Symbolic Determinisation of Extended Automata

Thierry Jéron, Hervé Marchand, and Vlad Rusu
Irisa/Inria Rennes, Campus de Beaulieu, 35042 Rennes France.
{Thierry.Jeron | Herve.Marchand | Vlad.Rusu} @iris.fr

Abstract. We define a symbolic determinisation procedure for a class of infinite-state systems, which consists of automata extended with symbolic variables that may be infinite-state. The subclass of extended automata for which the procedure terminates is characterised as bounded lookahead extended automata. It corresponds to automata for which, in any location, the observation of a bounded-length trace is enough to infer the first transition actually taken. We discuss applications of the algorithm to the verification, testing, and diagnosis of infinite-state systems.

Key words: symbolic automata, determinisation

1 Introduction

Most existing models of computation are nondeterministic, but they include restricted, deterministic versions as subclasses. A natural question is comparing the expressiveness of the general, nondeterministic class with that of the corresponding restricted, deterministic subclass. For example, it is well known that nondeterministic and deterministic finite automata on finite words are equivalent, but for finite automata on infinite words, the equivalence depends on the acceptance condition (e.g., Müller versus Büchi acceptance); and for pushdown and timed automata, the nondeterministic version is strictly more expressive than the deterministic one [1, 2].

Besides this theoretical interest, the distinction between nondeterministic and deterministic models has practical consequences. For example, verification consists in checking whether an implementation of a system satisfies a specification; both views of the system are modeled by automata of some kind. This problem can be seen as a language inclusion problem, which in turn can be encoded into a language emptiness problem (i.e., checking the emptiness of the language recognised by a product between the implementation and the complement of the specification). The complement of the specification is an automaton that accepts exactly the words that are rejected by the specification, and is easily computed if the specification is deterministic (by complementing the specification’s acceptance condition). Otherwise, if the specification is nondeterministic, it has to be determinised, i.e., turned into an equivalent deterministic machine.
Hence, determinisation is an important operation in formal verification. It is also important in other fields such as conformance testing and fault diagnosis where deterministic testers (resp. diagnosis) have to be derived from specifications that are, in general nondeterministic due to, e.g., partial observation.

In this paper we define a determinisation operation for a class of infinite-state systems, which consists of extended automata operating on symbolic variables and communicating with the environment via synchronising actions. Variants of this model are often encountered in the literature and can be used, e.g., for the formal specification of reactive systems. The determinisation procedure consists in iterating a sequence of local determinisation steps, which postpone operations on the variables until it becomes clear which exact operations should have been performed. The subclass of extended automata on which the procedure terminates is characterised as bounded-lookahead automata, for which the observation of a bounded-length trace is enough to infer the first transition actually taken.

The result is nontrivial because the order in which local determinisation steps are iterated has a strong influence on termination. The main difficulty was to find an order for which the bounded lookahead decreases at each iteration, thus ensuring termination of the procedure.

The rest of the paper is organized as follows. We first introduce extended automata and the determinisation operation by means of examples. Then, in Section 2 we formally define the syntax and semantics of extended automata, and in Section 3 the determinisation operation is formally defined. The operation may not terminate in general, and in Section 4 the subclass for which the procedure does terminate is precisely characterised via necessary and sufficient conditions. However, these conditions are undecidable, hence, we also provide sufficient, decidable conditions for termination. In Section 5 we discuss applications of our procedure to the verification, testing, and diagnosis of reactive systems, and conclude in Section 6. The technical report [3] contains proofs of all the results.

Example 1 (extended automata, determinisation). Figure 1 (left) depicts an extended automaton $\mathcal{S}$. In location $l_0$, the action $a$ occurs. If $x \geq 0$ then the control goes to location $l_1$ and the variable $x$ is decreased by 1, and if $x \leq 0$ then the control goes to location $l_2$ and $x$ is increased by 2. Clearly, if $x = 0$ then the next control location and the next value of $x$ are not uniquely defined: the system is nondeterministic.

The right-hand side of Figure 1 depicts the automaton $\det(\mathcal{S})$ obtained after determinising $\mathcal{S}$. Intuitively, the locations $l_1$ and $l_2$, which could be nondeterministically chosen as the next control location after an action $a$, are merged into one new location denoted by $\langle l_0, (l_1, l_2) \rangle$. A new transition labeled by $a$ goes from $l_0$ to $\langle l_0, (l_1, l_2) \rangle$. This transition is taken if $a$ occurs, and if $x$ satisfies the disjunction $x \geq 0 \lor x \leq 0$ (which actually simplifies to $true$). This condition is the disjunction of the guards of the two transitions involved in the nondeterministic choice in $\mathcal{S}$.

Note, however, that those transitions perform different assignments to variables: $x := x - 1$ for one, and $x := x + 2$ for the other. Hence, the new transition
Fig. 1. Left: extended automaton $S$  
Right: extended automaton $det(S)$

from $l_0$ to $(l_0, (l_1, l_2))$ of $det(S)$ does not “know” which assignment to perform. To solve this problem, the idea is to postpone assignments until it becomes clear which one of the transitions of the nondeterministic choice was actually taken, and then to “catch up” with the assignments in order to preserve the semantics.

Hence, if $b$ occurs after $a$, then the transition from $l_0$ to $l_1$ was taken (hence, $x := x - 1$ should have been performed), but if $c$ occurs after $a$, the transition from $l_0$ to $l_2$ was taken (hence $x := x + 2$ should have been performed). Note how the assignments are simulated in $det(S)$; the transition labeled by $b$ (resp. by $c$) has $x - 1$ (resp. $x + 2$) substituted for $x$ in its guard and assignments. To match the behaviour of $S$, in which the transition labeled by $b$ (resp. $c$) are fireable only after a transition labeled $a$ has been fired with $x \geq 0$ (resp. $x \leq 0$) holding, the guard of the transition labeled by $b$ (resp. $c$) in $det(S)$ is strengthened by $x \leq 0$ (resp. $x \geq 0$).

2 Extended automata

Extended automata consist of a finite control structure and a finite set of typed variables $V$. Each variable $x \in V$ takes values in some domain $\text{dom}_x$. A valuation $\nu$ of the variables $V$ is a function that associates to each variable $x \in V$ a value $\nu(x) \in \text{dom}_x$. The set of valuations of the variables $V$ is denoted by $V$. In the sequel, a predicate $P$ over variables $V$ is often identified with its set of “solutions”, i.e., the set of valuations $V' \subseteq V$ of the variables $V$ for which $P$ is true.

Definition 1 (extended automaton). An extended automaton (sometimes referred to simply as an automaton) is a tuple $S = \langle V, \Theta, L, t^0, \Sigma, T \rangle$:
- $V$ is a finite set of typed variables
- $\Theta$ is the initial condition, a predicate on $V$, assumed to have a unique solution $\nu_0 \in V$
- $L$ is a nonempty, finite set of locations and $l^0 \in L$ is the initial location,
- $\Sigma$ is a nonempty, finite alphabet of actions,
- $T$ is a set of transitions. Each transition $t \in T$ is associated with a tuple $\langle \alpha_t, G_t, a_t, A_t, d_t \rangle$, where
  - $\alpha_t \in L$ is called the origin of the transition,
  - $G_t$ is a Boolean expression over variables $V$, called the guard,
  - $A_t \in \Sigma$ is called the action of the transition,
  - $A_t$ is a set of assignments of the form $(x := A^x)_{x \in V}$ where, for each $x \in V$, the right-hand side $A^x$ of the assignment $x := A^x$ is an expression on $V$,
  - $d_t \in L$ is called the destination of the transition.

We sometimes write $t : (\alpha, G, a, A, d)$ to emphasise the tuple associated to $t$.

By slight abuse of notation, we shall denote by $\circ$ an operation of syntactical substitution: a guard $G$ (or an assignment $A$) is composed with another assignment $A'$ by replacing in $G$ (resp. in the right-hand side of $A$) all the variables by their corresponding right-hands sides from $A'$. Examples of such substitutions in guards and assignments have been given in Example 1 above.

The semantics of extended automata is described by labelled transitions systems.

**Definition 2 (Labelled Transition System (LTS)).** A Labelled Transition System is a tuple $S = (Q, Q^0, \Lambda, \rightarrow)$ where $Q$ is a set of states, $Q^0 \subseteq Q$ is the set of initial states, $\Lambda$ is a set of labels, and $\rightarrow \subseteq Q \times \Lambda \times Q$ is the transition relation.

The LTS semantics of an extended automaton enumerates the valuations $\nu$ of its variables $V$. For an expression $E$ involving (a subset of) $V$, and for $\nu \in V$, we denote by $E(\nu)$ the value obtained by substituting in $E$ each variable $x$ by its value $\nu(x)$.

**Definition 3 (Semantics of extended automata).** The semantics of an extended automaton $S = \langle V, \Theta, L, l^0, \Sigma, T \rangle$ is an LTS $\llbracket S \rrbracket = (Q, \{q^0\}, \Lambda, \rightarrow)$, where

- the set of states is $Q = L \times V$,
- the set of initial states is the singleton $\{q^0\} = \{ (l_0, \nu_0) \}$ where $\nu_0$ is the unique valuation satisfying $\Theta$,
- the set of labels is $\Lambda = T$,
- $\rightarrow$ is the smallest relation in $Q \times \Lambda \times Q$ defined by the following rule:

  $\langle (l, \nu), (l', \nu') \rangle \in Q \quad t : (l, G, a, A, l') \in T \quad G(\nu) = \text{true} \quad \nu' = A(\nu)$

  $\langle (l, \nu) \rightarrow (l', \nu') \rangle$
The rule says that the transition \( t : (l, G, a, A, l') \) is fireable in a state \( (l, \nu) \) if the guard \( G \) evaluates to true when the variables evaluate according to \( \nu \); then the transition takes the system to the state \( (l', \nu') \) where the assignment \( A \) of the transition maps the valuation \( \nu \) to \( \nu' \).

We extend this notion to sequences of transitions \( \sigma = t_1 \cdot t_2 \cdots t_n \in T^* \), saying that \( \sigma \) is fireable in a state \( q \in Q \) if there exists states \( q_1 = q, q_2, \ldots, q_n \in Q \) such that \( \forall i = 1 \ldots n-1, q_i \overset{t_i}{\rightarrow} q_{i+1} \). We then write \( q \vdash_\sigma \) to say that \( \sigma \) is fireable in \( q \). The transition sequence \( \sigma \) is initially fireable if it is fireable in the initial state \( q_0 \). A state \( q \) is reachable if there exists an initially fireable transition sequence \( \sigma \) leading to it, i.e., \( \exists \sigma \in T^*, q_0 \vdash_\sigma q \). We denote by \( \text{Reach}(S) \) the set of reachable states. For a sequence \( \sigma = t_1 \cdots t_n \in T^n \) \((n \geq 1)\), we let \( \text{first}(\sigma) \triangleq t_1 \).

**Definition 4 (trace).** The trace of a transition sequence \( \sigma = t_1 \cdot t_2 \cdots t_n \) is the projection \( \text{trace}(\sigma) = a_{t_1} \cdot a_{t_2} \cdots a_{t_n} \) of \( \sigma \) on the set \( \Sigma \) of actions. The set of traces of an extended automaton \( S \) is the set of traces of initially fireable transition sequences and is denoted by \( \text{Traces}(S) \).

### 3 Local Determinisation

Intuitively, an extended automaton is deterministic if in each location, the guards of the transitions labeled by the same action are mutually exclusive. Determinising an extended automaton \( S \) means computing a deterministic extended automaton \( \text{det}(S) \) with the same traces as \( S \).

**Definition 5 (deterministic extended automaton).** An extended automaton \( \langle V, \Theta, L, l_0, \Sigma, T \rangle \) is deterministic in a location \( l \in L \) if for all actions \( a \in \Sigma \) and each pair \( t_1 : (l, G_1, a, A_1, l_1) \) and \( t_2 : (l, G_2, a, A_2, l_2) \) of transitions with origin \( l \) and labeled by \( a \), the conjunction of the guards \( G_1 \land G_2 \) is unsatisfiable. The automaton is deterministic if it is deterministic in all locations \( l \in L \).

It is assumed that the guards are written in a theory where satisfiability is decidable, such as, e.g., combinations of quantifier-free Presburger arithmetic formulas, arrays, and lists. Such formulas are expressive enough to encode the most common data structures, and their satisfiability is decidable using, e.g., the classical Nelson-Oppen combination of decision procedures [4]. Note that determinism does not take reachability of states into account. However, since extended automata have a unique initial state, the definition of determinism is equivalent to the fact that the semantics of a deterministic extended automaton is a deterministic LTS in the usual sense.

Exemple 1 shows that determinising two transitions consists in merging the two transitions into a new one, and propagating guards and assignments onto transitions following them (cf. Figure 1). Formally, \( \text{follow}(t) \triangleq \{ t' \in T | \nu' = d_t \} \). We also denote by \( Id_V \) the identity assignments over variables \( V \), i.e., \( x := x \) for each \( x \in V \).
**Definition 6 (determinising two transitions).** Let \( \mathcal{S} \) be an extended automaton, and let \( t_1, t_2 \in T \) be two transitions with same origin \( o = o_{t_1} = o_{t_2} \) and same action \( a = a_{t_1} = a_{t_2} \). The automaton \( \text{det}_2(\mathcal{S}, t_1, t_2) \) is defined as follows. If \( G_{t_1} \land G_{t_2} \) is unsatisfiable then \( \text{det}_2(\mathcal{S}, t_1, t_2) = \mathcal{S} \), otherwise,

\[
\begin{align*}
& V_{\text{det}_2(\mathcal{S}, t, o)} = V_{\mathcal{S}}, \\
& \Theta_{\text{det}_2(\mathcal{S}, t, o)} = \Theta_{\mathcal{S}}, \\
& L_{\text{det}_2(\mathcal{S}, t, o)} = L_{\mathcal{S}} \cup \{ (o, \langle d_{t_1}, d_{t_2} \rangle) \}, \text{ where } \langle o, \langle d_{t_1}, d_{t_2} \rangle \rangle \text{ is a new location} \\
& L_{\text{det}_2(\mathcal{S}, t, o)}^0 = L_{\mathcal{S}}^0 \\
& \Sigma_{\text{det}_2(\mathcal{S}, t, o)} = \Sigma_{\mathcal{S}}, \\
& T_{\text{det}_2(\mathcal{S}, t, o)} = T_{\mathcal{S}} \setminus \{ t_1, t_2 \} \cup \{ t_{1,2} \} \cup T_1 \cup T_2, \text{ where} \\
& \quad t_{1,2} = \langle o, G_{t_1} \lor G_{t_2}, a, I_{d'V}, \langle o, \langle d_{t_1}, d_{t_2} \rangle \rangle \rangle, \\
& \quad \text{for } i = 1, 2, T_i = \bigcup_{t' \in \text{follow}(t_i)} \{ \text{mod}_i(t') \}, \text{ with the transitions } \text{mod}_i(t') : \\
& \qquad \langle o, \langle d_{t_i}, d_{t_2} \rangle \rangle, G_{t_i} \land G_{t'_i} \circ A_{t_i}, a_{t'_i}, A_{t'_i} \circ A_{t_i}, d_{t'_i}. 
\end{align*}
\]

The operation is illustrated in Figure 2. The transitions \( t_1 \) and \( t_2 \) in \( \mathcal{S} \) are replaced in \( \text{det}_2(\mathcal{S}, t_1, t_2) \) by the set of transitions \( \{ t_{1,2} \} \cup T_1 \cup T_2 \). The transition \( t_{1,2} \) leads from the common origin \( o \) of \( t_1, t_2 \) to the new location \( \langle o, \langle d_{t_1}, d_{t_2} \rangle \rangle \); its guard is the disjunction of those of \( t_1, t_2 \); hence, \( t_{1,2} \) can be fired whenever \( t_1 \) or \( t_2 \) can. However, \( t_{1,2} \) does not perform any of the assignments of \( t_1, t_2 \) because it does not know which ones to perform. The assignments are postponed onto copies of the transitions \( t' \in \text{follow}(t_i) \) (\( i = 1, 2 \)), modified in order to “catch up” with the effect of transition \( t_i \):

- the guard \( G_{\text{mod}_i(t')} \) equals \( G_{t_i} \land G_{t'_i} \circ A_{t_i} \). Intuitively, this amounts to firing the transition \( \text{mod}_i(t') \) in \( \text{det}_2(\mathcal{S}, t_1, t_2) \), under exactly the same conditions as the transition \( t' \) in \( \mathcal{S} \): the conjunct \( G_{t_i} \) “recalls” that \( t_i \) should have been fired before \( t' \), and by composing \( G_{t'_i} \) with \( A_{t_i} \), the effect of \( t_i \) on the variables is simulated before the guard of \( t' \) is evaluated.
- \( A_{\text{mod}_i(t')} \) performs the assignments of \( A_{t_i} \), composed with the assignments \( A_{t'_i} \).

In this way, the cumulated effect on the variables of firing in sequence \( t_i \) then \( t' \) in \( \mathcal{S} \) is simulated.

**Fig. 2.** Determinising 2 transitions: (left) before (right) after.
Definition 7 (Local determinisation in location). The local determinisation in location \( l \) of an extended automaton \( S = (V, \Theta, L, \nu, \Sigma, T) \), where \( l \in L \), is defined as follows. Let \( T_l \subseteq T \) be the set of all transitions with origin \( l \), then:

- \( \text{det}(S, l) = S \) if for every pair of distinct transitions \( t_1, t_2 \in T_l \) such that \( a_{t_1} = a_{t_2} \), the formula \( G_{t_1} \land G_{t_2} \) is unsatisfiable;
- otherwise, choose two distinct transitions \( t_1, t_2 \in T_l \) such that \( a_{t_1} = a_{t_2} \), \( G_{t_1} \land G_{t_2} \) is satisfiable, and let \( \text{det}(S, l) = \text{det}(\text{det}_2(S, t_1, t_2), l) \).

The operation terminates, as the set of pairs of nondeterministic transitions decreases.

4 Bounded-Lookahead Extended Automata

We now know how to eliminate nondeterminism from a location \( l \in L_S \). Then, to eliminate the nondeterminism globally from \( S \), one should iterate \( \text{det}(S, l) \) for all \( l \in L_S \). However, local determinisation creates new locations, which may themselves be nondeterministic and have to be determined, which may give rise to yet another set of nondeterministic locations, etc. This raises the question of whether the global determinisation process ever terminates. In this section we define a global determinisation procedure that we show to terminate exactly for the class of bounded lookahead extended automata. Intuitively, an automaton is deterministic with lookahead \( n \) if any nondeterministic choice can be resolved by looking \( n \) actions ahead.

Definition 8 (bounded lookahead). An automaton \( S = (V, \Theta, L, \nu^0, \Sigma, T) \) has lookahead \( n \in \mathbb{N} \) in a state \( q \in Q_{S^+} \) if \( \forall \sigma_1, \sigma_2 \in T^{n+1}, q \xrightarrow{\sigma_1} \land q \xrightarrow{\sigma_2} \land \text{trace}({\sigma_1}) = \text{trace}({\sigma_2}) \Rightarrow \text{first}(\sigma_1) = \text{first}(\sigma_2) \). The automaton has lookahead \( n \) in a set \( Q' \subseteq Q_{S^+} \) of states if it has lookahead \( n \) in every \( q \in Q' \). Finally, \( S \) has bounded lookahead if, for some \( n \in \mathbb{N} \), \( S \) has lookahead \( n \) in the whole set \( Q_{S^+} \).

We shall find it convenient to define the lookahead of a location of an automaton.

Definition 9 ((smallest) lookahead in location). An automaton \( S \) has lookahead \( n \) in location \( l \in L \) if \( S \) has lookahead \( n \) in the set \( \{ (l, \nu) | \nu \in V \} \). \( S \) has smallest lookahead \( n \in \mathbb{N} \) in a given location \( l \) if it has lookahead \( n \) in \( l \), and does not have lookahead \( n - 1 \) in \( l \). We denote by \( \text{look}(l, S) \in \mathbb{N} \) the smallest lookahead of location \( l \) in \( S \) (if it exists), otherwise, \( \text{look}(l, S) \triangleq \infty \).

For example, the automaton depicted in the left-hand side of Figure 3 has \( \text{look} = 1 \) in \( l_0 \) because, when \( e \) occurs, the left-hand side \( a \)-labeled transition must have been fired, but when \( b \) occurs, the right-hand side \( a \)-labeled transition has been fired.

On the other hand, the automaton depicted in the left-hand side of Figure 4 does not have \( \text{look} = 1 \) in \( l_0 \) because the occurrence of \( b \) does not reveal which of the \( a \)-labeled transitions was fired. However, the following action (either \( c \) or \( d \)) reveals all the past trace, hence, \( \text{look} = 2 \) in \( l_0 \) for the given automaton.
Fig. 3. Inherited nondeterminism may not decrease global lookahead.

Fig. 4. Created nondeterminism has decreased global lookahead.

**Definition 10 (global lookahead).** $\text{look}(S) \equiv \max_{l \in L_S} \{\text{look}(l, S)\}$. Clearly, a location $l$ is deterministic in an automaton $S$ iff $\text{look}(l, S) = 0$; and the automaton $S$ itself is deterministic iff $\text{look}(S) = 0$.

The following proposition says that the lookahead of an automaton does not increase by local determinisation.

**Proposition 1 (Global lookahead does not increase).** $\text{look}(\text{det}(S, l)) \leq \text{look}(S)$.

The following examples show that $\text{look}(S)$ may or may not decrease with local determinisation. Consider the automaton on the left-hand side of Figure 3, which has global lookahead 1. Determinising in $l_0$ leaves the automaton in the right-hand side, which still has the same global lookahead! The determinisation in $l_0$ in Figure 4, however, decreases the global lookahead of the automaton from 2 to 1.
The difference between these situations is the following: in Figure 3, the
determinisation step has merged the non-deterministic location \( l_2 \) into the new
location \( \langle l_0, \langle l_1, l_2 \rangle \rangle \), hence, the resulting automaton has inherited (in a sense
that will be made precise below) the non-determinism that \( l_2 \) had; because of
that non-determinism, the global lookahead has not decreased. On the other
hand, the determinisation step in Fig. 4 does not have this problem: both \( l_1, l_2 \)
are deterministic, and, even though the new location \( \langle l_0, \langle l_1, l_2 \rangle \rangle \) is non-deterministic, the non-determinism is created by the fact that \( l_1, l_2 \) bring one \( b \)-labeled transition each.

**Definition 11 (created/inherited non-determinism).** Let \( S \) be an extended
automaton and \( t_1, t_2 \) be two transitions of \( S \) involved into a non-determinism in
\( \alpha_{t_1} = \alpha_{t_2} = \alpha \). Let \( \langle \alpha, \langle d_{t_1}, d_{t_2} \rangle \rangle \) be the new location resulting from the deter-
minisation \( \det(S, t_1, t_2) \), and assume that \( \langle \alpha, \langle d_{t_1}, d_{t_2} \rangle \rangle \) is non-deterministic in \( \det(S, t_1, t_2) \). We say that this non-determinism is created if both \( d_{t_1}, d_{t_2} \) are
deterministic in \( S \), otherwise, the non-determinism is inherited.

Now, consider a global determinisation procedure that performs local deter-
minisation steps in a breadth-first order: the first iteration determinises the
non-deterministic locations of the original automaton, and each subsequent it-
eration determinises the new non-deterministic locations, generated during the
iteration that preceded it.

Figure 3 also illustrates the first iteration of such a breadth-first procedure
on the automaton in the left-hand side. The resulting automaton is depicted on
the right-hand side. Both automata have the same global lookahead \( = 1 \). Hence,
the lookahead cannot be used as a decreasing measure to ensure the termination
of the procedure.

Even worse, applying local determinisations in a depth-first order (i.e., deter-
minising new non-deterministic locations as soon as they are created) may
not terminate, even when the automaton has bounded lookahead. An example
is shown in Figure 5: the automaton in the left-hand side has global looka-
head 1, and, by determinising in \( l_0 \), one obtains the automaton depicted in the
right-hand side of the figure, which contains a sub-automaton isomorphic the
automaton in the left-hand side, with global lookahead still 1. After determinis-
ing in the newly created location, the sub-automaton is still there, and remains
present all through the process of depth-first determinisation, which, in this
case, clearly does not terminate.

Hence, applying local determinisation steps in depth-first or in breadth-
first order does not lead, in general, to a terminating global determinisation
procedure.

However, Proposition 2 below shows that if an iteration of a breadth-first
procedure only gives rise to created non-determinism, the global lookahead does
decrease.

**Proposition 2 (Global lookahead decreases if all new non-determinism
is created).** Let \( S' \) be an automaton obtained by determinising all non-determin-
istic locations \( \{l_1, \ldots, l_k\} \) of an automaton \( S \) in an arbitrary order, (i.e., \( S_0 = S \),
∀i ≤ k−1, S_{i+1} = det(S, l_i), and S' = S_k. If none of these local determinisation steps gave rise to inherited nondeterminism, then look(S') < look(S).

To ensure that all new nondeterminism is created, one must determinise locations whose direct successors are deterministic. But now we are faced with another difficulty: if the automaton has cycles in which every location is nondeterministic, it is impossible to choose a location on the cycle to start determinising with! This will lead us to “breaking” such cycles by determinising one location on each of them.

**Definition 12.** A location l' is a direct successor of a location l in S if there exists i ∈ ℤ such that o_i = l and d_i = l'. A cycle is a sequence c = t_1 . t_2 . . . . t_n ∈ ℤ such that ∀i = 1, . . . . n−1, d_i = o_{i+1}, and d_n = o_1. The cycle is elementary if moreover ∀i, j = 1, . . . . n−1, i < j ⇒ d_{ij} ≠ o_{i,j} holds. We say l ∈ c if ∃i ∈ {1, . . . . n}.l = d_i, denote by C(S) the set of cycles of S, and by C(S, l) = {c ∈ C(S) | l ∈ c}.

**Definition 13 (nondeterministic cycle).** A cycle c is nondeterministic if ∀i ∈ c, l is nondeterministic. We denote by N(S) the set of nondeterministic cycles of S.

**Lemma 1.** For S an automaton and all locations l ∈ L_S, C(det(S, l), l) ∩ N(det(S, l)) = ∅, and ∀c' ∈ C(S).c' ∉ C(S, l) ∧ c' ∉ N(S) ⇒ c' ∈ C(det(S, l)) \ N(det(S, l)).

**Proof.** For the first statement, note that l is deterministic in det(S, l), hence, by definition, a cycle c ∈ C(det(S, l), l) cannot be nondeterministic in det(S, l), i.e., it cannot be in N(det(S, l)). For the second statement, the left-hand side of the implication means that the cycle c' ∈ C(S) does not visit l, but visits some other location l' which is deterministic in S. Determinisation in l leaves c' unchanged, thus, c' ∈ C(det(S, l)), and l' is still deterministic in det(S, l), hence, c' ∉ N(det(S, l)). □
Lemma 1 says that cycles visiting \( l \) in \( \text{det}(S, l) \) are not nondeterministic, and cycles \( c' \) that do not visit \( l \) and that are not nondeterministic in \( S \) are still not nondeterministic cycles of \( \text{det}(S, l) \). The consequences are that determinising one location per elementary nondeterministic cycle generates an automaton without any nondeterministic cycles, and determinisation does not add new nondeterministic cycles.

We now introduce our global determinisation procedure (Fig. 6), which starts by “breaking” all elementary nondeterministic cycles, by determinising one location on each.

![Procedure \( \text{det}(S) \)](image-url)

**Theorem 1 (termination, sufficient condition).** \( \text{det}(S) \) terminates if \( \text{look}(S) < \infty \).

**Proof.** By Lemma 1 and Proposition 1, the elimination of nondeterministic cycles (first while loop in Figure 6) terminates and does not increase \( \text{look}(S) \). Consider the sets \( L' \subseteq L \) computed at each new iteration of the inner (third) while loop.

Note that \( L' \neq \emptyset \) and \( L'' = \emptyset \) implies that there exists a nondeterministic cycle in \( S_n \). Indeed, assume \( l_1 \in L' \), then \( L'' = \emptyset \) implies \( l_1 \notin L'' \), which implies that \( l_1 \) has a direct successor \( l_2 \in L_{\delta_n} \) where \( S_n' \) is also nondeterministic, which implies again \( l_2 \in L' \). The process continues, and we eventually build a nondeterministic cycle in \( S_n \), which is impossible since all nondeterministic cycles were eliminated.

Inside the inner while loop, \( L' \neq \emptyset \), and by the above reasoning, \( L'' \neq \emptyset \). Hence, the choose \( l \) operation (from \( L'' \)) inside the loop is always possible, and then determinising in location \( l \) decreases the cardinal of \( L' \) by one. Since \( L' \)
is finite \((L' \subseteq L_{sn})\) and its cardinal decreases, eventually \(L' = \emptyset\) and the inner while loop terminates. \(L' = \emptyset\) also means that at the end of the inner while loop, \(S_n'\) is deterministic in all locations \(L_{sn}\), hence, nondeterministic locations in \(S_n'\) are new.

For termination of the outer while loop, we prove \(\text{look}(S_{n+1}) < \text{look}(S_n)\).

We know that after the inner loop, the nondeterministic locations in \(S_n'\) are new (in \(L_{sn} \setminus L_{sn}\)) and cannot have inherited nondeterminism, because they were generated by determining locations in \(L''\), whose direct successors are, by construction, deterministic. Finally, by Proposition 2, \(\text{look}(S_n') < \text{look}(S_n)\), and \(S_{n+1}\) becomes \(S_n'\) after \(n\) is incremented, and the proof is done. \(\square\)

The fact that bounded lookahead is necessary for termination is based on:

**Proposition 3 (look decreases by at most 1).** \(\text{look}(\text{det}_2(S, t_1, t_2)) \geq \text{look}(S) - 1.\)

Then, a finite sequence of \(\text{det}_2()\) operations cannot decrease lookahead from \(\infty\) to \(0\);

**Theorem 2 (necessary condition).** If \(\text{det}(S)\) terminates then \(\text{look}(S) < \infty.\)

This concludes the study of the procedure’s termination. It also preserves traces:

**Theorem 3.** If \(\text{det}(S)\) terminates then \(\text{Traces}(\text{det}(S)) = \text{Traces}(S)\).

The determinisation procedure can be improved using approximate reachability analysis. Assume that an over-approximation \(\text{Reach}^\alpha \supseteq \text{Reach}(S)\) of the reachable set of states is known (e.g., by abstract interpretation). Moreover, assume that this set is described using a formula in the same logic as the automaton’s guards, which we have assumed to be decidable for satisfiability (cf. Section 2). Then, Definition 5 of a deterministic extended automaton can be weakened, by requiring that \(\text{Reach}^\alpha \land G_{t_1} \land G_{t_2}\) be unsatisfiable (instead of \(G_{t_1} \land G_{t_2}\) unsatisfactory).

This new definition of determinism increases the subclass of extended automata on which the determinisation procedure terminates. The procedure now terminates for automata satisfying a modified definition of bounded lookahead, which, intuitively, requires only states in the set \(\text{Reach}^\alpha\) (instead of \(Q_{[t]}\)) to have bounded lookahead.

**Checking for Bounded Lookahead** The bounded lookahead condition is clearly undecidable for extended automata. We now give a sufficient criterion for this condition. We need a notion of product of extended automata:

**Definition 14 (Synchronous Product).** For \(j = 1, 2\), the extended automata \(S_j = \langle V_j, \Theta_j, L_j, l_0^j, \Sigma_j, T_j \rangle\) are compatible if \(V_1 \cap V_2 = \emptyset\) and \(\Sigma_1 = \Sigma_2\). The synchronous product \(S = S_1 || S_2\) of two compatible automata \(S_1, S_2\) is the automaton \(\langle V, \Theta, L, l_0, \Sigma, T \rangle\) with: \(V = V_1 \cup V_2, \Theta = \Theta_1 \land \Theta_2, L = L_1 \times L_2, l_0 = \langle l_0^1, l_0^2 \rangle, \Sigma = \Sigma_1 = \Sigma_2\), and the set \(T\) of transitions of the composed system is the smallest set defined by the rule:

\[
\begin{align*}
t_1 : \langle l_1, a, G_1, A_1, l_1' \rangle & \in T_1 \\
t_2 : \langle l_2, a, G_2, A_2, l_2' \rangle & \in T_2 \\
t : \langle (l_1, l_2), a, G_1 \land G_2, A_1 \cup A_2, (l_1', l_2') \rangle & \in T
\end{align*}
\]
Then, the bounded lookahead condition for an extended automaton can be equivalently formulated as follows. Consider an extended automaton $S = \langle V, \Theta, L, l_0, \Sigma, T \rangle$, and let the primed copy $S'$ of $S$ be the automaton obtained by “priming” all the components of $S$ except the alphabet $\Sigma$, i.e., $S' = \langle V', \Theta', L', l_0', \Sigma, T' \rangle$, where $V' = \{ \nu' | \nu \in V \}$, $L' = \{ l | l \in L \}$, and for states $q' = (l', \nu') = (l', \nu')$ where $\nu'$ is the same valuation as $\nu$, but for variables $V'$, i.e., $\forall x' \in V'$, $\nu'(x') \equiv \nu(x)$.

**Proposition 4 (checking for bounded lookahead).** An extended automaton $S$ has bounded lookahead iff, for all $q, q_1, q_2 \in Q_s$ and distinct transitions $t_1, t_2 \in T_s$ with $a_{t_1} = a_{t_2}$, if $q \xrightarrow{t_1} q_1 \land q \xrightarrow{t_2} q_2$ then there exists no infinite execution in $S||S$ starting from $(q_1, q_2)$, where $S'$ denotes the primed copy of $S$.

The conditions of Proposition 4 are decidable if $S$ is finite-state but are not decidable in general. For infinite-state extended automata $S$, we can build finite-state abstractions $S^\alpha$ that simulate the transition sequences $\sigma$ of $S$ (i.e., whenever $q \xrightarrow{\sigma} q'$ holds in $S$, $\alpha(q) \alpha(\sigma) \alpha(q')$ holds in $S^\alpha$). The bounded lookahead conditions of Proposition 4 can be then automatically checked on $S^\alpha$, and, if they hold, the simulation property guarantees that they also hold on $S$. This gives a sufficient criterion for bounded lookahead, which is, in general, not necessary ($S^\alpha$ may contain cycles not present in $S$), and whose precision can be improved by taking more precise abstractions $S^\alpha$.

5 Applications of Determinisation

**Verification** A standard verification problem is that of trace (or language) inclusion; given two systems $I$ (the implementation) and $S$ (the specification), decide whether $\text{Traces}(I) \subseteq \text{Traces}(S)$. When $I, S$ are extended automata and $S$ is deterministic, the problem reduces to a reachability problem in the extended automaton $I||S$, where $S$ is obtained from $S$ by adding a new location $\text{fail} \notin L$, and for each $l \in L$ and $a \in \Sigma$, a new transition with $l_1$ destination $\text{fail}$, action $a'$, identity assignments, and guard $\bigwedge_{(l, a, A_1, A_2, l_1) \in T} \neg a'$. The new transitions allow actions in $S$ whenever they are not allowed in $S$. Hence, when $S$ is deterministic, $\text{Traces}(I) \subseteq \text{Traces}(S)$ iff no location in the set $\{ (l, \text{fail} | l \in L_z) \}$ is reachable in $I||S$.

When $S$ is not deterministic, the above statement is incorrect. Let $S$ be the nondeterministic automaton in the left-hand side of Figure 3. A naive application of the completion operation on $S$ builds a transition labeled $b$ from $l_1$ to $\text{fail}$, suggesting that $a \cdot b$ is not a trace of $S$, which is obviously false. In particular, verification would wrongly declare erroneous an implementation that exhibits the trace $a \cdot b$. Hence, to be adequate for verification, $S$ has to be *determinised* before being completed.
Conformance Testing Conformance testing is a functional testing that consists in comparing a black-box implementation \( Z \) to a formal specification \( S \) according a conformance relation. The implementation is a black box, i.e., only its interface (input and output alphabet) is known. In [5] we show that conformance of an implementation \( Z \) to a specification according to the standard \( \text{ooco} \) relation [6] is equivalent to the fact that running a canonical tester in parallel with the implementation never reaches a certain set of locations. The tester can be automatically computed from the specification using operations similar to the completion operation, defined above, and, of course, determinisation. Without determinisation, the tester might wrongly declare non-conformant an implementation that is conformant to the specification (a phenomenon similar to that exhibited by the trace \( a \cdot b \), noted in the previous paragraph).

Fault Diagnosis The determinisation problem for extended automata also has a close relationship with diagnosis for discrete event systems [7]. For instance, an extended automaton with bounded lookahead can be seen as an automaton in which nondeterministic choices are diagnosable; and checking membership to the class of bounded lookahead automata can be reduced to a diagnosability problem in this model. Also, the sufficient criterion for bounded lookahead (around Proposition 4) was inspired by the algorithm used to check diagnosability [8], based on the search of specific cycles in a product of the specification with itself.

Conversely, it could be profitable to re-define diagnosability in terms of our bounded lookahead condition, in order to capture a notion of diagnosability for richer, infinite-state models. Finally, the construction of a diagnoser from an automaton specifying a plant and a fault model is based on determinisation; one has to determinise the plant “decorated” with past occurrences of (unobservable) faults. Our determinisation procedure then constitutes a basic block for the construction of diagnosers from plants specified as extended automata, thus extending the works on diagnosis to expressive, infinite-state models.

6 Conclusion, Related Work, and Future Work

In this paper we present a determinisation procedure for extended automata and prove that the procedure terminates exactly for the class of extended automata with bounded lookahead. The intuition behind this class is that in any location, for any trace, there exists a bounded number of steps after which the first transition taken is uniquely identified. Technical difficulties for proving termination arise from the fact that the order in which elementary determinisation steps are applied has a strong influence on termination. The main difficulty was to find an adequate order, for which the bounded lookahead provides a decreasing measure.

The models of extended automata considered in this paper only have observable actions. One can also consider models with internal (unobservable) actions.
In this case, determinisation first consists in an extended \( \epsilon \)-closure generalising that of finite automata. The extended \( \epsilon \)-closure algorithm is then based on the propagation of guards and actions onto the next transitions labeled by observable actions [9], and terminates iff there are no cycles of transitions labeled by internal actions.

The present work was initially motivated by \textit{conformance testing}, more specifically, model-based testing based on the \textit{ioco} theory [6]. In this framework, off-line test generation (computation of test cases from specifications) involves \textit{determinising} the specification in order to compute the next possible observable actions after each trace, and, therefore, to obtain \textit{deterministic} test cases [10]. In that work, we consider an extension of the model presented here (actions are either inputs or outputs and may carry communication parameters), which can be handled by a small modification of our determinisation procedure. The procedure also has potentially interesting application in the verification and diagnosis of infinite-state systems.

An alternative approach, which is also used in conformance testing and in fault diagnosis, is on-the-fly determinisation of a bounded number of transitions of a (basic, symbolic, or timed) automaton, starting from the initial state [6, 11, 12]. In this case, the problems related to termination disappear, because the number of determinisation steps is finite and defined in advance by the bounded exploration depth. However, this approach cannot be used for constructing canonical testers, which we found to be a useful object, and cannot be used for proving trace inclusion.

References