Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 231 (2009) 343–361
www.elsevier.com/locate/entcs

CaRet With Forgettable Past

Laura Bozzelli[1]

Università di Napoli Federico II, Via Cintia, 80126 - Napoli, Italy

Abstract

We study the extension of the full logic CaRet with the unary regular modality N (which reads "from now on") which allows to model forgettable past. For such an extension, denoted NCaRet, we show the following: (1) NCaRet is expressively complete for the first-order fragment of MSO_μ, which extend MSO over words with a binary matching predicate, (2) satisfiability and pushdown model checking are 2EXPTIME-complete, and (3) pushdown model checking against the regular fragment of NCaRet remains 2EXPTIME-hard.

Keywords: verification, expressive completeness, pushdown model checking, CaRet, NCaRet

1 Introduction

Verification of pushdown systems. An active field of research is model-checking of pushdown systems. These represent an infinite–state formalism suitable to model the control flow of recursive sequential programs. While for regular properties, the model checking problem of pushdown systems is decidable (see for example [15,4,10]), for context-free properties, such a problem is in general undecidable. However, algorithmic solutions have been proposed for checking some interesting classes of context-free requirements [9,11,8,2]. In particular, the linear temporal logic CaRet, a context–free extension of PLTL (LTL + Past) [14], has been recently introduced [2] which preserves decidability of pushdown model checking (the time complexity of the problem is the same as that of the pushdown model checking problem against LTL, i.e. EXPTIME-complete). CaRet formulas are interpreted on infinite words over an alphabet (called *pushdown alphabet*) which is partitioned into three disjoint sets of calls, returns, and internal symbols. A call denotes invocation of a procedure (i.e., a push stack-operation) and the *matching* return (if any) along the given word denotes the exit from this procedure (corresponding to a pop stack-operation). Full CaRet extends PLTL by also allowing non-regular (past and future)

[1] Email: laura.bozzelli@dma.unina.it

doi:10.1016/j.entcs.2009.02.045

versions of the standard LTL temporal modalities: the past and future *abstract modalities* can specify non-regular context–free properties which require matching of calls and returns such as correctness of procedures with respect to pre and post conditions, while the (past) *caller modalities* are useful to express a variety of security properties that require inspection of the call-stack [9,11,8]. In [3], the class of *nondeterministic visibly pushdown automata* (NVPA) is proposed as an automata theoretic generalization of CaRet. NVPA are pushdown automata which push onto the stack only when a call is read, pops the stack only at returns, and do not use the stack on reading internal symbols. Hence, the input controls the kind of stack operations which can performed. The resulting class of languages (*visibly pushdown languages* or VPL, for short) is closed under all boolean operations and problems such as universality and inclusion that are undecidable for context–free languages are EXPTIME–complete for VPL. Moreover, NVPA have the same expressiveness as MSO_μ [3], which extend the classical monadic second order logic (MSO) over words with a binary matching predicate $\mu(x, y)$ that holds iff y is the matching return for the call x. The logic CaRet is less expressive than NVPA and is easily expressible in the first-order fragment FO_μ of MSO_μ. However, it is an open question whether CaRet is FO_μ-complete [1]. In [1] the authors propose an extension of CaRet with the non-regular unary modality "within" W: a formula $\mathsf{W}\varphi$ holds at position i iff i is a *call position* and the computation fragment from position i to j (initially) satisfies φ, where j is the matching-return of i if any, and $j = \infty$ otherwise (in other words, φ is evaluated on a single procedure). The resulting logic is proved to be FO_μ-complete and exponentially more succinct than CaRet [1]. Moreover, satisfiability and pushdown model checking for this new logic are both 2EXPTIME-complete. An other interesting result in [1] is that past modalities in CaRet + W are necessary to obtain expressive completeness w.r.t. FO_μ sentences. This situation is quite different from the logic PLTL, for which the separation property ensures that LTL has the same expressiveness as PLTL and, thus, corresponds to the class of sentences of the first-order fragment of MSO over words.

Forgettable Past in Temporal Logics. The semantics of standard past modalities is cumulative in the sense that the whole history of the computation is used for evaluating past formulas at the current time. In [13], the authors proposed a new unary regular modality N (which reads "from now on") for situations where at some point one wants to forget the past, and start anew. Formally, a linear temporal formula $\mathsf{N}\varphi$ holds at position i iff the computation fragment from position i (initially) satisfies φ. In [12], it is shown that PLTL + N (NLTL, for short), which has the same expressiveness as PLTL or LTL [13], can be exponentially more succinct than PLTL. Moreover, adding modality N to PLTL raises the complexities of satisfiability and finite–state model checking to EXPSPACE [12].

Our contribution. We study the extension of full CaRet with the modality N. We denote such a new logic by NCaRet. We demonstrate the following results:

- NCaRet has the same expressiveness as FO_μ.
- Satisfiability and pushdown model checking for NCaRet are 2EXPTIME-complete.