Temporal Logics of Repeating Values[*]

Stéphane Demri
LSV, ENS Cachan, CNRS, INRIA
email: demri@lsv.ens-cachan.fr

Deepak D'Souza
Dept. of Computer Science & Automation,
Indian Institute of Science, Bangalore, India
email: deepakd@csa.iisc.ernet.in

Régis Gascon
AOSTE Project, I3S/INRIA
Université Nice Sophia-Antipolis & INRIA Sophia-Antipolis Méditérranée
email: regis.gascon@inria.fr

Abstract

Various logical formalisms with the freeze quantifier have been recently considered to model computer systems even though this is a powerful mechanism that often leads to undecidability. In this paper, we study a linear-time temporal logic with past-time operators such that the freeze operator is only used to express that some value from an infinite set is repeated in the future or in the past. Such a restriction has been inspired by a recent work on spatio-temporal logics that suggests such a restricted use of the freeze operator. We show decidability of finitary and infinitary satisfiability by reduction into the verification of temporal properties in Petri nets by proposing a symbolic representation of models. This is a quite surprising result in view of the expressive power of the logic since the logic is closed under negation, contains future-time and past-time temporal operators and can express the nonce property and its negation. These ingredients are known to lead to undecidability with a more liberal use of the freeze quantifier. The paper also contains developments about the relationships between temporal logics with the freeze operator and counter automata as well as reductions into first-order logics over data words.

Keywords: temporal logics, freeze quantifier, logical methods in program verification.

1 Introduction

Temporal logic with freeze. In logical languages, the freeze mechanism allows one to store a value in a register and to test later the value in the register with a current value. This operator is useful to compare values at distinct states of Kripke-like structures. The freeze quantifier has found applications in real-time logics [Hen90], in hybrid logics [Gor96, ABM01], in modal logics with predicate λ-abstraction [Fit02] and for the specification of computations of systems with unboundedly many locations as resources [LP05]. Although it is known that the freeze operator can lead to undecidability (even with only equality on data [LP05, DLN07, FS09]), many decidable temporal logics have a freeze mechanism, sometimes implicitly, see e.g. [AH94, LMS02, KV06]. Recent developments have shown the ubiquity of the freeze operator [LP05, tCF05, DLN07, Laz06, Seg06] and its high expressive power as witnessed by the Σ_1^1-completeness results shown in [DLN07].

[*] Work supported by the Indo-French project "Timed-DISCOVERI" (P2R/RNP scheme).

The need to design decidable fragments of simple linear-time temporal logic LTL with the freeze quantifier stems from [DLN07, Laz06] and most known decidable fragments in [DLN07, Laz06] do not allow unrestricted use of negation. Potential applications range from the verification of infinite-state systems [Hen90, DLN07] to querying XML documents [Fig10] or more modestly data strings [BMS$^+$06, Seg06]. In this paper, we are interested in studying fragments of LTL with the freeze operator that are decidable over both finite and infinite models, that allow unrestricted use of negation (by contrast to the flat fragments in [DLN07]) and all standard past-time operators (in contrast to what is done in [BMS$^+$06, DL06]). These are strong requirements. In terms of expressive power, the fragment shown to be decidable in the paper can express the "nonce property" (all the values of a variable are different at every position) and its negation. Moreover, in [WZ00, Section 7], the authors advocate the need to consider infinitary disjunction of the form $\bigvee_{i>0} x = \mathsf{X}^i y$ where $\mathsf{X}^i y$ refers to the value of y at the i^{th} next position. This states that a future value of y is equal to the current value of x. Our fragment can express this property, with the formula $x = \mathsf{XF}y$, as well as the dual one: $\bigwedge_{i>0} x = \mathsf{X}^i y$ can be expressed by the formula $\neg(x \textit{ diff } \mathsf{XF}y)$ (cf. Section 2.1).

Our contribution. In the paper we introduce the constraint logic $\mathrm{CLTL}^{\mathsf{XF}}$, which is the logic $\mathrm{CLTL}(\mathbb{N}, =)$ from [DD07] extended with atomic formula of the form $x = \mathsf{XF}y$, and past-time operators X^{-1} and S. The logic $\mathrm{CLTL}^{\mathsf{XF}}$ is interpreted over models which are sequences of valuations for a set of variables. In the logic one can make assertions in temporal logic, using atomic constraints of the form $x = \mathsf{X}^i y$ ("the current value of x is the same value as y i steps ahead") and $x = \mathsf{XF}y$ ("the current value of x is repeated in a future value of y"). Thus in effect $\mathrm{CLTL}^{\mathsf{XF}}$ allows the use of the freeze quantifier only to specify that some values are repeated.

We show that the satisfiability problem for $\mathrm{CLTL}^{\mathsf{XF}}$ with temporal operators $\{\mathsf{X}, \mathsf{X}^{-1}, \mathsf{S}, \mathsf{U}\}$ is decidable over both finite and infinite models. We note that $\mathrm{CLTL}^{\mathsf{XF}}$ over infinite models is the first decidable fragment of $\mathrm{CLTL}^{\downarrow}_1(\mathbb{N}, =)$ [DLN07] which allows unrestricted use of negation and contains all the temporal operators from $\{\mathsf{X}, \mathsf{X}^{-1}, \mathsf{S}, \mathsf{U}\}$.

Our decision procedure is a substantial extension of the automata-based approach for LTL [VW94], and for constraint LTL [DD07]. The main idea is to view the problem of finding a concrete model satisfying a given $\mathrm{CLTL}^{\mathsf{XF}}$ formula in two steps. We first consider the "symbolic model" induced by a given concrete model, which essentially captures the obligations to repeat values in the future, as well as the equality relations between variables, in a finite "window" or "frame". We then find all the symbolic models that satisfy the given formula viewed as a standard LTL formula. In the second step we filter out symbolic models that are "unrealizable" in the sense that they don't admit any concrete model. For this purpose we give a characterisation of symbolic models that are realizable. We show that this characterisation can be checked by special kind of counter automata which we show to have a decidable nonemptiness problem. To decide the nonemptiness problem of these automata we take advantage of a result from [Jan90] that establishes that verifying fairness properties based on the temporal operator GF ("always eventually") in Petri nets is decidable (by reduction into reachability questions).

The decidability of $\mathrm{CLTL}^{\mathsf{XF}}$ can also be seen via a reduction into $\mathrm{FO2}(\sim, <, +\omega)$, a first-order logic over data words introduced in [BMS$^+$06]. We give the details of this reduction in Section 3, but concentrate in the rest of the paper on our decision procedure based on symbolic models described above. The symbolic approach is interesting for several reasons. Firstly, it gives us a characterisation of realizable symbolic models, which is interesting in its own right. Secondly, the technique separates the problem of satisfiability for the "carrier" logic (in this case LTL) and the problem of checking realizability of symbolic models. Thus, as a by-product of our technique, one can immediately observe that the carrier logic can be replaced by any logic whose models can be described by an automaton (for example Monadic Second Order Logic), and the logic remains decidable. The same holds if we add the atomic constraint $x = \mathsf{XF}^{-1}y$ ("a value of y in the past is equal to the current value of x"). Finally, our approach also lets us identify a fragment of $\mathrm{CLTL}^{\mathsf{XF}}$ obtained by restricting the vocabulary of variables to a singleton, for which the finitary and infinitary satisfiability problems are PSPACE-complete.

Plan of the paper. Section 2 introduces the main properties of the temporal logic of repeating values CLTL$^{\mathsf{XF}}$. In Section 3 we present decidability proofs for fragments of CLTL$^{\mathsf{XF}}$ by translation into logics introduced in [DL06], and reductions of the full logic into FO2$(\sim, <, +\omega)$. Sections 4 and 5 are dedicated to the symbolic models for CLTL$^{\mathsf{XF}}$ and to the characterization of such models that are realizable. Section 6 introduces the class of simple counter automata for which the nonemptiness problem is shown decidable using [Jan90]. This allows us to establish the decidability of CLTL$^{\mathsf{XF}}$ satisfiability in Section 7. In Section 8 we consider the PSPACE-fragment, and in Section 9 we consider repeating values in the past. Section 10 contains concluding remarks and open problems.

This paper is a completed version of [DDG07a]. The decidability proof from Section 3.2 is new (not present in [DDG07a, DDG07b]).

2 Preliminaries

2.1 Temporal Logic of Repeating Values

Let VAR $= \{x_1, x_2, \ldots\}$ be a countably infinite set of variables. We denote by CLTL$^{\mathsf{XF}}$ the logic whose formulae are defined as follows:

$$\phi ::= x = \mathsf{X}^i y \mid x = \mathsf{XF} y \mid \phi \wedge \phi \mid \neg\phi \mid \mathsf{X}\phi \mid \phi \mathsf{U} \phi \mid \mathsf{X}^{-1}\phi \mid \phi \mathsf{S} \phi$$

where $x, y \in$ VAR, and $i \in \mathbb{N}$, the set of natural numbers. Formulae of the form either $x = \mathsf{X}^i y$ or $x = \mathsf{XF} y$ are said to be *atomic* and an expression of the form $\mathsf{X}^i x$ (abbreviation for i next symbols followed by a variable) is called a *term*.

A *valuation* is defined to be a map from VAR to $\mathbb{N}$. A CLTL$^{\mathsf{XF}}$ model is a non-empty sequence σ of valuations, which is either finite, or infinite (of length ω). All the subsequent developments can be equivalently done with the domain $\mathbb{N}$ replaced by an infinite set D since only equality tests are performed in the logics. We write $|\sigma|$ to denote the length of σ (equal to ω when the sequence is infinite). For every model σ and $0 \leq i < |\sigma|$, the satisfaction relation $\models$ is defined inductively as follows:

- $\sigma, i \models x = \mathsf{X}^j y$ iff $i + j < |\sigma|$ and $\sigma(i)(x) = \sigma(i+j)(y)$,
- $\sigma, i \models x = \mathsf{XF} y$ iff there exists j such that $i < j < |\sigma|$ and $\sigma(i)(x) = \sigma(j)(y)$,
- $\sigma, i \models \phi \wedge \phi'$ iff $\sigma, i \models \phi$ and $\sigma, i \models \phi'$,
- $\sigma, i \models \neg\phi$ iff $\sigma, i \not\models \phi$,
- $\sigma, i \models \mathsf{X}\phi$ iff $i + 1 < |\sigma|$ and $\sigma, i + 1 \models \phi$,
- $\sigma, i \models \mathsf{X}^{-1}\phi$ iff $i > 0$ and $\sigma, i - 1 \models \phi$,
- $\sigma, i \models \phi \mathsf{U} \phi'$ iff there is $i \leq j < |\sigma|$ such that $\sigma, j \models \phi'$ and for every $i \leq l < j$, we have $\sigma, l \models \phi$.
- $\sigma, i \models \phi \mathsf{S} \phi'$ iff there is $0 \leq j \leq i$ such that $\sigma, j \models \phi'$ and for $j < l \leq i$ we have $\sigma, l \models \phi$.

We write $\sigma \models \phi$ if $\sigma, 0 \models \phi$. We shall use the standard derived temporal operators (G, F, F^{-1}, ...), and derived Boolean operators ($\vee$, $\Rightarrow$, ...) and constants $\top$, $\bot$. We also use the notation $\mathsf{X}^i x = \mathsf{X}^j y$ as an abbreviation for the formula $\mathsf{X}^i(x = \mathsf{X}^{j-i} y)$ (assuming without any loss of generality that $i \leq j$). Given a set of temporal operators $\mathcal{O}$ definable from those in $\{\mathsf{X}, \mathsf{X}^{-1}, \mathsf{S}, \mathsf{U}\}$ and a natural number $k \geq 0$, we write CLTL$_k^{\mathsf{XF}}(\mathcal{O})$ to denote the fragment of CLTL$^{\mathsf{XF}}$ restricted to formulae with temporal operators from $\mathcal{O}$ and with at most k variables.

The *finitary [resp. infinitary] satisfiability problem* for CLTL$^{\mathsf{XF}}$ is to check for a given CLTL$^{\mathsf{XF}}$ formula ϕ, whether there exists a finite [resp. infinite] model σ such that $\sigma \models \phi$. It is known that finitary satisfiability for LTL can be easily reduced in logarithmic space to infinitary satisfiability by introducing an additional propositional variable p and by requiring that $p \mathsf{U} \mathsf{G} \neg p$ holds true. In that way, there is a prefix of the model such that p holds true at every state of a prefix and p does not hold on the complement suffix. The same principle does not apply for reducing finitary satisfiability for CLTL$^{\mathsf{XF}}$ to infinitary satisfiability, even if we introduce additional variables in order to simulate a propositional variable. Indeed, for an atomic formula of the form $x = \mathsf{XF}y$ we cannot enforce a future value of y that satisfies the equality constraint to occur before a given position. For this reason, we will address the two problems separately in the sequel.

As far as expressiveness is concerned, we note that the constraint "the value of x differs from some future value of y", denoted x *diff* $\mathsf{XF}y$, can be expressed in CLTL$^{\mathsf{XF}}$:

$$x \textit{ diff } \mathsf{XF}y \Leftrightarrow (\neg(x = \mathsf{X}y) \wedge \mathsf{X}\top) \vee ((x = \mathsf{X}y) \wedge \mathsf{X}(y = \mathsf{X}y)\mathsf{U}(\neg(y = \mathsf{X}y) \wedge \mathsf{X}\top))). \qquad (1)$$

With infinite models, the conjunct $\mathsf{X}\top$, stating the existence of a next position in the model, can be deleted. The constraint x *diff* $\mathsf{XF}y$ is different from the constraint $\neg(x = \mathsf{XF}y)$ which means that x is different from all future values of y. Constraints of the form $x = \mathsf{X}^{-i}y$ can also be expressed in the language using the equivalence $x = \mathsf{X}^{-i}y \Leftrightarrow \mathsf{X}^{-i}\top \wedge \mathsf{X}^{-i}(y = \mathsf{X}^{i}x)$. Similarly, CLTL$^{\mathsf{XF}}$ can express that a variable is a "nonce" by the formula $\mathsf{G}\neg(x = \mathsf{XF}x)$. The formula below states a valid property when x and y are nonces:

$$(\mathsf{G}\neg(x = \mathsf{XF}x) \wedge \mathsf{G}\neg(y = \mathsf{XF}y)) \Rightarrow \mathsf{G}(x = y \Rightarrow \neg(x = \mathsf{XF}y)).$$

Other properties witnessing the high expressive power of CLTL$^{\mathsf{XF}}$ can be found in [LP05, Section 3] on systems of pebbles evolving in time.

Lemma 1 *The satisfiability problems for* CLTL$^{\mathsf{XF}}$ *is PSPACE-hard* ***even restricted to one variable****.*

Propositional variables can be simulated by atomic formulae of the form $x = \mathsf{X}x$ where x is a fresh variables dedicated only to this purpose. PSPACE-hardness is then a direct consequence of the PSPACE-hardness of the satisfiablity problem for LTL. This result holds also for the one-variable fragment since the one variable fragment of LTL is PSPACE-complete (see [DS98]).

2.2 Known extensions of CLTL$^{\mathsf{XF}}$

In [DLN07], the authors introduced the logic CLTL$^{\downarrow}(\mathbb{N}, =)$ that subsumes CLTL$^{\mathsf{XF}}$. This logic includes a freeze operator (denoted by $\downarrow$) allowing to store values in register variables. In order to compare the different fragments of this logic with CLTL$^{\mathsf{XF}}$, we define below the logic CLTL$^{\downarrow}$ whose definition is equivalent to CLTL$^{\downarrow}(\mathbb{N}, =)$. Let VAR be a countably infinite set of variables and REG $= \{r_1, r_2, \ldots\}$ a countably infinite set of registers. The formulae of CLTL$^{\downarrow}$ are defined by

$$\phi ::= r = x \mid \downarrow_{r=x} \phi \mid \phi \wedge \phi \mid \neg\phi \mid \mathsf{X}\phi \mid \phi\mathsf{U}\phi \mid \mathsf{X}^{-1}\phi \mid \phi\mathsf{S}\phi$$

where $r \in$ REG and $x \in$ VAR. The satisfaction relation $\models$ is parameterized by a register assignment $\rho :$ REG $\rightarrow \mathbb{N}$ and we have:

- $\sigma, i \models_{\rho} \downarrow_{r=x} \phi$ iff $\sigma, i \models_{\rho[r \mapsto \sigma(i)(x)]} \phi$
- $\sigma, i \models_{\rho} r = x$ iff $\rho(r) = \sigma(i)(x)$

where $\rho[r \mapsto \sigma(i)(x)]$ is the valuation that associates $\sigma(i)(x)$ to r and $\rho(r')$ to every variable $r' \neq r$. The remaining cases are similar to CLTL$^{\mathsf{XF}}$. We write CLTL$^{\downarrow}_{(k,k')}(\mathcal{O})$ to denote the fragment of CLTL$^{\downarrow}$ restricted to the temporal operators from $\mathcal{O}$ with at most k variables and k' registers. Satisfiability problems for CLTL$^{\downarrow}$ are defined as those for CLTL$^{\mathsf{XF}}$ except that we require that in formulae every occurrence of $r = x$ is in the scope of a subformula of the form $\downarrow_{r=y}$ (no free occurrences of registers).

The logic CLTL$^{\mathsf{XF}}$ is a fragment of CLTL$^{\downarrow}_{(\omega,1)}(\mathcal{O})$ since the atomic constraints $x = \mathsf{X}^{i}y$ and $x = \mathsf{XF}y$ can be rewritten equivalently into $\downarrow_{r=x} \mathsf{X}^{i}(r = y)$ and $\downarrow_{r=x} \mathsf{XF}(r = y)$, respectively. Like CLTL$^{\downarrow}$, the logic CLTL$^{\mathsf{XF}}$ is strictly more expressive than its fragment without atomic formulae of the form $x = \mathsf{XF}y$ since the nonce property cannot be expressed without a storing mechanism (same argument as in [DLN07]). On the other hand, $\mathrm{CLTL}^{\mathsf{XF}}$ is neither a syntactic fragment of the pure-future safety fragment of $\mathrm{CLTL}^{\downarrow}$ studied in [Laz06] nor a syntactic fragment of the flat fragment of $\mathrm{CLTL}^{\downarrow}$. The safety fragment restricts the use of the until operator (U) only in the scope of an odd number of negations and the flat fragment restricts the use of the freeze operator in subformulae in the scope of an until operator depending of the number of negations (see [DLN05]). Unlike these fragments, $\mathrm{CLTL}^{\mathsf{XF}}$ contains past-time operators and negation can be used without any restriction. It has been shown that infinitary satisfiability for safety $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X},\mathsf{U})$ is EXPSPACE-complete [Laz06] and Π^0_1-complete for full $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X},\mathsf{U})$. Finitary and infinitary satisfiability for flat $\mathrm{CLTL}^{\downarrow}$ are PSPACE-complete [DLN05]. By contrast, in this paper we show that finitary and infinitary satisfiability for $\mathrm{CLTL}^{\mathsf{XF}}$ (with full past-time temporal operators) are decidable problems.

3 Decidability by Reductions into Data Logics

In this section we show how $\mathrm{CLTL}^{\mathsf{XF}}$ and some of its fragments can be decided by translation into decidable logics from [DL06, BMS$^+$06, Dav09].

3.1 Decidable fragments for finitary satisfiability

By taking advantage of [DLN07, DL06], it is already possible to establish decidability of *finitary* satisfiability for *strict* fragments of $\mathrm{CLTL}^{\mathsf{XF}}$.

Theorem 1 **(I)** *Finitary satisfiability for* $\mathrm{CLTL}^{\mathsf{XF}}(\mathsf{X},\mathsf{U})$ *is decidable.*
(II) *Finitary satisfiability for* $\mathrm{CLTL}^{\mathsf{XF}}(\mathsf{X},\mathsf{X}^{-1},\mathsf{F},\mathsf{F}^{-1})$ *is decidable.*

Proof. **(I)** Finitary satisfiability for $\mathrm{CLTL}^{\mathsf{XF}}(\mathsf{X},\mathsf{U})$ can be reduced to finitary satisfiability for $\mathrm{CLTL}^{\downarrow}_{(\omega,1)}(\mathsf{X},\mathsf{U})$ by expressing every atomic constraint using the freeze operator (see above). By [DLN07, Proposition 4], from every formula in $\mathrm{CLTL}^{\downarrow}_{(\omega,1)}(\mathsf{X},\mathsf{U})$, we can build an equivalent formula using the same number of registers but with a unique variable. So we can reduce the problem to finitary satisfiability for $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X},\mathsf{U})$ that is decidable by [DL06, Corollary 13].

(II) Let ϕ be a $\mathrm{CLTL}^{\mathsf{XF}}(\mathsf{X},\mathsf{X}^{-1},\mathsf{F},\mathsf{F}^{-1})$ formula built over variables in $\{x_1,\ldots,x_k\}$ and l be the maximal i such that a term of the form $\mathsf{X}^i x$ occurs in ϕ. This formula is equivalent to a formula in $\mathrm{CLTL}^{\downarrow}_{(\omega,1)}(\mathsf{X},\mathsf{X}^{-1},\mathsf{F},\mathsf{F}^{-1})$ by using the following equivalences

(X) $x = \mathsf{X}^i y \Leftrightarrow \downarrow_{r=x} \mathsf{X}^i(r = y)$

(XF) $x = \mathsf{XF}y \Leftrightarrow \downarrow_{r=x} \mathsf{XF}(r = y)$

Let $N = 3k(l+1)$ and $\mathcal{O}_N$ be the set of temporal operators below:

$$\mathcal{O}_N = \{\mathsf{X},\mathsf{X}^2,\ldots\mathsf{X}^N,\mathsf{X}^{N+1}\mathsf{F},\mathsf{X}^{-1},\mathsf{X}^{-2},\ldots\mathsf{X}^{-N},\mathsf{X}^{-(N+1)}\mathsf{F}^{-1}\}.$$

Using a proof technique from [DG09], we build a formula ϕ' in the *simple fragment* of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathcal{O}_N)$ such that ϕ is satisfiable iff ϕ' is. The formulae in the simple fragment of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathcal{O}_N)$ satisfy the property that every occurrence of a temporal operator $\mathrm{O} \in \mathcal{O}_N$ is in the direct scope of a freeze operator and there are no other occurrences of the freeze operator. Finitary satisfiability for the simple fragment of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathcal{O}_N)$ is decidable (see [BMS$^+$06] and [DL06]).

The idea is to encode one state from a k-variable model into $3k$ states in a 1-variable model. Only one state over three encodes a value from the original model. Intermediate states are used to know when a sequence of $3k$ states corresponds to a state in the k-variable model. For instance, the 2-variable model below

$$\begin{pmatrix} y_1^0 \\ y_2^0 \end{pmatrix} \begin{pmatrix} y_1^1 \\ y_2^1 \end{pmatrix} \cdots$$

is encoded as the 1-variable model

$$\boxed{y_1^0 = \circ} \neq \circ \neq y_2^0 \neq \circ \neq \circ \neq \boxed{y_1^1 = \circ} \neq \circ \neq y_2^1 \neq \circ \neq \circ \ldots$$

where $\circ$ denotes arbitrary values satisfying the mentioned relations with its neighbors (each occurrence of $\circ$ corresponds to a possibly distinct value). These values always exist because the interpretation domain $\mathbb{N}$ is infinite. The beginning of the encoding of some state from the 2-variable model satisfies that two consecutive values of x in the 1-variable model are identical. More generally, in the 1-variable model, $x = \mathsf{X}x$ holds true exactly when the current position starts the encoding of a position in the k-variable model. The value for $\mathsf{X}^i x_j$ in the k-variable model is done via the term $\mathsf{X}^{3ik+3(j-1)}x$. We can impose that $x = \mathsf{X}x$ every $3k$ states and the length of the model is a multiple of $3k$ by using the CLTL$^{\mathsf{XF}}$ formula below:

$$\phi_{3k} \overset{\text{def}}{\equiv} (x = \mathsf{X}x) \wedge \bigwedge_{0<i<3k} \mathsf{X}^i(x \neq \mathsf{X}x) \wedge$$

$$\mathsf{G}\big(((x = \mathsf{X}x) \wedge \mathsf{X}^{3k+1}\top) \Leftrightarrow \mathsf{X}^{3k}(x = \mathsf{X}x)\big) \wedge \mathsf{G}((x = \mathsf{X}x) \Rightarrow \bigwedge_{0<i<3k} \mathsf{X}^i\top)$$

which is equivalent to the following CLTL$^{\downarrow}$ formula (using the equivalence (X))

$$\downarrow_{r=x} \mathsf{X}(r = x) \wedge \bigwedge_{0<i<3k} \mathsf{X}^i \downarrow_{r=x} \mathsf{X}(r \neq x) \wedge \neg\mathsf{F}\big((\downarrow_{r=x} \mathsf{X}(r = x) \wedge \mathsf{X}^{3k+1}\top$$
$$\wedge\, \mathsf{X}^{3k} \downarrow_{r=x} \mathsf{X}(r \neq x)) \vee ((\downarrow_{r=x} \mathsf{X}(r \neq x) \vee \neg\mathsf{X}^{3k+1}\top) \wedge \mathsf{X}^{3k} \downarrow_{r=x} \mathsf{X}(r = x))\big)\big) \wedge$$
$$\neg\mathsf{F}(\downarrow_{r=x} \mathsf{X}(r = x) \wedge (\bigvee_{0<i<3k} \neg\mathsf{X}^i\top))$$

This latter formula can be expressed in the simple fragment using the equivalence rules below

($\star$) $\mathsf{F}\phi \Leftrightarrow \phi \vee \mathsf{X}\phi \vee \cdots \vee \mathsf{X}^N\phi \vee \mathsf{X}^{N+1}\mathsf{F}\phi$ (and similarly with F^{-1}) ,

($\star\star$) $\mathrm{O}(\downarrow_{r=x} \phi_1 \otimes \cdots \otimes \downarrow_{r=x} \phi_m) \Leftrightarrow \downarrow_{r=x} \mathrm{O}(\downarrow_{r=x} \phi_1 \otimes \cdots \otimes \downarrow_{r=x} \phi_m)$
for all $\mathrm{O} \in \mathcal{O}_N$ and $\otimes \in \{\wedge, \vee\}$.

Now, we define a map f from the set of CLTL$^{\mathsf{XF}}$ formulae into the set of CLTL$^{\downarrow}_{(1,1)}(\mathcal{O}_N)$ formulae as follows:

- (X) $f(x_m = \mathsf{X}^i x_n) \overset{\text{def}}{\equiv} \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3ik+3n-3m}(r = x)$
  because $x_m = \mathsf{X}^i x_n \Leftrightarrow \downarrow_{r=x_m} \mathsf{X}^i(r = x_n))$,
- (XF) $f(x_m = \mathsf{XF}x_n) \overset{\text{def}}{\equiv} \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3k-3(m-1)}\mathsf{F}((\mathsf{X}^{-3(n-1)} \downarrow_{r=x} \mathsf{X}(r = x)) \wedge (r = x))$
  since $x_m = \mathsf{XF}x_n \Leftrightarrow \downarrow_{r=x_m} \mathsf{XF}(r = x_n)$,
- f is homomorphic for the Boolean operators,
- $f(\mathsf{X}\psi) = \mathsf{X}^{3k} f(\psi)$,
- $f(\mathsf{F}\psi) = \mathsf{F}((x = \mathsf{X}x) \wedge f(\psi))$,
- $f(\mathsf{X}^{-1}\psi) = \mathsf{X}^{-3k} f(\psi)$,
- $f(\mathsf{F}^{-1}\psi) = \mathsf{F}^{-1}((x = \mathsf{X}x) \wedge f(\psi))$.

Finally, we can prove that any formula obtained by applying the map f is equivalent to a formula in the simple fragment of CLTL$^{\downarrow}_{(1,1)}(\mathcal{O}_N)$. We proceed by induction on the structure of the formula. Since most of the cases are obvious, we develop below only the cases (X) and (XF).

(X) $\mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3ik+3n-3m)}(r = x)$
$\equiv \downarrow_{r=x} \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3ik+3n-3m}(r = x)$.

$$(\mathsf{XF})\ \ \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3(k+1-m)}\mathsf{F}(\mathsf{X}^{-3(n-1)} \downarrow_{r=x} \mathsf{X}(r = x) \wedge (r = x))$$
$$\equiv \downarrow_{r=x} \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3(k+1-m)}\mathsf{F}(\downarrow_{r=x} \mathsf{X}^{-3(n-1)} \downarrow_{r=x} \mathsf{X}(r = x) \wedge (r = x)).$$

We can see that these formulae have one register, one free variable and all the temporal operators are directly under the scope of a freeze quantifier. For the cases with temporal operators from $\mathcal{O}_N$ we need to use $(\star)$ and $(\star\star)$ in order to find an equivalent formula in the simple fragment of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathcal{O}_N)$.

It remains to show that the formula ϕ is satisfiable iff $\phi_{3k} \wedge f(\phi)$ is satisfiable, say ϕ is built over variables in $\{x_1, \ldots, x_k\}$. Consider a sequence of integers σ_1 and a k-variable model $\sigma_k : \mathbb{N} \to (\mathrm{VAR} \to \mathbb{N})$ defined by $\sigma_k(i)(x_j) = \sigma_1(3ik + 3(j-1))(x)$ for every $i \in \mathbb{N}$ and $x_j \in \mathrm{VAR}$. Note that for every model σ_k the corresponding sequence σ_1 such that for all $i \in \mathbb{N}$ and $j \in \{1, \ldots, k\}$, we have $\sigma_k(i)(x_j) = \sigma_1(3ik+3(j-1))(x)$ and $\sigma_1 \models \phi_{3k}$ can be built since the interpretation domain $\mathbb{N}$ contains enough distinct values to satisfy ϕ_{3k}. So, we suppose without any loss of generality that $\sigma_1 \models \phi_{3k}$.

We can show by induction on the structure of ϕ that for all $i \in \mathbb{N}$ we have $\sigma_1, 3ik \models \phi_{3k} \wedge f(\phi)$ iff $\sigma_k, i \models \phi$.

- If ϕ is of the form $(x_m = \mathsf{X}^j x_n)$ with $j > 0$ then $\phi_{3k} \wedge f(\phi)$ is equivalent to the formula $\phi_{3k} \wedge \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3jk+3n-3m}(r = x)$. Thus, the property is satisfied since for every $i \in \mathbb{N}$ we have $\sigma_1(3ik + 3(m-1))(x) = \sigma_1(3(i+j)k + 3(n-1))(x)$ iff $\sigma_k(i)(x_m) = \sigma_k(i+j)(x_n)$.

- If ϕ is of the form $(x_m = \mathsf{XF}x_n)$ then $\phi_{3k} \wedge f(\phi)$ is equivalent to the formula $\phi_{3k} \wedge \mathsf{X}^{3(m-1)} \downarrow_{r=x} \mathsf{X}^{3k-3(m-1)}\mathsf{F}(\mathsf{X}^{-3(n-1)} \downarrow_{r=x} (r = x) \wedge (r = x))$. Suppose that we have $\sigma_1, 3ik \models \phi_{3k} \wedge f(\phi)$. By ϕ_{3k}, for every $i \in \mathbb{N}$ there is a position $j > 3ik$ verifying $\sigma_1(j)(x) = \sigma(j+1)(x)$ iff $j = 3j'k$ for every $j' \in \mathbb{N}$. Moreover, if $\sigma_1, 3ik \models \phi_{3k} \wedge f(\phi)$ then $\sigma_1(3ik + 3(m-1))(x) = \sigma_1(3(i+j')k + 3(n-1))(x)$. This means that we have $\sigma_k(i)(x_m) = \sigma_k(i+j')(x_n)$ and so $\sigma_k \models \phi$.

  The converse implication is direct since by construction we have supposed that $\sigma_1 \models \phi_{3k}$.

  We omit the remaining cases that are obtained by an easy verification. □

Note that showing similar results in the infinitary case with the same kind of reductions seems difficult since infinitary satisfiability for $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X}, \mathsf{F})$ is undecidable (Π^0_1-complete).

3.2 Translation into first-order data logic

We now show that decidability for $\mathrm{CLTL}^{\mathsf{XF}}$ can be established by translation into the logic $\mathrm{FO2}(\sim, <, +\omega)$ introduced in [BMS+06]. Formulae of the logic $\mathrm{FO}^{\Sigma}(\sim, <, +1)$ [BMS+06] where Σ is a finite alphabet are defined as follows:

$$\phi ::= a(\mathtt{x}) \ \mid\ \mathtt{x} \sim \mathtt{y} \ \mid\ \mathtt{x} < \mathtt{y} \ \mid\ \mathtt{x} = \mathtt{y} + 1 \ \mid\ \neg\phi \ \mid\ \phi \wedge \phi \ \mid\ \exists \mathtt{x}\ \phi$$

where $a \in \Sigma$ and $\mathtt{x}, \mathtt{y}$ range over a countably infinite set VAR' of variables. We write $\mathrm{FO}(\sim, <, +1)$ to denote $\mathrm{FO}^{\Sigma}(\sim, <, +1)$ for some unspecified finite alphabet Σ. Models for $\mathrm{FO}^{\Sigma}(\sim, <, +1)$ are (finite or infinite) sequences of pairs from $\mathbb{N} \times \Sigma$, also known as data words in [BMS+06]. Equivalently, they are models for $\mathrm{CLTL}^{\mathsf{XF}}_1$ (restriction to a unique flexible variable) in which each position is augmented by a letter from Σ. By the way, in [KSZ10], decidable logics over multi-attribute data words are investigated. A variable valuation v for a model σ is a map from VAR' to the indices of σ. We write $\mathbb{N}(\mathtt{x})$ to denote the natural number in the pair $\sigma(v(\mathtt{x}))$ (the "datum") and $\Sigma(\mathtt{x})$ to denote its letter (the "label"). The satisfaction relation $\models$ is defined as follows (Boolean clauses are omitted):

$$\begin{array}{rcl}
\sigma \models_v \ a(\mathtt{x}) & \overset{\text{def}}{\Leftrightarrow} & \Sigma(\mathtt{x}) = a \\
\sigma \models_v \ \mathtt{x} \sim \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & \mathbb{N}(\mathtt{x}) = \mathbb{N}(\mathtt{y}) \\
\sigma \models_v \ \mathtt{x} < \mathtt{y} & \overset{\text{def}}{\Leftrightarrow} & v(\mathtt{x}) < v(\mathtt{y}) \\
\sigma \models_v \ \mathtt{x} = \mathtt{y} + 1 & \overset{\text{def}}{\Leftrightarrow} & v(\mathtt{x}) = v(\mathtt{y}) + 1 \\
\sigma \models_v \ \exists \ \mathtt{x} \ \phi & \overset{\text{def}}{\Leftrightarrow} & \text{there is } i < |\sigma| \text{ such that } \sigma \models_{v[\mathtt{x} \mapsto i]} \ \phi.
\end{array}$$

Here $v[\mathtt{x} \mapsto i]$ denotes the variable valuation equal to v except that the variable $\mathtt{x}$ is mapped to the position i. In the sequel, we omit the subscript "v" in $\models_v$ when sentences (formulae with no free occurrences of variables) are involved.

In the sequel, we consider the two following variant logics:

- $\mathrm{FO2}^{\Sigma}(\sim, <, +1)$ is defined as the fragment of $\mathrm{FO}^{\Sigma}(\sim, <, +1)$ restricted to two variables, say $\mathtt{x}_0$ and $\mathtt{x}_1$.
- $\mathrm{FO2}^{\Sigma}(\sim, <, +\omega)$ is defined as the extension of $\mathrm{FO2}^{\Sigma}(\sim, <, +1)$ by replacing the atomic formulae of the form $\mathtt{x}_i = \mathtt{x}_j + 1$ by $\mathtt{x}_i = \mathtt{x}_j + k$ for $k \in \mathbb{N}$ (with the obvious semantics).

The finitary [resp. infinitary] satisfiability problem for $\mathrm{FO2}^{\Sigma}(\sim, <, +\omega)$ is to check whether a sentence from $\mathrm{FO2}^{\Sigma}(\sim, <, +w)$ has a finite [resp. infinite] model.

Theorem 2 *[BMS+06, Dav09] The finitary and infinitary satisfiability problems for* $\mathrm{FO2}(\sim, <, +\omega)$ *are decidable.*

In order to be precise, what is formally shown in [BMS+06] is that the finitary satisfiability problem for $\mathrm{FO2}(\sim, <, +\omega)$ and the infinitary satisfiability problem for $\mathrm{FO2}(\sim, <, +1)$ are decidable. However, by a careful analysis of the developments in [BMS+06], the proof can be extended to the infinitary satisfiability problem for $\mathrm{FO2}(\sim, <, +\omega)$. Let us recall briefly how decidability for infinitary satisfiability is shown in [BMS+06] (finitary satisfiability follows a similar but simpler argument). Satisfiability is first reduced to nonemptiness for data ω-automata, which in turn is reduced to nonemptiness for Büchi bag automata. Both data ω-automata and Büchi bag automata are classes of automata newly introduced in [BMS+06]. Then, nonemptiness for Büchi bag automata is reduced to reachability for Petri nets (or equivalently for Vector Addition Systems with States – VASS).

Let us now show how the infinitary satisfiability problem for $\mathrm{CLTL}^{\mathsf{XF}}$ is reduced to the infinitary satisfiability problem for $\mathrm{FO2}(\sim, <, +\omega)$. Let ϕ be a formula in $\mathrm{CLTL}^{\mathsf{XF}}$ built over the variables in $\{x_1, \ldots, x_k\}$. The finite alphabet Σ_ϕ is defined as the set of subsets of subformulae of ϕ augmented with the dummy value $\sharp$. For each subformula ψ, we shall write $\psi(\mathtt{x})$ instead of

$$\bigvee_{\psi \in a, a \in \Sigma_\phi} a(\mathtt{x}).$$

We shall effectively build a formula ϕ' in $\mathrm{FO2}^{\Sigma_\phi}(\sim, <, +\omega)$ such that ϕ is satisfiable iff ϕ' is. For each subformula ψ, we define a formula φ_ψ and ϕ' will be precisely

$$\varphi_{k+1} \wedge \exists \ \mathtt{x}_0 \ (\mathtt{x}_0 = 0 \wedge \phi(\mathtt{x}_0)) \wedge \bigwedge_{\psi \in sub(\phi)} \varphi_\psi.$$

In the above formula, $\mathtt{x}_i = 0$ is an abbreviation for $\neg(\exists \ \mathtt{x}_{1-i} \ \mathtt{x}_{1-i} < \mathtt{x}_i)$. The formula φ_{k+1} states that the set of positions with datum equal to the datum at position zero is precisely the set of positions that are multiples of $k+1$. φ_{k+1} can be expressed in $\mathrm{FO2}^{\Sigma_\phi}(\sim, <, +\omega)$ as follows (when the models are infinite):

$$\exists \ \mathtt{x}_0 \ \mathtt{x}_0 = 0 \wedge [(\forall \ \mathtt{x}_1 \ (\mathtt{x}_1 \sim \mathtt{x}_0 \wedge \mathtt{x}_1 \neq 0) \Rightarrow \exists \ \mathtt{x}_0 \ \mathtt{x}_0 + (k+1) = \mathtt{x}_1 \wedge \mathtt{x}_0 \sim \mathtt{x}_1) \wedge$$

$$(\forall \ \mathtt{x}_1 \ \mathtt{x}_1 \sim \mathtt{x}_0 \Rightarrow \exists \ \mathtt{x}_0 \ ((\mathtt{x}_0 = \mathtt{x}_1 + (k+1) \wedge \mathtt{x}_0 \sim \mathtt{x}_1) \wedge (\forall \ \mathtt{x}_1 \ \mathtt{x}_1 \sim \mathtt{x}_0 \Leftrightarrow \neg\sharp(\mathtt{x}))))]$$

In models satisfying φ_{k+1}, $k+1$ consecutive positions starting at a position with datum equal to the datum at position zero can encode a value for each variable in $\{x_1, \ldots, x_k\}$. Note also that only the labels at a position with datum equal to the datum at position zero are meaningful: the others have the dummy value. Below, we write $\mathtt{x}_i \sim 0$ as an abbreviation for $\exists\ \mathtt{x}_{1-i}\ \neg(\exists\ \mathtt{x}_i\ \mathtt{x}_i < \mathtt{x}_{1-i}) \wedge \mathtt{x}_{1-i} \sim \mathtt{x}_i$. It is worth observing that in the above formulae we intensively recycle variables. It remains to define φ_ψ by a case analysis on ψ as shown below. The definitions for formulae with outermost connective a Boolean connective or a temporal connective are completely standard from the encoding of LTL formulae into monadic second-order logic (via Büchi automata for instance). The main difficulty is to express with only two individual variables that a valuation for k flexible variables from a CLTL$^{\mathsf{XF}}$ model can be encoded as $k+1$ successive positions in FO2$(\sim, <, +\omega)$ models.

$(\psi = \neg\psi')$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0) \Leftrightarrow (\mathtt{x}_0 \sim 0 \wedge \neg\ (\psi'(\mathtt{x}_0)))$$

$(\psi = \psi_1 \wedge \psi_2)$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0) \Leftrightarrow (\mathtt{x}_0 \sim 0 \wedge (\psi_1(\mathtt{x}_0) \wedge \psi_2(\mathtt{x}_0)))$$

$(\psi = \mathsf{X}\psi')$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0) \Leftrightarrow (\mathtt{x}_0 \sim 0 \wedge \exists\ \mathtt{x}_1\ \mathtt{x}_1 = \mathtt{x}_0 + (k+1) \wedge \psi'(\mathtt{x}_1))$$

$(\psi = \psi_1 \mathsf{U} \psi_2)$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0)\ \Leftrightarrow\ (\mathtt{x}_0 \sim 0\ \wedge$$
$$(\psi_2(\mathtt{x}_0)\ \vee\ (\psi_1(\mathtt{x}_0)\ \wedge\ \exists\ \mathtt{x}_1\ \mathtt{x}_1 = \mathtt{x}_0 + (k+1)\ \wedge\ \psi(\mathtt{x}_1)\ \wedge\ \exists\ \mathtt{x}_1\ \mathtt{x}_1 > \mathtt{x}_0\ \wedge\ \psi_2(\mathtt{x}_1)))$$

$(x_s = \mathsf{XF} x_{s'})$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0) \Leftrightarrow (\mathtt{x}_0 \sim 0\ \wedge$$
$$\exists\ \mathtt{x}_1\ (\mathtt{x}_1 = \mathtt{x}_0 + s\ \wedge\ (\exists\ \mathtt{x}_0\ \mathtt{x}_0 > \mathtt{x}_1\ \wedge\ \mathtt{x}_0 \sim \mathtt{x}_1\ \wedge\ (\exists\ \mathtt{x}_1\ \mathtt{x}_1 + s' = \mathtt{x}_0\ \wedge\ \mathtt{x}_1 \sim 0))))$$

$(x_s = \mathsf{X}^i x_{s'})$

$$\varphi_\psi = \forall\ \mathtt{x}_0\ \psi(\mathtt{x}_0) \Leftrightarrow (\mathtt{x}_0 \sim 0\ \wedge$$
$$\exists\ \mathtt{x}_1\ (\mathtt{x}_1 = \mathtt{x}_0 + s\ \wedge\ (\exists\ \mathtt{x}_0\ \mathtt{x}_0 \sim \mathtt{x}_1\ \wedge\ \mathtt{x}_1 + (i(k+1) + s' - s) = \mathtt{x}_0\ )))$$

This is valid for $i > 0$ or $s \leq s'$ (the other cases are similar).

We omit the definitions for the subformulae of the form $\mathsf{X}^{-1}\psi'$ and $\psi_1 \mathsf{S} \psi_2$ since they can easily be deduced from the above ones.

For the finitary case, we have to guarantee that the length of models is a multiple of $k+1$. So, φ_{k+1} is replaced by the formula below:

$$\exists\ \mathtt{x}_0\ \mathtt{x}_0 = 0 \wedge [(\forall\ \mathtt{x}_1\ (\mathtt{x}_1 \sim \mathtt{x}_0 \wedge \mathtt{x}_1 \neq 0) \Rightarrow \exists\ \mathtt{x}_0\ \mathtt{x}_0 + (k+1) = \mathtt{x}_1 \wedge \mathtt{x}_0 \sim \mathtt{x}_1) \wedge$$
$$(\forall\ \mathtt{x}_1\ (\mathtt{x}_1 \sim \mathtt{x}_0 \Rightarrow \exists \mathtt{x}_0\ \mathtt{x}_1 + k = \mathtt{x}_0) \wedge$$
$$(\forall\ \mathtt{x}_1\ (\mathtt{x}_1 \sim \mathtt{x}_0 \wedge \exists\ \mathtt{x}_0\ \mathtt{x}_1 + (k+1) = \mathtt{x}_0) \Rightarrow \exists\ \mathtt{x}_0\ \mathtt{x}_0 = \mathtt{x}_1 + (k+1) \wedge \mathtt{x}_0 \sim \mathtt{x}_1)$$
$$\wedge(\forall\ \mathtt{x}_1\ \mathtt{x}_1 \sim \mathtt{x}_0 \Leftrightarrow \neg\sharp(\mathtt{x}))]$$

Lemma 2 *For every formula ϕ in* CLTL$^{\mathsf{XF}}$*, ϕ has an infinite [resp. finite] model iff ϕ' in* FO2$(\sim, <, +\omega)$ *defined above has an infinite [resp. finite] model.*

Proof. We treat below the infinitary case, the finitary case being very similar. Let ϕ be a formula in $\mathrm{CLTL}^{\mathsf{XF}}$ built over the variables $\{x_1, \ldots, x_k\}$ and $\sigma : \mathbb{N} \to (\{x_1, \ldots, x_k\} \to \mathbb{N})$ be a model such that $\sigma, 0 \models \phi$. Without any loss of generality we can assume that for $i \in \mathbb{N}$ and $j \in \{1, \ldots, k\}$, $\sigma(i)(x_j) \neq 0$ (otherwise one increments each variable value by 1 which does not affect the satisfiability status of any subformulae).

We build a model σ' for $\mathrm{FO2}^{\Sigma_\phi}(\sim, <, +\omega)$ formulae as follows:

- For $i \in \mathbb{N}$ such that $i \not\equiv 0\ [k+1]$, the ith position of σ' has label $\sharp$.
- For $i \in \mathbb{N}$, the $i(k+1)$th position of σ' has label $\{\psi \in sub(\phi) : \sigma, i \models \psi\}$ and data value 0.
- For $i \in \mathbb{N}$ and $j \in \{1, \ldots, k\}$, the $i(k+1) + j$th position of σ' has data value $\sigma(i)(x_j)$.

Observe that obviously $\sigma' \models \varphi_{k+1}$. Moreover, by structural induction, one can show that for any subformula ψ of ϕ and $i \in \mathbb{N}$, we have $\sigma, i \models \psi$ iff the label of the $i(k+1)$th position contains the subformula ψ. Consequently, $\sigma' \models \bigwedge_{\psi \in sub(\phi)} \varphi_\psi$. Since $\sigma, 0 \models \phi$, we also get $\sigma' \models \exists\ \mathtt{x}_0\ \mathtt{x}_0 = 0 \wedge \phi(\mathtt{x}_0)$. Hence $\sigma' \models \phi'$.

Now suppose that σ' is a model for $\mathrm{FO2}^{\Sigma_\phi}(\sim, <, +\omega)$ such that $\sigma' \models \phi'$. We build a model σ for $\mathrm{CLTL}^{\mathsf{XF}}$ formulae as follows: for $i \in \mathbb{N}$ and $j \in \{1, \ldots, k\}$, $\sigma(i)(x_j)$ is equal to the data value at the $i(k+1) + j$th position of σ'. Similarly, by structural induction, one can show that for any subformula ψ of ϕ and $i \in \mathbb{N}$, we have $\sigma, i \models \psi$ iff the label at the $i(k+1)$th position of σ' contains the subformula ψ. Consequently, since $\sigma' \models \exists\ \mathtt{x}_0\ \mathtt{x}_0 = 0 \wedge \phi(\mathtt{x}_0)$, we obtain $\sigma \models \phi$. □

Corollary 1 *The finitary and infinitary satisfiability problems for* $\mathrm{CLTL}^{\mathsf{XF}}$ *are decidable.*

4 Automata-based Approach with Symbolic Models

In this section we explain how satisfiability can be solved using symbolic models which are abstractions of concrete $\mathrm{CLTL}^{\mathsf{XF}}$ models. We describe here the outline of our automata-based approach, and consider the technical details in Sections 5 to 7. We will treat the case of infinite models first, and then provide the main modifications needed for dealing with the case of finite models.

4.1 Symbolic Models

Let ϕ be a $\mathrm{CLTL}^{\mathsf{XF}}$ formula built over variables in $\{x_1, \ldots, x_k\}$. Let l be the maximal i such that a term of the form $\mathsf{X}^i x$ occurs in ϕ. The value l is called the X-*length* of ϕ. In order to define the set of atomic formulae used in our symbolic models we introduce the set of constraints Ω^l_k that contains constraints of the form either $\mathsf{X}^i x = \mathsf{X}^j y$ or $\mathsf{X}^i(x = \mathsf{XF} y)$ with $x, y \in \{x_1, \ldots, x_k\}$ and $i, j \in \{0, \ldots, l\}$. We show here that models can be abstracted by sequences of "frames" which are subsets of Ω^l_k.

For infinite models, we define an (l, k)-*frame* to be a set of constraints $fr \subseteq \Omega^l_k$ that is *maximally consistent* in that it satisfies the conditions below:

(F1) For all $i \in \{0, \ldots, l\}$ and $x \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^i x = \mathsf{X}^i x \in fr$.

(F2) For all $i, j \in \{0, \ldots, l\}$ and $x, y \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^i x = \mathsf{X}^j y \in fr$ iff $\mathsf{X}^j y = \mathsf{X}^i x \in fr$.

(F3) For all $i, j, j' \in \{0, \ldots, l\}$ and $x, y, z \in \{x_1, \ldots, x_k\}$, if $\{\mathsf{X}^i x = \mathsf{X}^j y, \mathsf{X}^j y = \mathsf{X}^{j'} z\} \subseteq fr$ then $\mathsf{X}^i x = \mathsf{X}^{j'} z \in fr$.

(F4) For all $i, j \in \{0, \ldots, l\}$ and $x, y \in \{x_1, \ldots, x_k\}$ such that $\mathsf{X}^i x = \mathsf{X}^j y \in fr$:

- if $i = j$, then for every $z \in \{x_1, \ldots, x_k\}$ we have $\mathsf{X}^i(x = \mathsf{XF} z) \in fr$ iff $\mathsf{X}^j(y = \mathsf{XF} z) \in fr$;
- if $i < j$ then $\mathsf{X}^i(x = \mathsf{XF} y) \in fr$, and for $z \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^i(x = \mathsf{XF} z) \in fr$ iff either $\mathsf{X}^j(y = \mathsf{XF} z) \in fr$ or there exists $i < j' \leq j$ such that $\mathsf{X}^i x = \mathsf{X}^{j'} z \in fr$.

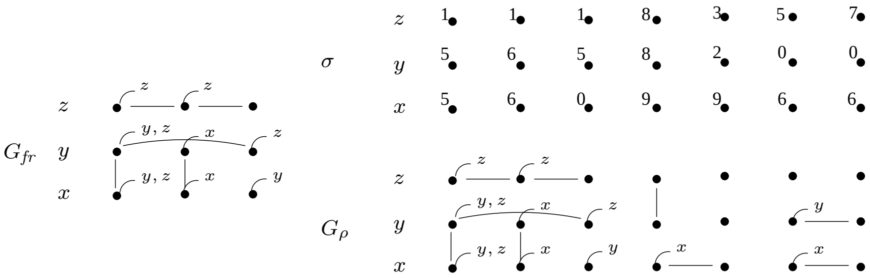


Figure 1: Example of (2,3)-frame graph, concrete model σ and its induced (2,3)-frame graph G_ρ.

Conditions (F1)–(F3) simply encode that equality is an equivalence relation while condition (F4) states a consistency property related to repetition constraints. We denote by $\texttt{Frame}_k^l$ the set of (l,k)-frames. We say that a model σ satisfies a frame fr at position i (denoted $\sigma, i \models fr$) iff $\sigma, i \models \varphi$ for every constraint φ in fr. A frame is therefore a finite set of constraints about $l+1$ consecutive positions.

An (l,k)-frame fr can be represented as an annotated undirected graph G_{fr} which has vertices (x,i) for $x \in \{x_1,\ldots,x_k\}$ and $i \in \{0,\ldots,l\}$, and an edge between (x,i) and (y,j) iff the constraint $\mathsf{X}^i x = \mathsf{X}^j y$ belongs to fr. Each vertex (x,i) in the graph is annotated with an "open" arc labelled by the set of *future obligations* (i.e., repetition constraints) $\mathsf{XF}_{fr}(x,i)$ for that vertex, which is defined by

$$\mathsf{XF}_{fr}(x,i) \overset{\text{def}}{=} \{y \mid \mathsf{X}^i(x = \mathsf{XF}y) \in fr\}.$$

The *level* of a node (x,i) in fr is defined to be i, and the equivalence class of x at level i in fr is defined to be

$$[(x,i)]_{fr} \overset{\text{def}}{=} \{y \mid \mathsf{X}^i x = \mathsf{X}^i y \in fr\}.$$

Figure 1 presents an example of (2,3)-frame over the set $\{x,y,z\}$. Some edges obtained by transitivity are omitted for the sake of clarity.

A pair of (l,k)-frames $\langle fr, fr'\rangle$ is said to be *one-step consistent* iff

(OSC1) for all $\mathsf{X}^i x = \mathsf{X}^j y \in \Omega_k^l$ with $0 < i, j$, we have $\mathsf{X}^i x = \mathsf{X}^j y \in fr$ iff $\mathsf{X}^{i-1} x = \mathsf{X}^{j-1} y \in fr'$,

(OSC2) for all $\mathsf{X}^i(x = \mathsf{XF}y) \in \Omega_k^l$ with $i > 0$, we have $\mathsf{X}^i(x = \mathsf{XF}y) \in fr$ iff $\mathsf{X}^{i-1}(x = \mathsf{XF}y) \in fr'$.

An (infinite) (l,k)*-symbolic model* is an infinite sequence ρ of (l,k)-frames such that for every $i \in \mathbb{N}$, the pair $\langle \rho(i), \rho(i+1)\rangle$ is one-step consistent. We say a model σ *realizes* a symbolic model ρ (or equivalently that ρ *admits* a model σ) iff for every $i \in \mathbb{N}$, we have $\rho(i) = \{\varphi \in \Omega_k^l \mid \sigma, i \models \varphi\}$.

An (l,k)-symbolic model ρ can also be represented as an annotated graph G_ρ as done for (l,k)-frames. Thus the vertices of G_ρ are of the form (x,i) with an edge between (x,i) and (y,j) with $0 \le j - i \le l$ iff there is an edge between $(x,0)$ and $(y, j-i)$ in the frame graph $G_{\rho(i)}$. The annotations for future obligations are added similarly. We say the *level* of a node (x,i) in G_ρ is i. The notations for future obligations and equivalence classes in symbolic models are extended as following:

$$\mathsf{XF}_\rho(x,i) = \mathsf{XF}_{\rho(i)}(x,0) \qquad \text{and} \qquad [(x,i)]_\rho = [(x,0)]_{\rho(i)}.$$

Figure 1 shows the initial portion of the graph representation of a $(2,3)$-symbolic model ρ.

A *path* p in G_ρ is a (finite or infinite) sequence of vertices $v_0, v_1 \ldots$ in G_ρ such that for each i, the vertices v_i and v_{i+1} are connected by an edge in G_ρ. A *forward* (or *level-increasing*) path is a path $v_0, v_1 \ldots$ such that for each i, the level of v_{i+1} is strictly greater than the level of v_i.

Let us define the *symbolic satisfaction relation* $\rho, i \models_{\text{symb}} \phi$ where ϕ is a formula of X-length at most l, ρ is an (l,k)-symbolic model and $i < |\rho|$. The relation $\models_{\text{symb}}$ is defined in the same way as $\models$ for CLTL$^{\mathsf{XF}}$, except that for atomic formulae φ we have:

$$\rho, i \models_{\text{symb}} \varphi \overset{\text{def}}{\Leftrightarrow} \varphi \in \rho(i).$$

We can now make an observation that plays a central role in our symbolic approach.

Lemma 3 *A* CLTL$^{\mathsf{XF}}$ *formula ϕ of* X*-length l over the variables $\{x_1, \ldots, x_k\}$ is satisfiable over infinite models iff there exists an infinite (l,k)-symbolic model ρ such that $\rho \models_{\text{symb}} \phi$ and ρ admits a model (i.e. ρ is realizable).*

Proof. Suppose that a CLTL$^{\mathsf{XF}}$ formula ϕ is satisfied by an infinite model σ. Now σ induces a natural symbolic model ρ given by $\rho(i) = \{\psi \in \Omega^l_k \mid \sigma, i \models \psi\}$. It is easy to see that ρ satisfies the one-step consistency property. By definition of the symbolic satisfaction relation $\sigma, i \models \psi$ iff $\rho, i \models_{\text{symb}} \psi$ for every atomic constraint ψ of ϕ. It then follows by induction on the structure of ϕ that $\rho \models_{\text{symb}} \phi$ since the symbolic satisfaction relation differs from CLTL$^{\mathsf{XF}}$ satisfaction relation only at the atomic level.

Conversely, suppose that there is a realizable symbolic model ρ such that $\rho \models_{\text{symb}} \phi$. Since ρ is realizable, let σ be an infinite model admitted by ρ. Thus, for every $i \in \mathbb{N}$, we have that $\rho(i)$ is exactly the set of atomic constraints in Ω^l_k satisfied by σ at position i. So for every atomic constraint ψ of ϕ we again have that $\rho, i \models_{\text{symb}} \psi$ iff $\sigma, i \models \psi$. Once again, we can now proceed by induction on the structure of ϕ to show that $\sigma \models \phi$. □

4.2 Automata for Symbolic Models

We can now outline our automata-based decision procedure for infinitary satisfiability of CLTL$^{\mathsf{XF}}$. This approach is similar to the automata-theoretic approach for LTL defined in [VW94], and for constraint LTL in [DD07]. Given a CLTL$^{\mathsf{XF}}$ formula ϕ, we will construct an automaton $\mathcal{A}_\phi$ whose language is nonempty iff ϕ is satisfiable. The automaton $\mathcal{A}_\phi$ will be a special kind of counter automaton with a generalised Büchi acceptance condition, whose nonemptiness problem is decidable.

Let ϕ be a CLTL$^{\mathsf{XF}}$ formula of X-length l, over the variables $\{x_1, \ldots, x_k\}$. We exploit Lemma 3, to define $\mathcal{A}_\phi$ as an automaton over the alphabet $\mathtt{Frame}^l_k$, that accepts the intersection of the languages accepted by the three automata $\mathcal{A}_{\text{1sc}}$, $\mathcal{A}_{\text{symb}}$ and $\mathcal{A}_{\text{real}}$ described below:

- $\mathcal{A}_{\text{1sc}}$ recognizes the set of "valid" symbolic models (i.e. sequences of frames such that every pair of consecutive frames is one-step consistent),
- $\mathcal{A}_{\text{symb}}$ recognizes the set of symbolic models satisfying ϕ,
- $\mathcal{A}_{\text{real}}$ recognizes the set of symbolic models that are realizable.

The automaton $\mathcal{A}_{\text{1sc}}$ is a Büchi automaton that checks that the sequence is one-step consistent. Formally, we build $\mathcal{A}_{\text{1sc}} = \langle Q, Q_0, F, \rightarrow \rangle$ such that

- Q is the set of (l,k)-frames and $Q_0 = Q$,
- the transition relation is defined by $fr_1 \xrightarrow{fr} fr_2$ iff $fr = fr_1$ and the pair $\langle fr_1, fr_2 \rangle$ is one-step consistent,
- the set of final states F is equal to Q.

We define the generalized Büchi automaton $\mathcal{A}_{\text{symb}}$ by adapting the construction from [VW94] for LTL. We define $cl(\phi)$ to be the standard *closure* of ϕ, namely the smallest set of formulas X that contains ϕ, is closed under subformulas, and satisfies the following conditions:

- If $\psi \in X$ and ψ is not of the form $\neg\psi_1$ for some ψ_1, then $\neg\psi \in X$.
- If $\psi_1 \mathsf{U} \psi_2 \in X$ then $\mathsf{X}(\psi_1 \mathsf{U} \psi_2) \in X$.
- If $\psi_1 \mathsf{S} \psi_2 \in X$ then $\mathsf{X}^{-1}(\psi_1 \mathsf{S} \psi_2) \in X$.

An *atom* of ϕ is a subset At of $cl(\phi)$ which is maximally consistent in that it satisfies the following conditions:

- For every $\neg\psi \in cl(\phi)$, we have $\neg\psi \in At$ iff $\psi \notin At$.
- For every $\psi_1 \wedge \psi_2 \in cl(\phi)$, we have $\psi_1 \wedge \psi_2 \in At$ iff ψ_1 and ψ_2 are in At.
- For every $\psi_1 \vee \psi_2 \in cl(\phi)$, we have $\psi_1 \vee \psi_2 \in At$ iff ψ_1 or ψ_2 is in At.
- For every $\psi_1 \mathsf{U} \psi_2 \in cl(\phi)$, we have $\psi_1 \mathsf{U} \psi_2 \in At$ iff either $\psi_2 \in At$ or both ψ_1 and $\mathsf{X}(\psi_1 \mathsf{U} \psi_2)$ are in At.
- For every $\psi_1 \mathsf{S} \psi_2 \in cl(\phi)$, we have $\psi_1 \mathsf{S} \psi_2 \in At$ iff either $\psi_2 \in At$ or both ψ_1 and $\mathsf{X}^{-1}(\psi_1 \mathsf{S} \psi_2)$ are in At.

We denote by $\mathrm{Atom}(\phi)$ the set of atoms of ϕ.

We now define $\mathcal{A}_{\mathrm{symb}} = (Q, Q_0, \rightarrow, \mathcal{F})$ over the alphabet $\mathtt{Frame}^l_k$, where:

- $Q = \mathrm{Atom}(\phi)$ and $Q_0 = \{At \in Q \mid \phi \in At,\ \mathsf{X}^{-1}\top \notin At\}$,
- $At \xrightarrow{fr} At'$ iff

  (atomic) The set of atomic constraints in At is exactly fr, that is $At \cap \Omega^l_k = fr$.

  (one step) For every $\mathsf{X}\psi \in cl(\phi)$, $\mathsf{X}\psi \in At$ iff $\psi \in At'$, and for every $\mathsf{X}^{-1}\psi \in cl(\phi)$, $\psi \in At$ iff $\mathsf{X}^{-1}\psi \in At'$.
- Let $\{\psi_1 \mathsf{U} \phi_1, \ldots, \psi_r \mathsf{U} \phi_r\}$ be the set of until formulae in $cl(\phi)$. We set $\mathcal{F} = \{F_1, \ldots, F_r\}$ where for every $i \in \{1, \ldots, r\}$, $F_i = \{At \in Q : \psi_i \mathsf{U} \phi_i \notin At \text{ or } \phi_i \in At\}$. We recall that a run is accepting according to the generalized Büchi condition $\{F_1, \ldots, F_r\}$ iff the run visits each F_i set infinitely often. A generalized Büchi condition can be easily converted to a standard Büchi condition.

We will need to dedicate the following sections to the construction of the automaton $\mathcal{A}_{\mathrm{real}}$ recognizing the set of realizable symbolic models. But assuming we have this construction, we can state the following result as a direct consequence of Lemma 3.

Theorem 3 *A* $\mathrm{CLTL}^{\mathsf{XF}}$ *formula* ϕ *is satisfiable over infinite models iff the language recognized by* $\mathcal{A}_\phi$ *is nonempty.*

An interesting feature of this automata-theoretic approach is the separation between the machinary for handling the carrier logic (namely temporal logic), and the logic of atomic constraints, by defining different automata to handle each part separately. This allows us to extend the decidability results to any extension of LTL that induces an ω-regular class of models, by changing the definition of $\mathcal{A}_{\mathrm{symb}}$ suitably.

4.3 Updates for treating finitary satisfiability

The symbolic approach can be easily adapted for finitary satisfiability. We briefly explain below the main modifications. First, we slightly change the definition of frames in order to add an information about the possibility to end the model before the end of the current window of length $l+1$. This allows to handle also the particular case when the finite model has a length smaller than $l+1$. The set of (l,k) frames for the finite case will be denoted $\mathtt{FFrame}^l_k$, and is made up of pairs comprising a maximal consistent set of atomic constraints, along with some information about the last position of the model. This latter component is an element of $\{0, \ldots, l\} \uplus \{\mathrm{nd}\}$ where nd means that the model does not end before the end of the frame. We have $\langle fr, i\rangle \in \mathtt{FFrame}^l_k$ iff $i = \mathrm{nd}$ and fr satisfies the conditions (F1)–(F5) (from the infinitary case) or $i \in \{0, \ldots, l\}$ and $fr \subseteq \Omega^i_k$ satisfies the conditions below:

(F1′) For all $j \in \{0, \ldots, i\}$ and $x \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^j x = \mathsf{X}^j x \in fr$.

(F2′) For all $j, j' \in \{0, \ldots, i\}$ and $x, y \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^j x = \mathsf{X}^{j'} y \in fr$ iff $\mathsf{X}^{j'} y = \mathsf{X}^j x \in fr$.

(F3′) For all $j, j', j'' \in \{0, \ldots, i\}$ and $x, y, z \in \{x_1, \ldots, x_k\}$, if $\{\mathsf{X}^j x = \mathsf{X}^{j'} y, \mathsf{X}^{j'} y = \mathsf{X}^{j''} z\} \subseteq \mathit{fr}$ then $\mathsf{X}^j x = \mathsf{X}^{j''} z \in \mathit{fr}$.

(F4′) For all $j, j' \in \{0, \ldots, i\}$ and $x, y \in \{x_1, \ldots x_k\}$ such that $\mathsf{X}^j x = \mathsf{X}^{j'} y \in \mathit{fr}$:

- if $j = j'$, then for every $z \in \{x_1, \ldots, x_k\}$ we have $\mathsf{X}^j(x = \mathsf{XF}z) \in \mathit{fr}$ iff $\mathsf{X}^{j'}(y = \mathsf{XF}z) \in \mathit{fr}$;
- if $j < j'$ then $\mathsf{X}^j(x = \mathsf{XF}y) \in \mathit{fr}$, and for $z \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^j(x = \mathsf{XF}z) \in \mathit{fr}$ iff either $\mathsf{X}^{j'}(y = \mathsf{XF}z) \in \mathit{fr}$ or there exists $j < j'' \leq j'$ such that $\mathsf{X}^j x = \mathsf{X}^{j''} z \in \mathit{fr}$.

(F5′) For every constraint $\mathsf{X}^j(x = \mathsf{XF}y) \in \mathit{fr}$ such that $j \in \{0, \ldots, i\}$ there is $j < j' \leq i$ such that $\mathsf{X}^j x = \mathsf{X}^{j'} y \in \mathit{fr}$.

The last condition (F5′) imposes that every future obligation is satisfied before the end of the model. The conditions (F1′)–(F4′) are variants of (F1)–(F4) in which, roughly speaking, the value l is replaced by i (index of the last position in the model). A finite model σ satisfies a frame $\langle \mathit{fr}, i\rangle \in \mathtt{FFrame}^l_k$ at position j iff

- either $i = \mathrm{nd}$ and $|\sigma| - (j+1) \geq l + 1$, or $i = |\sigma| - (j+1)$,
- for every constraint φ in fr we have $\sigma, j \models \varphi$.

In this case, we write $\sigma, j \models \langle \mathit{fr}, i\rangle$.

We also need to adapt the notations related to frames. We set $\mathsf{XF}_{\langle \mathit{fr}, j\rangle}(x, i) = [(x, i)]_{\langle \mathit{fr}, j\rangle} = \emptyset$ when $j \neq \mathrm{nd}$ and $i > j$. If $j = \mathrm{nd}$ or $i \leq j$ then the definition is similar to the infinitary case. In the finitary case, a pair of (l, k)-frames $\langle\langle \mathit{fr}, i\rangle, \langle \mathit{fr}', i'\rangle\rangle$ is one-step consistent iff

- $\langle i, i'\rangle$ belongs to $\{\langle j, j'\rangle \in \{1, \ldots, l\} \times \{0, \ldots, l-1\} : j' = j - 1\} \cup \{\langle \mathrm{nd}, \mathrm{nd}\rangle, \langle \mathrm{nd}, l\rangle\}$.
- $\langle \mathit{fr}, \mathit{fr}'\rangle$ satisfies the conditions for the infinitary case when $i = i' = \mathrm{nd}$.
- $\langle \mathit{fr}, \mathit{fr}'\rangle$ satisfies the conditions below when $i \in \{1, \ldots, l\}$:
  - for every $\mathsf{X}^j x = \mathsf{X}^{j'} y \in \Omega^i_k$ with $0 < j, j'$, we have $\mathsf{X}^j x = \mathsf{X}^{j'} y \in \mathit{fr}$ iff $\mathsf{X}^{j-1} x = \mathsf{X}^{j'-1} y \in \mathit{fr}'$,
  - for every $\mathsf{X}^j(x = \mathsf{XF}y) \in \Omega^i_k$ with $j > 0$, we have $\mathsf{X}^j(x = \mathsf{XF}y) \in \mathit{fr}$ iff $\mathsf{X}^{j-1}(x = \mathsf{XF}y) \in \mathit{fr}'$.

A symbolic model is a finite one-step consistent sequence of frames ending with a symbolic valuation of the form $\langle \mathit{fr}, 0\rangle$. Hence, for every position i in a finite symbolic model ρ, if $|\rho| - (i+1) \geq l + 1$ then $\rho(i)$ is of the form $\langle \mathit{fr}, \mathrm{nd}\rangle$, otherwise $\rho(i)$ is of the form $\langle \mathit{fr}, |\rho| - (i+1)\rangle$.

The symbolic satisfaction relation $\rho, i \models_{\mathrm{symb}} \phi$ is defined similarly to the infinitary case but we consider that $\varphi \in \langle \mathit{fr}, i\rangle$ whenever φ belongs to the set fr. The following correspondence between symbolic and concrete models can be shown similarly:

Lemma 4 *A* CLTL$^{\mathsf{XF}}$ *formula ϕ of* X*-length l over the variables $\{x_1, \ldots, x_k\}$ is satisfiable over finite models iff there exists a finite (l, k)-symbolic model ρ such that $\rho \models_{\mathrm{symb}} \phi$ and ρ is realizable.*

Consequently, the automaton construction follows the same lines. We just state the changes in the different automata. In the finitary case, the automaton $\mathcal{A}_{1\mathrm{sc}}$ checking one-step consistency has the additional constraint that the last frame must be of the form $\langle \mathit{fr}, 0\rangle$. The set of final states is therefore equal to $\{\langle \mathit{fr}, 0\rangle \mid \langle \mathit{fr}, 0\rangle \in \mathtt{FFrame}^l_k\}$. As usual, a run is accepting if it ends in a final state.

The finite-state automaton $\mathcal{A}_{\mathrm{symb}}$ accepting finite words over the alphabet $\mathtt{FFrame}^l_k$ has to take care of the end of the model in order to evaluate the subformulae; the run has to end with a state corresponding to the end of the model. So we have to store the last frame read by defining $Q = \mathrm{Atom}(\phi) \times (\mathtt{FFrame}^l_k \cup \{\sharp\})$ ($\sharp$ is used for initial states). The set of initial states I is $\{\langle At, \sharp\rangle \mid \phi \in At\}$ and the set of final states F is the set of states of the form $\langle At, \langle \mathit{fr}, 0\rangle\rangle$. Finally, the transition relation is such that $\langle At, X\rangle \xrightarrow{\langle \mathit{fr}, i\rangle} \langle At', \langle \mathit{fr}, i\rangle\rangle$ iff

(atomic) if $i = \text{nd}$ then $At \cap \Omega^l_k = fr$, otherwise $At \cap \Omega^i_k = fr$,

(one-step) 1. if $i = 0$ then there is no formula of the form $\mathsf{X}\psi$ in At, otherwise for every $\mathsf{X}\psi \in cl(\phi)$, we have $\mathsf{X}\psi \in At$ iff $\psi \in At'$

2. for every $\mathsf{X}^{-1}\psi \in cl(\phi)$, we have $\psi \in At$ iff $\mathsf{X}^{-1}\psi \in At'$.

The construction of the automaton $\mathcal{A}_{\text{real}}$ that recognizes the set of realizable symbolic models will be described in the following sections.

5 Characterization of Realizable Symbolic Models

In order to determine whether a symbolic model ρ is realizable (i.e., it admits a concrete model), we introduce counters that record the number of constraints of the form $x = \mathsf{XF}y$ left unsatisfied at the current position. If the conjunction $x = \mathsf{XF}y_1 \wedge \cdots \wedge x = \mathsf{XF}y_n$ needs to be satisfied at the current position i and none of the conjuncts is satisfied by $\rho(i)$, then we shall increment a counter associated with $\{y_1, \ldots, y_n\}$ that remembers this set of obligations. In a finite model, all the obligations need to be fulfilled at the last position whereas in an infinite model either no more unsatisfied obligations arise after a point, or they are essentially fulfilled infinitely often. The exact conditions will be spelt out soon.

For the rest of this section we consider (l, k)-symbolic models, for a fixed l and k.

5.1 Counting Sequence along a Symbolic Model

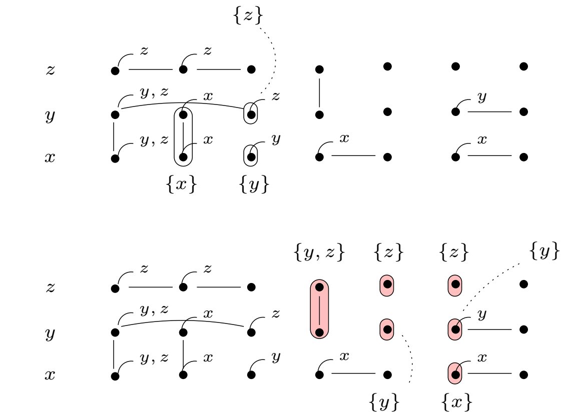
For each $X \in \mathcal{P}^+(\{x_1, \ldots, x_k\})$ (the set of non-empty subsets of $\{x_1, \ldots, x_k\}$), we introduce a counter that keeps track of the number of obligations that need to be satisfied by X. We identify the counters with finite subsets of $\{x_1, \ldots, x_k\}$. A *counter valuation* $\vec{c}$ is a map from $\mathcal{P}^+(\{x_1, \ldots, x_k\})$ to $\mathbb{N}$. For instance, we write $\vec{c}(\{x, y\})$ to denote the value of the counter $\{x, y\}$, which will stand for the number of distinct obligations to repeat a value in x and in y.

We define below a canonical sequence of counter valuations along a symbolic model. We will need to introduce some additional definitions first. For an (l, k)-frame fr and a counter $X \in \mathcal{P}^+(\{x_1, \ldots, x_k\})$, we define a *point of increment* for X in fr to be an equivalence class of the form $[(x, 0)]_{fr}$ such that $\mathsf{XF}_{fr}(x, 0) = X$ and $(x, 0)$ is not connected by a forward edge to a node in fr (i.e., there is no edge between $(x, 0)$ and some (y, j) with $j \in \{1, \ldots l\}$). Such an equivalence class corresponds to a value at the current state that is not repeated in a future value of an X-variable in the current frame, but which needs to be repeated in some future value of each of the variables in X. Note that if the node was connected to a node of higher level then the set of obligations would be propagated to this node (condition **(F4)**) and we would not need to store this obligation. In a similar way, a *point of decrement* for X in fr is defined to be an equivalence class of the form $[(x, l)]_{fr}$ such that $\mathsf{XF}_{fr}(x, l) \cup [(x, l)]_{fr} = X$, and (x, l) is not connected by a backward edge to another node in fr (i.e., there is no edge between (x, l) and some (y, j) with $j \in \{0, \ldots l - 1\}$). Intuitively, such an equivalence class is not constrained by values in the past so it can be used to satisfy some obligation linked to X. Note that the obligation may be only partially satisfied (when $[(x, l)]_{fr}$ is a strict subset of X) but since $X \setminus [(x, l)]_{fr} \subseteq \mathsf{XF}_{fr}(x, l)$ the remaining obligations will be treated when considering the set of obligations $\mathsf{XF}_{fr}(x, l)$ associated with the elements of $[(x, l)]_{fr}$.

For partial frames that arise in the case of finite symbolic models, namely frames of the form $\langle fr, i \rangle \in \mathtt{FFrame}^l_k$ with $i \neq \text{nd}$, we define a point of increment in a similar way as above; however there are no points of decrement in a partial frame.

Note that the definition above allows the existence of several points of increment for a given set X in the same frame, as different equivalence classes can have the same set of future obligations. Similarly, it is possible to have several points of decrement for the same set X.

We denote by u^+_{fr} the counter valuation which records the number of points of increment for each counter X in fr. Similarly u^-_{fr} is the counter valuation which records the number of points of decrement for each counter X in fr. Observe that the codomain of both u^+_{fr} and u^-_{fr} is $\{0, \ldots, k\}$.



$\{x\}$	0	0	1	0	0
$\{y\}$	0	0	0	0	0
$\{z\}$	0	0	0	0	0
$\{y, z\}$	0	0	0	0	0

Figure 2: Points of increment, points of decrement (shaded), and the induced counting sequence.

Let ρ be an (l, k)-symbolic model. For $X \in \mathcal{P}^+(\{x_1, \ldots, x_k\})$, a *point of increment* for X in ρ is an equivalence class of the form $[(x, i)]_\rho$ such that $[(x, 0)]_{\rho(i)}$ is a point of increment for X in the frame $\rho(i)$. Similarly, a *point of decrement* for X in ρ is an equivalence class of the form $[(x, i)]_\rho$ such that $i \geq l + 1$ and $[(x, l)]_{\rho(i-l)}$ is a point of decrement for X in $\rho(i - l)$. Figure 2 shows the points of increment (top), and points of decrement (middle), for the example symbolic model of Fig 1.

We can now define a canonical counter valuation sequence α along ρ, called the *counting sequence* along ρ, which counts the number of obligations corresponding to each subset of variables X that remain unsatisfied at each position. Let $\dot{+}$ denote the *proper addition* of integers, defined by $n \dot{+} m = \max(0, n + m)$. We define α inductively: for each $X \in \mathcal{P}^+(\{x_1, \ldots, x_k\})$ we have $\alpha(0)(X) = 0$ and

$$\alpha(i + 1)(X) = \alpha(i)(X) \dot{+} (u^+_{\rho(i)}(X) - u^-_{\rho(i+1)}(X)),$$

for every $0 \leq i < |\rho|$.

5.2 Characterising Realizable Symbolic Models

The following result shows that the set of realizable symbolic models can be characterized using their counting sequences.

Lemma 5 **(I)** *A finite symbolic model ρ is realizable iff for every counter X the final value of the counting sequence α along ρ is equal to* 0 *(i.e., $\alpha(|\rho| - 1)(X) = 0$).*

(II) *An infinite symbolic model ρ is satisfiable iff all the following conditions are satisfied:*

(C1) *There does not exist an infinite forward path p in ρ and a counter X, such that every node in the path has future obligation X, and there is a variable y in X which is never connected by a forward edge from a node in p (i.e. no node in p is connected by a forward edge to a node of the form (y, i)).*

(C2) *In the counting sequence along ρ, each counter X satisfies one of the conditions:*

(a) there is a point after which the value of counter X is always zero and after which we never see a point of increment for X, or,

(b) infinitely often we see a point of decrement for X which is connected by a forward path to a point of increment of the form $[u]_\rho$ with $\mathsf{XF}_\rho(u) \subset X$ (where '$\subset$' denotes "strict subset"), or,

(c) for each $x \in X$, we infinitely often see a point of decrement for X, which is connected by a forward path to an x node (i.e a node of the form (x, i)).

Proof. Let ρ be an (l, k)-symbolic model, which admits a concrete model σ. We show that ρ satisfies the conditions above.

Consider a point of increment $[(x, i)]_\rho$ for a counter X. Then in the concrete model σ, the value $\sigma(i)(x)$ subsequently repeats in all the variables in X. Let (y, j) be the *first* time this happens. So $y \in X$ and $\sigma(j)(y) = \sigma(i)(x)$. We claim that $[(y, j)]_\rho$ must be a point of decrement for X. This is true since by the choice of (y, j), it cannot be connected to any node to the left of it, and clearly $\mathsf{XF}_\rho(x, i) = [(y, j)]_\rho \cup \mathsf{XF}_\rho(y, j)$. Further, the correspondence between points of increment and points of decrement described above is injective. If not, let $[(x, i)]_\rho$ and $[(x', i')]_\rho$ be two distinct points of increment with the same corresponding point of decrement $[(y, j)]_\rho$. Without loss of generality, we assume $i \leq i'$. If $i = i'$, it would mean $\sigma(i)(x) = \sigma(i)(x')$ (since they both have the same value as (y, j) by assumption), which would contradict the fact that $[(x, i)]_\rho$ and $[(x', i')]_\rho$ were assumed to be distinct. If $i < i'$, then (y, j) could not have been the first repeat for (x, i) since (x', i') is one such repeat and it occurs strictly before (y, j).

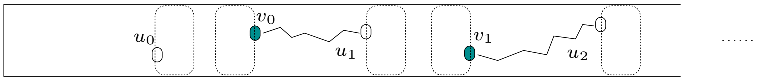
Now if ρ was a finite sequence, then clearly the value of each counter X is 0 in $\alpha(|\rho|-1)$. This is due to the fact that by the above correspondence, each point of increment for X is cancelled out by a unique point of decrement for X. Furthermore, the last frame in ρ clearly cannot have any unsatisfied obligations. This proves that the conditions of Lemma 5 **(I)** are satisfied for the case of finite symbolic models.

Consider now the case when ρ is an infinite symbolic model. We show that conditions (C1) and (C2) are satisfied. Let p be an infinite forward path from a vertex u in G_ρ and let $y \in \mathsf{XF}_\rho(u)$. Since $y \in \mathsf{XF}_\rho(u)$, it must be the case that the value of u in the concrete model σ repeats at some future point in a y-node, say (y, j). Now the path p must pass through a node v in the (l, k)-frame $\rho(j - l)$ to which (y, j) belongs. Since the value of v must be same as that of u, which in turn is same as that of (y, j), there must be an edge between v and (y, j) in $\rho(j - l)$. This proves that ρ satisfies the condition (C1).

To see that condition (C2) is satisfied, let X be any counter. Two cases arise: either we have only finitely many points of increment for X in ρ, or there are infinitely many. For the first case, the correspondence between increment points and decrement points implies that there is a level i at which the last point of decrement corresponding to a point of increment for X occurs. At this position we clearly have $\alpha(i - l)(X) = 0$. Further, by the choice of i, we never see a point of increment for X after level i, and the value of X in α stays 0. Thus in this case condition (C2.a) is satisfied.

For the case when there are infinitely many points of increment for X, suppose that X satisfies neither (C2.b) nor (C2.c). Then there must be a variable $y \in X$ and a level i after which we never see a point of decrement for X which is connected by a forward path to a point of increment for X with future obligation strictly smaller than X, nor a point of decrement for X which is connected by a forward path to a y-node. Consider any point of increment $[u_0]_\rho$ for X after level i. Let its value in the concrete model be m. In the concrete model, m must subsequently repeat in a y-node. Let this node be (y, j). Now for $[u_0]_\rho$ there is a corresponding point of decrement $[v_0]_\rho$ for X (obtained as above by taking the first node where the value m repeats). Note that there cannot exist an infinite forward path from v_0, since otherwise by an argument similar to the one for C1 above, we would have a forward path from v_0 to (y, j), contradicting our assumption. So there is a maximal forward path (possibly of length 0) from v_0 to a node u_1, which (again by our assumptions) must necessarily be such that $[u_1]_\rho$ forms a point of increment for X. This argument can be repeated to construct a sequence of nodes

$u_0, v_0, u_1, v_1, \ldots$ such that each $[u_i]_\rho$ and $[v_i]_\rho$ are respectively points of increment and decrement for X, and there is a forward path from each v_i to each u_{i+1}. This is shown below:



It is also clear that by construction, all the nodes above (as well as the nodes in the paths between the v_i's and u_{i+1}'s) have the value m in the concrete model σ. Now consider the node (y, j). Clearly it cannot lie between any u_i and v_i. Thus it must lie between some v_i and u_{i+1}, and must be connected by a forward edge from a node in the path between them. This contradicts our assumption that after level i, no point of decrement for X was connected by a forward path to a y-node.

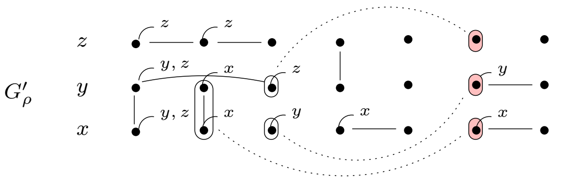
Thus for the case when ρ is infinite, we have shown that ρ must satisfy the conditions of Lemma 5 **(II)**.

For the converse direction, let ρ be an (l, k)-symbolic model satisfying the conditions of Lemma 5. We will show that ρ admits a concrete model by first describing an augmented graph G'_ρ which is obtained from G_ρ by adding additional edges, and then describing a labelling procedure for G_ρ which respects the edges in G_ρ.

For the case when ρ is finite, the augmented graph G'_ρ is obtained from G_ρ by adding edges (which we call *augmented* edges) as follows:

> From each level i going from $l + 1$ upto $|\rho| - 1$, for each counter X, and for each point of decrement $[v]_\rho$ for X at level i, if there is a point of increment $[u]_\rho$ for X at a level less than $i - l$ for which an augmented edge has not been added (we call this an "unmatched" point of increment), add augmented edges between every node in $[u]_\rho$ and every node in $[v]_\rho$.

Here is (the only) way of adding augmented edges according to the procedure above in the example symbolic model of Fig. 1:



We note that when the procedure has completed for level i, the number of unmatched points of increment for every counter X is precisely $\alpha(i)(X)$, the value for the counter X at position i in the counting sequence α for ρ. Since $\alpha(|\rho| - 1)(X) = 0$ for each X, it follows that at the end of the procedure above, we will have no unmatched points of increment.

For the case when ρ is infinite, we add the augmented edges in a slightly different way. If a counter X is such that a point of increment for it occurs only finitely often in G_ρ, we add the augmented edges between points of increment and points of decrement for X in the same way as the procedure above for the case of finite models. By condition (C2.a), every point of increment for X will be matched. If X is a counter for which points of increment occur infinitely often, then by condition (C2.b) and (C2.c) two cases are possible: either there are infinitely many points of decrement for X which are connected by a forward path to a point of increment with a strictly smaller set of obligations than X, or for each $x \in X$, we infinitely often see a point of decrement for X which is connected by a forward path to an x-node. In the former case, we assign matches by proceeding from left to right, adding augmented edges from each point of increment for X to a subsequent point of decrement for X from which there is a forward path to a point of increment with a strictly smaller set of obligations than X. In the latter case, suppose $X = \{z_1, \ldots, z_m\}$. We assign matches by cycling through the z_i's repeatedly: thus, we proceed from left to right, and assign to the first point of increment for X, a point of decrement for X

that is connected to a z_1-node, to the next point of increment for X a point of decrement for X that is connected by a forward path to z_2 node, and so on till z_m; and keep repeating this process. Thus, this process of matching points of increment covers all points of increment, and so every point of increment has an augmented edge to a subsequent point of decrement.

We now describe a way of labelling the nodes of G_ρ with natural numbers. We use a natural ordering on nodes in G_ρ, given by $(x_m, i) \prec (x_p, j)$ iff $i < j$ or, $i = j$ and $m < p$.

> We label the first vertex $(x_1, 0)$ by 0. The remaining vertices are labelled in order according to the following rule: If L is the portion of the graph already labelled, and u is the next vertex to be labelled:
>
> 1. if there is a path in G'_ρ from u to a vertex v in L, give u the same label as v.
> 2. else, label u by $n + 1$ where n is the maximum label used so far in L.

We note that the labelling above is deterministic, in the sense that in step 1, u can only be assigned a single value. If not, consider the first point that a vertex u had a path to two vertices v and v' with distinct labels. Without loss of generality, say v was labelled before v'. Then there is a path from v' to v in G'_ρ (via u), and hence v' must have been labelled with the same value as v.

The labelling above thus gives us a concrete model σ, and we claim that ρ is in fact the (l, k)-symbolic model l induced by σ, and thus that ρ is realizable. For this it is sufficient to argue that the labelling σ "respects" both the normal and annotated edges of G_ρ, in the following sense: For nodes u and v in G_ρ which lie in the same frame, we have an edge between u and v in G_ρ iff $\sigma(u) = \sigma(v)$. Further, for each u in G_ρ we have an annotated edge from u with x in its label (i.e. $x \in \mathsf{XF}_\rho(u)$) iff there exists an x-node v at a higher level than u with $\sigma(v) = \sigma(u)$.

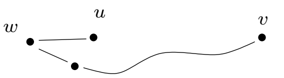
Before we do this let us first observe a useful property of G'_ρ.

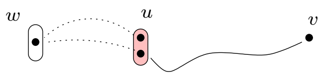
Claim 1. Let $u = (x, i)$ and $v = (y, j)$ be distinct vertices which are connected by a path in G'_ρ. Then

1. if the level of u is strictly less than the level of v (i.e. $i < j$), we have a *forward* path from u to v in G'_ρ.
2. if u and v are at the same level (i.e. $i = j$), we have an edge between u and v.

Proof. [of Claim 1.] We proceed by induction on the length of the shortest path between u and v. In fact we show that the shortest path must be a forward path in the case of $i < j$, and a single edge in the case of $i = j$. If the shortest path between u and v is of length 1, then if $i < j$ we have a forward edge from u to v, and if $i = j$, an edge at level i between u and v.

For the induction step, let us assume it holds for nodes connected by a shortest path of length m or less, and suppose the shortest path between u and v is of length $m+1$. Consider the case when $i < j$. Let the first node on this shortest path after u be w. Now w cannot be to the left of u: for if this was the case, there must be either an original edge (i.e. an edge of G_ρ) from u to w, or an augmented edge. Suppose it was an original edge, then by induction hypothesis we have a forward path from w to v. The first edge in this forward path from w clearly cannot be an augmented edge, since a forward augmented edge must begin at a point of increment, and w cannot be a point of increment since it is connected by a forward edge to u. Neither can the first edge in the forward path from w be an original edge, since then we must have an edge between u and the target vertex of this edge, which gives us a strictly shorter path from u to v. For the case when have an augmented edge from u to w, the forward path from w to v must pass through this or an "equivalent" edge, i.e. an edge from w to u' where $u' \in [u]_\rho$. In either case, we have a contradiction to the fact that we had started out with a shortest path from u to v.





Similarly, the first edge from u to w cannot be an edge at the same level, since this would again contradict the fact that it was part of the shortest path from u to v.

Hence it must be a forward edge from u to w, and using the induction hypothesis we obtain a forward path from u to v.

The case when $i = j$ is handled similarly. This completes the proof of our claim. □

Here are some more properties of G'_ρ which are easily verified:

Claim 2.

1. If we have a forward path from a node u to an x-node in G'_ρ then we must have $x \in \mathsf{XF}_\rho(u)$.
2. If we have a forward path p from u to v in G'_ρ, and $x \in \mathsf{XF}_\rho(u)$, then either some node in p is connected by a forward edge to an x-node, or $x \in \mathsf{XF}_\rho(v)$. □

We can now prove that the labelling σ of G_ρ is an edge-respecting one. We first argue that σ respects the normal edges in G_ρ. Let (u, v) be an edge in G_ρ, with say $u \prec v$. Then by the deterministic property of the labelling procedure, v would be given the same value as u in step 1. Further, if u and v were in the same (l, k)-frame (i.e. their levels differ by at most $l + 1$) and there was no edge between them in G_ρ, then we argue that they would be given different labels. Suppose to the contrary that u and v were given the same label m. Then it is easy to see that both u and v must be connected to a vertex w which was the first vertex to be labelled m. Thus there is a path between u and v, and by Claim 1 we must have a forward path from u to v. Since u and v lie in a common (l, k)-frame, this means that they must be connected by an edge in G_ρ.

Let us now consider the annotated edges in G_ρ and show that the labelling σ respects these edges also. Let u be a node in G_ρ with a variable $x \in \mathsf{XF}_\rho(u)$. Let us first consider the case when ρ is finite. Consider a maximal forward path from u in G'_ρ, and let w be the final node in this path. Then we claim that w cannot have any future obligations. Suppose not. Then since w has no forward edges from it (due to the maximality of the foward path from u), it must be a point of increment. It follows from the assumptions on the symbolic model ρ that w must have a matching subsequent point of decrement. But then w would have a forward augmented edge to this point of decrement, again contridicting the maximality of the forward path from u. Thus w can have no future obligations. In particular $x \notin \mathsf{XF}_\rho(w)$. Thus by Claim 2, we have that there must be a vertex v in the path which is connected by a forward edge to an x-node. This x-node would have been labelled m, and we have a required x-node which satisfies the obligation x of u.

For the case when ρ is infinite, let $\mathsf{XF}_\rho(u) = X$ (with $x \in X$). We argue by induction on the size of X, that the x-obligation of u is satisfied. When X is a singleton, i.e. $X = \{x\}$, suppose u was not connected by a forward path to an x-node in G'_ρ. Then it must be the case (using Claim 2) that we have an infinite forward path from u in G'_ρ, along which all nodes have future obligation exactly $\{x\}$. If this path uses only finitely many augmented edges, we have a contradiction of the assumption that ρ satisfies the condition C1 of Lemma 5. If the path uses infinitely many augmented edges, we must have infinitely many points of increment for $\{x\}$ along the path, and by the way we added the augmented edges in G'_ρ, these augmented edges are to points of decrement for $\{x\}$ which are necessarily connected by a forward path to an x-node. For the induction step, suppose X had more than 1 element, and suppose once again that u was not connected by a forward path to any x-node in G'_ρ. Then again, there must be an infinite forward path from u in G'_ρ along which the obligation x is preserved. Since the obligations along a forward path can only decrease (or stay the same), it must be the case that after a point the set of future obligations remains at some X' with $x \in X'$. Again, if this path had only finitely many augmented edges, it would contradict condition C1. Otherwise, it has infinitely many augmented edges (and hence points of increment for X') and by the way augmented edges were added, it must be the case that these edges are to points of decrement for X' from which there is a forward path to a point of increment for X'' with $X'' \subset X'$. By our induction hypothesis, there is a path from these points of increment for X'' to a y-node for each $y \in X''$. Since $x \in X''$, we have a path from u to an x-node, contradicting our assumption. Thus, it cannot be the case that there is no forward path from u to an x-node. Thus there is a forward path from u to an x-node, say v. By our labelling procedure, v would also be given the same value as u. Thus the obligation x in $\mathsf{XF}_\rho(u)$ is satisfied.

We now argue that for every node u in G_ρ that if $x \notin \mathsf{XF}_\rho(u)$ then there is no x-node at a level greater than that of u which is given the same label. Suppose some such x-node v was given the same label, say m, as u. Then, as similarly observed before, both u and v must be connected by a path in G'_ρ (via the first vertex labelled m). By Claim 1, there is a forward path from u to v. By Claim 2(1), we must have $x \in \mathsf{XF}_\rho(u)$.

This completes the proof of the fact that the labelling σ respects the edges of G_ρ, and hence ρ is the symbolic model induced by σ.

With this we have finally completed the proof of Lemma 5. □

We are going to show in Section 7 that we can check the conditions on counting sequences stated in Lemma 5 by using a class of counter automata with a decidable nonemptiness problem.

6 Simple Counter Automata

We now want to characterize the set of realizable symbolic models by means of automata. Towards this aim, we introduce in this section a class of counter automata with a disjunctive variant of the generalized Büchi acceptance condition in which, along any run, a zero test is performed at most once for each counter. Then we use this class of automata to complete the decision procedure for CLTL$^{\mathsf{XF}}$ satisfiability sketched in Section 4.2.

6.1 Classes of counter automata

The definition of counter automata we use is not standard since the acceptance condition is a disjunction of generalized Büchi acceptance conditions. A *counter automaton* $\mathcal{A}$ is a tuple $\langle \Sigma, C, Q, \mathcal{F}, I, \rightarrow \rangle$ where:

- Q is a finite set of locations,
- Σ is a finite alphabet,
- C is a finite set of counters,
- $I \subseteq Q$ is the set of initial locations,
- the set of final locations is defined by $\mathcal{F} = \{F_0, F_1, \ldots, F_K\}$ where $K \geq 0$ and $F_i \subseteq \mathcal{P}(Q)$ for each $i \in \{0, \ldots, K\}$,
- $\rightarrow$ is a finite subset of $Q \times \mathcal{P}(C) \times \mathbb{Z}^C \times \Sigma \times Q$.

The elements of $\rightarrow$ are also denoted by $q \xrightarrow{Y,up,a} q'$ where Y is interpreted as a set of simultaneous zero-tests on the counters in Y. A configuration $\langle q, \vec{c} \rangle$ of $\mathcal{A}$ is an element of $Q \times \mathbb{N}^C$ and we say $\langle q, \vec{c} \rangle \rightarrow \langle q', \vec{c}' \rangle$ iff there is a transition $q \xrightarrow{Y,up,a} q'$ in $\mathcal{A}$ such that for every $c \in C$ we have $c \in Y \Rightarrow \vec{c}(c) = 0$ and $\vec{c}'(c) = \vec{c}(c) + up(c)$. As usual, a run is a sequence of configurations governed by the transitions of $\mathcal{A}$. An infinite run is accepting iff there exists a set $F \in \mathcal{F}$ such that every set $Y \in F$ is visited infinitely often. The set of words in Σ^ω labelling accepting runs forms the language accepted by $\mathcal{A}$. Observe that considering $\mathcal{F}$ (instead of a single set F_i) for the encoding of the acceptance condition is not essential since for checking nonemptiness of $\mathcal{A}$ one can alternatively consider $\mathcal{A}_0, \ldots, \mathcal{A}_K$ with generalized Büchi acceptance condition $F_0, \ldots, F_K$, respectively.

The counter automaton above is called *simple* if there is a partition $\{Q_0, \ldots, Q_K\}$ of Q and corresponding sets of counters $C_0, C_1, \ldots, C_K$ such that

- $C_0 = \emptyset$,

- $I \subseteq Q_0$,
- for every $i \in \{1, \ldots, K\}$, a transition from a location in Q_0 to a location in Q_i requires that exactly the counters in C_i are tested for zero,
- if $i \neq 0$, then every transition from a location in Q_i goes to another location of Q_i,
- every transition from a location of Q_i leaves the value of the counters in C_i untouched.

As a consequence of the two last points, when the execution enters the component Q_i, the counters in C_i are equal to zero forever thereafter. Finally, for $i \in \{0, \ldots, K\}$ we must have $F_i \subseteq \mathcal{P}(Q_i)$. Let us formally summarize the conditions:

1. $Q = Q_0 \uplus \cdots \uplus Q_K$ and $I \subseteq Q_0$,
2. $\mathcal{F} = \{F_0, F_1, \ldots, F_K\}$ where each $F_i \subseteq \mathcal{P}(Q_i)$,
3. there are $K + 1$ sets of counters $C_0, \ldots, C_K \subseteq C$ with $C_0 = \emptyset$ such that the transition relation $\rightarrow \subseteq Q \times \mathcal{P}(C) \times \mathbb{Z}^C \times \Sigma \times Q$ verifies the condition below:
   for all $i, i' \in \{0, \ldots, K\}$, $q \in Q_i$ and $q' \in Q_{i'}$, the transitions from q to q' are of the form $q \xrightarrow{Y,up,a} q'$ where
   (a) $i \neq i'$ implies $i = 0$ and $Y = C_{i'}$,
   (b) $i = i'$ implies $Y = \emptyset$,
   (c) for every $X \in C_{i'}$, $up(X) = 0$.

The class of languages accepted by simple counter automata can be seen to be closed under intersection with ω-regular languages.

Proposition 1 *If $\mathcal{A}$ is simple counter automaton, and $\mathcal{B}$ is a Büchi automaton, then we can construct a simple counter automaton accepting the language $L(\mathcal{A}) \cap L(\mathcal{B})$.*

Proof. Let $\mathcal{A} = \langle \Sigma, C, Q, \mathcal{F}, I, \rightarrow \rangle$, with $Q = Q_0 \uplus \cdots \uplus Q_K$, and $\mathcal{F} = \{F_1, \ldots, F_K\}$. Let $\mathcal{B} = \langle S, S_0, G, \rightarrow' \rangle$. We can define a simple counter automaton $\mathcal{C}$ for the intersection of the two languages, where the partition structure and counters are inherited from $\mathcal{A}$. Thus $\mathcal{C} = \langle \Sigma, C, Q \times S, \mathcal{F}', I \times S_0, \rightarrow'' \rangle$, where $\mathcal{F}' = \{F'_1, \ldots, F'_K\}$ and each $F'_i = \{F \times S \mid F \in F_i\} \cup \{Q \times G\}$. The transition relation $\rightarrow''$ is the usual product of the transition relations $\rightarrow$ and $\rightarrow'$. □

In the sequel we will consider simple counter automata with $C = \mathcal{P}^+(\{x_1, \ldots, x_k\})$, $K = 2^k - 1$, and each set F_i contains sets of states reached by decrementing the counters in C_i.

The class of simple counter automata introduced above forms a subclass of Minsky machines [Min67] with multiple counters. The restriction on the zero-tests is essential for decidability. The restriction that the acceptance condition can be expressed as a disjunction of generalized Büchi acceptance conditions, is not essential. We also observe that our counter automata are quite different from the data automata in [BMS$^+$06] and from the register automata in [KF94, NSV04, DL06]. Our automata are similar to Minsky machines, in that they operate by updating counters with increments and with decrements whenever possible. By constrast, register automata accept data words and possess registers that can store elements from an infinite alphabet. Finally, each data automaton also accepts data words and is made up of a regular transducer and of a finite-state automaton see details in [BMS$^+$06]. However, the nonemptiness problem for subclasses of register automata or data automata can be reduced to nonemptiness in counter automata (with incrementing errors in [DL06] or without zero-tests in [BMS$^+$06]). Consequently, our underlying model of counter automata is quite standard but our restrictions are essential to get decidability.

6.2 Checking nonemptiness for simple counter automata

We now show that simple counter automata have a decidable nonemptiness problem. We will show this by appealing to a result from [Jan90].

Lemma 6 *The nonemptiness problem for simple counter automata is decidable.*

Proof. We reduce this problem to the problem $\mathbb{P}_{\rm temp}$ shown to be decidable in [Jan90]. We briefly define a fragment of the problem $\mathbb{P}_{\rm temp}$ that consists in checking fairness conditions in Petri nets. Let $N = \langle S, T, W, M_0 \rangle$ be a Petri net where S is a set of places, T is a set of transitions, $W : (S \times T) \cup (T \times S) \to \mathbb{N}$ is a weight function and M_0 is an initial marking. We assume that the reader is familiar with the semantics of this model (otherwise see e.g., [Pet81]). The fragment of the language $L(S, \mathsf{GF})$ [Jan90] we consider here is the following:

$$\psi ::= s = i \;\mid\; \psi \vee \psi \;\mid\; \psi \wedge \psi \;\mid\; \mathsf{GF}\psi,$$

where $s \in S$ and $i \in \mathbb{N}$. The atomic formula $s = i$ states that the number of tokens in the place s is i. As expected, $\mathsf{GF}\psi$ states that infinitely often ψ holds true. In full generality, the problem $\mathbb{P}_{\rm temp}$ takes as input a formula ψ in $L(S, \mathsf{GF})$ and an initial marking M_0 for a Petri net N and checks whether there is an infinite execution from M_0 that satisfies ψ.

Consider a simple counter automaton $\mathcal{A}$ (we use the previous notations). We can build a Petri net $N_{\mathcal{A}}$ that simulates $\mathcal{A}$ apart from the zero tests, by using a standard translation from counter automata without zero tests to Petri nets. For every location q in $\mathcal{A}$, we introduce a place s_q in $N_{\mathcal{A}}$ and for every counter $c \in C$, we introduce a place s_c. An initial marking contains one token in some place s_{q_0} for some initial location q_0 and no token in places of the form s_c (meaning that the initial value of the counters is 0). From this marking, we obtain markings where a unique token belongs to a place of the form s_q $(q \in Q)$ which means that a unique control location is active for every marking. For every transition in $\mathcal{A}$, say $q \xrightarrow{Y,up,a} q'$, we add a transition in $N_{\mathcal{A}}$ that consumes a token in s_q, produces a token in $s_{q'}$ and produces [resp. consumes] $up(c)$ tokens in the place s_c when $up(c) \geq 0$ [resp. when $up(c) < 0$]. The zero tests Y will be taken into account separately in the $L(S, \mathsf{GF})$ formula below. To ensure the correctness of our reduction, we need to handle transitions of the form $t = q \xrightarrow{\emptyset,up,a} q$ in $\mathcal{A}$ separately as follows. This is similar to what is done in the reduction from VASS to Petri nets, see e.g. [Reu90]. We implement a transition of the form $t = q \xrightarrow{\emptyset,up,a} q$ in $\mathcal{A}$ by the two transitions $q \xrightarrow{\emptyset,up,a} q^t$ and $q^t \xrightarrow{\emptyset,\mathbf{0},a} q$ in $N_{\mathcal{A}}$, where q^t is a new location and $\mathbf{0}$ is the zero vector.

We claim that checking the nonemptiness of $\mathcal{A}$ is equivalent to verifying whether the following formula holds true in $N_{\mathcal{A}}$

$$\bigvee_{0 \leq i \leq K} \big(\mathsf{GF}(\bigwedge_{c \in C_i} s_c = 0) \wedge (\bigwedge_{Y \in F_i} \mathsf{GF}(\bigvee_{q \in Y} s_q = 1)\big).$$

If this property is satisfied, there is $i \in \{0, \ldots, K\}$ such that all the counters of C_i are equal to zero infinitely often and each set of places corresponding to the set of locations of F_i is visited infinitely often, which means that the corresponding run is accepted by $\mathcal{A}$. We have to prove that this corresponding run of $\mathcal{A}$ is valid by showing that the values of the counters in C_i are equal to zero before entering in a state of Q_i. Indeed, the zero tests have not been taken into account in the construction of $N_{\mathcal{A}}$.

Since $N_{\mathcal{A}}$ is obtained by translation of a simple counter automaton, whenever we enter a subcomponent Q_i with $i > 0$, the counters of C_i are not modified anymore. This means that for $j \geq 0$, if $s_c = j$ for a marking of $N_{\mathcal{A}}$ where $s_q = 1$ also holds for some location q of Q_i then $s_c = j$ always holds in the future. So the conjunction implies that the counters of C_i are equal to zero before entering the subcomponent Q_i and they remain zero afterwards. Otherwise, the conjunct $\mathsf{GF}(\bigwedge_{c \in C_i} s_c = 0)$ cannot be satisfied.

The converse implication is obvious, since an accepting run in $\mathcal{A}$ is such that there exists $i \in \{0, \ldots, K\}$ for which all the counters of C_i are equal to zero infinitely often (they remain zero after the test) and the set of locations of F_i is visited infinitely often (acceptance condition). The execution of $N_{\mathcal{A}}$ corresponding to such a run of $\mathcal{A}$ satisfies the formula. □

7 Decidability

7.1 Automata recognizing realizable symbolic models

We recall that our goal is to build the automaton $\mathcal{A}_{\mathrm{real}}$ recognizing the set of realizable symbolic models that is needed in the construction described in Section 4.2.

We begin with the case of infinite models. We can build the automaton $\mathcal{A}_{\mathrm{real}}$ as a simple counter automaton. This automaton is defined as the intersection of two automata $\mathcal{A}^1$ and $\mathcal{A}^2$ which check respectively the conditions (C1) and (C2) from Lemma 5. Since $\mathcal{A}_{1\mathrm{sc}}$ checks the one-step consistency condition in the construction of $\mathcal{A}_\phi$, we assume that the sequences considered in the following are valid symbolic models.

The automaton $\mathcal{A}^1$ has to recognize the set of (l,k)-frame sequences ρ satisfying the condition (C1). It is easier to describe the construction of this automaton using its complement $\tilde{\mathcal{A}}^1$ which accepts the sequences ρ that do not satisfy (C1), i.e. the sequences for which there is an infinite forward path p in ρ and a counter X such that

- every node in the path has future obligation X, and
- there is a variable y in X which is never connected by a forward edge from a node in p.

The automaton $\tilde{\mathcal{A}}^1$ is a Büchi automaton whose set of states is $Q = \{q_0\} \uplus ((\{x_1,\dots,x_k\} \times \{0,\dots,l\}) \times \{x_1,\dots,x_k\})$. The set of initial states and final states are respectively $I = \{q_0\}$ and $F = Q \setminus \{q_0\}$, and the transition relation is defined by

- $q_0 \xrightarrow{fr} q_0$ for every $fr \in \mathtt{Frame}^l_k$.
  This rule allows to skip the frames until the beginning of the path.

- $q_0 \xrightarrow{fr} (\langle x,i\rangle, y)$ for every $fr \in \mathtt{Frame}^l_k$ such that $y \in \mathsf{XF}_{fr}(x,i)$.
  This rule is for the non-deterministic choice of the beginning of the path and the variable y which is never linked to this path.

- $(\langle x,i\rangle, y) \xrightarrow{fr} (\langle x,i-1\rangle, y)$ for every $i > 0$ and $fr \in \mathtt{Frame}^l_k$.
  This rule allows to skip the frames until the current node of the path is in the border (level 0) of the current frame.

- $(\langle x,0\rangle, y) \xrightarrow{fr} (\langle x',i'\rangle, y)$ for every $fr \in \mathtt{Frame}^l_k$ verifying the following conditions:

  1. $x = \mathsf{X}^{i'+1}x'$ belongs fr,
  2. $\mathsf{XF}_{fr}(x,0) = \mathsf{XF}_{fr}(x',i'+1)$,
  3. for every $j \in \{1,\dots,l\}$ the constraint $x = \mathsf{X}^j y$ is not in fr.

  The first condition expresses that $\langle x',i'\rangle$ is the next node of the path while the second states that the set of obligations on the path remains the same. Finally, the last condition ensures that no node corresponding to the variable y is connected to the path by a forward edge.

The automaton $\mathcal{A}^1$ is the Büchi automaton obtained by complementing the above automaton.

We now focus on the construction of the counter automaton $\mathcal{A}^2$. Formally, we define $\mathcal{A}^2 = \langle \Sigma, C, Q, F, s, \rightarrow\rangle$ such that $\Sigma = \mathtt{Frame}^l_k$, $C = \mathcal{P}^+(\{x_1,\dots,x_k\})$ and $Q = \mathtt{Frame}^l_k \cup \bigcup_{Z\subseteq C} Q_{\mathcal{A}_Z}$, where for every $Z \subseteq C$, $Q_{\mathcal{A}_Z}$ is the set of states of the automaton $\mathcal{A}_Z$ defined below which verifies the different conditions of (C2) after testing that the counters of Z are equal to zero. The set of initial states is $I = \mathtt{Frame}^l_k$ and the transition relation verifies the following rules:

- $fr \xrightarrow{\emptyset, up, fr'} fr'$
  for all $fr, fr' \in \mathtt{Frame}^l_k$ such that $u^+_{fr}(X) - u^-_{fr'}(X) \leq up(X) \leq u^+_{fr}(X)$ for each $X \in C$.

- $\mathit{fr} \xrightarrow{Z,\mathit{up},\mathit{fr}'} s_{\mathcal{A}_Z}$
  for all $\mathit{fr}, \mathit{fr}' \in \mathtt{Frame}^l_k$ and $Z \subseteq C$ such that

  1. $u^+_{\mathit{fr}}(X) - u^-_{\mathit{fr}'}(X) \leq \mathit{up}(X) \leq u^+_{\mathit{fr}}(X)$ for each $X \in C \setminus Z$,
  2. $\mathit{up}(X) = u^+_{\mathit{fr}}(X) = 0$ for each $X \in Z$,
  3. $s_{\mathcal{A}_Z}$ is the initial state of $\mathcal{A}_Z$.

For every $Z \subseteq C$, the Büchi automaton $\mathcal{A}_Z$ is given by:

$$\mathcal{A}_Z = \mathcal{A}^{2a}_Z \cap \bigcap_{X \in C \setminus Z} (\mathcal{A}^{2b}_X \cup \mathcal{A}^{2c}_X)$$

such that the different components are defined as follows.

- The Büchi automaton $\mathcal{A}^{2a}_Z$ checks the condition (C2.a) for the counters in Z. It accepts the set of symbolic models such that there is no point of increment for counters in Z. This ensures that the counters of Z remain to zero in $\mathcal{A}_Z$ since they have been tested to zero before entering $\mathcal{A}^{2a}_Z$ and they are not modified after this test.

  The automaton $\mathcal{A}^{2a}_Z$ has a unique state q_0 and so $Q = I = F = \{q_0\}$. The only transition rule is the following

  > $q_0 \xrightarrow{\mathit{fr}} q_0$ for every frame $\mathit{fr} \in \mathtt{Frame}^l_k$ such that there is no point of increment for every counter $X \in Z$ in fr.

  So an execution can continue only if the counters of Z are not incremented in the counting sequence.

- The Büchi automaton $\mathcal{A}^{2b}_X$ checks that the condition (C2.b) is satisfied for some counter $X \notin Z$. This automaton accepts the symbolic models such that there are infinitely many points of decrement corresponding to X from which one can reach by a forward path a node whose set of obligations is strictly included in X. To do so, during an execution of $\mathcal{A}^{2b}_X$ one nondeterministically chooses in the sequence an element belonging to a point of decrement for X and then one checks that there is a path from this node to a node whose set of obligations is strictly included in X. When this latter node is reached, we are in a final state. An execution is accepted if such a final state is visited infinitely often. Formally, we have

  - the set of states of $\mathcal{A}^{2b}_X$ is $Q = \{q_0, q_f\} \uplus (\{x_1, \ldots, x_k\} \times \{0, \ldots, l\})$,
  - $Q_0 = \{q_0\}$ is the set of initial states and $F = \{q_f\}$ the set of final states,
  - the transition relation is defined by
    - $q_0 \xrightarrow{\mathit{fr}} q_0$ for every $\mathit{fr} \in \mathtt{Frame}^l_k$,
    - $q_0 \xrightarrow{\mathit{fr}} \langle x, l \rangle$ for every frame $\mathit{fr} \in \mathtt{Frame}^l_k$ such that $[(x, l)]_{\mathit{fr}}$ is a point of decrement for X in fr,
    - $\langle x, i \rangle \xrightarrow{\mathit{fr}} \langle x, i-1 \rangle$ for every $i > 0$ and $\mathit{fr} \in \mathtt{Frame}^l_k$,
    - $\langle x, 0 \rangle \xrightarrow{\mathit{fr}} \langle y, i-1 \rangle$ if $\mathsf{XF}(x, 0)_{\mathit{fr}} = X$, $i > 0$ and $x = \mathsf{X}^i y$ belongs to fr,
    - $\langle x, 0 \rangle \xrightarrow{\mathit{fr}} q_f$ if $\mathsf{XF}(x, 0)_{\mathit{fr}}$ is strictly included in X,
    - $q_f \xrightarrow{\mathit{fr}} q_0$ for every $\mathit{fr} \in \mathtt{Frame}^l_k$.

- The automaton $\mathcal{A}^{2c}_X$ checks the condition (C2.c) for some counter $X \notin Z$. The construction is similar to the previous case except that one visits a final state only when a point of decrement for X from which one can reach x has been guessed for every $x \in X$.

We can easily verify that the automaton $\mathcal{A}^2$ that we obtain is a simple counter automaton. Indeed, the transition relation of $\mathcal{A}^2$ ensures that for every $Z \subseteq C$ the counters in Z are equal to zero before entering $\mathcal{A}_Z$ and then the component $\mathcal{A}_Z^{2a}$ ensures that these counters are never modified again. Moreover, all the transitions of $\mathcal{A}_Z$ stay in $\mathcal{A}_Z$ for every $Z \subseteq C$.

Coming now to the case of finite models, the construction of $\mathcal{A}_{\text{real}}$ is simpler. This construction is very close to the first part the construction of $\mathcal{A}^2$ defined above. The automaton $\mathcal{A}_{\text{real}}$ for the finitary case is a counter automaton without zero tests $\langle Q, I, F, \Sigma, C, \rightarrow\rangle$ such that

- $Q = \mathtt{FFrame}_k^l$ is a finite set of states, $I = Q$ and $F = Q$
- $\Sigma = \mathtt{FFrame}_k^l$,
- $C = \mathcal{P}^+(\{x_1, \ldots, x_k\})$ is a set of counters,
- The transition relation is defined by

  $$\langle \mathit{fr}, i\rangle \xrightarrow{\emptyset, \mathit{up}, \langle \mathit{fr}, i\rangle} \langle \mathit{fr}', i'\rangle$$

  for every $\langle \mathit{fr}, i\rangle, \langle \mathit{fr}', i'\rangle \in \mathtt{FFrame}_k^l$ and up verifying $u_{\mathit{fr}}^+(X) - u_{\mathit{fr}'}^-(X) \leq \mathit{up}(X) \leq u_{\mathit{fr}}^+(X)$ for every $X \in C$.

The accepting condition for this automaton is the following: a finite execution is accepted iff it ends in a final state with all the counters equal to zero. Note that this automaton is zero-test free. So, the nonemptiness test for this automaton can be reduced to the reachability of a marking in a Petri net since a counter automaton without zero test can easily be transformed into a Petri net (see for instance the proof of Lemma 6 or [Reu90]).

Lemma 7 *A symbolic model ρ is accepted by $\mathcal{A}_{\text{real}}$ iff ρ is realizable.*

Proof. In the infinitary case, the construction of $\mathcal{A}_{\text{real}}$ allows us to verify all the conditions of Lemma 5. The only problem is that the sequence of counter valuations in the accepting run may be different from the counting sequence associated with the accepted symbolic model. Indeed, a sequence ρ can be accepted by a run that fires a transition $q_i \xrightarrow{\emptyset, \mathit{up}, \rho(i)} q_{i+1}$ in $\mathcal{A}^2$ where there exists X verifying $\alpha(i)(X) + \mathit{up}(X) > \alpha(i)(X) \dot{+} (u_{\rho(i)}^+(X) - u_{\rho(i+1)}^-(X))$ (where α is the counting sequence along ρ). However, the transition relation of $\mathcal{A}^2$ allows every update between $u_{\rho(i)}^+(X) - u_{\rho(i+1)}^-(X)$ and $u_{\rho(i)}^+(X)$ for every transition from the state q_i to q_{i+1}. This allows to find another run in $\mathcal{A}^2$ (on the same input ρ) that visits the same control states and such that for every $i \in \mathbb{N}$ we have $q_i \xrightarrow{\emptyset, \mathit{up}, \rho(i)} q_{i+1}$ iff for every $X \in C$, $\alpha(i)(X) + \mathit{up}(X) = \alpha(i)(X) \dot{+} (u_{\rho(i)}^+(X) - u_{\rho(i+1)}^-(X))$. The run is still accepting since the values of the counters in this execution are smaller and so the counter of Z are equal still to zero when entering the component $\mathcal{A}_Z$. Then the other conditions are not modified by the new values of the counters. This execution witnesses that ρ is satisfiable.

Conversely, a satisfiable symbolic model ρ satisfies the conditions of Lemma 5. So, it is obvious that there is an accepting run in $\mathcal{A}^1$ on the input ρ since the sequence satisfies (C1). The most difficult part concerns the components that check condition (C2.a). Let α be the counting sequence along ρ. By definition, for every $i \in \mathbb{N}$ we have,

$$\alpha(i+1)(X) = \alpha(i)(X) \dot{+} (u_{\rho(i)}^+(X) - u_{\rho(i+1)}^-(X)),$$

and this means that

$$\alpha(i)(X) + (u_{\rho(i)}^+(X) - u_{\rho(i+1)}^-(X)) \leq \alpha(i+1)(X) \leq \alpha(i)(X) + u_{\rho(i)}^+(X).$$

By construction of $\mathcal{A}^2$, every update between the bounds above is defined. So, there is always a transition allowing us to update the counters according to α. By hypothesis, there exist a position i and a set of counters Z that remain at zero in the counting sequence α after the position i. All these facts imply that there is a run of $\mathcal{A}^2$ where the counters of Z remain at zero after the position i too. We can then enter the component $\mathcal{A}_Z$ after the position i and this component will accept the sequence since ρ satisfies (C2).

Similar to the infinitary case, given a finite symbolic model ρ accepted by $\mathcal{A}_{\mathrm{real}}$, we can build from the run that accepts ρ another run where the values of the counters correspond to the counting sequence along ρ. Since we use the same method as in the infinitary case, the values of the counters in the latter run can only decrease and so the final values are still 0. So this run is accepted which means that ρ is satisfiable because $\mathcal{A}_{\mathrm{real}}$ checks that the counting sequence satisfies the conditions of Lemma 5. Conversely, every counting sequence along a symbolic model can be simulated by the values of the counters in an accepting run of $\mathcal{A}_{\mathrm{real}}$. The arguments are identical to the infinitary case since the transition relation of $\mathcal{A}_{\mathrm{real}}$ is similar. By Lemma 5, if ρ is satisfiable then the counting sequence is such that the final value of every counter is 0. So the corresponding run in $\mathcal{A}_{\mathrm{real}}$ is accepted. □

We are now in position to state again the main result of the paper.

Theorem 4 *The finitary and infinitary satisfiability problems for* CLTL$^{\mathsf{XF}}$ *are decidable.*

Proof. Let ϕ be a CLTL$^{\mathsf{XF}}$ formula over k variables with X-length l. Let $\mathcal{A}_{\mathrm{symb}}$ and $\mathcal{A}_{\mathrm{1sc}}$ be the Büchi automata corresponding to ϕ, defined in Section 4.2. Let $\mathcal{A}_{\mathrm{real}}$ be the simple counter automaton defined above. Then, using Proposition 1, we can construct a simple counter automaton $\mathcal{A}_\phi$ accepting the intersection of the languages accepted by $\mathcal{A}_{\mathrm{real}}$, $\mathcal{A}_{\mathrm{symb}}$, and $\mathcal{A}_{\mathrm{1sc}}$.

By Theorem 3 the language accepted by $\mathcal{A}_\phi$ is nonempty iff ϕ is satisfiable. Using Lemma 6) we can check whether the language accepted by $\mathcal{A}_\phi$ is nonempty. Thus it follows that checking the satisfiability of ϕ is decidable.

We also note that according to the acceptance condition of $\mathcal{A}_{\mathrm{real}}$ in the case of finite models, finitary satisfiability reduces to the reachability problem in Petri nets, see e.g. [May84, Kos82]. □

Theorems 3 and 4 entail that this decidability result can be extended if we replace the carrier logic of LTL by any logic whose formulas define ω-regular sets of models. This also holds if we extend LTL with any temporal operators definable in Monadic Second Order Logic (MSOL). We just have to update the construction of $\mathcal{A}_{\mathrm{symb}}$ by using the construction of [GK03].

Corollary 2 *Finitary and infinitary satisfiability for* CLTL$^{\mathsf{XF}}$ *augmented with MSOL definable temporal operators are decidable.*

The above decidability result can be alternatively obtained by adapting the developments from Section 3.2. Note also that the reduction used for checking nonemptiness implies that the conditions (C1) and (C2) should have been expressed directly in Jančar's formalism (see the proof of Lemma 6). However, we think our approach is more modular and more natural since the conditions use zero-tests that cannot be expressed directly in Petri nets. The zero-tests as well as the Büchi acceptance condition are taken into account in the formula to check. This is the tricky point of the proof of Lemma 6. Using directly Jancar's formalism in this context would be very difficult.

8 A PSPACE fragment of CLTL$^{\mathsf{XF}}$

In this section, we consider CLTL$^{\mathsf{XF}}_1$, the fragment of CLTL$^{\mathsf{XF}}$ in which the formulae are built over the single variable x. The models of the logic are sequences of natural numbers and the only counter in counting sequences α is $\{x\}$. In the following, we identify $\alpha(i)(\{x\})$ with $\alpha(i)$ for every counting sequence α. Let ρ be a symbolic model over the elements of $\mathtt{Frame}^l_1$. By definition, the counting sequence α along ρ is such that for every $0 \leq i < |\rho|$ we have $\alpha(i+1) = \alpha(i) \dot{+} (u^+_{\rho(i)} - u^-_{\rho(i+1)})$ with $u^+_{\rho(i)}, u^-_{\rho(i+1)} \in \{0, 1\}$ (because there cannot exist more than one point of increment/decrement in a one variable frame).

When formulae from $\mathrm{CLTL}_1^{\mathsf{XF}}$ are considered, the conditions stated in Lemma 5 can be simplified as follows: *a symbolic model over* $\mathtt{Frame}_1^l$ *is satisfiable iff its counting sequence is such that either the unique counter remains equal to zero after a finite number of steps or it is decremented infinitely often.* For finite symbolic models, we only have to check that the last value of the counter is 0. The verification of these conditions is simplified by the fact that the value of the counter is bounded.

Lemma 8 *For every symbolic model* ρ *of the form* $\mathbb{N} \rightarrow \mathtt{Frame}_1^l$ *the counting sequence* α *along* ρ *verifies* $\alpha(i) \leq l$ *for every* $0 \leq i < |\rho|$.

Proof. Let ϕ be a $\mathrm{CLTL}_1^{\mathsf{XF}}$ formula, l be its X-length and ρ be a symbolic model built with respect to ϕ (i.e. $\rho : \mathbb{N} \rightarrow \mathtt{Frame}_1^l$). We show that for every $i \in \mathbb{N}$ the number of distinct equivalence classes in the frame $\rho(i)$, denoted by $\sharp(\rho(i))$, is bounded by $l + 1 - \alpha(i)$ where α is the counting sequence along ρ.

We proceed by induction on i. By definition, if $i = 0$ then we have $\alpha(i) = 0$. The property is verified since the inequality $\sharp(\rho(0)) \leq l + 1$ is always true. Indeed, there are $l + 1$ different terms in a frame of $\mathtt{Frame}_1^l$. So we cannot have more equivalence classes in such a frame.

Now we suppose that $\sharp(\rho(i)) \leq l + 1 - \alpha(i)$ and we show that the property holds at position $i + 1$. Several cases arise:

- If $\alpha(i+1) = \alpha(i)+1$ then we must have $u^+_{\rho(i)} = 1$ and $u^-_{\rho(i+1)} = 0$. So, $[(x, 0)]_{\rho(i)}$ is a point of increment and $[(x, l)]_{\rho(i+1)}$ is not a point of decrement. By definition of the points of increment and decrement, there are no edges from $(x, 0)$ to the other nodes of $\rho(i)$ while (x, l) is linked to another node of $\rho(i + 1)$. Since the constraints between the other terms are shared by both frames (the pair $\langle \rho(i), \rho(i + 1)\rangle$ is one-step consistent), we can deduce that the number of equivalence classes in $\rho(i+1)$ decreases by one w.r.t. $\rho(i)$. By induction hypothesis, we have $\sharp(\rho(i)) \leq l+1-\alpha(i)$ which implies $\sharp(\rho(i+1)) \leq l+1-\alpha(i+1)$ since $\sharp(\rho(i + 1)) = \sharp(\rho(i)) - 1$ and $\alpha(i + 1) = \alpha(i) + 1$.

- If $\alpha(i + 1) = \alpha(i) - 1$ then we must have $u^+_{\rho(i)} = 0$ and $u^-_{\rho(i+1)} = 1$. Using the same arguments as in the previous case, we can show that $\sharp(\rho(i + 1)) = \sharp(\rho(i)) + 1$, since $[(x, 0)]_{\rho(i)}$ is not a point of increment and $[(x, l)]_{\rho(i+1)}$ is a point of decrement. So, we also obtain $\sharp(\rho(i + 1)) \leq l + 1 - \alpha(i + 1)$ by using the induction hypothesis and the fact that $\alpha(i + 1) = \alpha(i) - 1$.

- If $\alpha(i + 1) = \alpha(i)$ and $u^+_{\rho(i)} = u^-_{\rho(i+1)} = 1$ the proof is still the same by considering that $[(x, 0)]_{\rho(i)}$ is a point of increment and $[(x, l)]_{\rho(i+1)}$ is a point of decrement which imply that $\sharp(\rho(i + 1)) = \sharp(\rho(i))$.

- Finally, the case where $\alpha(i + 1) = \alpha(i)$ and $u^+_{\rho(i)} = 0$ requires to distinguish two cases. By definition, $[(x, 0)]_{\rho(i)}$ is not a point of increment but $[(x, l)]_{\rho(i+1)}$ can be a point of decrement or not. If $[(x, l)]_{\rho(i+1)}$ is not a point of decrement then we can use the same development as in all the other cases. Otherwise, $\alpha(i + 1) = \alpha(i)$ means that the counter cannot be decremented because $\alpha(i) = 0$. In that case, we have to prove that $\sharp(\rho(i)) \leq l+1$. However, this inequality always holds because there are only $l+1$ different terms in a frame of $\mathtt{Frame}_1^l$ (and so at most $l + 1$ equivalence classes).

By induction, we have $\sharp(\rho(i)) \leq l + 1 - \alpha(i)$ for every $i \in \mathbb{N}$. Since the number of equivalence classes is always strictly positive, for every $i \in \mathbb{N}$ we have $l + 1 - \alpha(i) \geq \sharp(\rho(i)) > 0$. So we can deduce that $l + 1 > \alpha(i)$ for every $i \in \mathbb{N}$.

The proof for finite symbolic models is essentially the same except that we also have to consider the frames that indicate the end of the model. So we have more different cases but they do not cause any problem since the terms after the end of the model do not induce equivalence classes. □

This result allows us to modify our construction in order to use automata without counters in the case of one-variable formulae.

Lemma 9 *The set of realizable symbolic models over the alphabet* $\mathtt{Frame}_1^l$ *can be recognized by a standard Büchi automaton in the infinitary case, or by a finite-state automaton in the finitary case.*

Proof. An infinite symbolic model $\rho : \mathbb{N} \to \mathtt{Frame}_1^l$ is satisfiable iff there is a position after which either every value in the counting sequence is equal to zero or there are infinitely many points of decrement in ρ. Since the value of the counter is always smaller than l (by Lemma 8) this condition can be checked by the Büchi automaton $\mathcal{A}'_{\mathrm{real}} = \langle Q, Q_0, F, \to \rangle$ such that:

- the set of states is $Q = \mathtt{Frame}_1^l \times \{0, \ldots, l\} \times \{\mathrm{dec}, \neg\mathrm{dec}, \mathrm{zero}\}$ where the second component of the triple encodes the value of the counter and the last one is helpful for the acceptance condition,
- $Q_0 = \{\langle fr, 0, \neg\mathrm{dec}\rangle \mid fr \in \mathtt{Frame}_1^l\}$ is the set of initial states,
- the set of final states is $F = \{\langle fr, 0, \mathrm{zero}\rangle \mid fr \in \mathtt{Frame}_1^l\} \cup \{\langle fr, i, \mathrm{dec}\rangle \mid fr \in \mathtt{Frame}_1^l \text{ and } i \in \{0, \ldots, l\}\}$,
- the transition relation is described by the following rules

  (T1) for all $fr, fr' \in \mathtt{Frame}_1^l$, $i \in \{0, \ldots, l\}$ and $u \in \{\mathrm{dec}, \neg\mathrm{dec}\}$ we have a transition $\langle fr, i, u\rangle \xrightarrow{fr} \langle fr', i', u'\rangle$ iff the pair $\langle fr, fr'\rangle$ is one-step consistent, $i' = i \dot{+} (u^+_{fr} - u^-_{fr'})$ and u' satisfies the following conditions:

  – if $u' = \mathrm{zero}$ then $i' = 0$,
  – if $u' = \mathrm{dec}$ then $u^-_{fr'} = 1$,
  – if $u' = \neg\mathrm{dec}$ then $u^-_{fr'} = 0$.

  (T2) for all $fr, fr' \in \mathtt{Frame}_1^l$, we have $\langle fr, 0, \mathrm{zero}\rangle \xrightarrow{fr} \langle fr', 0, \mathrm{zero}\rangle$ iff $\langle fr, fr'\rangle$ is one-step consistent and $u^+_{fr} = u^-_{fr'}$.

By construction, any satisfiable symbolic model ρ is recognized by $\mathcal{A}'_{\mathrm{real}}$. Indeed, the counting sequence along ρ has to satisfy the conditions in Lemma 5. If there is a position after which every value in the counting sequence is equal to zero then we can enter into a state of $\mathcal{A}'_{\mathrm{real}}$ where the last component is zero (see rule **(T1)**) after this position. Then, we can see in the definition of the rule **(T2)** that the run is never blocked since the counter remains to 0 in the counting sequence along ρ. Since every state of the form $\langle fr, 0, \mathrm{zero}\rangle$ is accepting, this run is accepting. Otherwise, the sequence ρ must have infinitely many points of decrements. In this case, there is also an accepting run since we can visit infinitely often a final state of the form $\langle fr, i, \mathrm{dec}\rangle$ (see the definition of **(T1)**).

Conversely, any accepted sequence is one-step consistent and the corresponding run verifies one of the following properties:

- either the run stays in the component of the automaton made up of the states of the form $\langle fr, 0, \mathrm{zero}\rangle$ after a certain position (since by **(T2)** every transition from a state of the form $\langle fr, 0, \mathrm{zero}\rangle$ goes to a state of the form $\langle fr', 0, \mathrm{zero}\rangle$). This means that the counter remains to 0 after a certain position (since in **(T2)** transitions are allowed only if $u^+_{fr} = u^-_{fr'}$).
- or the run visits infinitely often a state of the form $\langle fr, i, \mathrm{dec}\rangle$ which means that there are infinitely many points of decrements in the sequence.

In both cases, the condition stated in Lemma 5 is verified for this one-variable symbolic model. Indeed, the updates of the counter in the transition relation correspond to the definition of the counting sequence along ρ. So the symbolic model is satisfiable.

For the finitary case, we want that the execution ends with the value of the counter equal to 0. So we can use the following finite-state automaton $\mathcal{A}'_{\mathrm{real}} = \langle Q, Q_0, F, \to \rangle$ such that:

- $Q = \mathtt{FFrame}_1^l \times \{0, \ldots, l\}$,
- $Q_0 = \{\langle\langle fr, i\rangle, 0\rangle \mid \langle fr, i\rangle \in \mathtt{FFrame}_1^l\}$,
- $F = \{\langle\langle fr, 0\rangle, 0\rangle \mid \langle fr, 0\rangle \in \mathtt{FFrame}_1^l\}$,
- for every $\langle fr, i\rangle, \langle fr', i'\rangle \in \mathtt{FFrame}_1^l$ and $j \in \{0, \ldots, l\}$ we have $\langle\langle fr, i\rangle, j\rangle \xrightarrow{\langle fr, i\rangle} \langle\langle fr', i'\rangle, j'\rangle$ iff $\langle\langle fr, i\rangle, \langle fr', i'\rangle\rangle$ is one-step consistent and $j' = j \dot{+} (u^+_{fr} - u^-_{fr'})$.

The correctness proof for this automaton is obvious. Indeed, any run corresponds to a counting sequence along the accepted word and the acceptance condition enforces that the last value of this counting sequence is 0. □

The automaton $\mathcal{A}'_{\mathrm{real}}$ has an exponential size and can be built in polynomial space in l. Checking nonemptiness for this type of automata can be done in nondeterministic logarithmic space which allows to establish Theorem 5 below.

Theorem 5 *The finitary and infinitary satisfiability problems for* $\mathrm{CLTL}_1^{\mathsf{XF}}$ *are* PSPACE*-complete.*

Note that the models for $\mathrm{CLTL}_1^{\mathsf{XF}}$ corresponds to models of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X}, \mathsf{U})$. Therefore, a corollary of this result is that the finitary and infinitary satisfiability problems for the fragment of $\mathrm{CLTL}^{\downarrow}_{(1,1)}(\mathsf{X}, \mathsf{X}^{-1}, \mathsf{U}, \mathsf{S})$ restricting the freeze operator to subformulae of the form $\downarrow_{r=x} \mathsf{XF}(r = x)$ and $\downarrow_{r=x} \mathsf{X}^i(r = x)$ is decidable in polynomial space (where r is the unique register and x is the unique variable).

Moreover, the PSPACE upper bound is not a consequence of either Corollary 1 or Theorem 4 since in both cases the problems with an unbounded number of variables are translated into the reachability problem for Petri nets whose complexity is open (primitive recursiveness is even not known).

9 Repeating values in the past is still decidable

In this section we explain why we can allow the constraints of the language to state properties about past repetitions of a value without loosing decidability. Let $\mathrm{CLTL}^{\mathsf{XF},\mathsf{XF}^{-1}}$ be the extension of $\mathrm{CLTL}^{\mathsf{XF}}$ with atomic formulae of the form $x = \mathsf{XF}^{-1}y$. The satisfaction relation is extended as follows:

$$\sigma, i \models x = \mathsf{XF}^{-1}y \text{ iff there exists } j > 0 \text{ such that } \sigma(i)(x) = \sigma(i-j)(y) \text{ and } 0 \leq i - j.$$

As in Section 2.1, we can freely add constraints of the form x *diff* $\mathsf{XF}^{-1}y$ in the language since they can be defined from $x = \mathsf{XF}^{-1}y$ (using a simple variant of the equivalence (1)). The extended logic is strictly more expressive. One can show for instance that $x = \mathsf{XF}^{-1}y$ is not equivalent to $\mathsf{X}^{-1}\mathsf{F}^{-1}(y = \mathsf{XF}x)$. Indeed, the term $\mathsf{XF}x$ in $\mathsf{X}^{-1}\mathsf{F}^{-1}(y = \mathsf{XF}x)$ does not necessarily refer to the current value of x.

We consider a $\mathrm{CLTL}^{\mathsf{XF},\mathsf{XF}^{-1}}$ formula ϕ built over the variables from $\{x_1, \ldots, x_k\}$ and whose X-length is l. In order to deal with satisfiability for $\mathrm{CLTL}^{\mathsf{XF},\mathsf{XF}^{-1}}$ we need to extend the symbolic representation of models. The set of frames in this case are maximal consistent sets of constraints from the set Ω'^l_k that extends the set Ω^l_k defined previously with constraints of the form $\mathsf{X}^i(x = \mathsf{XF}^{-1}y)$ and their negation for all $x, y \in \{x_1, \ldots, x_k\}$ and $i \in \{0, \ldots, l\}$. The remaining of the definition of frames is very similar to the case without past repetitions. In addition to the conditions (F1)–(F5) defined in Section 4.1, a frame *fr* has to verify the following property that expresses consistency of past repetitions (the finitary case admits a similar update):

(FP) for all $i, j \in \{0, \ldots, l\}$ and $x, y \in \{x_1, \ldots x_k\}$, if $\mathsf{X}^i x = \mathsf{X}^j y$ is in *fr* then

- if $i = j$, then for every $z \in \{x_1, \ldots, x_k\}$ we have $\mathsf{X}^i(x = \mathsf{XF}^{-1}z) \in fr$ iff $\mathsf{X}^j(y = \mathsf{XF}^{-1}z) \in fr$,

- if $i > j$ then $\mathsf{X}^i(x = \mathsf{XF}^{-1}y) \in \mathit{fr}$, and for every $z \in \{x_1, \ldots, x_k\}$, $\mathsf{X}^i(x = \mathsf{XF}^{-1}z) \in \mathit{fr}$ iff either $\mathsf{X}^j(y = \mathsf{XF}^{-1}z) \in \mathit{fr}$ or there exists $i > j' \geq j$ such that $\mathsf{X}^i x = \mathsf{X}^{j'}z$ is in fr.

A symbolic model for ϕ is defined as a sequence ρ of frames such that two consecutive frames are one-step consistent and $\rho(0)$ satisfies the following initial condition: for every $\mathsf{X}^i x = \mathsf{XF}^{-1}y \in \rho(0) \in \Omega'^l_k$, $\mathsf{X}^i x = \mathsf{XF}^{-1}y \in \rho(0)$ iff there is $j < i$ such that $\mathsf{X}^i x = \mathsf{X}^j y$. One-step consistency requires one additional condition in order to take into account the past repetition constraints. Hence if $\langle \mathit{fr}, \mathit{fr}' \rangle$ is a pair of consecutive pairs in ρ, the conditions (OSC1) and (OSC2) from Section 4 are satisfied as well as the new one below:

(OSC3) for every $\mathsf{X}^i(x = \mathsf{XF}^{-1}y) \in \Omega^l_k$ with $i > 0$, we have $\mathsf{X}^i(x = \mathsf{XF}^{-1}y) \in \mathit{fr}$ iff $\mathsf{X}^{i-1}(x = \mathsf{XF}^{-1}y) \in \mathit{fr}'$.

All these definitions can naturally be adapted for the finite case.

The graphical representation of frames and symbolic models can easily be extended for $\mathrm{CLTL}^{\mathsf{XF},\mathsf{XF}^{-1}}$. We define $\mathsf{XF}^-_{\mathit{fr}}(\mathsf{X}^i x) \stackrel{\text{def}}{=} \{y \mid \mathsf{X}^i(x = \mathsf{XF}^{-1}y) \in \mathit{fr}\}$ which corresponds to the label of a new open edge from the node representing $\mathsf{X}^i x$ and refers to the past obligation linked to this node. The definition can be extended for symbolic models in a natural way.

Since we need to deal with past obligations, a counter is now represented by a pair $\langle X_p, X_f \rangle$ in $\mathcal{P}^+(\{x_1, \ldots, x_k\}) \times \mathcal{P}^+(\{x_1, \ldots, x_k\})$ where X_p is for past obligations and X_f for future obligations. We update the notion of counter valuations accordingly. A value n for $\langle X_p, X_f \rangle$ is the number of values that occurred in a past state of every variable of X_p and that have to be repeated in a future state of every variable in X_f.

The way we count the unsatisfied obligations has also to be updated. A *point of increment* for a counter $\langle X_p, X_f \rangle$ in the l-frame fr is an equivalence class of the form $[(x, 0)]_{\mathit{fr}}$ such that $\mathsf{XF}_{\mathit{fr}}(x, 0) = X_f$, $(x, 0)$ is not connected by a forward edge to a node in fr and $[(x, 0)]_{\mathit{fr}} \cup \mathsf{XF}^{-1}_{\mathit{fr}}(x, 0) = X_p$. A *point of decrement* for $\langle X_p, X_f \rangle$ in fr is an equivalence class of the form $[(x, l)]_{\mathit{fr}}$ such that $\mathsf{XF}_{\mathit{fr}}(x, l) \cup [(x, l)]_{\mathit{fr}} = X_f$, (x, l) is not connected by a backward edge to another node in fr and $\mathsf{XF}^{-1}_{\mathit{fr}}(x, l) = X_p$. Let u^+_{fr} denote a counter valuation which records the number of points of increment for each counter $\langle X_p, X_f \rangle$ in fr. Similarly, let u^-_{fr} denote the counter valuation which records the number of points of decrement for each counter $\langle X_p, X_f \rangle$ in fr. The canonical counter valuation sequence α along ρ, also called the *counting sequence* along ρ, is defined by: for every $\langle X_p, X_f \rangle \in (\mathcal{P}^+(\{x_1, \ldots, x_k\}))^2$ we have $\alpha(0)(\langle X_p, X_f \rangle) = 0$ and for every $0 \leq i < |\rho|$,

$$\alpha(i+1)(\langle X_p, X_f \rangle) = \alpha(i)(\langle X_p, X_f \rangle) + (u^+_{\rho(i)}(\langle X_p, X_f \rangle) - u^-_{\rho(i+1)}(\langle X_p, X_f \rangle))$$

with the new definition of u^+_{fr} and u^-_{fr}. Unlike the counting sequences along symbolic models of $\mathrm{CLTL}^{\mathsf{XF}}$, decrementing is this time compulsory and we allow $\alpha(i)(\langle X_p, X_f \rangle)$ to be negative. However, we will require in the acceptance condition that the counters remain non-negative: a counter with a negative value means that some past obligations could not be satisfied. Though we need more counters, dealing with past repeating values does not introduce serious complications. This is analogous to the passage from LTL to LTL with past-time operators since past is finite and information about past can be accumulated smoothly.

Lemma 10 *A symbolic model ρ for the logic $\mathrm{CLTL}^{\mathsf{XF},\mathsf{XF}^{-1}}$ is satisfiable iff the counting sequence along ρ satisfies the conditions from Lemma 5 for the future part of the counters and for all $0 \leq i < |\rho|$, we have $\alpha(i)(\langle X_p, X_f \rangle) \geq 0$.*

Proof. Suppose that a symbolic model ρ admits a model σ. A development similar to the proof of Lemma 5 can be used to treat the part linked to future obligations, so that we can prove that ρ verifies conditions of Lemma 5. We just have to show that for $0 \leq i < |\rho|$, we have $\alpha(i)(\langle X_p, X_f \rangle) \geq 0$. This fact is obvious since one can easily shown that there is a one-one correspondence between points of increment and decrement induced by the values that

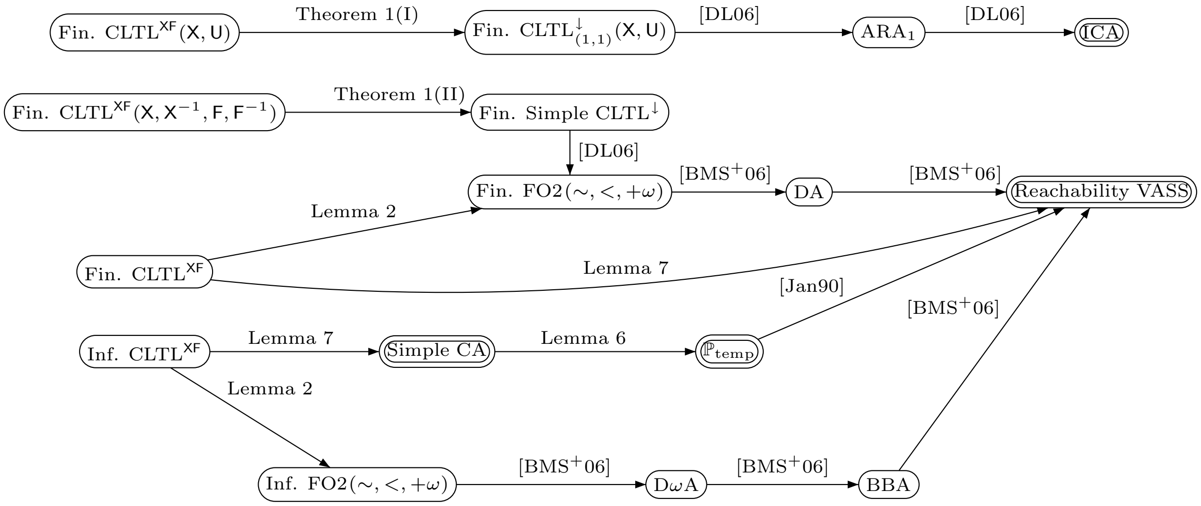

Fin. CLTL$^{\mathsf{XF}}(\mathsf{X},\mathsf{U})$
Theorem 1(I)
Fin. CLTL$^{\downarrow}_{(1,1)}(\mathsf{X},\mathsf{U})$
[DL06]
ARA$_1$
[DL06]
ICA
Fin. CLTL$^{\mathsf{XF}}(\mathsf{X},\mathsf{X}^{-1},\mathsf{F},\mathsf{F}^{-1})$
Theorem 1(II)
Fin. Simple CLTL$^{\downarrow}$
[DL06]
Fin. FO2$(\sim,<,+\omega)$
[BMS$^+$06]
DA
[BMS$^+$06]
Reachability VASS
Lemma 2
Fin. CLTL$^{\mathsf{XF}}$
Lemma 7
[Jan90]
[BMS$^+$06]
Inf. CLTL$^{\mathsf{XF}}$
Lemma 7
Simple CA
Lemma 6
$\mathbb{P}_{\mathrm{temp}}$
Lemma 2
Inf. FO2$(\sim,<,+\omega)$
[BMS$^+$06]
DωA
[BMS$^+$06]
BBA

Figure 3: Summary of reductions

are repeated in σ such that each point of increment occurs before the corresponding point of decrement in ρ (see the beginning of the proof of Lemma 5). So the values of the counters cannot become negative.

For the converse direction, we just have to update the way we add the augmented edges from the proof of Lemma 5 by considering the past repetitions. The additional condition stating that every counter is always positive ensure that each point of decrement can be related to a node of lower level by an augmented edge. Then the proof is similar to Lemma 5. □

As a consequence, we can easily update the construction of $\mathcal{A}_\phi$ in order to deal with past repeating values. The definitions of the automata $\mathcal{A}_{1\mathrm{sc}}$, $\mathcal{A}_{\mathrm{symb}}$ and $\mathcal{A}_{\mathrm{real}}$ are just extended by considering the new definition for frames. It is also important to observe that the automaton $\mathcal{A}_\phi$ obtained by synchronization of these automata still belongs to the class of simple counter automata and so the decidability result still holds for CLTL$^{\mathsf{XF},\mathsf{XF}^{-1}}$ satisfiability problem. The construction for the one-variable fragment can also be adapted according to the extended definitions. So we obtain the following results.

Theorem 6
(I) *Finitary and infinitary satisfiability for* CLTL$^{\mathsf{XF},\mathsf{XF}^{-1}}$ *are decidable.*
(II) *Finitary and infinitary satisfiability for* CLTL$_1^{\mathsf{XF},\mathsf{XF}^{-1}}$ *are* PSPACE*-complete.*

The above decidability result can be alternatively obtained by adapting the developments from Section 3.2. The corollary of Theorem 4 about the extension with MSO-definable operators still holds when adding past repetition constraints.

Corollary 3 *The finitary and infinitary satisfiability problems for* CLTL$^{\mathsf{XF},\mathsf{XF}^{-1}}$ *augmented with MSOL definable temporal operators are decidable.*

10 Concluding Remarks

We have shown that satisfiability for CLTL$^{\mathsf{XF}}$ with operators in $\{\mathsf{X}, \mathsf{X}^{-1}, \mathsf{S}, \mathsf{U}\}$ is decidable by reduction into the verification of fairness properties in Petri nets [Jan90]. The proof in Sections 4–7 is uniform for the finitary and infinitary cases and it can be extended to atomic constraints of the form $x = \mathsf{XF}^{-1}y$ and to any set of MSOL definable temporal operators. Moreover, satisfiability for CLTL$^{\mathsf{XF}}$ restricted to one variable is shown to be PSPACE-complete. Hence, we have defined and studied a well-designed decidable fragment of LTL with the freeze quantifier using a repeating operator inspired from [WZ00] (viewing $x = \mathsf{XF}y$ as the generalized disjunction $\bigvee_{i>0} x = \mathsf{X}^i y$) and circumventing some undecidability results from [DL06, FS09]. Finally, as done also in [DL06, Laz06, BMS$^+$06], we show relationships between fragments of LTL with freeze and counter automata. Our connection is all the more interesting because we deal with the finitary and infinitary cases while preserving decidability. Alternative proofs are also presented in Section 3, some of them for strict fragments of CLTL$^{\mathsf{XF}}$. However, we believe that even though some decidability results are proved in different ways in the paper, they help understanding the essential ingredients of repeating constraints in CLTL$^{\mathsf{XF}}$.

In Figure 3, we summarize the reductions presented in the paper as well as related reductions to nonemptiness problems to various classes of automata. We use the following abbreviations: ARA$_1$ for alternating register automata restricted to one register [DL06], ICA for incrementing counter automata [DL06] (zero-tests are allowed but incrementing errors can occur), DA for data automata [BMS$^+$06], DωA for data ω-automata [BMS$^+$06], BBA for Büchi bag automata [BMS$^+$06]. Nonemptiness problems for classes of counter automata are presented by nodes with two lines. It is worth observing that most of the problems are decidable by reduction into the reachability problem for VASS that has been shown decidable in [May84, Kos82, Lam92].

The main question left open by our work is the complexity of satisfiability for CLTL$^{\mathsf{XF}}$ and more precisely we do not know whether CLTL$^{\mathsf{XF}}$ satisfiability has elementary complexity. Similarly, are there natural fragments of CLTL$^{\mathsf{XF}}$ that are of lower complexity, for instance the one involved in Theorem 1? Another promising extension consists in considering other concrete domains as $\langle \mathbb{R}, <, = \rangle$ and to allow atomic formulae of the form $x < \mathsf{XF}y$. The decidability status of such a variant is still open, even if in absence of the restricted use of the freeze quantifier, PSPACE-completeness is known [DD07]. Finally, it would be interesting to investigate branching-time extensions.

Acknowledgements: We are grateful to Petr Jančar (TU Ostrava) for pointing us to [Jan90] in order to solve the nonemptiness problem for simple counter automata and for suggesting the proof of Lemma 6 and Ranko Lazić (U. of Warwick) for remarks about a preliminary version. We wish also to thank Luc Segoufin (LSV, Cachan) for pointing out to us in January 2008 that CLTL$^{\mathsf{XF}}_1$ satisfiability could be encoded into EMSO2($\sim, <, +1$) (FO2($\sim, <, +1$) with a prefix of existential monadic second-order quantifications), which then allows us to reduce full CLTL$^{\mathsf{XF}}$ satisfiability to that of FO2($\sim, +1, +\omega$). This insight has been the starting point for developing Section 3.2. Finally, we would like to thank the anonymous referees of previous versions for their helpful suggestions and remarks.

References

[ABM01] C. Areces, P. Blackburn, and M. Marx. Hybrid logics: characterization, interpolation and complexity. *The Journal of Symbolic logic*, 66(3):977–1010, 2001.

[AH94] R. Alur and Th. Henzinger. A really temporal logic. *Journal of the ACM*, 41(1):181–204, 1994.

[BMS$^+$06] M. Bojańczyk, A. Muscholl, Th. Schwentick, L. Segoufin, and C. David. Two-variable logic on words with data. In *LICS'06*, pages 7–16. IEEE, 2006.

[Dav09] C. David. *Analyse de XML avec données non-bornées.* PhD thesis, LIAFA, Université Paris VII, 2009.

[DD07] S. Demri and D. D'Souza. An automata-theoretic approach to constraint LTL. *Information & Comptutation*, 205(3):380–415, 2007.

[DDG07a] S. Demri, D. D'Souza, and R. Gascon. Decidable temporal logic of repeating values. In *LFCS'07*, volume 4514 of *Lecture Notes in Computer Science*, pages 180–194. Springer, 2007.

[DDG07b] S. Demri, D. D'Souza, and R. Gascon. A decidable temporal logic of repeating values. Technical Report LSV-07-17, LSV, April 2007.

[DG09] S. Demri and R. Gascon. The effects of bounding syntactic resources on Presburger LTL. *Journal of Logic and Computation*, 19(6):1541–1575, December 2009.

[DL06] S. Demri and R. Lazić. LTL with the freeze quantifier and register automata. In *LICS*, pages 17–26. IEEE, 2006.

[DLN05] S. Demri, R. Lazić, and D. Nowak. On the freeze quantifier in constraint LTL: Decidability and complexity. In *TIME'05*, pages 113–121. IEEE, 2005.

[DLN07] S. Demri, R. Lazić, and D. Nowak. On the freeze quantifier in constraint LTL: decidability and complexity. *Information & Comptutation*, 205(1):2–24, 2007.

[DS98] S. Demri and P. Schnoebelen. The complexity of propositional linear temporal logics in simple cases. *I&C*, 174:61–72, 1998.

[Fig10] D. Figueira. *Reasoning on words and trees with data.* PhD thesis, ENS Cachan, 2010.

[Fit02] M. Fitting. Modal logic between propositional and first-order. *Journal of Logic and Computation*, 12(6):1017–1026, 2002.

[FS09] D. Figueira and L. Segoufin. Future-looking logics on data words and trees. In *MFCS'09*, volume 5734 of *Lecture Notes in Computer Science*, pages 331–343. Springer, 2009.

[GK03] P. Gastin and D. Kuske. Satisfiability and model checking for MSO-definable temporal logics are in PSPACE. In *CONCUR'03*, volume 2761 of *Lecture Notes in Computer Science*, pages 222–236. Springer, 2003.

[Gor96] V. Goranko. Hierarchies of modal and temporal logics with references pointers. *Journal of Logic, Language, and Information*, 5:1–24, 1996.

[Hen90] Th. Henzinger. Half-order modal logic: how to prove real-time properties. In *PODC'90*, pages 281–296. ACM, 1990.

[Jan90] P. Jančar. Decidability of a temporal logic problem for Petri nets. *Theoretical Computer Science*, 74(1):71–93, 1990.

[KF94] M. Kaminski and N. Francez. Finite-memory automata. *Theoretical Computer Science*, 134(2):329–363, 1994.

[Kos82] S. Rao Kosaraju. Decidability of reachability in vector addition systems. In *STOC'82*, pages 267–281, 1982.

[KSZ10] A. Kara, Th. Schwentick, and Th. Zeume. Temporal logics on words with multiple data values. In *FST&TCS'10*, pages 481–492. LZI, 2010.

[KV06] O. Kupferman and M. Vardi. Memoryful Branching-Time Logic. In *LICS'06*, pages 265–274. IEEE, 2006.

[Lam92] J.L. Lambert. A structure to decide reachability in Petri nets. *Theoretical Computer Science*, 99:79–104, 1992.

[Laz06] R. Lazić. Safely freezing LTL. In *FST&TCS'06*, volume 4337 of *Lecture Notes in Computer Science*, pages 381–392. Springer, 2006.

[LMS02] F. Laroussinie, N. Markey, and Ph. Schnoebelen. Temporal logic with forgettable past. In *LICS'02*, pages 383–392. IEEE, 2002.

[LP05] A. Lisitsa and I. Potapov. Temporal logic with predicate λ-abstraction. In *TIME'05*, pages 147–155. IEEE, 2005.

[May84] E.W. Mayr. An algorithm for the general petri net reachability problem. *SIAM Journal of Computing*, 13(3):441–460, 1984.

[Min67] M. Minsky. *Computation, Finite and Infinite Machines*. Prentice Hall, 1967.

[NSV04] F. Neven, T. Schwentick, and V. Vianu. Finite state machines for strings over infinite alphabets. *ACM Transactions on Computational Logic*, 5(3):403–435, 2004.

[Pet81] J.L. Peterson. *Petri Net Theory and the Modelling of Systems*. Prentice-Hall, 1981.

[Reu90] C. Reutenauer. *The mathematics of Petri nets*. Masson and Prentice, 1990.

[Seg06] L. Segoufin. Automata and logics for words and trees over an infinite alphabet. In *CSL'06*, volume 4207 of *Lecture Notes in Computer Science*, pages 41–57. Springer, 2006.

[tCF05] B. ten Cate and M. Franceschet. On the complexity of hybrid logics with binders. In *CSL'05*, volume 3634 of *Lecture Notes in Computer Science*, pages 339–354. Springer, 2005.

[VW94] M. Vardi and P. Wolper. Reasoning about infinite computations. *Information & Comptutation*, 115:1–37, 1994.

[WZ00] F. Wolter and M. Zakharyaschev. Spatio-temporal representation and reasoning based on RCC-8. In *KR'00*, pages 3–14. Morgan Kaufmann, 2000.