

Enhanced Distributed Behavioral Cartography of Parametric Timed Automata

Étienne André, Camille Coti, and Hoang Gia Nguyen

Université Paris 13, Sorbonne Paris Cité, LIPN, CNRS, UMR 7030, F-93430, Villetaneuse, France

Abstract

Parametric timed automata (PTA) [1] allow the specification and verification of timed systems incompletely specified, or featuring timing constants that may change either in the design phase, or at runtime.

The behavioral cartography of PTA (BC) [4] relies on the idea of covering a bounded parameter domain with tiles, i.e., parts of the parameter domain in which the discrete behavior is uniform. This is achieved by iterating the inverse method (IM) [2] on the (yet uncovered) integer parameter valuations (“points”) of the bounded parametric domain: given a reference point, IM generalizes the behavior corresponding to this point by synthesizing a constraint containing other (integer and real-valued) points with the same discrete behavior. Then, given a linear time property, it is easy to partition the parametric domain into a subset of “good” tiles and a subset of “bad” ones (which correspond to good and bad behaviors).

Useful applications of BC include the optimization of timing constants, and the measure of the system robustness (values around the reference parameters) w.r.t. the untimed language. In practice, a parameter domain with a large number of integer points will require a long time to compute BC. To alleviate that, our goal is to take advantage of powerful distributed architectures.

Distributing BC is theoretically easy, since it is trivial that two executions of IM from two different points can be performed on two different nodes. However, distributing it efficiently is challenging. For example, calling two executions of IM from two contiguous integer points has a large probability to yield the same tile in both cases, resulting in a loss of time for one of the two nodes. Thus, the critical question is how to distribute efficiently the point on which to call IM.

In a previous work [3], a master-worker scheme is proposed, where the master assigns points to each worker process, which is called a point-based distribution scheme. In this point-based distribution scheme, choosing the point distribution approach on the master side is the key point that will decide the algorithm performance. Since the master has no ability to foresee the tiles on cartography (the “shape” of a cartography is unknown in general), two or more processes can receive close points, that then yield the same result, leading to a loss of efficiency. Besides that, two or more tiles can overlap each other; hence, the question is whether we stop an ongoing process starting from a point that is already covered by another tile. Finally, a very large parameter domain (with many integer points) can cause a bottleneck phenomenon on the master side since many worker processes ask for point, while the master is busy to find uncovered points.

From the previous problems, we proposed an enhanced master-worker distributed algorithm, based on a domain decomposition scheme. The main idea is that the master splits the parameter domain into subdomains, and assigns them to the workers. Then workers will work on their own set of points, hence reducing the probability of choosing close points since the workers work as far as possible from each other. Then, when a worker finishes the coverage of its subdomain, it asks the master for a new subdomain: the master splits a slow worker’s subdomain into two parts, and sends it to the fast worker. Furthermore, we used a heuristic approach to decide whether to stop a process working on a point that has been covered by a tile of another worker. In all our experiments, our enhanced distributed algorithm outperforms previous algorithms.

1998 ACM Subject Classification D.2.4 Software/Program Verification



© Étienne André, Camille Coti, and Hoang Gia Nguyen;
licensed under Creative Commons License CC-BY

2nd International Workshop on Synthesis of Complex Parameters (SynCoP’15).

Editors: Étienne André and Goran Frehse; pp. 104–105

OpenAccess Series in Informatics



OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



Keywords and phrases Formal methods, model checking, distributed algorithmic, real-time systems, parameter synthesis

Digital Object Identifier 10.4230/OASICS.SynCoP.2015.104

Category Informal Presentation

References

- 1 Rajeev Alur, Thomas A. Henzinger, and Moshe Y. Vardi. Parametric real-time reasoning. In *STOC*, pages 592–601. ACM, 1993.
- 2 Étienne André, Thomas Chatain, Emmanuelle Encrenaz, and Laurent Fribourg. An inverse method for parametric timed automata. *International Journal of Foundations of Computer Science*, 20(5):819–836, 2009.
- 3 Étienne André, Camille Coti, and Sami Evangelista. Distributed behavioral cartography of timed automata. In *EuroMPI/ASIA*, pages 109–114. ACM, 2014.
- 4 Étienne André and Laurent Fribourg. Behavioral cartography of timed automata. In *RP*, volume 6227 of *Lecture Notes in Computer Science*, pages 76–90. Springer, 2010.