Bounded Reachability for Temporal Logic over Constraint Systems*

Marcello M. Bersani and Achille Frigeri

Politecnico di Milano, Milano, Italy
{bersani, frigeri}@elet.polimi.it

1 Introduction

Many extensions of Propositional Linear Temporal Logic (PLTL) are proposed with the goal of verifying infinite-state systems whose formulae may include arithmetic constraints belonging to a specific constraint system [3, 6]. Among these, CLTL (Counter LTL) extends Propositional LTL with future operators (PLTL) adding subformulae with Difference Logic (DL) constraints. Unfortunately, this logic is shown to be undecidable. However, many infinite-state systems can be effectively represented by counters automata enjoying decidability of model checking problem for safety and reachability properties, e.g., by constraining the control graph of the automata to be flat [4]. Properties are defined by means of Presburger formulae and then they do not describe any temporal behavior. Their verification is realized by exploiting the equivalence with flat counters automata. An alternative approach [5] exploits a reduction of infinite BMC to a satisfiability problem of Boolean constraints formulae. By translating LTL formulae into a corresponding Büchi automaton, the BMC problem is reduced to the satisfiability of a mixed arithmetic-Boolean formula. In [2] we defined CLTLB($\mathcal{D}$), which is an extension of PLTLB (PLTL with Both future and past operators), allowing arithmetic constraints belonging to a generic constraint system $\mathcal{D}$, and then we considered the Bounded Reachability Problem (BRP) for arithmetic systems. To cope with undecidability we introduced suitable assumptions concerning the structure of models without any syntactic restrictions on formulae. Models only consider partial valuations of arithmetic variables: the satisfiability of CLTLB($\mathcal{D}$) then turns to be decidable, provided that the constraint system has a decidable decision procedure. The BRP for CLTLB($\mathcal{D}$) can be decided by showing its equivalence to the satisfiability of CLTLB($\mathcal{D}$) formulae over partial valuations. Finally, we implemented the decision procedure in a BRP checker by using SMT-solvers and we used it in a practical application of Service Oriented engineering [1].

* This extended abstract summarize results presented in a joint work with Matteo Rossi, Matteo Pradella, Angelo Morzenti and Pierluigi San Pietro [2].

2 A Temporal Logic over Constraint Systems

Let V be a set of variables; a *constraint system* is a relational structure $\mathcal{D} = \langle D, \Pi \rangle$ where D is a set and Π is a family of relations on D. An *atomic $\mathcal{D}$-constraint* is a term of the form $R(x_1, \ldots, x_n)$, where R is an n-ary relation in Π and $x_1, \ldots, x_n$ are variables. A $\mathcal{D}$-valuation is a mapping $v : V \to D$; a constraint is *satisfied* by a $\mathcal{D}$-valuation v, written $v \models R(x_1, \ldots, x_n)$, if $(v(x_1), \ldots, v(x_n)) \in R$. Let AP be a set of atomic propositions; the syntax of a CLTLB($\mathcal{D}$) formula ϕ is defined as follows:

$$\begin{gathered} \phi := p \mid R(\varphi_1, \ldots, \varphi_n) \mid \phi \wedge \phi \mid \neg\phi \mid \mathbf{X}\phi \mid \mathbf{Y}\phi \mid \phi\mathbf{U}\phi \mid \phi\mathbf{S}\phi \\ \varphi := x \mid \mathbf{X}\varphi \mid \mathbf{Y}\varphi \end{gathered} \tag{1}$$

where $p \in AP$, $x \in V$, $\mathbf{X}$ and $\mathbf{Y}$ are the usual "next" and "previous" operators, $\mathbf{U}$ and $\mathbf{S}$ are the usual "until" and "since" operators and $R \in \Pi$. Each formula α is called an *arithmetic temporal term* (a.t.t.); its *depth* $|\alpha|$ is recursively defined as: $|\mathbf{X}(\alpha)| = |\alpha| + 1, |\mathbf{Y}(\alpha)| = |\alpha| - 1$ with $|x| = 0$. We define also the "look-forwards" $\lceil \phi \rceil_x$ (resp. "look-backwards" $\lfloor \phi \rfloor_x$) of ϕ relatively to x as the maximum (resp. minimum) depth of all a.t.t.'s occurring in ϕ in which x appears (this definition naturally extends to set of formulae or set of variables). The semantics of a formula ϕ of CLTLB($\mathcal{D}$) is defined w.r.t. a linear time structure $\pi_\sigma = (S, s_0, I, \pi, \sigma, L)$, where S is a set of states, s_0 is the initial state, $I : \{j \mid \lfloor \phi \rfloor \leq j \leq -1\} \times V \to D$ is an assignment, $\pi \in s_0 S^\omega$ is an *infinite path*, $\sigma : \mathbb{N} \times V \to D$ is a sequence of $\mathcal{D}$-valuations and $L : S \to 2^{AP}$ is a labeling function. Function I defines the valuation of variables for each time instant in $\{j \mid \lfloor \phi \rfloor \leq j \leq -1\}$, i.e., for time instants before 0; this way σ can be extended to a.t.t.'s. Indeed, if α is an a.t.t., x is the variable in α, $i \in \mathbb{N}$ and $\sigma^i(x)$ is a shorthand for $\sigma(i, x)$, then:

$$\sigma^i(\varphi) = \begin{cases} \sigma^{i+|\varphi|}(x), & \text{if } i + |\varphi| \geq 0; \\ I(i + |\varphi|, x), & \text{if } i + |\varphi| < 0. \end{cases} \tag{2}$$

The semantics of a CLTLB($\mathcal{D}$) formula ϕ at instant $i \in \mathbb{N}$ over a linear structure π_σ is recursively defined as in the LTL and it extends to relations, including a.t.t.'s α, as follows:

$$\pi_\sigma^i \models R(\alpha_1, \ldots, \alpha_n) \Leftrightarrow (\sigma^{i+|\alpha_1|}(x_{\alpha_1}), \ldots, \sigma^{i+|\alpha_n|}(x_{\alpha_n})) \in R,$$

where x_{α_i} is the variable that appears in α_i. The semantics of ϕ is well defined, as any valuation σ^i is defined for all $i \geq \lfloor \phi \rfloor$, because of assignment I. A formula $\phi \in$ CLTLB($\mathcal{D}$) is *satisfiable* if it has a model, i.e., a linear time structure π_σ, such that $\pi_\sigma^0 \models \phi$.

3 (Un)decidability of CLTLB($\mathcal{D}$)

By exploiting well-know properties of PLTLB, we proved the equivalence of CLTLB($\mathcal{D}$) to CLTL($\mathcal{D}$) w.r.t. *initial* equivalence obtaining the undecidability of CLTLB($\mathcal{D}$) for a large class of constraint systems. Two CLTLB formulae ϕ, ψ are *globally* (resp. *initially*) equivalent if $\pi^i_\sigma \models \phi \Leftrightarrow \pi^i_\sigma \models \psi$ (resp. $\pi^0_\sigma \models \phi \Leftrightarrow \pi^0_\sigma \models \psi$) for all linear-time structures π_σ and for all $i \in \mathbb{N}$. In [7] is proved that any PLTLB formula is globally equivalent to a separated PLTLB formula, i.e., a Boolean combination of formulae containing either the strict version of "until" or "since", but not both. Since this theorem preserves all semantic properties, it extends also to the case of CLTLB($\mathcal{D}$), provided that each arithmetic constraint is accounted as a propositional letter.

Theorem 1. *Any CLTLB($\mathcal{D}$) formula is initially equivalent to a CLTL($\mathcal{D}$) formula, while the two logics are not globally equivalent. Moreover, if $\mathcal{D} = \langle D, \Pi \rangle$ is a constraint system where Π contains equality and a binary relation R such that (D, R) is a DAG; then satisfiability of CLTLB($\mathcal{D}$) is undecidable.*

Nevertheless, we can prove the decidability for the satisfiability problem in CLTLB($\mathcal{D}$) for a suitable restriction of the semantics.

Definition 1. *Let ϕ be a CLTLB($\mathcal{D}$) w.f.f. and $k \in \mathbb{N}$, then a k-*partial *$\mathcal{D}$-valuation σ_k for ϕ is a relation in $\{i \in \mathbb{Z} \mid i \geq \lfloor \phi \rfloor\} \times V \times D$ with the condition that for each variable x in ϕ, its restriction over $\{i \in \mathbb{Z} \mid \lfloor \phi \rfloor_x \leq i \leq k + \lceil \phi \rceil_x\} \times \{x\} \times D$ is a function from $\{i \in \mathbb{Z} \mid \lfloor \phi \rfloor_x \leq i \leq k + \lceil \phi \rceil_x\} \times \{x\}$ to D.*

Informally, σ_k defines a unique value for each counter x from 0 up to the bound k by means of boundaries conditions (for $\lfloor \phi \rfloor_x \leq i < 0$ and $k < i \leq k + \lceil \phi \rceil_x$), and it accounts for relations over infinite, even periodic, paths, after k. For the case of k-partial $\mathcal{D}$-valuation one can define a semantics of CLTLB($\mathcal{D}$) formulae. It coincides with the semantics of the (full) $\mathcal{D}$-valuations except for the case of arithmetic relations R; namely, if x_{α_j} is the variable that appears in α_j and $\bar{y} = (y_1, \ldots, y_n)$:

$$\pi^i_{\sigma_k} \models R(\alpha_1, \ldots, \alpha_n) \Leftrightarrow \forall \bar{y} \left(\bigwedge_{j=1}^{n} (i + |\alpha_j|, x_{\alpha_j}, y_j) \in \sigma_k \Rightarrow \bar{y} \in R \right). \quad (3)$$

Theorem 2. *The satisfiability of a CLTLB($\mathcal{D}$) formula ϕ over k-partial $\mathcal{D}$-valuations is decidable when $\mathcal{D}$ is decidable.*

4 Bounded Reachability Problem

By using a suitable bounded semantics, i.e., a semantics for formulae on finite structures, we defined the Bounded Reachability Problem. Let $k > 0$, let

ϕ be a CLTLB($\mathcal{D}$) formula and let $\widehat{\sigma}_k : \{i \in \mathbb{Z} \mid \lfloor\phi\rfloor_x \leq i \leq k + \lceil\phi\rceil_x\} \times \{x\} \to \mathcal{D}$, for each $x \in V$, be a *local* sequence of assignments to variables: to correctly define the value of all a.t.t's between instants 0 and k, values of some variables before 0 and after k are defined. Although $\widehat{\sigma}_k$ considers the value of counters only for a fixed number of steps, counting mechanisms of $\mathcal{D}$, if defined, are not altered along finite paths by imposing periodicity of values of variables; and all relations are still considered over infinite, possibly periodic, paths. This allows us to define a complementary approach to the one of [5]: any periodic behavior which induces a finite, even periodic, prefix of values of variables ruled by the counting mechanism and satisfying a CLTLB($\mathcal{D}$) formula, can be represented. Arithmetic variables varying over a bounded set may still be represented by its Boolean representation and be part of the propositional infinite paths. Formally, let $\pi \in S^+$ be a finite path. A *cyclic* finite path ($usvs$, for some $s \in S$, $u, v \in S^*$) can be considered a finite representation of an infinite one, e.g., $u(sv)^\omega$. If π is cyclic, then a bounded semantics for ϕ over π and a local assignment $\widehat{\sigma}_k$ is defined as (3), by replacing σ_k with $\widehat{\sigma}_k$ and π with $u(sv)^\omega$. If π is not cyclic, instead, the semantics of each relation R is, for $0 \leq i \leq k$: $\pi^i_{\widehat{\sigma}_k} \models_k R(\alpha_1, \ldots, \alpha_n) \Leftrightarrow (\widehat{\sigma}_k^{i+|\alpha_1|}(x_{\alpha_1}), \ldots, \widehat{\sigma}_k^{i+|\alpha_n|}(x_{\alpha_n})) \in R$. Then we have:

Theorem 3. *For every* CLTLB($\mathcal{D}$) *formula* ϕ*, if there exist* $k > 0$*, a finite path* π *of length k and a local assignment* $\widehat{\sigma}_k$ *such that* $\pi_{\widehat{\sigma}_k} \models_k \phi$*, then* ϕ *is satisfiable over k-partial* $\mathcal{D}$*-valuations.*

Acknowledgments Many thanks to Luca Cavallaro. This research was funded by the European Commission, Programme IDEAS-ERC, Project 227977-SMScom, and by the project PRIN 2007 D-ASAP (2007XKEHFA).

References

1. M. M. Bersani, L. Cavallaro, A. Frigeri, M. Pradella, and M. Rossi. SMT-based Verification of LTL Specifications with Integer Constraints and its Applications to Runtime Checking of Service Substitutability. In *Proc. SEFM*, 2010.
2. M. M. Bersani, A. Frigeri, M. Pradella, M. Rossi, A. Morzenti, and P. San Pietro. Bounded Reachability for Temporal Logic over Constraint System. In *Proc. TIME*, 2010.
3. H. Comon and V. Cortier. Flatness Is Not a Weakness. In *CSL*, pages 262–276, 2000.
4. H. Comon and Y. Jurski. Multiple Counters Automata, Safety Analysis and Presburger Arithmetic. In *CAV*, pages 268–279, 1998.
5. L. M. de Moura, H. Rueß, and M. Sorea. Lazy theorem proving for bounded model checking over infinite domains. In *CADE-18*, pages 438–455, 2002.
6. S. Demri and D. D'Souza. An automata-theoretic approach to constraint LTL. In *FSTTCS*, pages 121–132, 2002.
7. D. M. Gabbay. The declarative past and imperative future: Executable temporal logic for interactive systems. In *TLS*, pages 409–448, 1987.