Liveness Analysis over Automatic Transition Systems

Anthony Widjaja To and Leonid Libkin

LFCS, School of Informatics, University of Edinburgh
anthony.w.to,libkin@ed.ac.uk

Many real-world systems are more suitably represented as infinite, rather that finite-state transition systems. Some potential sources of infinity include unbounded number of processes, unbounded stacks/queues, and unbounded numeric variables. The past decade saw a lot of effort in extending the tools and techniques of model checking to handle infinite-state systems. The main hurdle one has to face in such an endeavor is that in general model checking infinite-state systems is undecidable. Broadly speaking, there are two approaches to circumvent such a problem. The first approach concerns finding subclasses of infinite systems with decidable properties of interests (e.g. safety and liveness). Such subclasses include pushdown systems, prefix-recognizable systems, and timed systems. At the other extreme, one might start with a broad class of infinite systems and develop semi-algorithms of various kinds (e.g. ones that are guaranteed to terminate but might also give a "don't know" answer).

In this talk, we briefly present some results from a conference paper [6] and some unpublished results from the PhD thesis of the first author. We consider the generic class of automatic transition systems [2] whose domain is represented by a set of words, while the transition relations are represented by (finite) synchronous transducers over words. Although model checking first-order logic over such a class is decidable (e.g. see [2]), it is known that checking safety, liveness, and, more generally, LTL-expressible properties is undecidable.

We are primarily interested in checking liveness and LTL-expressible properties. Define *recurrent reachability* over automatic transition systems to be the problem of checking whether there exists an infinite path in the given automatic transition system $\mathcal{S}$ from a given configuration s_0 (i.e. word) that visits a given regular "target" set T infinitely often. We first make an easy observation that using the classical Vardi-Wolper conversion of LTL formulae into Büchi automata [7], liveness and LTL-expressible properties over automatic transition systems can be effectively (and even quite "efficiently") reduced to the problem of recurrent reachability.

To alleviate the problem of undecidability for recurrent reachability, we then propose a semantic (i.e. not necessarily decidable) condition **(C1)** on the general class of automatic transition systems: that the transitive closure relation $\rightarrow^+$ is effectively regular and that a transducer R^+ for $\rightarrow^+$ is computable from the given input transducers. We shall later see that such a condition is not too restrictive for two reasons: 1) many decidable subclasses of infinite systems satisfy this condition, and 2) many quite successful semi-algorithms have been implemented whose goal is to compute R^+. The following was shown in [6].

Theorem 1 ([6]). *Given an automatic transition system $\mathcal{S}$ satisfying **(C1)** (i.e. a transducer R^+ for $\rightarrow^+$ is available as input), an input word w, and a regular set T, the problem of recurrent reachability is solvable in time $O(|R^+|^3 \times |T|^2)$. Furthermore, an NFA of size $O(|R^+|^2 \times |A|)$ recognizing the set of all w satisfying the recurrent reachability property is computable in that time bound.*

We shall emphasize now that this theorem is by no means obvious since in proving it *one has to take into account non-looping infinite paths*, i.e. infinite paths that do not visit any configurations twice. A restriction, considered in the literature, to *length-preserving transducers* (i.e., $(s, s') \in R$ implies $|s| = |s'|$) reduces recurrent reachability to reachability; however, we do *not* make this assumption, as many interesting classes of infinite-state transition systems do not satisfy it (e.g., pushdown systems, and other examples listed below). The proof of the theorem combines Ramsey theory techniques to obtain a compact representation of an infinite path with automata techniques.

We apply the above theorem to solving LTL model checking over specific classes of automatic transition systems satisfying **(C1)**. In particular, our results apply to the following classes:

- *Pushdown systems*. In this case, we derive an optimal upper bound which is exponential in the size of the LTL formula and polynomial in the size of the system. This matches the known bound of [4].
- *Prefix-recognizable systems*. In this case, we also match an optimal upper bound of [5] which is exponential in both the size of the LTL formula and the size of the system.
- *Reversal-bounded counter systems*. In this case, we derive an algorithm which is double-exponential in the size of the LTL formula (but single-exponential in the size of the specification if it is given as a Büchi automaton) and single-exponential in the size of the system and the number of counters. This upper bound on the problem is new (decidability was obtained in [3]), but it is open whether such a bound is optimal.
- *Reversal-bounded counter systems with discrete-timed clocks and one extra real counter*. In this case, we derive an algorithm which is double exponential in the size of the LTL formula and the number of clocks, but is single-exponential in the size of the system and the number of counters. Even decidability for this class of systems was open (see [3]). The upper bound is not known to be tight.

We have also obtained an initial experimental results. We have implemented a prototype of our algorithm in combination with the tool FAST [1] restricted to the generic class of counter systems with Presburger-definable transition relations. We have successfully verified a particular liveness property called *freedom from global starvation* for many cache-coherence protocols in a fully-automatic way. Most were verified in under ten minutes, the bulk of the time were spent in computing by the tool FAST [1] for computing transducers for the transitive closure relations.

References

1. S. Bardin, A. Finkel, J. Leroux, L. Petrucci. FAST: acceleration from theory to practice. *STTT* 10(5): 401–424 (2008)
2. A. Blumensath and E. Grädel. Automatic structures. In *LICS '00*, pages 51–60.
3. Z. Dang, O. Ibarra, P.S. Pietro. Liveness verification of reversal-bounded multicounter machines with a free counter. In *FSTTCS'01*, pages 132–143.
4. J. Esparza, D. Hansel, P. Rossmanith, and S. Schwoon. Efficient algorithms for model checking pushdown systems. In *CAV '00*, pages 232–247.
5. O. Kupferman, N. Piterman, M. Vardi. Model checking linear properties of prefix-recognizable systems. In *CAV 2002*, pages 371–385.
6. A. W. To and L. Libkin. Recurrent reachability analysis in regular model checking. In *LPAR'08*, pages 198–213.
7. M. Y. Vardi, P. Wolper. Automata-theoretic techniques for modal logics of programs. *JCSS* 32(2): 183–221 (1986).