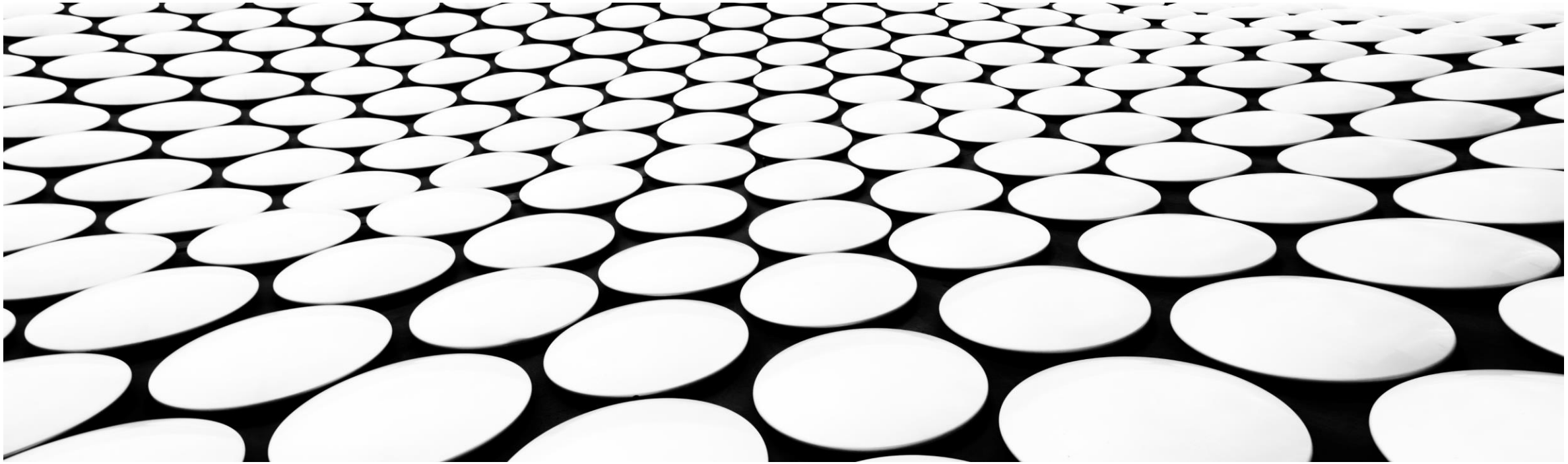
COMPUTING ACCUMULATED DELAYS IN REAL-TIME SYSTEMS



MOTIVATION

- Model Checking has emerged as a powerful tool for automatic verification of FSM and it has been extended to real-time systems.
- Given the description of a finite-state system together with its timing assumptions, there are algorithms that test whether the system satisfies a specification written in a real-time temporal logic.

MOTIVATION

- A time-bounded causality property can be specified using Real-time temporal logics.
- For e.g.,

  An alarm rings whenever the door of a refrigerator is open continuously for 30 seconds.

- But a duration-bounded causality property is not expressible by Real-time temporal logics.
- Thus, Standard real-time temporal logics have limited expressiveness. In particular, they do not allow us to constrain the accumulated satisfaction times of state predicates.
- For e.g.,

  A response is obtained whenever a ringer has been pressed, possibly intermittently, for a total duration of 20 seconds

THE PROBLEM STATEMENT

- To address the algorithmic verification problem for duration properties of real-time systems by using the formalism of timed automata for representing real-time systems.
- More formally, Given a timed automaton with a duration measure, an initial and a final state, and an arithmetic constraint, the duration-bounded reachability problem asks if there is a run of the automaton from the initial state to the final state such that the duration of the run satisfies the constraint.
- They show that the duration-bounded reachability problem is PSPACE-complete, and provide an optimal solution. The algorithm can be used to verify duration properties of real-time systems that are modeled as timed automata, such as the duration-bounded causality property.

A BRIEF OVERVIEW

- The basic question about a timed automaton is the following time-bounded reachability problem:

Given an initial state σ, a final state τ, and an interval I, is there a run of the automaton starting in state σ and ending in state τ such that the total elapsed time of the run is in the interval I?

- Note: The state of a timed automaton includes, apart from the location of the control, also the real-numbered values of all clocks. Consequently, the state space of a timed automaton is infinite.
- The solution to this problem relies on a partition of the infinite state space into finitely many regions, which are connected with transition and time edges to form the region graph of the timed automaton.

A BRIEF OVERVIEW

- Unfortunately, the region graph is not enough for checking duration properties such as the duration-bounded causality property.
- Why? Because the regions doesn’t capture the accumulated satisfaction time.
- Hence a new technique is needed for analyzing duration properties!

A BRIEF OVERVIEW

- To introduce the concept of durations in a timed automaton, they associate with every finite run a nonnegative real number, which is called the duration of the run.
- The duration of a run is defined inductively using a duration measure, which is a function that maps the control locations to nonnegative integers:
- i.e., the duration of an empty run is 0; and the duration measure of a location gives the rate at which the duration of a run increases while the automaton control resides in that location.
- For example, a duration measure of 0 means that the duration of the run stays unchanged (i.e., the time spent in the location is not accumulated),
- a duration measure of 1 means that the duration of the run increases at the rate of time (i.e., the time spent in the location is accumulated), and
- a duration measure of 2 means that the duration of the run increases at twice the rate of time.

A BRIEF OVERVIEW

- The time-bounded reachability problem can now be generalized to the duration-bounded reachability problem:

Given an initial state σ, a final state τ,a duration measure and an interval I, is there a run of the automaton starting in state σ and ending in state τ such that the duration of the run is in the interval I?

A BRIEF OVERVIEW

Brief outline of the construction.

- Given a region R, a final state τ, and a path in the region graph from R to τ, they show that the lower and upper bounds on the durations of all runs that start at some state in R and follow the chosen path can be written as linear expressions over the variables that represent the clock values of the start state.
- In a first step, they provide a recipe for computing these so-called bound expressions.
- In the next step, they define an infinite graph, the bounds graph, whose vertices are regions tagged with bound expressions that specify the set of possible durations for any path to the final state.
- In the final step, they show that the infinite bounds graph can be collapsed into a finite graph for solving the duration-bounded reachability problem.

THE DURATION BOUNDED REACHABILITY PROBLEM

SOME PRELIMINARY DEFINITIONS

- Formally, a **timed automaton A** is a triple (S, X, E) with the following components:
- • S is a finite set of locations;
- • X is a finite set of clocks;
- • E is a finite set of transitions of the form (s, t, φ, x), for a source location $s \in S$, a target location $t \in S$, a clock constraint φ, and a clock $x \in X$. Each clock constraint is a positive Boolean combination of atomic formulas of the form $y < k$ or $y \leq k$ or $k \leq y$ or $k < y$, for clock $y \in X$ and a nonnegative integer constant $k \in \mathbb{N}$.

SOME PRELIMINARY DEFINITIONS

- A configuration of the timed automaton A is fully described by specifying the location of the control and the values of all clocks.
- A clock valuation $c \in \mathbb{R}^X$ is an assignment of non-negative reals to the clock X.
- A state σ of A is a pair (s,c) consisting of a location $s \in S$ and a clock valuation c.
- [Notation]: Σ for the infinite set of states of A.

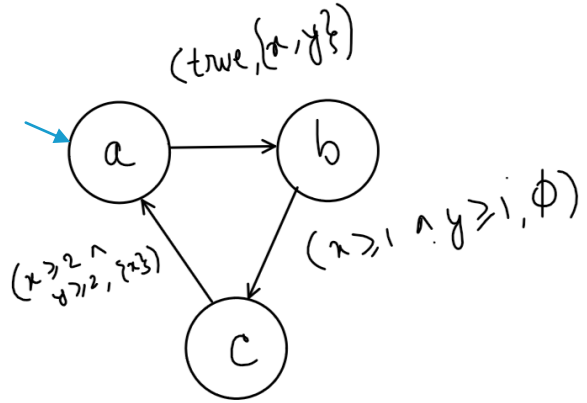
SOME PRELIMINARY DEFINITIONS

- The possible behaviors of the timed automaton A are defined through a successor relation on the states of A:
- **Transition successor** For all states $(s, c) \in \Sigma$ and transitions $(s, t, \varphi, x) \in E$, if c satisfies φ, then $(s, c) \rightarrow^{0} (t, c[x := 0])$
- Note: Here precisely one clock is reset with each transition but it does not affect the expressiveness of timed automata. Why?
- **Time successor** For all states $(s, c) \in \Sigma$ and time increments $\delta \in \mathbb{R}$, we have $(s, c) \rightarrow^{\{\delta\}} (s, c + \delta)$.

SOME PRELIMINARY DEFINITIONS

- A state (t, d) is a successor of the state (s, c), written $(s, c) \rightarrow (t, d)$, iff there exists a nonnegative real S such that $(s, c) \rightarrow (t, d)$.
- The successor relation defines an infinite graph $\mathrm{K}(A)$ on the state space Σ of A. The transitive closure $\rightarrow^*$ of the successor relation $\rightarrow$ is called the *reachability relation of A.*

EXAMPLE OF A TIMED RUN



- An example of Successor relation is :
- $(a, 0,0) \rightarrow^{1.2} (a, 1.2,1.2) \rightarrow^{0} (b, 0,0) \rightarrow^{1} (b, 1,1) \rightarrow^{0} (c, 1,1) \rightarrow^{2.2} (c, 3.2,2.2) \rightarrow^{0} (a, 0,3.2)$

CLOCK REGIONS AND REGION GRAPH

- Suppose that we are given a timed automaton A and an equivalence relation $\cong$ on the states Σ of A.
- For $\sigma \in \Sigma$, we write $[\sigma]_{\cong} \subseteq \Sigma$ for the equivalence class of states that contains the states σ.
- The successor relation $\rightarrow$ is extended to $\cong$ equivalence classes as follows:

$[\sigma]_{\cong} \rightarrow [\tau]_{\cong}$ iff there is a state $\sigma' \in [\sigma]_{\cong}$ a state $\tau' \in [\tau]_{\cong}$, and a nonnegative real δ such that $\sigma' \rightarrow^{\delta} \tau'$ and for all nonnegative reals $\epsilon < \delta$, we have $(\sigma + \epsilon) \in ([\sigma]_{\cong} \cup [\tau]_{\cong})$.

CLOCK REGIONS AND REGION GRAPH

- The **quotient graph** of A with respect to the equivalence relation $\cong$, written $[K(A)]_{\cong}$, is a graph whose vertices are the $\cong$-equivalence classes and whose edges are given by the successor relation $\rightarrow$.
- $\cong$ is **back stable** iff whenever $\sigma \rightarrow \tau$, then for all states $\tau' \in [\tau]_{\cong}$, there is a state $\sigma' \in [\sigma]_{\cong}$ such that $\sigma' \rightarrow \tau'$.
- The quotient graph with respect to a (back) stable equivalence relation can be used for solving **the reachability problem** between equivalence classes:

Given two $\cong$ equivalence classes R_0 and R_f, is there a state $\sigma \in R_0$ and a state $\tau \in R_f$ such that $\sigma \rightarrow^* \tau$?

If the equivalence relation $\cong$ is (back) stable, then the answer to the reachability problem is affirmative iff there is a path from R_0 to R_f in the quotient graph $[K(A)]_{\cong}$.

REGION GRAPH

- The region graph of the timed automaton A is a quotient graph of A with respect to the particular equivalence relation defined below.
- For $x \in X$, let m_x be the largest constant that the clock x compared to in any clock constraint of A.
- For $\delta \in \mathbb{R}$, let $\backslash\mathrm{floor}(\delta)$ denote the integral part of δ, and let δ' denote the fractional part of δ(thus, $\delta = \delta' + \backslash\mathrm{floor}(\delta)$). Two states (s, c) and (t, d) of A are region-equivalent written (s, c) $\approx$ (t, d), iff the following four conditions hold:
  - s = t
  - for each clock x ∈ X, either $\backslash\mathrm{floor}(c(x)) = \backslash\mathrm{floor}(d(x))$, or both $c(x) > m_x$ and $\mathrm{d}(x) > m_x$
  - for all clocks x, y ∈ X, the valuation c satisfies x' ≤ y' iff the valuation d satisfies x' ≤ y'
  - for each clock x ∈ X, the valuation c satisfies x' = 0 iff the valuation d satisfies x' = 0.

REGION GRAPH

- Example:
- If we have 3 clocks x,y,z then the region R = [s, x=2, y = 1.2 , z =0.9] contains all the states (s,c) such that c satisfies $\floor(x) = 2, \floor(y) = 1, \floor(z) = 0$ and $0 = x' < y' < z'$
- Thus the region R generalizes to [s, $\floor(x) = 2, \floor(y) = 1, \floor(z) = 0, 0 = x' < y' < z'$]
- There are only finitely many regions, because the exact value of the integral part of a clock x is recorded only if it is smaller than m_x. The number of regions is bounded by $|S| \times 2^n \times \mathrm{n}! \times \pi_{x \in \mathrm{X}}(m_x + 1)$, where n = |X| is the number of clocks.

REGION GRAPH

- The region equivalence relation $\approx$ is stable as well as back-stable.
- Hence the region graph can be used for solving reachability problems between regions, and also for solving time-bounded reachability problems!
- A region R is a boundary region iff there is some clock x such that R satisfies the constraint $x' = 0$.
- A region that is not a boundary region is called an open region.

REGION GRAPH

- For a boundary region R, we define its predecessor region pred(R) to be the open region Q such that for all states (s, c) ∈ Q, there is a time increment $\delta \in \mathbb{R}$ such that (s,c+δ) ∈ R and for all nonnegative reals $\epsilon < \delta$, we have (s,c+ϵ) ∈ Q.
- Similarly, we define its successor region succ(R) to be the open region Q' such that for all states (s, c) ∈ Q', there is a time increment $\delta \in \mathbb{R}$ such that (s,c-δ) ∈ R and for all nonnegative reals $\epsilon < \delta$, we have (s,c-ϵ) ∈ Q'.
- For example, a boundary region R given by,

[s, $\backslash\text{floor}(x) = 2, \backslash\text{floor}(y) = 1, \backslash\text{floor}(z) = 0, 0 = x' < y' < z'$]

Pred(R) is the open region [s, $\backslash\text{floor}(x) = 1, \backslash\text{floor}(y) = 1, \backslash\text{floor}(z) = 0, y' < z' < x'$]

Succ(R) is the open region [s, $\backslash\text{floor}(x) = 1, \backslash\text{floor}(y) = 1, \backslash\text{floor}(z) = 0, 0 < x' < y' < z'$]

REGION GRAPH

- The edges of the region graph R(A) fall into two categories:
- **Transition edges** If (s, c) $\rightarrow^0$ (t, d), then there is an edge from the region $[s, c]_{\cong}$ to the region $[t, d]_{\approx}$.
- **Time edges** For each boundary region R, there is an edge from pred(R) to R, and an edge from R to succ(R).
- Note: Regions with self loops can be ignored for reachability problems.

DURATION MEASURES AND DURATION BOUNDED REACHABILITY

- A **duration measure** for the timed automaton A is a function p from the locations of A to the nonnegative integers.
- A **duration constraint** for A is of the form $\int p \in I$, where p is a duration measure for A and I is a bounded interval of the nonnegative real line whose endpoints are integers (I may be open, half-open, or closed).
- Let p be a duration measure for A. We extend the state space of A to evaluate the integral $\int p$ along the runs of A.
- An extended state of A is a pair (σ, ϵ) consisting of a state σ of A and a nonnegative real number ϵ.

DURATION MEASURES AND DURATION BOUNDED REACHABILITY

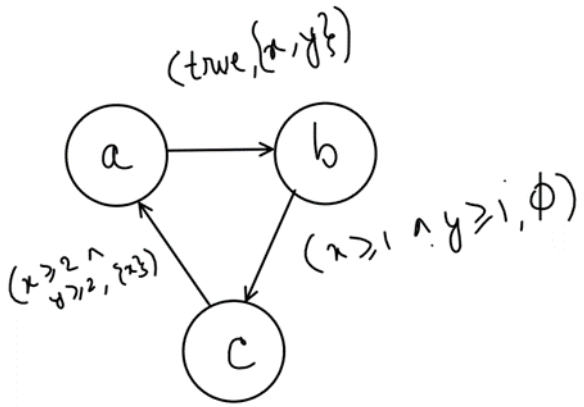
- The successor relation on states is extended as follows:
- **Transition successor** For all extended states (s, c, ϵ) and all transitions (s, t, φ, x) such that c satisfies φ, define

$(s, c, \epsilon) \rightarrow^{\delta} (t, c[x := 0], \epsilon)$.

- **Time successor** For all extended states (s, c, ϵ) and all time increments $\delta \in \mathbb{R}$, define

(s,c,ϵ) $\rightarrow^{\delta} (s, c + \delta, \epsilon + \delta \,.\, p(s))$

DURATION MEASURES AND DURATION BOUNDED REACHABILITY



- The duration measure p is defined by p(a)=0 p(b)=1 p(c)=2.
- Let Initial region R_0 be a singleton $\{(a, x = 0, y = 0)\}$ and the final region R_f be $\{(a, 0,2)\}$.
- For the duration constraint $\int p \geq 3$, The duration bounded reachability holds:
  - $(a, 0,0,0) \rightarrow^2 (a, 2,2,0) \rightarrow^0 (b, 0,0,0) \rightarrow^1 (b, 1,1,1) \rightarrow^0 (c, 1,1,1) \rightarrow^1 (c, 2,2,3) \rightarrow^0 (a, 0,2,3)$
- For the duration constraint $\int p = 0$, The duration bounded reachability doesn't hold

DURATION MEASURES AND DURATION BOUNDED REACHABILITY

- We consider the duration-bounded reachability problem between regions:
- given two regions R_0 and R_f of a timed automaton A, and a duration constraint $\int p \in I$ for A, is there a state $\sigma \in R_0$, a state $\tau \in R_f$, and a nonnegative real $\delta \in I$ such that $(\sigma, 0) \rightarrow^* (\tau, \delta)$? We refer to this duration-bounded reachability problem using the tuple $(A, R_0, R_f, \int p \in I)$.
- If the duration measure p is the constant function 1 (i.e., p(s) = 1 for all locations s), then the integral $\int p$ measures the total elapsed time, and the duration-bounded reachability problem between regions is called a time-bounded reachability problem.
- In this case, if $(\sigma, 0) \rightarrow^* (\tau, \delta)$ for some $\delta \in I,$ then for all the states $\sigma' \in [\sigma]_{\approx}$ there is a state $\tau' \in [\sigma]_{\approx}$ and a real number $\delta' \in I\ such\ that\ (\sigma^\wedge{}', 0) \rightarrow^* (\tau', \delta')$. **Hence, the region graph suffices to solve the time-bounded reachability problem. This, however, is not true for general duration measures.**

BOUNDED-LABELED REGIONS AND THE BOUNDS GRAPH

- Consider a timed automaton A, two regions R_0 and R_f, and a duration measure p. We determine the set I of possible values of δ such that $(\sigma, 0) \rightarrow^* (\tau, \delta)$ for some $\sigma \in R_0$ and $\tau \in R_f$.
- To compute the **lower and upper bounds** on the integral $\int p$ along a path of the region graph, we refine the graph by labeling all regions with expressions that specify the extremal values of the integral.

BOUNDED-LABELED REGIONS AND THE BOUNDS GRAPH

- We define an infinite graph with vertices of the form (R, L, l, U, u), where R is a region, L and U are linear expressions over the clock variables, and l and u are boolean values.
- The intended meaning of the bound expressions L and U is that in moving from a state (s,c) ∈ R to a state in the final region R_f, the set of possible values of the integral $\int p$ has the infimum L and the supremum U, both of which are functions of the current clock values c.
- If the bit l is 0, then the infimum L is included in the set of possible values of the integral, and if l is 1, then L is excluded.
- Similarly, if the bit u is 0, then the supremum U is included in the set of possible values of $\int p$, and if u is 1, then U is excluded.
- For example, if l = 0 and u = 1, then the left-closed right-open interval [L, U) gives the possible values of the integral $\int p$.

BOUND EXPRESSION

- The bound expressions L and U associated with the region R have a special form.
- Suppose that $X = \{x_i, \ldots, x_n\}$ is the set of clocks and that for all states $(s, c) \in R$, the clock valuation c satisfies $0 \leq x_i' \leq \ldots \leq x_n' < 1$; that is, x_1 is the clock with the smallest fractional part in R, and $\mathrm{x_n}$ is the clock with the largest fractional part.
- The fractional parts of all n clocks partition the unit interval into n + 1 subintervals represented by the expressions $e_0, \ldots, e_n$:

$$e_0 = x_1'$$

$$e_1 = x_2' - x_1'$$

$$\ldots$$

$$e_{\{n-1\}} = x_n' - x_{\{n-1\}}'$$

$$e_n = 1 - x_n'$$

BOUND EXPRESSION

- A **Bound expression** for R is a positive linear combination of the expressions $e_0, \ldots, e_n$; that is, a bound expression for R has the form $a_0.e_0 + \ldots + a_n.e_n$, where $a_0, \ldots, a_n$ are nonnegative integer constants.
- We denote bound expressions by (n+1)-tuples of coefficients and write $(a_0, \ldots, a_n)$ for the bound expression $a_0.e_0 + \ldots + a_n.e_n$.

BOUND-LABELED REGIONS

- A **Bound-labeled region** (R, L, I, U, u) of the timed automaton A consists of a clock region R of A, two bound expressions L and U for R, and two bits $l, u \in \{0,1\}$. We construct $B_{\{p,R_f\}}$(A), the bounds graph of A for the duration measure p and the final region R_f. The vertices of $B_{\{p,R_f\}}$(A) are the bound-labeled regions of A and the special vertex R_f, which has no outgoing edges.

BOUND-LABELED REGIONS

- We first define the edges with the target R_f .
- The edges with the target R_f that reaches a state in R_f without passing through other regions.
- Let R_f be an open region with p(s)=a for all s ∈ R_f which is reachable from a state $(s, c) \in R_f$ by remaining in the state for atmost $|1 - x_n'|_c$ time units.
- As $\int p$ increases at rate a, the lower bound on the integral value over all states $(s, c) \in R_f$ is 0 and the upper bound is a.(1-$x_n{}'$).

BOUND-LABELED REGIONS

- While the lower bound 0 is a possible value of the integral, if a>0, then the upper bound is only the supremum of all the possible values.
- Thus, add an edge in the bound graph to R_f from $(R_f, L, 0, U, u)$ for
  - L = (0,..,0,0) and U=(0,...,0,a); if a=0 then u=0 else 1
- If R_f is a boundary region then no time can be spent in R_f , and both the bounds are 0. In this case, add an edge to R_f from $(R_f, L, 0, U, u)$ for L=U=(0,...,0,0)

BOUND-LABELED REGIONS

- For paths that reach final region R_f by passing through other regions.
- For each edge from R to R' In the region graph $R(A)$, the bounds graph $B_{\{p,R_f\}}(A)$ has exactly one edge to each bound-labeled region of the form (R', L', l', U', u'), from some bounded-labeled region of the form (R, L, l, U, u).
- For the Lower bound L and bit l, look at the example:
  - Let $X = \{x, y, z\}$ and that the boundary region R_1 which satisfies $0 = x' < y' < z'$ is labeled with the lower bound $L_1 = (0, a_1, a_2, a_3)$ and the bit l_1.
  - Starting from $(s, c) \in R_1$ the lower bound on the integral $\int p$ for some reaching state in R_f is
    - $[a_1.y' + a_2.(z' - y') + a_3.(1 - z')]_c$

BOUND-LABELED REGIONS

- Look at the open predecessor region $R_2\ of\ R_1$ that satisfies $0 < y' < z' < x'$.
- Duration measure P(s)=a for all $s \in R_2$
- There is a time edge from $R_2\ to\ R_1$ in the graph.
- To compute the lower bound label for $L_2\ for\ R_2$ from the lower bound label $L_1\ of\ R_1$.
- Starting from (s,c) $\in R_2$, the state (s,c+δ) $\in R_1$ is reached after the time $\delta = [1 - x']_c$ and

$$
\begin{aligned}
[\![\bar{y}]\!]_{c+\delta} &= [\![\bar{y}]\!]_c + \delta = [\![\bar{y} + (1 - \bar{x})]\!]_c, \\
[\![\bar{z} - \bar{y}]\!]_{c+\delta} &= [\![\bar{z} - \bar{y}]\!]_c, \\
[\![1 - \bar{z}]\!]_{c+\delta} &= [\![1 - \bar{z}]\!]_c - \delta = [\![\bar{x} - \bar{z}]\!]_c.
\end{aligned}
$$

BOUND-LABELED REGIONS

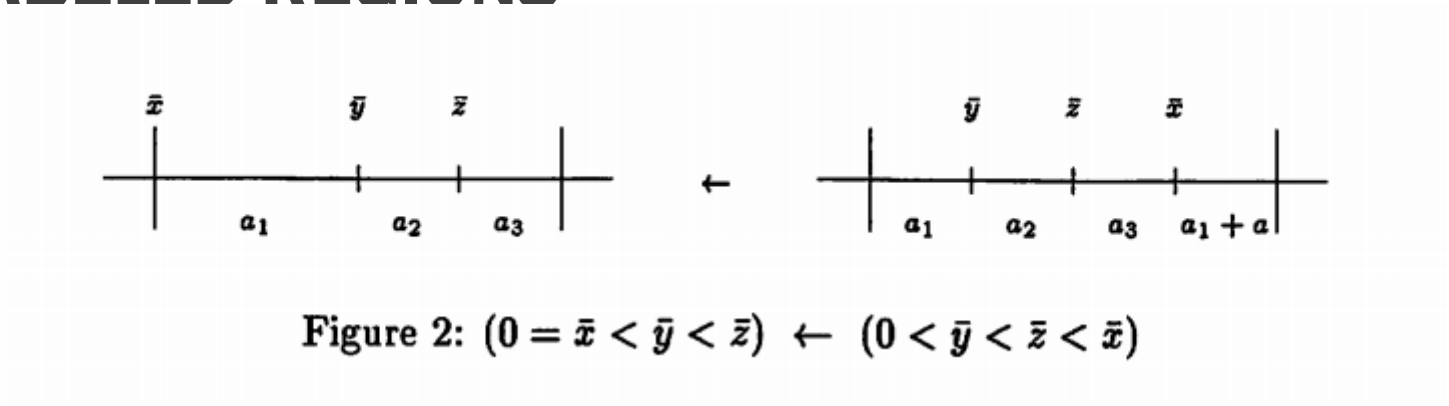


Figure 2: $(0 = \bar{x} < \bar{y} < \bar{z}) \leftarrow (0 < \bar{y} < \bar{z} < \bar{x})$

- Also, from the state $(s, c) \in R_2$ the integral $\int p$ has the value $[a.(1 - x')]_c$ before entering the region R_1.
- Hence, the new lower bound is
  - $[a_1.(y' + (1 - x') + a_2.(z' - y') + a_3.(x' - z') + a.(1 - x')]_c$
- The label L_2 is $(a_1, a_2, a_3, a_1 + a)$.
- If the lower bound L_2 is valid w.r.t. the integral depends on whether the original lower bound L_1 is a possible value of the integral starting in R_1.
- So, the bits l_2 labelling R_2 is the same as the bit L_1 labelling R_1.

BOUND-LABELED REGIONS

Figure 3: $(0 < \bar{y} < \bar{z} < \bar{x}) \leftarrow (0 = \bar{y} < \bar{z} < \bar{x})$

- Consider the boundary region R_3 such that R_2 is the successor region of R_3.
- The region R_3 satisfies $0 = y' < z' < x'$, and there is a time edge from R_3 to R_2.
- The updated lower-bound label L_3 of R_3 is the same as $L_2, i.e., (a_1, a_2, a_3, a_1 + a)$
- Simplified to $(0, a_2, a_3, a_1 + a)$, since R_3 is a boundary region.
- The updated bits are also same.

BOUND-LABELED REGIONS

- The process repeats if we take further time edges.
- Let us consider an edge from $R_4\ to\ R_3$. With reset of clock y.
- We assume $region\ R_4$ is open with the duration measure b and that R_4 satisfies $0 < z' < y' < x'$.
- Take the state (t,d) ∈ R_4.
- Let the transition happen after $time\ \delta, then\ 0 \leq \delta < [1 - x']_d$.
- If the state reached is $(s, c) \in R_3, then\ [x']_c = [x']_d + \delta, \quad [y']_c = 0 \quad and \quad [z']_c = [z']_d + \delta$.
- The lower bound L_4 is the value of the integral before the transition, $b.\ \delta$, added to the value of the lower bound $L_3\ at\ the\ state\ (s, c)$

$$[a_2.z' + a_3.(x' - z') + (a_1 + a).(1 - x')]_c$$

BOUND-LABELED REGIONS

- To get the lower bound L_4 at the state (t,d), compute the infimum over all the choices of δ, for $0 \leq \delta < [1 - x']_d$.
- The required lower bound is :
  - $\inf_{\{0 \leq \delta < [1-x']_d\}} \{b.\delta + [a_2.z' + a_3.(x' - z') + (a_1 + a).(1 - x')]_c\}$
- Substituting $[x']_c = [x']_d + \delta \quad and \quad [z']_c = [z']_d + \delta, we\ get$
  - $[a_2.z' + a_3.(x' - z')]_d + \inf_{\{0 \leq \delta < [1-x']_d\}} \{(a_2 + b).\delta + [\,(a_1 + a).(1 - x' - \delta)]_d\}$
- The infimum of the monotonic function in δ is reached at one of the two extreme points. When $\delta = 0$, then the value of L_4 at (t, d) is
  - $[a_2.z' + a_3.(x' - z') + (a_1 + a).(1 - x')]_d$
- When δ reaches $[1 - x']_d$ (longest time), then the value of $L_4\ at\ (t, d) is$
  - $[a_2.z' + a_3.(x' - z') + (a_2 + b).(1 - x')]_d$

BOUND-LABELED REGIONS

Figure 4: $(0 = \bar{y} < \bar{z} < \bar{x}) \leftarrow (0 = \bar{z} < \bar{y} < \bar{x})$

- As R_4 satisfies $0 < z' < y' < x'$ and $(x' - z') = (y' - z') + (x' - y')$, the lower bound label $L_4\ for\ R_4\ \ is\ \ (a_2, a_3, a_3, a_4),\ \ where\ a_4\ is\ the\ minimum\ of\ a_1 + a\ and\ a_2 + b.$

BOUND-LABELED REGIONS

- Finally, deduce the bit l_4, that indicates if the lower bound L_4 is valid w.r.t. the integral.
- If $a_1 + a \leq a_2 + \delta$, then the lower bound is achieved with $\delta = 0$
- L_4 is possible for R_4 iff L_3 $is\ possible\ for\ R_3$ $hence\ l_4 = l_3$.
- Else, if $a_1 + a > a_2 + b$, then the lower bound is obtained with $\delta \rightarrow [1 - x']_d$
- $L_4\ is\ possible\ iff\ both\ b = 0\ and\ l_3\ is\ possible\ for\ R_3$
- $so\ l_4 = 0\ if\ b = 0\ and\ l_3 = 0\ else\ l_4 = 1.$

BOUND-LABELED REGIONS

- Let the region graph $R(A)$ has an edge from $R \ \ to\ R'$
- Formal definition of Edges between bounded-labeled regions of the bound graph $B_{p,R_f}(A)$.
- Let a be the duration measure of R
- The bounds graph has an edge from $(R, L, l, U, u)\ to\ (R', L', l', U', u')$ iff the bound expression
  - $L = (a_0, a_1, .., a_n),\ L' = (a'_0, a'_1, \dots, a'_n), U = (b_0, b_1, \dots, b_n)\ and\ U' = (b'_0, b'_1, \dots, b'_n)\ and\ the\ bits\ l, u, u', l'\ relations\ are\ given\ from\ the\ next\ page$ …

BOUND-LABELED REGIONS

Figure 5: $(0 = \bar{x} = \bar{z} < \bar{y} < \bar{u}) \leftarrow (0 = \bar{x} < \bar{y} < \bar{z} < \bar{u})$

Time edge 1 R' is a boundary region and $R = pred(R')$ is an open region: let $1 \leq k \leq n$ be the largest index such that R' satisfies $\bar{x}_k = 0$, then

for all $0 \leq i \leq n - k$, we have $a_i = a'_{i+k}$ and $b_i = b'_{i+k}$;
for all $n - k < i < n$, we have $a_i = 0$ and $b_i = 0$;
$a_n = a'_k + a$ and $b_n = b'_k + a$;
$l = l'$ and $u = u'$.

Time edge 2 R is a boundary region and $R' = succ(R)$ is an open region:

$a_0 = 0$ and $b_0 = 0$;
for all $0 < i \leq n$, we have $a_i = a'_i$ and $b_i = b'_i$;
$l = l'$ and $u = u'$.

BOUND-LABELED REGIONS

Transition edge 1 R' is a boundary region, R is an open region, and the clock with the k-th smallest fractional part in R is reset:

for all $0 \leq i < k$, we have $a_i = a'_{i+1}$ and $b_i = b'_{i+1}$;
for all $k \leq i < n$, we have $a_i = a'_i$ and $b_i = b'_i$;
if $a'_n \leq a'_1 + a$ then $a_n = a'_n$, else $a_n = a'_1 + a$;
if $b'_n \geq b'_1 + a$ then $b_n = b'_n$, else $b_n = b'_1 + a$;
if $a'_n > a'_1 + a$ and $a > 0$ then $l = 1$, else $l = l'$;
if $b'_n < b'_1 + a$ and $a > 0$ then $u = 1$, else $u = u'$.

Transition edge 2 Both R and R' are boundary regions, and the clock with the k-th smallest fractional part in R is reset:

for all $0 \leq i < k$, we have $a_i = a'_{i+1}$ and $b_i = b'_{i+1}$;
for all $k \leq i \leq n$, we have $a_i = a'_i$ and $b_i = b'_i$;
$l = l'$ and $u = u'$.

REACHABILITY IN THE BOUNDS GRAPH

- Given a state $\sigma = (s, c)$, two bound expressions L and U, and two bits $l \; and \; u$,
- Define the bounded interval $I(\sigma, L, l, U, u)$ of the +ve real line as:
  - The left endpoint is $[L]_c$
  - The right endpoint is [U]_c
  - If l =0, the interval is left-closed else it is left open
  - If u=0, then the interval is right closed else it is right open.

REACHABILITY IN THE BOUNDS GRAPH REGIONS

LEMMA 1 *Let A be a timed automaton, let p be a duration measure for A, and let R_f be a region of A. For every state σ of A and every nonnegative real δ, there is a state $\tau \in R_f$ such that $(\sigma, 0) \rightarrow^* (\tau, \delta)$ iff in the bounds graph $\mathcal{B}_{p,R_f}(A)$, there is path to R_f from a bound-labeled region (R, L, l, U, u) with $\sigma \in R$ and $\delta \in I(\sigma, L, l, U, u)$.*

LEMMA 2 *Let A be a timed automaton, let $\int p \in I$ be a duration constraint for A, and let R_0, R_f be two regions of A. There are two states $\sigma \in R_0$ and $\tau \in R_f$ and a real number $\delta \in I$ such that $(\sigma, 0) \rightarrow^* (\tau, \delta)$ iff in the bounds graph $\mathcal{B}_{p,R_f}(A)$, there is path to R_f from a bound-labeled region B with region component R_0 and $I(B) \cap I \neq \emptyset$.*

REACHABILITY IN THE BOUNDS GRAPH REGIONS

- To solve duration bounded reachability problem, construct the bounds graph from which the special vertex R_f is reached.
- By a backward breadth-first manner from the final region R_f.
- Same region may appear with different bounds expression. [infinitely many bound expressions]
- But the backward search terminates in finite steps [shown next]

COLLAPSING THE BOUNDS GRAPH

- Define an equivalence relation $\cong_m$ over bounded-labeled regions given a non-negative integer m.
- For two +ve integers a and b, define a $\cong_m$ b iff either
  - a=b
  - Both a>m and b>m
- For two bounded expressions $e = (a_0, \ldots, a_n)$ and $f = (b_0, \ldots, b_n)$, define e $\cong_m$ f iff
  - For all $0 \leq i \leq n, a_i \cong_m b_i$.
- For two bounded regions $B_1 = (R_1, L_1, l_1, U_1, u_1)$ and $B_2 = (R_2, L_2, l_2, U_2, u_2)$ define $B_1 \cong_m B_2$ iff:
  - $R_1 = R_2$
  - $L_1 \cong_m L_2$ and $U_1 \cong_m U_2$.
  - $either$ $l_1 = l_2$ or $some$ $coefficient$ in $L_1 > m$
  - $either$ $u_1 = u_2$ or $some$ $coefficient$ in $U_1 > m$.

LEMMA 3 *If the bounds graph $\mathcal{B}_{p,R_f}(A)$ contains an edge from a bound-labeled region B_1 to a bound-labeled region B_1', and $B_1' \cong_m B_2'$, then there exists a bound-labeled region B_2 such that $B_1 \cong_m B_2$ and the bounds graph contains an edge from B_2 to B_2'.*

LEMMA 4 *Consider two bound-labeled regions B_1 and B_2 and a bounded interval $I \subseteq \mathbb{R}$ with integer endpoints. If $B_1 \cong_m B_2$ for the right endpoint m of I, then $I \cap I(B_1) = \emptyset$ iff $I \cap I(B_2) = \emptyset$.*

LEMMA 5 *Let A be a timed automaton with location set S and clock set X such that n is the number of clocks, and no clock x is compared to a constant larger than m_x. For every nonnegative integer m, the number of m-constrained bound-labeled regions of A is at most*

$$4 \cdot |S| \cdot n! \cdot 2^{n+2} \cdot (m+2)^{2(n+1)} \cdot \Pi_{x \in X}(m_x + 1).$$

THEOREM 1 *Let $m \in \mathbf{N}$ be the right endpoint of the interval $I \subseteq \mathbb{R}$. The answer to the duration-bounded reachability problem $(A, R_0, R_f, \int p \in I)$ is affirmative iff there exists a finite sequence $B_0, \ldots, B_k$ of m-constrained bound-labeled regions of A such that*

1. *the bounds graph $\mathcal{B}_{p,R_f}(A)$ contains an edge to R_f from some bound-labeled region B with $\gamma(B) = B_0$;*
2. *for all $0 \leq i < k$, the bounds graph $\mathcal{B}_{p,R_f}(A)$ contains an edge to B_i from some bound-labeled region B with $\gamma(B) = B_{i+1}$;*
3. *$I(B_k) \cap I \neq \emptyset$ and the clock region of B_k is R_0.*

COROLLARY 1 *The duration-bounded reachability problem for timed automata can be decided in* PSPACE.

The duration-bounded reachability problem for timed automata is PSPACE-hard, because already the (unbounded) reachability problem between clock regions is PSPACE-hard [AD94].