Expand, Enlarge, and Check

New algorithms for the coverability problem of WSTS

G. Geeraerts [1], J.-F. Raskin [1], L. Van Begin [1,2]

Département d'Informatique, Université Libre de Bruxelles
Boulevard du Triomphe, CP 212 – B-1050 Bruxelles
Telephone: +32 2 650 59 14 *Telefax: +32 2 650 56 04*

Abstract

In this paper, we present a general algorithmic schema called 'Expand, Enlarge and Check' from which new algorithms for the coverability problem of WSTS can be constructed. We show here that our schema allows us to define forward algorithms that decide the coverability problem for several classes of systems for which the Karp and Miller procedure cannot be generalized, and for which no complete forward algorithms were known. Our results have important applications for the verification of parameterized systems and communication protocols.

A preliminary version of this paper has been published as [1] in the proceedings of FST&TCS 2004.

Key words: Well-structured transition systems, verification, coverability problem, parameterized systems, Petri nets, lossy channel systems.

1 Introduction

Model-checking is nowadays widely accepted as a powerful technique for the automatic verification of reactive systems that have natural finite state abstractions. However, many reactive systems are only naturally modeled as infinite-state systems. This is why a large research effort was done in the recent years to allow the direct application of model-checking techniques to

Email addresses: gigeerae@ulb.ac.be (G. Geeraerts), jraskin@ulb.ac.be (J.-F. Raskin), lvbegin@ulb.ac.be (L. Van Begin).

[1] This author has been partially supported by the FRFC grant 2.4530.02.
[2] This author has been supported by a "First Europe" grant EPH3310300R0012 of the Walloon Region.

infinite-state models. This research line has shown successes for several interesting classes of infinite-state systems, for example: timed automata [2], hybrid automata [3], FIFO channel systems [4–6], extended Petri nets [7,8], broadcast protocols [9], etc.

General decidability results hold for a large class of infinite-state systems called the *well-structured transition systems*, WSTS for short. WSTS are transition systems whose sets of states are well-quasi ordered and whose transition relations enjoy monotonicity properties with respect to the well quasi-ordering. Examples of WSTS are Petri nets [10], monotonic extensions of Petri nets (Petri nets with transfer arcs [11], Petri nets with reset arcs [12], and Petri nets with non-blocking arcs [13]), Broadcast protocols [14], Lossy FIFO systems [5]. For all those classes of infinite-state systems, we know that an interesting and large class of *safety properties* are decidable by reduction to the *coverability problem*. The coverability problem is defined as follows: 'given a WSTS for the well-quasi order $\leq$, and two states of his c_1 and c_2, does there exist a state c_3 which is reachable from c_1 and such that $c_2 \leq c_3$?' (in that context, we say that c_3 covers c_2)

There exists a general algorithm to solve the coverability problem [15,16] which is applicable to all the classes of infinite-state systems cited above as examples of WSTS. Note that by algorithm, we mean a procedure that decides the problem, and so, is guaranteed to terminate. This algorithm is symbolic: it manipulates upward-closed sets of states (for the wqo) and applies a *backward exploration* of the state space by iterating the Pre operator (a function that returns all the states that have a one-step successor in a given set of states). While very elegant, this backward algorithm is often inefficient in practice. On the other hand, it is well-known that *forward exploration* of state spaces is usually much more efficient [17]. Unfortunately, there is currently no general forward algorithm that is able to solve the coverability problem for all the examples above. In fact, with the notable exception of Petri nets for which the Karp and Miller (KM, for short) procedure [18] is a forward algorithm that solves the coverability problem, the forward approaches proposed in the literature so far are incomplete.

Let us try to understand the rationale behind this situation. First, when applied to a Petri net, the KM procedure computes a finite representation of the so-called *covering set* of the net, this set is the smallest downward-closed set of markings that includes the set of reachable markings of the net. This set is perfect to solve the coverability problem because for any marking m, the covering set covers m if and only if the set of reachable markings covers m. The main ingredient of the KM procedure is a simple forward exploration of the state space of the net combined with a simple acceleration technique. As this procedure is simple and elegant, there have been several attempts to generalize it [19,14]. Unfortunately, those generalisations try to compute an effective

representation of the exact covering set. It has been shown later [12] that, although this set always exists and has a finite representation, it is impossible to construct it effectively, for all the examples of WSTS above, see [12,13] for the details (with the exception of Petri nets). As a consequence, the recent proposal of forward exploration techniques for WSTS have given up the idea of completeness: either they are not guaranteed to terminate [14,20] or they are approximate [21] (and they may be inconclusive on some examples). The main contribution of this paper is to show that it is not necessary to give up the idea of completeness when trying to define forward exploration techniques to decide the coverability problem for a large class of WSTS. This class includes all the classes of systems cited above as examples.

More precisely, we show that there exists a simple schema of algorithms, that we call 'Expand, Enlarge and Check', which constructs a sequence of abstractions that are more and more precise. This schema is guaranteed to provide, after a finite number of steps, an abstraction which is sufficiently precise to decide the coverability problem. Those abstractions are constructed from reachable states together with elements taken in a well chosen *domain of limits*. To show the practical interest of our method, we show how to obtain from our general schema an efficient forward algorithm for a class of extended Petri nets that subsumes *Petri nets with transfer arcs, with reset arcs and with non-blocking arcs*. We also show that our method can similarly be applied to the class of *Lossy Channel Systems*, and produce a forward algorithm for this class of systems too.

Plan of the paper. The rest of this work is organized as follows. In section 2, we recall several definition and results about well-quasi orderings, (effective) well-structured transition systems, coverability sets (and their finite representations), the coverability problem and And-Or graphs (and their related avoidability problem). After these preliminaries, section 3 explains how we compute under and over-approximations of the systems considered, and studies their properties. These two sorts of approximations will turn out to be the basis of the 'Expand, Enlarge and Check' approach to solve the coverability problem, which we discuss in section 4. Since 'Expand, Enlarge and Check' is nothing but a general schema of algorithm, we provide the reader with practical evidence of its possible application to two important classes of WSTS (i.e., strongly monotonic Petri nets and lossy channel systems), in section 5 and 6 respectively. Finally, section 7 draws some conclusion.

Additional online material. A web page dedicated to 'Expand, Enlarge and Check' is available at: `http://www.ulb.ac.be/di/ssd/ggeeraer/eec/`. It provides an access to relevant papers, as well as a set of practical examples we are able to verify thanks to the algorithms presented here.

2 Preliminaries

In this section, we recall some fundamental results about *well-quasi orderings* and *well-structured transition systems* (the systems we analyze here). We show how to *finitely* represent upward- and downward-closed sets of states (which will allow us to devise *symbolic* algorithms). The definition of the *coverability problem* is also recalled.

At the end of the section, we discuss And-Or graphs. These objects will be useful to represent abstractions of systems, and we will need to decide whether the set of executions represented by a given And-Or graph always leads to bad states. This question is formalized by the *And-Or graph avoidability problem*.

Well quasi-orderings and adequate domains of limits. A *well-quasi ordering* $\leq$ on the elements of a set C (wqo for short) is a *reflexive* and *transitive* relation such that for any infinite sequence $c_0 c_1 \ldots c_n \ldots$ of elements in C, there exist two indices i and j, such that $i < j$ and $c_i \leq c_j$.

Let $\langle C, \leq \rangle$ be a well-quasi ordered set. A $\leq$-*upward-closed set* $U \subseteq C$ is such that for any $c \in U$, for any $c' \in C$ such that $c \leq c'$: $c' \in U$. A $\leq$-*downward closed set* $D \subseteq C$ is such that for any $c \in D$, for any $c' \in C$ such that $c' \leq c$: $c' \in D$. It is well-known that any $\leq$-upward-closed set $U \subseteq C$ is uniquely determined by its finite set of minimal elements. Formally, a set of $\leq$-*minimal* elements $\mathsf{Min}(U)$ of a set $U \subseteq C$ is a minimal set such that $\mathsf{Min}(U) \subseteq U$ and $\forall s' \in U : \exists s \in \mathsf{Min}(U) : s \leq s'$. The following proposition is a direct consequence of wqo:

Proposition 1 *Let $\langle C, \leq \rangle$ be a wqo set and $U \subseteq C$ be an $\leq$-upward-closed set, then: $\mathsf{Min}(U)$ is finite and $U = \{c \mid \exists c' \in \mathsf{Min}(U) : c' \leq c\}$.*

Thus, any $\leq$-upward-closed set can be *effectively represented* by its finite set of minimal elements. $\leq$-Downward-closed sets are more difficult to represent effectively. To obtain a finite representation of those sets, we must use well-chosen limit elements $\ell \notin C$ to represent $\leq$-downward-closures of infinite increasing chains of elements. Thus, we introduce the notion of *adequate* domain of limits.

Definition 1 Let $\langle C, \leq \rangle$ be a well-quasi ordered set and L be a set of elements disjoint from C, the tuple $\langle L, \sqsubseteq, \gamma \rangle$ is called an *adequate domain of limits* for $\langle C, \leq \rangle$ if the following conditions are satisfied:

(L_1) *representation mapping*: $\gamma : L \cup C \mapsto 2^C$ associates to each element in $L \cup C$ a $\leq$-downward-closed set $D \subseteq C$, furthermore, for any $c \in C$, we impose that $\gamma(c) = \{c' \mid c' \leq c\}$. In the following, γ is extended to sets $\mathcal{S} \subseteq L \cup C$ in the natural way: $\gamma(\mathcal{S}) = \cup_{c \in \mathcal{S}} \gamma(c)$;

(L_2) *top element*: there exists a special element $\top \in L$ such that $\gamma(\top) = C$;
(L_3) *precision order*: the elements of $L \cup C$ are ordered by the quasi-order $\sqsubseteq$, defined as follows: $d_1 \sqsubseteq d_2$ if and only if $\gamma(d_1) \subseteq \gamma(d_2)$;
(L_4) *completeness*: for any $\leq$-downward-closed set $D \subseteq C$, there exists a finite set $D' \subseteq L \cup C$ such that $\gamma(D') = D$.

Well-structured transition systems and coverability problem. A *transition system* is a tuple $S = \langle C, c_0, \rightarrow \rangle$ where C is a (possibly infinite) set of states, $c_0 \in C$ is the initial state, $\rightarrow \subseteq C \times C$ is a transition relation. In the following, $c \rightarrow c'$ will denote that $(c, c') \in \rightarrow$. For any state c, $\mathsf{Post}(c)$ denotes the set of one-step successors of c, i.e. $\mathsf{Post}(c) = \{c' \mid c \rightarrow c'\}$. This operator is extended to sets of states $C' \subseteq C$ as follows: $\mathsf{Post}(C') = \{c \mid \exists c' \in C' : c' \rightarrow c\}$. A *path* of S is a sequence of states $c_1, c_2, \ldots, c_k$ such that $c_1 \rightarrow c_2 \rightarrow \cdots \rightarrow c_k$. A state c' is reachable from a state c, noted $c \rightarrow^* c'$, if we have a path $c_1, c_2, \ldots, c_k$ in S with $c_1 = c$ and $c_k = c'$. Given a transition system $S = \langle C, c_0, \rightarrow \rangle$, $\mathsf{Reach}(S)$ denotes the set $\{c \in C \mid c_0 \rightarrow^* c\}$. Finally, we require a transition system to be without deadlock states[3]. That is, for any state $c \in C$, there exists $c' \in C$ such that $c \rightarrow c'$.

Definition 2 A transition system $S = \langle C, c_0, \rightarrow \rangle$ is a *well-structured transition system* for the quasi order $\leq \subseteq C \times C$ if the two following properties hold:

(W_1) *well-ordering*: $\leq$ is a well-quasi ordering and
(W_2) *monotonicity*: for all $c_1, c_2, c_3 \in C$ such that $c_1 \leq c_2$ and $c_1 \rightarrow c_3$, there exists $c_4 \in C$ such that $c_3 \leq c_4$ and $c_2 \rightarrow^* c_4$.

Remark that, in this definition, condition W_2 is more general than the classical one-step monotonicity condition. Condition W_2 can be found, for instance in [16], where it is called 'compatibility condition'.

From now on, $S = \langle C, c_0, \rightarrow, \leq \rangle$ will denote the well-structured transition system $\langle C, c_0, \rightarrow \rangle$ for $\leq$. In the sequel, we need to manipulate algorithmically WSTS and adequate domain of limits. In particular, we need the following effectiveness properties:

Definition 3 A WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ and an adequate domain of limits $\langle L, \sqsubseteq, \gamma \rangle$ are *effective* if the following conditions are satisfied:

(E_1) C and L are recursively enumerable;
(E_2) for any $c_1, c_2 \in C$, we can decide whether $c_1 \rightarrow c_2$;

[3] Note that this condition is not restrictive since we can always add a self-loop on the deadlock. Remark that this does not change the set of states that are covered in the system.

($\mathsf{E_3}$) for any $d \in L \cup C$ and for any finite subset $D \subseteq L \cup C$, we can decide whether $\mathsf{Post}(\gamma(d)) \subseteq \gamma(D)$;
($\mathsf{E_4}$) For any finite subsets $D_1, D_2 \subseteq L \cup C$, we can decide whether $\gamma(D_1) \subseteq \gamma(D_2)$.

These four conditions are necessary to ensure the effectiveness and termination of the algorithms we are about to present. However, it is important to remark that the domains proposed in the literature to handle forward analysis of WSTS, respect these conditions. For instance, in sections 5 and 6, we recall the domains of *extended markings* and *simple regular expressions* to handle extended Petri nets and lossy channel systems respectively. From classical results of the literature, it is not difficult to deduce that conditions ($\mathsf{E_1}$) through ($\mathsf{E_4}$) hold on these two domains.

Problem 1 The *coverability problem for well-structured transition systems* is defined as follows: 'Given a well-structured transition system S and the $\leq$-upward-closed set $U \subseteq C$, determine whether $\mathsf{Reach}(S) \cap U = \emptyset$?'

To solve the coverability problem, we use covering sets, defined as the downward-closure of the set of reachable configurations:

Definition 4 Let $S = \langle C, c_0, \rightarrow, \leq \rangle$ be a WSTS. The *covering set* of S, noted $\mathsf{Cover}(S)$, is the set $\{c \mid \exists c' \in \mathsf{Reach}(S) : c \leq c'\}$.

The following proposition states that the covering set is indeed suitable to decide the coverability problem.

Proposition 2 ([19]) *For any* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, the covering set of S is such that for any $\leq$-upward-closed set $U \subseteq C$:* $\mathsf{Reach}(S) \cap U = \emptyset$ *if and only if* $\mathsf{Cover}(S) \cap U = \emptyset$.

Effective representation of the covering set. Let $S = \langle C, c_0, \rightarrow, \leq \rangle$ be a WSTS with an adequate domain of limits $\langle L, \sqsubseteq, \gamma \rangle$ for $\langle C, \leq \rangle$. By property $\mathsf{L_4}$ of Definition 1, there exists a finite subset $\mathsf{CS}(S) \subseteq L \cup C$ such that $\gamma(\mathsf{CS}(S)) = \mathsf{Cover}(S)$. In the following, $\mathsf{CS}(S)$ is called a *coverability set* of the covering set $\mathsf{Cover}(S)$ and it is a finite representation of that set.

And-Or graphs and their avoidability problem. An *And-Or graph* is a tuple $G = \langle V_A, V_O, v_i, \Rightarrow \rangle$ where $V = V_A \cup V_O$ is the set of nodes (V_A is the set of 'And' nodes and V_O is the set of 'Or' nodes), $V_A \cap V_O = \emptyset$, $v_i \in V_O$ is the initial node, and $\Rightarrow \subseteq (V_A \times V_O) \cup (V_O \times V_A)$ is the transition relation such that for any $v \in V$, there exists $v' \in V$ with $(v, v') \in \Rightarrow$.

Definition 5 A *compatible unfolding* of an And-Or graph $G = \langle V_A, V_O, v_i, \Rightarrow \rangle$ is an infinite labelled tree $T_G = \langle N, root, B, \Lambda \rangle$ where: (i) N is the set of nodes of T_G, (ii) $root \in N$ is the root of T_G, (iii) $B \subseteq N \times N$ is the transition

relation of T_G, (iv) $\Lambda : N \mapsto V_A \cup V_O$ is the labelling function of the nodes of T_G by nodes of G. Λ respects the three following compatibility conditions (Λ is extended to sets of nodes in the usual way):

- (C_1) $\Lambda(root) = v_i$;
- (C_2) for all $n \in N$ such that $\Lambda(n) \in V_A$, we have that: (i) for all nodes $v' \in V_O$ such that $\Lambda(n) \Rightarrow v'$, there exists one and only one $n' \in N$ such that $B(n, n')$ and $\Lambda(n') = v'$, and conversely (ii) for all nodes $n' \in N$ such that $B(n, n')$, there exists $v' \in V_O$ such that $\Lambda(n) \Rightarrow v'$ and $\Lambda(n') = v'$.
- (C_3) for all $n \in N$ such that $\Lambda(n) \in V_O$, there exists one and only one $n' \in N$ such that $B(n, n')$, and $\Lambda(n) \Rightarrow \Lambda(n')$;

Problem 2 The *And-Or Graph Avoidability Problem* is defined as follows: 'Given an And-Or graph $G = \langle V_A, V_O, v_i, \Rightarrow \rangle$ and a set $E \subseteq V_A \cup V_O$, does there exist $T = \langle N, root, \Lambda, B \rangle$, a compatible unfolding of G such that $\Lambda(N) \cap E = \emptyset$?'. When the answer is positive, we say that E is *avoidable* in G.

It is well-known that this problem is complete for *PTIME* [22].

3 Under and Over-approximations

In the present section, we define two kinds of (parameterized) approximations of WSTS that will be used by our new schema of algorithm (which is discussed in section 4).

We first explain, in section 3.1, how to build an *underapproximation* of a given WSTS w.r.t. to a finite subset of reachable states $C' \subseteq C$. Intuitively, that approximation contains all the traces of the WSTS that visit states of C' only. It allows us to decide the *positive instances* of the coverability problem.

In section 3.2, we show how to build an *overapproximation* of a given WSTS, w.r.t. a given finite set of reachable states $C' \subseteq C$ and a given finite set of limit elements $L' \subseteq L$. These abstractions are *And-Or graphs* whose nodes are annotated by $\leq$-downward-closed sets of states of a WSTS. We show that any unfolding of this And-Or graph is able to *simulate* [23] the behaviours of its associated WSTS (Proposition 3). Moreover, if the $\leq$-downward-closed sets that are used to annotate the And-Or graph are *precise enough* (in a sense that we make clear in Theorem 2), then the And-Or graph allows us to decide *negative instances* of the coverability problem.

3.1 The C'-Exact Partial Reachability Graph $\mathsf{EPRG}(S, C')$

Given a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ and a set $C' \subseteq C$ (with $c_0 \in C'$), can build the *C'-exact partial reachability graph* (C'-EPRG for short) $\mathsf{EPRG}(S, C')$. It is an under-approximation of S (in the sense of Lemma 1). Let us first define precisely the notion of C'-EPRG:

Definition 6 *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ *and a set* $C' \subseteq C$*, the* C'-EPRG *of* S *is the transition system* $\mathsf{EPRG}(S, C') = \Big\langle C', c_0, \big(\rightarrow \cap (C' \times C') \big) \Big\rangle$.

The following lemmata state the usefulness of the C'-EPRG to decide the coverability problem. The first lemma states that these graphs are *adequate* in the sense that when an $\leq$-upward-closed U is reachable in the C'-EPRG, it is also reachable in the corresponding WSTS.

Lemma 1 *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, a finite set* $C' \subseteq C$ *with* $c_0 \in C'$ *and an* $\leq$*-upward-closed* $U \subseteq C$*:* **If** $\mathsf{Reach}(\mathsf{EPRG}(S, C')) \cap U \neq \emptyset$ **then** $\mathsf{Reach}(S) \cap U \neq \emptyset$.

The second lemma states the *completeness* of C'-EPRG for some sets $C' \subseteq C$: when a given upward-closed set U is actually reachable in a WSTS, there exists a set $C' \subseteq C$ that allows to prove the reachability of U thanks to the C'-EPRG.

Lemma 2 *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ *and an* $\leq$*-upward-closed* $U \subseteq C$*:* **if** $\mathsf{Reach}(S) \cap U \neq \emptyset$*,* **then** *there exists a finite set* $C' \subseteq C$ *with* $c_0 \in C'$ *such that* $\mathsf{Reach}(\mathsf{EPRG}(S, C')) \cap U \neq \emptyset$.

3.2 The And-Or Graph $\mathsf{Abs}(S, C', L')$

Let us now show how to over-approximate a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$. Just as the EPRG was parameterized by a finite set of *concrete* elements, this over-approximation relies upon $C' \subseteq C$, a finite set of concrete elements; and L', a finite set of limit elements. It has the form of an And-Or graph $\mathsf{Abs}(S, C', L')$ whose unfoldings all simulate S (as shown later, in Proposition 3):

Definition 7 Given a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$, an adequate domain of limits $\langle L, \sqsubseteq, \gamma \rangle$ for $\langle C, \leq \rangle$, a finite subset $C' \subseteq C$ with $c_0 \in C'$, and a finite subset $L' \subseteq L$ with $\top \in L'$, the And-Or graph $G = \langle V_A, V_O, v_i, \Rightarrow \rangle$, noted $\mathsf{Abs}(S, C', L')$, is defined as follows:

- (A_1) $V_O = L' \cup C'$;
- (A_2) And-nodes are non empty subsets of $L' \cup C'$ and contain $\sqsubseteq$-incomparable elements only: $V_A = \{S \in 2^{L' \cup C'} \setminus \{\emptyset\} \mid \nexists d_1 \neq d_2 \in S : d_1 \sqsubseteq d_2\}$;

($\mathsf{A_3}$) $v_i = c_0$;

($\mathsf{A_{4.1}}$) The successors of any And-node are Or nodes: $(n_1, n_2) \in \Rightarrow$ with $n_1 \in V_A, n_2 \in V_O$ if and only if $n_2 \in n_1$;

($\mathsf{A_{4.2}}$) The successors of an Or-node n are all the most precise elements of $L' \cup C'$ that represent the set of successors of $\gamma(n)$: for any $n_1 \in V_O, n_2 \in V_A$: $(n_1, n_2) \in \Rightarrow$ if and only if (i) *successor covering:* $\mathsf{Post}(\gamma(n_1)) \subseteq \gamma(n_2)$, (ii) *preciseness:* $\neg\exists n \in V_A : \mathsf{Post}(\gamma(n_1)) \subseteq \gamma(n) \subset \gamma(n_2)$.

Notice that all the nodes of $\mathsf{Abs}(S, C', L')$ have at least one successor. Indeed, for all $n \in V_A$, since $n \neq \emptyset$ (following point $\mathsf{A_{4.1}}$ and point $\mathsf{A_2}$ of Definition 7), n has at least one successor. Since, by point $\mathsf{A_2}$ of Definition 7, And-nodes are subsets of $L' \cup C'$ that do not contain comparable elements, and since $\top \in L'$, with $\gamma(\top) = C$, by point $\mathsf{L_2}$ of Definition 1, there exists an And node which is exactly $\{\top\}$. Hence, for any $n \in V_O$, we can always approximate the (non-empty) set of successors of $\gamma(n)$, and we are guaranteed that n will have at least one successor (point $\mathsf{A_{4.2}}$ of Definition 7).

Given a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$, an associated And-Or graph $\mathsf{Abs}(S, L', C') = \langle V_A, V_O, v_i, \Rightarrow \rangle$, and an $\leq$-upward-closed set of states $U \subseteq C$, we denote by $\mathcal{U}$ the set of nodes $v \in V_A \cup V_O$ such that $\gamma(v) \cap U \neq \emptyset$, that is, the set of nodes whose associated $\leq$-downward-closed set of states intersects with U.

Degenerated case. If an And-Or graph is such that any Or-node has exactly one successor, the And-Or graph is said to be *degenerated*. In that case, the avoidability problem is equivalent to the (un)reachability problem in a plain graph. From the definition of $\mathsf{Abs}(S, C', L')$, we can easily see that the And-Or graph will be degenerated if for any $d \in L' \cup C'$, there exists a *unique* minimal set $\gamma(D)$ such that $D \in V_A$ and $\mathsf{Post}(\gamma(d)) \subseteq \gamma(D)$. This motivates the next definition:

Definition 8 Given a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ and an adequate domain of limits $\langle L, \sqsubseteq, \gamma \rangle$ for $\langle C, \leq \rangle$, we say that a pair $\langle C', L' \rangle$, where $C' \subseteq C$ with $c_0 \in C$ and $L' \subseteq L$ with $\top \in L'$, is *perfect* if for any $d \in L' \cup C'$, there exists a unique minimal set $D \subseteq L' \cup C'$ such that (i) $\mathsf{Post}(\gamma(d)) \subseteq \gamma(D)$ and (ii) there is no $D' \subseteq L' \cup C'$ with $\mathsf{Post}(\gamma(d)) \subseteq \gamma(D') \subset \gamma(D)$.

Lemma 3 *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, an adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *for* $\langle C, \leq \rangle$*, a finite subset* $C' \subseteq C$ *with* $c_0 \in C'$*, and a finite subset* $L' \subseteq L$ *with* $\top \in L'$*:* **if** $\langle C', L' \rangle$ *is perfect,* **then** $\mathsf{Abs}(S, C', L')$ *is a degenerated And-Or graph.*

Properties. Let us now prove important properties of $\mathsf{Abs}(S, C', L')$ that show how it is related to the coverability problem. More precisely, we first prove that, for any pair $\langle C', L' \rangle$ such that $c_0 \in C'$ and $\top \in L'$, this abstraction is *adequate* to decide negative instances of the coverability problem (Theorem 1). Then, we prove that, for some pair $\langle C', L' \rangle$, it is *complete* to decide

negative instances (Theorem 2). To establish those results, we first show that $\mathsf{Abs}(S, C', L')$ can simulate its corresponding WSTS for any $\langle C', L' \rangle$ such that $c_0 \in C'$ and $\top \in L'$:

Proposition 3 (Simulation) *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ *with an adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *for* $\langle C, \leq \rangle$*, the following holds for any* $C' \subseteq C$ *with* $c_0 \in C'$ *and* $L' \subseteq L$ *with* $\top \in L'$*: for any path* $c_0 c_1 \dots c_k$ *of* S *and any unfolding* $T = \langle N, root, B, \Lambda \rangle$ *of* $\mathsf{Abs}(S, C', L')$ *there exists a path* $n_0 n_1 \dots n_{2k}$ *of* T *with* $n_0 = root$ *and* $c_i \in \gamma(\Lambda(n_{2i}))$ *for any* $0 \leq i \leq k$*.*

Proof. Let $c_0, \dots, c_k$ be a path of S. For any unfolding, we will show, by induction on the length k of the path in S, that there exists a path $n_0 n_1 \dots n_{2k}$ of the unfolding such that $c_i \in \gamma(\Lambda(n_{2i}))$ for all i such that $0 \leq i \leq k$.
Base case: The base case is trivial since $\Lambda(root) = c_0$ following $\mathsf{A_3}$ and $\mathsf{C_1}$.
Induction step: Suppose that there exists a path $P = n_0, \dots, n_{2i}$ $(i < k)$ of the unfolding, such that $c_j \in \gamma(\Lambda(n_{2j}))$ for all j such that $1 \leq j \leq i$. Let us show that there exists a path $n_0 \dots n_{2(i+1)}$ of the unfolding, where $c_j \in \gamma(\Lambda(n_{2j}))$ for all j such that $1 \leq j \leq i+1$. Since $c_i \rightarrow c_{i+1}$, from point $\mathsf{A_{4.2}}$ of Definition 7, all the And-nodes $v = \{d_1, \dots, d_\ell\}$ in $\mathsf{Abs}(S, C', L')$ with $\Lambda(n_{2i}) \Rightarrow v$ are such that $c_{i+1} \in \gamma(d_j)$ for some $1 \leq j \leq \ell$. Hence, following $\mathsf{C_3}$, the successor of n_{2i} in the unfolding is an And-node n with $\Lambda(n) = \{d_1, \dots, d_\ell\}$ such that $c_{i+1} \in \gamma(d_j)$ for some $1 \leq j \leq \ell$. Moreover, following $\mathsf{A_{4.1}}$ and $\mathsf{C_2}$, each And-node v has a successor v' such that $\Lambda(v') = d_j$. Thus, $c_{i+1} \in \gamma(\Lambda(v'))$. We conclude that in the path P extended with the nodes v and v', each Or-node n_{2j} covers its corresponding c_j, i.e., $c_j \in \gamma(\Lambda(n_{2j}))$. □

Theorem 1 states the *adequacy* of the And-Or graph to decide the negative instances of the coverability problem.

Theorem 1 (Adequacy) *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, an adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *for* $\langle C, \leq \rangle$*, and an* $\leq$*-upward-closed set* $U \subseteq C$*, the following holds for any* $C' \subseteq C$ *with* $c_0 \in C'$ *and* $L' \subseteq L$ *with* $\top \in L'$*:* if $\mathcal{U}$ *is avoidable in* $\mathsf{Abs}(S, C', L')$*,* then $\mathsf{Reach}(S) \cap U = \emptyset$*.*

Proof. We prove the contraposition: suppose that $\mathsf{Reach}(S) \cap U \neq \emptyset$. Hence, there exists a path $c_0, \dots, c_k$ in S with $c_k \in U$. From Proposition 3, there exists in any unfolding $T = \langle N, root, B, \Lambda \rangle$ of $\mathsf{Abs}(S, C', L')$, a path $n_0 \dots n_{2k}$ with $n_0 = root$ and $c_i \in \gamma(\Lambda(n_{2i}))$, for all i such that $0 \leq i \leq k$. We conclude that $\Lambda(N) \cap \mathcal{U} \neq \emptyset$ and get the theorem. □

Finally, we prove a theorem of *completeness*. Intuitively, Theorem 2 says that, when the pair $\langle C', L' \rangle$ is *precise enough*, $\mathsf{Abs}(S, C', L')$ allows us to decide *negative instances* of the coverability problem. To prove that theorem, we first prove Lemma 4 that says that, if $L' \cup C'$ contains a coverability set and the

$\leq$-upward-closed set U of configurations is not reachable into the WSTS, then there exists an unfolding that does not intersect with U.

Lemma 4 *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, an adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *for* $\langle C, \leq \rangle$ *and an* $\leq$*-upward-closed set* $U \subseteq C$*, the following holds for any* $C' \subseteq C$ *with* $c_0 \in C'$ *and* $L' \subseteq L$ *with* $\top \in L'$ *such that* $\mathsf{CS}(S) \subseteq L' \cup C'$*:* **if** $\mathsf{Reach}(S) \cap U = \emptyset$ **then** *there exists an unfolding* $T = \langle N, root, B, \Lambda \rangle$ *of* $\mathsf{Abs}(S, C', L')$ *such that* $\forall n \in N : \gamma(\Lambda(n)) \cap U = \emptyset$*.*

Proof. We construct such an unfolding by induction, and use Proposition 2 to conclude. More precisely, we show how to compute an unfolding whose nodes n are such that $\gamma(\Lambda(n)) \subseteq \gamma(\mathsf{CS}(S))$. Following Proposition 2 and the fact that $\mathsf{Reach}(S) \cap U = \emptyset$, that implies that $\gamma(\Lambda(n)) \cap U = \emptyset$ for all the nodes n of the unfolding.

Base case: Notice that $root = c_0$ following $\mathsf{C_1}$ and $\mathsf{A_3}$, and $c_0 \in \gamma(\mathsf{CS}(S))$ following Definition 4. Moreover, $\mathsf{Post}(\gamma(c_0)) \subseteq \gamma(\mathsf{CS}(S))$. Indeed, following $\mathsf{W_2}$, $\forall c \in \gamma(c_0), \forall c' : c \rightarrow c'$, there exists $c'' \in C$ such that $c_0 \rightarrow^* c''$ with $c' \leq c''$. Since $c'' \in \gamma(\mathsf{CS}(S))$ and $\mathsf{CS}(S)$ is $\leq$-downward-closed, we have that $c' \in \mathsf{CS}(S)$ and we conclude that $\mathsf{Post}(\gamma(c_0)) \subseteq \gamma(\mathsf{CS}(S))$.

Following $\mathsf{A_{4.2}}$, there exists $v \in V_A$ (the set of And-nodes) with $v_i \Rightarrow v$ and $\gamma(v) \subseteq \gamma(\mathsf{CS}(S))$ since v satisfies the preciseness property of $\mathsf{A_{4.2}}$ and $\mathsf{CS}(S)$ covers the successors of v_i. Thus, we extend the unfolding by choosing such an And-node v and add one successor node n to $root$ such that $\Lambda(n) = v$.

Induction step: Suppose that we can construct $2k$ layers of the unfolding such that for all the nodes n of the $2k$ first layers, $\gamma(n) \subseteq \gamma(\mathsf{CS}(S))$. Let us show that we can construct $2k+2$ layers such that for all the nodes n of the $2k+2$ first layers, $\gamma(n) \subseteq \gamma(\mathsf{CS}(S))$.

By induction hypothesis, all the And-nodes n in the $2k$-th layer are such that $\Lambda(n) = \{d_1, \ldots, d_\ell\}$ and $\gamma(\Lambda(n)) \subseteq \gamma(\mathsf{CS}(S))$. Since, following $\mathsf{A_{4.1}}$, all the successors nodes v of $\Lambda(n)$ in $\mathsf{Abs}(S, C', L')$ are such that $v \in \Lambda(n)$, we have that $\gamma(v) \subseteq \gamma(\mathsf{CS}(S))$. We conclude, following $\mathsf{C_2}$, that all the Or-nodes n' of the $2k+1$-th layer are such that $\gamma(\Lambda(n')) \subseteq \gamma(\mathsf{CS}(S))$.

For each node n of the $2k+1$-th layer, since S is monotonic ($\mathsf{W_2}$) and $\gamma(n) \subseteq \gamma(\mathsf{CS}(S))$, we have that $\forall c \in \gamma(n), \forall c'$ s.t. $c \rightarrow c'$, there exists $c'' \in \mathsf{Reach}(S)$: $c \leq c''$ and $c'' \rightarrow^* c'''$ with $c' \leq c'''$ and $c''' \in \gamma(\mathsf{CS}(S))$. Since $\gamma(\mathsf{CS}(S))$ is $\leq$-downward-closed we obtain that $\mathsf{Post}(\gamma(n)) \subseteq \gamma(\mathsf{CS}(S))$ for all the nodes n of the $2k+1$-th layer.

Moreover, there exists following $A_{4.2}$ an And-node v with $\gamma(v) \subseteq \gamma(\mathsf{CS}(S))$ and $\Lambda(n) \Rightarrow v$ since v satisfies the preciseness property of $\mathsf{A_{4.2}}$ and $\mathsf{CS}(S)$ covers the successors of $\gamma(\Lambda(n))$. So, we extend the unfolding by choosing such a

node v and add one successor n' to n such that $\Lambda(n') = v$. That allows us to conclude that we can construct the $2k+2$-th first layers of the unfolding with the property that all the nodes n are such that $\gamma(\Lambda(n)) \subseteq \mathsf{CS}(S)$. □

Theorem 2 (Completeness) *Given a* WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$*, an adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *for* $\langle C, \leq \rangle$ *and an* $\leq$*-upward-closed set* $U \subseteq C$*, the following holds for any* $C' \subseteq C$ *with* $c_0 \in C'$ *and* $L' \subseteq L$ *with* $\top \in L'$ *such that* $\mathsf{CS}(S) \subseteq L' \cup C'$*:* if $\mathsf{Reach}(S) \cap U = \emptyset$ then $\mathcal{U}$ *is avoidable in* $\mathsf{Abs}(S, C', L')$*.*

Proof. As $\mathsf{Reach}(S) \cap U = \emptyset$, there exists, form Lemma 4, an unfolding that does not intersect with $\mathcal{U}$, which means that $\mathcal{U}$ is avoidable in $\mathsf{Abs}(S, C', L')$. □

4 The 'Expand, Enlarge and Check' algorithm

On the basis of the results presented in section 3, we now propose a new algorithmic schema to decide the coverability problem of effective WSTS (in the sense of Definition 3). It works by iteratively constructing pairs of approximations (under and overapproximations) of the WSTS which become more and more precise. After a finite number of steps either a concrete trace to a *covering state* will be found, or *precise enough abstraction* will be computed to prove that no covering state can ever be reached. This informal statement is formalized in Theorem 3.

Let $C_0, C_1, \ldots, C_n, \ldots$ be an infinite sequence of finite sets of reachable states of S such that (i) $\forall i \geq 0 : C_i \subseteq C_{i+1}$, (ii) $\forall c \in \mathsf{Reach}(S) : \exists i \geq 0 : c \in C_i$, and (iii) $c_0 \in C_0$. Let $L_0, L_1, \ldots, L_n, \ldots$ be a infinite sequence of finite sets of limits such that (i) $\forall i \geq 0 : L_i \subseteq L_{i+1}$, (ii) $\forall \ell \in L : \exists i \geq 0 : \ell \in L_i$ and (iii) $\top \in L_0$. Those sequences of sets exist because C and L are recursively enumerable, by E_1. Remark that these conditions imply that, for any finite subset D of C (resp. $L \cup C$), there exists i (resp. j) such that $D \subseteq C_i$ (resp. $D \subseteq L_j \cup C_j$). The schema is given at Algorithm 1 and its proof of correctness is stated in Theorem 3.

Theorem 3 *For any* WSTS S *with adequate domain of limits* $\langle L, \sqsubseteq, \gamma \rangle$ *that are effective, for any* $\leq$*-upward-closed set* U *represented by* $\mathsf{Min}(U)$*, Algorithm 1 terminates after a finite amount of time and returns 'Reachable' if* $\mathsf{Reach}(S) \cap U \neq \emptyset$*, 'Unreachable' otherwise.*

Proof. Let us first prove that the body of the main loop always terminate. In order to establish this, let us notice that C_i is finite for all $i \geq 0$, that the transition relation $\rightarrow$ is decidable (following E_2) and that $\leq$ is decidable too.

Algorithm 1: Abstract algorithm

Data : a finite representation of a WSTS $S = \langle C, c_0, \rightarrow, \leq \rangle$ with the adequate limit domain $\langle L, \sqsubseteq, \gamma \rangle$ for $\langle C, \leq \rangle$

Data : a finite representation of an $\leq$-upward-closed set of states $U \subseteq C$

begin

$i \leftarrow 0$;

while *(*`true`*)* **do**

'Expand'

Compute $\mathsf{EPRG}(S, C_i)$;

'Enlarge'

Compute $\mathsf{Abs}(S, C_i, L_i)$;

'Check'

if $\mathsf{Reach}(\mathsf{EPRG}(S, C_i)) \cap U \neq \emptyset$ **then**

return *'Reachable'* ;

else if $\mathcal{U}$ *is avoidable in* $\mathsf{Abs}(S, C_i, L_i)$ **then**

return *'Unreachable'* ;

$i \leftarrow i + 1$;

end

Hence we can test whether $\mathsf{Reach}(\mathsf{EPRG}(S, C_i)) \cap U \neq \emptyset$ for all $i \geq 0$. Then, let us remark that the And-Or graph, as well as $\mathcal{U}$ are both constructible, because of the effectiveness properties of Definition 3. Hence, we can effectively test whether $\mathcal{U}$ is avoidable in $\mathsf{Abs}(S, C_i, L_i)$ (remember that the avoidability problem is PTIME-complete).

It remains to prove that the algorithm returns a correct answer after a finite number of iterations of the loop.

If $\mathsf{Reach}(S) \cap U \neq \emptyset$, $\mathcal{U}$ is not avoidable in $\mathsf{Abs}(S, C_i, L_i)$ for all $i \geq 0$ (by Theorem 1). Moreover, following Lemma 2 there is j s.t. $\mathsf{Reach}(\mathsf{EPRG}(S, C_j)) \cap U \neq \emptyset$. We conclude that Algorithm 1 returns 'Reachable' if $\mathsf{Reach}(S) \cap U \neq \emptyset$.

If $\mathsf{Reach}(S) \cap U = \emptyset$, then, following Lemma 1, $\mathsf{Reach}(\mathsf{EPRG}(S, C_i)) \cap U = \emptyset$ for all $i \geq 0$. Moreover, there exists $i \geq 0$ such that $\mathsf{CS}(S) \subseteq L_i \cup C_i$. Hence, from Lemma 4, $\mathcal{U}$ is avoidable in $\mathsf{Abs}(S, C_i, L_i)$ and we conclude that Algorithm 1 returns 'Unreachable' if $\mathsf{Reach}(S) \cap U = \emptyset$. □

Remark 1 *Note that Theorem 3, that states the adequation and completeness of our algorithmic schema (for the coverability problem of effective* WSTS*), is not in contradiction with the result of [12] which establishes that there does not exist a procedure that always terminates and returns a coverability set for a large class of* WSTS*, including ours. Indeed, to establish the correctness of*

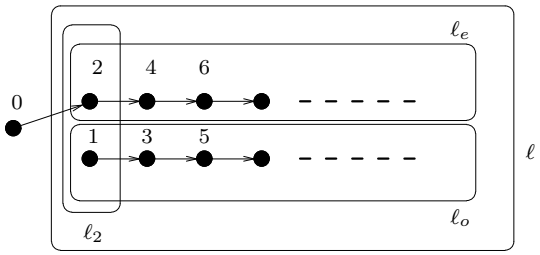

Fig. 1. The configurations of $S_{\mathbb{N}}$ and the limits that cover them.

our algorithm, we only need to ensure that a coverability set will eventually be included in the sequence of C_i's and L_i's. Nevertheless, given a pair $\langle C_i, L_i \rangle$, it is not possible to establish algorithmically that this pair contains a coverability set. Furthermore, given a particular $\leq$-upward-closed set U, our algorithm may terminate before reaching a pair $\langle C_i, L_i \rangle$ that contains a coverability set, because the set U is reachable or because the abstraction constructed from a pair $\langle C_j, L_j \rangle$, with $j < i$, is sufficiently precise to prove that U is not reachable.

Remark 2 *Note that the constraints on the sequence of L_i's computed by Algorithm 1 may be relaxed. Indeed, those constraints ensure that the algorithm eventually considers a set of limits which allows to construct a graph that is precise enough to decide negative instances of the coverability problem. However, following Theorem 2, it is sufficient to ensure that there exists $i \geq 0$ such that $L_i \cup C_i$ contains a coverability set. Hence, only the limits of a coverability set must appear in the sequence of L_i's.*

Remark 3 *In order to convince the reader that the And-Or graph is necessary to build precise abstractions of* WSTS*, we discuss the following example. Consider the* WSTS *$S_{\mathbb{N}} = \langle \mathbb{N}, 0, \rightarrow, \leq_p \rangle$, where:*

(1) $\rightarrow = \{(i, i+2) \mid i \geq 0\}$
(2) $\leq_p = \{(i, i+2j) \mid i \geq 1, j \geq 0\}$

Thus, the state space of this system contains two infinite ascending chains: $2, 4, 6, \ldots$ and $1, 3, 5, \ldots$ Remark that 0, the initial state, is incomparable to any other state and that only the ascending chain of even number is reachable.

Let us fix the adequate domain of limits for $S_{\mathbb{N}}$ defined as: $L = \{\ell, \ell_e, \ell_o, \ell_2, \top\}$, where (Fig. 1 depicts this):

(1) $\gamma(\ell) = \mathbb{N} \setminus \{0\}$;
(2) $\gamma(\ell_e) = \{2, 4, 6, \ldots\}$;
(3) $\gamma(\ell_o) = \{1, 3, 5, \ldots\}$;
(4) $\gamma(\ell_2) = \{1, 2\}$;
(5) $\gamma(\top) = \{0, 1, 2 \ldots\}$.

Thus, the coverability set of the system is $\mathsf{CS}(S_{\mathbb{N}}) = \{0, \ell_e\}$.

Let us now fix $C' = \{0\}$ *and* $L' = \{\ell, \ell_e, \ell_2, \top\}$*, and let us build* $\mathsf{Abs}(S_{\mathbb{N}}, C', L')$*. Remark that* $\mathsf{CS}(S_{\mathbb{N}}) \subseteq L' \cup C'$*. We obtain the And-Or graph of Fig. 2 (where And-nodes are represented by rectangles and Or-nodes are represented by ellipses). Indeed,* ℓ_e *and* ℓ_2 *are two incomparable limits which are both suitable to cover the one-step successor of the initial configuration. However, while* ℓ_e *is sufficient to cover all the successors of* 0*, we need* ℓ *to over-approximate the successors of* ℓ_2*.*

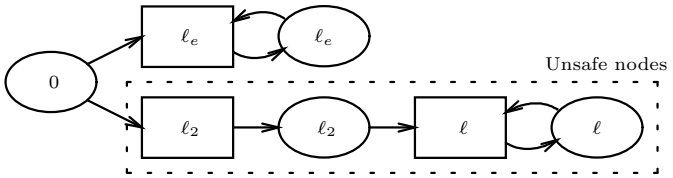

Fig. 2. The And-Or graph obtained with C' and L'

Finally, let us chose the $\leq_p$*-upward-closed set of* bad *states* $U = \{i \mid 1 \leq_p i\}$*. Remark that the system is* safe *w.r.t.* U*, since only* even *natural numbers (which are all* $\leq_p$*-incomparable to 1) can be reached. But, due to the coarse over-approximation, one of the unfoldings of the And-Or graph intersects with* U *(see Fig. 2). And this happens even though all the elements of the coverability set are present in* $L' \cup C'$*. Thus, one cannot thoroughly represent this over-approximation of the system thanks to a plain graph. Otherwise, one would have to* chose *the* right *successor of the initial node. At each step* i *of the algorithm, an exponential number of such plain graphs could have to be constructed, in order to test for all the possible choices. Such a procedure is clearly less efficient than the* PTime *algorithm that decides the avoidability on And-Or graphs. Remark that all the possible graphs have to explored at each step, otherwise the algorithm could never terminate. This happens, e.g. if the system is safe and the only abstractions the algorithm builds are repeatedly too coarse.*

5 Application to Self-modifying Petri nets

Let us show how to apply the approach proposed in the previous section to solve the coverability problem for a large subclass of *Self-modifying Petri nets* [24] (SMPN), a general extension of Petri nets that includes, to the best of our knowledge, all the monotonic extensions of Petri nets defined in the literature and for which, so far, there was no complete forward procedure.

In subsection 5.1, we present our subclass of SMPN, called *strongly monotonic self-modifying Petri nets*. In subsection 5.2, we instantiate the schema of algorithm presented in section 4 to the case of strongly monotonic SMPN. We first define the set of limits we will consider and how to construct the

sequences of C_i's and L_i's. Then, we show that in this particular case, the And-Or graph one obtains is *degenerated* (Corollary 2). As a consequence, we deduce a simpler algorithm, that contains a decision procedure for the classical graph reachability problem instead of the avoidability problem in an And-Or graph.

5.1 Self-modifying Petri nets

A *Self-Modifying Petri net* [24], SMPN for short, is a tuple $\langle P, T, D^-, D^+, \mathbf{m}_0\rangle$. $P = \{p_1, \ldots, p_{k_P}\}$ is a finite set of places. A *marking* is a function $\mathbf{m} : P \mapsto \mathbb{N}$ that assigns a natural value to each place. In the following, markings are also seen as tuples in $\mathbb{N}^{k_P}$ where the ith dimension is the value assigned to place p_i. $T = \{t_1, \ldots, t_{k_T}\}$ is a finite set of transitions. For any $1 \leq i \leq k_T$ and any $1 \leq j \leq k_P$, $D^-_{ij} : \mathbb{N}^{k_P} \mapsto \mathbb{N}$ and $D^+_{ij} : \mathbb{N}^{k_P} \mapsto \mathbb{N}$ describe respectively the input and output effect of transition t_i on place p_j. Namely, D^-_{ij} and D^+_{ij} are functions of the marking $\mathbf{m}$ of the form $\alpha + \sum_{k=1..k_P} \beta_k \cdot \mathbf{m}(p_k)$ where $\alpha \in \mathbb{N}$ and $\beta_k \in \mathbb{N}$ for all $1 \leq k \leq k_P$. $\mathbf{m}_0$ is the initial marking of the SMPN.

We define the quasi order $\preccurlyeq \subseteq \mathbb{N}^{k_P} \times \mathbb{N}^{k_P}$ on markings such that $\langle m_1,\ldots,m_{k_P}\rangle \preccurlyeq \langle m'_1,\ldots,m'_{k_P}\rangle$ if $m_i \leq m'_i$ for all $1 \leq i \leq k_P$. It is well-known that $\preccurlyeq$ is a well-quasi ordering.

A transition t_i is firable from a marking $\mathbf{m}$ if $\mathbf{m}(p_j) \geq D^-_{ij}(\mathbf{m})$ for all $p_j \in P$. Firing t_i from $\mathbf{m}$ leads to a marking $\mathbf{m}' \in \mathbb{N}^{k_P}$, noted $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$, which is computed as follows. First, we compute $\mathbf{m}''$, s.t. for any $p_j \in P : \mathbf{m}''(p_j) = \mathbf{m}(p_j) - D^-_{ij}(\mathbf{m})$. Then, we let $\mathbf{m}'$ be s.t. for any $p_j \in P : \mathbf{m}'(p_j) = \mathbf{m}''(p_j) + D^+_{ij}(\mathbf{m})$. Remark that these two steps can be swapped when we manipulate (plain) markings of SMPN. However, the order of these steps will become relevant when we will manipulate extended markings, as defined in section 5.2. Given a set S of markings and a transition t_i, $\mathsf{Post}(S, t_i) = \{\mathbf{m}' \mid \exists \mathbf{m} \in S : t_i \text{ is firable from } \mathbf{m} \text{ and } \mathbf{m} \rightarrow_{t_i} \mathbf{m}'\}$.

A SMPN $\mathcal{P}$ defines a transition system $\mathcal{T}_\mathcal{P} = \langle \mathbb{N}^{k_P}, \mathbf{m}_0, \rightarrow\rangle$ where $\rightarrow \subseteq \mathbb{N}^{k_P} \times \mathbb{N}^{k_P}$ is a transition relation and is such that we have $\langle \mathbf{m}, \mathbf{m}'\rangle \in \rightarrow$, noted $\mathbf{m} \rightarrow \mathbf{m}'$, if and only if there exists $t_i \in T$ such that t_i is firable from $\mathbf{m}$ and $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$.

A SMPN $\mathcal{P}$ is $\preccurlyeq$-*monotonic* when the underlying transition system $\mathcal{T}_\mathcal{P}$ satisfies the monotonicity property for $\preccurlyeq$. A SMPN $\mathcal{P}$ is $\preccurlyeq$-*strongly monotonic* when for every transition t_i and markings $\mathbf{m}_1, \mathbf{m}_2$ and $\mathbf{m}_3$, the following holds: if $\mathbf{m}_1 \rightarrow_{t_i} \mathbf{m}_3$ and $\mathbf{m}_1 \preccurlyeq \mathbf{m}_2$, there exists $\mathbf{m}_4$ such that $\mathbf{m}_2 \rightarrow_{t_i} \mathbf{m}_4$ and $\mathbf{m}_3 \preccurlyeq \mathbf{m}_4$. Obviously, all the $\preccurlyeq$-strongly monotonic SMPN are $\preccurlyeq$-monotonic.

We say that a transition t is *unfirable*, whenever there exists no marking $\mathbf{m}$

such that t is enabled in $\mathbf{m}$. In the following, we assume that the SMPN we consider do not contain unfirable transitions. The following lemma defines the syntactical subclass of SMPN that are $\preccurlyeq$-strongly monotonic.

Lemma 5 *Given a* SMPN $\mathcal{P} = \langle P, T, D^-, D^+, \mathbf{m}_0 \rangle$ *without unfirable transitions,* $\mathcal{P}$ *is* $\preccurlyeq$*-strongly monotonic if and only if for all* $t_i \in T, p_j \in P : D^-_{ij} = \alpha$ *with* $\alpha \in \mathbb{N}$ *or* $D^-_{ij} = \mathbf{m}(p_j)$.

Proof. $\Rightarrow$ Suppose that it is not the case, that is $\mathcal{P}$ is $\preccurlyeq$-strongly monotonic and there exist $t_i \in T, p_j \in P$ such that D^-_{ij} is not of the form α with $\alpha \in \mathbb{N}$ or $\mathbf{m}(p_j)$. Let $D^-_{ij} = \sum_{p_k \in P} \beta_k \cdot \mathbf{m}(p_k) + \alpha$. We consider two cases:

(1) $\beta_j > 1$ or ($\beta_j = 1$ and $\alpha > 0$). In both cases, t_i is unfirable, which contradicts the hypothesis.
(2) $\beta_j = 0$ or ($\beta_j = 1$ and $\alpha = 0$). Since D^-_{ij} is not of the form α or $\mathbf{m}(p_j)$, there is $k' \neq j$ such that $\beta_{k'} > 0$. By hypothesis, t_i is firable from at least one marking $\mathbf{m}$. Let us construct the marking $\mathbf{m}'$ as follows: $\forall p_k \neq p_{k'} \in P : \mathbf{m}'(p_k) = \mathbf{m}(p_k)$, and $\mathbf{m}'(p_{k'}) = \mathbf{m}(p_{k'}) + \mathbf{m}(p_j) + 1$. By construction, $\mathbf{m} \preccurlyeq \mathbf{m}'$ but t_i is not firable from $\mathbf{m}'$. Indeed, for t_i to be firable we should have $\mathbf{m}'(p_j) = \mathbf{m}(p_j) \geq D^-_{ij}(\mathbf{m}') \geq \beta_{k'} \cdot \Big(\mathbf{m}(p_{k'}) + \mathbf{m}(p_j) + 1\Big)$. Since $\beta_{k'} > 0$, this is not possible. We conclude that $\mathcal{P}$ is not $\preccurlyeq$-strongly monotonic.

In both cases, we obtain a contradiction.

$\Leftarrow$ We proceed by contradiction. Suppose that $\mathcal{P}$ is not $\preccurlyeq$-strongly monotonic but for all $t_i \in T, p_j \in P : D^-_{ij} = \alpha$ with $\alpha \in \mathbb{N}$ or $D^-_{ij} = \mathbf{m}(p_j)$. Hence there exists three markings $\mathbf{m}_1, \mathbf{m}_2$ and $\mathbf{m}_3$ and a transition t_i such that $\mathbf{m}_1 \rightarrow_{t_i} \mathbf{m}_3$, $\mathbf{m}_1 \preccurlyeq \mathbf{m}_2$ and there does not exist a marking $\mathbf{m}_4$ such that $\mathbf{m}_2 \rightarrow_{t_i} \mathbf{m}_4$ and $\mathbf{m}_3 \preccurlyeq \mathbf{m}_4$.

Since $\mathbf{m}_1 \preccurlyeq \mathbf{m}_2$ and $\mathbf{m}_1(p_j) \geq D^-_{ij}(\mathbf{m}_1)$ for all $p_j \in P$, $\mathbf{m}_2(p_j) \geq D^-_{ij}(\mathbf{m}_2)$ for all $p_j \in P$. As a consequence, t_i is firable from $\mathbf{m}_2$. Suppose that $\mathbf{m}_2 \rightarrow_{t_i} \mathbf{m}_4$.

Let $\mathbf{m}'_k$ ($k \in \{1, 2\}$) be such that $\mathbf{m}'_k(p_j) = \mathbf{m}_k(p_j) - D^-_{ij}(\mathbf{m}_k)$ for all $p_j \in P$. Since $\mathbf{m}_1 \preccurlyeq \mathbf{m}_2$, $\mathbf{m}'_1 \preccurlyeq \mathbf{m}'_2$. Moreover, we have that $D^+_{ij}(\mathbf{m}_1) \leq D^+_{ij}(\mathbf{m}_2)$ for all j such that $1 \leq j \leq |P|$. Since $\mathbf{m}_3(p_j) = \mathbf{m}'_1(p_j) + D^+_{ij}(\mathbf{m}_1)$ and $\mathbf{m}_4(p_j) = \mathbf{m}'_2(p_j) + D^+_{ij}(\mathbf{m}_2)$ for all $p_j \in P$, we conclude that $\mathbf{m}_3 \preccurlyeq \mathbf{m}_4$ and we obtain a contradiction. □

Although the class of $\preccurlyeq$-strongly monotonic SMPN form a sub-class of SMPN, it remains a general class of monotonic systems. Indeed, almost all the monotonic extensions of Petri nets studied in the literature are syntactical subclasses of $\preccurlyeq$-strongly monotonic SMPN, because they can be defined by imposing constraints on the linear expressions that express the effect of the tran-

sitions. Examples of such extensions are Petri nets with transfers [11], with reset [25] and Post self-modifying Petri nets [24]. On the other hand, Petri nets with non-blocking arcs (PN+NBA, for short) [13] and lossy Petri nets [26] are not syntactical sub-classes of $\preccurlyeq$-strongly monotonic SMPN. But, for any PN+NBA or lossy Petri net, we can construct (in polynomial time) an SMPN with the same set of places that is equivalent to the original net with respect to the coverability problem. So, to the best of our knowledge, the algorithm that we propose in the next section is a forward algorithm that decides the coverability problem for all monotonic extensions of Petri nets proposed in the literature.

5.2 A forward algorithm to decide the coverability problem for strongly monotonic SMPN

Domain of Limits. We will consider the domain of limits $\langle \mathcal{L}, \preccurlyeq_e, \gamma \rangle$ where $\mathcal{L} = (\mathbb{N} \cup \{+\infty\})^k \setminus \mathbb{N}^k$, $\preccurlyeq_e \subseteq (\mathbb{N} \cup \{+\infty\})^k \times (\mathbb{N} \cup \{+\infty\})^k$ is such that $\langle m_1, \ldots, m_k \rangle \preccurlyeq_e \langle m'_1, \ldots, m'_k \rangle$ if and only if $\forall 1 \leq i \leq k : m_i \leq m'_i$ where $c < +\infty$ for all $c \in \mathbb{N}$. γ is defined as: $\gamma(\mathbf{m}) = \{\mathbf{m}' \in \mathbb{N}^k \mid \mathbf{m}' \preccurlyeq_e \mathbf{m}\}$. In the following, tuples in $\mathcal{L}$ are called *extended markings*. We also note $\mathbf{m}_1 \prec_e \mathbf{m}_2$ when $\mathbf{m}_1 \preccurlyeq_e \mathbf{m}_2$ but $\mathbf{m}_2 \not\preccurlyeq_e \mathbf{m}_1$. Notice that in the present case, the $\top$ element (with $\gamma(\top) = \mathbb{N}^k$) is the extended marking that assigns $+\infty$ to all the places. One can remark that the following property holds on extended markings:

Property 1 *Given an extended marking* $\mathbf{m}$ *and a finite set of extended markings* $S = \{\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_n\}$*, the following property holds:* $\gamma(\mathbf{m}) \subseteq \gamma(S)$ *if and only if there exists* $1 \leq i \leq n$ *s.t.* $\mathbf{m} \preccurlyeq_e \mathbf{m}_i$*.*

It is also useful to remark that any downward-closed set in this domain can be uniquely and finitely represented by a set of extended markings, as stated by the next lemma:

Lemma 6 *For any* $\preccurlyeq_e$*-downward-closed set* D *in* $\mathbb{N}^k$ *there exists a set* $\mathcal{D} \subseteq \left(\mathbb{N} \cup \{+\infty\}\right)^k$ *which:*

(1) is a generator *of* D*:* $\gamma(\mathcal{D}) = D$*;*
(2) is minimal*: for any* $\mathbf{m}_1, \mathbf{m}_2 \in \mathcal{D}$*,* $\mathbf{m}_1 \neq \mathbf{m}_2$ *implies that* $\mathbf{m}_1 \not\preccurlyeq_e \mathbf{m}_2$*;*
(3) is finite*;*
(4) is unique*.*

Proof. The proof is constructive: for any $\preccurlyeq_e$-downward-closed $D \subseteq \mathbb{N}^k$, we show, by induction on k, how to construct a finite and minimal representation of D (points 1 through 3). Then, we prove that is representation is unique (point 4).

Base Case $k = 1$ We consider two cases: either $D = \{n | n \leq m\}$ or $D = \mathbb{N}$. In the former case, D is represented by $\langle n \rangle$, in the latter, by $\langle +\infty \rangle$. It is not difficult to see that this representation is both unique and minimal.

Inductive Case $k = i+1$. Let D^i_m be the set $\{\langle m_1, \ldots, m_i \rangle | \langle m_1, \ldots, m_i, m \rangle \in D\}$. Intuitively, D^i_m is the projection on the i first coordinates of all the markings of D whose $i+1$st coordinate is equal to m. Clearly, D^i_m is a $\preccurlyeq_e$-downward closed set. By induction hypothesis, D^i_m is representable by an unique minimal finite set $R^i_m \subseteq (\mathbb{N} \cup \{+\infty\})^i$, for every $m \in \mathbb{N}$.

Let $M = \cup_{m \in \mathbb{N}} R^i_m$. Clearly:

$$D = \bigcup_{\langle m_1, \ldots, m_i \rangle \in M} \left(\bigcup_{n \in \mathbb{N}} \{\langle m'_1, \ldots, m'_i, n \rangle \in D \mid \forall 1 \leq j \leq i : m'_j \leq m_j\} \right)$$

Let us show that this union allows us to find a finite representation for D. For this purpose, we first show that the set M is *finite*, hence the outermost union in the above representation is finite too. Then, we show that for each $\mathbf{m} = \langle m_1, \ldots, m_i \rangle \in M$, the set $S_{\mathbf{m}} = \cup_{n \in \mathbb{N}} \{\langle m'_1, \ldots m'_i, n \rangle \in D \mid \forall 1 \leq j \leq i : m'_i \leq m_i\}$ can be finitely represented.

M **is finite** Suppose it is not the case. As each R^i_m is finite, there exists an infinite sequence $R^i_{m_1}, R^i_{m_2}, \ldots, R^i_{m_j}, \ldots$ in which all the $R^i_{m_j}$ are not empty (for any $j \geq 1$). From this sequence, let us build an infinite sequence of markings $\mathbf{m}_1, \mathbf{m}_2, \ldots, \mathbf{m}_j, \ldots$ such that $\forall j \geq 1 : \mathbf{m}_j \in R^i_{\pi(j)}$ and $\pi(j) < \pi(j+1)$. Since $\preccurlyeq_e$ is a wqo, one can find ℓ_1 and ℓ_2 s.t. $\ell_1 < \ell_2$ and $\mathbf{m}_{\ell_1} \prec_e \mathbf{m}_{\ell_2}$.

Since $\mathbf{m}_{\ell_2} \in R^i_{\pi(\ell_2)}$, any *marking*[4] $\mathbf{n} \preccurlyeq_e \langle \mathbf{m}_{\ell_2}, \pi(\ell_2) \rangle$ is in D. But since $\pi(\ell_1) < \pi(\ell_2)$, we have: $\langle \mathbf{m}_{\ell_2}, \pi(\ell_1) \rangle \prec_e \langle \mathbf{m}_{\ell_2}, \pi(\ell_2) \rangle$. Hence, for any marking $\mathbf{n} \preccurlyeq_e \langle \mathbf{m}_{\ell_2}, \pi(\ell_1) \rangle$: $\mathbf{n} \in D$. Thus $\{\mathbf{m}' \mid \mathbf{m}' \preccurlyeq \mathbf{m}_{\ell_2}\} \subseteq D^i_{\pi(\ell_1)}$, by definition of $D^i_{\pi(\ell_1)}$. Otherwise stated, $\gamma(\mathbf{m}_{\ell_2}) \subseteq D^i_{\pi(\ell_1)}$, and thus $\gamma(\mathbf{m}_{\ell_2}) \subseteq \gamma(R^i_{\pi(\ell_1)})$, by definition of $R^i_{\pi(\ell_1)}$. Following Property 1, this implies that there exists $\mathbf{m} \in R^i_{\pi(\ell_1)}$ with $\mathbf{m}_{\ell_2} \preccurlyeq_e \mathbf{m}$, and thus $\mathbf{m}_{\ell_1} \prec_e \mathbf{m}$, since $\mathbf{m}_{\ell_1} \prec_e \mathbf{m}_{\ell_2}$.

We conclude that $R^i_{\pi(\ell_1)}$ contains two different comparable markings $\mathbf{m}$ and $\mathbf{m}_{\ell_1}$, and is thus not minimal, which contradicts the induction hypothesis.

$S_{\mathbf{m}}$ **can be finitely represented** For any $\mathbf{m} = \langle m_1, \ldots, m_i \rangle$, we show how to construct $R_{\mathbf{m}}$, a finite representation for $S_{\mathbf{m}}$. We consider two cases: either, there exists c such that $\{\langle m'_1, \ldots, m'_i, c+1 \rangle \in S_{\mathbf{m}} \mid \forall 1 \leq j \leq i : m'_i \leq m_i\}$ is empty, or there is no such c. In the first case, the finite representation is: $R_{\mathbf{m}} = \langle m_1, \ldots, m_i, d \rangle$, where d is the least natural number

[4] Throughout this part of the proof, we will explicitely use the word *marking* to differentiate the *plain markings* (that do not contain $+\infty$), from the *extended markings*.

such that $\{\langle m'_1, \ldots, m'_i, d+1\rangle \in S_{\mathbf{m}} \mid \forall 1 \leq j \leq i : m'_i \leq m_i\}$ is empty. In the latter case, it is $R_{\mathbf{m}} = \langle m_1, \ldots, m_i, +\infty\rangle$.

Now let $\mathcal{D} = \{R_{\mathbf{m}} \mid \mathbf{m} \in M \wedge \nexists \mathbf{m}' \in M : \mathbf{m}' \neq \mathbf{m} \wedge R_{\mathbf{m}} \preccurlyeq_e R_{\mathbf{m}'}\}$. We have already shown that this set is a finite representation of D. It is clearly minimal.

We now show that there exists a unique minimal finite set $\mathcal{D}$ such that $\gamma(\mathcal{D}) = D$. This can be done by contradiction: suppose there is another minimal finite set $\mathcal{D}'$ of markings that represents D. Without loss of generality, that means that there exists $\mathbf{m} \in \mathcal{D}$ such that $\mathbf{m} \notin \mathcal{D}'$. Since $\forall \mathbf{m}' \in \gamma(\mathbf{m}) : \mathbf{m}' \in D$ and $\gamma(\mathcal{D}') = D$ by hypothesis, we have following Property 1 that there exists $\mathbf{m}' \in \mathcal{D}' : \mathbf{m} \prec_e \mathbf{m}'$. Since $\gamma(\mathbf{m}) \subset \gamma(\mathbf{m}')$ and $\gamma(\mathcal{D}) = D$, we conclude, by Property 1, that there exists $\mathbf{m}'' \in \mathcal{D} : \mathbf{m} \prec_e \mathbf{m}''$. Hence, $\mathcal{D}$ is not minimal, which is a contradiction.

We conclude that $\mathcal{D}$ is indeed a finite, unique and minimal representation of $D \subseteq \mathbb{N}^{i+1}$. □

A direct consequence of this lemma and of the definition of γ, is given by this corollary:

Corollary 1 *$\langle \mathcal{L}, \preccurlyeq_e, \gamma\rangle$ is an adequate domain of limits for $\langle \mathbb{N}^k, \preccurlyeq\rangle$.*

Approximation of the successors. Given a $\preccurlyeq$-strongly monotonic SMPN $\mathcal{P}$, we extend the underlying transition relation from markings to extended markings by assuming that $+\infty + +\infty = +\infty$, $+\infty - +\infty = 0$, $c \cdot +\infty = +\infty$ for all $c \in \mathbb{N} \setminus \{0\}$, $0 \cdot +\infty = 0$, $+\infty + c = +\infty$ for all $c \in \mathbb{Z}$. For example, let us suppose that for some place j and some transition i, we have $D^-_{ij}(\mathbf{m}) = \mathbf{m}(p_j)$, $D^+_{ij} = 5$, and $D^-_{ik}(\mathbf{m}) = D^+_{ik}(\mathbf{m}) = 0$ for any $k \neq j$. Let us consider the extended marking $\mathbf{m}$ s.t. $\mathbf{m}(p_j) = +\infty$, and let us compute $\mathbf{m}'$ s.t. $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$. According to the definition of $\rightarrow$, we first compute $\mathbf{m}''$, which is s.t. $\mathbf{m}''(p_j) = \mathbf{m}(p_j) - D^-_{ij}(\mathbf{m}) = +\infty - +\infty = 0$, and $\mathbf{m}''(p_k) = \mathbf{m}(p_k)$, for any $k \neq j$. Then, we obtain $\mathbf{m}'$, by letting $\mathbf{m}'(p_j) = \mathbf{m}''(p_j) + D^+_{ij}(\mathbf{m}) = 0 + 5 = 5$, and $\mathbf{m}'(p_k) = \mathbf{m}''(p_k) = \mathbf{m}(p_k)$, for $k \neq j$.

Let us show that the way we have extended the transition relation is well-suited in the following sense. Let $\mathbf{m}$ and $\mathbf{m}'$ be two (extended) markings such that $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$ for some transition t_i. Then $\gamma(\mathbf{m}')$ is the most precise $\preccurlyeq_e$-downward-closed overapproximation for $\mathsf{Post}(\gamma(\mathbf{m}), t_i)$.

Lemma 7 *Let $\mathcal{P}$ be a $\preccurlyeq$-strongly monotonic* SMPN *with set of transitions T and $\mathbf{m}, \mathbf{m}'$ be two (possibly extended) markings. If $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$ for some $t_i \in T$, then $\gamma(\mathbf{m}')$ has the two following properties:* [covering] $\mathsf{Post}(\gamma(\mathbf{m}), t_i) \subseteq \gamma(\mathbf{m}')$ *and* [preciseness] *there is no finite set $S \subseteq \mathcal{L} \cup \mathbb{N}^{k_P}$ such that $\mathsf{Post}(\gamma(\mathbf{m}), t_i) \subseteq$*

$\gamma(S) \subset \gamma(\mathbf{m}')$.

Proof. **(Covering)** Suppose that the covering property is not verified. In this case, there exist four (possibly extended) markings $\mathbf{m}, \mathbf{m}', \mathbf{n}$ and $\mathbf{n}'$, and a transition $t_i \in T$ such that such that $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$, $\mathbf{n} \rightarrow_{t_i} \mathbf{n}'$, $\mathbf{n} \in \gamma(\mathbf{m})$ and $\mathbf{n}' \notin \gamma(\mathbf{m}')$. Hence, there exists $p_j \in P$ such that $\mathbf{n}'(p_j) > \mathbf{m}'(p_j)$.

Following Lemma 5, the effect $D^+_{ij}(m) - D^-_{ij}(m)$ of a transition t_i on place p_j for a marking m, may be of two forms. Either $D^+_{ij}(m) - D^-_{ij}(m) = \sum_{p_k \in P} \beta_k \cdot m(p_k) + \alpha$ or $D^+_{ij}(m) - D^-_{ij}(m) = \sum_{p_k \in P} \beta_k \cdot m(p_k) + \alpha - m(p_j)$ with $\beta_k \in \mathbb{N}$ for all k and $\alpha \in \mathbb{Z}$. Hence, either $\mathbf{n}'(p_j) = \mathbf{n}(p_j) + \sum_{p_k \in P} \beta_k \cdot \mathbf{n}(p_k) + \alpha$ and $\mathbf{m}'(p_j) = \mathbf{m}(p_j) + \sum_{p_k \in P} \beta_k \cdot \mathbf{n}(p_k) + \alpha$, or $\mathbf{n}'(p_j) = \sum_{p_k \in P} \beta_k \cdot \mathbf{n}(p_k) + \alpha$ and $\mathbf{m}'(p_j) = \sum_{p_k \in P} \beta_k \cdot \mathbf{m}(p_k) + \alpha$. In both cases, since $\mathbf{n} \in \gamma(\mathbf{m})$, $\mathbf{n}(p_k) \leq \mathbf{m}(p_k)$ for all $p_k \in P$, hence $\sum_{p_k \in P} \beta_k \cdot \mathbf{n}(p_k) + \alpha \leq \sum_{p_k \in P} \beta_k \cdot \mathbf{m}(p_k) + \alpha$. We conclude that $\mathbf{n}'(p_j) \leq \mathbf{m}'(p_j)$ and we obtain a contradiction.

(Preciseness) In order to establish the preciseness property, we prove that if $\mathbf{m} \rightarrow_{t_i} \mathbf{m}'$, then any marking $\mathbf{n} \in \gamma(\mathbf{m}')$ is covered by a marking $\mathbf{n}' \in \mathsf{Post}(\gamma(\mathbf{m}), t_i)$. This clearly implies that the set $\gamma(\mathbf{m}')$ is the minimal $\preccurlyeq_e$-downward-closed set that contains $\mathsf{Post}(\gamma(\mathbf{m}), t_i)$, since for any $\preccurlyeq_e$-downward-closed set $D \subset \gamma(\mathbf{m}')$, there exists at least one marking $\mathbf{n} \in \mathsf{Post}(\gamma(\mathbf{m}), t_i)$ that is not in D. The proof is by contradiction. Suppose that it is not the case, thus there exists $\mathbf{n} \in \gamma(\mathbf{m}')$ such that there is no $\mathbf{n}'' \in \mathsf{Post}(\gamma(\mathbf{m}), t_i)$ with $\mathbf{n} \preccurlyeq \mathbf{n}''$.

Let c be such that $c > \max\{|\alpha_1|, \ldots, |\alpha_{k_P}|\}$ where α_j is the constant term in $D^+_{ij} - D^-_{ij}$. We first construct the marking $\mathbf{n}'$ in the following manner: $\mathbf{n}'(p_j) = \mathbf{m}(p_j)$ if $\mathbf{m}(p_j) \in \mathbb{N}$; otherwise $\mathbf{n}'(p_j) > \max\{\mathbf{n}(p_k) \mid p_k \in P\} + c$. By construction, $\mathbf{n}' \in \gamma(\mathbf{m})$ and t_i is firable from $\mathbf{n}'$. Let $\mathbf{n}' \rightarrow_{t_i} \mathbf{n}''$. From the covering property, $\mathbf{n}'' \in \gamma(\mathbf{m}')$. Let us show that $\mathbf{n} \preccurlyeq \mathbf{n}''$.

For all $p_j \in P$, two cases hold following Lemma 5 again:

- $D^+_{ij}(\mathbf{m}) - D^-_{ij}(\mathbf{m}) = \sum_{p_k \in P} \beta_k \cdot \mathbf{m}(p_k) + \alpha_j - \mathbf{m}(p_j)$ with $\beta_k \in \mathbb{N}$ for all k and $\alpha_j \in \mathbb{Z}$. Either $\mathbf{m}(p_k) \in \mathbb{N}$, for any k s.t. $\beta_k > 0$. In that case, $\mathbf{n}''(p_j) = \mathbf{m}'(p_j)$, hence $\mathbf{n}(p_j) \leq \mathbf{n}''(p_j)$. Or there is some $p_k \in P$ such that $\beta_k > 0$ and $\mathbf{m}(p_k) = +\infty$. By construction, $\mathbf{n}''(p_j) > \max\{\mathbf{n}(p_k) \mid p_k \in P\}$, hence $\mathbf{n}(p_j) < \mathbf{n}''(p_j)$;
- $D^+_{ij}(\mathbf{m}) - D^-_{ij}(\mathbf{m}) = \sum_{p_k \in P} \beta_k \cdot \mathbf{m}(p_k) + \alpha_j$ with $\beta_k \in \mathbb{N}$ for all k and $\alpha_j \in \mathbb{Z}$. By using a similar reasoning than in the previous case, we obtain that $\mathbf{n}(p_j) \leq \mathbf{n}''(p_j)$.

We conclude that $\mathbf{n} \preccurlyeq \mathbf{n}''$ and we obtain a contradiction. □

Since our algorithm requires the WSTS and its associated domain of limits to

be effective (Definition 3), we state the following lemma (proof omitted):

Lemma 8 *Any $\preccurlyeq$-strongly monotonic* SMPN $\mathcal{P}$ *with the adequate domain of limits $\langle \mathcal{L}, \preccurlyeq_e, \gamma \rangle$ are effective.*

The following definition explains how we construct the C_i's and L_i's. Following Definition 7, this is sufficient to define the And-Or graphs built by our verification algorithm.

Definition 9 *The sequences of C_i's and L_i's are defined as follows:*

(D_1) $C_i = \{0, \ldots, i\}^k \cup \{\mathbf{m}_0\}$, *i.e. C_i is the set of markings where each place is bounded by i (plus the initial marking);*
(D_2) $L_i = \{\mathbf{m} \in \{0, \ldots i, +\infty\}^k \mid \mathbf{m} \notin \mathbb{N}^k\}$.

It is easy to see that (i) for all $i \geq 0 : C_i \subset C_{i+1}$ and $L_i \subset L_{i+1}$, (ii) for any $\mathbf{m} \in \mathbb{N}^k$, there exists $i \in \mathbb{N}$ such that for all $j \geq i : \mathbf{m} \in C_j$, (iii) for any $\mathbf{m} \in \mathcal{L}$, there exists $i \in \mathbb{N}$ such that for all $j \geq i : \mathbf{m} \in L_j$, and (iv) $\mathbf{m}_0 \in C_0$ and $\top = \langle +\infty, \ldots, +\infty \rangle \in L_0$.

Degenerated And-Or graph. Let us show that in the present case, one obtains a *degenerated* And-Or graph. We establish this result by showing, following Lemma 3, that the pairs $\langle C_i, L_i \rangle$ are *perfect* pairs. For this purpose, we first introduce the function $\mathsf{Bound}(\mathbf{m}, k)$ and establish an auxiliary lemma about this function. Given a (possibly extended) marking $\mathbf{m}$ over set of places P and $k \in \mathbb{N}$, we define $\mathsf{Bound}(\mathbf{m}, k) : (\mathbb{N} \cup \{+\infty\})^{|P|} \mapsto \{0, 1, \ldots, k, +\infty\}^{|P|}$ such that for any place $p_i \in P$: $\mathsf{Bound}(\mathbf{m}, k)(p_i) = \mathbf{m}(p_i)$ if $\mathbf{m}(p_i) \leq k$, $\mathsf{Bound}(\mathbf{m}, k)(p_i) = +\infty$ otherwise. We can now state the following lemma, that says that , for any marking $\mathbf{m} \in L_i \cup C_i$, $\mathsf{Bound}(\mathbf{m}, i)$ is the most precise approximation of $\mathbf{m}$ inside $L_i \cup C_i$.

Lemma 9 *Given any $i \in \mathbb{N}$, let C_i and L_i be constructed following Definition 9 and $\mathbf{m} \in L_i \cup C_i$. There does not exist a finite set $S \subseteq L_i \cup C_i$ such that $\gamma(\mathbf{m}) \subseteq \gamma(S)$ and $\gamma(\mathsf{Bound}(\mathbf{m}, i)) \not\subseteq \gamma(S)$.*

We can now prove that the pairs $\langle C_i, L_i \rangle$ constructed according to Definition 9 are *perfect pairs*.

Lemma 10 *Given a* SMPN $\mathcal{P} = \langle P, T, D^-, D^+ \rangle$ *with the adequate domain of limits $\langle \mathcal{L}, \preccurlyeq_e, \gamma \rangle$ and the sets $C_i \subseteq \mathbb{N}^{k_P}$ and $L_i \subseteq \mathcal{L}$ constructed following Definition 9, any pair $\langle C_i, L_i \rangle$ is a perfect pair.*

Proof. Let us first define $\mathfrak{Post}(\mathbf{m}, i)$ as the set of *maximal elements* of $\cup_{t_k \in T} \mathsf{Bound}(\mathsf{Post}(\mathbf{m}, t_k), i)$. Following the definition of a perfect pair (Definition 8), we show that for any (extended) marking $\mathbf{m} \in L_i \cup C_i$, $\mathfrak{Post}(\mathbf{m}, i)$ is the unique, minimal and *most precise* subset of $L_i \cup C_i$ to cover $\mathsf{Post}(\gamma(\mathbf{m}))$.

From Lemma 9 and Lemma 7, we have that for any $i \geq 0$ and $\mathbf{m} \in L_i \cup C_i$: $\mathfrak{Post}(\mathbf{m}, i)$ is such that $\mathsf{Post}(\gamma(\mathbf{m})) \subseteq \gamma(\mathfrak{Post}(\mathbf{m}, i))$. Moreover, for all $\mathbf{m}_1, \mathbf{m}_2 \in \mathfrak{Post}(\mathbf{m}, i) : \mathbf{m}_1 \neq \mathbf{m}_2$ implies $\mathbf{m}_1 \not\preccurlyeq_e \mathbf{m}_2$ (because we keep the maximal elements only). Let $L \subseteq L_i \cup C_i$ be a set such that $L \neq \mathfrak{Post}(\mathbf{m}, i)$, $\mathsf{Post}(\gamma(\mathbf{m})) \subseteq \gamma(L), \forall \mathbf{m}_1, \mathbf{m}_2 \in L : \mathbf{m}_1 \neq \mathbf{m}_2$ implies $\mathbf{m}_1 \not\preccurlyeq_e \mathbf{m}_2$, and $\nexists L' \subseteq L_i \cup C_i : \mathsf{Post}(\gamma(\mathbf{m})) \subseteq \gamma(L') \subset \gamma(L)$. If such a set L does not exist (and we prove in the next paragrpah that such a set does not exist), we can conclude that there does not exist $L' \subseteq C_i \cup L_i : \mathsf{Post}(\gamma(\mathbf{m})) \subseteq L' \subset \mathfrak{Post}(\mathbf{m}, i)$. Indeed, if such a L' existed there should also exist $L'' \subseteq C_i \cup L_i$ with $\mathsf{Post}(\gamma(\mathbf{m})) \subseteq L'' \subset L'$. By iterating the reasoning we conclude that there should exist an infinite sequence $K_1, K_2, \ldots$ such that $\forall j \geq 1 : K_j \subseteq C_i \cup L_i$ and $\gamma(K_j) \subset \gamma(K_{j+1})$. However, since there exists only a finite number of subsets of $C_i \cup L_i$ that sequence does not exist. Hence $\gamma(\mathfrak{Post}(\mathbf{m}, i))$ is a most precise $\preccurlyeq_e$-downward-closed overapproximation of $\mathsf{Post}(\gamma(\mathbf{m}))$, and $\mathfrak{Post}(\mathbf{m}, i)$ is the unique most precise $\preccurlyeq_e$-downward-closed overapproximation of $\mathsf{Post}(\gamma(\mathbf{m}))$, which implies that any pair $\langle C_i, L_i \rangle$ is a perfect pair.

Thus, we can finish the proof by showing that such a L does not exist. We proceed by contradiction. Suppose that there exists $L \subseteq L_i \cup C_i$ such that $L \neq \mathfrak{Post}(\mathbf{m}, i)$, $\mathsf{Post}(\gamma(\mathbf{m})) \subseteq \gamma(L)$, $\forall \mathbf{m}_1, \mathbf{m}_2 \in L : \mathbf{m}_1 \neq \mathbf{m}_2$ implies $\mathbf{m}_1 \not\preccurlyeq_e \mathbf{m}_2$, and there is no $L' \subseteq L_i \cup C_i : \mathsf{Post}(\gamma(\mathbf{m})) \subseteq \gamma(L') \subset \gamma(L)$. By hypothesis, both L and $\mathfrak{Post}(\mathbf{m}, i)$ are minimal, and $L \neq \mathfrak{Post}(\mathbf{m}, i)$. Thus, by Lemma 6, $\gamma(\mathfrak{Post}(\mathbf{m}, i)) \not\subseteq \gamma(L)$. Hence, there exists $\mathbf{n} \in \mathfrak{Post}(\mathbf{m}, i)$, s.t. $\gamma(\mathbf{n}) \not\subseteq \gamma(L)$. By definition of $\mathfrak{Post}(\mathbf{m}, i)$, $\mathbf{n} = \mathsf{Bound}(\mathsf{Post}(\mathbf{m}, t_j), i)$ for some $t_j \in T$. Remark that $\gamma(\mathsf{Post}(\mathbf{m}, t_j)) \subseteq \gamma(L)$, because $\gamma(\mathsf{Post}(\mathbf{m})) \subseteq \gamma(L)$, by hypothesis. Since L is a finite subset of $L_i \cup C_i$, we can apply Lemma 9 and obtain that $\gamma(\mathbf{n}) = \gamma(\mathsf{Bound}(\mathsf{Post}(\mathbf{m}, t_j), i)) \subseteq \gamma(L)$ which is a contradiction. □

From Lemma 10 and Lemma 3, the following corollary holds.

Corollary 2 *Given a $\preccurlyeq$-strongly monotonic* SMPN *net $\mathcal{P}$ with the adequate domain of limits $\langle \mathcal{L}, \preccurlyeq_e, \gamma \rangle$ and the sets $C_i \subseteq \mathbb{N}^{k_P}$ and $L_i \subseteq \mathcal{L}$ constructed following Definition 9, $\mathsf{Abs}(\mathcal{P}, C_i, L_i)$ is a degenerated And-Or graph.*

Algorithm for the coverability problem. Let $\mathsf{Abs}(\mathcal{P}, i)$ be the graph (degenerated And-Or graph) $\mathsf{Abs}(\mathcal{P}, C_i, L_i)$ constructed from $\mathcal{P}$, C_i and L_i. We note $\Rightarrow$ its transition relation. We define $\mathsf{EPRG}(\mathcal{P}, i)$ as $\mathsf{EPRG}(\mathcal{P}, C_i)$ and $\mathsf{Reach}(\mathsf{Abs}(\mathcal{P}, i))$ as the set $\{\mathbf{m} \mid \mathbf{m}_0 \Rightarrow \mathbf{m}_1 \Rightarrow \ldots \Rightarrow \mathbf{m}_n$ with $\forall 1 \leq j \leq n : \mathbf{m}_j \in L_i \cup C_i, \mathbf{m}_n = \mathbf{m}\}$. By applying the schema presented in Section 4 to $\preccurlyeq$-strongly monotonic self-modifying Petri nets, we obtain the algorithm at Algorithm 2. Remark that this algorithm is *incremental*: one can compute $\mathsf{Reach}(\mathsf{EPRG}(\mathcal{P}, i+1))$ by extending $\mathsf{Reach}(\mathsf{EPRG}(\mathcal{P}, i))$ for all $i \geq 0$. Similarly, one can construct $\mathsf{Reach}(\mathsf{Abs}(\mathcal{P}, i))$ from $\mathsf{Reach}(\mathsf{EPRG}(\mathcal{P}, i))$.

Algorithm 2: A forward algorithm to decide the coverability problem on SMPN.

Data : $\mathcal{P}$, a $\preccurlyeq$-strongly monotonic self-modifying Petri system

Data : G_U, the set of minimal element of the $\preccurlyeq$-upward-closed set U.

begin

  $i \leftarrow 1$;

  while *(***true***)* **do**

    if $\mathsf{Reach}(\mathsf{EPRG}(\mathcal{P}, i)) \cap U \neq \emptyset$ **then**

      return *'Reachable'*;

    else if $\nexists \mathbf{m} \in \mathsf{Reach}(\mathsf{Abs}(\mathcal{P}, i)), \mathbf{m}' \in G_U : \mathbf{m} \preccurlyeq_e \mathbf{m}'$ **then**

      return *'Unreachable'*;

    $i \leftarrow i + 1$;

end

Theorem 4 *Algorithm 2 returns 'Reachable' if* $\mathsf{Reach}(\mathcal{P}) \cap U \neq \emptyset$*, 'Unreachable' otherwise.*

6 Application to Lossy Channel Systems

To show the generality of our new approach, we apply our algorithmic schema to *lossy channel systems*, which are systems made up of automata extended with FIFO channels that may lose messages. We recall the model, define an adequate domain of limits, show how to construct the sets C_i's and L_i's and discuss the construction of the And-Or graph.

A *Lossy Channel System*, LCS for short, is a tuple $\mathcal{C} = \langle Q, q_i, F, \Sigma, T \rangle$ where Q is a finite set of locations, $q_i \in Q$ is the initial location, F is a finite set of channels, Σ is a finite alphabet, $T \subseteq Q \times Op \times Q$ where $Op : F \mapsto \bigcup_{a \in \Sigma} \{?a, !a\} \cup \{\mathsf{nop}\}$. A state is a pair $\langle q, W \rangle$ where $q \in Q$, $W : F \mapsto \Sigma^*$. In the following, $\mathcal{S}_\mathcal{C}$ will denote the set of states of the LCS $\mathcal{C}$. We define the order $\precsim$ on states in $\mathcal{S}_\mathcal{C}$ such that for any $s = \langle q, W \rangle, s' = \langle q', W' \rangle : s \precsim s'$ if and only if $q = q'$ and $W(f)$ is a (not necessarily contiguous) subword of $W'(f)$ for all $f \in F$. That is, $W(f)$ is obtained from $W'(f)$ by deleting characters. It is well-known that $\precsim$ is a well-quasi order (see for instance [5]). Let $\cdot$ denote the word concatenation. We define $\mathsf{subword} : \Sigma^* \mapsto 2^{\Sigma^*}$ such that $\mathsf{subword}(w)$ is the set of subwords of w. We extend subword to function $W : F \mapsto \Sigma$, such that $\mathsf{subword}(W)$ denotes the set of functions $W' : F \mapsto \Sigma^*$ such that $\forall f \in F : W'(f) \in \mathsf{subword}(W(f))$. A transition $t = \langle q_1, Op, q_2 \rangle \in T$ is firable from state $\langle q, W \rangle$ if $q = q_1$ and for all $f \in F : Op(f) = ?a$ implies that $W(f)$ contains at least one letter 'a'. Firing t from $\langle q, W \rangle$ leads to states $\langle q', W' \rangle$ (noted $\langle q, W \rangle \rightarrowtail_t \langle q', W' \rangle$) such that $q' = q_2$ and there exist $\overline{W} \in \mathsf{subword}(W)$ and $\overline{W'}$ with $W' \in \mathsf{subword}(\overline{W'})$ such that $\forall f \in F : Op(f) = ?a$ implies $\overline{W}(f) = a \cdot \overline{W'}(f), Op(f) = !a$ implies $\overline{W'}(f) =$

$\overline{W}(f)\cdot a$ and $Op(f) = \mathsf{nop}$ implies $\overline{W}(f) = \overline{W'}(f)$. Given a set S of states and a transition t, $\mathsf{Post}(S,t) = \{s' \mid \exists s \in S : s \rightarrowtail_t s'\}$. A LCS $\mathcal{C} = \langle Q, q_i, F, \Sigma, T\rangle$ defines a transition system $\langle \mathcal{S}_\mathcal{C}, s_0, \rightarrow\rangle$ where $s_0 = \langle q_i, W_i\rangle$ such that $W_i(f) = \varepsilon$ for all $f \in F$ and for all $s_1, s_2 \in \mathcal{S}_\mathcal{C} : s_1 \rightarrow s_2$ if and only if $\exists t \in T : s_1 \rightarrowtail_t s_2$. It is well-known that transition relations defined by LCS are $\precsim$-monotonic.

In the following, we always consider a LCS $\mathcal{C} = \langle Q, q_i, F, \Sigma, T\rangle$.

Domain of limits. Let $L(\Sigma)$ be the set of $\precsim$-downward-closed regular expressions (dc-re) $\{(a_1 + \ldots + a_n)^* \mid \forall 1 \leq i \leq n : a_i \in \Sigma, \forall i,j : i \neq j$ implies that $a_i \neq a_j\} \cup \{(a + \varepsilon) \mid a \in \Sigma\} \cup \{\varepsilon\}$. A simple regular expression (sre) is either a dc-re or an expression $d_1 \cdot \ldots \cdot d_n$ where $\forall 1 \leq i \leq n : d_i$ is a dc-re. The size of a sre is the number of dc-re that compose it. The set of limits is the set $\mathcal{L}(\Sigma, Q) = \{\langle q, E\rangle \mid q \in Q, E : F \mapsto L(\Sigma)^*$ assigns a sre to each channel [5] $\} \cup \{\top\}$. For $\langle q, E\rangle \in \mathcal{L}(\Sigma, Q)$: $[\![\langle q, E\rangle]\!]$ denotes the set of pairs $\langle q, W\rangle \in \mathcal{S}_\mathcal{C}$ such that $W(f)$ is a word in the language generated by the regular expression $E(f)$ for all $f \in F$. We define the function $\gamma : \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q) \mapsto 2^{\mathcal{S}_\mathcal{C}}$ such that (i) for all $\langle q, W\rangle \in \mathcal{S}_\mathcal{C} : \gamma(\langle q, W\rangle) = \{\langle q, W'\rangle \mid \langle q, W'\rangle \precsim \langle q, W\rangle\}$, (ii) $\gamma(\top) = \{\langle q, W\rangle \mid q \in Q, W(f) \in \Sigma^*$ for all $f \in F\}$ and (iii) for all $\langle q, E\rangle \in \mathcal{L}(\Sigma, Q) \setminus \{\top\} : \gamma(\langle q, E\rangle) = [\![\langle q, E\rangle]\!]$. We define $\overline{\sqsubseteq} : (\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)) \times (\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q))$ as follows : $c_1 \overline{\sqsubseteq} c_2$ if and only if $\gamma(c_1) \subseteq \gamma(c_2)$. The following theorem holds:

Theorem 5 *$(\mathcal{L}(\Sigma, Q), \overline{\sqsubseteq}, \gamma)$ is an adequate domain of limits for $(\mathcal{S}_\mathcal{C}, \precsim)$.*

Proof. We establish this result by proving the four points of Definition 1:

- (L_1) It is easy to show that for any $\langle q, E\rangle \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$, $\gamma(\langle q, E\rangle)$ is $\precsim$-downward-closed (see [5]);
- (L_2) the element $\top$ is such that $\gamma(\top)$ is the whole set of states $\mathcal{S}_\mathcal{C}$;
- (L_3) by definition $c_1 \overline{\sqsubseteq} c_2$ if and only if $\gamma(c_1) \subseteq \gamma(c_2)$ for all $c_1, c_2 \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$;
- (L_4) from Theorem 1 of [5] we deduce that if $S \subseteq \mathcal{S}_\mathcal{C}$ is $\precsim$-downward-closed, then there exists $S' \subseteq \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$ such that S' is finite and $\gamma(S') = S$.

□

Moreover, the following theorem says that any LCS $\mathcal{C}$ with the adequate domain of limits $(\mathcal{L}(\Sigma, Q), \overline{\sqsubseteq}, \gamma)$ are effective.

Theorem 6 *Any LCS $\mathcal{C}$ with the adequate domain of limits $(\mathcal{L}(\Sigma, Q), \overline{\sqsubseteq}, \gamma)$ are effective.*

[5] We also require that E does not assign ε to all the channels because we require in Definition 1 that the set of limits is disjoint from $\mathcal{S}_\mathcal{C}$.

Proof. We establish the theorem by proving that the four properties of Definition 3 hold:

(E_1) it is easy to show that $\mathcal{S}_\mathcal{C}$ and $\mathcal{L}(\Sigma, Q)$ are recursively enumerable;
(E_2) it is shown in [5] that the transition relation of LCS is decidable;
(E_3) it is shown in [5] how to compute an operator that returns, given $c \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$, $c' \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$ such that $\gamma(c') = \mathsf{Post}(\gamma(c))$. By using that operator and since $\overline{\sqsubseteq}$ is decidable following [5], we conclude that we can decide whether $\mathsf{Post}(\gamma(c)) \subseteq \gamma(c')$ for any $c, c' \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$;
(E_4) as noticed in the previous point, an algorithm is given in [5] to decide whether $c_1 \overline{\sqsubseteq} c_2$ for any $c_1, c_2 \in \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$. Moreover, for any $C_1, C_2 \subseteq \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$, $\gamma(C_1) \subseteq \gamma(C_2)$ if and only if for all $c \in C_1$, there exists $c' \in C_2$ such that $c \precsim c'$ (see [5] for proofs). Hence, we can decide for any finite sets $C_1, C_2 \subseteq \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$ whether $\gamma(C_1) \subseteq \gamma(C_2)$.

□

Construction of the C_i's and the L_i's. We construct the sequences of the C_i's and L_i's as follows. $C_i = \{\langle q, W\rangle \in \mathcal{S}_\mathcal{C} \mid q \in Q, \forall f \in F : W(f) = \varepsilon \text{ or } W(f) = a_1 \cdot \ldots \cdot a_n \text{ with } \forall 1 \leq j \leq n : a_j \in \Sigma, n \leq i\}$. That is, C_i is the set of states where the contents of the channels are words of size at most i. Similarly, $L_i = \{\langle q, E\rangle \in \mathcal{L}(\Sigma, Q) \mid q \in Q, \forall f \in F : E(f) = \varepsilon \text{ or } E(f) = d_1 \cdot \ldots \cdot d_n \text{ with } \forall 1 \leq j \leq n : d_j \in L(\Sigma), n \leq i\} \cup \{\top\}$. That is, L_i is the set of limits that assign sre of size of most i to channels (plus the $\top$ element).

It is easy to see that (i) $C_i \subseteq C_{i+1}$ and $L_i \subseteq L_{i+1}$ for all $i \geq 0$, (ii) for all $c \in \mathcal{S}_\mathcal{C}$ there exists $i \geq 0$ such that $c \in C_i$ and for all $\ell \in \mathcal{L}(\Sigma, Q)$ there exists $i \geq 0$ such that $\ell \in L_i$, (iii) $\langle q_i, W_i\rangle \in C_0$ where $\forall c \in C : W_i(c) = \varepsilon$ and (iv), by construction $\top \in L_0$.

Construction of the And-Or graph. In order to construct the And-Or graph, we need to construct the set of Or-nodes (point $\mathsf{A_1}$), the set of And-nodes (point $\mathsf{A_2}$) and the transition relation between nodes (points $\mathsf{A_{4.1}}$ and $\mathsf{A_{4.2}}$). The two first points are obvious. Let us focus on the construction of the transition relation. Given the two sets C_i and L_i as defined above, the successors of And-nodes are computed as follows. For any And-node $n \in 2^{L_i \cup C_i} \setminus \{\emptyset\}$, we have $(n, n') \in \Rightarrow$ if and only if $n' \in n$. In order to define the successors of an Or-node, we need the following functions. Let $\widetilde{\mathsf{Post}}(.,.) : (\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)) \times T \mapsto \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$ be the partial function defined in [5] that returns the element ℓ' in $\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)$ such that $\gamma(\ell')$ is the set of successors of $\gamma(\ell)$ by firing t ($\widetilde{\mathsf{Post}}(\ell, t)$ is undefined when t is not firable from $\gamma(\ell)$). The partial function $\mathsf{App}(\ell, t, i) : (\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)) \times T \times \mathbb{N} \mapsto 2^{\mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma, Q)}$ is such that $\widetilde{\mathsf{App}}(\ell, t, i)$ is defined iff t is firable from $\gamma(\ell)$. In that case, $\widetilde{\mathsf{App}}(\ell, t, i) = \widetilde{\mathsf{Post}}(\ell, t)$ if $\widetilde{\mathsf{Post}}(\ell, t) \in C_i \cup L_i$, otherwise $\widetilde{\mathsf{App}}(\ell, t, i) = \{\ell' \in L_i \cup C_i \mid \widetilde{\mathsf{Post}}(\ell, t) \overline{\sqsubseteq} \ell', \neg\exists \ell'' \in$

$L_i \cup C_i : \widetilde{\mathsf{Post}}(\ell,t)\overline{\sqsubseteq}\ell''\overline{\sqsubset}\ell'\}$. Otherwise stated, when $\mathsf{App}(\ell,t,i)$ is defined, it returns $\widetilde{\mathsf{Post}}(\ell,t)$ if this latter set is in the set $L_i \cup C_i$ of states and limits that we consider during the construction of the graph, otherwise it returns the set of all the $\ell' \in L_i \cup C_i$ such that each $\gamma(\ell')$ is one of the best overapproximations of $\gamma(\widetilde{\mathsf{Post}}(\ell,t))$. Notice that we can always construct $\mathsf{App}(\ell,t,i)$ since $\widetilde{\mathsf{Post}}(\ell,t)$ is constructible [5], C_i and L_i are finite and $\overline{\sqsubseteq}$ is decidable. Let $\mathsf{Firable}(\ell) = \{t_1,\ldots,t_{k_\ell}\}$ be the set of k_ℓ transitions that are firable from $\gamma(\ell)$ and $\mathfrak{Post}(\ell,i) = \{\{c_1,\ldots,c_{k_\ell}\} \subseteq L_i \cup C_i \mid \mathsf{Firable}(\ell) = \{t_1,\ldots,t_{k_\ell}\}, \forall 1 \leq j \leq k_\ell : c_j \in \mathsf{App}(\ell,t_j,i)\}$, that is, $\mathfrak{Post}(\ell,i)$ is the set of sets of elements in $L_i \cup C_i$ that represent an over-approximation of the successors of $\gamma(\ell)$. Sets in $\mathfrak{Post}(\ell,i)$ satisfy the *covering* property of point $\mathsf{A}_{4.2}$, but they may not be minimal, because they could contain two elements that are ordered, and they may not represent most precise overapproximations of the set of successors. For any $n \in V_O$, we define the set of And-nodes that are successor of n as: $\mathsf{Succ}(n,i) = \{S \subseteq L_i \cup C_i \mid \exists S' \in \mathfrak{Post}(n,i) : S \subseteq S', \gamma(S) = \gamma(S'), \forall c_1,c_2 \in S : c_1 \neq c_2$ implies $c_1\overline{\not\sqsubseteq}c_2, \neg\exists S'' \in \mathfrak{Post}(n,i) : \gamma(S'') \subset \gamma(S)\}$. That is $\mathsf{Succ}(n,i)$ is the set of most precise and minimal approximations of the set of successors of $\gamma(n)$. That set is constructible since $\mathfrak{Post}(\ell,i)$ is constructible and, following Theorem 6 and so E_4 of Definition 3, $\gamma(S) \subseteq \gamma(S')$ is decidable for any finite $S, S' \subseteq \mathcal{S}_\mathcal{C} \cup \mathcal{L}(\Sigma,Q)$.

Remark 4 *Contrary to the* SMPN*, an And-Or graph is necessary in the present case to ensure the termination of our algorithm. Let us illustrate this thanks to the* LCS *of Fig. 3. It is made up of one automaton and a single channel. Its set of reachable configurations is the $\precsim$-downward-closure of $\{\langle 1,\varepsilon\rangle\} \cup \{\langle 2, \mathtt{c}\cdot w_{ab}\rangle\}$, where w_{ab} can be any word made up of an arbitrary number of* a *and* b*'s.*

Let us suppose we want to prove that the number of c *in the channel is always bounded, when the* LCS *reaches state 2. This property holds on the* LCS *of Fig 3, and it corresponds to showing that the $\precsim$-upward-closed set $\{c|\langle 2,\mathtt{cc}\rangle \precsim c\}$ is not reachable. Let us further suppose we are trying to compute an over-approximation of the* LCS *for some value $i \geq 2$ of the bound*[6] *. At some point, we will end up computing the set of successors of the configuration $\langle 2, \mathtt{c}\cdot\mathtt{a}^j\cdot\mathtt{b}^k\rangle$ with $|\mathtt{c}\cdot\mathtt{a}^j\cdot\mathtt{b}^k| = j+k+1 = i$, $j \geq 1$ and $k \geq 0$. Remark that this configuration is in C_i, but its successors are not. Hence we need to use limit elements to represent them.*

Actually, two incomparable *set of limit elements can be used for this purpose: $\ell_1 = \left\{\left\langle 2, (\mathtt{c}+\mathtt{a})^*\cdot(\mathtt{b}+\varepsilon)^{k+1}\right\rangle, \left\langle 2, (\mathtt{c}+\mathtt{a})^*\cdot(\mathtt{b}+\varepsilon)^k\cdot(\mathtt{a}+\varepsilon)\right\rangle\right\}$ and $\ell_2 = \left\{\left\langle 2, (\mathtt{c}+\varepsilon)\cdot(\mathtt{a}+\mathtt{b})^*\right\rangle\right\}$. If we represent the over-approximation by an And-*

[6] It is easy to see that the algorithm can't prove the safety of the system for $i = 1$. For this value, the only limit that contains a, b and c is $(\mathtt{a}+\mathtt{b}+\mathtt{c})^*$, which is clearly too coarse.

Or graph, this is not a problem, since we can choose between ℓ_1 and ℓ_2, and ℓ_2 allows us to prove the safety of the system (under the hypothesis that the other branches of the unfolding are also safe*). On the other hand, if we use a* plain graph*, we have to* guess *which limit is the good one. By choosing ℓ_1, we are not able to prove the safety, which compels the algorithm to build another graph. As stated in Remark 3, one could imagine two different ways to do this. The first solution would be to keep the same value of i, and build another graph (in which ℓ_2, for instance, will be chosen). It is not difficult to see that such a procedure could have to build an number of graphs that is exponential in the size of $L_i \cup C_i$. This solution is clearly less efficient than the* PTime *algorithm that explores And-Or graphs. The other solution could be to try to refine the bound, and build a new approximation for the value $i+1$. However, suppose now that the* bad guess *occurs repeatedly for any i. In this case, it is not difficult to see that the algorithm will fail to terminate and prove the safety of the system, although the system is safe !*

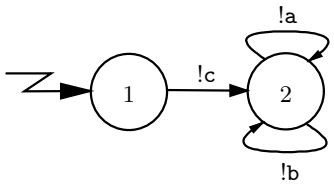

Fig. 3. A LCS with one channel: locations are represented by circles (location 1 is initial); transitions by arrows. The labels are the operations on the channel.

7 Conclusion

In this paper, we have defined 'Expand, Enlarge and Check', a new approach to solve the coverability problem of WSTS. The main idea of this new approach consists in building, in parallel, two sequences of approximations of the system considered. The first sequence provides more and more precise under-approximations of the system. They allow us to decide the positive instances of the coverability problem. Similarly, the second sequence is made up of successive over-approximations of the system, which allow us to decide the negative instances of the problem. These sequences of approximations have been thoroughly defined and studied in section 3, leading to the schema of algorithms of section 4.

Although the 'Expand, Enlarge and Check' approach is a general and theoretical schema of algorithm, it can be easily adapted to several practically interesting classes of WSTS, in order to produce efficient algorithms. In particular, we have explained, in section 5, how to obtain an algorithm that uses forward analysis to decide the coverability problem for a large class of monotonic counter systems (the strongly monotonic Self-modifying Petri nets). Up

to now, such a forward approach was known only for Petri nets (the Karp and Miller algorithm), a restricted subclass of strongly monotonic SMPN. Similarly, we have showed in section 6 that the 'Expand, Enlarge and Check' algorithm can also be applied to the important class of Lossy Channel Systems.

In this paper, we have intendedly kept a purely theoretical point of view along the whole discussion. However, prototypes implementations of 'Expand, Enlarge and Check' have been realized, and their performances are really promizing. Our new prototypes are able to analyze a whole set of classical examples of SMPN and LCS from the literature, on which a previous fine-tuned prototype, based on backward-search, does not always terminate. We refer the interested reader to [27], in which we present several additional optimizations of the algorithm, and report on the practical performances of our prototypes.

Acknowledgements. The authors are deeply grateful to Ahmed Bouajjani and Mihaela Sighireanu, who gave them access to their very neat implementation of a C++ library that manipulates Simple Regular Expressions. This piece of work greatly eased the implementation of the aforementioned LCS prototype.

References

[1] G. Geeraerts, J.-F. Raskin, L. Van Begin, Expand, enlarge and check: new algorithms for the coverability problem of WSTS, in: Proceedings of the 24th International Conference on Fondation of Software Technology and Theoretical Computer Science (FSTTCS 04), Vol. 3328 of LNCS, Springer, 2004, pp. 287–298.

[2] R. Alur, D. Dill, A Theory of Timed Automata, Theoretical Computer Science 126 (2) (1994) 183–236.

[3] T. A. Henzinger, The theory of hybrid automata, in: Proceedings of the 11th Symposium on Logic in Computer Science (LICS '96), IEEE Computer Society, 1996, p. 278.

[4] P. Abdulla, B. Jonsson, Verifying Programs with Unreliable Channels, in: Proceedings of the 8th IEEE International Symposium in Logic in Computer Science (LICS'93), IEEE Computer Society Press, 1993, pp. 160–170.

[5] P. Abdulla, A. Bouajjani, B. Jonsson, On-the-Fly Analysis of Systems with Unbounded, Lossy FIFO Channels, in: Proceedings of the 10th International Conference on Computer Aided Verification (CAV'98), Vol. 1427 of LNCS, Springer, 1998, pp. 305–318.

[6] P. Abdulla, A. Annichini, A. Bouajjani, Symbolic verification of lossy channel systems: Application to the bounded retransmission protocol, in: Proc. 5th

Intern. Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'99), no. 1579 in LNCS, Springer-Verlag, 1999, pp. 208–222.

[7] G. Delzanno, J.-F. Raskin, L. Van Begin, Towards the Automated Verification of Multithreaded Java Programs, in: Proceedings of the International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS 2002), Vol. 2280 of LNCS, Springer, 2002, pp. 173–187.

[8] S. Bardin, A. Finkel, J. Leroux, L. Petrucci, FAST: Fast acceleration of symbolic transition systems, in: Proceedings of the 15th International Conference on Computer Aided Verification (CAV'03), will be published in LNCS, Springer, 2003.

[9] J. Esparza, A. Finkel, R. Mayr, On the Verification of Broadcast Protocols, in: Proceedings of the 14th Annual Symposium on Logic in Computer Science (LICS'99), IEEE Computer Society Press, 1999, pp. 352–359.

[10] J. L. Peterson, Petri Net Theory and the Modeling of Systems, Prentice Hall, 1981.

[11] G. Ciardo, Petri nets with marking-dependent arc multiplicity: properties and analysis, in: Proceedings of the 15th International Conference on Applications and Theory of Petri Nets (ICATPN 94), Vol. 815 of LNCS, Springer, 1994, pp. 179–198.

[12] C. Dufourd, A. Finkel, P. Schnoebelen, Reset Nets Between Decidability and Undecidability, in: In Proceedings of the 25th International Colloquium on Automata, Languages, and Programming (ICALP'98), Vol. 1443 of LNCS, Springer, 1998, pp. 103–115.

[13] J.-F. Raskin, L. Van Begin, Petri Nets with Non-blocking Arcs are Difficult to Analyse, in: Proceedings of the 5th International Workshop on Verification of Infinite-state Systems (INFINITY 2003), Vol. 96 of ENTCS, Elsevier, 2003.

[14] E. A. Emerson, K. S. Namjoshi, On Model Checking for Non-deterministic Infinite-state Systems, in: Proceedings of the 13th Annual Symposium on Logic in Computer Science (LICS '98), IEEE Computer Society Press, 1998, pp. 70–80.

[15] P. A. Abdulla, K. Cerans, B. Jonsson, Y.-K. Tsay, General Decidability Theorems for Infinite-state Systems, in: Proceedings of the 11th Annual Symposium on Logic in Comuter Science (LICS'96), IEEE Computer Society Press, 1996, pp. 313–321.

[16] A. Finkel, P. Schnoebelen, Well-structured transition systems everywhere!, Theoretical Computer Science 256 (1-2) (2001) 63–92.

[17] T. A. Henzinger, O. Kupferman, S. Qadeer, From *pre*historic to *post*modern symbolic model checking, Formal Methods in System Design 23 (3) (2003) 303–327.

[18] R. M. Karp, R. E. Miller, Parallel Program Schemata, Journal of Computer and System Sciences 3 (1969) 147–195.

[19] A. Finkel, Reduction and Covering of Infinite Reachability Trees, Information and Computation 89 (2) (1990) 144–179.

[20] A. Bouajjani, B. Jonsson, M. Nilsson, T. Touili, Regular Model Checking, in: Proceedings of the 2th International Conference on Computer Aided Verification (CAV 2000), Vol. 1855 of LNCS, Springer, 2000, pp. 403–418.

[21] A. Finkel, J.-F. Raskin, M. Samuelides, L. Van Begin, Monotonic Extensisions of Petri Nets : Forward and Backward Search Revisited, in: Proceedings of the 4th international workshop on verification of infinite-state systems (INFINITY 2002), Vol. 68 of ENTCS, Elsevier, 2002.

[22] N. Immerman, Number of quantifiers is better than number of tape cells, Journal of Computer and System Sciences 22 (3) (1981) 384–406.

[23] R. Milner, Communication and Concurrency, Prentice-Hall International series in computer science, Prentice Hall, New York, 1989.

[24] R. Valk, On the computational power of extended petri nets, in: Proceedings of the 7th symposium on Mathematical Foundations of Computer Science, Vol. 64 of LNCS, Springer, 1978, pp. 527–535.

[25] T. Araki, T. Kasami, Some decision problems related to the reachability problem for petri nets, Theoretical Computer Science 3 (1) (1977) 85–104.

[26] A. Bouajjani, R. Mayr, Model Checking Lossy Vector Addition Systems, in: Proceedings of the 16th Annual Symposium on Theoretical Aspects of Computer Science (STACS'99), Vol. 1563 of LNCS, Springer, 1999, pp. 323–333.

[27] G. Geeraerts, J.-F. Raskin, L. Van Begin, Expand, enlarge and check... made efficient, no. 3576 in Lecture Notes in Computer Science, Springer Verlag, 2005, pp. 394–404, to appear.