Robust Timed Automata*

Vineet Gupta 1 Thomas A. Henzinger 2 Radha Jagadeesan 3

1 Xerox PARC, 3333 Coyote Hill Road, Palo Alto, CA 94304; vgupta@parc.xerox.com
2 EECS Department, University of California, Berkeley, CA 94720; tah@eecs.berkeley.edu
3 Mathematical Sciences Department, Loyola Univ.-Lake Shore Campus, Chicago, IL 60626; radha@math.luc.edu

Abstract. We define robust timed automata, which are timed automata that accept all trajectories "robustly": if a robust timed automaton accepts a trajectory, then it must accept neighboring trajectories also; and if a robust timed automaton rejects a trajectory, then it must reject neighboring trajectories also. We show that the emptiness problem for robust timed automata is still decidable, by modifying the region construction for timed automata. We then show that, like timed automata, robust timed automata cannot be determinized. This result is somewhat unexpected, given that in temporal logic, the removal of real-time equality constraints is known to lead to a decidable theory that is closed under all boolean operations.

1 Introduction

The formalism of timed automata [AD94] has become a standard model for real-time systems, and its extension to hybrid automata [ACHH93, ACH+95, Hen96] has become a standard model for mixed discrete-continuous systems. Yet it may be argued that the precision inherent in the formalism of timed and hybrid automata gives too much expressive power to the system designer. For example, while there is a timed automaton $A$ that issues an event $a$ at the exact real-numbered time $t$, such a system cannot be realized physically. This is because for every physical realization $R_A$ of $A$ there is a positive real $\epsilon$, however small, so that one can guarantee at most that $R_A$ issues the event $a$ in the time interval $(t-\epsilon, t+\epsilon)$. The discretization of time into units of size $\epsilon$, on the other hand, may not allow a sufficiently abstract representation of $A$. Among the reasons for leaving the precision $\epsilon$ parametric are the following: the actual value of $\epsilon$ may be unknown; future realizations of $A$ may achieve a precision smaller than $\epsilon$; if $A$ is an open system, it may be composed with systems whose precision is smaller than $\epsilon$; a small $\epsilon$ may cause a dramatic increase in the state space.

Similarly, consider two hybrid automata $B_\leq$ and $B_<$ for modeling the controller of a chemical plant. The two automata are identical except that $B_\leq$ activates a furnace iff the plant temperature falls to $T$ degrees, and $B_<$ activates the furnace iff the plant temperature falls below $T$ degrees. These two formal objects differ, and may have entirely different mathematical properties; for example, some plant transition may be possible only at temperatures less than $T$, thus causing any number of states to be reachable

* The first and third author were supported in part by grants from ARPA and ONR. The second author was supported in part by the ONR YIP award N00014-95-1-0520, by the NSF CAREER award CCR-9501708, by the NSF grant CCR-9504469, by the AFOSR contract F49620-93-1-0056, by the ARO MURI grant DAAH-04-96-1-0341, by the ARPA grant NAG2-892, and by the SRC contract 95-DC-324.036. The third author was also supported by the NSF.
in $B_\leq$ but not in $B_\leq$. Yet the difference between the two automata cannot be realized physically, because every physical thermometer has a positive error $\epsilon$, however small, and cannot reliably distinguish between $T$ and $T - \epsilon$ degrees. Again, the discretization of temperature into $\epsilon$-units may not be adequate for reasons given above.

We remove the “excessive” expressive power of timed and hybrid automata without discretization, by having automata define (i.e., generate or accept) not individual trajectories, but bundles of closely related trajectories. A bundle of very similar trajectories is called a tube. For example, while a single trajectory $\tau$ may have event $a$ at time $t$, every tube containing $\tau$ also contains some trajectories with event $a$ very close to, but not exactly at time $t$. Formally, we suggest several metrics on the trajectories of timed and hybrid automata, and define a tube to be an open set of trajectories. This definition is shown to be independent of the choice of metric, because the “reasonable” metrics all induce the same topology. Then, a tube is accepted by a timed or hybrid automaton iff the accepted trajectories form a dense subset of the tube. Accordingly, while “isolated” accepted trajectories do not belong to any accepted tube, isolated rejected trajectories are added to accepted tubes, as motivated by the observation that an automaton ought not be able to accept or reject individual trajectories.

Timed and hybrid automata with tube acceptance are called robust, because they are insensitive against small input perturbations (and they may produce small output perturbations). In this paper, we look at some theoretical implications of robustness. First, we solve the emptiness problem for robust timed automata: given a timed automaton $A$, does $A$ accept any tube? Our emptiness check for tube acceptance is derived from the region method of [AD94] for trajectory acceptance, but is somewhat more efficient, because only open regions need be considered. The emptiness check leads, in the usual way, to algorithms for verifying requirements of robust timed automata that are specified in a linear-time logic such as MITL [AFH96], in a branching-time logic such as TCTL [ACD93], or by event-clock automata [AFH94].

Second, we study the complementation problem for robust timed automata. Complementation is instrumental for using automata as a requirements specification language: abstract requirements of trajectories are often specified naturally using non-deterministic automata; then, in order to check that all trajectories that are generated by an implementation automaton $A$ are accepted by the specification automaton $B$, the latter needs to be complemented (before checking the product of $A$ and $\neg B$ for emptiness). While timed automata with trajectory acceptance are not closed under complement [AD94] (i.e., there is a timed automaton whose rejected trajectories are not the accepted trajectories of any other timed automaton), one may harbor some hope that robust timed automata can be complemented (i.e., for every timed automaton $B$ there may be a timed automaton $\neg B$ that accepts precisely the tubes which are disjoint from the tubes accepted by $B$). This hope stems from the following observations:

1. In the case of linear-time temporal logic, the removal of all timing constraints that enforce exact real-numbered time differences between events leads to a decidable theory, called MITL, which is closed under all boolean operations [AFH96]. It is therefore not unreasonable to expect that in the case of timed automata, the removal of individual trajectories, which express exact real-numbered time differences between events, leads likewise to a decidable and boolean-closed theory.

2. The impossibility of complementation for timed automata follows from the fact that while the emptiness problem is decidable, the universality problem (i.e., given a timed automaton, does it accept all trajectories?) is not [AD94]. Undecidabil-