I N F S Y S

R E S E A R C H

R E P O R T

INSTITUT FÜR INFORMATIONSSYSTEME

ABTEILUNG WISSENSBASIERTE SYSTEME

ON ACTL FORMULAS HAVING DETERMINISTIC COUNTEREXAMPLES

Francesco BUCCAFURRI Thomas EITER
Georg GOTTLOB Nicola LEONE

INFSYS RESEARCH REPORT 1843-99-01

JANUARY 1999

Institut für Informationssysteme
Abtg. Wissensbasierte Systeme
Technische Universität Wien
Treitlstraße 3
A-1040 Wien, Austria
Tel: +43-1-58801-18405
Fax: +43-1-58801-18493
sek@kr.tuwien.ac.at
www.kr.tuwien.ac.at

TECHNISCHE UNIVERSITÄT WIEN

INFSYS RESEARCH REPORT

INFSYS RESEARCH REPORT 1843-99-01, JANUARY 1999

ON ACTL FORMULAS HAVING DETERMINISTIC COUNTEREXAMPLES

Francesco Buccafurri,[1] Thomas Eiter,[2] Georg Gottlob,[3] Nicola Leone[3]

Abstract. In case an *ACTL* formula ϕ fails over a labeled transition graph M, it is most useful to provide a counterexample, i.e., a computation tree of M witnessing the failure. If there exists a *single path* in M which by itself witnesses the failure of ϕ, then ϕ has a *deterministic counterexample*. We show that, given M and ϕ, where $M \not\models \phi$, it is NP-hard to determine whether there exists a deterministic counterexample. Moreover, it is PSPACE-hard to decide whether an *ACTL* formula ϕ always admits a deterministic counterexample if it fails. This means that there exists no simple characterization of the *ACTL* formulas that guarantee deterministic counterexamples. Consequently, we study *templates* of *ACTL* formulas, i.e., skeletons of modal formulas whose atoms are disregarded. We identify the (unique) maximal set $\mathbf{DET}$ of templates whose instances (obtained by replacing atoms with arbitrary pure state formulas) always guarantee deterministic counterexamples. We show that for each *ACTL* formula ϕ which is an instance of a template $\gamma^\star \in \mathbf{DET}$, and for each Kripke structure M such that $M \not\models \phi$, a single path of M witnessing the failure by itself can be computed in polynomial time.

[1]DIMET, Universitá di Reggio Calabria, I-89100 Reggio Calabria, Italy. E-mail: bucca@ns.ing.unirc.it

[2]Institut und Ludwig Wittgenstein Labor für Informationssysteme, Technische Universität Wien, Treitlstraße 3, A-1040 Wien, Austria. E-mail: eiter@kr.tuwien.ac.at

[3]Institut und Ludwig Wittgenstein Labor für Informationssysteme, Technische Universität Wien, Paniglgasse 16, A-1040 Wien, Austria. E-mail: (leone|gottlob)@dbai.tuwien.ac.at

Contents

1 Introduction

ACTL is a well-known particular fragment of Computational Tree Logic (*CTL*), which is a propositional branching-time temporal logic [2]; see [7, 6] for a rich background on this and further such logics. *ACTL* formulas are specified and evaluated over *Kripke structures* which model finite-state systems. Besides Boolean connectives, *ACTL* provides linear-time and branching time operators. The linear-time operators allow for expressing properties of a particular evolution of the systems given by a series of events in time. Branching time operators allow to take into account the existence of multiple possible future scenarios, starting from a given system state at a point in time. The temporal order defines an evolution tree, which branches from that point towards the future. Thus, every point in time has a unique past, but, in general, more than one future. Each branch of the tree amounts to a particular evolution series.

The elementary linear-time operators are $\mathbf{X}$ (*next time*), $\mathbf{U}$ (*until*), and $\mathbf{V}$ (*unless, releases*). Informally, $\mathbf{X}\phi$ means that ϕ is true at the next point in time; $\phi_1 \mathbf{U} \phi_2$ means that ϕ_1 is true until ϕ_2 is true; and $\phi_1 \mathbf{V} \phi_2$ means that truth of ϕ_2 releases truth of ϕ_1. Further operators such as $\mathbf{F}\phi$ (*sometimes* ϕ), $\mathbf{G}\phi$ (*always* ϕ) can be derived from the elementary operators. *ACTL* has the branching time operator $\mathbf{A}$, by which it is possible to express *necessary* properties for an evolution tree. Informally, $\mathbf{A}\phi$ means that ϕ is true for all branches of the tree. Note that in full *CTL*, a dual operator $\mathbf{E}$ for expressing *possible* properties (true along some branch) is provided.

1.1 Counterpaths and deterministic counterexamples

The task of an automatic *ACTL* model checker is the verification of a given *ACTL* formula ϕ on a Kripke Structure M. In case M does not satisfy ϕ (denoted by $M \not\models \phi$), the more advanced implemented model checkers (e.g. McMillan's SMV system [10]) provide more information. In particular, as a witness for the failure, a finite representation of an infinite computation path π of M is provided. This path represents a counterexample to ϕ in M. In the ideal case, such a path π witnesses *by itself* that $M \not\models \phi$, in other terms, all information needed to disprove that $M \models \phi$ is already contained in π. In this case, we call π a *counterpath*.

To make the above concepts precise, we give in Section 3 a formal definition of the concept of *counterexample*. Roughly, a counterexample to an *ACTL* formula ϕ on structure M is a computation tree represented as a *multi-path* disproving that $M \models \phi$. In case this multi-path has no true branching, and thus actually represents a unique path, we speak about a *deterministic counterexample*. A counterpath for ϕ in M is then the unique path corresponding to a deterministic counterexample. Note that if there exists such a counterpath π, then it holds that $M_\pi \not\models \phi$, where M_π is the Kripke structure induced by π, i.e., the structure whose states are all those states of M that also occur in π, where the states are, moreover, labeled by the same labels as in M, and whose transitions are those that occur in π.

Example 1.1 *Let M amount to the labeled transition graph in Figure 1, and consider the formula $\phi = \mathbf{A}(true\mathbf{U}a_1)$, which can be written shortly as $\mathbf{AF}a_1$.*

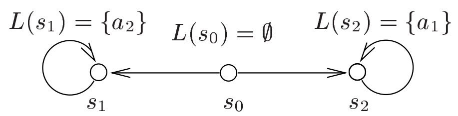

Figure 1: Labeled transition graph representing structure M (initial state s_0)

It holds that $M \not\models \phi$: Along the path $\pi = [s_0, s_1, s_1, \ldots]$, the atom a_1 is false at each stage $\pi(i)$ of π, $i \geq 0$. This implies $M, \pi \models \neg \mathbf{F} a_1$. Thus, π witnesses the failure of ϕ in M. Note that the information contained in π alone is sufficient for disproving ϕ; we do not have to consider elements of M (states or transitions) outside π to show that $M \not\models \phi$. Thus π is a counterpath of ϕ.

1.2 Deterministic counterexamples may not exist

A counterpath provides very useful, compactly presented, and self-contained information to a system designer or verifier, allowing him or her to locate a design error in a most comfortable way. It would thus be most desirable to be able to compute a (representation of a) counterpath in polynomial time whenever an *ACTL* formula ϕ fails over a structure M.

Unfortunately, as shown by the example below, if $M \not\models \phi$, a counterpath (or, equivalently, a deterministic counterexample) does not necessarily exist.

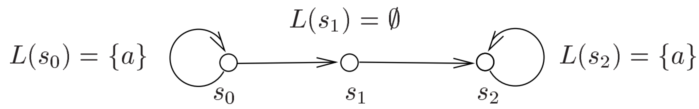

Figure 2: Another transition graph representing structure M (initial state s_0)

Example 1.2 *Let M amount to the labeled transition graph in Figure 2. Consider the formula $\phi = \mathbf{A}(true\mathbf{U}\mathbf{A}(false\mathbf{V}a))$, which can be abbreviated as $\mathbf{AFAG}a$. It is easy to verify that $M \not\models \phi$. Indeed, there is a path $\pi = [s_0, s_0, \ldots]$ starting from the initial state where always the nested formula $\mathbf{AG}a$ does not hold, as, for each $i \geq 0$, there exists a path starting at $\pi(i)$ where sometimes a is not true (e.g., on the path $\pi' = [s_0, s_1, s_2, s_2, \ldots]$ a is not true at s_1). The path π itself is not a complete counterexample. To disprove that $M \models \phi$, it is necessary to consider a further path for each state of π (here always s_0) in order to show that the subformula $\mathbf{AG}a$ does not hold. This gives rise to a multi-path Π, which we write as follows: $\Pi = [[s_0, s_1, s_2, s_2, \ldots], [s_0, s_1, s_2, s_2, \ldots], \ldots]$. This multi-path Π is a counterexample for ϕ in M, and not the single path π. Note that Π is <u>not</u> a deterministic counterexample, but a truly branching infinite tree. Note, furthermore, that no single path is a counterexample for ϕ. Therefore, no deterministic counterexample exists in this case, and thus no counterpath witnessing that $M \not\models \phi$ exists.*

Besides the above very simple example, many other cases can be found in which each counterexample is a truly branching computation tree. They include formulas of the shape $\mathbf{AF}\phi \vee \mathbf{AF}\psi$ (e.g., $\mathbf{AF}a_1 \vee \mathbf{AF}a_2$ on the structure M in Fig. 1), $\mathbf{AF}(\mathbf{AG}\phi \vee \mathbf{AG}\neg\phi)$, which informally states that any evolution must commit at some point about a condition ϕ being true or false, and $\mathbf{AF}\phi \vee \mathbf{AG}\psi$, which states that either ϕ becomes true at some stage or ψ always holds.

Thus, in many cases the "counterexample path" output by an *ACTL* model checker such as McMillan's system [10] is not a complete counterexample, but only one path – usually the main path or "backbone" – of a counterexample. Such a path may help to track the design or implementation error, but it does by itself not necessarily explain why the formula fails, and one may need to consider states and transitions outside that path in order to track the flaw.

$$
\begin{aligned}
\mathit{DET} &::= \mathit{PSF} \mid (\mathit{DET} \wedge \mathit{DET}) \mid (\mathit{DET} \vee \mathit{PSF}) \mid (\mathit{PSF} \vee \mathit{DET}) \mid \mathbf{AX}(\,\mathit{DET}\,) \mid \mathbf{A}(\,\mathit{PSF}\,\mathbf{V}\,\mathit{DET}\,) \mid \mathit{UDET} \\
\mathit{UDET} &::= \mathbf{A}(\,\mathit{DET}\,\mathbf{U}\,\mathit{PSF}\,) \mid \mathbf{A}(\,\mathit{PSF}\,\mathbf{U}\,\mathit{UDET}\,) \mid (\,\mathit{UDET} \vee \mathit{PSF}\,) \mid (\,\mathit{PSF} \vee \mathit{UDET}\,) \\
\mathit{PSF} &::= (\,\mathit{PSF} \wedge \mathit{PSF}\,) \mid (\,\mathit{PSF} \vee \mathit{PSF}\,) \mid \neg(\,\mathit{PSF}\,) \mid \star
\end{aligned}
$$

Table 1: BNF Grammar for deterministic templates

1.3 Main research questions addressed

Given that deterministic counterexamples (and counterpaths) are useful, but do not always exist, the following questions naturally arise:

○ Is there an efficient method of deciding whether an *ACTL* formula ϕ has a deterministic counterexample (and thus a counterpath) on a given Kripke structure M, where $M \not\models \phi$?

○ Is there a simple characterization of those *ACTL* formulas which *guarantee* deterministic counterexamples? In other terms, is there an efficient method for telling whether a formula ϕ has the property that whenever $M \not\models \phi$ holds for a structure M, then there exists a deterministic counterexample (and thus a counterpath) witnessing this?

○ If the above fails, how can we efficiently identify large classes of formulas that guarantee deterministic counterexamples?

○ Can we efficiently *compute* deterministic counterexamples in case they exist? If this is not generally possible, then maybe for large classes of *ACTL* formulas?

1.4 Main results

Our main results are shortly summarized as follows:

• We give, in Section 2, a precise definition of the concepts of deterministic counterexample and of the related concept of *counterpath*.

• We show that given M and ϕ, where $M \not\models \phi$, it is NP-hard to determine whether there exists a deterministic counterexample (Theorem 4.2).

• As a consequence, even in case counterpaths exist, *computing* a counterpath is a hard problem. Therefore, unless NP=P, for every *ACTL* model-checker $\mathcal{MC}$ that works in polynomial time and produces "single-path counterexamples" in case of failure, there exist infinitely many Kripke structures M and formulas ϕ, such that $M \not\models \phi$ and the counterexample path output by $\mathcal{MC}$ represents a partial (and not a complete) counterexample even though there exists a counterpath (i.e., a path representing a complete counterexample).

• It is PSPACE-hard to decide whether an *ACTL* formula ϕ in case of failure always admits a deterministic counterexample (Theorem 4.1). This means that there exists no simple characterization of the *ACTL* formulas that guarantee deterministic counterexamples.

• Consequently, we study *templates* of *ACTL* formulas, i.e., skeletons of modal formulas whose atoms are disregarded and replaced by the symbol $\star$. As main result of this paper, we identify the (unique) maximal set $\mathbf{DET}$ of templates whose instances, obtained by replacing $\star$'s with arbitrary pure state formulas, always guarantee deterministic counterexamples (Theorem 4.3). The set $\mathbf{DET}$ of templates is given by the BNF grammar in Table 1. For example, the templates $\mathbf{AX}(\star)$, $\mathbf{A}(\star\mathbf{V}\mathbf{AX}(\star)))$, and $(\star \wedge \mathbf{A}(\star\mathbf{V}\mathbf{AX}(\star)))$ are in

$\mathbf{DET}$, as well as $\mathbf{A}(\star\mathbf{U}\star)$, $\mathbf{A}(\star\mathbf{U}\mathbf{A}(\star\mathbf{U}\star))$, $\mathbf{A}(\mathbf{A}(\star\mathbf{V}\mathbf{A}\mathbf{X}(\star))\mathbf{U}(\star\wedge\star))$. On the other hand, the template $\mathbf{A}(\star\mathbf{U}\mathbf{A}(\star\mathbf{V}\star))$ of the formula $\phi = \mathbf{A}(\mathit{true}\mathbf{U}\mathbf{A}(\mathit{false}\mathbf{V}a))$ in Example 1.2 is not in $\mathbf{DET}$, and also the template $\mathbf{A}(\mathit{true}\mathbf{U}\mathbf{A}(\mathit{false}\mathbf{V}\star))$ of the formula $\mathbf{A}(\mathit{true}\mathbf{U}a_1) \vee \mathbf{A}(\mathit{true}\mathbf{U}a_2) = \mathbf{AF}a_1 \vee \mathbf{AF}a_2$ mentioned above is not in $\mathbf{DET}$.

Obviously, it is recognizable in polynomial time (and in fact in linear time) whether a template belongs to $\mathbf{DET}$, and whether an *ACTL* formula ϕ is an instance of some template in $\mathbf{DET}$. In particular, we prove:

* If ϕ is an instance of a template $\gamma^\star \in \mathbf{DET}$, then, for each structure M such that $M \not\models \phi$, there exists a deterministic counterexample, and thus a counterpath in M witnessing this failure.

* If $\gamma^\star$ is a template not contained in $\mathbf{DET}$, then there exist an instance ϕ of $\phi*$ and a structure M such that $M \not\models \phi$ but there exist no deterministic counterexample for ϕ in M.

• We show that for each *ACTL* formula ϕ which is an instance of a template $\gamma^\star \in \mathbf{DET}$, and for each Kripke structure M such that $M \not\models \phi$, a counterpath, i.e., a single path of M witnessing the failure, can be computed in polynomial time.

1.5 Structure of the paper

After this introduction, some preliminaries and notation are given in Section 2. In Section— 3, the formal definition of counterexamples is provided, for which multi-paths are introduced. Thereafter, we turn our attention in Section 4 to deterministic counterexamples and multi-paths. After proving that recognizing deterministic *ACTL* formulas is intractable, we define the class $\mathbf{DET}$ of templates; furthermore, we formally state the characterization of c-deterministic templates, which is the first main result of this paper. Sections 5–6 are devoted to the proof of this result and to the computation of counterpaths for $\mathbf{DET}$-instances, which is the second main result. The paper is closed in Section 7 with a discussion and an outlook on future work.

2 Preliminaries

Definition 2.1 (*ACTL* formulas) Let A be a set of atomic propositions. Then, *ACTL* is the set of *state formulas on A* inductively defined as follows:

(1) Any Boolean formula over atoms from AP built using the connectives $\wedge, \vee$, and $\neg$ is a *pure state formula*.

(2) if ϕ and ψ are state formulas, then $(\phi \vee \psi)$, and $(\phi \wedge \psi)$ are *state formulas*;

(3) if ϕ and ψ are state formulas, then $\mathbf{X}\phi$, $\phi\mathbf{U}\psi$ and $\phi\mathbf{V}\psi$ are *path formulas*;

(4) if ϕ is a path formula, then $\mathbf{A}(\phi)$ is a state formula. □

Intuitively, path formulas describe properties of evolution series because they use temporal operators next time, until, and unless.

Notation. For any sets D_1 and D_2 of formulas, we shall use the following notation:

$$\begin{aligned} \mathbf{AX}(D_1) &= \{\mathbf{AX}(\gamma) \mid \gamma \in D_1\}, \\ \mathbf{AU}(D_1, D_2) &= \{\mathbf{A}(\gamma_1\mathbf{U}\gamma_2) \mid \gamma_1 \in D_1, \gamma_2 \in D_2\}, \end{aligned}$$

$$\begin{aligned} \mathbf{AV}(D_1, D_2) &= \{\mathbf{A}(\gamma_1 \mathbf{V} \gamma_2) \mid \gamma_1 \in D_1, \gamma_2 \in D_2\}, \\ D_1 \wedge D_2 &= \{(\gamma_1 \wedge \gamma_2) \mid \gamma_1 \in D_1, \gamma_2 \in D_2\}, \\ D_1 \vee D_2 &= \{(\gamma_1 \vee \gamma_2) \mid \gamma_1 \in D_1, \gamma_2 \in D_2\}. \end{aligned}$$

Given a formula ϕ or a set of formulas S, we will denote by $AP(\phi)$ (resp., $AP(S)$) the set of atomic propositions occurring in ϕ (resp., S). We will use *true* and *false* as shorthand for pure state formulas which are tautologies and contradictions, respectively. We shall omit or add parentheses in formulas following the usual conventions.

The formal definition of the semantics of *ACTL* refers to particular *Kripke structures*. Informally, they are labeled finite transition graphs.

Definition 2.2 (Kripke Structure) A *Kripke structure* is a quintuple $M = (A, S_0, S, R, L)$ such that:

- A is a finite set of atomic propositions, denoted $A(M)$;
- S is a finite set of states, denoted $S(M)$;
- $S_0 \subseteq S$ is a finite set of initial states, denoted $S_0(M)$;
- $R \subseteq S \times S$ is a transition relation, denoted $R(M)$;
- $L : S \to 2^A$ is a mapping assigning each state of S the set of atomic propositions true in that state; L is called *label function*, and is denoted by $L(M)$. □

For convenience, we often denote by M_s the Kripke structure which is identical to M except $S_0(M_s) = \{s\}$ where $s \in S(M)$, i.e., s is the unique initial state. Furthermore, we will sometimes focus on structures M such that $S_0(M) = \{s_0\}$ and $(s, s_0) \notin R(M)$, for all $s \in S(M)$, i.e., M has a unique initial state s_0, and s_0 is not reachable from any state in M. We refer to such structures as *conic*.

The dynamic temporal evolution is modeled by infinite paths in the Kripke structure.

Definition 2.3 (path) A *path* π of a Kripke structure M is an infinite sequence $\pi = [s_0, s_1, \cdots, s_i, \cdots]$ such that for each $i \geq 0$ $(s_i, s_{i+1}) \in R$. Given an integer $i \geq 0$ and a path π we denote by $\pi(i)$ the i-th state of π. Given an integer $j \geq 0$ and a path π, the j-suffix π^j of π is the path $[\pi(j), \pi(j+1), \cdots]$. Clearly, $\pi = \pi^0$ and $\pi(i) = \pi^i(0)$. □

The semantics of *ACTL* is now defined through an entailment relation $\models$, which can be applied on states s and paths π for evaluating state and path formulas, respectively.

Definition 2.4 (satisfaction) Let s and π be a generic state and path in M, respectively. Then, the satisfaction relation $\models$ for state and path formulas, respectively, on a Kripke structure M is inductively defined as follows.

1. $M, s \models p$, if $p \in L(M)(s)$, for any atomic proposition $p \in A$;
2. $M, s \models \neg\phi$, if $M, s \not\models \phi$, where ϕ is a state formula;
3. $M, s \models \phi_1 \vee \phi_2$, if $M, s \models \phi_1$ or $M, s \models \phi_2$, where ϕ_1 and ϕ_2 are state formulas;
4. $M, s \models \phi_1 \wedge \phi_2$, if $M, s \models \phi_1$ and $M, s \models \phi_2$, where ϕ_1, ϕ_2 are state formulas;

5. $M, s \models \mathbf{A}(\psi)$, if $M, \pi \models \psi$ for all paths π such that $\pi(0) = s$;

6. $M, \pi \models \mathbf{X}\phi$, if $M, \pi(1) \models \phi$;

7. $M, \pi \models \phi_1 \mathbf{U} \phi_2$, if there exists an integer $k \geq 0$ such that $M, \pi(k) \models \phi_2$ and $M, \pi(j) \models \phi_1$, for all $0 \leq j < k$;

8. $M, \pi \models \phi_1 \mathbf{V} \phi_2$, if for every $k \geq 0$, $M, \pi(j) \not\models \phi_1$ for all $0 \leq j < k$ implies $M, \pi(k) \models \phi_2$

We write $M \models \phi$ if $M, s_0 \models \phi$, for every initial state $s_0 \in S_0(M)$, □

Intuitively, a state formula holds along a path, if it is true at its first state; $\phi_1 \mathbf{U} \phi_2$ is true, if ϕ_1 is true along the path until some state is reached at which ϕ_2 is true; and $\phi_1 \mathbf{V} \phi_2$ is true, if there is no stage such that ϕ_2 is false and ϕ_1 is false at all previous previous states. Note that $\mathbf{U}$ and $\mathbf{V}$ are dual operators: $\phi_1 \mathbf{U} \phi_2$ is true precisely if $\neg\phi_1 \mathbf{V} \neg\phi_2$ is false.

3 Multi-Paths and Counterexamples

If an *ACTL* formula ϕ is not true in a structure M, then there must be some evidence which proves the failure of the formula. For a pure state formula ϕ, an initial state s_0 at which ϕ is false is a witness of this fact; if ϕ is of the form $\mathbf{AX}\psi$, where ψ is a pure state formula,then a path π starting at some $s_0 \in S_0$ such that ψ is false at $\pi(1)$ is such a witness. The falsity of formulas $\mathbf{A}(\phi_1 \mathbf{U} \phi_2)$, $\mathbf{A}(\phi_1 \mathbf{V} \phi_2)$ where the ϕ_i are pure state formulas is witnessed similarly by a path π.

Intuitively, a path π as described is a *counterexample* for the truth of ϕ in M. It appears that for more complex formulas ϕ which involve nested $\mathbf{A}$ quantifiers, a single path π may not be by itself witness that ϕ fails in M. To formally capture this, nesting of paths must be taken into account. This motivates the definition of multi-paths, which serve as a basis for a formal definition of counterexamples [1].

3.1 Multi-Paths

Informally, a multi-path represents an infinite tree T, which has a designated branch as a backbone (called *main path*). The branches of the tree which spring off from the main path at a certain stage are collected in a tree, which is recursively represented as a multi-path. Thus, multi-paths can be inductively defined. Observe that this representation of a tree is different from the usual inductive definition in which a tree is built by assigning child nodes to a parent node. The main advantage of the multi-path concept is the preservation of the nesting of paths, which is lost in the standard tree definition.

Preliminary to the formal definition of multi-paths, we introduce multi-sequences.

Definition 3.1 (multi-sequence) Let S be a set of states. Then,

- for every state $s \in S$, $\Pi = s$ is a finite multi-sequence in S;
- if $\Pi_0, \Pi_1, \ldots$ are countably infinite many multi-sequences in S, then $\Pi = [\Pi_0, \Pi_1, \ldots]$ is a multi-sequence in S.

For any multi-sequence Π, its i-th element is denoted by $\Pi(i)$, for all $i \geq 0$; moreover, its *origin*, denoted $or(\Pi)$, is $or(\Pi) = s$, if $\Pi = s$ is a single state, and $or(\Pi) = or(\Pi(0))$, otherwise. □

Next we introduce the notion of *main sequence* of a multi-sequence. Informally, it is the sequence formed by the origins of all elements in a multi-sequence.

Definition 3.2 (main-sequence) Given a multi-sequence Π, the *main sequence of* Π, denoted by $\mu(\Pi)$, is

- s, if $\Pi = s$ is finite;
- the sequence $[or(\Pi(0)), or(\Pi(1)), or(\Pi(2)), \ldots]$, otherwise. □

Multi-paths are multi-sequences which model nested paths in M.

Definition 3.3 (multi-path) A multi-sequence Π is a *multi-path* in M, if either Π is finite, or $\mu(\Pi)$ is a path in M and for every $i \geq 0$, $\Pi(i)$ is a multi-path in M.

The main sequence of a multi-path Π is called the *main path* of Π. □

Note that multi-paths generalize paths. Indeed, a path can be seen as an infinite multi-path Π such that each element $\Pi(i)$ is a state.

An infinite multi-path Π represents intuitively an evolving computing tree, whose branches are the main path $\mu(\Pi)$ and all paths of form $\pi_0\pi_1$ where $\pi_0 = \mu(\Pi)(0), \ldots, \mu(\Pi)(i-1)$ is a finite prefix of $\mu(\Pi)$ and π_1 is a branch of the multi-path $\Pi(i)$, where $\Pi(i)$ must be infinite.

Example 3.1 Assuming proper M, the multi-sequence $\Pi = [[s_0, s_1, s_1, \ldots], s_2, s_2, \ldots]$ is a multi-path, which represents two paths $\pi_1 = [s_0, s_1, s_1, \ldots]$ and $\pi_2 = [s_0, s_2, s_2, \ldots]$ starting at s_0 (Figure 3). π_2 is the main path $\mu(\Pi)$ of Π. The multi-path $\Pi = [[s_0, s_1, s_1, \ldots], s_2, [s_0, s_1, s_1, \ldots], s_2, [s_0, s_1, s_1, \ldots], \ldots]$ has main path $\mu(\Pi) = [s_0, s_2, s_0, s_2, \ldots]$ and represents the computation tree in which from $\mu(\Pi)$ at every even stage $\mu(\Pi)(2k)$ a path $[s_0, s_1, s_1, \ldots]$ branches off; hence, Π contains besides $\mu(\Pi)$ all paths of form $[(s_0, s_2)^i, s_0, s_1, s_1, \ldots]$, $i \geq 0$. □

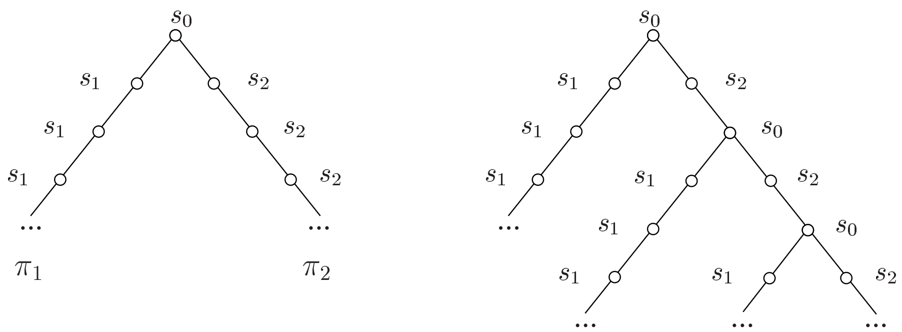

Figure 3: Branching paths

An important note is that in general, a multi-path Π may not directly reflect in its structure a truly branching computation tree. In fact, the definition allows fake branching, in the sense that two nested branching paths may amount to the same path in the structure. For example, in the multi-path $\Pi = [s_0, s_1, [s_2, s_3, s_4, \ldots]s_3, s_4, \ldots]$, the branch $s_2, s_3, s_4, \ldots$ is identical to the remainder of the main path $s_2, s_3, s_4, \ldots$. This is not a shortcoming of our definition, but an important feature; it allows to express that a particular path is a subpath of another one. In an extended vocabulary for multi-paths, this could be expressed more elegantly; however, we disregard such an extension here. Note that for our purposes, we can restrict to multi-paths which have effective finite representations [1].

3.2 Counterexamples

We are now prepared to formalize the notion of counterexample. Intuitively, a counterexample for a formula ϕ is a special multi-path Π originating at an initial state demonstrating the falsity of ϕ. Since counterexamples are defined inductively, we need the concept of a local counterexample, which may origin at an arbitrary state rather than an initial state. For the technical definition of local counterexamples, we use an operation for merging two multi-paths into a single one.

Definition 3.4 (merge) Let Π_1 and Π_2 be two multi-paths such that $or(\Pi_1) = or(\Pi_2)$. The *merge* of Π_1 and Π_2, denoted by $\Pi_1 * \Pi_2$, is the multi-path recursively defined as follows:

$$\Pi_1 * \Pi_2 = \begin{cases} \Pi_1, & \text{if } \Pi_2 \text{ is finite;} \\ [\Pi_1, \Pi_2(1), \Pi_2(2), \ldots], & \text{if } \Pi_2 \text{ is infinite and } \Pi_2(0) \text{ is finite;} \\ [\Pi_1 * \Pi_2(0), \Pi_2(1), \Pi_2(2), \ldots], & \text{otherwise.} \end{cases} \qquad \Box$$

Intuitively, the trees represented by Π_1 and Π_2 are merged at their common root.

Example 3.2 Merging $\Pi = [[s_0, s_{1_1}, s_{1_2}, \ldots], s_{2_1}, s_{2_3}, \ldots]$ and $\Pi' = [s_0, s_{3_1}, s_{3_2}, \ldots]$ yields

$$\begin{aligned} \Pi * \Pi' &= [\Pi, s_{3_1}, s_{3_2}, \ldots] = [[[s_0, s_{1_1}, s_{1_2}, \ldots], s_{2_1}, s_{2_2}, \ldots], s_{3_1}, s_{3_2}, \ldots], \quad \text{while} \\ \Pi' * \Pi &= [\Pi' * [s_0, s_{1_1}, s_{1_2}, \ldots], s_{2_1}, s_{2_2}, \ldots] \\ &= [[\Pi', s_{1_1}, s_{1_2}, \ldots], s_{2_1}, s_{2_2}, \ldots] \\ &= [[[s_0, s_{3_1}, s_{3_2}, \ldots], s_{1_1}, s_{1_2}, \ldots], s_{2_1}, s_{2_2}, \ldots]. \end{aligned}$$

The two merges essentially represent the same branching of three paths $\pi_i = [s_0, s_{i_1}, s_{i_2}, \ldots]$ for $i \in \{1, 2, 3\}$, starting from s_0. $\Box$

Note that merging Π_1 and Π_2 by adding Π_1 as first element to Π_2 does not work, since in general, this leads to a set of paths different from those in Π_1 and Π_2; the result may even not be a multi-path.

Definition 3.5 (l-counterexample) Let M be a Kripke structure and ϕ be an *ACTL* formula on $A(M)$. A multi-path Π in M is a *local (l-) counterexample for* ϕ if, depending on the structure of ϕ, the following holds:

- if ϕ is a pure state formula: $\Pi = s$ is a state and $M, s \not\models \phi$;
- otherwise, if
  1. $\phi = \mathbf{A}(\phi_1 \mathbf{U} \phi_2)$: Π is an infinite multi-path and either
     - 1.1 there exists $k \geq 0$ such that $\Pi(k)$ is an l-counterexample for $\phi_1 \vee \phi_2$, $\Pi(i)$ is an l-counterexample for ϕ_2, for each $0 \leq i \leq k$, and $\Pi(j)$ is a state, for $j > k$; or
     - 1.2 $\Pi(i)$ is a l-counterexample for ϕ_2, for each $i \geq 0$;
  2. $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$: Π is an infinite multi-path and there exists a k such that every $\Pi(j)$, $0 \leq j < k$, is an l-counterexample for ϕ_1, $\Pi(k)$ is an l-counterexample for ϕ_2, and every $\Pi(\ell)$ is a state, for $\ell > k$;
  3. $\phi = \mathbf{AX}\phi_1$: Π is an infinite multi-path, $\Pi(1)$ is an l-counterexample for ϕ_1, and $\Pi(i)$ is a state, for each $i \neq 1$;

4. $\phi = \phi_1 \vee \phi_2$: $\Pi = \Pi_1 * \Pi_2$, where Π_i, $i = 1, 2$, is an l-counterexample for ϕ_i;
5. $\phi = \phi_1 \wedge \phi_2$: Π is an l-counterexample for either ϕ_1 or ϕ_2. $\Box$

Recall that $M \not\models \phi$ if there exists an initial state s_0 at which ϕ is false. Hence, we introduce a notion of "global" counterexample.

Definition 3.6 (counterexample) Let M be a Kripke structure and ϕ be a formula on $A(M)$. Any l-counterexample Π for ϕ in M such that $\mathit{or}(\Pi) \in S_0(M)$ is called a *counterexample for ϕ in M*. $\Box$

Example 1.1 illustrates this definition. Let us consider some more examples.

Example 3.3 Reconsider the Kripke structure M from Figure 1, and let $\psi = \mathbf{A}(\mathit{false}\mathbf{V}\mathbf{A}(\mathit{true}\mathbf{U}a_1))$. Also this formula is false on M. Intuitively, this is witnessed by path π again. However, from the formal definition, π is not a counterexample of ψ, as it does not respect witness paths for the subformula $\mathbf{A}(\mathit{true}\mathbf{U}a_1)$ of ψ. The multi-path $\Pi = [[s_0, s_1, \ldots], s_1, s_1, \ldots]$ is a proper counterexample for ψ according to the definition, as well as any multi-path $[s_0, (s_1,)^i, [s_1, s_1, \ldots], s_1, s_1, \ldots]$, where $i \geq 0$.

Finally, also the formula $\rho = \mathbf{A}(\mathit{true}\mathbf{U}\mathbf{A}(\mathit{false}\mathbf{V}a_1))$ is false in M; again, intuitively the path $\pi = [s_0, s_1, s_1, \ldots]$ shows this. Formally, the multi-path $[[s_0, s_1, s_1, \ldots], [s_1, s_1, \ldots], [s_1, s_1, \ldots], \ldots]$ is a counterexample for ρ; in fact, it is the unique counterexample. $\Box$

The following result states that l-counterexamples appropriately model the failure of a formula in a state.

Theorem 3.1 ([1]) *Let M be a Kripke structure, ϕ a formula on $A(M)$, and $s \in S(M)$. Then, $M, s \not\models \phi$ if and only if there exists an l-counterexample Π for ϕ such that $\mathit{or}(\Pi) = s$.*

Corollary 3.2 ([1]) *For any Kripke structure M and formula ϕ on $A(M)$, $M \not\models \phi$ if and only if there exists at a counterexample Π for ϕ in M.*

As discussed earlier, in many cases a counterexample for a formula is (essentially) a single path. This is true e.g. for the formulas considered in the Examples 1.1 and 3.3. However, as Example 1.2 and the following example show, there are different cases in which a truly branching tree is needed.

Example 3.4 Consider the structure M as in Figure 1 again, but now the formula $\phi = \mathbf{A}(\mathit{true}\mathbf{U}a_1) \vee \mathbf{A}(\mathit{true}\mathbf{U}a_2)$. Clearly, $M \not\models \phi$: For every a_i, $i = 1, 2$, there is an infinite path $\pi_i = s_0, s_i, s_i, \ldots$ which never reaches a state at which a_i is true; hence, every disjunct $\mathbf{AF}a_i$ in ϕ is false. A counterexample for ϕ is the multi-path $\Pi = [[s_0, s_1, s_1, \ldots], s_2, s_2, \ldots]$, which results by merging the π_i's into $\Pi = (\pi_1 * \pi_2)$. Notice that no counterexample for ϕ exists that is an ordinary path, and that $\pi_1 * \pi_2$, $\pi_2 * \pi_1$ are the only (isomorphic) counterexamples for ϕ. $\Box$

4 Deterministic Counterexamples

In this section, we formalize our intuition of a single path counterexample from the previous section. For this purpose, we introduce first the concept of a deterministic multi-path. Such a path is built over a single path in the structure, which exactly prescribes the next state in each transition throughout the multi-path.

4.1 Deterministic counterexamples and c-deterministic formulas

Definition 4.1 (deterministic multi-path) A multi-path Π is *deterministic*, if one of the following applies:

1. Π is finite (i.e., a single state);
2. Π is a path; or
3. for each $i \geq 0$, either
   3.1 $\Pi(i)$ is a state, or
   3.2 $\mu(\Pi(i))$ coincides with $\mu(\Pi)^i$ (the i-suffix of $\mu(\Pi)$) and $\Pi(i)$ is deterministic. □

Informally, a multi-path is deterministic if the main paths of its elements are suffixes of its main path, and this is recursively true also for the multi-paths of the sequence. Thus, while in general, multi-paths represent evolutions with branching, deterministic multi-paths have only artificial branching, and represent essentially a single path.

Example 4.1 Consider the multi-path

$$\Pi = [s_0, s_1, s_2, s_3, [s_4, s_5, s_4, [s_5, s_4, s_5, s_4, ...]s_4, s_5, ...]s_5, s_4, s_5, s_4, ...].$$

As can be seen, this multi-path is deterministic. The path $[s_5, s_4, s_5, s_4, ...]$ nested into $\Pi(4)(3)$ represents a path branching from the main path of $\Pi(4)$. However, this path coincides with the suffix $\mu(\Pi(4))^3$ of the main path of $\Pi(4)$. Hence, it does not represent an alternative evolution. In this sense, a deterministic multi-path represents only deterministic evolutions.

Observe that the multi-path $\Pi' = [[s_0, s_1, s_2, s_3, s_2, s_3, ...], s_4, s_5, s_6, s_5, s_6, s_5, ...]$ is not deterministic. □

Definition 4.2 (deterministic counterexample and counterpath) A counterexample Π for an *ACTL* formula ϕ in a structure M is *deterministic*, if Π is a deterministic multi-path. The main path $\mu(\Pi)$ of any deterministic counterexample Π for ϕ in M is a *counterpath* for ϕ in M. □

As easily verified, the counterexamples for the formulas presented in Examples 1.1 and 3.3 are deterministic counterexamples, and the "intuitive" counterexamples there are the respective counterpaths.

As for counterexamples, it is of particular interest to have a deterministic counterexample at hand, since such a counterexample is in generally easier to understand than an arbitrary counterexample. Moreover, the description of such counterexamples can be simplified. Observe that McMillan's SMV procedure [10] returns a single path π rather than a counterexample as used here when an *ACTL* formula fails. This path plays a similar role as the main path of our notion of a counterexample Π. If Π and π grasp the same witness, then $\mu(\Pi)$ should coincide with π, and it contains in fact all relevant information which is needed for witnessing the failure of ϕ. From π, a counterexample respecting the (artificial) branching of paths as required from the structure of ϕ can be reconstructed.

We thus direct our attention to the existence of deterministic counterexamples.

Definition 4.3 (c-deterministic) An $ACTL$ formula ϕ is *c-deterministic*, if $M \not\models \phi$ implies that a deterministic counterexample for ϕ exists in M, for every Kripke structure M.

4.2 Complexity of recognizing c-deterministic formulas

Unfortunately, recognizing c-deterministic formulas is complex in general, which is expressed by the following result.

Theorem 4.1 *Deciding whether a given ACTL formula ϕ is c-deterministic is* PSPACE*-hard.*

Proof. This result is proved by a reduction from the unsatisfiability problem for *ACTL* formulas on structures M where $R(M)$ is *total*, i.e. $\forall s \exists s'.R(s, s')$ holds. This problem is PSPACE-complete by results of Vardi and Kupferman (see [9]).

Let ϕ be an arbitrary *ACTL*-formula, and let a be a fresh atom not occurring in ϕ. Let the formula ψ be defined as follows:

$$\psi = \mathbf{AX}a \vee \mathbf{AX}(\neg a \wedge \phi).$$

It holds that ψ is c-deterministic if and only if ϕ is unsatisfiable over structures M where $R(M)$ is total.

To prove this, suppose first that ϕ is unsatisfiable over all M where $R(M)$ is total. Let M be any structure (where $R(M)$ is not necessarily total) such that $M \not\models \psi$. This implies that $\mathbf{AX}a$ has a counterexample in M, which is a simple path π represented by a pair P, C where P is a path (prefix) and C a cycle in M. The assumption on ϕ implies that $\neg a \wedge \phi$ is globally false (and in particular, at $\pi(1)$) in the structure M_π which is naturally induced by π in M. Consequently, π is a counterpath for ψ in M_π, and thus also in M. This means that ψ is c-deterministic.

Now suppose that ϕ is satisfiable on some structure M with total $R(M)$. Hence, a state $s_0 \in S_0(M)$ exists such that $M, s_0 \models \phi$. Let M' be the structure corresponding to the labeled transition graph in Figure 4.

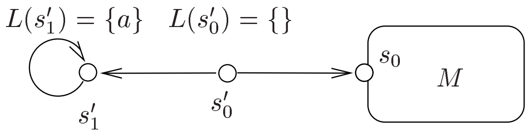

Figure 4: Structure M for $\psi = \mathbf{AX}a \vee \mathbf{AX}(\neg a \wedge \phi)$ (initial state s_0')

It holds that $M' \not\models \psi$. Indeed, the path $\pi_1 = [s_0', s_1, s_1, \ldots]$ is a counterpath for $\psi_1 = \mathbf{AX}a$, and any path $\pi_2 = [s_0', s_0, \ldots]$ is a counterpath for $\psi_2 = \mathbf{AX}(\neg a \wedge \phi)$; thus, their merge $\Pi = \pi_1 * \pi_2$ is a counterexample for ψ. Clearly, any counterexample for ψ in M' must contain both s_0 and s_1; thus, a deterministic counterexample for ψ in M' is impossible, which means that ψ is not c-deterministic. □

This result implies that a polynomial-sized and polynomial-time checkable proof witnessing that a formula is c-deterministic is illusive, and thus we may abandon the search for an appealing syntactical characterization of c-deterministic formulas.

A related, in practice perhaps more important issue is whether the existence of a deterministic counterexample for a formula can be efficiently decided *ad hoc*, i.e., given an *ACTL* formula ϕ and a structure M, decide whether ϕ has a deterministic counterexample in M (and, if so, return a counterpath represented in a suitable way). As it turns out, also this problem is intractable.

Theorem 4.2 *Given a Kripke structure M and an ACTL-formula ϕ, deciding whether ϕ has a deterministic counterexample (equivalently, a counterpath) in M is* NP*-hard.*

Proof. We describe a polynomial-time transformation of deciding whether a given directed graph $G = (V, E)$ has a Hamiltonian circuit, which is well-known NP-complete [8], into this problem. Recall that a Hamiltonian circuit is a sequence $C = v_{i_1}, \ldots, v_{i_n}$ of all the vertices $V = \{v_1, \ldots, v_n\}$ such that an edge is directed from v_{i_j} to $v_{i_{j+1}}$ and from v_{i_n} to v_{i_1}.

We construct M and ϕ as follows. The set S of states of M is V, which is also the set A of atomic propositions and the set S_0 of initial states. The transition relation R is E, and each $v \in V$ has the label $L(v) = \{v\}$.

The formula ϕ is as follows:

$$\phi = \mathbf{A}\Big(\mathit{true}\mathbf{U}\Big(\bigvee_{v\in V}\Big(v \wedge \bigvee_{w\in V\setminus\{v\}} \mathbf{AXA}(v\mathbf{V}\neg w)\Big)\Big)\Big)$$

Intuitively, a deterministic counterexample for ϕ in M is an infinite path π such that in each state $\pi(i) = v$, the path must be continued in states $\pi(i+1), \pi(i+2), \ldots$, such that all other vertices $w \neq v$ appear before v may reappear.

We claim that G has a Hamiltonian circuit if and only if ϕ has a counterpath in M.

($\Rightarrow$) Let $C = v_{i_1}, \ldots, v_{i_n}$ be a Hamiltonian circuit of G. We claim that the path $\pi = (v_{i_1}, v_{i_2}, \ldots, v_{i_n},)^\infty$ is a counterpath of ϕ. To verify this, we have to show that the formula

$$\bigvee_{v\in V} \psi_v, \qquad \text{where} \qquad \psi_v = v \wedge \Big(\bigvee_{w\in V\setminus\{v\}} \mathbf{AXA}(v\mathbf{V}\neg w)\Big)$$

is false in each state $\pi(i)$, $i \geq 0$, and that a local counterexample witnessing this fact can be built over π^i.

For each $v \in V$ such that $v \neq \pi(i)$, v is false at $\pi(i)$ and thus $\pi(i)$ is a local counterexample for ψ_v over π^i. For the $v \in V$ such that $v = \pi(i)$, we must show that for each $w \in V \setminus \{v\}$, the suffix π^i is a local counterpath of the formula $\mathbf{AXA}(v\mathbf{V}\neg w)$; that is, that the suffix π^{i+1} is a local counterexample of $\mathbf{A}(v\mathbf{V}\neg w)$. Clearly, this is true for the $w \in V \setminus \{v\}$ such that $w = \pi(i+1)$; any $w' \in V \setminus \{v, w\}$ occurs as $\pi(i+k)$, where $1 < k < n$, and v is false at $\pi(i+k-1)$; thus, π^{i+1} is a local counterexample for $\mathbf{A}(v\mathbf{V}\neg w)$. This proves that $\bigvee_{v\in V} \psi_v$ is false in $\pi(i)$, and that π^i is a local counterpath for each $\mathbf{AXA}(v\mathbf{V}\neg w)$ where $w \in V \setminus \{v\}$. Thus, π is a counterpath for ϕ in M.

($\Leftarrow$) Suppose that ϕ has a counterpath π in M. We show that the prefix $\pi(0),\ldots,\pi(n-1)$ of π is a Hamiltonian circuit of G. Let $v \in V$ be the node such that $\pi(0) = v$. Then, π is a counterpath for the formula ψ_v from above. This implies that π is a counterpath for the formula $\mathbf{AXA}(v\mathbf{V}\neg w)$, for each $w \in V \setminus \{v\}$. Thus, π^1 is a local counterpath for $\mathbf{A}(v\mathbf{V}\neg w)$. Hence, w must occur in π, and v must be false in each state $\pi(i)$ where $1 \leq i < k_w$ and $\pi(k_w)$ is the first occurrence of w in π. Consequently, $\pi(n)$ is the first possible position for a second occurrence of v in π.

Now consider $v^{(i)} = \pi(i)$, where $i > 0$. By similar arguments, we obtain that each $w \in V \setminus \{v^{(i)}\}$ occurs in π^i, and that w must occur in π^i before any possible further occurrence of $v^{(i)}$ after $\pi^i(0) = \pi(i)$. It follows that $\pi(0)$, $\pi(1)$,$\ldots$,$\pi(n-1)$ are all pairwise different, and that $\pi(n) = \pi(0)$ holds. This means that $\pi(0),\ldots,\pi(n-1)$ is a Hamiltonian circuit in G, and completes the proof of the claim.

Since M and π are constructible in polynomial time from G, the result is proved. □

4.3 *ACTL* templates

In the light of the previous results, we look into *structural properties* of formulas which guarantee the existence of a deterministic counterexample whenever a formula does not hold in a structure. This leads us to consider *templates* of *ACTL* formulas – formulas, in which the particular atomic propositions are meaningless, i.e., they can be substituted by arbitrary pure state formulas. Intuitively, a template expresses the structure of a formula in terms of linear-time and branching time operators. A pure state formula always has a deterministic counterexample (given by a single state); however, the application of these operators and Boolean connectives might destroy this property.

In the following, we shall identify the class of templates which are deterministic, i.e., each instantiation γ of a template $\gamma^\star$ obtained by filling in pure state formulas, has always a deterministic counterexample if γ is not true. As it turns out, this class is decidable, and in fact efficiently recognizable.

More formally, templates are defined as follows.

Definition 4.4 (template) A *template* $\gamma^\star$ is an $ACTL$ formula over "$\star$" as single atomic proposition. The template of an *ACTL* formula γ, denoted $\gamma^\star$, is the template obtained by uniformly substituting "$\star$" for all atomic propositions in γ.[1]

Observe that for any *ACTL* formula γ, its template $\gamma^\star$ is unique. As with ordinary formulas, we shall often omit or introduce parentheses as usual.

Example 4.2 The template of $\gamma = \mathbf{A}(a\mathbf{VAX}(b \wedge c))$ is $\gamma^\star = \mathbf{A}(\star\mathbf{VAX}(\star \wedge \star))$, and the template of $\phi = \mathbf{A}((b \vee \neg c)\,\mathbf{U}\,a) \wedge \mathbf{AX}(c \wedge a))$ is $\phi^\star = \mathbf{A}((\star \vee \neg\star)\mathbf{U}\star) \wedge \mathbf{AX}(\star \wedge \star))$. □

Definition 4.5 ($\mathbf{T}^\star$,$\mathcal{PSF}$) We denote by $\mathbf{T}^\star$ we denote the set of all $ACTL$ templates and by $\mathcal{PSF} \subseteq \mathbf{T}^\star$ the set of pure state formulas on the atomic proposition $\star$.

We next define a subset $\mathbf{DET} \subseteq \mathbf{T}^\star$ of templates in terms of the least fixpoint of a continuous operator which is applied to a pair of sets of templates. The main effort in the rest of the paper will be the proof that this set $\mathbf{DET}$ is precisely the set of all deterministic templates.

Definition 4.6 (operator Λ) The operator $\Lambda : 2^{\mathbf{T}^\star} \times 2^{\mathbf{T}^\star} \to 2^{\mathbf{T}^\star} \times 2^{\mathbf{T}^\star}$ is defined as follows:

$$\Lambda(S_1, S_2) = (S_1', S_2'),$$

where

$$\begin{aligned} S_1' &= \mathcal{PSF} \cup S_1{\wedge}S_1 \cup S_1{\vee}\mathcal{PSF} \cup \mathcal{PSF}{\vee}S_1 \cup \mathbf{AX}(S_1) \cup \mathbf{AV}(\mathcal{PSF}, S_1) \cup S_2 \\ S_2' &= \mathbf{AU}(S_1, \mathcal{PSF}) \cup \mathbf{AU}(\mathcal{PSF}, S_2) \cup S_2{\vee}\mathcal{PSF} \cup \mathcal{PSF}{\vee}S_2 \end{aligned}$$

Obviously, Λ is a continuous operator on a complete lattice, and hence by Kleene's Theorem, the least fixpoint $\Lambda^\infty = (S_1^\infty, S_2^\infty)$ exists and is the limit of the sequence $\Lambda^0 = (\emptyset, \emptyset)$, $\Lambda^{i+1} = \Lambda(\Lambda^i)$, $i \geq 0$.

Definition 4.7 ($\mathbf{DET}$) We define $\mathbf{DET} = S_1^\infty$ as the first component of the least fixpoint $\Lambda^\infty = (S_1^\infty, S_2^\infty)$ of Λ.

Example 4.3 As easily checked, the sample templates in Section 1 generated by the grammar in Table 1 are in $\mathbf{DET}$. In fact, it is easy to see that $\mathbf{DET}$ coincides with the language generated by that grammar. Further templates belonging to $\mathbf{DET}$ are: $\mathbf{AXAX}\star$, $\mathbf{AXA}(\star\mathbf{U}(\star \vee \neg\star))$, $\mathbf{A}(\mathbf{AX}\star\mathbf{U}(\star \wedge \star))$, $\mathbf{A}(\neg(\star \vee \star)\mathbf{VAX}\star)$, $\mathbf{A}(\star\mathbf{V}(\neg\star \vee \mathbf{A}(\star\mathbf{U}\star)))$, $\mathbf{A}(\mathbf{A}(\star\mathbf{U}\star)\mathbf{U}\star)$. On the other hand, the templates $\mathbf{A}(\mathbf{AX}(\star)\mathbf{V}\star)$ and $\mathbf{A}(\star\mathbf{U}(\star \wedge \mathbf{AX}(\star)))$ are not in $\mathbf{DET}$.

[1] Alternatively, we could define that maximal pure state formulas in γ are replaced by $\star$, rather than atoms. However, the definition of $\mathbf{DET}$ and the BNF grammar in Table 1 would become more complex, while the main results are not affected.

Instantiations of templates are defined as follows.

Definition 4.8 (instantiation) *An ACTL formula ϕ over atoms AP, where $\star \notin AP$, is an* instantiation *of a template $\gamma^\star \in \mathbf{T}^\star$, if ϕ results by substituting each occurrence of $\star$ in $\gamma^\star$ with a (possibly different) pure state formula over AP.*

Example 4.4 An instantiation of $\mathbf{A}(\star\mathbf{V}(\neg\star\vee\mathbf{A}(\star\mathbf{U}\star))$ is $\mathbf{A}(\mathit{false}\mathbf{V}(\neg\mathit{req}\vee\mathbf{A}(\mathit{true}\mathbf{U}\mathit{ack})))$, which expresses that a request is always finally acknowledged (see [5] for this formula). Instantiations of $\mathbf{A}((\star\vee\neg\star)\mathbf{U}\star)\wedge\mathbf{AX}(\star\wedge\star))$ are $\mathbf{A}((b\vee\neg c)\,\mathbf{U}\,(b\wedge a))\wedge\mathbf{AX}(c\wedge a))$ and $\mathbf{A}((a\vee\neg a)\,\mathbf{U}\,a)\wedge\mathbf{AX}(a\wedge\neg a))$, i.e., $\mathbf{A}(\mathit{true}\,\mathbf{U}\,a)\wedge\mathbf{AX}(\mathit{false}))$.

To formulate our main result, we formally define the notion of deterministic template as follows.

Definition 4.9 (c-deterministic template) An $ACTL$ formula ϕ is *c-deterministic*, if $M\not\models\phi$ implies that a deterministic counterexample for ϕ exists in M, for every Kripke structure M. A template $\gamma^\star$ is *c-deterministic*, if each instantiation ϕ of $\gamma^\star$ is c-deterministic.

The first of the main results of this paper can now be stated as follows.

Theorem 4.3 *Let $\gamma^\star\in\mathbf{T}^\star$. Then, $\gamma^\star$ is c-deterministic if and only if $\gamma^\star\in\mathbf{DET}$.*

From this result and the inductive definition of $\mathbf{DET}$, we easily obtain the following corollary concerning the recognition of deterministic templates; observe that membership of a template in $\mathbf{DET}$ can be checked in a single bottom up pass of the formula tree, in which each step is unambiguous.

Corollary 4.4 *Given a template $\gamma^\star\in\mathbf{T}^\star$, deciding whether $\gamma^\star$ is c-deterministic is possible in $O(|\gamma^\star|)$ time, where $|\gamma^\star|$ is the length of $\gamma^\star$.*

The proof of Theorem 4.3 is rather technical, and involves detailed case studies. It is given in Sections 5 (if-part) and 6 (only-if part).

5 Templates in DET are c-deterministic

In this section, we prove that all instances of templates in $\mathbf{DET}$ are c-deterministic. The proof proceeds along the inductive definition of $\mathbf{DET}$. However, it appears that the property of c-determinism is not strong enough to allow the induction step go through smoothly for all templates. We can remedy this problem by revealing that a strengthened version of c-determinism is satisfied by some of the templates, which has the benign property of being establishable in the induction step comparatively easy. We start with some useful definitions.

Definition 5.1 (strongly c-deterministic) An $ACTL$ formula ϕ is *strongly c-deterministic*, if ϕ is c-deterministic and the following two conditions hold for any Kripke structure M:

1. if Π is a deterministic l-counterexample Π for ϕ in M, then every path π of form $\pi=s_0,\ldots,s_k,\mu(\Pi)$ in M such that $s_0\in S_0(M)$ and ϕ has l-counterexamples at $s_0,\ldots,s_k$ is a counterpath of ϕ; and
2. if π is a path in M such that $\pi(0)\in S_0(M)$ and every $\pi(i)$, $i\geq 0$, is the origin of some l-counterexample for ϕ in M, then π is a counterpath for ϕ in M.

A template $\gamma^\star$ is *strongly c-deterministic*, if every instantiation ϕ of $\gamma^\star$ is strongly c-deterministic.

Example 5.1 The formula $\phi = \mathbf{A}(a\mathbf{U}b)$ is strongly c-deterministic: a local counterexample Π for ϕ is a path π, and at the state $\pi(0)$, the atom b is false. By adding a prefix $s_0, \ldots, s_{k-1}$ of states to π such that b is false in each state s_i, we clearly obtain a path $\pi' = s_0, \ldots, s_{k-1}, \pi$ witnessing that $a\mathbf{U}b$ is false, i.e., π' is a counterpath for ϕ. Thus, item 1 of strong c-determinism is satisfied. Also item 2 is satisfied: b must be false at the origin of any local counterexample of ϕ; thus, if π is a path as described in item 2, b is false at each state $\pi(i)$. This means that π is a counterexample (and thus a counterpath) for ϕ.

It is easy to see that this holds if the atoms a and b are replaced by arbitrary pure state formulas; thus, the templates $\mathbf{A}(\star\mathbf{U}\star)$ and all templates in $\mathbf{AU}(\mathcal{PSF}, \mathcal{PSF})$ are strongly c-deterministic.

On the other hand, the formula $\phi = \mathbf{A}(a\mathbf{V}b)$, even if it is c-deterministic (as we shall see below), is not strongly c-deterministic, since it fails to satisfy item 2 of the definition. Indeed, consider a path π where each $\pi(i)$ is the origin of a local counterexample for ϕ, in which a is false and b is true. Then, b is true in each state of π. However, a counterexample for ϕ must involve a state at which b is false. Thus, π is not a counterpath for ϕ and item 2 fails. It is easy to see from this that no template in $\mathbf{AV}(\mathcal{PSF}, \mathcal{PSF})$ is strongly c-deterministic. Similarly, it is easy to see that $\mathbf{AX}a$ is not strongly c-deterministic (both item 1 and 2 may fail), and that no template in $\mathbf{AX}(\mathcal{PSF})$ is strongly c-deterministic.

As for more complex formulas, e.g., the templates $\mathbf{A}(\star\mathbf{U}(\star\mathbf{U}\star))$ and $\mathbf{A}(\star\mathbf{U}\star) \vee \star$ are strongly c-deterministic. This will be formally proven below. $\Box$

The next theorem shows that the templates in the class $\mathbf{DET}$ are sound with respect to the property of c-determinism, i.e., each template in this class is c-deterministic. In fact, in the proof of the result we establish a little more, namely that all templates in the subset $S_2^\infty \subseteq \mathbf{DET}$ are strongly c-deterministic.

Theorem 5.1 *Every template in* $\mathbf{DET}$ *is c-deterministic.*

Proof. We establish the result proving by induction on the stages $\Lambda^i = (S_1^i, S_2^i)$, $i \geq 0$, that every template $\gamma^\star \in S_1^i$ is c-deterministic and every template $\gamma^\star \in S_2^i$ is strongly c-deterministic.
(Basis) The case $i = 0$ is trivial, since $S_1^0 = S_2^0 = \emptyset$.
(Induction) Consider $i+1$ and assume the statement holds for i. Let $\gamma^\star$ be any template such that $\gamma^\star \in S_1^{i+1} \setminus S_1^i$ (resp., $\gamma^\star \in S_2^{i+1} \setminus S_2^i$).

To complete the proof it suffices to show that $\gamma^\star$ is c-deterministic (resp., strongly c-deterministic), i.e. each instantiation ϕ of $\gamma^\star$ is c-deterministic (resp., strongly c-deterministic).

Let M be any Kripke structure such that $M \not\models \phi$. Then, we have to prove that a deterministic counterexample for ϕ exists in M. From the definition of Λ, the following cases for $\gamma^\star$ are possible.

- $\gamma^\star \in \mathcal{PSF} \subseteq S_1^{i+1}$. (In this case, $i = 0$.) Each counterexample of ϕ in M is finite, and thus deterministic.
- $\gamma^\star \in S_1^i \wedge S_1^i \subseteq S_1^{i+1}$. Thus, $\phi = \gamma_1 \wedge \gamma_2$, where both γ_1 and γ_2 are c-deterministic by induction hypothesis. Since $M \not\models \phi$, either $M \not\models \gamma_1$ or $M \not\models \gamma_2$. In both cases, the statement follows from the induction hypothesis.
- $\gamma^\star \in S_1^i \vee \mathcal{PSF} \cup \mathcal{PSF} \vee S_1^i \subseteq S_1^{i+1}$. Then, $\phi = \gamma_1 \vee \gamma_2$. Assume γ_2 is a pure state formula and γ_1 is an instantiation of a template in S_1^i; the other case (vice versa) is similar. By the induction hypothesis, γ_1 is c-deterministic.

Since $M \not\models \phi$, there exists a counterexample $\Pi = \Pi_1 * \Pi_2$ in M such that Π_1 is a counterexample for γ_1 and Π_2 is a counterexample for γ_2. Since γ_2 is a pure state formula, Π_2 is finite; thus, by definition of merge

(Def. 3.4) $\Pi = \Pi_1$. Further, $or(\Pi)$ is a state where γ_2 is false. Clearly, $M_{or(\Pi)} \not\models \gamma_1$. Moreover, since γ_1 is c-deterministic, it admits a deterministic counterexample Π_{γ_1} also in $M_{or(\Pi)}$. Clearly, $or(\Pi_{\gamma_1}) = or(\Pi)$, since $or(\Pi)$ is the only initial state of $M_{or(\Pi)}$. As $or(\Pi) \in S_0(M)$, Π_{γ_1} is a counterexample for γ_1 in M too. Hence the deterministic multi-path $\Pi_{\gamma_1} * or(\Pi_{\gamma_1})$ is a counterexample for $\gamma_1 \vee \gamma_2$ in M. Thus, ϕ is c-deterministic.

• $\gamma^\star \in \mathbf{AX}(S_1^i) \subseteq S_1^{i+1}$. Consequently, ϕ is of shape $\mathbf{AX}(\gamma_1)$, where γ_1 is an instantiation of a template in S_1^i. Suppose Π is a counterexample for ϕ. By definition of counterexample, $\Pi(1)$ is a l-counterexample for γ_1 and $\Pi(0)$ is a state. By the induction hypothesis, γ_1 is c-deterministic. Thus, γ_1 has a deterministic counterexample in every Kripke structure in which it fails, and hence also in $M_{\mu(\Pi)(1)}$. Denote by Π_{γ_1} any such deterministic counterexample. Consider now the multi-path Π_ϕ defined as follows: $\Pi_\phi(0) = \Pi(0)$, $\Pi_\phi(1) = \Pi_{\gamma_1}$, $\Pi_\phi(i) = \mu(\Pi_{\gamma_1})(i-1)$, for each $i > 1$. Clearly, $\Pi_\phi(1)$ is a l-counterexample for γ_1 in M. Hence, Π_ϕ is a counterexample for ϕ; clearly, it is deterministic.

• $\gamma^\star \in \mathbf{AV}(\mathcal{PSF}, S_1^i) \subseteq S_1^{i+1}$. Then $\phi = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$, where γ_1 is a pure state formula and γ_2 is c-deterministic by the induction hypothesis. Let Π be a counterexample for ϕ in M. By definition of counterexample, Π is such that there exists a $k \geq 0$ and $\Pi(k)$ is a l-counterexample for γ_2, and $\Pi(i)$ is a l-counterexample for γ_1, for $0 \leq i < k$. Since γ_1 is a pure state formula, $\Pi(i)$, for $0 \leq i < k$, is a state where γ_1 is false. Moreover, since γ_2 is c-deterministic, there exists a deterministic counterexample Π_{γ_2} for γ_2 in $M_{or(\Pi(k))}$. Hence, the multi-path Π_ϕ such that $\Pi_\phi(i) = \Pi(i)$, for each $0 \leq i < k$, $\Pi_\phi(k) = \Pi_{\gamma_2}$, and $\Pi_\phi(i+k) = \mu(\Pi_{\gamma_2})(i)$, for $i > 1$, is a counterexample for ϕ in M. Since Π_ϕ is deterministic, it follows that ϕ is c-deterministic.

• $\gamma^\star \in S_2^i \subseteq S_1^{i+1}$. By the induction hypothesis.

• $\gamma^\star \in \mathbf{AU}(S_1^i, \mathcal{PSF}) \subseteq S_2^{i+1}$. We first show that ϕ is c-deterministic. ϕ is of the form $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where γ_1 is c-deterministic by the induction hypothesis and γ_2 is a pure state formula. Let Π be a counterexample for ϕ in M. By definition of counterexample, Π is such that either (1) $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$, or (2) there exists a $k \geq 0$ such that $\Pi(k)$ is a counterexample for $\gamma_1 \vee \gamma_2$, $\Pi(i)$ is a counterexample for γ_2 (and thus it is a state), for each $0 \leq i \leq k$ and $\Pi(j)$ is a state, for each $j > k$.

In case (1), since γ_2 is a pure state formula, $\Pi(i)$ is a state, for each $i > 0$, and, hence, it is a deterministic counterexample. Consider now case (2). As shown above, each template in $S_1^i \vee \mathcal{PSF}$, is c-deterministic, and thus $\gamma_1 \vee \gamma_2$ is c-deterministic. Hence, $\gamma_1 \vee \gamma_2$ has a deterministic counterexample also in $M_{\mu(\Pi)(k)}$. Let $\Pi_{\gamma_1 \vee \gamma_2}$ be any such deterministic counterexample. Consider now the multi-path Π_ϕ defined as follows: $\Pi_\phi(i) = \Pi(i)$ for each $0 \leq i < k$, $\Pi_\phi(k) = \Pi_{\gamma_1 \vee \gamma_2}$, $\Pi_\phi(j) = \mu(\Pi_{\gamma_1 \vee \gamma_2})(j-k)$, for $j > k$. Clearly, $\Pi_\phi(k)$ is a counterexample for $\gamma_1 \vee \gamma_2$ in M. Hence, Π_ϕ is a counterexample for ϕ in M. Further, as can be easily checked, Π_ϕ is deterministic.

Now we prove that ϕ satisfies item 1 of Definition 5.1. Consider a path $\pi = s_0, \ldots, s_k, \mu(\Pi)$, as there, where Π is a deterministic l-counterexample for ϕ in M. Recall that $\phi = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where γ_1 is, by the induction hypothesis, c-deterministic and γ_2 is a pure state formula. $M_{s_i} \not\models \phi$ implies that γ_2 is false at s_i, for each $i = 0, \ldots, k$, Since Π is a deterministic counterexample for ϕ in $M_{or(\Pi)}$, either

2.1 there exists a $j \geq 0$ such that $\Pi(j)$ is a counterexample for $\gamma_1 \vee \gamma_2$ and $\Pi(i)$, for each $0 \leq i < j$, is a l-counterexample for γ_2 (and thus a state), or

2.2 $\Pi(i)$, is a l-counterexample for γ_2 for each $i \geq 0$ (hence Π is a path).

In either case, the multi-path $\bar{\Pi} = [s_0, \ldots, s_k, \Pi(0), \Pi(1), \ldots]$ is a counterexample for ϕ in M (recall that $s_0 \in S_0(M)$), which is clearly deterministic. Since $\pi = \mu(\bar{\Pi})$ item 1 of Definition 5.1 is satisfied.

To show that ϕ satisfies also item 2 of Definition 5.1, consider any path π such that $\pi(0) \in S_0(M)$ and $\pi(i)$ is the origin of some l-counterexample for ϕ in M, for each $i \geq 0$. Thus, γ_2 is false in each state $\pi(i)$, for $i \geq 0$. Hence, π is a counterpath for ϕ in M.

• $\gamma^\star \in \mathbf{AU}(\mathcal{PSF}, S_2^i) \subseteq S_2^{i+1}$. Then ϕ is of the shape $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where γ_1 is a pure state formula and γ_2 is strongly c-deterministic by the induction hypothesis. We have to prove that also ϕ is strongly c-deterministic. We first show that ϕ is c-deterministic. Consider thus a counterexample Π for ϕ. Then, either

8.1 there exists a $k \geq 0$ such that $\Pi(k)$ is a counterexample for $\gamma_1 \vee \gamma_2$ and $\Pi(i)$ is a counterexample for γ_2, for each $0 \leq i < k$, or

8.2 $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$.

In the case (8.1), by definition of counterexample $M_{or(\Pi(i))} \not\models \gamma_2$, for each $0 \leq i \leq k$. Consider now any deterministic counterexample Π_{γ_2} for γ_2 in $M_{or(\Pi(k))}$. Such a counterexample exists, since γ_2 is strongly c-deterministic (thus c-deterministic). Hence, by item 1 of Definition 5.1, it follows that for every path $\pi_j = [or((\Pi)(j)), ..., or((\Pi)(k-1)), \mu(\Pi_{\gamma_2})(0), \mu(\Pi_{\gamma_2})(1), ...]$, for all $0 \leq j \leq k$, there exists a deterministic counterexample Π_j for γ_2 in $M_{or(\Pi(j))}$ such that $\mu(\Pi_j) = \pi_j$. Hence, the multi-path $\bar{\Pi}$ such that $\bar{\Pi}(i) = \Pi_i$, for $0 \leq i < k$, $\bar{\Pi}(k) = \Pi_{\gamma_2}$, and $\bar{\Pi}(i+k) = \mu(\Pi_{\gamma_2})(i)$, for $i > 0$, is a counterexample for ϕ. Moreover, as can be easily verified, each Π_j, for $0 \leq j < k$, is deterministic.

In the case (8.2), by definition of counterexample $M_{or(\Pi(i))} \not\models \gamma_2$, for each $i \geq 0$. Since γ_2 is strongly c-deterministic, it satisfies item 2 of Definition 5.1. Thus, each suffix $\mu(\Pi)^j$ is a counterpath for γ_2. Hence, for any deterministic counterexamples of $\bar{\Pi}_i$ of γ_2 such that $\mu(\bar{\Pi}_i) = \mu(\Pi)^i$, $i \geq 0$, the deterministic multi-path $[\bar{\Pi}_0, \bar{\Pi}_1, ..., \bar{\Pi}_i, ...]$ is a deterministic counterexample for ϕ.

It remains to prove that ϕ satisfies items 1 and 2 of Definition 5.1. Let $\pi = s_0, s_1, \ldots, s_k, \mu(\Pi)$ be a path as in item 1 for a deterministic l-counterexample Π of ϕ in M. Recall that $\phi = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where γ_1 is a pure state formula and γ_2 is, by the induction hypothesis, strongly c-deterministic. Since s_i is origin of some l-counterexample for ϕ in M, it follows $M_{s_i} \not\models \gamma_2$, for each $0 \leq i \leq k$. Furthermore, since Π is a deterministic counterexample for ϕ, either

8.1′ there exists a $j \geq 0$ such that $\Pi(j)$ is a counterexample for $\gamma_1 \vee \gamma_2$ and $\Pi(i)$ is a counterexample for γ_2, for each $0 \leq i < j$, or

8.2′ $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$.

In any case, γ_2 has a deterministic l-counterexample $\bar{\Pi}$ at $or(\Pi)$ such that $\mu(\bar{\Pi}) = \mu(\Pi)$. Since γ_2 is strongly c-deterministic, item 1 of Definition 5.1 implies that for each $i = 0, \ldots, k$ a deterministic l-counterexample Π_i for γ_2 exists at s_i such that $\mu(\Pi_i) = \pi^i$. Hence, the multi-path $\Pi' = [\Pi_0, \ldots, \Pi_k, \bar{\Pi}(0), \bar{\Pi}(1), \ldots]$ is a deterministic counterexample for ϕ in M. Since $\mu(\Pi') = \pi$, π is a counterpath for ϕ in M; thus, item 1 is satisfied.

To show that ϕ satisfies also item 2 of Definition 5.1, let π be a path in M such that $\pi(0) \in S_0(M)$ and each $\pi(i)$ is origin of a l-counterexample for ϕ in M, $i \geq 0$. Then, each $\pi(0)$ must be the origin of a l-counterexample for γ_2. Since γ_2 is strongly c-deterministic, it follows from item 2 of Definition 5.1 that each suffix π^i of π, $i \geq 0$, is a counterpath for γ_2 in M, i.e., a corresponding deterministic l-counterexample Π_i for γ_2 exists in M at $\pi(i)$. Thus, $\Pi = [\Pi_0, \Pi_1, \ldots]$ is a deterministic counterexample for ϕ in M such that $\pi = \mu(\Pi)$. This means π is a counterpath for ϕ in M, and item 2 of Definition 5.1 is satisfied.

• $\gamma^\star \in S_2^i \vee \mathcal{PSF} \cup \mathcal{PSF} \vee S_2^i \subseteq S_2^{i+1}$. The proof that $\gamma^\star$ is c-deterministic is analogous to the case $\gamma^\star \in S_1^i \vee \mathcal{PSF} \cup \mathcal{PSF} \vee S_1^i$ above. The verification of points 1 and 2 in Definition 5.1 is straightforward. $\Box$

The proof of the previous theorem intuitively explains why the only possible nesting for ϕ_2 in an until $\phi_1 \mathbf{U} \phi_2$ is another until operator. On the other hand, if the formula ϕ_2 in $\phi_1 \mathbf{U} \phi_2$ is a pure state formula, then ϕ_1 can be any c-deterministic formula.

Concerning nesting into an unless $\mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$, it is not possible to nest an arbitrary non-pure state formula in the left position. In this case, strong c-determinism does not ensure that the formula is c-deterministic. Recall that a counterexample for $\mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$ is a multi-path $\Pi = [\Pi(0), \Pi(1), \ldots]$ such that $\Pi(0)$,...,$\Pi(k-1)$ prove the falsity of γ_1 and $\Pi(k)$ the falsity of γ_2. Trying to construct from Π a deterministic counterexample $\bar{\Pi}$ for $\mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$, we have to replace each $\Pi(i)$, $0 \leq i \leq k$, with a suitable deterministic counterexample $\bar{\Pi}(i)$. We can do so easily for all $i < k$: Since γ_1 is strongly c-deterministic, for any deterministic counterexample $\bar{\Pi}(k-1)$ for γ_1 we can find appropriate $\bar{\Pi}(0)$,...,$\bar{\Pi}(k-2)$ by exploiting the property in item 1 of Definition 5.1. However, it may happen that every possible $\bar{\Pi}(k-1)$ misses some state from $\Pi(k)$ which is necessary to refute γ_2; thus, a deterministic counterexample $\bar{\Pi}$ can not be built.

5.1 Computing a counterpath for $\mathbf{DET}$-instances

In Section 4, we have shown that deciding whether an arbitrary formula ϕ has a counterpath on a given structure M is intractable in general, and so is computing a counterpath. Since instances of $\mathbf{DET}$-templates always have a counterpath if they are false in M, the question whether there is an (efficient) procedure for computing any counterpath is natural. Note that existence of a counterpath does not a priori mean that computing a counterpath is easy; this could still be a difficult problem.

Our second main result shows that this is not the case. Let for any path $P = s_0, s_1, \ldots, s_k$ in a structure M denote $|P|$ the length of P (= $k+1$), and let for any formula γ denote $d_{\mathbf{A}}(\gamma)$ the $\mathbf{A}$-nesting depth of γ (where $d_{\mathbf{A}}(\gamma) = 0$ for every pure state formula γ).

Theorem 5.2 *Let γ be such that $\gamma^\star \in \mathbf{DET}$. If $M \not\models \gamma$, then γ has a counterpath in M which is either a single state (if $\gamma^\star \in \mathcal{PSF}$), or representable as P, C where P is a finite path (prefix) and C a cycle in M such that $|P| + |C| \leq d_{\mathbf{A}}(\gamma)|S(M)|$. Moreover, given γ and M, such P and C can be computed in polynomial time.*

Proof. The first part (existence of a representation P, C as described) is shown following the induction in the proof of Theorem 4.3. For each instance ϕ of a template $\gamma^\star \in S_1^i \cup S_2^i$, we can construct the desired representation P, C from the main path of the deterministic counterexample constructed in the proof there, exploiting that deterministic counterexamples Π' used in the constructions have representations P', C' as described. We omit repeating all these constructions in detail, and focus here on the relevant facts that establish P, C:

1. In cases where ϕ is of the form $\phi_1 \vee \phi_2$, $\phi_1 \wedge \phi_2$, a counterpath for ϕ is immediately obtained by the induction hypothesis.

2. In cases where ϕ is of the form $\mathbf{AX}\phi_1$, $\mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, and in some cases of $\mathbf{A}(\phi_1 \mathbf{U} \phi_2)$, the deterministic counterexample Π constructed for ϕ is of the form $[\Pi(0), \ldots, \Pi(k), \Pi(k+1), \ldots]$ where

$\Pi(0)$,...,$\Pi(k-1)$ are states except if $\phi^\star \in \mathbf{AU}(\mathcal{PSF}, \mathbf{DET} \setminus \mathcal{PSF})$, $\Pi(k)$ is a deterministic counterexample for a formula ψ' such that $d_{\mathbf{A}}(\psi') < d_{\mathbf{A}}(\phi)$, and all $\Pi(j)$ are states, $j > k$. Two subcases arise, depending on the formula ψ':

2.1 $d_{\mathbf{A}}(\psi') = 0$, i.e., $\psi'^\star \in \mathcal{PSF}$. Then, Π is a simple path in M, and the states $\Pi(j)$, $j > k$, in Π are meaningless (i.e., the suffix $[\Pi(k), \Pi(k+1)\ldots]$ can be replaced by any infinite path starting at $\Pi(k)$). Thus, a counterpath for ϕ can be represented by P, C such that $|P| + |C| \leq |S(M)| \leq d_{\mathbf{A}}(\phi)|S(M)|$.

2.2 $d_{\mathbf{A}}(\psi') > 0$. Then, ψ' can be assumed to have a counterpath P', C' as in the induction hypothesis, and P, C is given by $s_0, \ldots, s_{k-1}$,P', C', where $s_i = \mathit{or}(\Pi(i))$, for $i = 0, \ldots, k-1$. For a minimal k, it holds that $k \leq |S(M)|$, and we obtain

$$|P| + |C| \;=\; k + |P'| + |C'| \;\leq\; |S(M)| + d_{\mathbf{A}}(\psi')|S(M)| \;\leq\; d_{\mathbf{A}}(\phi)|S(M)|.$$

3. In the case where $\phi = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, a deterministic counterexample Π may be constructed such that each $\Pi(i)$ is a counterexample for γ_2. In the case where $\gamma_2^\star \in \mathcal{PSF}$, Π is a simple path in M, which can be replaced by a prefix-cycle pair P, C such that $|P| + |C| \leq |S(M)| \leq d_{\mathbf{A}}(\phi)|S(M)|$ (cf. 2.1); otherwise, if $\gamma_2^\star \in \mathbf{DET} \setminus \mathcal{PSF}$, then P, C is given by P', C' representing $\mu(\Pi(0))$, and by the induction hypothesis $|P| + |C| = |P'| + |C'| = \leq d_{\mathbf{A}}(\gamma_2)|S(M)| \leq d_{\mathbf{A}}(\phi)|S(M)|$.

This concludes the proof of the first part of the theorem. For computing P, C in polynomial time (second part of Theorem 5.2) we describe an algorithm which proceeds in two steps. Suppose that ϕ and M are given for input.

Step 1. Label each state $s \in S$ with the set

$$F(s) = \{\phi' \mid \phi' \text{ is a subformula of } \phi \text{ such that } M, s \not\models \phi'\}.$$

It is well-known that this labeling is possible in polynomial time (in fact in $O(|\phi|(|S(M)| + |R(M)|)$ time) [3].

Step 2. Construct a counterpath for ϕ, which is either a single state or P, C representing an infinite path, using the following procedure:

Procedure COUNTERPATH

Input: Labeled graph $G = (S, R, F)$, $\mathbf{DET}$ instance ϕ, state $s \in S$ s.t. $\phi \in F(s)$.

Output: s, if $\phi^\star \in \mathcal{PSF}$; otherwise, P, C representing a counterpath π for ϕ starting at s.

Execute COUNTERPATH(G, ϕ, s_0) for *some arbitrary* $s_0 \in S$ such that $\phi \in F(s_0)$, and return the result.

COUNTERPATH proceeds *top-down*, and constructs the output either directly, or by making a recursive call; thus, COUNTERPATH extends an initially empty prefix P_0 to $P_1 \leq P_2 \leq \cdots$ repeatedly until it is eventually completed with a cycle. In general, different choices exist for extending P_i to P_{i+1}. The crucial fact is that membership of $\phi^\star$ in $\mathbf{DET}$ guarantees a "don't care" nondeterminism, i.e., no backtracking is necessary. If P_i is properly extended to P_{i+1}, then it can be finally completed with a cycle.

We now describe how COUNTERPATH proceeds for $\phi^\star \notin \mathcal{PSF}$, depending on the structure of ϕ. We consider the different possible cases:

• $\phi = \gamma_1 \wedge \gamma_2$. Then, either $\gamma_1 \in F(s)$ or $\gamma_2 \in F(s)$ (or both). Call either COUNTERPATH(G, γ_1, s) or COUNTERPATH(G, γ_2, s), respectively, and return the result.

• $\phi = \gamma_1 \vee \gamma_2$. If $\gamma_1^\star \in \mathcal{PSF}$, then call COUNTERPATH$(G, \gamma_2, s)$; otherwise, call COUNTERPATH(G, γ_1, s). Return the result.

• $\phi = \mathbf{AX}(\gamma_1)$. Choose any s' such that $(s, s') \in R$ and $\gamma_1 \in F(s')$. If $\gamma_1^\star \notin \mathcal{PSF}$, then call COUNTERPATH$(G, \gamma_1, s')$ and return the result; otherwise, complete the path s, s' to an arbitrary prefix-cycle path P, C (where P may be void) containing at most $|S(M)|$ states.

• $\phi = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$. Determine any node s' reachable by a (possible empty) path $s = s_0, s_1, \ldots, s_k = s'$ in R such that $\gamma_1 \mathbf{V} \gamma_2 \in F(s_i)$, for all $i = 0, \ldots, k-1$ and $\gamma_2 \in F(s')$. If $\gamma_2^\star \notin \mathcal{PSF}$, then call COUNTERPATH$(G, \gamma_2, s')$, and return $s_0, \ldots, s_{k-1}, P', C'$ where P', C' is the result of the call; otherwise, if $\gamma_2^\star \in \mathcal{PSF}$, then complete $s_0, \ldots, s_k$ to any prefix-cycle path P, C having at most $|S(M)|$ states and return it.

• $\phi = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$. If there exists a prefix-cycle pair $P, C = s_0, s_1, \ldots, s_k$ in G such that $k < |S(M)|$ and $\gamma_2 \in F(s_i)$, for each $i = 0, \ldots, k$ then return P, C (this can be efficiently determined).

In the other case, determine any state s' which is reachable from s by a path $s = s_0, \ldots, s_k = s'$ such that $\gamma_2 \in F(s_i)$, for all $i = 0, \ldots, k$ and $\gamma_1 \in F(s_k)$. Now, if both $\gamma_1^\star, \gamma_2^\star \in \mathcal{PSF}$, then complete the path $s_0, \ldots, s_k$ to an arbitray prefix-cycle pair P, C such that $|P| + |S| \leq |S(M)|$ and return it.

Otherwise, call COUNTERPATH(G, γ_1, s'), if $\gamma_1^\star \notin \mathcal{PSF}$, and call COUNTERPATH$(G, \gamma_2, s')$, if $\gamma_2^\star \notin \mathcal{PSF}$; note that only one of the two cases can apply. Return $P, C = s_0, \ldots, s_{k-1}, P', C'$ where P', C' is the result of the call.

The correctness of the procedure COUNTERPATH(G, ϕ, s) follows from the proof of Theorem 5.1. It is not hard to see that each of the cases in the body of COUNTERPATH can be completed in polynomial time (modulo recursion). Since the recursion depth is bounded by the formula length $|\phi|$, it follows that some P, C can be constructed in polynomial time. Using proper data structures (in particular for the maximal strongly conneceted components in subgraphs of R induced by labelings in F), each case can be handled in $O(|S(M)| + |R(M)|)$ time, i.e., in linear time in the size of M. Thus, the procedure COUNTERPATH(G, ϕ, s) takes $O(|\phi|(|S(M)| + |R(M)|))$ time.

Since, as remarked above, also the construction of $G = (S, R, F)$ is possible in $O(|\phi|(|S(M)| + |R(M)|))$ time, it follows that some P, C can be computed from M and ϕ in $O(|\phi|(|S(M)| + |R(M)|))$ time. This proves the second part and the result. $\Box$

Remarks. (1) We remark that the representation P, C of the path π returned by COUNTERPATH can be adorned in order to provide more information about the failure of subformulas. In particular, for an unless $\mathbf{A}(\phi_1 \mathbf{V} \phi_2)$ the stage s_k in π demonstrating the failure of $\phi_1 \mathbf{V} \phi_2$ can be marked, and similarly for an until $\mathbf{A}(\phi_1 \mathbf{U} \phi_2)$; if ϕ_2 is false in each state of π, this could be marked at $\pi(0)$. An adorned cycle-prefix pair P, C can be seen as a compact representation of a deterministic counterexample, which, different from a counterpath, retains all structural information of the underlying multi-path.

(2) There are instances ϕ of templates in $\mathbf{DET}$ and structures M such that for any prefix-cycle pair P, C of an arbitrary counterpath for ϕ in M, the size $|P| + |C|$ is $\Omega(d_{\mathbf{A}}(\phi)|S(M)|)$; the prefix P may cycle through states in M for a number of times that is bounded by $d_{\mathbf{A}}(\phi)$, which can not be expressed by an (infinite) cycle.

6 All c-deterministic Templates are in DET

The proof of the converse of Theorem 5.1 is based on the observation that particular instantiations of non-deterministic templates can be used to derive the result. The structure of these instantiations allows to build structures in which no deterministic counterexamples exist in a systematic way.

Definition 6.1 (disjoint and positive instantiation) A *disjoint instantiation* of a template $\gamma^\star \in \mathbf{T}^\star$ is an instantiation ϕ of $\gamma^\star$ which can be built starting from pure state formulas such that $\wedge$, $\vee$, $\mathbf{A}(\cdot\mathbf{U}\cdot)$, $\mathbf{A}(\cdot\mathbf{V}\cdot)$ are only applied to formulas ϕ_1 and ϕ_2 having disjoint sets of atomic propositions, i.e. $AP(\phi_1) \cap AP(\phi_2) = \emptyset$.

An instantiation ϕ is *positive*, if each occurrence of an atom in ϕ is under an even number of negations.

Notice that in a positive template instantation ϕ, each subformula $\neg\psi$ which is not in the scope of another negation is logically equivalent to a monotone (negation-free) Boolean formula over $AP(\psi)$. Observe also that $\neg\psi \not\equiv$ *true* and $\neg\psi \not\equiv$ *false* holds in this case.

Positive disjoint instantiations have the nice property that with respect to counterexamples, any part of a Boolean combination ϕ of formulas $\phi_1, \ldots, \phi_m$ can be "projected out" in suitable structures, i.e., to counterexamples for a simplified formula ϕ' give rise to counterexamples for ϕ. This is particularly useful for showing that ϕ is not c-deterministic if any of $\phi_1, \ldots, \phi_m$ is not c-deterministic.

Lemma 6.1 *Let ϕ be a positive disjoint instantiation of $\phi^\star \in \mathbf{T}^\star$ which is a monotone Boolean combination of distinct formulas $\phi_1, \ldots, \phi_m$ (each of which is considered as atom and used only once). Let ϕ^+ be any nonempty formula which results by removing arbitrary subformulas from ϕ. Let M^+ be any structure such that $R(M^+)$ is total, i.e., each state reaches some state, and $AP(M^+) = AP(\phi^+)$. Then, there exists a structure M coinciding with M^+ except $AP(M) = AP(\phi)$ and $L(M^+)(s) \subseteq L(M)(s)$, for each state s, such that (1) $M, s \models \phi$ iff $M^+, s \models \phi^+$ holds for each state s, and (2) for each path π, it holds that π is a local counterpath for ϕ in M iff π is a local counterpath for ϕ^+ in M^+.*

Proof. Since ϕ is positive, all ϕ_i are positive. Thus, every formula ϕ_i which does not occur in ϕ^+ can be made globally true in M^+ by including $AP(\phi_i)$ in the label of each state s; otherwise, since $AP(\phi_i) \cap AP(M^+) = \emptyset$, ϕ_i is false in each state of M^+.

Let M result from M^+ by making each ϕ_i globally true such that ϕ_i occurs in a maximal subformula ψ that is pruned from ϕ and ψ is connected in ϕ by conjunction. (Any other other pruned ϕ_j occurs in a maximal pruned subformula which is connected by disjunction; it is globally false in M^+ and thus also in M.) It is not hard to see that this M satisfies the property stated in the lemma. □

The next lemma informally states that for any positive disjoint instantiation of a template in $\mathbf{DET}$, we can always find a structure such that the formula is true in it, but false if we proceed long enough from an initial state. Observe that this property is not true for all formulas that are instantiations of templates in $\mathbf{DET}$. Consider e.g. the formula $\phi = \mathbf{A}(\mathit{false}\mathbf{V}a)$, where a is an atomic proposition. This formula is an instance of the template $\mathbf{A}(\star\mathbf{V}\star)$, which belongs to $\mathbf{DET}$. A counterexample for ϕ is a path π along which a is false in some state $\pi(i)$. Here, it is impossible to prefix π with a sequence $s_0, \ldots, s_k$ of states such that along the resulting path $\mathit{false}\mathbf{V}a$ becomes true.

Definition 6.2 (single-path structure) A conic structure M is called a *single-path* structure, if M has a single path π starting at the initial state, and each state in M occurs in it.

An immediate consequence of this definition is that for any single-path structure M and non pure-state formula γ it holds that $M \not\models \gamma$ just in case where $\pi(M)$ is a counterpath for γ.

Lemma 6.2 *For every positive disjoint instantiation γ of a template $\gamma^\star \in \mathbf{DET}$, there exist a single-path structure M and a $k \geq 1$ such that $M \models \gamma$ and $\pi(M)^k$ is a local counterpath for γ (resp., $\pi(M)(k) \not\models \gamma$ if $\gamma^\star \in \mathcal{PSF}$), where $\pi(M)$ denotes the unique infinite path in M.*

Proof. We prove the statement by induction on the stage $i \geq 0$ of $\Lambda^i = (S_1^i, S_2^i)$ in which $\gamma^\star$ first occurs.
(Basis) The case $i = 0$ is trivial.
(Induction) Assume that the statement holds for i and consider the possible cases for $\gamma^\star \in S_1^{i+1} \cup S_2^{i+1}$ where $i+1 > 0$. By the induction hypothesis, it remains to consider $\gamma^\star \notin S_1^i \cup S_2^i$.

• $\gamma^\star \in \mathcal{PSF}$. (In this case, $i = 1$.) Let M have the states s_0 and s_1, where s_0 is the unique initial state, and the transitions (s_0, s_1), (s_1, s_1). Let $L(M)(s_0) = AP(\gamma)$ and $L(M)(s_1) = \emptyset$. Clearly, M is a single-path structure such that $M \models \gamma$, and $M, \pi(M)^1(0) \not\models \gamma$. Thus the statement holds.

• $\gamma^\star \in \mathbf{AX}(S_1^i)$. Thus, $\gamma = \mathbf{AX}(\gamma_1)$. By the induction hypothesis, a single-path structure M with initial state s_0 and a $k \geq 1$ exist for γ_1 which satisfy the statement of the lemma. Let k^* be the least such k. If $k^* > 1$ we are done, since M is a single-path structure where also γ satisfies the statement of the lemma. Otherwise (i.e., if $k^* = 1$), we can modify M by adding a new state s_0' which reaches s_0 and has an arbitrary label. Denote by M' the resulting single-path structure with initial state s_0'. Since $\pi(M')^1 = \pi(M)$, it holds that $M' \models \gamma$. Furthermore, $\pi(M')^1$ is a local counterpath for γ, since $\pi(M')^2 = \pi(M)^1$. Hence the statement holds.

• $\gamma^\star \in \mathbf{AV}(\mathcal{PSF}, S_1^i)$. Let $\gamma = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$. By induction hypothesis, for γ_2 exist a single-path structure M and an index $k \geq 1$ such that the property of the lemma holds. We modify M by adding $AP(\gamma_1)$ to every state label in M. It is easy to see that the resulting structure M' satisfies $M' \models \gamma$ because γ_1 is globally true along $\pi(M')$. Furthermore, $\pi(M')^k$ is still a local counterpath for γ_2 (resp., $\pi(M')(k) \not\models \gamma_2$) since γ is a disjoint positive instantiation. Hence, the statement holds.

• $\gamma^\star \in \mathbf{AU}(S_1^i, \mathcal{PSF})$. Thus, $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$. Consider the single-path structure M with states s_0 and s_1, where s_0 is the initial state, transitions (s_0, s_1), (s_1, s_1) and labeling $L(M)(s_0) = AP(\gamma_2)$ and $L(M)(s_1) = \emptyset$. This M and $k = 1$ prove the statement for γ. Indeed, $M \models \gamma$ since γ_2 is true in s_0. Further, $\pi(M)^1$ is a local counterpath for γ since γ_2 is globally false along it.

• $\gamma^\star \in \mathbf{AU}(\mathcal{PSF}, S_2^i)$. Thus, $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$. By induction hypothesis, for γ_2 exist a single-path structure M and an index $k \geq 1$ as in the lemma. Without loss of generality, no atomic proposition from $AP(\gamma_1)$ occurs in any state label of M. Since γ is a positive disjoint instantiation, it is easy to see that M and k witness the statement also for γ. Indeed, $M \models \gamma$ since γ_2 is true in the initial state of M. Furthermore, $\pi(M)^k$ is a local counterpath for γ, since it is a local counterpath for γ_2 (resp., γ_2 is false in $\pi(M)(k)$) and γ_1 is globally false along it.

• $\gamma^\star \in S_1^i \vee \mathcal{PSF} \cup \mathcal{PSF} \vee S_1^i$. Thus, $\gamma = \gamma_1 \vee \gamma_2$. Assume that $\gamma_1^\star \notin \mathcal{PSF}$; the case $\gamma_2^\star \notin \mathcal{PSF}$ is similar. By induction hypothesis, for γ_1 exist a single-path structure M and an index $k \geq 1$ as stated in the lemma. Without loss of generality, no atomic proposition from $AP(\gamma_2)$ occurs in any state label of M. Since γ is a positive disjoint instantiation, it is easy to see that M and k witness the statement also for γ. Indeed, $M \models \gamma$ since $M \models \gamma_1$. Further, $\pi(M)^k$ is a local counterpath for γ since it is a local counterpath for γ_1 (resp., γ_1 is false in $\pi(M)(k)$) and γ_2 is globally false along it. Thus, the statement holds.

• $\gamma^\star \in S_1^i \wedge S_1^i$. Thus, $\gamma = \gamma_1 \wedge \gamma_2$, and w.l.o.g. $\gamma_1^\star \notin \mathcal{PSF}$. By induction hypothesis, for γ_1 exist a single-path structure M and an index $k \geq 1$ as stated in the lemma. We modify M by adding to every state label the set of atomic propositions appearing in γ_2. It is easy to see that the resulting structure M' and k

witness the statement also for γ. Clearly, $M' \models \gamma$ since $M' \models \gamma_1$ and $M' \models \gamma_2$ since γ_2 is globally true in M'. Furthermore, $\pi(M')^k$ is a local counterpath for γ since it is a local counterpath for γ_1. Thus, the statement holds. This concludes the proof. □

The next lemma informally says that for any positive disjoint instantiation γ of a template in $\mathbf{DET}$, it is possible to find a single-path structure which does not satisfy γ, but γ is always satisfied if we proceed long enough on the single path. This lemma is in a sense complementary to the previous lemma. Similar as there, the property is not true for arbitrary instantiations of templates from $\mathbf{DET}$. E.g., a single-path structure falsifying $\gamma = \mathbf{A}(\mathit{true}\mathbf{U}a)$ does not contain any "suffix" structure in which γ holds.

Prior to the lemma, we introduce the notion of k-structure.

Definition 6.3 (k-structure) A *k-structure* for a positive disjoint instantiation γ of a template $\gamma^\star \in \mathbf{T}^\star$ is any conic structure M such that $M \not\models \gamma$ and for each path π in M starting at s_0, there exists an index $k \geq 1$ such that $M, \pi^i(0) \models \gamma$, for each $i \geq k$. □

We will use k-structures repeatedly in constructions of structures which do not have deterministic counterexamples for formulas involving the until operator.

Lemma 6.3 *Each positive disjoint instantiation γ of any template $\gamma^\star \in \mathbf{DET}$ has some k-structure M. In fact, always single-path k-structures M do exist.*

Proof. As previously, we prove the statement by induction on the stage $i \geq 0$ of $\Lambda^i = (S_1^i, S_2^i)$ in which $\gamma^\star$ first occurs.
(Basis) The case $i = 0$ is trivial.
(Induction) Assume that the statement holds for i, and consider the possible cases for $\gamma^\star \in S_1^{i+1} \cup S_2^{i+1}$, where $i + 1 > 0$. By the induction hypothesis, it remains to consider $\gamma^\star \notin S_1^i \cup S_2^i$.

• $\gamma^\star \in \mathcal{PSF}$. (In this case, $i = 1$.) Let M have the states s_0 and s_1, where s_0 is the unique initial state, and the transitions (s_0, s_1), (s_1, s_1). Let $L(M)(s_0) = \emptyset$ and $L(M)(s_1) = AP(\gamma)$. Clearly, M is a single path structure such that $M \not\models \gamma$, and $M, \pi(M)^1(0) \models \gamma$. Thus the statement holds.

• $\gamma^\star \in \mathbf{AX}(S_1^i)$. Let $\gamma = \mathbf{AX}(\gamma_1)$. By induction hypothesis, there exist a single-path structure M and an index $k \geq 1$ such that $M \not\models \gamma_1$ and $M, \pi(M)^i(0) \models \gamma_1$ for all $i \leq k$. Let s_0 be the initial state of M. We modify M by changing the initial state to a new state s with arbitrary label and adding the transition (s, s_0). Clearly, the resulting structure M' is single-path and $M' \not\models \gamma$. From the induction hypothesis, it follows that for each $i \geq k + 1$, $M', \pi(M')^i(0) \models \gamma_1$. Hence, the statement holds.

• $\gamma^\star \in \mathbf{AV}(\mathcal{PSF}, S_1^i)$. Let $\gamma = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$. Let s_0 be the initial state of a single-path structure M for γ_2 and $k \geq 1$ as stated in the lemma, which exist by the induction hypothesis. Since $M \not\models \gamma_2$, it follows $M \not\models \gamma$. Furthermore, $M, \mu(\Pi)^i(0) \models \gamma_2$ implies $M, \mu(\Pi)^i(0) \models \gamma$, for each $i \geq k$. Thus the statement holds.

• $\gamma^\star \in \mathbf{AU}(S_1^i, \mathcal{PSF})$. Let $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$. Let for γ_1 be M and $k \geq 1$ as stated in the lemma, which exist by induction hypothesis. Without loss of generality, M includes $AP(\gamma_2)$ in each state label $L(s)$ except for the initial state s_0, which contains no atomic proposition from $AP(\gamma_2)$. Then, $M, s_0 \not\models \gamma_2$, and since $M \not\models \gamma_1$, it follows $M \not\models \gamma$. Furthermore, $M, \pi(M)^i(0) \models \gamma$ for all $i \geq k$ since γ_2 is true in $\pi(M)^i(0)$. Thus, the statement holds.

• $\gamma^\star \in \mathbf{AU}(\mathcal{PSF}, S_2^i)$. Let $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$. Let for γ_2 be M and $k \geq 1$ as stated in the lemma, whose existence follows from the induction hypothesis. Without loss of generality, we assume that the initial state s_0 of M contains no atomic proposition from $AP(\gamma_1)$. Since $M \models \gamma_2$, it follows $M \not\models \gamma$. Furthermore, since $M, \pi(M)^i(0) \models \gamma_2$ it follows that $M, \pi(M)^i(0) \models \gamma$, for all $i \geq k$. Thus the statement holds.

• $\gamma^\star \in S_1^i \vee \mathcal{PSF} \cup \mathcal{PSF} \vee S_1^i$. Let $\gamma = \gamma_1 \vee \gamma_2$. Assume $\gamma_1^\star \notin \mathcal{PSF}$; the case $\gamma_2^\star \notin \mathcal{PSF}$ is similar. Let for γ_1 be M and $k \geq 1$ as stated in lemma, which exist by induction hypothesis. Assume without loss of generality that no atomic proposition from $AP(\gamma_2)$ occurs in any label of M. Then, it is easy to see that M and k witness the statement for γ.

• $\gamma^\star \in S_1^i \wedge S_1^i$. Let $\gamma = \gamma_1 \wedge \gamma_2$. Let for γ_1 be M and $k \geq 1$ as stated in the lemma, which exist by the induction hypothesis. Assume without loss of generality that $\gamma_1^\star \notin \mathcal{PSF}$, and that each label of M includes $AP(\gamma_2)$. Since γ_2 is globally true in M, it is easy to see that M and k witness the statement also for γ. This concludes the proof. $\Box$

In the next lemma, we show that a large class of templates in $\mathbf{T}^\star \setminus \mathbf{DET}$ which involve nesting into the until operator $\mathbf{U}$ or the unless operator $\mathbf{V}$, respectively, are not deterministic. We establish this by proving that positive disjoint instantiations of these templates are not c-deterministic. Prior to that, we introduce some useful concepts.

Definition 6.4 (left- and right-structures) A *left-structure* M for a positive disjoint instantiation $\phi = \mathbf{A}\psi$ is a conic structure with initial state s_0 and $AP(M) = AP(\phi)$, which satisfies, depending on the linear-time operator guarding ψ, the following properties (see Figure 5):

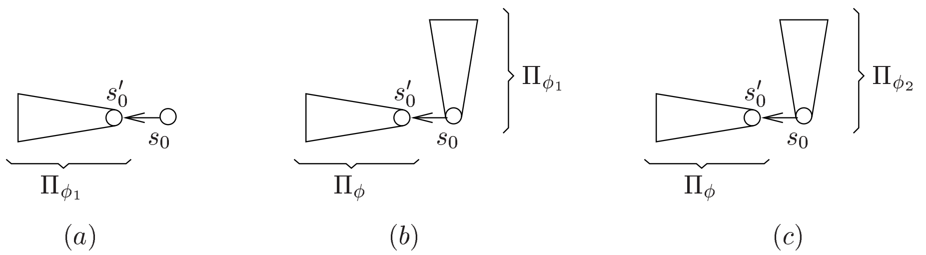

Figure 5: Left-structures for (a) $\phi = \mathbf{AX}\phi_1$, (b) $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, and (c) $\phi = \mathbf{A}(\phi_1 \mathbf{U} \phi_2)$

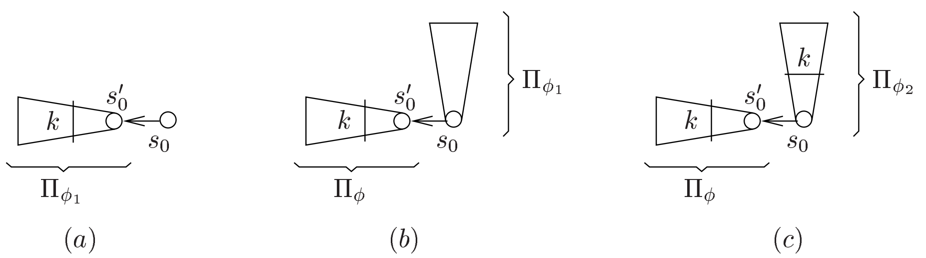

Figure 6: Right-structures for (a) $\phi = \mathbf{AX}\phi_1$, (b) $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, and (c) $\phi = \mathbf{A}(\phi_1 \mathbf{U} \phi_2)$

If $\phi = \mathbf{AX}(\phi_1)$, then only one transition (s_0, s_0') leaving from s_0 exists, and

- s_0' is the initial state of another structure, denoted by Π_{ϕ_1},

- s_0 does not appear in the set of states of Π_{ϕ_1},
- $\Pi_{\phi_1} \not\models \phi_1$.

If $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, then

- s_0 is the initial state of another structure, denoted by Π_{ϕ_1}, such that $\Pi_{\phi_1} \not\models \phi_1$;
- there is only one transition from s_0 to a state s'_0 not belonging to Π_{ϕ_1}, which is the initial state of another structure, denoted by Π_ϕ, such that $\Pi_\phi \not\models \phi$;
- the sets of states of Π_{ϕ_1} and Π_ϕ are disjoint.

For $\phi = \mathbf{A}(\phi_1 \mathbf{U} \phi_2)$, M is similar as for $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, but with the roles of ϕ_1 and ϕ_2 exchanged.

Right-structures for ϕ are particular left structures, such that all structures Π_ϕ, Π_{ϕ_1}, and Π_{ϕ_2} involved—with the exception of Π_{ϕ_1} for $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$—are k-structures (see Figure 6). □

Left- and right-structures will be used as components for the left-nested and right-nested formulas γ_1 and γ_2, respectively, in the constructions of structures M witnessing the fact that formulas $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$ are not c-deterministic in general, and similarly for formulas $\mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$.

We note the following proposition.

Proposition 6.4 *Let M be any left-structure for a positive disjoint instantiation ϕ. Then $M \not\models \phi$.*

Proof. For $\phi = \mathbf{AX}(\phi_1)$, this is obvious. To see this for $\phi = \mathbf{A}(\phi_1 \mathbf{V} \phi_2)$, let Π be a counterexample for ϕ in Π_ϕ (which exists by Theorem 3.1), and let Π_0 be a counterexample for ϕ_1 in Π_{ϕ_1} (starting at s_0). Then, the multi-path $[\Pi_0, \Pi(0), \Pi(1), \cdots]$ is a counterexample for ϕ. In case $\phi = \mathbf{A}(\phi_1 \mathbf{U} \phi_2)$, let Π be a counterexample for ϕ in Π_ϕ (which exists by Theorem 3.1), and let Π_0 be a counterexample for ϕ_2 in Π_{ϕ_2} (starting at s_0). Then, the multi-path $[\Pi_0, \Pi(0), \Pi(1), \cdots]$ is a counterexample for ϕ. □

Definition 6.5 (fusion of structures) Let M_1 and M_2 be conic structures with initial states s_0^1 and s_0^2, respectively, having disjoint sets of states. Then, the *fusion* of M_1 and M_2 is the conic structure M obtained by taking the union of M_1 and M_2, where s_0^1 and s_0^2 are merged into a single state s_0 with label $L(s_0) = L(s_0^1) \cup L(s_0^2)$. □

Lemma 6.5 *Let γ be a positive disjoint instantiation of a template $\gamma^\star \in \mathbf{T}^\star$ such that either*

1. $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$*, where* $\gamma_1^\star = \notin \mathcal{PSF}$ *and* $\gamma_2^\star \in \mathbf{DET} \setminus \mathcal{PSF}$*, or*
2. $\gamma = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$*, where* $\gamma_1^\star \notin \mathcal{PSF}$*, and* $\gamma_2^\star \in \mathbf{DET}$.

Then, γ is not c-deterministic.

Proof. To prove the statement, we have to find a structure M such that both $M \not\models \gamma$ and each counterexample for γ in M is not a deterministic multi-path. We will construct such a M starting from left- and right-structures M_1 and M_2 for the subformulas γ_1 and γ_2, respectively. Unless stated otherwise, such structures will have disjoint sets of states. We observe the following fact.

Fact. For each γ_1, some left-structure exists, and for each γ_2, by Lemma 6.3 some right-structure exists.

(Recall that right-structures are particular left-structures, and thus Lemma 6.3 implies also the existence of left-structures for each γ_2. However, for each γ_2 simple left-structures can be found.)

Technically, we prove the statement in the lemma first for the case in which γ_1 and γ_2 are either of the form $\mathbf{A}\psi$ or pure state formulas. By exploiting Lemma 6.1, we can then conclude that the statement is true in general. Thus, according to $\gamma_1^\star$ and $\gamma_2^\star$, we consider the following cases (1) and (2).

(1) $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1^\star = \mathbf{A}\psi_1^\star \notin \mathcal{PSF}$ and $\gamma_2^\star = \mathbf{A}\psi_2^\star \in \mathbf{DET} \setminus \mathcal{PSF}$. We construct M as the fusion of a left-structure M_1 for γ_1 and a right-structure M_2 for γ_2 with initial state s_0, and modify M according to the linear time operators $\mathbf{X}$, $\mathbf{V}$, and $\mathbf{U}$, guarding ψ_1 and ψ_2, respectively. The following cases are possible:

• $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$. We modify M as follows. In each state s of the structure $\Pi_{\gamma_{1,1}}$ in M_1 (see Def. 6.4), we include $AP(\gamma_{2,1})$ (i.e., in its label $L(s)$), and in each state of $\Pi_{\gamma_{2,1}}$ in M_2, we include $AP(\gamma_{1,1})$ (see Figure 7).

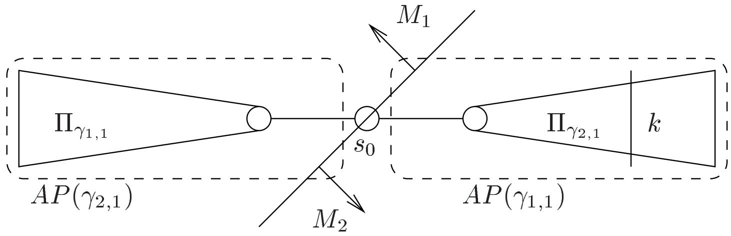

Figure 7: The $\mathbf{X}$-$\mathbf{X}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$

Clearly, these additions preserve the existence of counterexamples for $\gamma_{1,1}$ in $\Pi_{\gamma_{1,1}}$ and for $\gamma_{2,1}$ in $\Pi_{\gamma_{2,1}}$, respectively, since $AP(\gamma_{1,1})$ and $AP(\gamma_{2,1})$ are disjoint.

It holds that $M \not\models \gamma$, since $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$. Indeed, we can find a counterexample for $\gamma_1 \vee \gamma_2$ simply by merging a counterexample for γ_1 in M_1 with a counterexample for γ_2 in M_2. Clearly, this counterexample is not deterministic.

It remains to show that no deterministic counterexample for γ in M exists. First observe that no counterexample for γ_1 is in M_2. Indeed, for every multi-path Π in M_2, $\Pi(1)$ cannot be a counterexample for $\gamma_{1,1}$, since each state of M_1 except s_0 contains the set $AP(\gamma_{1,1})$. Similarly, there is no counterexample for γ_2 is in M_1. Hence, each counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic.

By Definition 3.5, any counterexample for γ must involve counterexamples for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. Clearly, this concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample such that $\Pi(i)$ is a counterexample for γ_2, for every $i \geq 0$. Since γ_2 is globally true in M_1, $\mu(\Pi)$ must lead into M_2, and thus into $\Pi_{\gamma_{2,1}}$. However, $\Pi_{\gamma_{2,1}}$ is a k-structure, which means that γ_2 is eventually true. This raises the desired contradiction.

• $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{V} \gamma_{2,2})$. We modify M in the following way. We add to every state s of M_1 except s_0 the set $AP(\gamma_2)$. Similarly, we add to every state of M_2 except s_0 the set $AP(\gamma_1)$. Finally, we add in every other state of $\Pi_{\gamma_{2,1}}$ in M_2 (see definition of right-structure), including s_0, the set $AP(\gamma_{2,2})$ (see Figure 8).

It easy to see that after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$ still hold. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, for every multi-path Π in M_2, $\Pi(1)$ cannot be a counterexample for $\gamma_{1,1}$, since each state of M_2 except contains the set $AP(\gamma_{1,1})$. Finally, no counterexample for γ_2 is in M_1. Indeed, a counterexample for γ_2 must contain a counterexample for $\gamma_{2,2}$. However, this is impossible, since $\gamma_{2,2}$ is globally true in M_1. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5 a counterexample for γ must involve counterexamples for γ_2.

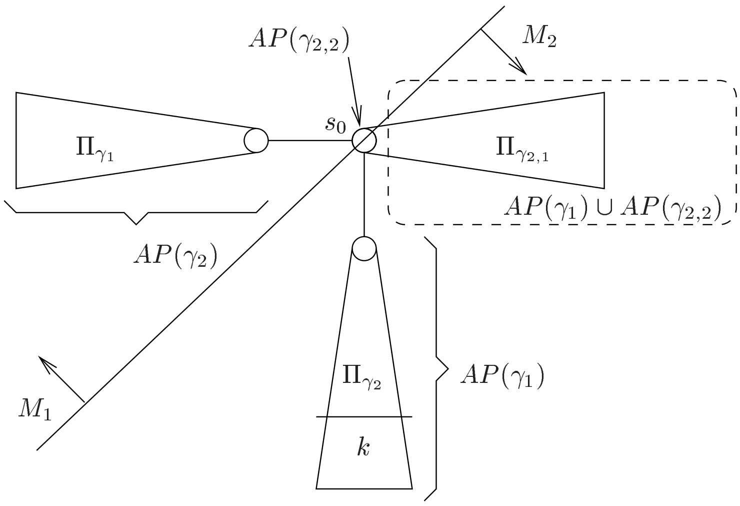

Figure 8: The $\mathbf{X}$-$\mathbf{V}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{V} \gamma_{2,2})$

Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. Clearly, this concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample involving only counterexamples for γ_2. By Definition 3.5, Π is such that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, Π cannot lead into Π_{γ_2}, since it is a k-structure of γ_2. On the other hand, it cannot lead into M_1 or $\Pi_{\gamma_{2,1}}$, since a counterexample for γ_2 must contain a counterexample for $\gamma_{2,2}$, and $\gamma_{2,2}$ is globally true in $\Pi_{\gamma_{2,1}}$. Hence, every counterexample for γ in M is not deterministic.

• $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{U} \gamma_{2,2})$. We modify M as follows. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$, and to every state of M_2 except s_0 the set $AP(\gamma_1)$. Finally, we add in every state of $\Pi_{\gamma_{2,2}}$ in M_2 including s_0 the set $AP(\gamma_{2,1})$ (see Figure 9).

It easy to see that after these additions $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$ still hold. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, for every multi-path Π in M_2, $\Pi(1)$ cannot be a counterexample for $\gamma_{1,1}$, since each state of M_2 except s_0 contains the set $AP(\gamma_{1,1})$. Finally, no counterexample for γ_2 is in M_1. Indeed, since each state of M_1 contains $AP(\gamma_{2,1})$, a counterexample for γ_2 in M_1 could only be a multi-path Π such that $\Pi(i)$ is a counterexample for $\gamma_{2,2}$, for each $i \geq 0$. But this is impossible, since for every multi-path Π in M_1, each state appearing in $\Pi(i)$, for $i \geq 1$ contains $AP(\gamma_{2,2})$. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. Definition 3.5 request that a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample for γ such that $\Pi(i)$ is a counterexample for γ_2, for every $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, it can neither lead into M_1 nor into Π_{γ_2}, since this is a k-structure of γ_2. Furthermore, it cannot lead into $\Pi_{\gamma_{2,2}}$. Indeed, a counterexample for γ_2 cannot involve a counterexample for $\gamma_{2,1}$ as $\Pi_{\gamma_{2,2}}$ contains in each state the set $AP(\gamma_{2,1})$. Thus, such a counterexample could only be a multi-path Π such that $\Pi(i)$ is a (deterministic) counterexample for $\gamma_{2,2}$, for each $i \geq 0$. But this is not possible, since $\Pi_{\gamma_{2,2}}$ is a k-structure of $\gamma_{2,2}$. Hence, no counterexample for γ in M is deterministic.

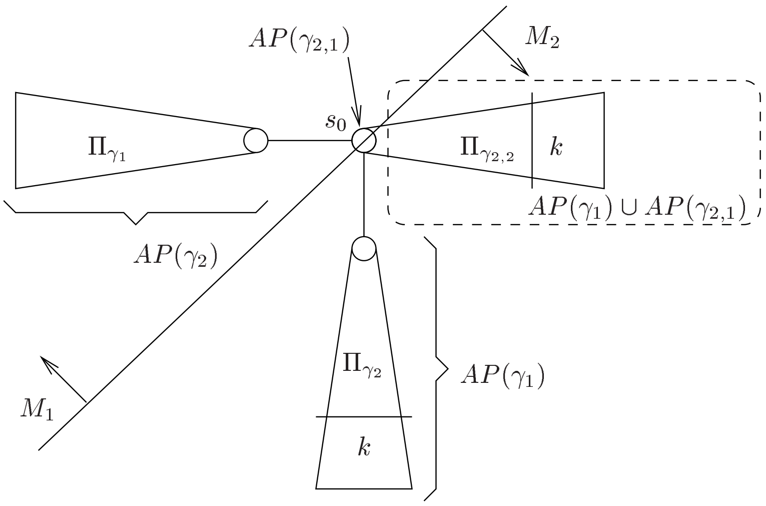

Figure 9: The $\mathbf{X}$-$\mathbf{U}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{U} \gamma_{2,2})$

• $\gamma_1 = \mathbf{A}(\gamma_{1,1} \mathbf{V} \gamma_{1,2})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$. We modify M as follows. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$ and to every state of M_2 except s_0 the set $AP(\gamma_1)$. Moreover, we add to s_0 the set $AP(\gamma_{1,2})$. Finally, we add in every other state of $\Pi_{\gamma_{1,1}}$ in M_1 (see definition of left-structure), the set $AP(\gamma_{1,2})$ (see Figure 10).

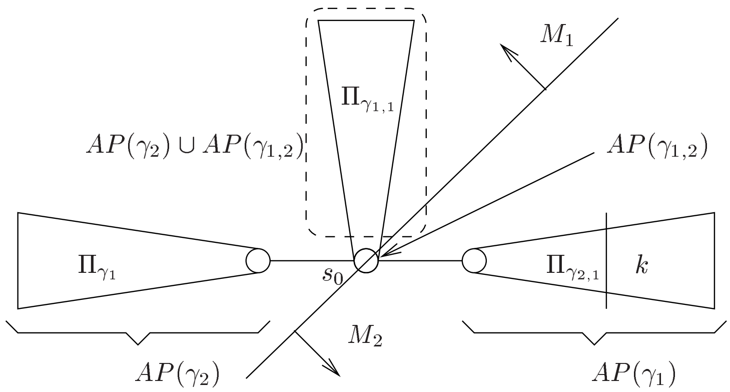

Figure 10: The $\mathbf{V}$-$\mathbf{X}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1} \mathbf{V} \gamma_{1,2})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$

After these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$ still hold. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_2 is in M_1. Indeed, for every multi-path Π in M_1, $\Pi(1)$ cannot be a counterexample for $\gamma_{2,1}$, since each state of M_1 except s_0 contains the set $AP(\gamma_{2,1})$. Finally, no counterexample for γ_1 is in M_2. Indeed, a counterexample for γ_1 must contain a counterexample for $\gamma_{1,2}$, but this is impossible, since each state in M_2 contains $AP(\gamma_{1,2})$. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5, a counterexample for γ must involve counterexamples for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample involving only counterexamples for γ_2. Definition 3.5 implies that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, Π cannot lead into M_1 and not into M_2, since $\Pi_{\gamma_{2,1}}$ is a k-structure of $\gamma_{2,1}$. This proves the statement.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$. We modify M as follows. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$. Then, we add to every state of M_2 except s_0 the set $AP(\gamma_1)$. Moreover, we add to s_0 the set $AP(\gamma_{1,2})$. Finally, we add in every state of $\Pi_{\gamma_{2,1}}$ in M_2, including s_0, the set $AP(\gamma_{2,2})$ (see Figure 11).

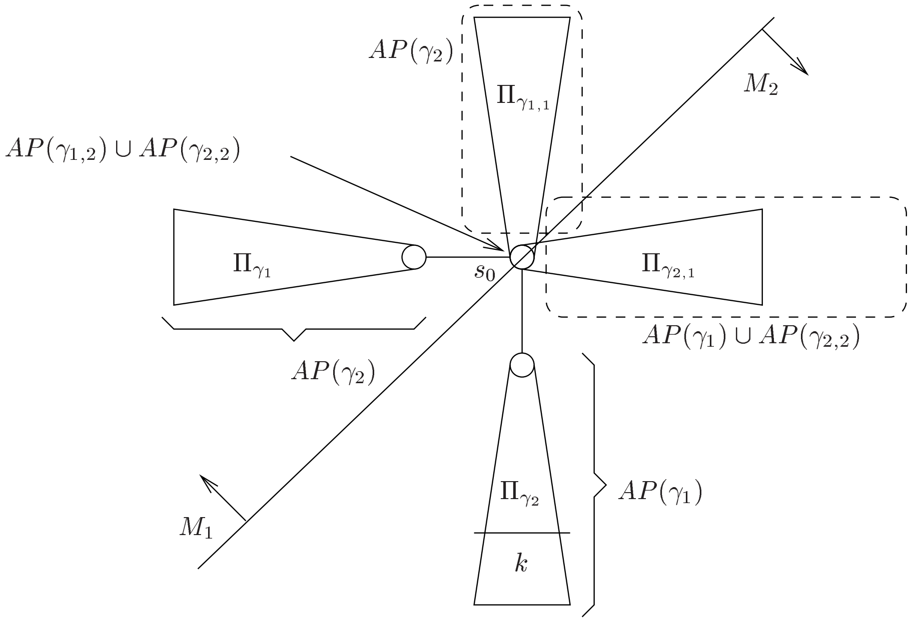

Figure 11: The $\mathbf{V}$-$\mathbf{V}$ case: $\mathbf{A}(\gamma_1\mathbf{U}\gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$

It easy to see that, also after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, $\gamma_{1,2}$ is globally true in M_2. Similarly, no counterexample for γ_2 is in M_1. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic.

By Definition 3.5, a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample for γ_2 such that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, Π cannot lead into M_1, and it cannot lead into Π_{γ_2} since it is a k-structure of γ_2. On the other hand, it cannot lead into $\Pi_{\gamma_{2,1}}$, since a counterexample for γ_2 must contain a counterexample for $\gamma_{2,2}$ and $\gamma_{2,2}$ is globally true in $\Pi_{\gamma_{2,1}}$. Hence, every counterexample for γ in M is not deterministic.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. We modify M as follows. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$. Then, we add to every state of M_2 except s_0 the set $AP(\gamma_1)$. Moreover we add to s_0 the set $AP(\gamma_{1,2}) \cup AP(\gamma_{2,1})$. Finally, we add in every other state of $\Pi_{\gamma_{2,2}}$ in M_2 the set $AP(\gamma_{2,1})$ (see Figure 12).

It easy to see that, also after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, a counterexample for γ_1 must contain a counterexample for $\gamma_{1,2}$.

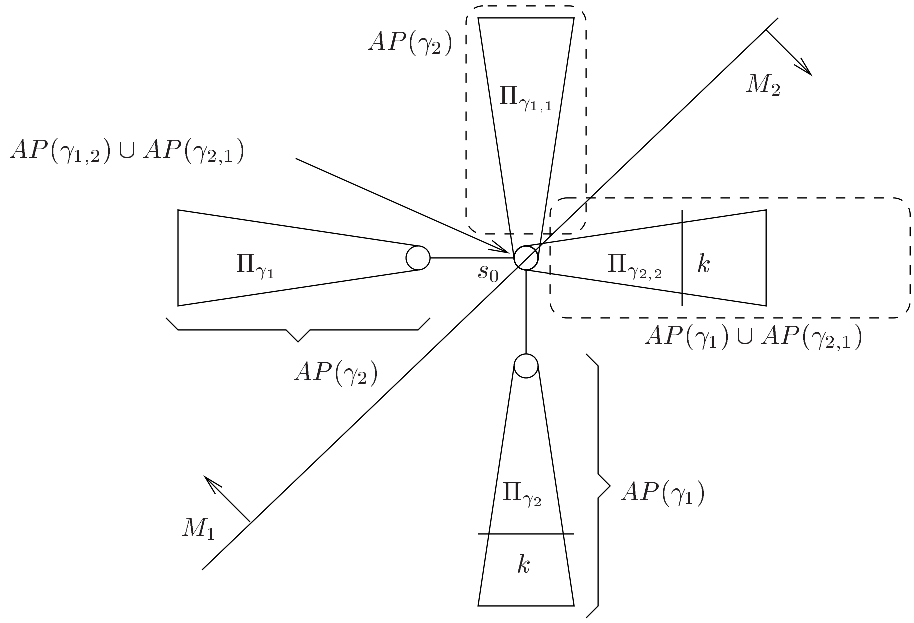

Figure 12: The $\mathbf{V}$-$\mathbf{U}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1} \mathbf{V} \gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{U} \gamma_{2,2})$

But this is impossible, since each state in M_2 contains $AP(\gamma_{1,2})$. Finally, no counterexample for γ_2 is in M_1. Indeed, since each state of M_1 contains the set $AP(\gamma_{2,1})$, a counterexample for γ_2 in M_1 could only be a multi-path Π such that each element $\Pi(i)$ is a counterexample for $\gamma_{2,2}$, for each $i \geq 0$. But this is impossible, since $\gamma_{2,2}$ is globally true in M_1.

Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5 a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is such a deterministic counterexample, i.e., $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, it cannot lead into Π_{γ_2}, since this is a k-structure of γ_2. On the other hand, it cannot lead into $\Pi_{\gamma_{2,2}}$. Indeed, a counterexample for γ_2 cannot involve a counterexample for $\gamma_{2,1}$ as $\Pi_{\gamma_{2,2}}$ contains in each state the set $AP(\gamma_{2,1})$. Thus, such a counterexample could only be a multi-path Π such that $\Pi(i)$ is a (deterministic) counterexample for $\gamma_{2,2}$, for each $i \geq 0$. But this is not possible, since $\Pi_{\gamma_{2,2}}$ is a k-structure of $\gamma_{2,2}$. Hence, no counterexample for γ in M is deterministic.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1} \mathbf{U} \gamma_{1,2})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$. We modify M in the following way. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$ and to every state of M_2 except s_0 the set $AP(\gamma_1)$. Finally, we add in every state of $\Pi_{\gamma_{1,2}}$ in M_1 the set $AP(\gamma_{1,1})$ (see Figure 13).

It easy to see that, also after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_2 is in M_1. Indeed, for every multi-path Π in M_1, $\Pi(1)$ cannot be a counterexample for $\gamma_{2,1}$, since each state of M_1 except s_0 contains the set $AP(\gamma_{2,1})$. Finally, no counterexample for γ_1 is in M_2. Indeed, since each state of M_2 contains the set $AP(\gamma_{1,1})$, a counterexample for γ_1 in M_2 could only be a multi-path Π such that each element $\Pi(i)$ is a counterexample for $\gamma_{1,2}$, for each $i \geq 0$. But this is impossible, since for every multi-path Π in M_2, each state appearing in $\Pi(i)$ contains the set $AP(\gamma_{1,2})$,

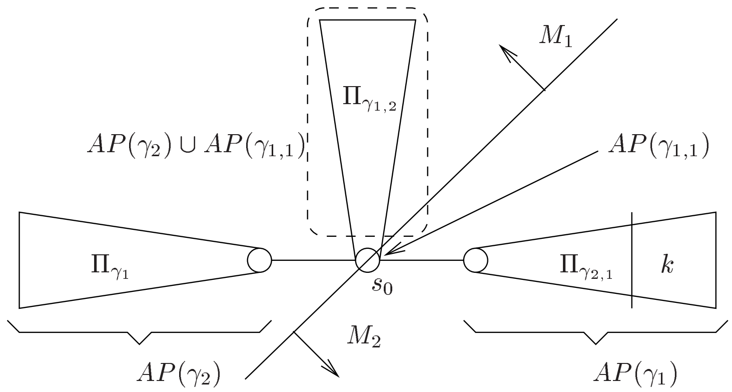

Figure 13: The $\mathbf{U}$-$\mathbf{X}$ case: $\mathbf{A}(\gamma_1\mathbf{U}\gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$

for each $i \geq 1$. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5 a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample such that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, Π cannot lead into M_1, since γ_2 is globally true in M_1, and it cannot lead into M_2, since $\Pi_{\gamma_{2,1}}$ is a k-structure of $\gamma_{2,1}$. Thus, the statement is proven.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$. We modify M in the following way. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$. Then, we add to every state of M_2 except s_0 the set $AP(\gamma_1)$. Moreover, we add to s_0 the set $AP(\gamma_{1,1}) \cup AP(\gamma_{2,2})$. Finally, we add to every other state of $\Pi_{\gamma_{2,1}}$ in M_2 the set $AP(\gamma_{2,2})$ (see Figure 14).

It easy to see that after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$ hold. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, $\gamma_{1,1}$ is globally true in M_2 and for every multi-path Π in M_2, $\Pi(i)$, for $i \geq 1$, cannot be a counterexample for $\gamma_{1,2}$, since each state of M_2 except s_0 contains the set $AP(\gamma_{1,2})$. Finally, no counterexample for γ_2 is in M_1. Indeed, $\gamma_{2,2}$ is globally true in M_1. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5, a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, suppose Π is a deterministic counterexample for γ such that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. Such a counterexample cannot be deterministic. Indeed, Π can neither lead into M_1 (cf. above) nor into $\Pi_{\gamma_{2,1}}$, since a counterexample for γ_2 must contain a counterexample for $\gamma_{2,2}$ which is globally true in $\Pi_{\gamma_{2,1}}$. Furthermore, Π cannot lead into Π_{γ_2}, since it is a k-structure of γ_2. Hence, no counterexample for γ in M is deterministic.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. We modify M in the following way. We add to every state of M_1 except s_0 the set $AP(\gamma_2)$ and to every state of M_2 except s_0 the set $AP(\gamma_1)$. Moreover, we add in s_0 the set $AP(\gamma_{1,1}) \cup AP(\gamma_{2,1})$. Finally, we add in every other state of $\Pi_{\gamma_{2,2}}$ in M_2 (see definition of right-structure) the set $AP(\gamma_{2,1})$ (see Figure 15).

It easy to see that after these additions, $M_1 \not\models \gamma_1$ and $M_2 \not\models \gamma_2$ hold. Thus, $M \not\models \gamma$. Moreover, no counterexample for γ_1 is in M_2. Indeed, $\gamma_{1,1}$ is globally true in M_2 and for every multi-path Π in M_2, $\Pi(i)$,

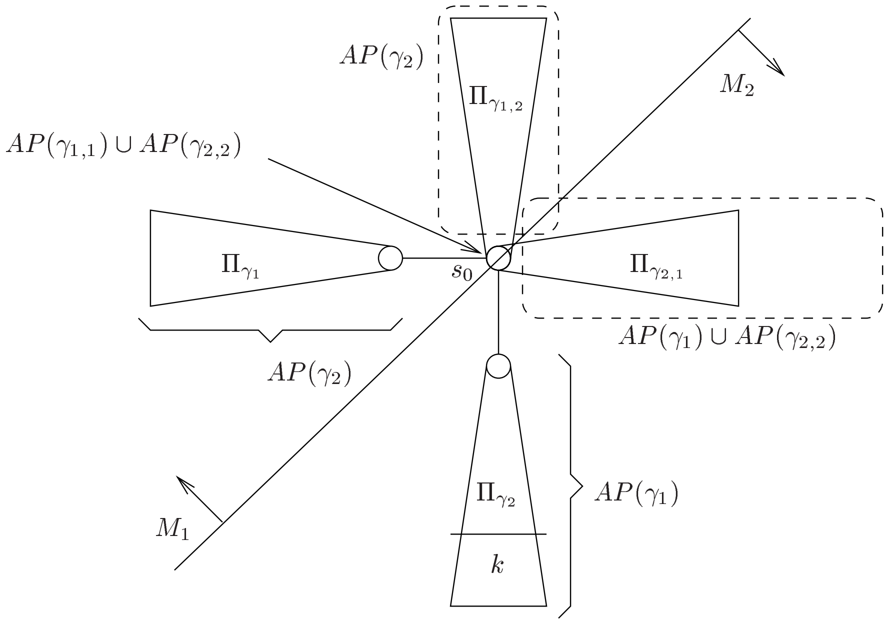

Figure 14: The $\mathbf{U}$-$\mathbf{V}$ case: $\mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1} \mathbf{U} \gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{V} \gamma_{2,2})$

for $i \geq 1$, cannot be a counterexample for $\gamma_{1,2}$, since each state of M_2 except s_0 contains the set $AP(\gamma_{1,2})$. Similarly, no counterexample for γ_2 is in M_1. Hence, a counterexample for γ involving counterexamples for both γ_1 and γ_2 cannot be deterministic. By Definition 3.5, a counterexample for γ must involve a counterexample for γ_2. Now we show that every counterexample for γ involving only counterexamples for γ_2 is not deterministic. This, clearly, concludes the proof. Towards a contradiction, let Π be a deterministic counterexample for γ such that $\Pi(i)$ is a counterexample for γ_2, for each $i \geq 0$. But such a counterexample cannot be deterministic. Indeed, Π cannot lead into M_1, and furthermore, it cannot lead into Π_{γ_2}, since this is a k-structure of γ_2. Finally, it also cannot lead into $\Pi_{\gamma_{2,2}}$. Indeed, a counterexample for γ_2 cannot involve a counterexample for $\gamma_{2,1}$, as $\Pi_{\gamma_{2,2}}$ contains in each state the set $AP(\gamma_{2,1})$. Thus, such a counterexample could only be a multi-path Π such that $\Pi(i)$ is a (deterministic) counterexample for $\gamma_{2,2}$, for each $i \geq 0$. But this is not possible, since $\Pi_{\gamma_{2,2}}$ is a k-structure of $\gamma_{2,2}$. Hence, every counterexample for γ in M is not deterministic.

(2) The second case is $\gamma = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$, where $\gamma_1^\star = \mathbf{A}\psi_1^\star \notin \mathcal{PSF}$ and either $\gamma_2^\star = \mathbf{A}\psi_2^\star \in \mathbf{DET}$ or $\gamma_2^\star \in \mathcal{PSF}$.

In this case, we consider all possible shapes of the template $\gamma_1^\star$. In each case, we construct a structure M such that both $M \not\models \gamma$ and each counterexample for γ in M is not deterministic. The structure M is obtained by a modification of the structure M_γ which we define next.

Let M' be a single-path structure as stated in Lemma 6.2 for formula γ_2. Thus, $M' \models \gamma_2$. Furthermore, there exists an index $k \geq 1$ such that $\pi(M')^k$ is a local counterpath for γ_2 (resp., γ_2 is false in $\pi(M')(k)$). Without loss of generality, k is the least index having this property. Denote by $s_i = \pi(M')(i)$, for $i = 0, \ldots, k$, the first $k+1$ states appearing in $\pi(M')$. Note that the s_i (hence also the suffixes $\pi(M')^i$) are pairwise distinct. Furthermore, s_k is the initial state of a structure M^+ induced by s_k in M' (i.e., the suffix $\pi(M')^k$) such that $M^+ \not\models \gamma_2$.

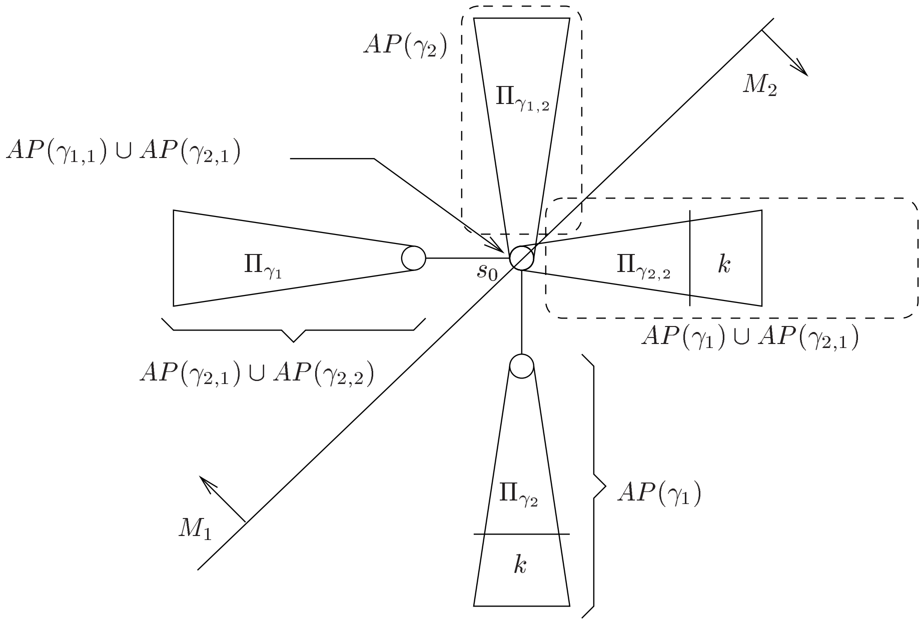

Figure 15: The $\mathbf{U}$-$\mathbf{U}$ case: $\mathbf{A}(\gamma_1\mathbf{U}\gamma_2)$, where $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$

Let M_0 be a left-structure for γ_1. We take copies $M_1, \ldots, M_{k-1}$ and repeatedly take the fusion of M_i with the substructure of M' induced by the state s_i in M', for $i = 0, \ldots, k-1$. The repeatedly so revised structure M' is the desired structure M_γ with initial state s_0 (cf. Figure 16).

We now consider the possible types of $\gamma_1^\star$.

• $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$, i.e., $\gamma = \mathbf{A}(\mathbf{AX}(\gamma_{1,1})\mathbf{V}\gamma_2)$. To construct M, we modify the above structure M_γ as follows. Include in the label of each state not appearing in $\pi(M')^k$ the set $AP(\gamma_2)$. Note that this addition does not affect the existence of (local) counterexamples for γ_1 starting at $s_0, s_1, \ldots, s_{k-1}$, since $AP(\gamma_1)$ and $AP(\gamma_2)$ are disjoint. Finally, we add the set $AP(\gamma_1)$ in every state of M' (thus, to each state appearing in $\pi(M')$). This addition preserves the existence of counterexamples for γ_1 starting with $s_0, s_1, \ldots, s_{k-1}$, since γ_1 involves the next-time operator. Furthermore, $\pi(M')^k$ is still a local counterpath for γ_2, since $AP(\gamma_1)$ and $AP(\gamma_2)$ are disjoint. The resulting conic structure with initial state s_0 is M (see Figure 16).

We can see that $M \not\models \gamma$. Indeed, there exists a multi-path Π_2, such that $\Pi_2(i)$ is a l-counterexample for γ_1, for $0 \leq i \leq k-1$ (recall that each state s_i is origin of a l-counterexample for γ_1), and $\Pi_2(k)$ is a local counterexample for γ_2 with main path $\pi(M')^k$. Clearly, this multi-path is not deterministic. Moreover, no deterministic counterexample for γ is in M. Indeed, each counterexample for γ needs a counterexample for γ_2. But all paths starting with the initial state s_0 cannot be a local counterpath for γ_2. Indeed, each path π not reaching states beyond s_k cannot be a counterpath for γ_2, since the label of each state appearing in π would contain the set $AP(\gamma_2)$. On the other hand, the only path starting with s_0 and reaching s_k is $\pi(M')$. However, as M' was chosen according to Lemma 6.2, this path cannot be a counterpath for γ_2. Hence, we need a counterexample whose first element is a counterexample for γ_1. Clearly, we cannot find a counterexample for γ_1 along the path $\pi(M')$, since each state in it contains $AP(\gamma_1)$. Hence, each counterexample for γ necessarily contains branching, that is, it is not deterministic.

• $\gamma_1^\star = \mathbf{A}(\gamma_{1,1}^\star\mathbf{V}\gamma_{1,2}^\star)$. Then, $\gamma = \mathbf{A}(\mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})\mathbf{V}\gamma_2)$. To construct M, we modify the above structure

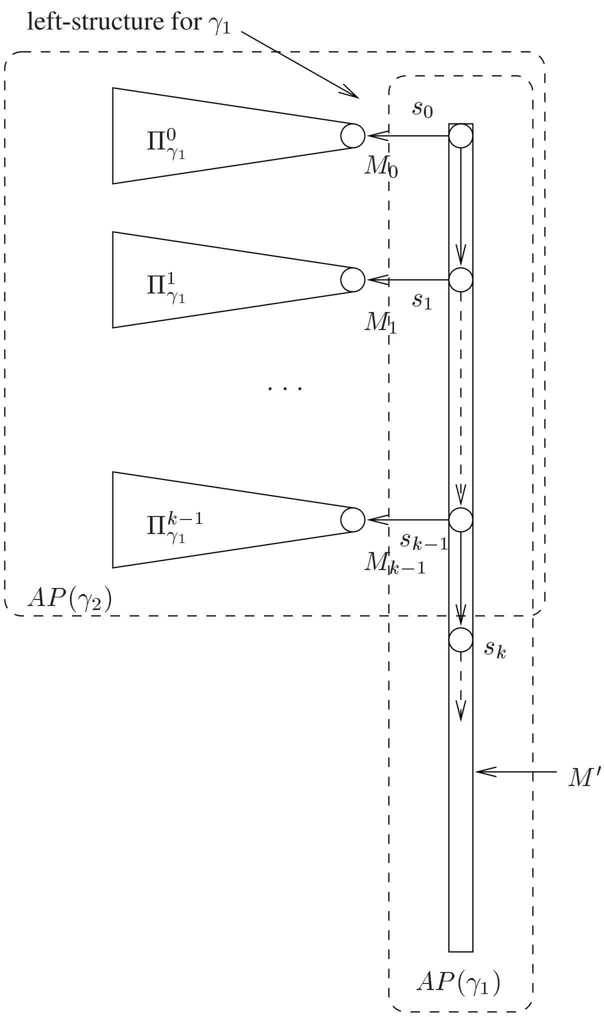

Figure 16: Nesting into unless, the $\mathbf{X}$ case: $\gamma = \mathbf{A}(\mathbf{A}\mathbf{X}(\gamma_{1,1})\mathbf{V}\gamma_2)$

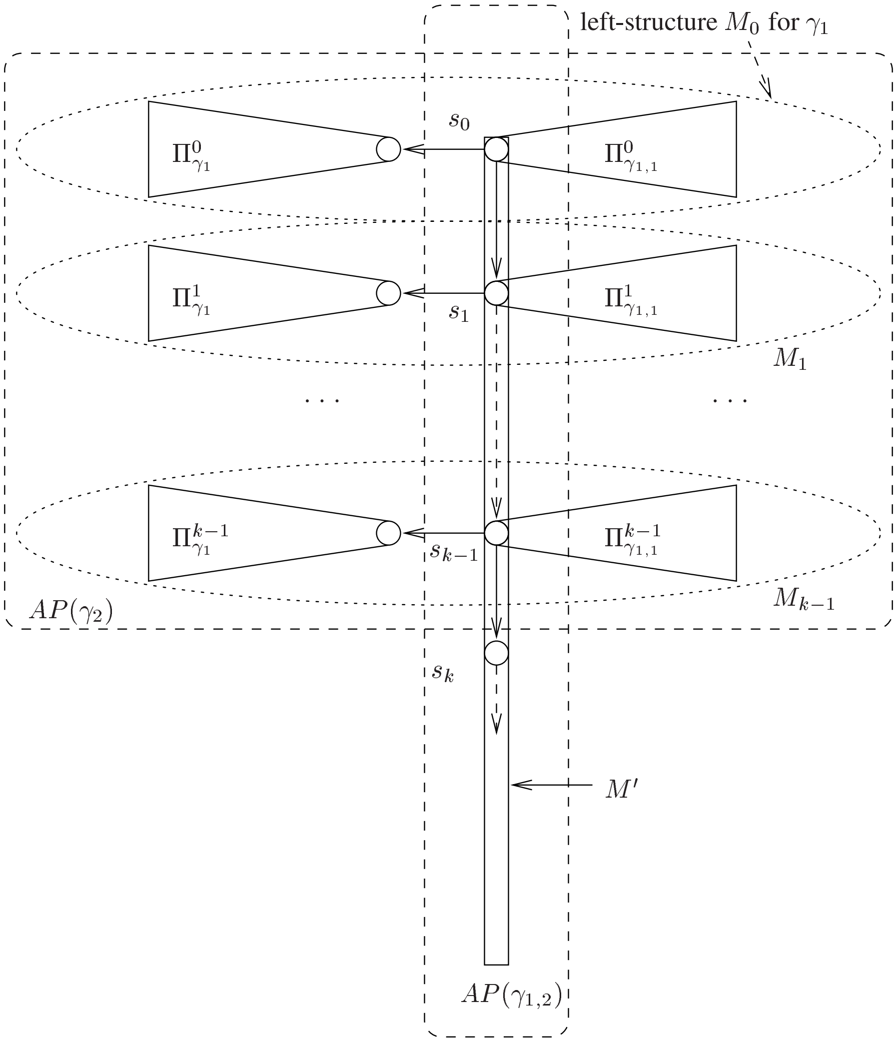

Figure 17: Nesting into unless, the $\mathbf{V}$ case: $\gamma = \mathbf{A}(\mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})\mathbf{V}\gamma_2)$

M_γ as follows. We add in each state not appearing in $\pi(M')^k$ the set $AP(\gamma_2)$. Note that this addition does not affect the existence of counterexamples for γ_1 starting with $s_0, s_1, \ldots, s_{k-1}$, since $AP(\gamma_1)$ and $AP(\gamma_2)$ are disjoint. Finally, we add the set $AP(\gamma_{1,2})$ in every state appearing in $\pi(M')$. This addition preserves the existence of counterexamples for $\gamma_{1,1}$ (hence, for γ_1) starting with $s_0, s_1, \ldots, s_{k-1}$. Furthermore, $\pi(M')^k$ is still a local counterpath for γ_2, since $AP(\gamma_2)$ and $AP(\gamma_{1,2})$ are disjoint. The resulting conic structure with initial state s_0 is M (see Figure 17).

We can see that $M \not\models \gamma$. Indeed, there exists a multi-path Π_2, such that $\Pi_2(i)$ is a l-counterexample for γ_1, for $0 \leq i \leq k-1$ (recall that each state s_i is origin of a l-counterexample for γ_1), and $\Pi_2(k)$ is a local counterexample for γ_2 with main path $\pi(M')^k$. Clearly, this multi-path is not deterministic. Moreover, no deterministic counterexample for γ in M exists. Indeed, each counterexample for γ needs a counterexample for γ_2. It holds that every path starting at s_0 cannot be a counterpath for γ_2. Indeed, each path π not reaching the state s_k cannot be a counterpath for γ_2, since the label of each state appearing in π would contain the set

$AP(\gamma_2)$.

On the other hand, the only path starting at s_0 and reaching s_k is $\pi(M')$. As M' was chosen according to Lemma 6.2, this path cannot be a counterpath for γ_2 by construction. Hence, we need a counterexample such that the first element is a counterexample for γ_1. Clearly, we cannot find a counterexample for γ_1 along the path $\pi(M')$, since each state in it contains $AP(\gamma_{1,2})$ (and a counterexample for γ_1 necessarily contains a counterexample for $\gamma_{1,2}$). Hence, each counterexample for γ necessarily contains branching, that is, it is not deterministic.

• $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$, i.e., $\gamma = \mathbf{A}(\mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})\mathbf{V}\gamma_2)$. We modify the structure M_γ from above as follows. We add to each state not appearing in $\pi(M')^k$ the set $AP(\gamma_2)$. Note that this addition does not affect the existence of local counterexamples for γ_1 starting at $s_0, s_1, ..., s_{k-1}$, since $AP(\gamma_1)$ and $AP(\gamma_2)$ are disjoint. Furthermore, add the set $AP(\gamma_{1,1})$ in every state appearing in $\pi(M')$. This addition preserves the existence of counterexamples for $\gamma_{1,2}$ (hence for γ_1) starting at $s_0, s_1, ..., s_{k-1}$. Finally, we add in every state appearing in $\pi(M)^k$ the set $AP(\gamma_{1,2})$. Clearly, after this addition $\pi(M')^k$ is still a local counterpath for γ_2, since $AP(\gamma_1)$ and $AP(\gamma_2)$ are disjoint. The resulting conic structure with initial state s_0 is M (see Figure 18).

We can see that $M \not\models \gamma$. Indeed, there exists a multi-path Π_2, such that $\Pi_2(i)$ is a l-counterexample for γ_1, for $0 \leq i \leq k-1$, and $\Pi_2(k)$ is a counterexample for γ_2 with main path $\pi(M')^k$. Clearly, this multi-path is not deterministic. Moreover, no deterministic counterexample for γ exists in M. Indeed, each counterexample for γ needs a counterexample for γ_2. Every path π starting at the initial state s_0 cannot be a counterpath for γ_2. Indeed, if π does not reach the state s_k, it cannot be a counterpath for γ_2, since the label of each state appearing in π would contain the set $AP(\gamma_2)$. On the other hand, the only path starting at s_0 and reaching s_k is $\pi(M')^k$. Since M' was chosen according to Lemma 6.2, it is not a counterpath for γ_2. Hence, we need a counterexample whose first element is a counterexample for γ_1. Clearly, we cannot find a counterexample for $\gamma_{1,1}$ along the path $\pi(M')$, since each state in it contains the set $AP(\gamma_{1,1})$. Hence, a counterexample for γ_1 could only be a multi-path Π such that $\Pi(i)$ is a counterexample for $\gamma_{1,2}$, for each $i \geq 0$. But such a counterexample cannot be found along the path $\pi(M')$. Indeed, along its suffix $\pi(M')^k$ the formula $\gamma_{1,2}$ is always true.

Hence, each counterexample for γ necessarily contains branching, that is, it is not deterministic.

This concludes the proof for the case in which $\gamma_1^\star$,$\gamma_2^\star$ have form $\mathbf{A}\psi$ or $\gamma_2^\star \in \mathcal{PSF}$.

For the case of a general $\gamma_1^\star$, we observe that Lemma 6.1 can be exploited: the instantiation γ_1 is a monotone Boolean combination of positive disjoint instantiations $\gamma_{1,1}, \ldots, \gamma_{1,m}$ (each of which occurs only once) such that w.l.o.g. $\gamma_{1,1}$ is of the form $\mathbf{A}\psi$. We proceed then for γ_1 as for $\gamma_{1,1}$, but use the structure M from Lemma 6.1 for $\phi = \gamma_1$ instead of the structure M^+ for $\phi^+ = \gamma_{1,1}$ (observe that M^+ can always be chosen such that $R(M^+)$ is total). For the general case of γ_2, we proceed analogously. This proves the result. □

Theorem 6.6 *Let γ be any positive disjoint instantiation of a template $\gamma^\star \in \mathbf{T}^\star$. If $\gamma^\star \notin \mathbf{DET}$, then γ is not c-deterministic.*

Proof. We proceed by induction on the number of universal quantifiers $\mathbf{A}$ appearing in γ, which is denoted by $n_{\mathbf{A}}(\gamma)$.
(Basis) The case $n_{\mathbf{A}}(\gamma) = 0$ is trivial, since $\gamma^\star$ belongs to $\mathcal{PSF} \subseteq \mathbf{DET}$.
(Induction) Assume that the statement is true for every γ such that $n_{\mathbf{A}}(\gamma) < k$. We have to show that each positive disjoint instantiation γ of $\gamma^\star \in \mathbf{T}^\star \setminus \mathbf{DET}$ such that $n_A(\gamma) = k$ is not c-deterministic, i.e., that there is a structure M such that both $M \not\models \gamma$ and each counterexample for γ in M is not deterministic.

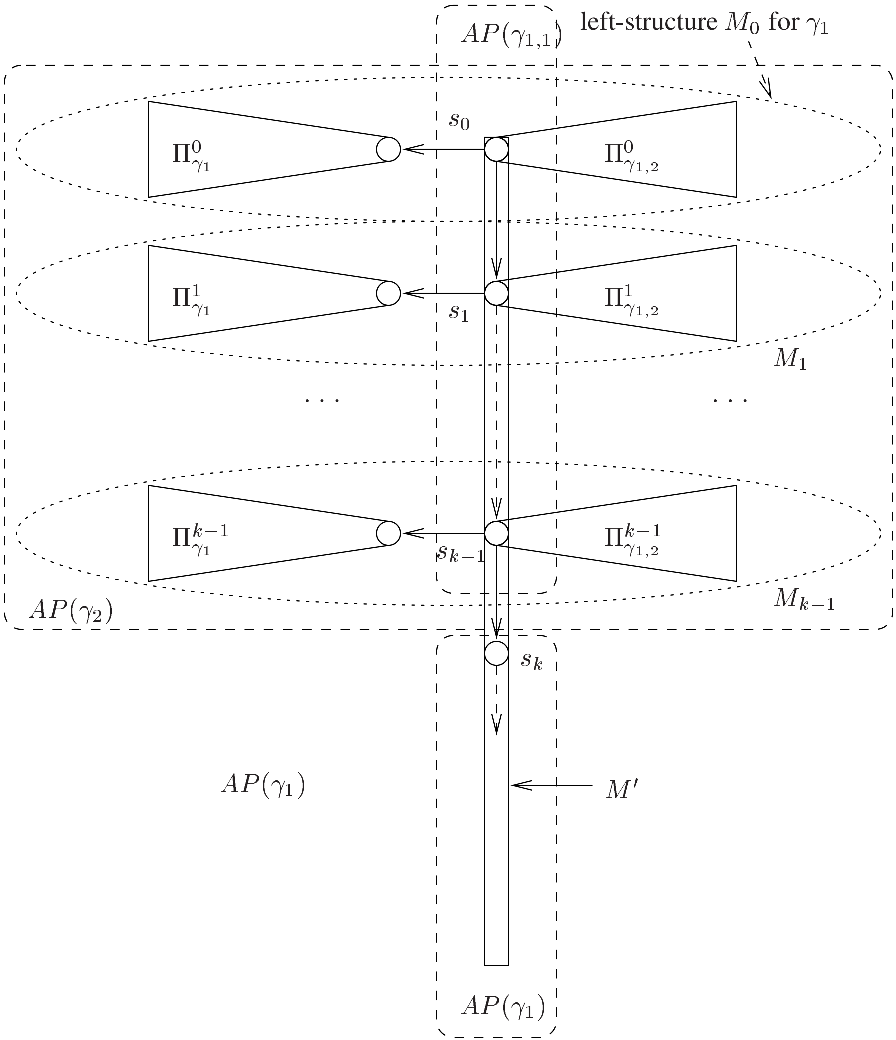

Figure 18: Nesting into unless, the $\mathbf{V}$ case: $\gamma = \mathbf{A}(\mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})\mathbf{V}\gamma_2)$

The formula γ is either of the form $\mathbf{A}\psi$, or a Boolean combination of formulas $\gamma_1, \ldots, \gamma_m$. We consider the possible cases.

• $\gamma = \mathbf{AX}\phi$, where $n_{\mathbf{A}}(\phi) = k-1$. By Definition 4.7, $\gamma^\star \notin \mathbf{DET}$ if and only if $\phi^\star \notin \mathbf{DET}$. Thus, since $n_{\mathbf{A}}(\phi) = k-1$, the induction hypothesis implies that ϕ is not c-deterministic. Hence, there exists a structure M' such that both $M' \not\models \phi$ and no counterexample for ϕ in M' is deterministic. Without loss of generality, M' is conic and has the initial state s_0'. Let the conic structure M with initial state s_0 result by connecting a new state s_0 to M' via the transition (s_0, s_0'). Clearly, $M \not\models \gamma$. Furthermore, each counterexample Π for γ is such that $\Pi(1)$ is a counterexample for ϕ. Since $or(\Pi(1)) = s_0'$, $\Pi(1)$ cannot be deterministic, by hypothesis. Hence, Π is not deterministic.

• $\gamma = \mathbf{A}(\gamma_1 \mathbf{V} \gamma_2)$, where $n_{\mathbf{A}}(\gamma_1) + n_{\mathbf{A}}(\gamma_2) = k-1$. By the definition of $\mathbf{DET}$, the following two cases cover each γ such that $\gamma^\star \notin \mathbf{DET}$:

1. $\gamma_1^\star \notin \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{DET}$. This case has been already proven in Lemma 6.5.
2. $\gamma_2^\star \notin \mathbf{DET}$. By the induction hypothesis, γ_2 is not c-deterministic. Thus, there exists a structure M such that $M \not\models \gamma_2$ and no counterexample in M is deterministic. We modify M by adding in each state the set $AP(\gamma_1)$. Clearly, no local counterexamples for γ_1 can be found in M. However, $M \not\models \gamma$. Moreover, each counterexample for γ in M must start with a counterexample for γ_2. Hence, it is not deterministic.

• $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, where $n_{\mathbf{A}}(\gamma_1) + n_{\mathbf{A}}(\gamma_2) = k-1$. Due to the intricate possibilities of nesting into an until from $\mathbf{DET}$, this case requires a careful analysis of several subcases. The following cases exhaust each possibility of $\gamma^\star \notin \mathbf{DET}$:

1. $\gamma_1^\star \notin \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{DET} \setminus \mathcal{PSF}$;
2. $\gamma_1^\star \notin \mathbf{DET}$ and $\gamma_2^\star \in \mathcal{PSF}$;
3. $\gamma_2^\star \notin \mathbf{DET}$;
4. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{AX}(\mathbf{DET})$;
5. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{AV}(\mathcal{PSF}, \mathbf{DET})$;
6. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in S_2^\infty \wedge S_2^\infty$;
7. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathcal{PSF} \wedge S_2^\infty \cup S_2^\infty \wedge \mathcal{PSF}$.

We now consider these cases.

1. $\gamma_1^\star \notin \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{DET} \setminus \mathcal{PSF}$. This case has been already proven in Lemma 6.5.
2. $\gamma_1^\star \notin \mathbf{DET}$ and $\gamma_2^\star \in \mathcal{PSF}$. Since $\gamma_1^\star \notin \mathbf{DET}$, by the induction hypothesis a structure M exists such that $M \not\models \gamma_1$ and no counterexample for γ_1 in M is deterministic. Without loss of generality, M is conic with initial state s_0 and $AP(\gamma_2) \cap AP(M) = \emptyset$.

   Clearly, $M \not\models \gamma$, since $M \not\models \gamma_2$. Modify now M by adding to each state except s_0 the set $AP(\gamma_2)$. Since $AP(\gamma_1) \cap AP(\gamma_2) = \emptyset$, still $M \not\models \gamma_1$ holds. Moreover, since $L(M)(s_0) \cap AP(\gamma_2) = \emptyset$,

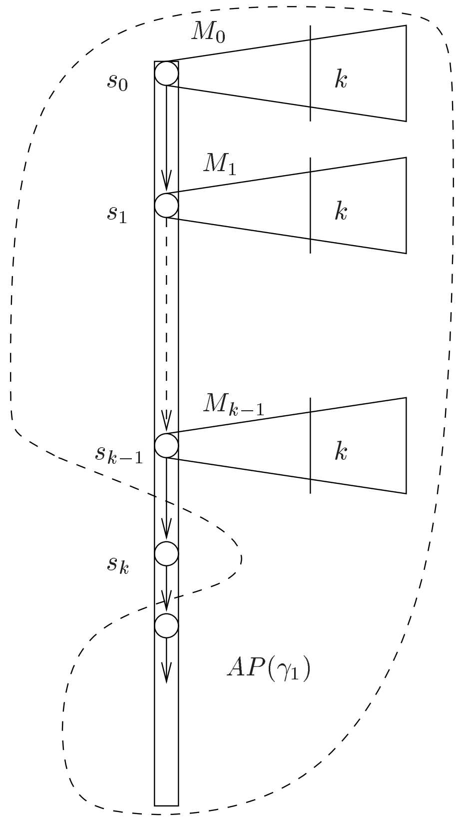

Figure 19: Nesting of $\mathcal{PSF}$ and $\mathbf{AX}(\mathbf{T}^\star)$ into until: $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \mathbf{AX}(\gamma_{2,1}))$.

also $M \not\models \gamma_2$ holds. Thus, $M \not\models \gamma$. It holds that each counterexample for γ in M must contain a counterexample for γ_1, and thus it is not deterministic. Indeed, in any alternative counterexample Π for γ the element $\Pi(i)$ would a local counterexample for γ_2, for every $i \geq 0$. Since all states of M except s_0 contain $AP(\gamma_2)$, this is impossible.

3. $\gamma_2^\star \notin \mathbf{DET}$. By the inductive hypothesis, there exists a structure M such that both $M \not\models \gamma_2$ and each counterexample for γ_2 in M is not deterministic. W.l.o.g., M is conic with initial state s_0 and $AP(\gamma_1) \cap AP(M) = \emptyset$.

   Clearly, $M \not\models \gamma$, where $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \gamma_2)$, since $M \not\models \gamma_1$ and $M \not\models \gamma_2$. We can conclude that each counterexample for γ in M is not deterministic. Indeed, if Π is a counterexample for γ in M, $\Pi(0)$ must be a l-counterexample for γ_2. Moreover $or(\Pi(0)) = s_0$. Hence, $\Pi(0)$ is a counterexample for γ_2 in M. Consequently, $\Pi(0)$ and hence also Π cannot be deterministic.

4. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{AX}(\mathbf{DET})$. Let M' be a single-path structure and $k \geq 1$ for formula γ_2 as described in Lemma 6.2. Thus, $M' \models \gamma_2$, and $\pi(M')^k$ is a local counterpath for γ_2 (resp., $M', \pi(M')(k) \not\models \gamma_2$). Let k w.l.o.g. be the least such index.

   Let $s_0, s_1, \ldots, s_k$ denote the first $k+1$ states appearing in $\pi(M')$. These s_i are pairwise distinct. Clearly, s_k is the first state of the suffix $\pi(M')^k$. We assume w.l.o.g. $L(M')(s_k) \cap AP(\gamma_1) = \emptyset$. Let

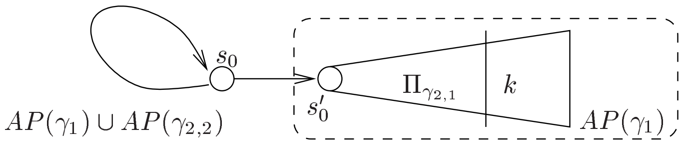

Figure 20: Nesting of $\mathcal{PSF}$ and $\mathbf{AV}(\mathbf{T}^\star)$ into until: $\gamma = \mathbf{A}(\gamma_1 \mathbf{U} \mathbf{A}(\gamma_{2,1} \mathbf{V} \gamma_{2,2}))$

M_0 be a $k-$structure for γ_2 such that the initial state has an empty label. Lemma 6.3 implies that such a M_0 exists; observe that $M_0 \not\models \gamma_2$. Let $M_1, \ldots, M_{k-1}$ be copies of M_0. For $i = 0, \ldots, k-1$ we repeatedly take the fusion of M_i with the structure induced by s_i in M'. Since the initial state of M_i has an empty label, these fusions do not change any label in M'. Finally, we add to every state except s_k the set $AP(\gamma_1)$. The resulting structure is the desired M (see Figure 19).

First observe that $M \not\models \gamma$. Indeed, each state s_i, for $0 \leq i \leq k$ is origin of a local counterexample for γ_2. Furthermore, s_k is also origin of a local counterexample for γ_1. It remains to show that no deterministic counterexample is in M. In any counterexample Π for γ the element $\Pi(0)$ must be a counterexample for γ_2. This implies that a counterpath for γ cannot reach state s_k. Indeed, the only path reaching state s_k is $\pi(M')$, which by construction is not a counterpath for γ_2. Thus, a counterpath π for γ could only lead into some structure M_i, where $0 \leq i \leq k-1$. However, in each M_i formula γ_1 is globally true. Hence π would have to satisfy that π^j, for each $j \geq 1$, is a local counterpath for γ_2. Since each M_i is a k-structure for γ_2, this is impossible. This proves that no deterministic counterexample for γ exists in M.

5. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathbf{AV}(\mathcal{PSF}, \mathbf{DET})$. Thus, $\gamma_2 = \mathbf{A}(\gamma_{2,1} \mathbf{V} \gamma_{2,2})$, where $\gamma_{2,1}$ is a pure state formula and $\gamma_{2,2}$ is c-deterministic by Theorem 5.1.

   Let M be a k-structure for γ_2 with initial state s'_0. Such a structure exists by Lemma 6.3, and w.l.o.g. $AP(M) \cap AP(\gamma_1) = \emptyset$. We modify M by adding a new initial state s_0 with empty label and the transitions (s_0, s'_0) and (s_0, s_0). Then, we add to each state the set $AP(\gamma_1)$ and to s_0 the set $AP(\gamma_{2,2})$ (see Figure 20).

   The path $[s_0, s'_0, ...]$ is a counterpath for γ_2. Thus, the multi-path $[[s_0, s'_0, ...], [s_0, s'_0 ...], ...]$ is a counterexample for the γ. It holds that no deterministic counterexample for γ exists in M. Indeed, since $AP(\gamma_1)$ is contained in each state, any counterexample for γ must contain infinitely many counterexamples for γ_2. Since s'_0 is the initial state of a k-structure for γ_2, no counterpath for γ is possible which reaches s'_0. Hence, the only possibility for a counterpath of γ is $\pi = [s_0, s_0, s_0, ...]$. Since s_0 contains $AP(\gamma_{2,2})$, this is impossible. Thus, non deterministic counterexample for γ exists.

6. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in S_2^\infty \wedge S_2^\infty$. Thus, $\gamma_2^\star = \phi_1 \wedge \phi_2$, where $\phi_1 = \mathbf{A}(\phi_{1,1} \mathbf{U} \phi_{1,2})$ and $\phi_2 = \mathbf{A}(\phi_{2,1} \mathbf{U} \phi_{2,2})$; moreover, each $\phi_{i,j}$, $i, j \in \{1, 2\}$ is an instantiation of a template in $\mathbf{DET}$.

   We construct the requested structure M in the following way. Let M' be a single-path structure as stated in Lemma 6.2 for formula ϕ_2. Thus, $M' \models \phi_2$. Furthermore, there exists an index $k \geq 1$ such that $\pi(M')^k$ is a local counterpath for ϕ_2 (and hence for γ_2). Let k w.l.o.g. be the least such index. Let $s_0, s_1, ..., s_k$, denote the first $k+1$ states appearing in $\pi(M')$; observe that they are pairwise distinct. Clearly, s_k is the first state of the suffix $\pi(M')^k$. Since γ is a positive disjoint instantiation, we can always assume that no atomic proposition from $AP(\gamma_1) \cup AP(\phi_1)$ occurs in any state of M'.

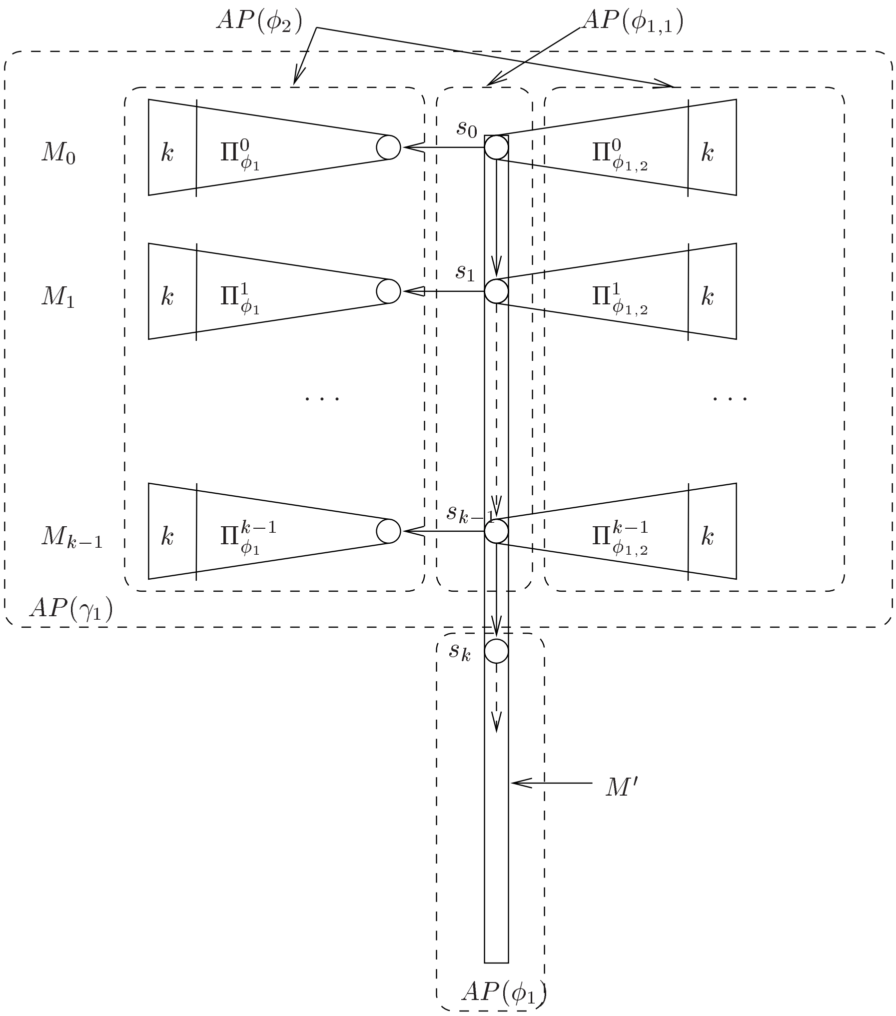

Figure 21: Right-Nesting of $S_2^\infty \wedge S_2^\infty$ into until: $\gamma = \mathbf{A}(\gamma_1 \mathbf{U}(\phi_1 \wedge \phi_2))$, where $\phi_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\phi_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$.

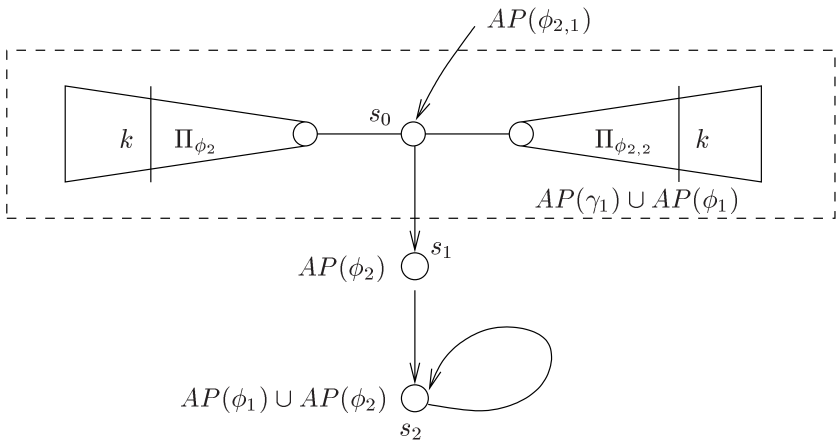

Figure 22: Right-Nesting of $\mathcal{PSF} \wedge S_2^{\infty}$ into until: $\gamma = \mathbf{A}(\gamma_1 \mathbf{U}(\phi_1 \wedge \phi_2))$, $\phi_2 = \mathbf{A}(\phi_{2,1}\mathbf{U}\phi_{2,2})$

Let M_0 be a right-structure for ϕ_1. Since $\phi_1^{\star} \in \mathbf{DET}$, such a structure exists (cf. Lemma 6.3). We remark that, by definition of right-structure, $M_0 \not\models \phi_1$. Let $M_1, \ldots, M_{k-1}$ be copies of M_0. For $i = 0, \ldots, k-1$ we repeatedly take the fusion of M_i and the structure induced by the state s_i in M'. Next, we add in every state $s_0, \ldots, s_{k-1}$ the set $AP(\phi_{1,1})$. Note that after this addition, each structure M_i still satisfies $M_i \not\models \phi_1$, for $i = 1, \ldots, k-1$. Indeed, since $AP(\phi_{1,1}) \cap AP(\phi_{1,2}) = \emptyset$ for $\Pi^i_{\phi_{1,2}}$, still $\Pi^i_{\phi_{1,2}} \not\models \phi_{1,2}$ holds.

Now we add in every state belonging to structures M_i, for $0 \leq i \leq k-1$, including states $s_0, ..., s_{k-1}$, the set $AP(\gamma_1)$. Since $AP(\gamma_1) \cap AP(\gamma_2) = \emptyset$, this has no effect on the properties of M_i described above. Moreover, we add in every state belonging to the structures M_i, for $0 \leq i \leq k-1$, except the states $s_0, ..., s_{k-1}$, the set $AP(\phi_2)$. Since $AP(\phi_1) \cap AP(\phi_2) = \emptyset$, this addition preserves the existence of counterexamples for ϕ_1 in the structures M_i. Finally, we add in every state occurring in the path $\pi(M')^k$, the set $AP(\phi_1)$. After this addition, $\pi(M')^k$ is still a local counterpath for formula ϕ_2. The resulting structure is the desired M (see Figure 21).

First observe that $M \not\models \gamma$. Indeed, each state s_i, for $0 \leq i \leq k-1$ is origin of a local counterexample for ϕ_1 and thus for γ_2. Furthermore, s_k is also origin of a local counterexample for ϕ_2, and then for γ_2. Moreover, s_k is a local counterexample for the formula γ_1.

Now we show that no deterministic counterexample for γ exists in M. By Definition 3.5, in any counterexample Π for γ the element $\Pi(0)$ must be a counterexample for γ_2. Hence, a counterpath for γ cannot reach state s_k. Indeed, the only path reaching state s_k is $\pi(M')$. This path is not a counterpath for γ_2 by construction: $\Pi(M')$ does not contain any local counterpath for ϕ_1, and, moreover, $\pi(M')$ is not an counterpath for ϕ_2. Thus, a counterpath π for γ could only lead into some structure M_i, where $0 \leq i \leq k-1$. Since in each M_i formula γ_1 is globally true, the suffix π^i must be a local counterpath for γ_2, for each $i \geq 1$. Since each state in M_i except the initial state s_i contains $AP(\phi_2)$, this counterpath for γ_2 can only be a counterpath for ϕ_1. But this is impossible, since a right-structure for formula ϕ_1 cannot contain a deterministic counterexample Π such that $\Pi(i)$ is a counterexample for ϕ_1, for each $i \geq 0$. Thus, it follows that no deterministic counterexample for γ exists in M.

7. $\gamma_1^\star \in \mathcal{PSF}$ and $\gamma_2^\star \in \mathcal{PSF} \wedge S_2^\infty \cup S_2^\infty \wedge \mathcal{PSF}$. Thus, $\gamma_2 = \phi_1 \wedge \phi_2$. Assume that ϕ_1 is a pure state formula and $\phi_2 = \mathbf{A}(\phi_{2,1}\mathbf{U}\phi_{2,2})$, where $\phi_{2,1}$ and $\phi_{2,2}$ are instantiations of templates in $\mathbf{DET}$. The other case (vice versa) is similar.

   Let M_2 be a right-structure for the formula $\phi_2 = \mathbf{A}(\phi_{2,1}\mathbf{U}\phi_{2,2})$. We modify M_2 by adding $AP(\gamma_1) \cup AP(\phi_1)$ to each state and by further adding $AP(\phi_{2,1})$ to the initial state s_0. Observe that after this modification $M_2 \not\models \phi_2$ still holds. We now add two new states s_1, s_2 and connect them via (s_0, s_1) and (s_1, s_2); their labels are $L(s_1) = AP(\phi_2)$ and $L(s_2) = AP(\phi_1) \cup AP(\phi_2) = AP(\gamma_2)$. Furthermore, we add the loop (s_2, s_2). The resulting structure is the desired M (see Figure 22).

   It holds that $M \not\models \gamma$. Indeed, there exists a counterexample Π for γ where $\Pi(0)$ is a counterexample for γ_2, and $\Pi(1)$ is a counterexample for both γ_1 and γ_2. Furthermore, no deterministic counterexample for γ exists in M. To see this, observe that no path π leading into Π_{ϕ_2} or into $\Pi_{\phi_{2,2}}$ can be a counterpath for γ, as γ_1 and ϕ_1 are always true there and Π_{ϕ_2}, $\Pi_{\phi_{2,2}}$ are k-structures for $\phi_{2,2}$ (consequently, ϕ_2 is not globally false). Thus, only $\pi = [s_0, s_1, s_2, s_2, ...]$ remains as a candidate for a counterpath for γ. To eliminate π, assume towards a contradiction that $\pi = \mu(\Pi)$ for some deterministic counterexample Π for γ. The first element $\Pi(0)$ of every counterexample Π for γ must be a counterexample for $\gamma_2 = \phi_1 \wedge \phi_2$; since ϕ_1 is true in s_0, it must be a counterexample of ϕ_2. Along π, however, $\phi_{2,2}$ is not always false, which means that $\Pi(0)$ must involve a counterexample for $\phi_{2,1}$. Along π, however, $\phi_{2,1}$ is by construction always true. This raises a contradiction, and proves that in M no deterministic counterexample for γ exists.

• $\gamma^\star = \phi_1^\star \wedge \phi_2^\star$ or $\gamma^\star = \phi_1^\star \vee \phi_2^\star$, where $n_{\mathbf{A}}(\phi_1^\star) + n_{\mathbf{A}}(\phi_2^\star) = k$. Thus, γ can be viewed as a monotone Boolean combination of formulas $\gamma_1, \ldots, \gamma_m$. By applying Lemma 6.1, if one of the γ_i is not c-deterministic either by the induction hypothesis or by one of the already considered cases, then γ is not c-deterministic as well. To complete the proof, by the inductive definition of $\mathbf{DET}$ and Lemma 6.1 it remains to consider the case $\gamma = \gamma_1 \vee \gamma_2$ where $\gamma_1^\star = \mathbf{A}\psi_1^\star \in \mathbf{DET}$ and $\gamma_2^\star = \mathbf{A}\psi_2^\star \in \mathbf{DET}$.

We construct a conic structure M having three states s_0, s_1, and s_2 such that $M \not\models \gamma$ and no deterministic counterexample for γ exists in M. The initial state is s_0 and reaches both s_1 and s_2, which have loops (s_1, s_1) and (s_2, s_2), respectively. The labels of the states depend on the outermost linear-time operators in $\gamma_1^\star$ and $\gamma_2^\star$. By commutativity of logical conjunction, it suffices to consider the following cases:

- $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2}), \gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. Define $L(M)(s_0) = AP(\gamma_{1,1}) \cup AP(\gamma_{2,1})$, $L(M)(s_1) = AP(\gamma_1) \cup AP(\gamma_{2,1})$, $L(M)(s_2) = AP(\gamma_{1,1}) \cup AP(\gamma_2)$ (see Figure 23).

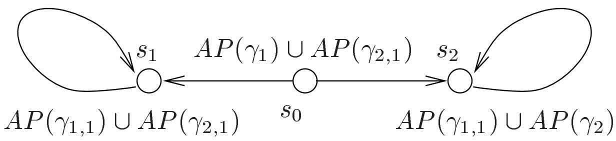

Figure 23: Disjunction of $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$

It easy to see that $M \not\models \gamma$. Indeed, from s_0 start both a counterpath for $\mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$ and a counterpath for $\mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. The path $\pi_1 = [s_0, s_1, s_1, ...]$ is a counterpath for $\mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$, since the formula $\gamma_{2,2}$ is always false along it. Similarly, the path $\pi_2 = [s_0, s_2, s_2, ...]$ is a counterpath for $\mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$, since the formula $\gamma_{1,2}$ is always false along it. On the other hand, π_1 cannot be a counterpath for $\mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$, since therein $\gamma_{1,1}$ is always true and $\gamma_{1,2}$ is not always false. By symmetry, π_2 cannot be a counterpath for $\mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. Hence, each counterexample for γ in M not deterministic.

- $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{U}\gamma_{1,2})$, $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$. Set $L(M)(s_0) = AP(\gamma_{1,1}) \cup AP(\gamma_{2,2})$, $L(M)(s_1) = AP(\gamma_1)$, and $L(M)(s_2) = AP(\gamma_{1,1}) \cup AP(\gamma_{2,2})$. This M witnesses that γ is not deterministic. We omit the details.
- $\gamma_1 = \mathbf{A}(\gamma_{1,1}\mathbf{V}\gamma_{1,2})$, $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$. Set $L(M)(s_0) = AP(\gamma_{1,2}) \cup AP(\gamma_{2,2})$, $L(M)(s_1) = AP(\gamma_{1,2})$, and $L(M)(s_2) = AP(\gamma_{2,2})$.
- $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$, $\gamma_2 = \mathbf{AX}(\gamma_{2,1})$. Set $L(M)(s_0) = \emptyset$, $L(M)(s_1) = AP(\gamma_{1,1})$, and $L(M)(s_2) = AP(\gamma_{2,1})$.
- $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$, $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{U}\gamma_{2,2})$. Set $L(M)(s_0) = AP(\gamma_{2,1})$, $L(M)(s_1) = AP(\gamma_1)$, and $L(M)(s_2) = AP(\gamma_2)$.
- $\gamma_1 = \mathbf{AX}(\gamma_{1,1})$, $\gamma_2 = \mathbf{A}(\gamma_{2,1}\mathbf{V}\gamma_{2,2})$. Set $L(M)(s_0) = AP(\gamma_{2,2})$, $L(M)(s_1) = AP(\gamma_{1,1})$, and $L(M)(s_2) = AP(\gamma_{2,2})$. $\square$

The main result of this paper on templates, Theorem 4.3, follows from Theorems 5.1 and 6.6.

7 Discussion and Conclusion

For the class of *ACTL* formulas which are positive disjoint instantiations, the results in the preceding sections give a complete characterization of the c-deterministic fragment. This class is given by those formulas γ such that $\gamma^\star \in \mathbf{DET}$. Observe that this class is efficiently recognizable.

This result can be extended by the same proof technique to more general classes of formulas γ, as long as certain independency properties hold on the pure state formulas. Introduce for each occurrence of a maximal pure state formula ϕ in γ a new propositional atom p_ϕ, and consider the formula

$$F(\gamma) = \bigwedge_{\phi \in MP(\gamma)} (p_\phi \leftrightarrow \phi),$$

where $MP(\gamma)$ is a list of all occurrences of maximal pure state formulas in γ. Call γ *pure state independent*, if for every truth value assignment to the atomic propositions p_ϕ, the formula $F(\gamma)$ is satisfiable. Observe that every positive disjoint instantiation γ is pure state independent.

Then, along the same line of proof as above we can show the following.

Theorem 7.1 *Let γ be any pure state independent formula. Then, γ is c-deterministic if and only if $\gamma^\star \in$* $\mathbf{DET}$.

However, testing pure state independence is complex in general; this amounts to evaluating the quantified Boolean formula (QBF) $\Phi = \forall P_\phi \exists AP.F(\gamma)$, where P_ϕ is the collection of all atomic propositions p_ϕ introduced for occurrences of maximal pure state formulas, and AP is the collection of all atomic propositions in γ. This problem is complete for the class Π_2^p of the polynomial hierarchy (cf. [8] for Π_2^p). Indeed, the evaluation of the QBFs $\forall X \exists Y.\psi$ is in Π_2^p [8], and the QBF Φ is constructible in polynomial time from γ. On the other hand, consider a QBF $\forall X \exists Y.\psi$, where ψ is of the form $y_1 \wedge \psi'$ where $y_1 \in Y$. Then, the *ACTL* formula $\gamma = (\mathbf{AX}x_1) \wedge \cdots \wedge (\mathbf{AX}x_n) \wedge (\mathbf{AX}\psi)$, where $X = \{x_1,\ldots,x_n\}$, is pure state independent, just if $\forall X \exists Y.\psi$ is true. Since deciding the latter is Π_2^p-hard, also deciding pure state independence is Π_2^p-hard.

Our results can be adapted for the concept of witness [5] in the existential fragment of *CTL* (denote this by *ECTL*), i.e., a portion of a computation tree which witnesses the truth of a formula $\mathbf{E}\phi$. Since on any structure M it holds that $M \models \mathbf{E}\phi$ if and only if $M \not\models \mathbf{A}\neg\phi$, the existence of deterministic witnesses (formally defined in the same vein as counterexamples) is related to the existence of deterministic counterexamples. As well-known [6], the equivalences $\neg\mathbf{A}(\phi\mathbf{V}\psi) = \mathbf{E}(\neg\phi\mathbf{U}\neg\psi)$ and $\neg\mathbf{A}(\phi\mathbf{U}\psi) = \mathbf{E}(\neg\phi\mathbf{V}\neg\psi)$ hold. It follows that a formula γ in the existential *CTL*-fragment has always a deterministic witness (call this *w-deterministic*), if and only if the formula obtained by dualization of γ and negating all elementary atomic propositions, is c-deterministic. As a consequence, all instantiations of an *ECTL*-template $\gamma^\star$ (defined as obvious) have deterministic witnesses (call this w-deterministic), just if the dual template $d(\gamma^\star)$ is c-deterministic. As a consequence, we obtain the following characterization of the class of w-deterministic *ECTL*-templates.

Theorem 7.2 *Let $\gamma^\star$ be an ECTL-template. Then, $\gamma^\star$ is w-deterministic if and only if $d(\gamma^\star) \in \mathbf{DET}$.*

Several issues remain for further work. One issue is the consideration of linear time operators which are derived from the basic operators $\mathbf{X}, \mathbf{V}, \mathbf{U}$. The most important such operators are $\mathbf{F}$ (*sometimes*) and $\mathbf{G}$ (*globally, always*) defined as $\mathbf{F}\phi = \mathit{true}\mathbf{U}\phi$,, $\mathbf{G}\phi = \mathit{false}\mathbf{V}\phi$. It is easily recognized from the definition of $\mathbf{DET}$ and our results that these operators correspond to c-deterministic templates. However, the use of these templates in nesting remains to be explored. The characterization of the class of c-deterministic templates *ACTL* enriched by derived linear time operators is as an interesting issue.

Finally, an extension of our study by fairness constraints [4] would be interesting. In the general framework, path quantifiers do not range over all infinite paths, but instead over paths along which the fairness constraints, expressed by formulas, must be satisfied infinitely often. E.g., fair schedules in a system of concurrent infinite processes, represented through a Kripke structure, can be expressed easily through fairness constraints. Our results do not immediately carry over to this case. Techniques applied in [5] might be useful.

References

[1] F. Buccafurri, T. Eiter, G. Gottlob, and N. Leone. Enhancing Symbolic Model Checking by AI Techniques. Technical Report 9701, Institut für Informatik, Universität Gießen, Germany, September 1997. Abstract in: *Proc. 2nd Workshop on Trends in Theoretical Informatics*, Albrecht and G. Nemeth (eds), Budapest, March 1997.

[2] E. Clarke and E. Emerson. Skeletons for Branching Time Temporal Logic. In *Logic in Programs: Workshop Proceedings*, number 131 in LNCS. Springer, 1981.

[3] E. Clarke, E. Emerson, and A. Sistla. Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications. *ACM Transactions on Programming Languages and Systems*, 8(2):244–263, 1986.

[4] E. Clarke, O. Grumberg, and D. Long. Verification Tools for Finite-State Concurrent Systems. In J. de Bakker, W. de Roever, and G. Rozenberg, editors, *A Decade of Concurrency - Reflections and Perspectives*, number 803 in LNCS, pages 124–175. Springer, 1994.

[5] E. Clarke, O. Grumberg, K. McMillan, and K. Zhao. Efficient Generation of Counterexamples and Witnesses in Symbolic Model Checking. In *Proc. 32nd ACM/SIGDA Design Automation Conference 1995 (DAC '95)*. ACM Press, 1994. Also Technical Report CMU-CS-94-204, Carnegie Mellon University, Pittsburgh, PA, 1994.

[6] E. Clarke, O. Grumberg, and D. Long. Model Checking. In M. Broy, editor, *Deductive Program Design*, volume 152 of *NATO ASI Series F*. Springer, 1996.

[7] E. Emerson. Temporal and Modal Logics. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 16. Elsevier Science Publishers B.V. (North-Holland), 1990.

[8] M. Garey and D. S. Johnson. *Computers and Intractability – A Guide to the Theory of NP-Completeness*. W. H. Freeman, New York, 1979.

[9] O. Kupferman and M. Y. Vardi. An automata-theoretic approach to modular model checking. Manuscript based on LICS '95 and CONCUR '95 abstracts, 1998, submitted for publication.

[10] K. McMillan. *Symbolic Model Checking*. Kluwer, 1993.