Combination Methods for Satisfiability and Model-Checking of Infinite-State Systems

Silvio Ghilardi[1], Enrica Nicolini[2], Silvio Ranise[2], and Daniele Zucchelli[1,2]

[1] Dipartimento di Informatica, Università degli Studi di Milano (Italia)
[2] LORIA & INRIA-Lorraine, Nancy (France)

Abstract. Manna and Pnueli have extensively shown how a mixture of first-order logic (FOL) and discrete Linear time Temporal Logic (LTL) is sufficient to precisely state verification problems for the class of reactive systems. Theories in FOL model the (possibly infinite) data structures used by a reactive system while LTL specifies its (dynamic) behavior. In this paper, we derive undecidability and decidability results for both the satisfiability of (quantifier-free) formulae and the model-checking of safety properties by lifting combination methods for (non-disjoint) theories in FOL. The proofs of our decidability results suggest how decision procedures for the constraint satisfiability problem of theories in FOL and algorithms for checking the satisfiability of propositional LTL formulae can be integrated. This paves the way to employ efficient Satisfiability Modulo Theories solvers in the model-checking of infinite state systems. We illustrate our techniques on two examples.

1 Introduction

In [12] and many other writings, Manna and Pnueli have extensively shown how a mixture of first-order logic (FOL) and discrete Linear time Temporal Logic (LTL) is sufficient to precisely state verification problems for the class of reactive systems. Theories in FOL model the (possibly infinite) data structures used by a reactive system while LTL specifies its (dynamic) behavior. The combination of LTL and FOL allows one to specify infinite state systems and the subtle ways in which their data flow influences the control flow. Indeed, the capability of automatically solving satisfiability and model-checking problems is of paramount importance to support the automation of verification techniques using this framework. In this paper, our approach is to reduce both problems to first-order combination problems over non-disjoint theories.

Preliminarily, we describe our framework for *integrating LTL operators with theories in FOL* (cf. Section 2.1): we fix a theory T in a first-order signature Σ and consider as a temporal model a sequence $\mathcal{M}_1, \mathcal{M}_2, \ldots$ of standard (first-order) models of T and assume such models to share the same carrier (or, equivalently, the domain of the temporal model is 'constant'). Following [15], we consider symbols from a subsignature Σ_r of Σ to be *rigid*, i.e. in a temporal model $\mathcal{M}_1, \mathcal{M}_2, \ldots$, the Σ_r-restrictions of the $\mathcal{M}_i$'s must coincide. The symbols in $\Sigma \setminus \Sigma_r$ are called 'flexible' and their interpretation is allowed to change

F. Pfenning (Ed.): CADE 2007, LNAI 4603, pp. 362-378, 2007.

over time (free variables are similarly divided into 'rigid' and 'flexible'). For model-checking, the *initial states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model (cf. Section 4).

The *first contribution* (cf. Theorem 3.1 in Section 3) of the paper is a reduction of the satisfiability problem for quantifier-free LTL formulae modulo the background theory T to an instance of the Nelson-Oppen combination problem for first-order theories (the combination being disjoint if the rigid subsignature is empty). More precisely, we consider a theory T whose constraint satisfiability problem consists of non-deterministically solving one of the (decidable) constraint satisfiability problem of two signature-disjoint theories T_1, T_2. Although the satisfiability problem of T is decidable, it is possible to write a quantifier-free LTL formula which is equisatisfiable to a constraint of $T_1 \cup T_2$, whose satisfiability problem turns out to be undecidable if T_1 and T_2 are chosen as shown in [1]. The undecidability of the safety model-checking problem follows (under mild hypotheses) from a well-known reduction to the reachability problem for Minsky machines [13].

Since the satisfiability problem for quantifier-free LTL formulae modulo a background theory T looks very much like a non-disjoint combination problem, the hope is that the same (or similar) requirements yielding the decidability of the constraint satisfiability problem in unions of theories [8], will also give decidability here. The *second contribution* (cf. Theorem 3.2 in Section 3) of the paper is to show that this is indeed the case: we derive the decidability of the satisfiability problem for quantifier-free LTL formulae modulo T, in case T has decidable universal fragment and is T_r-compatible [8], where T_r is the restriction of the universal fragment of T to the rigid subsignature. For termination, one must also assume T_r to be locally finite [8].

The *third* (and main) *contribution* (Theorem 4.1 in Section 4) of the paper is that (under the same hypotheses of T_r-compatibility and local finiteness) the model-checking problem for quantifier-free safety properties is also decidable. The proof of this result suggests how decision procedures for the constraint satisfiability problem of theories in FOL and algorithms for checking the satisfiability of propositional LTL formulae can be integrated. This paves the way to employ efficient *Satisfiability Modulo Theories* (SMT) solvers in the model-checking of infinite state systems, as previous proposals have suggested their use for bounded model-checking [4]. Finally, we illustrate our techniques on two examples.

For lack of space, the proofs of our results are omitted: they can be found in the on-line version of the paper and also in the Technical Report [9].

2 Background

We assume the usual first-order syntactic notions of signature, term, position, atoms, formula, and so on. Let Σ be a first-order signature; we assume the equality symbol '=' to be part of the language ('equality is a logical constant'), so that it can be used to build formulae, but it is not explicitly displayed in

a signature. A Σ-*constraint* is a set of Σ-literals (intended conjunctively). A positive Σ-clause is a disjunction of Σ-atoms. A Σ-theory T is a set of sentences in the signature Σ; the sentences in T are also called *axioms*. A theory is *universal* iff it has universal closures of open formulas as axioms. We also assume the usual first-order notions of interpretation, satisfiability, validity, and logical consequence. The equality symbol '=' is interpreted as the identity. If $\Sigma_0 \subseteq \Sigma$ is a subsignature of Σ and if $\mathcal{M}$ is a Σ-structure, the Σ_0-*reduct* of $\mathcal{M}$ is the Σ_0-structure $\mathcal{M}_{|\Sigma_0}$ obtained from $\mathcal{M}$ by forgetting the interpretation of function and predicate symbols from $\Sigma \setminus \Sigma_0$. A Σ-structure $\mathcal{M}$ is a *model* of a Σ-theory T (in symbols, $\mathcal{M} \models T$) iff all the sentences of T are true in $\mathcal{M}$. A Σ-theory T admits *elimination of quantifiers* iff for every formula $\varphi(\underline{x})$ there is a quantifier-free formula $\varphi'(\underline{x})$ such that $T \models \varphi(\underline{x}) \leftrightarrow \varphi'(\underline{x})$. Standard versions of Linear Arithmetics, Real Arithmetics, acyclic lists, and any theory axiomatizing enumerated datatypes admit elimination of quantifiers. Let Σ be a finite signature; an *enumerated datatype theory* in the signature Σ is the theory consisting of the set of sentences which are true in a finite given Σ-structure $\mathcal{M} = (M, \mathcal{I})$; we also require that for every $m \in M$ there is $c \in \Sigma$ such that $c^{\mathcal{M}} = m$. It is easy to see that an enumerated datatype theory has a finite set of universal axioms and admits elimination of quantifiers.

The *(constraint) satisfiability problem* for the theory T is the problem of deciding whether a Σ-sentence (Σ-constraint, resp.) is satisfiable in a model of T. We will use free constants instead of variables in constraint satisfiability problems, so that we (equivalently) redefine a constraint satisfiability problem for the theory T as the problem of *establishing the satisfiability of* $T \cup \Gamma$ (or, equivalently, the T-satisfiability of Γ) *for a finite set* Γ *of ground* $\Sigma^{\underline{a}}$*-literals* (where $\Sigma^{\underline{a}} := \Sigma \cup \{\underline{a}\}$, for a finite set of new constants $\underline{a}$). For the same reason, from now on, *by a '*Σ*-constraint' we mean a 'ground* $\Sigma^{\underline{a}}$*-constraint'*, where the free constants $\underline{a}$ should be clear from the context.

A Σ-*embedding* (or, simply, an embedding) between two Σ-structures $\mathcal{M} = (M, \mathcal{I})$ and $\mathcal{N} = (N, \mathcal{J})$ is any mapping $\mu : M \longrightarrow N$ among the corresponding support sets satisfying the condition

$$(*) \qquad \mathcal{M} \models \varphi \text{ iff } \mathcal{N} \models \varphi,$$

for all Σ^M-atoms φ (here $\mathcal{M}$ is regarded as a Σ^M-structure, by interpreting each additional constant $a \in M$ into itself and $\mathcal{N}$ is regarded as a Σ^M-structure by interpreting each additional constant $a \in M$ into $\mu(a)$). If $M \subseteq N$ and if the embedding $\mu : \mathcal{M} \longrightarrow \mathcal{N}$ is just the identity inclusion $M \subseteq N$, we say that $\mathcal{M}$ is a *substructure* of $\mathcal{N}$ or that $\mathcal{N}$ is an *extension* of $\mathcal{M}$. In case condition (*) holds for all first order formulas, the embedding μ is said to be *elementary*. Correspondingly, in case μ is also an inclusion, we say that $\mathcal{M}$ is an elementary substructure of $\mathcal{N}$ or that $\mathcal{N}$ is an elementary extension of $\mathcal{M}$.

The T_0-compatibility notion is crucial for the completeness of combination schemas [8].

Definition 2.1 (T_0-compatibility [8]). *Let T be a theory in the signature Σ and T_0 be a universal theory in a subsignature $\Sigma_0 \subseteq \Sigma$. We say that T is T_0-*

compatible *iff* $T_0 \subseteq T$ *and there is a* Σ_0*-theory* $T_0^\star$ *such that* (1) $T_0 \subseteq T_0^\star$*;* (2) $T_0^\star$ *has quantifier elimination;* (3) *every model of* T_0 *can be embedded into a model of* $T_0^\star$*; and* (4) *every model of* T *can be embedded into a model of* $T \cup T_0^\star$*.*

If T_0 is the empty theory over the empty signature, then $T_0^\star$ is the theory axiomatizing an infinite domain and (4) above can be shown equivalent to the stably infinite requirement of the Nelson-Oppen schema [14,19].

Local finiteness yields termination of combination schemas [8].

Definition 2.2 (Local Finiteness [8]). *A* Σ_0*-theory* T_0 *is* locally finite *iff* Σ_0 *is finite and, for every finite set of free constants* $\underline{a}$*, there are finitely many ground* $\Sigma_0^{\underline{a}}$*-terms* $t_1, \ldots, t_{k_{\underline{a}}}$ *such that for every further ground* $\Sigma_0^{\underline{a}}$*-term* u*, we have that* $T_0 \models u = t_i$ *(for some* $i \in \{1, \ldots, k_{\underline{a}}\}$*). If such* $t_1, \ldots, t_{k_{\underline{a}}}$ *are effectively computable from* $\underline{a}$ *(and* t_i *is computable from* u*), then* T_0 *is* effectively locally finite*.*

If T_0 is effectively locally finite, for any finite set of free constants $\underline{a}$ it is possible to compute finitely many $\Sigma_0^{\underline{a}}$-atoms $\psi_1(\underline{a}), \ldots, \psi_m(\underline{a})$ such that for any $\Sigma_0^{\underline{a}}$-atom $\psi(\underline{a})$, there is some i such that $T_0 \models \psi_i(\underline{a}) \leftrightarrow \psi(\underline{a})$. These atoms $\psi_1(\underline{a}), \ldots, \psi_m(\underline{a})$ are the *representatives* (modulo T_0-equivalence) and they can replace arbitrary $\Sigma_0^{\underline{a}}$-atoms for computational purposes. For example, any theory in a purely relational signature is locally finite (this will be used in Example 4.1).

The following technical Lemma is the key combination result allowing us to reduce satisfiability in first-order LTL to satisfiability in first-order logic.

Lemma 2.1. *Let* $\Sigma_i^{\underline{c},\underline{a}_i}$ *(here* i *ranges over a given set* I *of indexes) be signatures expanded with free constants* $\underline{c} \cup \underline{a}_i$*, whose pairwise intersections are all equal to a certain signature* $\Sigma_r^{\underline{c}}$ *(i.e.* $\Sigma_i^{\underline{c},\underline{a}_i} \cap \Sigma_j^{\underline{c},\underline{a}_j} = \Sigma_r^{\underline{c}}$*, for all distinct* $i, j \in I$*). Suppose we are also given* Σ_i*-theories* T_i *which are all* T_r*-compatible, where* $T_r \subseteq \bigcap_i T_i$ *is a universal* Σ_r*-theory; let finally* $\{\mathcal{N}_i = (N_i, \mathcal{I}_i)\}_{i \in I}$ *be a sequence of* $\Sigma_i^{\underline{c},\underline{a}_i}$*-structures which are models of* T_i *and satisfy the same* $\Sigma_r^{\underline{c}}$*-atoms. Under these hypotheses, there exists a* $\bigcup_i (\Sigma_i^{\underline{c},\underline{a}_i})$*-structure* $\mathcal{M} \models \bigcup_i T_i$ *such that* $\mathcal{N}_i$ *has a* $\Sigma_i^{\underline{c},\underline{a}_i}$*-embedding into* $\mathcal{M}$*, for each* $i \in I$*.*

2.1 Temporal Logic

We assume the standard syntactic and semantic notions concerning Propositional LTL (PLTL), such as PLTL-formula and PLTL-Kripke model. Following [12], we fix a first-order signature Σ and we consider formulae obtained by applying temporal and Boolean operators (but no quantifiers) to first-order Σ-formulae.

Definition 2.3 (LTL($\Sigma^{\underline{a}}$)-Sentences). *Let* Σ *be a signature and* $\underline{a}$ *be a (possibly infinite) set of free constants. The set of LTL*($\Sigma^{\underline{a}}$)*-sentences is inductively defined as follows: (i) if* φ *is a first-order* $\Sigma^{\underline{a}}$*-sentence, then* φ *is an LTL*($\Sigma^{\underline{a}}$)*-sentence and (ii) if* ψ_1, ψ_2 *are LTL*($\Sigma^{\underline{a}}$)*-sentences, so are* $\psi_1 \wedge \psi_2$*,* $\neg\psi_1$*,* $X\psi_1$*,* $\psi_1 U \psi_2$*.*

We abbreviate $\neg(\neg\psi_1 \wedge \neg\psi_2), \top U\psi, \neg\Diamond\neg\psi, \neg(\neg\psi_1 U \neg\psi_2)$ as $\psi_1 \vee \psi_2, \Diamond\psi, \Box\psi$, and $\psi_1 R \psi_2$, respectively. Notice that free constants are allowed in the definition of a LTL($\Sigma^{\underline{a}}$)-sentence.

Definition 2.4. *Given a signature Σ and a set $\underline{a}$ of free constants, an* LTL($\Sigma^{\underline{a}}$)-structure *(or simply a* structure*) is a sequence $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n\in\mathbb{N}}$ of $\Sigma^{\underline{a}}$-structures. The set M is called the* domain *(or the* universe*) and $\mathcal{I}_n$ is called the n-*th level interpretation function *of the LTL($\Sigma^{\underline{a}}$)-structure.*

So, an LTL($\Sigma^{\underline{a}}$)-structure is a family of $\Sigma^{\underline{a}}$-structures indexed over the naturals. When considering a background Σ-theory T, these structures will also be models of T. What should the various $\Sigma^{\underline{a}}$-structures of the family share? Our answer (according to Definition 2.4) is that they should share their domains or, equivalently, we assume M_n to be *constant*.

Definition 2.5. *Given an LTL($\Sigma^{\underline{a}}$)-sentence φ and $t \in \mathbb{N}$, the notion of "φ being true in the LTL($\Sigma^{\underline{a}}$)-structure $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n\in\mathbb{N}}$ at the instant t" (in symbols $\mathcal{M} \models_t \varphi$) is inductively defined as follows:*

- *if φ is a first-order $\Sigma^{\underline{a}}$-sentence, $\mathcal{M} \models_t \varphi$ iff $\mathcal{M}_t \models \varphi$;*
- *$\mathcal{M} \models_t \neg\varphi$ iff $\mathcal{M} \not\models_t \varphi$;*
- *$\mathcal{M} \models_t \varphi \wedge \psi$ iff $\mathcal{M} \models_t \varphi$ and $\mathcal{M} \models_t \psi$;*
- *$\mathcal{M} \models_t X\varphi$ iff $\mathcal{M} \models_{t+1} \varphi$;*
- *$\mathcal{M} \models_t \varphi U \psi$ iff there exists $t' \geq t$ such that $\mathcal{M} \models_{t'} \psi$ and for each t'', $t \leq t'' < t' \Rightarrow \mathcal{M} \models_{t''} \varphi$.*

We say that φ is true in *$\mathcal{M}$ or, equivalently, that $\mathcal{M}$* satisfies *φ (in symbols $\mathcal{M} \models \varphi$) iff $\mathcal{M} \models_0 \varphi$.*

Which is the relationship between the interpretations $\mathcal{I}_n$ in an LTL($\Sigma^{\underline{a}}$)-structure? Following [15], our answer is that certain symbols are declared *rigid* (i.e. their interpretation is time independent) while the remaining are considered *flexible* (i.e. time dependent). There are various reasons supporting this choice. The most important is that our framework allows us more flexibility in solving certain problems: actions from the environment on a reactive systems are somewhat unpredictable and can be better modelled by flexible function symbols, as demonstrated by the following Example.

Example 2.1. Suppose we want to model a a water level controller. To this aim, we need two functions symbols *in*(flow)/*out*(flow) expressing the water level variations induced by the environment and by the opening action of the valve, respectively: these functions depend both on the current water level and on the time instant, thus the natural choice is to model them by just *unary* function symbols, which are then *flexible* because the time dependency becomes in this way implicit. On the other hand, the constants expressing the alarm and the overflow level should not depend on the time instant, hence they are modeled as *rigid* constants; for obvious reasons, the arithmetical binary comparison symbol $<$ is also time-independent, hence *rigid* too. Having chosen these (flexible and rigid) symbols, we can express constraints on the behavior of our system by introducing a suitable theory (see Example 4.1 below for details).

There is also a more technical (but still crucial) reason underlying our distinction between rigid and flexible symbols: we can avoid some undecidability problems by carefully choosing problematic function or predicates to be flexible. In fact, if we succeed to keep the rigid part relatively simple (e.g., a locally finite theory), then we usually do not lose decidability.

Definition 2.6. *An* LTL-theory *is a 5-tuple* $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ *where* Σ *is a signature,* T *is a* Σ*-theory (called the underlying theory of* $\mathcal{T}$*),* Σ_r *is a subsignature of* Σ*, and* $\underline{a}, \underline{c}$ *are sets of free constants.*

Σ_r is the *rigid subsignature* of the LTL-theory; the constants $\underline{c}$ will be rigidly interpreted, whereas the constants $\underline{a}$ will be interpreted in a time-dependant way. The constants $\underline{a}$ are also (improperly) called the *system variables* of the LTL-theory, and the constants $\underline{c}$ are called its *system parameters*. The equality symbol will always be considered as rigid. A LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ is *totally flexible* iff Σ_r is empty and is *totally rigid* iff $\Sigma_r = \Sigma$.

3 The Satisfiability Problem

We formally state the satisfiability problem for LTL($\Sigma^{\underline{a}}$)-sentences.

Definition 3.1. *An LTL*($\Sigma^{\underline{a},\underline{c}}$)*-structure* $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$ *is* appropriate *for an LTL-theory* $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ *iff we have*

$$\mathcal{M}_n \models T, \quad \mathcal{I}_n(f) = \mathcal{I}_m(f), \quad \mathcal{I}_n(P) = \mathcal{I}_m(P), \quad \mathcal{I}_n(c) = \mathcal{I}_m(c).$$

for all $m, n \in \mathbb{N}$*, for each function symbol* $f \in \Sigma_r$*, for each relational symbol* $P \in \Sigma_r$*, and for all constants* $c \in \underline{c}$*. The* satisfiability problem for $\mathcal{T}$ *is the following: given an LTL*($\Sigma^{\underline{a},\underline{c}}$)*-sentence* φ*, decide whether there is an LTL*($\Sigma^{\underline{a},\underline{c}}$)*-structure* $\mathcal{M}$ *appropriate for* $\mathcal{T}$ *such that* $\mathcal{M} \models \varphi$*. When* φ *is ground, we speak of* ground satisfiability problem for $\mathcal{T}$*.*

In the following, it is useful to distinguish two classes of LTL-theories.

Definition 3.2. *An LTL-theory* $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ *is*

1. finite state *iff it is totally rigid and* T *is an enumerated datatype theory;*
2. locally finite compatible *iff there is a* Σ_r*-universal and effectively locally finite theory* T_r *such that* T *is* T_r*-compatible;*

Enumerated datatype theories are locally finite, but not conversely (for instance, the theory of dense linear orders is locally finite but cannot be the theory of a single finite structure, because finite linear orders are not dense).

In the hope to derive decidability results for the satisfiability of first-order LTL formulae, we restrict ourselves to consider only ground formulae and assume the decidability of the constraint satisfiability problem of the theory underlying any LTL-theory (cf. Assumption 1 in Figure 1). Unfortunately, this assumption alone is not sufficient to guarantee the decidability of the ground satisfiability problem (cf. Definition 3.1).

Assumptions

1. We assume the underlying theory T of an LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ to have decidable constraint satisfiability problem.
2. For any LTL-system specification $(\mathcal{T}, \delta, \iota)$, the transition relation δ and the initial state description ι in a system specification $(\mathcal{T}, \delta, \iota)$ are assumed to be ground sentences. Furthermore, we assume all our LTL-systems specifications to be serial.

Fig. 1. The main assumptions of the paper

Theorem 3.1. *There exists a totally flexible LTL-theory $\mathcal{T}$ whose ground satisfiability problem is undecidable.*

There are two key observations underlying the proof of our undecidability result. First, we build a theory T whose constraint satisfiability problem consists of non-deterministically solving the constraint satisfiability problem among two signature-disjoint theories T_1, T_2. It is easy to see that the decidability of the constraint satisfiability problem transfer from T_1, T_2 to T. The second observation is that for every constraint Γ it is possible to write an LTL($\Sigma^{\underline{a}}$)-sentence whose satisfiability is equivalent to the satisfiability of Γ in $T_1 \cup T_2$. In [1], it is shown that such a problem is undecidable for suitable T_1 and T_2.

These arguments suggest that the undecidability of the ground satisfiability problem for a given LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ arises precisely for the same reasons leading to the undecidability of combined constraint satisfiability problems in the first-order framework. It turns out that the requirements yielding the decidability of the constraint satisfiability problem in unions of theories will also give the decidability of the ground satisfiability problem for $\mathcal{T}$.

Theorem 3.2. *The ground satisfiability problem for a locally finite compatible LTL-theory is decidable.*

Below, we give two constructive proofs of this Theorem (cf. Proposition 3.1 and Corollary 3.1).

For the rest of this Section, we fix a locally finite compatible LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$. A syntactic relationship between (ground) first-order and propositional LTL-formulae can be introduced as follows.

Definition 3.3 (PLTL-Abstraction). *Given a signature $\Sigma^{\underline{a}}$ and a set $\mathcal{L}$ of propositional letters (of the same cardinality as the set of ground $\Sigma^{\underline{a}}$-atoms), let $[\![\cdot]\!]$ be a bijection from the set of ground $\Sigma^{\underline{a}}$-atoms into $\mathcal{L}$. By translating identically Boolean and temporal connectives, the map is inductively extended to a bijective map (also denoted with $[\![\cdot]\!]$) from the set of ground LTL($\Sigma^{\underline{a}}$)-sentences onto the set of propositional $\mathcal{L}$-formulae.*

Given a ground LTL($\Sigma^{\underline{a}}$)-sentence φ, we call $[\![\varphi]\!]$ the *PLTL-abstraction* of φ; if Θ is a set of ground LTL($\Sigma^{\underline{a}}$)-sentences, then $[\![\Theta]\!] := \{ [\![\varphi]\!] \mid \varphi \in \Theta \}$.

Eager Reduction to Propositional LTL-Satisfiability. The key of our reduction to the satisfiability problem in PLTL is guessing.

Definition 3.4 (Guessing). *Let Σ be a signature Σ and S be a finite set of Σ-atoms. A S-*guessing *$\mathcal{G}$ is a Boolean assignment to members of S. We also view $\mathcal{G}$ as the set $\{\varphi \mid \varphi \in S$ and $\mathcal{G}(\varphi)$ is assigned to true$\} \cup \{\neg\varphi \mid \varphi \in S$ and $\mathcal{G}(\varphi)$ is assigned to false$\}$.*

Indeed, guessing must take into account rigid constants. Since $\mathcal{T}$ is locally finite compatible, there must exist a Σ_r-theory T_r such that $T_r \subseteq T$ is effectively locally finite. So, given a finite subset $\underline{c}_0$ of $\underline{c}$, it is possible to compute a finite set S of ground $\Sigma_r^{\underline{c}_0}$-atoms which are representative modulo T-equivalence: for this choice of S, an S-guessing is called a *rigid $\underline{c}_0$-guessing*. Now, let $\tilde{S}$ be any finite set of $\Sigma^{\underline{a},\underline{c}}$-atoms and let $\mathcal{G}$ be a rigid $\underline{c}_0$-guessing: an $\tilde{S}$-guessing $\tilde{\mathcal{G}}$ is *$\mathcal{G}$-compatible* iff $\mathcal{G} \cup \tilde{\mathcal{G}}$ is T-satisfiable. The set of $\mathcal{G}$-compatible $\tilde{S}$-guessing is denoted by $C(\tilde{S}, \mathcal{G})$. Theorem 3.2 is an immediate consequence of the fact that PLTL-satisfiability is decidable and the following Proposition.

Proposition 3.1. *Let $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c}\rangle$ be a locally finite compatible LTL-theory. Let $\mathcal{L}$ be a set of propositional letters and $[\![\cdot]\!]$ be a PLTL-abstraction function mapping ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentences into propositional $\mathcal{L}$-formulae. A ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence φ is satisfiable in an LTL($\Sigma^{\underline{a},\underline{c}}$)-structure $\mathcal{M}$ appropriate for $\mathcal{T}$ iff there exists a rigid $\underline{c}_0$-guessing $\mathcal{G}$ such that the propositional formula*

$$[\![\varphi]\!] \wedge \Box \bigwedge_{\psi \in \mathcal{G}} [\![\psi]\!] \wedge \Box \Big(\bigvee_{\tilde{\mathcal{G}} \in C(At(\varphi), \mathcal{G})} \bigwedge_{\psi \in \tilde{\mathcal{G}}} [\![\psi]\!] \Big) \tag{1}$$

is satisfiable in a PLTL-Kripke model (here $\underline{c}_0 \subseteq \underline{c}$ is the set of system parameters occurring in φ and $At(\varphi)$ is the set of $\Sigma^{\underline{a},\underline{c}}$-atoms occurring in φ).

To prove this Proposition, we use Lemma 2.1 with $I := \mathbb{N}$, $T_i := T$ (symbols from $\Sigma \setminus \Sigma_r$ are disjointly renamed when building the signature Σ_i for the i-th copy of T). The Σ_i-structures $\mathcal{M}_i$ required to build a temporal model are obtained by signature restrictions from the model of $\bigcup T_i$ which is provided by Lemma 2.1.

The main advantage of the *eager reduction algorithm* suggested by Proposition 3.1 is that decision procedures for the constraint satisfiability problem of the underlying locally finite theory and PLTL-decision procedures (based on tableau, automata, or temporal resolution) can be used 'off-the-shelf'. Its main drawback is that the resulting PLTL-satisfiability problem may be quite large.

A Lazy Tableau Procedure. Avoiding the up-front generation of possibly very large PLTL-formulae should allow one to scale up more smoothly. The price to pay is a finer grain integration between the constraint reasoner for the underlying locally finite theory and the PLTL satisfiability solver.

A ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence is in *Negation Normal Form* (NNF) iff it is built up from LTL($\Sigma^{\underline{a},\underline{c}}$)-literals by using $\vee, \wedge, X, R, U$. It can be shown that every ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence is logically equivalent to one in NNF. If φ is a ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence in NNF, then the *closure* of φ is the set $cl(\varphi)$

containing: (i) all subformulae of φ and all negations of atoms occurring in φ; (ii) the formulae $X(\psi U \chi)$, where $\psi U \chi$ is a subformula of φ; (iii) the formulae $X(\psi R \chi)$, where $\psi R \chi$ is a subformula of φ and, most importantly, (iv) a *representative set (modulo T-equivalence) of $\Sigma_r^{\underline{c}_0}$-literals*, where $\underline{c}_0$ is the finite set of system parameters occurring in φ.

Definition 3.5. *Given a ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence φ in NNF, a* Hintikka set *for φ is a subset $H \subseteq cl(\varphi)$ such that: (i) H contains a maximal T-satisfiable set of literals from $cl(\varphi)$; (ii) if $\psi_1 \wedge \psi_2 \in H$, then $\psi_1, \psi_2 \in H$; (iii) if $\psi_1 \vee \psi_2 \in H$, then $\psi_1 \in H$ or $\psi_2 \in H$; (iv) if $\psi_1 U \psi_2 \in H$, then $\psi_2 \in H$ or ($\psi_1 \in H$ and $X(\psi_1 U \psi_2) \in H$); (v) if $\psi_1 R \psi_2 \in H$, then $\psi_1, \psi_2 \in H$ or $\psi_2, X(\psi_1 R \psi_2) \in H$.*

To design the lazy reduction procedure, we extend the tableaux-based approach to PLTL-satisfiability by lifting the definition of Hintikka sets to take into account ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentences in NNF.

Definition 3.6. *The* Hintikka graph $\mathcal{H}(\varphi)$ *of φ is the directed graph having as nodes the Hintikka sets for φ and as edges the pairs $H \to H'$ such that* (i) $H' \supseteq \{\psi \mid X\psi \in H\}$ *and* (ii) *H and H' contain the same ground $\Sigma_r^{\underline{c}_0}$-literals.*

A *strongly connected subgraph* (scs) of $\mathcal{H}(\varphi)$ is a set $\mathcal{C}$ of nodes of $\mathcal{H}(\varphi)$ such that for every $H, H' \in \mathcal{C}$ there is a (non-empty) $\mathcal{H}(\varphi)$-path from H to H' whose nodes belong to $\mathcal{C}$. An scs $\mathcal{C}$ is *fulfilling* [12] iff for every $\psi_1 U \psi_2 \in cl(\varphi)$ there is $H \in \mathcal{C}$ such that either $\psi_1 U \psi_2 \notin H$ or $\psi_2 \in H$. A node H in $\mathcal{H}(\varphi)$ is *initial* iff $\varphi \in H$.

Corollary 3.1. *A ground LTL($\Sigma^{\underline{a},\underline{c}}$)-formula φ in NNF is satisfiable in an LTL($\Sigma^{\underline{a},\underline{c}}$)-structure $\mathcal{M}$ appropriate for $\mathcal{T}$ iff there is an $\mathcal{H}(\varphi)$-path leading from an initial node into a fulfilling scs.*

This Corollary is a consequence of Proposition 3.1 and basic properties of Tableaux (see, e.g., Section 5.5 of [12]). When the set of representative $\Sigma_r^{\underline{c}_0}$-atoms has polynomial size, the decision procedure derived from Corollary 3.1 is in PSPACE (provided that the T-constraint satisfiability problem is in PSPACE too): the key to achieve this is to explore the Hintikka graph 'on-the-fly' by using well-known techniques of the PLTL literature without explicitly constructing it.

4 The Model-Checking Problem

Given two signatures Σ_r and Σ such that $\Sigma_r \subseteq \Sigma$, we define the *one-step signature* as $\Sigma \oplus_{\Sigma_r} \Sigma := ((\Sigma \setminus \Sigma_r) \uplus (\Sigma \setminus \Sigma_r)) \cup \Sigma_r$, where $\uplus$ denotes disjoint union. In order to build the one-step signature $\Sigma \oplus_{\Sigma_r} \Sigma$, we first consider two copies of the symbols in $\Sigma \setminus \Sigma_r$; the two copies of $r \in \Sigma \setminus \Sigma_r$ are denoted by r^0 and r^1, respectively. Notice that the symbols in Σ_r are not renamed. Also, arities in the one-step signature $\Sigma \oplus_{\Sigma_r} \Sigma$ are defined in the obvious way: the arities of the symbols in Σ_r are unchanged and if n is the arity of $r \in \Sigma \setminus \Sigma_r$, then n is the arity of both r^0 and r^1. The one-step signature $\Sigma \oplus_{\Sigma_r} \Sigma$ will be also written as $\bigoplus^2_{\Sigma_r} \Sigma$; similarly, we can define the n-step signature $\bigoplus^{n+1}_{\Sigma_r} \Sigma$ for

$n > 1$ (our notation for the copies of $(\Sigma \setminus \Sigma_r)$-symbols extends in the obvious way, that is we denote by $r^0, r^1, \ldots, r^n$ the $n+1$ copies of r).

Definition 4.1. *Given two signatures Σ_r and Σ such that $\Sigma_r \subseteq \Sigma$, two Σ-structures $\mathcal{M}_0 = \langle M, \mathcal{I}_0 \rangle$ and $\mathcal{M}_1 = \langle M, \mathcal{I}_1 \rangle$ whose Σ_r-reducts are the same, the* one-step $(\Sigma \oplus_{\Sigma_r} \Sigma)$-structure $\mathcal{M}_0 \oplus_{\Sigma_r} \mathcal{M}_1 = \langle M, \mathcal{I}_0 \oplus_{\Sigma_r} \mathcal{I}_1 \rangle$ *is defined as follows:*

- *for each function or predicate symbol $s \in \Sigma \setminus \Sigma_r$, $(\mathcal{I}_0 \oplus_{\Sigma_r} \mathcal{I}_1)(s^0) := \mathcal{I}_0(s)$ and $(\mathcal{I}_0 \oplus_{\Sigma_r} \mathcal{I}_1)(s^1) := \mathcal{I}_1(s)$;*
- *for each function or predicate symbol $r \in \Sigma_r$, $(\mathcal{I}_0 \oplus_{\Sigma_r} \mathcal{I}_1)(r) := \mathcal{I}_0(r)$.*

If φ is a Σ-formula, the $\Sigma \oplus_{\Sigma_r} \Sigma$ formulae φ^0, φ^1 are obtained from φ by replacing each symbol $r \in \Sigma \setminus \Sigma_r$ by r^0 and r^1, respectively. The one-step theory $T \oplus_{\Sigma_r} T$ is taken to be the combination of the theory T with a partially renamed copy of itself:

Definition 4.2. *Given two signatures Σ_r and Σ such that $\Sigma_r \subseteq \Sigma$, the $(\Sigma \oplus_{\Sigma_r} \Sigma)$-theory $T \oplus_{\Sigma_r} T$ is defined as $\{\varphi^0 \wedge \varphi^1 \mid \varphi \in T\}$.*

We will write $\bigoplus^2_{\Sigma_r} T$ instead of $T \oplus_{\Sigma_r} T$; the n-step theories $\bigoplus^{n+1}_{\Sigma_r} T$ (for $n > 1$) are similarly defined.

Let now $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ be an LTL-theory with *finitely* many parameters and system variables. A *transition relation* for the LTL-theory $\mathcal{T}$ is a $(\Sigma^{\underline{a},\underline{c}} \oplus_{\Sigma^{\underline{c}}_r} \Sigma^{\underline{a},\underline{c}})$-sentence δ: we write such formula as $\delta(\underline{a}^0, \underline{a}^1)$ to emphasize that it contains the two copies of the system variables $\underline{a}$ (on the other hand, the system parameters $\underline{c}$ are not duplicated and will never be displayed). An *initial state description* for the LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ is simply a $\Sigma^{\underline{a},\underline{c}}$-sentence $\iota(\underline{a})$ (again, the system parameters $\underline{c}$ will not be displayed).

Definition 4.3 (LTL-System Specification and Model-Checking). *An* LTL-system specification *is a LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ (with finitely many system variables and parameters) endowed with a transition relation $\delta(\underline{a}^0, \underline{a}^1)$ and with an initial state description $\iota(\underline{a})$. An LTL($\Sigma^{\underline{a},\underline{c}}$)-structure $\mathcal{M} = \{\mathcal{M}_n = (M, \mathcal{I}_n)\}_{n \in \mathbb{N}}$ is* a run *for such an LTL-system specification iff it is appropriate for $\mathcal{T}$ and moreover it obeys the initial state description ι and the transition δ, i.e. (1) $\mathcal{M}_0 \models \iota(\underline{a})$, and (2) $\mathcal{M}_n \oplus_{\Sigma^{\underline{c}}_r} \mathcal{M}_{n+1} \models \delta(\underline{a}^0, \underline{a}^1)$, for every $n \geq 0$. The* model-checking problem *for the system specification $(\mathcal{T}, \delta, \iota)$ is the following: given an LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence φ, decide whether there is a run $\mathcal{M}$ for $(\mathcal{T}, \delta, \iota)$ such that $\mathcal{M} \models \varphi$.*[1] *The* ground model-checking problem for $(\mathcal{T}, \delta, \iota)$ *is similarly defined for a ground φ.*

The (syntactic) *safety model-checking problem* is the model-checking problem for formulae of the form $\Diamond \upsilon$, where υ is a $\Sigma^{\underline{a},\underline{c}}$-sentence. Since υ is intended to describe the set of *unsafe* states, we say that the system specification $(\mathcal{T}, \delta, \iota)$ is *safe for* υ iff the model-checking problem for $\Diamond \upsilon$ has a negative solution. This implies that $\Box \neg \upsilon$ is true for all runs of $(\mathcal{T}, \delta, \iota)$.

[1] In the literature, the model-checking problem is the complement of ours, i.e. it is the problem of deciding whether a given sentence is true in all runs.

In the literature about model-checking (especially, for finite-state systems), it is usually assumed the seriality of the transition relation: every state of the system must have at least one successor state (see, e.g., [3] for more details).

Definition 4.4. *An LTL-system specification $(\mathcal{T}, \delta, \iota)$, based on the LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$, is said to be* serial *iff for every $\Sigma^{\underline{a},\underline{c}}$-structure $\mathcal{M}_0 = (M, \mathcal{I}_0)$ which is a model of T, there is another $\Sigma^{\underline{a},\underline{c}}$-structure $\mathcal{M}_1 = (M, \mathcal{I}_1)$ (still a model of T) such that $(\mathcal{M}_0)_{|\Sigma_r} = (\mathcal{M}_1)_{|\Sigma_r}$ and $\mathcal{M}_0 \oplus_{\Sigma^{\underline{c}}_r} \mathcal{M}_1 \models \delta(\underline{a}^0, \underline{a}^1)$.*

Although the notion of seriality defined above is non-effective, there exist simple and effective conditions ensuring it. For example, if the transition relation δ consists of the conjunction of (possibly guarded) assignments of the form $P(\underline{a}^0) \rightarrow a^1 = t^0(\underline{a}^0)$ where P is the condition under which the assignment is executed, then δ is serial (see, e.g., Example 4.1). The standard trick [3] of ensuring seriality by a 0-ary predicate describing error states works in our framework too.

Definition 4.5. *An LTL-system specification $(\mathcal{T}, \delta, \iota)$, based on the LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$, is* finite state *or* locally finite compatible *iff so is $\mathcal{T}$.*

Finite state system specifications are investigated by traditional symbolic model-checking methods [3]. Since we are interested in ground safety model-checking problems we assume Assumption 2 in Figure 1, besides Assumption 1. Unfortunately, these two hypotheses are not sufficient to guarantee the decidability, even in the case the underlying LTL-theory is totally rigid. In fact, it is possible to reduce the ground safety model-checking problem to the the reachability problem of Minsky machines, which is known to be undecidable (see, e.g., [9]).

Fortunately, the safety model-checking problem is decidable for locally finite compatible LTL-system specifications. In the rest of this Section, let $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ be a locally finite compatible LTL-theory, $(\mathcal{T}, \delta, \iota)$ be an LTL-system specification based on $\mathcal{T}$, and $\upsilon(\underline{a})$ be a ground $\Sigma^{\underline{a},\underline{c}}$-sentence. The related safety model-checking problem amounts to checking whether there exists a run $\mathcal{M} = \{\mathcal{M}_n\}_{n \in \mathbb{N}}$ for $(\mathcal{T}, \delta, \iota)$ such that $\mathcal{M} \models_n \upsilon(\underline{a})$ for some $n \geq 0$: if this is the case, we say that the system is *unsafe* since there is a *bad run of length n*.

We can ignore bad runs of length $n = 0$, because the existence of such runs can be preliminarily decided by checking the ground sentence $\iota(\underline{a}) \wedge \upsilon(\underline{a})$ for T-satisfiability. So, for $n \geq 1$, taking into account the seriality of the transition, a bad run of length $n + 1$ exists iff the ground $(\bigoplus^{n+2}_{\Sigma^{\underline{c}}_r} \Sigma^{\underline{a},\underline{c}})$-sentence

$$\iota^0(\underline{a}^0) \wedge \delta^{0,1}(\underline{a}^0, \underline{a}^1) \wedge \delta^{1,2}(\underline{a}^1, \underline{a}^2) \wedge \cdots \wedge \delta^{n,n+1}(\underline{a}^n, \underline{a}^{n+1}) \wedge \upsilon^{n+1}(\underline{a}^{n+1}) \quad (2)$$

is $\bigoplus^{n+2}_{\Sigma^{\underline{c}}_r} T$-satisfiable, where $\iota^0(\underline{a}^0)$ is obtained by replacing each flexible symbol $r \in \Sigma \setminus \Sigma_r$ with r^0 in $\iota(\underline{a})$ (the system variables $\underline{a}$ are similarly renamed as $\underline{a}^0$); $\delta^{i,i+1}(\underline{a}^i, \underline{a}^{i+1})$ is obtained by replacing in $\delta(\underline{a}^0, \underline{a}^1)$ the copy r^0 and r^1 of each flexible symbol $r \in \Sigma \setminus \Sigma_r$ with r^i and r^{i+1} respectively (the two copies $\underline{a}^0, \underline{a}^1$ of the system variables $\underline{a}$ are similarly renamed as $\underline{a}^i, \underline{a}^{i+1}$); and $\upsilon^{n+1}(\underline{a}^{n+1})$ is obtained by replacing each flexible symbol $r \in \Sigma \setminus \Sigma_r$ with r^{n+1} in $\upsilon(\underline{a})$ (the system variables $\underline{a}$ are similarly renamed as $\underline{a}^{n+1}$). For the sake of simplicity,

we will write formula (2) by omitting the superscripts of ι, δ, and υ (but we maintain those of the system variables $\underline{a}$).

Now, for a given $n+1$, an iterated application of the main combination result in [8] and the fact that T_0-compatibility is a modular property (see again [8]) yield the decidability of the satisfiability of formula (2). Unfortunately, this is not sufficient to solve the model-checking problem for LTL-system specifications since the length of a bad run is not known apriori. To solve this problem, we reduce the existence of a satisfiable formula of the form (2) to a reachability problem in a safety graph (see Definition 4.7 below).

Definition 4.6. *A ground $(\Sigma^{\underline{a},\underline{c}} \oplus_{\Sigma_r^{\underline{c}}} \Sigma^{\underline{a},\underline{c}})$-sentence δ is said to be* purely left *(*purely right*) iff for each symbol $r \in \Sigma \setminus \Sigma_r$, we have that r^1 (r^0, resp.) does not occur in δ. We say that δ is* pure *iff it is a Boolean combination of purely left or purely right atoms.*

Given a formula $\delta(\underline{a}^0, \underline{a}^1)$, it is always possible (see, e.g., [8]) to obtain an equisatisfiable formula $\tilde{\delta}(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ which is pure by introducing "fresh" constants that we call $\underline{d}^0$ (i.e., $\underline{d}^0 \cap (\underline{a}^0 \cup \underline{a}^1) = \emptyset$) to name "impure" subterms. Usually, $\tilde{\delta}$ is called the purification of δ. Let $A_1, \ldots, A_k$ be the atoms occurring in $\tilde{\delta}(\underline{a}^0, \underline{a}^1, \underline{d}^0)$. A *$\tilde{\delta}$-assignment* is a conjunction $B_1 \wedge \cdots \wedge B_k$ (where B_i is either A_i or $\neg A_i$, for $1 \leq i \leq k$), such that $B_1 \wedge \cdots \wedge B_k \rightarrow \tilde{\delta}$ is a propositional tautology. Since $\tilde{\delta}$ is pure, we can represent a $\tilde{\delta}$-assignment V in the form $V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0)$, where V^l is a purely left conjunction of literals and V^r is a purely right conjunction of literals. As a consequence, a bad run of length $n+1$ exists iff the ground sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^{n} (V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V_{i+1}^r(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge \upsilon(\underline{a}^{n+1}) \tag{3}$$

is $\bigoplus_{\Sigma_r}^{n+2} T$-satisfiable, where $\underline{d}^0, \underline{d}^1, \ldots, \underline{d}^n$ are $n+1$ copies of the fresh constants $\underline{d}^0$ and $V_1, \ldots, V_{n+1}$ range over the set of $\tilde{\delta}$-assignments. Since T_r is locally finite, there are finitely many ground $\Sigma_r^{\underline{c},\underline{a}^0,\underline{a}^1,\underline{d}^0}$-literals which are representative (modulo T_r-equivalence) of all $\Sigma_r^{\underline{c},\underline{a}^0,\underline{a}^1,\underline{d}^0}$-literals. A guessing $G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ (cf. Definition 3.4) over such literals will be called a *transition Σ_r-guessing.*

Definition 4.7. *The* safety graph *associated to the LTL-system specification $(\mathcal{T}, \delta, \iota)$ based on the locally finite compatible LTL-theory $\mathcal{T}$ is the directed graph defined as follows:*

- *the nodes are the pairs (V, G) where V is a $\tilde{\delta}$-assignment and G is a transition Σ_r-guessing;*
- *there is an edge $(V, G) \rightarrow (W, H)$ iff the ground sentence*

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1) \tag{4}$$

is T-satisfiable.

The initial nodes *of the safety graph are the nodes* (V, G) *such that* $\iota(\underline{a}^0) \wedge V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ *is* T*-satisfiable; the* terminal nodes *of the safety graph are the nodes* (V, G) *such that* $V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge \upsilon(\underline{a}^1) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ *is* T*-satisfiable.*

The decision procedure for safety model-checking relies on the following fact.

Proposition 4.1. *The system is unsafe iff either* $\iota(\underline{a}) \wedge \upsilon(\underline{a})$ *is* T*-satisfiable or there is a path in the safety graph from an initial to a terminal node.*

The idea behind the proof is the following: by contradiction, assume there is a path from an initial to a terminal node and the system is safe. Repeatedly, compute Σ_r-ground interpolants of (3) between T and $\bigoplus^j_{\Sigma_r} T$, for $j = n + 1, \ldots, 1$ (an argument based on Lemma 2.1 guarantees they exist). This yields the T-unsatisfiability of the final node (formula) in the graph; a contradiction.

Theorem 4.1. *The ground safety model-checking problem for a locally finite compatible LTL-system specification is decidable.*

For complexity, the same remarks after Corollary 3.1 apply here too.

Example 4.1 ([18]). Consider a water level controller such that (i) changes in the water level by $in(\text{flow})/out(\text{flow})$ depend on the water level l and on the time instant; (ii) if $l \geq l_{\text{alarm}}$ at a given state (where l_{alarm} is a fixed value), then a valve is opened and, at the next observable instant, $l' = in(out(l))$; and (iii) if $l < l_{\text{alarm}}$ then the valve is closed and, at the next observable instant, $l' = in(l)$.

Let us now consider the LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ where l is the only system variable ($\underline{a} := \{l\}$) and there are no system parameters ($\underline{c} := \emptyset$); $\Sigma_r = \{l_{\text{alarm}}, l_{\text{overflow}}, <\}$, $l_{\text{alarm}}, l_{\text{overflow}}$ are two constant symbols and $<$ is a binary predicate symbol; $\Sigma := \Sigma_r \cup \{in, out\}$; T_r is the theory of dense linear orders without endpoints endowed with the additional axiom $l_{\text{alarm}} < l_{\text{overflow}}$; and

$$T := T_r \cup \left\{ \begin{array}{l} \forall x\, (x < l_{\text{alarm}} \rightarrow in(x) < l_{\text{overflow}}), \\ \forall x\, (x < l_{\text{overflow}} \rightarrow out(x) < l_{\text{alarm}}) \end{array} \right\}$$

It can be shown that the constraint satisfiability problem for T is decidable, T_r admits quantifier elimination, and T_r is effectively locally finite. From these, it follows that $\mathcal{T}$ is a locally finitely compatible LTL-theory. We consider now the LTL-system specification $(\mathcal{T}, \delta, \iota)$ where $\iota := l < l_{\text{alarm}}$ and

$$\delta := \big(l_{\text{alarm}} \leq l^0 \rightarrow l^1 = in^0(out^0(l^0))\big) \wedge \big(l^0 < l_{\text{alarm}} \rightarrow l^1 = in^0(l^0)\big).$$

Notice that δ is a purely left $(\Sigma^{\underline{a}} \oplus_{\Sigma_r} \Sigma^{\underline{a}})$-formula.

We consider the safety model-checking problem specified by the LTL-system above and whose unsafe states are described by $\upsilon := l_{\text{overflow}} < l$. Using the procedure suggested by Theorem 4.1 we can prove that the system is safe, i.e. that there is no run $\mathcal{M}$ for $(\mathcal{T}, \delta, \iota)$ such that $\mathcal{M} \models \Diamond \upsilon$. We can observe that the task in practice is not extremely hard computationally. It is sufficient to consider just 50 nodes (modulo T-equivalence) of the safety graph that are T-satisfiable (i.e. the nodes (V, G) such that $V \wedge G$ is T-satisfiable). Also, instead

of considering all the edges of the safety graph, it is sufficient to build just the paths starting from the initial nodes or ending in a terminal node (namely to apply a forward/backward search strategy). In the first case, only 26 nodes of the safety graph are reachable from an initial node. In the latter, just 12 nodes are backward reachable from a terminal node. Hence the the problem is clearly amenable to automatic analysis by combining a decision procedure for T with a SAT-solver which is able to enumerate the $\tilde{\delta}$-assignments needed to traverse the safety graph.

Example 4.2. The aim of this example is to use our techniques to analyze the safety of the well-known Lamport's mutual exclusion "Bakery" algorithm. If the number of involved processes is unknown, we can build for the problem an appropriate LTL-system specification $\mathcal{T}$ which violates our assumptions in Figure 1 because it has universal (instead of ground) transition relation and initial state description. More in detail, we use a language with two sorts, one for the individuals (i.e the involved processes), the other for the tickets. The tickets are ruled by the theory of dense total order with named distinct (rigid) endpoints 0 and 1; moreover, a (flexible) function for the ticket assignment is constrained by an "almost-injectivity" axiom (i.e., people cannot have the same ticket with the exception of the ticket 1 that means being out of the queue). Finally, a flexible constant models the current ticket bound and a flexible predicate captures the served individuals. The transition says the following: (i) the values of the current ticket bound are strictly increasing; (ii) every individual is removed from the queue immediately after being served; (iii) if an individual is in the queue and is not served, then its ticket is preserved; (iv) if an individual is not the first in the queue, it cannot be served; (v) if an individual is not in the queue, either remains out of the queue or takes a ticket lying in the interval between two consecutive values of the current ticket bound (without being immediately served). The initial state description says that no one is in the queue and the current ticket bound is set to 0, whereas the unsafe states are the ones in which at least two people are served at the same time.

By Skolemization and instantiation, we produce out of $\mathcal{T}$ a locally finite compatible LTL-system specification $\mathcal{T}'$ which is safe iff $\mathcal{T}$ is safe. Safety of $\mathcal{T}'$ can then be easily checked through our techniques (see [9] for details). We point out that the features of $\mathcal{T}$ that make the whole construction to work are *purely syntactic* in nature: they basically consist of the finiteness of the set of terms of certain sorts in the skolemized Herbrand universe.

5 Discussion

The undecidability of quantified modal logics over a discrete flow was discovered by D. Scott already in the sixties. Recent works isolated quite interesting fragments of quantified LTL which are computationally better behaved (see [7] for a survey). However such fragments are often insufficient for verification; in this respect, a more promising restriction is to prohibit the interplay between quantifiers and temporal operators [12]. In this paper, we have taken a similar approach

by enriching the extensional part of the language so to be able to model infinite data structures manipulated by systems. This lead us to consider satisfiability of quantifier-free LTL formulae built up from a first-order signature Σ and models with constant domain consisting of a sequence $\{\mathcal{M}_i\}_i$ of first-order models of a Σ-theory T. Furthermore, symbols in Σ and free variables were divided into two groups. The former are interpreted rigidly whereas the latter flexibly in the $\mathcal{M}_i$'s. This approach was already taken in the seminal paper [15] by Plaisted, who established a decidability result when the quantifier-free fragment of T is decidable and the flexible symbols are considered as free symbols by the theory T. By using recent techniques and results from the combination literature, we were able to attack the problem in its full generality and derive both the undecidability in the unrestricted case and the decidability under the 'combinability' hypotheses for T of [8]. Such hypotheses, besides decidability of the universal first-order fragment, were compatibility over a locally finite subtheory in the rigid subsignature (local finiteness may be replaced by the weaker requirement of Noetherianity, but this result has been omitted in the paper for lack of space and can be found in [9]).

In the second part of the paper we considered model-checking problems under the same 'combinability' hypotheses on T. We were able to derive positive decidability results for the safety properties and we plan to extend our results to different kinds of properties (such as liveness) as well as to full LTL model-checking. Our framework generalizes finite state model-checking in two respects. First, the rigid symbols are constrained by a locally finite theory, not just by an enumerated datatype theory. Second, we do not impose limitations on the flexible symbols, whose interpretation is only constrained by the axioms of T.

The literature on infinite state model-checking is extremely vast (see [20,16,2] to name but a few approaches). For lack of space, we consider works which are closely related to ours. The paper [5] extensively reviews constrained LTL, which can be the basis for model checking of infinite state systems but it does not allow for flexible symbols (apart from system variables). Furthermore, fixed purely relational structures play there the same role of the models of the theory T in our approach. However, [5] is not limited to safety properties. If our results can be extended beyond safety (as it seems likely), *some* of the results in [5] could be seen as specializations of our work to totally rigid system specifications. Other results and techniques from [5] (and also from the recent [6]) should be taken into account for integration in our framework so to be able to handle richer underlying theories such as Linear Arithmetic.

An integration of classic tableaux and automated deduction techniques is presented in [17,11]. While using a similar approach, [17] only provides a uniform framework for such an integration with no guarantee of full automation, whereas [11] focuses on the decidability of the model-checking problem of particular classes of parametrized systems. Both works do not use combination techniques. The approach in [4] proposes the reduction of bounded model-checking problems to SMT problems. Theorem 4.1 identifies precise conditions under which our reduction yields a decision procedure: our safety graph is not just

an approximation of the set of reachable states. With [4], we share the focus on using SMT solvers, which is also a common feature of the "abstract-check-refine" approach to infinite-state model-checking (see the seminal work in [10]). However, our work is foundational whereas abstract-check-refine techniques focus more on practical usability.

References

1. M. P. Bonacina, S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Decidability and undecidability results for Nelson-Oppen and rewrite-based decision procedures. In U. Furbach and N. Shankar, editors, *Proc. of IJCAR 2006*, volume 4130 of *LNCS (LNAI)*, Heidelberg, 2006. Springer.
2. O. Burkart, D. Caucal, F. Moller, and B. Steffen. Verification of infinite state structures. In *Handbook of Process Algebras*. 2001.
3. E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. MIT Press, Cambridge, 2000.
4. L. de Moura, H. Rueß, and M. Sorea. Lazy theorem proving for bounded model checking over infinite domains. In A. Voronkov, editor, *Proc. of CADE 2002*, volume 2392 of *LNCS (LNAI)*, Heidelberg, 2002.
5. S. Demri. Linear-time temporal logics with Presburger constraints: An overview. *Journal of Applied Non-Classical Logics*, 16(3–4), 2006.
6. S. Demri, A. Finkel, V. Goranko, and G. van Drimmelen. Towards a model-checker for counter systems. In S. Graf and S. Zhang, editors, *Proc. of ATVA 2006*, volume 4218 of *LNCS*, Heidelberg, 2006.
7. D. M. Gabbay, A. Kurucz, F. Wolter, and M. Zakharyaschev. *Many-Dimensional Modal Logics: Theory and Applications*. North-Holland Publishing Co., 2003.
8. S. Ghilardi. Model theoretic methods in combined constraint satisfiability. *Journal of Automated Reasoning*, 33(3-4), 2004.
9. S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Combination methods for satisfiability and model-checking of infinite-state systems. Technical Report RI313-07, Università degli Studi di Milano, 2007. Available at `http://homes.dsi.unimi.it/~zucchell/publications/techreport/GhiNiRaZu-RI313-07.pdf`.
10. S. Graf and H. Saïdi. Construction of abstract state graphs with PVS. In O. Grumberg, editor, *Proc. of CAV 1997*, volume 1254 of *LNCS*, Heidelberg, 1997. Springer.
11. M. Maidl. A unifying model checking approach for safety properties of parameterized systems. In G. Berry, H. Comon, and A. Finkel, editors, *Proc. of CAV 2001*, volume 2102 of *LNCS*, Heidelberg, 2001. Springer.
12. Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer-Verlag, 1995.
13. M. L. Minsky. Recursive unsolvability of Post's problem of "tag" and other topics in the theory of Turing machines. *Annals of Mathematics*, 74(3), 1961.
14. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Transaction on Programming Languages and Systems*, 1(2), 1979.
15. D. A. Plaisted. A decision procedure for combination of propositional temporal logic and other specialized theories. *Journal of Automated Reasoning*, 2(2), 1986.
16. A. Pnueli, S. Ruath, and L. D. Zuck. Automatic deductive verification with invisible invariants. In T. Margaria and W. Yi, editors, *Proc. of TACAS 2001*, volume 2031 of *LNCS*, Heidelberg, 2001.

17. H. B. Sipma, T. E. Uribe, and Z. Manna. Deductive model checking. *Formal Methods in System Design*, 15(1), 1999.
18. V. Sofronie-Stokkermans. Interpolation in local theory extensions. In U. Furbach and N. Shankar, editors, *Proc. of IJCAR 2006*, volume 4130 of *LNCS (LNAI)*, Heidelberg, 2006.
19. C. Tinelli and M. T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In *Proc. of FroCoS 1996*, 1996.
20. M. Y. Vardi. Verification of concurrent programs: the automata-theoretic framework. *Annals of Pure and Applied Logic*, 51(1–2), 1991.

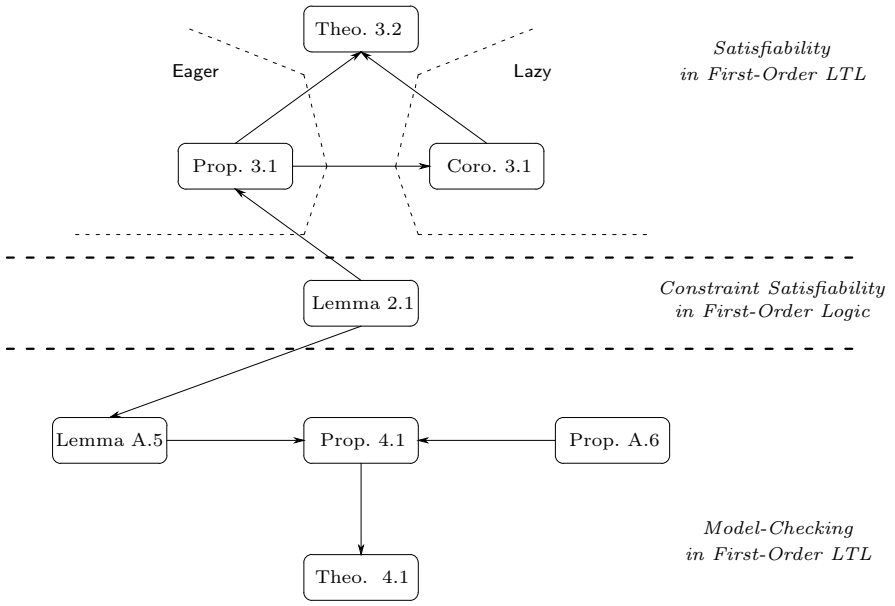

Fig. 2. Some of the conceptual dependencies among theorems and lemmas

A Proofs

Here we include the proofs of the main results (cf. Appendix A.3). For formally stating them, we recall some basic facts in model theory (cf. Appendix A.1), we state some properties culminating into the proof of our key technical Lemma 2.1, and finally we introduce two more results (ground Σ_r-interpolation and modularity of T_r-compatibility) needed for the decidability of safety model-checking (cf. Appendix A.2).

Figure 2 gives a rough idea of the dependencies among selected statements of the paper.

A.1 Basic Facts in Model Theory

We first recall some more background notions. Given a Σ-structure $\mathcal{M} = (M, \mathcal{I})$ and a subset $C \subseteq M$, the substructure of $\mathcal{M}$ generated by C is the substructure obtained from $\mathcal{M}$ by restricting $\mathcal{I}$ to the subset $\{t^{\mathcal{M}}(\underline{c}) \mid \underline{c} \subseteq C$ and $t(\underline{x})$ is a Σ-term$\}$ (here $t^{\mathcal{M}}$ is the function interpreting the term t in $\mathcal{M}$). In case this substructure coincides with $\mathcal{M}$, we say that C is a set of generators for $\mathcal{M}$.

If C is a set of generators for $\mathcal{M}$, the *diagram* $\Delta(\mathcal{M})$ of $\mathcal{M}$ (w.r.t. Σ, C) consists of all ground Σ^C-literals that hold in $\mathcal{M}$; analogously, the *elementary diagram* $\Delta^e(\mathcal{M})$ of $\mathcal{M}$ (w.r.t. Σ, C) consists of all ground Σ^C-sentences that hold in $\mathcal{M}$ (often C is not specified at all, in these cases it is assumed to coincide with the whole carrier set of $\mathcal{M}$).

Diagrams (in combination with the compactness of the logical consequence relation) will be repeatedly used. A typical use is the following. Suppose that we want to embed $\mathcal{M}$ into a model of a theory T, then it is sufficient to check that $T \cup \Delta(\mathcal{M})$ is consistent. This argument is justified by Robinson's Diagram Lemma A.1 relating embeddings and diagrams.

Lemma A.1 (Robinson's Diagram Lemma). *Let $\mathcal{M}$ be a Σ-structure generated by a set C, and let $\mathcal{N}$ be another Σ-structure; then $\mathcal{M}$ can be embedded (resp. elementarily embedded) into $\mathcal{N}$ iff $\mathcal{N}$ can be expanded to a Σ^C-model of the diagram $\Delta(\mathcal{M})$ (resp. of the elementary diagram $\Delta^e(\mathcal{M})$) of $\mathcal{M}$ w.r.t. Σ, C.*

The technique used for proving Lemma A.1 is simple, we sketch it. If we have an expansion of $\mathcal{N}$ to a Σ^C-structure (to be called $\mathcal{N}$ again for simplicity), then, since every element of the support of $\mathcal{M}$ is of the form $t^{\mathcal{M}}(\underline{c})$ for some $\underline{c} \subseteq C$, we can define the embedding μ by putting $\mu(t^{\mathcal{M}}(\underline{c})) := t^{\mathcal{N}}(\underline{c}^{\mathcal{N}})$: this is well-defined and it is an embedding precisely because $\mathcal{N} \models \Delta(\mathcal{M})$. Conversely, if we have the embedding μ, then we can get the desired expansion by taking $c^{\mathcal{N}} := \mu(c)$ for all $c \in C$.

Since a surjective embedding is just an isomorphism, the argument just sketched proves also the following fact.

Lemma A.2. *If two Σ-structures $\mathcal{M}$, $\mathcal{N}$ are both generated by a set C and if one of them, say $\mathcal{N}$, satisfies the diagram of the other (w.r.t. Σ, C), then the two structures are Σ^C-isomorphic.*

The next result is also part of basic classical model theory: a proof of it can be easily deduced from Craig's Interpolation Theorem (alternatively, a direct proof using a double chain argument is possible, see [22], pp. 141-142). To formally state the Lemma, we need to introduce a particular class of theories. A Σ-theory T is *complete* iff for every Σ-sentence φ, either φ or $\neg\varphi$ is a logical consequence of T

Theorem A.1 (Robinson's Joint Consistency Theorem). *Let H_1, H_2 be, respectively, consistent Θ_1, Θ_2-theories and let Θ_0 be the signature $\Theta_1 \cap \Theta_2$. Suppose that there is a complete Θ_0-theory H_0 such that $H_0 \subseteq H_1$ and $H_0 \subseteq H_2$; then $H_1 \cup H_2$ is a consistent $\Theta_1 \cup \Theta_2$-theory.*

Ground formulae are invariant under embeddings in the following sense.

Lemma A.3. *Let $\mathcal{M} = (M, \mathcal{I})$ be a Σ-structure that can be embedded into another Σ-structure $\mathcal{N}$. For all ground Σ^M-sentences φ, we have that*

$$\mathcal{M} \models \varphi \qquad \Leftrightarrow \qquad \mathcal{N} \models \varphi,$$

where $\mathcal{N}$ is extended to a Σ^M-structure by interpreting every $a \in M$ by its image under the embedding.

The next Lemma states the well-known property (called submodel-completeness) of theories enjoying quantifier-elimination.

Lemma A.4. *Suppose that $T^\star$ is a Σ_r-theory enjoying quantifier elimination and that Δ is a diagram of a substructure $\mathcal{R} = (R, \mathcal{J})$ of a model $\mathcal{M}$ of $T^\star$; then the Σ^R-theory $T^\star \cup \Delta$ is complete.*

Proof. By Robinson's Diagram Lemma A.1, the models of $T^\star \cup \Delta$ are the models of $T^\star$ endowed with a Σ_r-embedding from $\mathcal{R}$. One such model is $\mathcal{M}$; we show that any other model $\mathcal{M}'$ satisfies the same Σ^R-sentences as $\mathcal{M}$ (we assume without loss of generality the Σ_r-embedding from $\mathcal{R}$ into $\mathcal{M}'$ to be an inclusion). Pick an arbitrary Σ^R-sentence $\varphi(\underline{c})$ (where the $\underline{c}$ are parameters from the set of generators of $\mathcal{R}$ used in order to build Δ): this sentence is equivalent, modulo $T^\star$, to a ground Σ^R-sentence $\varphi^\star(\underline{c})$. Since truth of ground sentences is preserved by substructures (see Lemma A.3), the following chain of equivalences

$$\mathcal{M}' \models \varphi(\underline{c}) \Leftrightarrow \mathcal{M}' \models \varphi^\star(\underline{c}) \Leftrightarrow \mathcal{R} \models \varphi^\star(\underline{c}) \Leftrightarrow \mathcal{M} \models \varphi^\star(\underline{c}) \Leftrightarrow \mathcal{M} \models \varphi(\underline{c}),$$

proves our claim.

A.2 Structure amalgamations, Interpolation, Modularity

We prove now an important technical ingredient for our results, namely Lemma 2.1 (it is an extension of Lemma 9.4 in [8]).

Lemma 2.1. *Let $\Sigma_i^{\underline{c},\underline{a}_i}$ (for $i \in I$) be signatures (expanded with free constants $\underline{c}, \underline{a}_i$), whose pairwise intersections are all equal to a certain signature $\Sigma_r^{\underline{c}}$ (that is, we have $\Sigma_i^{\underline{c},\underline{a}_i} \cap \Sigma_j^{\underline{c},\underline{a}_j} = \Sigma_r^{\underline{c}}$ for all distinct $i, j \in I$). Suppose we are also given Σ_i-theories T_i which are all T_r-compatible, where $T_r \subseteq \bigcap_i T_i$ is a universal Σ_r-theory; let finally $\{\mathcal{N}_i = (N_i, \mathcal{I}_i)\}_{i \in I}$ be a sequence of $\Sigma_i^{\underline{c},\underline{a}_i}$-structures which are models of T_i and satisfy the same $\Sigma_r^{\underline{c}}$-atoms. Under these hypotheses, there exist a $\bigcup_i(\Sigma_i^{\underline{c},\underline{a}_i})$-structure $\mathcal{M} \models \bigcup_i T_i$ such that for each i, $\mathcal{N}_i$ has a $\Sigma_i^{\underline{c},\underline{a}_i}$-embedding into $\mathcal{M}$.*

Proof. By Robinson's Diagram Lemma A.1 and Lemma A.2 (and up to a partial renaming of the support sets), the fact that the $\mathcal{N}_i$ satisfy the same $\Sigma_r^{\underline{c}}$-atoms is another way of saying that they share the same $\Sigma_r^{\underline{c}}$-substructure generated by the $\underline{c}$ (let us call $\mathcal{R} = (R, \mathcal{J})$ this substructure); by T_r-compatibility, we may also freely assume that $\mathcal{N}_i \models T_i \cup T_r^\star$. Notice also that, by Lemma A.4 above, the theory $T_r^\star \cup \Delta$ is complete, where Δ is the diagram of $\mathcal{R}$ as a Σ_r-structure.

Again by Robinson's Diagram Lemma, we only need to show that the union of the elementary diagrams $\Delta_i^e(\mathcal{N}_i)$ is consistent:[2] here $\Delta_i^e(\mathcal{N}_i)$ is the elementary diagram of $\mathcal{N}_i$ as a $\Sigma_i^{\underline{c},\underline{a}_i}$-structure.

By compactness, we can freely assume that the index set I is finite, let it be $\{1, \ldots, k\}$ and let us argue by induction on k. The case $k = 1$ is trivial. For $k > 1$, we use Robinson's Joint Consistency Theorem as follows.

By renaming some elements in the supports if needed, we can freely suppose that the sets $N_1 \setminus R$ and $(N_2 \cup \cdots \cup N_k) \setminus R$ are disjoint. Given the hypotheses of the

[2] We need the elementary diagrams here, and not just diagrams, because we want the model being defined to be a model of $\bigcup_i T_i$.

Lemma on the signatures $\Sigma_i^{\underline{c},\underline{a}_i}$, we can apply the Joint Consistency Theorem to the theories $\Delta^e(\mathcal{N}_1)$ and $\Delta^e(\mathcal{N}_2) \cup \cdots \cup \Delta^e(\mathcal{N}_k)$: in fact, they are both consistent (the latter by induction) and they both contain the complete subtheory $T_r^\star \cup \Delta$ in the shared subsignature. This proves that $\Delta^e(\mathcal{N}_1) \cup \cdots \cup \Delta^e(\mathcal{N}_k)$ is consistent, as desired.

The following Lemma is a variant of Theorem 5.2 from [8] (but the proof below is different).

Lemma A.5. *Suppose that T_0, T_1, T_2 are $\Sigma_0, \Sigma_1, \Sigma_2$-theories (respectively) such that $\Sigma_0 = \Sigma_1 \cap \Sigma_2$, T_1 is T_0-compatible, and T_2 is T_0-compatible; if the ground $\Sigma_1^{\underline{a},\underline{b}}$-sentence $\psi_1(\underline{a},\underline{b})$ and the ground $\Sigma_2^{\underline{b},\underline{c}}$-sentence $\psi_2(\underline{b},\underline{c})$ (here the tuples of free constants $\underline{a},\underline{b},\underline{c}$ are pairwise disjoint) are such that $\psi_1(\underline{a},\underline{b}) \wedge \psi_2(\underline{b},\underline{c})$ is $T_1 \cup T_2$-inconsistent, then there is a ground $\Sigma_0^{\underline{b}}$-sentence $\psi_0(\underline{b})$ such that $T_1 \models \psi_1(\underline{a},\underline{b}) \rightarrow \psi_0(\underline{b})$ and $T_2 \models \psi_0(\underline{b}) \rightarrow \neg\psi_2(\underline{b},\underline{c})$.*

Proof. By compactness, it is sufficient to show that the set Ψ of ground $\Sigma_0^{\underline{b}}$-sentences $\psi_0(\underline{b})$ such that $T_1 \models \psi_1(\underline{a},\underline{b}) \rightarrow \psi_0(\underline{b})$ is not T_2-consistent with $\psi_2(\underline{b},\underline{c})$. Suppose it is, hence there is a T_2-model $\mathcal{M}_2$ of $\Psi \cup \{\psi_2(\underline{b},\underline{c})\}$. Let $\mathcal{R}$ be the Σ_0-substructure of $\mathcal{M}$ generated by the $\underline{b}$'s and let Δ be its diagram. We claim that Δ is T_1-consistent with $\psi_1(\underline{a},\underline{b})$: this is because, if $\psi_0(\underline{b})$ is a ground $\Sigma_0^{\underline{b}}$-sentence true in $\mathcal{R}$ and not consistent with $\psi_1(\underline{a},\underline{b})$, then $\neg\psi_0(\underline{b})$ would be in Ψ and hence would be true in $\mathcal{R}$, contradiction. Since Δ is T_1-consistent with $\psi_1(\underline{a},\underline{b})$, there is a model $\mathcal{M}_1$ of T_1 (having $\mathcal{R}$ as a substructure) in which $\psi_1(\underline{a},\underline{b})$ is true. By Lemma 2.1 (take $I = \{1,2\}$), the models $\mathcal{M}_1, \mathcal{M}_2$ embed, over $\mathcal{R}$, into a model $\mathcal{M}$ of $T_1 \cup T_2$; but then $\mathcal{M}$ is also a model of $\psi_1(\underline{a},\underline{b}) \wedge \psi_2(\underline{b},\underline{c})$ (because $\psi_1(\underline{a},\underline{b})$ and $\psi_2(\underline{b},\underline{c})$ are ground, see Lemma A.3), a contradiction.

We now prove the modularity of T_0-compatibility.

Lemma A.6. *If T_0, T_1, T_2 are $\Sigma_0, \Sigma_1, \Sigma_2$-theories (respectively) such that $\Sigma_0 = \Sigma_1 \cap \Sigma_2$, T_1 is T_0-compatible, and T_2 is T_0-compatible, then $T_1 \cup T_2$ is T_0-compatible too.*

Proof. This is Proposition 4.4 from [8]: we report the proof here. Take a model $\mathcal{M} = (M, \mathcal{I})$ of $T_1 \cup T_2$ and embeds its Σ_i-reducts into models $\mathcal{M}_i = (M_i, \mathcal{I}_i)$ of $T_i \cup T_0^\star$ $(i = 1, 2)$. We can freely suppose that the embeddings are inclusions and that we have $M = M_1 \cap M_2$ for supports. Now $T_0^\star \cup \Delta(\mathcal{M})$ is a complete theory by Lemma A.4 (here $\Delta(\mathcal{M})$ is the diagram of $\mathcal{M}$ as a Σ_0-structure), hence by Robinson's Joint Consistency Theorem A.1 there is a model $\mathcal{N} = (N, \mathcal{J})$ of $\Delta^e(\mathcal{M}_1) \cup \Delta^e(\mathcal{M}_2)$. It follows that $\mathcal{N}$ is a $(\Sigma_1 \cup \Sigma_2)^{M_1 \cup M_2}$-model of $T_1 \cup T_2 \cup T_0^\star$ and that there are Σ_i^M-embeddings $\mu_i : \mathcal{M}_i \longrightarrow \mathcal{N}$. In particular, for $b \in M$, we have $\mu_1(b) = b^{\mathcal{N}} = \mu_2(b)$; let us call μ the common restriction of μ_1 and μ_2 to M. We show that μ is a $(\Sigma_1 \cup \Sigma_2)$-embedding of $\mathcal{M}$ into $\mathcal{N}$. Observe in fact that for every n-ary Σ_i-function symbol f and for every n-tuple $\underline{b}$ of elements from the support of $\mathcal{M}$, we have[3]

$$\mu(f^{\mathcal{M}}(\underline{b})) = \mu_i(f^{\mathcal{M}_i}(\underline{b})) = f^{\mathcal{N}}(\mu_i(\underline{b})) = f^{\mathcal{N}}(\mu(\underline{b}));$$

[3] Here, if $\underline{b} = (b_1, \ldots, b_n)$, we write e.g. $\mu(\underline{b})$ for the tuple $(\mu(b_1), \ldots, \mu(b_n))$.

analogously, for every n-ary Σ_i-predicate symbol P, we have

$$\mathcal{M} \models P(\underline{b}) \text{ iff } \mathcal{M}_i \models P(\underline{b}) \text{ iff } \mathcal{N} \models P(\mu_i(\underline{b})) \text{ iff } \mathcal{N} \models P(\mu(\underline{b})).$$

This proves that $\mu : \mathcal{M} \longrightarrow \mathcal{N}$ is a $(\Sigma_1 \cup \Sigma_2)$-embedding.

A.3 Main results

We first prove our undecidability result.

Theorem 3.1. *There exists a totally flexible LTL-theory $\mathcal{T}$ whose ground satisfiability problem is undecidable.*

Proof. We must define a LTL-theory $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c} \rangle$ such that $\Sigma_r = \emptyset$, i.e. $\mathcal{T}$ is totally flexible, and the constraint satisfiability problem of T is decidable, according to Assumption 1.

To define a suitable T, the following two facts about combinations of theories are crucial.

(i) There exist theories T_1, T_2 whose constraint satisfiability problem is decidable, whose signatures Σ_1, Σ_2 are disjoint and such that the constraint satisfiability problem of $T_1 \cup T_2$ is undecidable (this is shown in [1]).
(ii) Let T be a Σ-theory whose constraint satisfiability problem is decidable and Σ' be a signature such that $\Sigma' \supseteq \Sigma$. If we consider T as a Σ'-theory, then the constraint satisfiability problems of T is still decidable (this is proved in, e.g., [23,24]).

Consider now theories T_1, T_2 as in (i) above and let us define a new Σ-theory T as follows:

$$\Sigma := \Sigma_1 \cup \Sigma_2 \cup \{P\} \text{ and } T := \{P \rightarrow \psi \mid \psi \in T_1\} \cup \{\neg P \rightarrow \psi \mid \psi \in T_2\},$$

where P is a fresh 0-ary predicate symbol (or, otherwise said, a fresh propositional letter). We claim that the constraint satisfiability problem for the Σ-theory T is decidable. In fact, given a $\Sigma_1 \cup \Sigma_2 \cup \{P\}$ constraint Γ, we first guess the truth value of P and add either P or $\neg P$ to Γ, accordingly. At this point, we are left with the problem of solving a constraint satisfiability problem of the $(\Sigma_1 \cup \Sigma_2 \cup \{P\})$-theory T_i for either $i = 1$ or $i = 2$. This is decidable by fact (ii) above: the constraint satisfiability problem of the Σ_i-theory T_i is decidable by assumption and the symbols from $\Sigma_j \cup \{P\}$ $(j \neq i)$ are free for T_i.

We now show that the ground satisfiability problem for $\mathcal{T}$ is undecidable by identifying a particular class of ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentences whose satisfiability cannot be decided. We assume that there are infinitely many system parameters (whereas the cardinality of the set of system variables is irrelevant). We claim that it is not possible to decide the $\mathcal{T}$-satisfiability of the following type of ground LTL($\Sigma^{\underline{c}}$)-sentences:

$$P \wedge \Gamma_1 \wedge X(\neg P \wedge \Gamma_2), \tag{5}$$

where Γ_i is a finite conjunction of $\Sigma_i^{\underline{c}}$-literals (for $i = 1, 2$) and the $\underline{c}$ are the free constants of the LTL-theory $\mathcal{T}$ (i.e. the rigid system parameters). In fact, if (5) is satisfiable (in the sense of Definition 3.1) then it is easy to build a model (in first-order semantics) for $T_1 \cup T_2$ satisfying $\Gamma_1 \cup \Gamma_2$, and also the converse holds. Thus the satisfiability of the sentences of the kind described in (5) is reduced to the satisfiability w.r.t. $T_1 \cup T_2$ of the arbitrary constraint $\Gamma_1 \cup \Gamma_2$: this is undecidable by fact (i) above (notice that the satisfiability of pure constraints, like $\Gamma_1 \cup \Gamma_2$ is equivalent to satisfiability of arbitrary $(\Sigma_1 \cup \Sigma_2)$-constraints, because every constraint is equisatisfiable with an effectively built pure constraint, see e.g. [21],[8]).

The following straightforward Lemma explains why PLTL-abstractions (cf. Definition 3.3) are relevant for satisfiability checking of LTL($\Sigma^{\underline{a}}$)-sentences.

Lemma A.7. *Let $\mathcal{L}$ be a set of propositional letters, Σ be a signature, $\underline{a}$ be a set of free constants, and $[\![\cdot]\!]$ be a PLTL-abstraction function mapping ground LTL($\Sigma^{\underline{a}}$)-sentences into propositional $\mathcal{L}$-formulae. Suppose we are given a ground LTL($\Sigma^{\underline{a}}$)-sentence φ, a Kripke model V for $\mathcal{L}$ and an LTL($\Sigma^{\underline{a}}$)-structure $\mathcal{M} = \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ such that for every $t \in \mathbb{N}$ and for every $\Sigma^{\underline{a}}$-ground atom ψ occurring in φ we have*

$$\mathcal{M}_t \models \psi \qquad \textit{iff} \qquad V \models_t [\![\psi]\!].$$

Then we have also

$$\mathcal{M} \models_t \varphi \qquad \textit{iff} \qquad V \models_t [\![\varphi]\!],$$

for every $t \in \mathbb{N}$.

The next Proposition immediately yields the decidability of ground satisfiability for locally finite compatible LTL-theories (by an eager reduction to PLTL).

Proposition 3.1. *Let $\mathcal{T} = \langle \Sigma, T, \Sigma_r, \underline{a}, \underline{c}\rangle$ be a locally finite and compatible LTL-theory. Let $\mathcal{L}$ be a set of propositional letters and $[\![\cdot]\!]$ be a PLTL-abstraction function mapping ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentences into propositional $\mathcal{L}$-formulae. A ground LTL($\Sigma^{\underline{a},\underline{c}}$)-sentence φ is satisfiable in an LTL($\Sigma^{\underline{a},\underline{c}}$)-structure $\mathcal{M}$ appropriate for $\mathcal{T}$ iff there exists a rigid $\underline{c}_0$-guessing $\mathcal{G}$ such that the propositional formula*

$$[\![\varphi]\!] \wedge \Box \bigwedge_{\psi\in\mathcal{G}} [\![\psi]\!] \wedge \Box \Big(\bigvee_{\tilde{\mathcal{G}}\in C(At(\varphi),\mathcal{G})} \bigwedge_{\psi\in\tilde{\mathcal{G}}} [\![\psi]\!] \Big) \tag{1}$$

is satisfiable in a PLTL-Kripke model (here $\underline{c}_0 \subseteq \underline{c}$ is the set of system parameters occurring in φ and $At(\varphi)$ is the set of $\Sigma^{\underline{a},\underline{c}}$-atoms occurring in φ).

Proof. The 'only if' is immediate from Lemma A.7. The converse can be derived from Lemma 2.1. Suppose that the PLTL-formula (1) is satisfiable in a Kripke model V for a certain rigid $\underline{c}_0$-guessing $\mathcal{G}$. This means that for every n there is $\tilde{\mathcal{G}}_n \in C(At(\varphi), \mathcal{G})$ such that $V \models_n \bigwedge_{\psi\in\mathcal{G}} [\![\psi]\!] \wedge \bigwedge_{\psi\in\tilde{\mathcal{G}}_n} [\![\psi]\!]$. Since $\tilde{\mathcal{G}}_n$ is $\mathcal{G}$-compatible, there is a $\Sigma^{\underline{a},\underline{c}_0}$-structure $\mathcal{N}_n$ which is a model of $T \cup \tilde{\mathcal{G}}_n \cup \mathcal{G}$; by

Lemma 2.1, the $\mathcal{N}_n$ can be $\Sigma^{\underline{a},\underline{c}_0}$-embedded into $\Sigma^{\underline{a},\underline{c}_0}$-structures $\mathcal{M}_n$ such that $\mathcal{M} := \{\mathcal{M}_n\}_{n\in\mathbb{N}}$ is appropriate for $\mathcal{T}$.[4] The $\mathcal{M}_n$ can be seen as $\Sigma^{\underline{a},\underline{c}}$-structures by interpreting rigid parameters $\underline{c} \setminus \underline{c}_0$ arbitrarily (but in the same way in all $\mathcal{M}_n$). Since truth of ground literals is preserved through embeddings, $\mathcal{M}_n$ is again a model of $\tilde{\mathcal{G}}_n$ for every n. But then Lemma A.7 ensures that $\mathcal{M} \models_0 \varphi$, given that $V \models_0 [\![\varphi]\!]$.

Below, we make essential use of notation explained in Section 4. In particular, we fix an LTL-system specification $(\mathcal{T}, \delta, \iota)$ based on the locally finite compatible LTL-theory $\mathcal{T}$ (let $\upsilon(\underline{a})$ be the unsafety formula we want to test); we work on the safety graph of the system. Recall that the latter is the directed graph defined as follows:

- the nodes are the pairs (V, G) where V is a $\tilde{\delta}$-assignment and G is a transition Σ_r-guessing;
- there is an edge $(V, G) \to (W, H)$ iff the ground sentence

$$G(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge W^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge H(\underline{a}^1, \underline{a}^2, \underline{d}^1) \qquad (4)$$

  is T-satisfiable.[5]

We also recall that the initial nodes of the safety graph are the nodes (V, G) such that $\iota(\underline{a}^0) \wedge V^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ is T-satisfiable; the terminal nodes of the safety graph are the nodes (V, G) such that $V^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge \upsilon(\underline{a}^1) \wedge G(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ is T-satisfiable.

The next proposition immediately yields decidability of ground safety model-checking for locally finite compatible LTL-system specifications.

Proposition 4.1. *The system is unsafe iff either $\iota(\underline{a}) \wedge \upsilon(\underline{a})$ is T-satisfiable or there is a path in the safety graph from an initial to a terminal node.*

Proof. Recall from Section 4 that a bad run of length $n+1$ exists iff the ground sentence

$$\iota(\underline{a}^0) \wedge \bigwedge_{i=0}^{n} (V^l_{i+1}(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i) \wedge V^r_{i+1}(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)) \wedge \upsilon(\underline{a}^{n+1}) \qquad (3)$$

[4] Lemma 2.1 is used with $I := \mathbb{N}$, and $T_i := T$, but symbols from $\Sigma \setminus \Sigma_r$ are disjointly renamed when building the signature Σ_i for the i-th copy of T (the same observation applies also to the flexible constants $\underline{a}$). In this way, a model of $\bigcup_i T_i$ is the same thing as a sequence of models $\{\mathcal{M}_n\}_{n\in\mathbb{N}}$ of T whose Σ_r-reducts coincide.

[5] Here we still follow our convention of writing only the system variable renamings (flexible symbols being renamed accordingly). In more detail: we make three copies r^0, r^1, r^2 of every flexible symbol $r \in \Sigma \setminus \Sigma_r$. Both V^r and W^l might contain in principle two copies r^0, r^1 of r: the two copies in V^r keep their original names, whereas the two copies in W^l are renamed as r^1, r^2, respectively. However, V^r is a right formula (hence it does not contain r^0) and W^l is a left formula (hence it does not contain r^1): the moral of all this is that only the copy r^1 of r occurs after renaming, which means that (4) is after all just a plain $\Sigma^{\underline{a}^0,\underline{a}^1,\underline{a}^2,\underline{d}^0,\underline{d}^1}$-sentence (thus, it makes sense to test it for T-satisfiability). Notice that the Skolem constants $\underline{d}^0$ of V^r are renamed as $\underline{d}^1$ in W^l.

is $\bigoplus_{\Sigma_r}^{n+2} T$-satisfiable, where the V_{i+1} range over the set of $\tilde{\delta}$-assignments.

Preliminary to the main argument of the proof, which is based on interpolations, let us better analyze the shape of the formula (3) with particular attention to symbols occurring in the various literals. In formula (3), each symbol $r \in \Sigma \setminus \Sigma_r$ can occur in $n+2$-copies $r^0, r^1, \ldots, r^{n+1}$ and the locations of these copies are the following:

(i) r^0 can only occur in $\iota(\underline{a}^0) \wedge V_1^l(\underline{a}^0, \underline{a}^1, \underline{d}^0)$;
(ii) r^i can only occur in $V_i^r(\underline{a}^{i-1}, \underline{a}^i, \underline{d}^{i-1}) \wedge V_{i+1}^l(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)$, for $i = 1, \ldots, n$;
(iii) r^{n+1} can only occur in $V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \upsilon(\underline{a}^{n+1})$.

Now, we are ready to develop the main argument of the proof. Suppose that the system is unsafe. Then, either there is a bad run of length 0 or the formula (3) is satisfiable in a model $\mathcal{N}$ of $\bigoplus_{\Sigma_r}^{n+2} T$ for some $n > 0$. For $i = 0, \ldots, n$, let $G_{i+1}(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ be the Σ_r-transition guessing realized by $(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)$ in $\mathcal{N}$ (by this, we mean the set of representative $\Sigma_r^{\underline{c}, \underline{a}^0, \underline{a}^1, \underline{d}^0}$-literals $\psi(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ such that $\mathcal{N} \models \psi(\underline{a}^i, \underline{a}^{i+1}, \underline{d}^i)$). With this choice for the G_i's, the satisfiability of (3) in $\mathcal{N}$ guarantees the existence of the path

$$(V_1, G_1) \rightarrow (V_2, G_2) \rightarrow \cdots \rightarrow (V_{n+1}, G_{n+1}) \tag{6}$$

from the initial node (V_1, G_1) to the terminal node (V_{n+1}, G_{n+1}) within the safety graph.

Vice versa, suppose that there is a path like (6) and that, by contradiction, the system is safe. In particular, this means that the formula

$$\begin{aligned} \iota(\underline{a}^0) \wedge V_1^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V_1^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge \cdots \\ \cdots \wedge V_{n+1}^l(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \upsilon(\underline{a}^{n+1}) \end{aligned}$$

is not $\bigoplus_{\Sigma_r}^{n+2} T$-satisfiable. If we apply the interpolation Lemma A.5 to the T_0-compatible theories T and $\bigoplus_{\Sigma_r}^{n+1} T$ (the hypotheses of Lemma A.5 hold by the modularity Lemma A.6), we get a ground $\Sigma_r^{\underline{c}, \underline{a}^0, \underline{a}^1, \underline{d}^0}$-sentence $\psi_1(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ such that

$$T \models \iota(\underline{a}^0) \wedge V_1^l(\underline{a}^0, \underline{a}^1, \underline{d}^0) \rightarrow \psi_1(\underline{a}^0, \underline{a}^1, \underline{d}^0) \tag{7}$$

and such that

$$\begin{aligned} \psi_1(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V_1^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge \cdots \wedge V_{n+1}^l(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \\ \wedge \upsilon(\underline{a}^{n+1}) \end{aligned} \tag{8}$$

is not $\bigoplus_{\Sigma_r}^{n+1} T$-satisfiable. Since $G_1(\underline{a}^0, \underline{a}^1, \underline{d}^0)$ is a transition Σ_r-guessing, G_1 represents a maximal choice of representative $\Sigma_r^{\underline{a}^0, \underline{a}^1, \underline{d}^0}$-literals, hence we must have either $T \models G_1 \rightarrow \psi_1$ or $T \models G_1 \rightarrow \neg\psi_1$ (that is, $T \models \psi_1 \rightarrow \neg G$). The

latter contradicts (7) and the fact that the node (V_1, G_1) is initial in the safety graph. The former, together with (8) implies that the formula

$$G_1(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V_1^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge \cdots \wedge V_{n+1}^l(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \\ \wedge \upsilon(\underline{a}^{n+1}) \tag{9}$$

is not $\bigoplus_{\Sigma_r}^{n+1} T$-satisfiable. We now repeat the argument: we apply the interpolation Lemma A.5 to the T_0-compatible theories T and $\bigoplus_{\Sigma_r}^{n} T$ and we get a ground $\Sigma_r^{\mathbf{c}, \underline{a}^1, \underline{a}^2, \underline{d}^1}$-sentence $\psi_2(\underline{a}^1, \underline{a}^2, \underline{d}^1)$ such that

$$T \models G_1(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V_1^r(\underline{a}^0, \underline{a}^1, \underline{d}^0) \wedge V_2^l(\underline{a}^1, \underline{a}^2, \underline{d}^1) \rightarrow \psi_2(\underline{a}^1, \underline{a}^2, \underline{d}^1) \tag{10}$$

and such that

$$\psi_2(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge V_2^r(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge \cdots \wedge V_{n+1}^l(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \\ \wedge \upsilon(\underline{a}^{n+1}) \tag{11}$$

is not $\bigoplus_{\Sigma_r}^{n} T$-satisfiable. Since $G_2(\underline{a}^1, \underline{a}^2, \underline{d}^1)$ is a transition Σ_r-guessing, we must have that either $T \models G_2 \rightarrow \psi_2$ or $T \models G_2 \rightarrow \neg\psi_2$. The latter contradicts (10) and the existence of an edge $(V_1, G_1) \rightarrow (V_2, G_2)$. The former, together with (11) implies that the formula

$$G_2(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge V_2^r(\underline{a}^1, \underline{a}^2, \underline{d}^1) \wedge \cdots \wedge V_{n+1}^l(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \\ \wedge \upsilon(\underline{a}^{n+1}) \tag{12}$$

is not $\bigoplus_{\Sigma_r}^{n} T$-satisfiable. Continuing in this way, we obtain the T-unsatisfiability of the formula

$$G_{n+1}(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge V_{n+1}^r(\underline{a}^n, \underline{a}^{n+1}, \underline{d}^n) \wedge \upsilon(\underline{a}^{n+1}) \tag{13}$$

thus contradicting the fact that the node (V_{n+1}, G_{n+1}) is final in the safety graph.

References

21. F. Baader and C. Tinelli. Deciding the word problem in the union of equational theories. *Information and Computation*, 178(2):346–390, 2002.
22. C.-C. Chang and J. H. Keisler. *Model Theory*. North-Holland Publishing Co., third edition, 1990.
23. H. Ganzinger. Shostak light. In *Proc. of CADE 2002*, volume 2392 of *LNCS*. Springer, 2002.
24. C. Tinelli and C. G. Zarba. Combining non-stably infinite theories. *Journal of Automated Reasoning*, 34(3):209–238, 2005.