process or all enabled actions of all processes. Our idea is to introduce
a gradation of the safety requirement based on the hierarchical structure of a system. To this end,
we introduce the concept of a clustering hierarchy to capture the system hierarchy and the induced
(in)dependencies among processes. This generalization allows ample sets consisting of actions from
different, but not necessarily all, processes. Our cluster-based algorithm is a true generalization of
the partial-order-reduction algorithm of [12, 19]. It can also be seen as a version of the algorithm
of Overman [18], adapted for clustering hierarchies and LTL model checking. We implemented
our algorithm on top of the verification tool SPIN. The results obtained with the prototype are
encouraging, in particular, considering that a visual language is being developed for SPIN [15] that
combines naturally with our cluster-based reduction algorithm.

The remainder of this paper is organized as follows. Section 2 explains the state-space-explosion
problem and the basic concepts that play a role in this paper. Section 3 presents some known
theoretical results on partial-order reduction as well as the reduction algorithm of [12, 19]. In Section
4, we present our cluster-based partial-order-reduction algorithm. Section 5 gives experimental
results. Finally, Section 6 contains concluding remarks.

Acknowledgments. Our work is inspired by the Next heuristic of Rajeev Alur and Bow-Yaw
Wang presented in [2]. We thank Dennis Dams and Jeroen Rutten for their contributions.

2 Preliminaries

State spaces of concurrent systems. Concurrent systems typically consist of a number of
processes running in parallel. To exchange information, these processes communicate via messages
and/or shared memory. The left part of Figure 1 shows the very simple concurrent system example.
It consists of three processes, $P_0$, $P_1$, and $P_2$, each one executing a sequence of two actions. Assuming
that there is no communication and, thus, all actions can be executed independently, the right part
of Figure 1 shows the state space of system example.

![Figure 1: A concurrent system and its state space.](image)

The numbers 00 through 08, 10 through 18, and 20 through 28 represent states of system example. The states encode all relevant information of example such as, for example, the values
of variables and local program counters. The initial state of the system is state 00 (marked with
a small arrow). The labeled arrows in Figure 1 correspond to state changes or transitions of the
system. The labels link transitions to actions of the system. For example, action labels $a_0$ and
b_1 correspond to actions a_0 and b_1 of system example. Note that parallel arrows in Figure 1 are assumed to have identical action labels.

The example of Figure 1 illustrates a well-known problem complicating the verification of concurrent systems. Clearly, each of the processes in example can only be in three different states. However, Figure 1 shows that the complete state space of example consists of 27 (=3^3) states. The state space of a system with a fourth process (executing two actions) already consist of 81 (=3^4) states, whereas the state space of a system consisting of two processes consists of only 9 (=3^2) states. This example illustrates that the state space of a concurrent system grows (in the worst case) exponentially if the number of processes in the system increases. This phenomenon is known as the state-space explosion. Obviously, the state-space explosion complicates verification techniques that are based on an exhaustive traversal of the entire state space of a concurrent system.

**Labeled transition systems.** The notion of a state space is the most important concept in this paper. To formally reason about state spaces, we introduce the notion of a labeled transition system.

**Definition 2.1.** (Labeled transition system) A labeled transition system, or simply an LTS, is a 6-tuple (S, s, A, τ, Π, L), where

- S is a finite set of states;
- s ∈ S is the initial state;
- A is a finite set of actions;
- τ : S × A → S is a (partial) transition function;
- Π is a finite set of boolean propositions;
- L : S → 2^Π is a state labeling function.

Consider again the example of the previous paragraph. The states, the initial state, the actions, and the transition function of an LTS for example are easily derived from the right-hand side of Figure 1. However, the figure does not contain any labeling of states with propositions. Propositions and state labeling are included in the definition of an LTS because they play a role when one is interested in verifying specific properties of a concurrent system. Before explaining these last two elements of an LTS in some more detail, we introduce some auxiliary notions. Let T = (S, s, A, τ, Π, L) be some LTS.

An action a ∈ A is said to be enabled in a state s ∈ S, denoted s ✷ a if τ(s, a) is defined. The set of all actions a ∈ A enabled in a state s ∈ S is denoted enabled(s); that is, for any s ∈ S, enabled(s) = {a ∈ A | s ✷ a}. A state s ∈ S is a deadlock state iff enabled(s) = ∅.

In the previous paragraph, the notion of a transition has already been mentioned. Formally, transition function τ of LTS T induces a set T ⊆ S × A × S of transitions defined as T = {(s, a, s') | s, s' ∈ S ∧ a ∈ A ∧ s' = τ(s, a)}. To improve readability, we write s ⇒ a s' for (s, a, s') ∈ T. Besides the number of states of a concurrent system, also the number of transitions of the system is a factor complicating verification. Note that the LTS of Figure 1 contains 54 transitions.

An execution sequence of LTS T is a (finite) sequence of subsequent transitions in T. Formally, for any natural number n ∈ N, states s_i ∈ S with i ∈ IN and 0 ≤ i ≤ n, and actions a_i ∈ A with i ∈ IN and 0 ≤ i < n, the sequence s_0 ⇒ a_0 s_1 ⇒ a_1 ... s_{n-1} ⇒ a_{n-1} s_n is an execution sequence of length n of T if s_i ⇒ a_i s_{i+1} for all i ∈ IN with 0 ≤ i < n. State s_n is said to be reachable from state s_0. A state is said to be reachable in T if it is reachable from s. The LTS of Figure 1 has 90 execution sequences of length six all starting from the initial state and leading to deadlock state 28.
Properties of concurrent systems. There are many different kinds of properties of concurrent systems that designers are interested in. We mention three well-known classes of properties. For each of these classes, verification techniques exist that are based on an exhaustive traversal of the state space of a concurrent system. Hence, the state-space-reduction technique presented in this paper can be useful to improve these verification techniques. In the remainder, neither the details of the specification of properties nor the details of the verification techniques are very important. Hence, we only give an informal explanation.

The first class of properties is the presence or absence of deadlocks. It is clear that deadlock properties can be verified in a straightforward way by means of an exhaustive state-space traversal.

The second class of properties are the so-called local properties. Local properties of a concurrent system are properties that typically depend only on the state of a single process of the system or on the state of a single shared object. The question whether or not a state satisfying some local property is reachable is essentially also verified by means of a state-space traversal. To verify whether a system state satisfies a local property, it is important to encode all relevant information concerning the property in the state labeling of the LTS representing the state space of the system. Thus, at this point, the reason for including a set of boolean propositions and an accompanying state labeling in the definition of an LTS becomes apparent. For more details on the verification of local properties, see [7, 11, 20].

The third class of properties are those expressible in (next-time-free) Linear-time Temporal Logic (LTL). Also LTL properties are formulated in terms of the propositions in an LTS. It is beyond the scope of this paper to give a formal definition of LTL; the interested reader is referred to [16]. The technique for verifying LTL formulae is referred to as (LTL) model checking. Again, the details are not important. For more information, see, for example, [12].

3 Partial-Order Reduction

Section 3.1 gives results, known from the literature on partial-order reduction (see, for example, [1, 7, 8, 11, 12, 18, 19, 20, 21, 22]), that are needed to prove that our reduction technique preserves deadlocks, local properties, and next-time-free LTL. Section 3.2 presents the partial-order-reduction algorithm of Holzmann and Peled [12, 19]. In Section 3.3, we briefly discuss implementation issues.

3.1 Basic theoretical framework

The basic idea of state-space-reduction techniques for enhancing verification is to restrict the part of the state space of a concurrent system that is explored during verification in such a way that properties of interest are preserved. There are several types of reduction techniques. In this paper, we focus on partial-order reduction. This technique exploits the independence of properties from the possible interleavings of the actions of the concurrent system. It uses the fact that the state-space explosion is often caused by the interleaving of independent actions of concurrently executing processes of the system (see Figure 1).

To be practically useful, a reduction of the state space of a concurrent system must be achieved during the traversal of the state space. This means that it must be decided per state which transitions, and hence which subsequent states, must be considered. Let \( T = (S, \delta, A, \tau, \Pi, L) \) be some LTS.

Definition 3.1. (Reduction) For any so-called reduction function \( r : S \rightarrow 2^A \), we define the (partial-order) \( r \)-reduction of \( T \) with respect to \( r \) as the smallest LTS \( T_r = (S_r, \delta_r, A, \tau_r, \Pi, L_r) \) satisfying the following conditions:
- $S_r \subseteq S$, $\delta_r = \delta$, $\tau_r \subseteq \tau$, and $L_r = L \cap (S_r \times \Pi)$;
- for every $s \in S_r$ and $a \in r(s)$ such that $\tau(s, a)$ is defined, $\tau_r(s, a)$ is defined.

Note that these two requirements imply that, for every $s \in S_r$ and $a \in A$, if $\tau_r(s, a)$ is defined, then also $\tau(s, a)$ is defined and $\tau_r(s, a) = \tau(s, a)$.

It may be clear that not all reductions preserve all properties of interest. Thus, depending on the properties that a reduction must preserve, we have to define additional restrictions on $r$. To this end, we need to formally capture the notion of independence introduced earlier. Actions occurring in different processes may still influence each other, for example, when they access global variables. The following notion of independence defines the absence of such mutual influence. Intuitively, two actions are independent iff, in every state where they are both enabled, (1) the execution of one action cannot disable the other and (2) the result of executing both actions is always the same.

**Definition 3.2. (Independence)** Actions $a, b \in A$ with $a \neq b$ are independent iff, for all states $s \in S$ such that $s \xrightarrow{a} s'$ and $s \xrightarrow{b} s'$,
- $\tau(s, a) \xrightarrow{b}$ and $\tau(s, b) \xrightarrow{a}$, and
- $\tau(\tau(s, a), b) = \tau(\tau(s, b), a)$.

An example of independent actions are two assignments to or readings from local variables in distinct processes. Note that two actions are trivially independent if there is no state in which they are both enabled. It is straightforward to see that, in our running example of Figure 1, all actions are mutually independent.

The first class of properties we are interested in is the presence or absence of deadlocks. In order to preserve deadlock states of an LTS in a reduced LTS, the reduction function $r$ must satisfy the following two conditions (called provisos):
- CO: $\tau(s) = \emptyset$ iff $\text{enabled}(s) = \emptyset$.
- C1 (persistency): For any $s \in S$ and execution sequence $s = s_0 \xrightarrow{a_0} s_1 \xrightarrow{a_1} \ldots \xrightarrow{a_n} s_n$ of length $n \in \mathbb{N} \setminus \{0\}$ such that, for all $i \in \mathbb{N}$ with $0 \leq i < n$, $a_i \notin \tau(s)$, action $a_{n-1}$ is independent of all actions in $\tau(s)$.

The basic idea behind the persistency proviso is that, during the state-space traversal, transitions caused by actions that are independent of all the actions chosen by the reduction function can be ignored.

**Theorem 3.3. (Deadlock preservation [7, Theorem 4.3])** Let $r$ be a reduction function for LTS $T$ that satisfies provisos C0 and C1. Any deadlock state reachable in $T$ is also reachable in the reduced LTS $T_r$ and vice versa.

A few remarks are in order. First, Theorem 4.3 in [7] does not state that any deadlock reachable in a reduced LTS is also reachable in the original LTS. However, this result follows immediately from proviso C0. Second, [7] uses a slightly stronger definition of independence. However, the proof of Theorem 4.3 in [7] carries over to our setting without change. Finally, observe that several authors presented state-space-reduction algorithms that preserve deadlocks [8, 18, 20].

Consider again Figure 1. It is not difficult to define a reduction function satisfying provisos C0 and C1 that reduces the LTS of Figure 1 to an LTS consisting of a single execution sequence from state 00 to state 28. Clearly, this reduction preserves deadlock state 28.

The second class of properties we discuss is the class of local properties. A local property is a boolean combination of propositions in $\Pi$ whose truth value cannot be changed by two independent
actions. That is, a property $\phi$ is local iff, for all states $s \in S$ and independent actions $a, b \in A$ such that $s \xrightarrow{a} s' \xrightarrow{a} s''$, and $\phi$ has different truth values in states $s$ and $\tau(s, a)$, the truth values of $\phi$ in $s$ and in $\tau(s, b)$ are the same. An LTS satisfies a local property $\phi$ iff there is a reachable state that satisfies $\phi$. Typical examples of local properties are properties that depend only on the state of a single process or shared object. To guarantee that a reduction of a state space preserves local properties, it suffices that the reduction function $r$ satisfies the following requirement (in addition to $C0$ and $C1$).

- **C2 (cycle proviso):** For any cycle $s_0 \xrightarrow{a_1} s_1 \xrightarrow{a_2} \ldots \xrightarrow{a_{n-1}} s_n = s_0$ of length $n \in \mathbb{N} \setminus \{0\}$, there is an $i \in \mathbb{N}$ with $0 \leq i < n$ such that $r(s_i) = enabled(s_i)$.

**Theorem 3.4. (Local-property preservation)** Let $r$ be a reduction function for LTS $T$ satisfying provisos $C0$, $C1$, and $C2$. Let $\phi$ be a local property. LTS $T$ satisfies $\phi$ iff the reduced LTS $T_r$ satisfies $\phi$.

Proviso $C2$ prevents the so-called “ignoring problem” identified in [20]. Informally, the ignoring problem occurs when a reduction of a state space ignores the actions of an entire process. Proofs of (variants of) Theorem 3.4 can be found in [7, 11, 20]. In fact, these references show that proviso $C2$ can be weakened if one is only interested in the preservation of local properties. The stronger proviso given above is needed for the preservation of next-time-free LTL properties.

The third class of properties we are interested in is the class of properties expressible in next-time-free LTL. For any LTL formula $\phi$, $prop(\phi)$ is the set of propositions occurring in $\phi$.

**Definition 3.5. (Invisibility)** An action $a \in A$ is $\phi$-invisible in state $s \in S$ iff $\tau(s, a)$ is undefined or, for all $\pi \in prop(\phi)$, $\pi \in L(s) \iff \pi \in L(\tau(s, a))$. Action $a$ is globally $\phi$-invisible iff it is $\phi$-invisible for all $s \in S$.

Informally, an action is globally $\phi$-invisible iff it cannot change the truth value of formula $\phi$.

Given a next-time-free LTL formula $\phi$ and assuming that a reduction function $r$ satisfies the following proviso in addition to $C0$, $C1$, and $C2$, it can be shown that the reduced LTS satisfies $\phi$ iff the original LTS satisfies $\phi$. For a precise definition of the satisfaction of an LTL formula by some LTS, see [16].

- **C3 (invisibility):** For any state $s \in S$, all actions in $r(s)$ are globally $\phi$-invisible or $r(s) = enabled(s)$.

**Theorem 3.6. (Next-time-free LTL preservation [19, 21])** Let $r$ be a reduction function for LTS $T$ satisfying $C0$, $C1$, $C2$, and $C3$. Let $\phi$ be a next-time-free LTL formula. LTS $T$ satisfies $\phi$ iff the reduced LTS $T_r$ satisfies $\phi$.

### 3.2 The partial-order-reduction algorithm of Holzmann and Peled

Given the three theorems of the previous subsection, the challenge is to find interesting reduction functions and efficient algorithms implementing the corresponding reductions. A well-known partial-order-reduction algorithm is the one described in [12, 19]. The most important aspects of the algorithm are the following: (1) It is based on a depth-first search (DFS) of the state space of a concurrent system and (2) it uses a reduction function based on the process structure of the system. For the full details of the algorithm, the reader is referred to the original references [12, 19]. In this paper, we concentrate on the reduction function. To this end, we introduce a notion of processes in our framework of LTSs.
Let $T = (S, \delta, A, \tau, \Pi, L)$ be some LTS. We assume that a given set of processes $P$ is associated with $T$ as follows. Each process $P \in P$ is a set of actions, i.e., $P \subseteq A$. We require that $A = \cup_{P \in P} P$ and that, for all $P, Q \in P$ with $P \neq Q$, $P \cap Q = \emptyset$. That is, the set of processes partitions the set of actions. Function $\text{Pid} : A \rightarrow P$ yields for each action the process it is contained in. Not every partitioning of actions yields a meaningful process structure. Concurrency within processes is not allowed. Therefore, we require the following. Let $a, b \in A$ with $a \neq b$ be a pair of distinct actions belonging to the same process in $P$. For any state $s \in S$ such that $a, b \in \text{enabled}(s)$, $b \notin \text{enabled}(\tau(s, a))$. That is, each two actions from a single process that are simultaneously enabled in a given state must disable each other. Clearly, this restriction disallows concurrency within processes, whereas it does allow choices.

The following definition is crucial in the formulation of the abovementioned reduction function. It depends on the class of properties one is interested in.

**Definition 3.7. (safety)** An action $a \in A$ is said to be safe if it is independent from any (other) action $b \in A$ with $\text{Pid}(b) \neq \text{Pid}(a)$. An action $a \in A$ is said to be safe for a given next-time-free LTL formula $\phi$ iff it is independent from any action $b \in A$ with $\text{Pid}(b) \neq \text{Pid}(a)$ and globally $\phi$-invisible.

As mentioned, the algorithm of [12, 19] performs the reduction of the state space during a DFS. A DFS uses a stack to store partially investigated states. The reduction is obtained by defining for each state a so-called ample set. Note that the definition uses safety and, hence, depends on the particular class of properties to be verified.

**Definition 3.8. (Reduction function ample)** Let $s \in S$. Consider the set of processes $P \in P$ such that $\text{enabled}(s) \cap P \neq \emptyset$, for all $a \in \text{enabled}(s) \cap P$, $a$ is safe (for some next-time-free LTL formula $\phi$), and $\tau(s, a)$ is not on the DFS stack. If the set is non-empty, then choose an arbitrary element $P$ of this set and define ample$(s) = \text{enabled}(s) \cap P$; otherwise, ample$(s) = \text{enabled}(s)$. Set ample$(s)$ is said to be the ample set for $s$.

It is not difficult to verify that reduction function ample satisfies provisos C0 through C3 given in the previous subsection. C0 follows easily from Definition 3.8. C1 and C3 follow from the safety requirement in Definition 3.8. Finally, C2 follows from the requirement in Definition 3.8 that the state resulting from the execution of an action in the ample set cannot be on the DFS stack unless the ample set consists of the entire set of enabled actions. As a result, the reduction via ample preserves deadlocks (Theorem 3.3), local properties (Theorem 3.4), and next-time-free LTL (Theorem 3.6). For more details, see [12, 19].

### 3.3 Implementation in SPIN

SPIN [9] is a tool supporting the automatic verification of deadlock-, local-, and next-time-free LTL properties. Specifications of concurrent system are written in the language PROMELA. The partial-order-reduction algorithm of [12, 19] has been implemented in SPIN. To allow for the efficient computation of ample sets during a DFS, sufficient conditions for the safety of actions are derived from the PROMELA specification before starting the DFS (see [12]). For instance, a sufficient condition for the safety of an action that can be derived from a PROMELA specification is that it does not touch any global objects such as variables or communication channels. Another good reference for readers interested in implementation issues concerning partial-order reduction is [7].
4 Cluster-based Partial-Order Reduction

We motivate our improvement of partial-order reduction by means of two different specifications of the same concurrent system given in Figure 2. Specification example1 has two global variables and four processes, each of them executing a single action assigning a value to one of these variables. Clearly, none of the actions is independent of all the other actions, which by Definition 3.7 means that none of the actions is safe. Thus, reduction function ample of Definition 3.8 yields no reduction.

The interested reader could verify that the LTS corresponding to the concurrent system has 25 states and 40 transitions.

System example1

| P0: a(u:=0); | P0: a(u:=0); |
| P1: b(u:=1); | P1: b(u:=1); |
| P2: c(v:=0); | P2: c(v:=0); |
| P3: d(v:=1); | P3: d(v:=1); |

System example2

| C0: int u; |
| P0: a(u:=0); |
| P1: b(u:=1); |
| C1: int v; |
| P2: c(v:=0); |
| P3: d(v:=1); |

Figure 2: Two specifications of a concurrent system and a reduced state space.

Specification example2 in Figure 2 is a variant of example1 with the processes clustered in pairs. The two clusters encapsulate the dependencies between processes. As a result, all actions within one cluster are independent of all actions within the other one. Our idea is to augment an LTS with a hierarchy of clusters and to generalize Definitions 3.7 and 3.8 to clusters. Thus, it is possible to reduce the state space of the system of Figure 2 to an LTS that includes all interleavings of actions within clusters C0 and C1 but only a single interleaving of actions from different clusters (see Figure 2), while preserving all properties of interest. Let \( T = (S, s, A, r, \Pi, L) \) be an LTS with processes \( P \).

Definition 4.1. (Clustering) A cluster of processes in \( P \) is simply a set of processes. A clustering \( \mathcal{C} \subseteq 2^P \) of \( P \) is a set of clusters partitioning \( P \), i.e., \( P = \bigcup_{C \in \mathcal{C}} C \) and, for all \( C, D \in \mathcal{C} \) with \( C \neq D \), \( C \cap D = \emptyset \). A clustering hierarchy \( \mathcal{H} \) for \( P \) is a finite ordered set \( \{C_0, C_1, \ldots, C_{n-1}\} \), where \( n \in \mathbb{N} \setminus \{0\} \), of clusterings of \( P \) such that, for all \( i \in \mathbb{N} \) with \( 0 < i < n \),
- \( |C_i| < |C_{i-1}| \) and
- for each \( C \in C_{i-1} \), there exists a \( D \in C_i \) such that \( C \subseteq D \).

For any \( i \in \mathbb{N} \) with \( 0 \leq i < n \), clustering \( C_i \) is called level \( i \) of the hierarchy. Level \( C_i \) is above level \( C_j \) iff \( i > j \); it is below \( C_j \) iff \( i < j \).

Clearly, Definition 4.1 implies that each level in a clustering hierarchy is a coarsening of all lower levels. Also note that the maximum number of levels in a clustering hierarchy is limited by the number of processes in \( P \). A clustering hierarchy for example2 consisting of three levels (numbered 0, 1, and 2) is the following: \( \{\{P0\}, \{P1\}, \{P2, P3\}\}, \{C0 = \{P0, P1\}, C1 = \{P2, P3\}\}, \{\{P0, P1, P2, P3\}\} \).
Definition 4.2. (Level-i safety) Let \( i \in \mathbb{N} \) with \( 0 \leq i < n \). Action \( a \in A \) is level-i safe (for a given next-time-free LTL formula \( \phi \)) if it is independent of any action \( b \in A \) with \( Cid(i)(Pd(b)) \neq Cid(i)(Pd(a)) \) (and globally \( \phi \)-invisible).

In the above clustering hierarchy for example 2, all actions are level-1 and (trivially) level-2 safe, but not level-0 safe.

Given a cluster \( C \subseteq P \), let \( actions(C) = \cup_{P \subseteq C} P \). Furthermore, for any state \( s \in S \), let \( enabled(s, C) = actions(C) \cap enabled(s) \).

Definition 4.3. (Reduction function \textit{ample}) Let \( s \in S \). Consider for each level \( C_i \in \mathcal{C} \) the set of clusters \( C \in C_i \) such that \( enabled(s, C) \neq \emptyset \), for all \( a \in enabled(s, C) \), \( a \) is level-i safe (for some next-time-free LTL formula \( \phi \)), and \( \tau(s, a) \) is not on the DFS stack. If there is a level \( C_i \) such that the aforementioned set is non-empty, then choose an arbitrary element \( C \) of this set and define \( ample(s) = enabled(s, C) \); otherwise, \( ample(s) = enabled(s) \).

It is interesting to observe that function \textit{ample} of Definition 3.8 is a special case of function \textit{ample} of Definition 4.3 with a trivial hierarchy of only one level that consists of trivial clusters each containing only one process.

Theorem 4.4. The reduction of an LTS obtained via reduction function \textit{ample} of Definition 4.3 preserves deadlock-, local-, and next-time-free LTL properties.

Proof. It is straightforward to prove that \textit{ample} satisfies provisos C0, C1, C2, and C3 of Section 3.1. The arguments are the same as in Section 3.2, where it is argued that function \textit{ample} of Definition 3.8 satisfies these provisos. The desired result follows immediately from Theorems 3.3, 3.4, and 3.6.

Consider again the concurrent system of Figure 2. The figure shows a reduced state space of this system. In each state, the values of variables \( u \) and \( v \) are given with \( \perp \) meaning that a value is undefined. The sets of actions chosen in each state are ample sets as defined by function \textit{ample} of Definition 4.3. The reduced state space has 13 states and 12 transitions. This means reductions of the complete state space, consisting of 25 states and 40 transitions, of 48% in states and 70% in transitions. (Recall that standard partial-order reduction yields no reductions.)

In practice, the largest state-space reductions are obtained by choosing the ample sets as small as possible. A simple way to obtain small ample sets is to search the levels in a clustering hierarchy for suitable clusters in increasing order.

Another practical issue is how to obtain useful clustering hierarchies. Such a clustering should maximize the dependencies between processes within a cluster and minimize the dependencies between clusters. It is our aim to obtain such hierarchies statically, derived from the concurrent-system specification. In that way, we avoid the overhead of forming a hierarchy on-the-fly by inspecting dependencies between processes during the DFS. One possibility to derive a hierarchy in a static way is to preprocess the system specification and to cluster processes based on shared objects. Another option is to use the existing hierarchical or modular structure of a specification; many contemporary specification and modeling languages such as UML and SDL include standard hierarchical structuring mechanisms. A final option could be the use of advanced statistical clustering techniques (based on run-time information) as described in [14].

5 Experiments

To validate our cluster-based reduction algorithm, we implemented a prototype on top of the verification tool SPIN, version 3.2.4. We applied our prototype implementation to several examples.
Since PROMELA, the input language of SPIN, does not support modular design, we provided the clustering hierarchies ourselves (based on a straightforward informal analysis of the examples). Our focus is on the generation of state spaces; we did not verify any properties. The goal of the experiments is to compare reductions in states and transitions obtained via our algorithm with reductions obtained via SPIN's standard partial-order reduction. As may be expected, similar to standard partial-order reduction, our algorithm performs best for systems with a large amount of concurrency. In all cases, we observe significantly larger reductions than the ones obtained with standard partial-order reduction. Moreover, in all cases, our algorithm reduces verification times. The overhead of upgrading the standard partial-order-reduction engine is marginalized by the gain in time because of the smaller number of generated states and transitions.

In the remainder, we show the results of three case studies. The experiments were performed on a Sun Ultra-10 machine, with a 299 MHz UltraSPARC-III processor and 128 MB of main memory, running the SunOS 5.6 operating system. All the verification times are given in seconds.

**Best-case example.** Our first case study consists of variants of system example2 of Figure 2. The systems we verified consist of N pairs of processes and N variables, each pair sharing one of these variables. The system with N=2 corresponds to system example2. Table 1 shows the obtained results, including the reductions in states and transitions in percentages compared to SPIN with standard partial-order reduction. The numbers deviate from the theoretical results given in Section 4 due to implementation details of SPIN. SPIN adds to each process a special end transition that is independent of all other transitions. The standard SPIN partial-order reduction captures the independence of these special end transitions. Our prototype implementation takes, in addition, advantage of the independence of some transitions involving shared variables, as explained in Section 4. We used a hierarchy of two layers, with the nontrivial layer consisting of clusters that coincided with process pairs.

<table>
<thead>
<tr>
<th>N</th>
<th>states</th>
<th>trans</th>
<th>time</th>
<th>states</th>
<th>trans</th>
<th>time</th>
<th>states</th>
<th>%</th>
<th>trans</th>
<th>%</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1356</td>
<td>108</td>
<td>0.1</td>
<td>60</td>
<td>76</td>
<td>&lt;0.1</td>
<td>30</td>
<td>50</td>
<td>66</td>
<td>61</td>
<td>&lt;0.1</td>
</tr>
<tr>
<td>3</td>
<td>329</td>
<td>784</td>
<td>0.1</td>
<td>304</td>
<td>480</td>
<td>&lt;0.1</td>
<td>66</td>
<td>78</td>
<td>66</td>
<td>86</td>
<td>&lt;0.1</td>
</tr>
<tr>
<td>4</td>
<td>1657</td>
<td>5216</td>
<td>0.1</td>
<td>1532</td>
<td>2908</td>
<td>0.1</td>
<td>138</td>
<td>91</td>
<td>138</td>
<td>95</td>
<td>&lt;0.1</td>
</tr>
<tr>
<td>5</td>
<td>8313</td>
<td>32680</td>
<td>0.9</td>
<td>7688</td>
<td>17064</td>
<td>0.7</td>
<td>282</td>
<td>96</td>
<td>282</td>
<td>98</td>
<td>&lt;0.1</td>
</tr>
</tbody>
</table>

Table 1: Results for the best-case example.

**Parity Computer.** The second example, taken from [2], models a Parity Computer with a tree structure. The system consists of a root module, N client modules as leaves, and join modules as intermediate nodes. The system with N=4 is shown in Figure 3. The figure also shows a clustering hierarchy that is immediately derived from the modular structure of the Parity Computer.

A client process starts with nondeterministically generating a bit value that it puts into the request variable that it shares with its parent join module. Subsequently, it continuously waits for an acknowledgment from its parent. Each time it receives an acknowledgment, it again sends an arbitrary bit value to its parent. A join process computes the parity (XOR) of its two inputs and transmits it upwards to its parent, while, simultaneously, sending an acknowledgment to its children. Eventually, parity bits are delivered to the root process.

Consider again the example in Figure 3. Our cluster-based partial-order-reduction algorithm takes advantage of the fact that a join process communicates with its parent and its children in alternating order. Because the cluster with root Join0 is independent of the cluster with root Join1, we can reduce the state space by basically serializing the transitions internal to one of these
clusters with those internal to the other one. SPIN’s standard reduction algorithm does not give any reduction because all transitions involve global variables. As Table 2 shows, the reduction with cluster-based partial-order reduction is quite impressive.

<table>
<thead>
<tr>
<th>N</th>
<th>states</th>
<th>trans</th>
<th>time</th>
<th>states</th>
<th>%</th>
<th>trans</th>
<th>%</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1749</td>
<td>4798</td>
<td>0.1</td>
<td>1294</td>
<td>26</td>
<td>2352</td>
<td>51</td>
<td>0.1</td>
</tr>
<tr>
<td>5</td>
<td>7933</td>
<td>27012</td>
<td>0.8</td>
<td>3938</td>
<td>50</td>
<td>6775</td>
<td>75</td>
<td>0.3</td>
</tr>
<tr>
<td>6</td>
<td>69615</td>
<td>288678</td>
<td>10.0</td>
<td>21620</td>
<td>69</td>
<td>38372</td>
<td>86</td>
<td>0.6</td>
</tr>
<tr>
<td>7</td>
<td>320095</td>
<td>1213520</td>
<td>47.3</td>
<td>25228</td>
<td>92</td>
<td>44730</td>
<td>98</td>
<td>1.6</td>
</tr>
<tr>
<td>8a</td>
<td>2782640</td>
<td>15381300</td>
<td>621.2</td>
<td>30377</td>
<td>99</td>
<td>55828</td>
<td>&gt;99</td>
<td>2.1</td>
</tr>
</tbody>
</table>

"Because of the large memory requirements, this experiment was performed on a Sun Ultra-Enterprise machine with three 248 MHz UltraSPARC-II processors and 2304 MB of main memory, running the SunOS 5.5.1 operating system.

Table 2: Results for the Parity Computer.

The reduction with cluster-based partial-order reduction is slightly worse (though of the same order of magnitude) than the reduction reported in [2] for the same examples, obtained with the Next heuristic. However, it is difficult to draw any final conclusions about the comparative efficiency of the two techniques based only on this one example. First, the input languages in which the models are specified are different, which inevitably leads to differences in the model. Second, the Parity-Computer example is one of the best cases for the Next heuristic and, as the authors note themselves in [2], there are many examples for which partial-order reduction gives better results than the Next heuristic.

**Concurrent Alternating-Bit Protocol.** Finally, we consider the Concurrent Alternating-Bit Protocol (CABP) of [13]. The CABP consists of six components, as depicted in Figure 4. Each component is modeled as a separate process.

![Figure 4: Concurrent Alternating-Bit Protocol](image)
The CABP uses the standard alternating-bit scheme to avoid communication errors. Component $A$ fetches data from its environment and transmits this data repeatedly through channel $K$ until an acknowledgment is received from $D$. $A$ does not wait for a negative response before retransmitting. Channel $K$ is unreliable in the sense that it can corrupt or lose data. The role of $B$ is to forward successfully received data to the environment; each correct reception is acknowledged to $C$. $C$ transmits acknowledgments repeatedly via unreliable channel $L$. $D$ receives acknowledgments from $L$ and passes them to $A$.

As for the Parity Computer, also for the CABP the standard reduction algorithm does not produce any reduction; all transitions involve communications through global synchronous (rendezvous) channels. The cluster-based reduction algorithm, however, capitalizes on part of the concurrency between the system modules, as the results in Figure 4 show. The hierarchy consists of two levels, with nontrivial level $\{A\}, \{K,B\}, \{C\}$, and $\{L,D\}$. The implementation of $A$ and $C$ is such that each action in these processes depends on both its neighbors. Thus, any other process clustering does not improve the results.

6 Conclusion

The main contribution of this paper is an enhancement of the partial-order-reduction scheme of [12, 19]. Using the inherent structure of concurrent systems, we improve the way the safety (i.e., independence and invisibility) of actions is determined syntactically during the compilation of the system specification. The resulting ample sets may contain actions from more than one process. Although ample sets with actions from several processes have been considered earlier (e.g., [1]), to the best of our knowledge, the idea of exploiting hierarchical system structure is not present in the literature. We implemented our algorithm on top of SPIN, by upgrading SPIN's standard partial-order-reduction engine. The prototype implementation has been tested on several examples known from the literature and the obtained results are encouraging: Compared to SPIN's standard partial-order-reduction algorithm, significantly larger reductions of state spaces are obtained and verification times are decreased.

It will be interesting to see how our approach works in combination with other state-space-reduction heuristics. Following [6], it is easy to show that our technique is fully compatible with symmetry reduction. The two techniques are orthogonal because they exploit different features of concurrent systems. We agree with the conjecture in [2] that partial-order reduction (and also our enhancement) is compatible with the Next heuristic. It seems though that cluster-based partial-order reduction and the Next heuristic are not fully orthogonal, because they capture to some extent the same redundancies in state spaces. It is interesting to study the relation between the Next heuristic and cluster-based partial-order reduction in more detail.

The main task in the near future is to fully automate our implementation. In the current prototype, the clustering hierarchy and safety levels must be included manually. A fully automatic implementation will allow us to test the implementation on larger, real-world examples. We also plan to take advantage of the improved partial-order reduction [10] introduced in the latest releases of SPIN, as well as the introduction of V-Promela [15]. Another interesting topic is the study of clustering heuristics (see, e.g., [14]). Good clustering heuristics might actually yield better clustering hierarchies than the ones obtained from the hierarchical structure specified by a system designer. Finally, our cluster-based algorithm is compatible with the upgrade of SPIN's engine for timed systems from [4]. It is very likely that it can be combined with recent attempts of partial-order reduction for timed automata [3, 5, 17].
References


If you want to receive reports, send an email to: m.m.j.philips@tue.nl (we cannot guarantee the availability of the requested reports)

**In this series appeared:**

<table>
<thead>
<tr>
<th>Volume</th>
<th>Authors</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>96/01</td>
<td>M. Voorhoeve and T. Basten</td>
<td>Process Algebra with Autonomous Actions, p. 12.</td>
</tr>
<tr>
<td>96/02</td>
<td>P. de Bra and A. Aerts</td>
<td>Multi-User Publishing in the Web: DreSS, A Document Repository Service Station, p. 12.</td>
</tr>
<tr>
<td>96/06</td>
<td>W.M.P. van der Aalst and T. Basten</td>
<td>Life-Cycle Inheritance A Petri-Net-Based Approach, p. 18.</td>
</tr>
<tr>
<td>96/07</td>
<td>M. Voorhoeve</td>
<td>Structural Petri Net Equivalence, p. 16.</td>
</tr>
<tr>
<td>96/11</td>
<td>T. Laan</td>
<td>AUTOMATH and Pure Type Systems, p. 30.</td>
</tr>
<tr>
<td>96/12</td>
<td>F. Kamardolbine and T. Laan</td>
<td>A Correspondence between Nuprl and the Ramified Theory of Types, p. 12.</td>
</tr>
<tr>
<td>96/13</td>
<td>T. Borghuis</td>
<td>Priorean Tense Logics in Modal Pure Type Systems, p. 61</td>
</tr>
<tr>
<td>96/14</td>
<td>S.H.J. Boi and M.A. Reniers</td>
<td>The J² C-bus in Discrete-Time Process Algebra, p. 25.</td>
</tr>
<tr>
<td>96/15</td>
<td>M.A. Reniers and J.J. Vereijken</td>
<td>Completeness in Discrete-Time Process Algebra, p. 139.</td>
</tr>
<tr>
<td>96/17</td>
<td>E. Boiten and P. Hoogenrijk</td>
<td>Nested collections and polymorphism, p. 11.</td>
</tr>
<tr>
<td>96/18</td>
<td>P.D.V. van der Sock</td>
<td>Real-Time Distributed Concurrency Control Algorithms with mixed time constraints, p. 71.</td>
</tr>
<tr>
<td>96/19</td>
<td>M.A. Reniers</td>
<td>Static Semantics of Message Sequence Charts, p. 71.</td>
</tr>
<tr>
<td>96/20</td>
<td>L. Feijs</td>
<td>Algebraic Specification and Simulation of Lazy Functional Programs in a concurrent Environment, p. 27.</td>
</tr>
<tr>
<td>96/23</td>
<td>W.M.P. van der Aalst</td>
<td>Structural Characterizations of sound workflow nets, p. 22.</td>
</tr>
<tr>
<td>96/24</td>
<td>M. Voorhoeve and W. van der Aalst</td>
<td>Conservative Adaption of Workflow, p.22</td>
</tr>
<tr>
<td>96/25</td>
<td>M. Vaccari and R.C. Backhouse</td>
<td>Deriving a systolic regular language recognizer, p. 28</td>
</tr>
<tr>
<td>97/06</td>
<td>M. Franssen</td>
<td>Tools for the Construction of Correct Programs: an Overview, p. 33.</td>
</tr>
<tr>
<td>97/07</td>
<td>J.C.M. Baeten and J.A. Bergstra</td>
<td>Bounded Stacks, Bags and Queues, p. 15.</td>
</tr>
</tbody>
</table>
97/08 P. Hoogendijk and R.C. Backhouse When do datatypes commute? p. 35.
97/10 P.C.N. v. Gorp, E.J. Luit, D.K. Hammer E.H.L. Aarts Distributed real-time systems; a survey of applications and a general design model, p. 31.
97/13 W.M.P. van der Aalst Exploring the Process Dimension of Workflow Management, p. 56.
97/14 J.F. Groote, F. Monin and J. Springintveld A computer checked algebraic verification of a distributed summation algorithm, p. 28.
97/15 M. Franssen λP: A Pure Type System for First Order Logic with Automated Theorem Proving, p. 35.
97/16 W.M.P. van der Aalst On the verification of inter-organizational workflows, p. 23
97/17 M. Vaccari and R.C. Backhouse Calculating a Round-Robin Scheduler, p. 23.
97/18 Werkgemeenschap Informatiewetenschap redactie: P.M.E. De Bra Informafiewetenschap 1997 Wetenschappelijke bijdragen aan de Vijfde Interdisciplinaire Conferentie Informatiewetenschap, p. 60.
98/02 M. Voorhoeve State / Event Net Equivalence, p. 25.
98/03 J.C.M. Baeten and J.A. Bergstra Deadlock Behaviour in Split and ST Bisimulation Semantics, p. 15.
98/05 D. Damis Flat Fragments of CTL and CTL*: Separating the Expressive and Distinguishing Powers, p. 22.
98/10 T. Basten and J. Hooman Process Algebra in PVS
98/11 J. Zwanenburg The Proof-assistent Yarrow, p. 15
98/14 T. Verhoef (artikel volgt)
99/01 V. Bos and J.J.T. Kleijn Structured Operational Semantics of μ, p. 27
99/02 H.M.W. Verbeek, T. Basten and W.M.P. van der Aalst Diagnosing Workflow Processes using Woflan, p. 44
<table>
<thead>
<tr>
<th>Year</th>
<th>Authors</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>99/03</td>
<td>R.C. Backhouse and P. Hoogendijk</td>
<td>Final Dialgebras: From Categories to Allegories</td>
<td>26</td>
</tr>
<tr>
<td>99/04</td>
<td>S. Andova</td>
<td>Process Algebra with Interleaving Probabilistic Parallel Composition</td>
<td>81</td>
</tr>
<tr>
<td>99/05</td>
<td>M. Franssen, R.C. Veltkamp and W. Wesselink</td>
<td>Efficient Evaluation of Triangular B-splines</td>
<td>13</td>
</tr>
<tr>
<td>99/06</td>
<td>T. Basten and W. v.d. Aalst</td>
<td>Inheritance of Workflows: An Approach to tackling problems related to change</td>
<td>66</td>
</tr>
<tr>
<td>99/10</td>
<td>T.A.C. Willemse</td>
<td>The Analysis of a Conveyor Belt System, a case study in Hybrid Systems and timed μ CRL</td>
<td>44</td>
</tr>
<tr>
<td>99/11</td>
<td>J.C.M. Baeten and C.A. Middelburg</td>
<td>Process Algebra with Timing: Real Time and Discrete Time</td>
<td>50</td>
</tr>
<tr>
<td>99/12</td>
<td>S. Andova</td>
<td>Process Algebra with Probabilistic Choice</td>
<td>38</td>
</tr>
<tr>
<td>99/13</td>
<td>K.M. van Hee, R.A. van der Toorn, J. van der Woude and P.A.C. Verkoulen</td>
<td>A Framework for Component Based Software Architectures</td>
<td>19</td>
</tr>
<tr>
<td>99/14</td>
<td>A. Engels and S. Mauw</td>
<td>Why men (and octopuses) cannot juggle a four ball cascade</td>
<td>10</td>
</tr>
<tr>
<td>99/16</td>
<td>G.J. Houben, P. Lemmens</td>
<td>A Software Architecture for Generating Hypermedia Applications for Ad-Hoc Database Output</td>
<td>13</td>
</tr>
<tr>
<td>99/17</td>
<td>T. Basten, W.M.P. v.d. Aalst</td>
<td>Inheritance of Behavior</td>
<td>83</td>
</tr>
<tr>
<td>99/18</td>
<td>J.C.M. Baeten and T. Basten</td>
<td>Partial-Order Process Algebra (and its Relation to Petri Nets)</td>
<td>79</td>
</tr>
<tr>
<td>99/19</td>
<td>J.C.M. Baeten and C.A. Middelburg</td>
<td>Real Time Process Algebra with Time-dependent Conditions</td>
<td>33</td>
</tr>
<tr>
<td>00/01</td>
<td>J.C.M. Baeten and J.A. Bergstra</td>
<td>Mode Transfer in Process Algebra</td>
<td>14</td>
</tr>
<tr>
<td>00/02</td>
<td>J.C.M. Baeten</td>
<td>Process Algebra with Explicit Termination</td>
<td>17</td>
</tr>
<tr>
<td>00/03</td>
<td>S. Mauw and M.A. Reniers</td>
<td>A process algebra for interworkings</td>
<td>63</td>
</tr>
<tr>
<td>00/04</td>
<td>R. Bloo, J. Hooman and E. de Jong</td>
<td>Semantical Aspects of an Architecture for Distributed Embedded Systems*</td>
<td>47</td>
</tr>
<tr>
<td>00/05</td>
<td>J.F. Groote and M.A. Reniers</td>
<td>Algebraic Process Verification</td>
<td>65</td>
</tr>
<tr>
<td>00/06</td>
<td>J.F. Groote and J. v. Wamel</td>
<td>The Parallel Composition of Uniform Processes with Data</td>
<td>19</td>
</tr>
<tr>
<td>00/07</td>
<td>C.A. Middelburg</td>
<td>Variable Binding Operators in Transition System Specifications</td>
<td>27</td>
</tr>
<tr>
<td>00/08</td>
<td>I.D. van den Ende</td>
<td>Grammars Compared: A study on determining a suitable grammar for parsing and generating natural language sentences in order to facilitate the translation of natural language and MSC use cases</td>
<td>33</td>
</tr>
<tr>
<td>00/09</td>
<td>R.R. Hoogerwoord</td>
<td>A Formal Development of Distributed Summation</td>
<td>35</td>
</tr>
<tr>
<td>00/10</td>
<td>T. Willemse, J. Tretmans and A. Klomp</td>
<td>A Case Study in Formal Methods: Specification and Validation on the OM/RR Protocol</td>
<td>14</td>
</tr>
</tbody>
</table>