Reachability for Multi-Priced Timed Automata and Diophantine Approximation

Andrew Scoones

Joint with Mahsa Shirmohammadi, Ben Worrell

June 2025

What are Multi-Priced Timed Automata?

- Timed automata are a widely studied model of real-time systems that extend classical finite state-automata with real-valued variables, called clocks, that evolve with derivative one and which can be queried and reset along transitions

What are Multi-Priced Timed Automata?

- Timed automata are a widely studied model of real-time systems that extend classical finite state-automata with real-valued variables, called clocks, that evolve with derivative one and which can be queried and reset along transitions
- Multi-Priced Timed Automata (MPTA) further extend timed automata with variables, called observers, that have a non-negative slope that can change from one location to another.

What are Multi-Priced Timed Automata?

- Timed automata are a widely studied model of real-time systems that extend classical finite state-automata with real-valued variables, called clocks, that evolve with derivative one and which can be queried and reset along transitions
- Multi-Priced Timed Automata (MPTA) further extend timed automata with variables, called observers, that have a non-negative slope that can change from one location to another.
- Such variables can model the accumulation of costs or the use of resources along a computation, such as energy and memory consumption in embedded systems, or bandwidth in communication networks

Aims

- Address a more expressive variant of MPTA than previously considered: namely those in which observers can have both positive and negative rates

Aims

- Address a more expressive variant of MPTA than previously considered: namely those in which observers can have both positive and negative rates
- Alternatively, and equivalently, one can consider MPTA with nonnegative rates, but in which one allows reachability specifications to contain constraints on the difference between two observers rather than just threshold constraints that compare observers to constants

Aims

- Address a more expressive variant of MPTA than previously considered: namely those in which observers can have both positive and negative rates
- Alternatively, and equivalently, one can consider MPTA with nonnegative rates, but in which one allows reachability specifications to contain constraints on the difference between two observers rather than just threshold constraints that compare observers to constants
- This extension is motivated by the desire to measure net resource use along computations

Definition

2.1 Multi-Priced Timed Automata

Let $\mathbb{R}_{\geq 0}$ denote the set of non-negative real numbers. Given a set $\mathcal{X} = \{x_1, \ldots, x_n\}$ of *clocks*, the set $\Phi(\mathcal{X})$ of *clock constraints* is generated by the grammar

$$\varphi ::= \mathtt{true} \mid x \leq k \mid x \geq k \mid \varphi \wedge \varphi,$$

where $k \in \mathbb{N}$ is a natural number and $x \in \mathcal{X}$. A *clock valuation* is a mapping $\nu : \mathcal{X} \to \mathbb{R}_{\geq 0}$ that assigns to each clock a non-negative real number. We denote by $\mathbf{0}$ the valuation such that $\mathbf{0}(x) = 0$ for all clocks $x \in \mathcal{X}$. We write $\nu \models \varphi$ to denote that ν satisfies the constraint φ. Given $t \in \mathbb{R}_{\geq 0}$, we let $\nu + t$ be the clock valuation such that $(\nu + t)(x) = \nu(x) + t$ for all clocks $x \in \mathcal{X}$. Given $\lambda \subseteq \mathcal{X}$, let $\nu[\lambda \leftarrow 0]$ be the clock valuation such that $\nu[\lambda \leftarrow 0](x) = 0$ if $x \in \lambda$, and $\nu[\lambda \leftarrow 0](x) = \nu(x)$ otherwise.

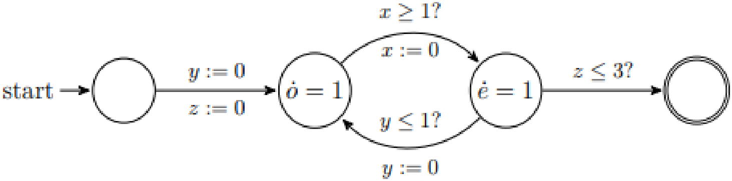
A *multi-priced timed automaton* (MPTA) $\mathcal{A} = \langle L, \ell_0, L_f, \mathcal{X}, \mathcal{Y}, E, R \rangle$ comprises a finite set L of *locations*, an *initial location* $\ell_0 \in L$, a set $L_f \subseteq L$ of *accepting locations*, a finite set $\mathcal{X}$ of *clock variables*, a finite set $\mathcal{Y}$ of *observers*, a set $E \subseteq L \times \Phi(\mathcal{X}) \times 2^{\mathcal{X}} \times L$ of *edges*, and a *rate function* $R : L \to \mathbb{Z}^{\mathcal{Y}}$. Here $R(\ell)(y)$ is the derivative of the observer $y \in \mathcal{Y}$ in location ℓ. Denote by $\|\mathcal{A}\|$ the length of the description of $\mathcal{A}$, where all integers are written in binary.

A *state* of $\mathcal{A}$ is a triple (ℓ, ν, t) where ℓ is a location, ν a clock valuation, and $t \in \mathbb{R}_{\geq 0}$ is a *time stamp*. A *run* of $\mathcal{A}$ is an alternating sequence of states and edges

$$\rho = (\ell_0, \nu_0, t_0) \xrightarrow{e_1} (\ell_1, \nu_1, t_1) \xrightarrow{e_2} \ldots \xrightarrow{e_m} (\ell_m, \nu_m, t_m),$$

where $t_0 = 0$, $\nu_0 = \mathbf{0}$, $t_{i-1} \leq t_i$ for all $i \in \{1, \ldots, m\}$, and $e_i = \langle \ell_{i-1}, \varphi, \lambda, \ell_i \rangle \in E$ is such that $\nu_{i-1} + (t_i - t_{i-1}) \models \varphi$ and $\nu_i = (\nu_{i-1} + (t_i - t_{i-1}))[\lambda \leftarrow 0]$ for $i = 1, \ldots, m$. The run is *accepting* if $\ell_m \in L_f$. The *value* of such a run is a vector $\mathrm{val}(\rho) \in \mathbb{R}^{\mathcal{Y}}$, defined by $\mathrm{val}(\rho) = \sum_{i=0}^{m-1} (t_{i+1} - t_i) R(\ell_i)$. We refer to Figure 1 for an example of an MPTA and its operational semantics.

Example



Problems

Definition

Given L, the set of finite locations, let $R : L \to \mathbb{Z}^{\mathcal{Y}}$ be the rate function, where $\mathcal{Y}$ is a finite set of observers.
The value of a run ρ is defined to be $\mathrm{val}(\rho) = \sum_{i=0}^{m-1}(t_{i+1} - t_i)R(l_i)$.

Problems

Definition

Given L, the set of finite locations, let $R : L \to \mathbb{Z}^{\mathcal{Y}}$ be the rate function, where $\mathcal{Y}$ is a finite set of observers.
The value of a run ρ is defined to be $\mathrm{val}(\rho) = \sum_{i=0}^{m-1}(t_{i+1} - t_i)R(l_i)$.

- Given an MPTA and a target $\gamma \in \mathbb{R}^{\mathcal{Y}}$, the Domination Problem is to decide whether there is an accepting run ρ such that $\mathrm{val}(\rho) \leq \gamma$ pointwise

Problems

Definition

Given L, the set of finite locations, let $R : L \to \mathbb{Z}^{\mathcal{Y}}$ be the rate function, where $\mathcal{Y}$ is a finite set of observers.
The value of a run ρ is defined to be $\mathrm{val}(\rho) = \sum_{i=0}^{m-1}(t_{i+1} - t_i)R(l_i)$.

- Given an MPTA and a target $\gamma \in \mathbb{R}^{\mathcal{Y}}$, the Domination Problem is to decide whether there is an accepting run ρ such that $\mathrm{val}(\rho) \leq \gamma$ pointwise
  - This is PSPACE-complete for MPTA with positive rates only, undecidable if negative rates are allowed

Problems

Definition

Given L, the set of finite locations, let $R : L \to \mathbb{Z}^{\mathcal{Y}}$ be the rate function, where $\mathcal{Y}$ is a finite set of observers.
The value of a run ρ is defined to be $\mathrm{val}(\rho) = \sum_{i=0}^{m-1}(t_{i+1} - t_i)R(l_i)$.

- Given an MPTA and a target $\gamma \in \mathbb{R}^{\mathcal{Y}}$, the Domination Problem is to decide whether there is an accepting run ρ such that $\mathrm{val}(\rho) \leq \gamma$ pointwise
  - This is PSPACE-complete for MPTA with positive rates only, undecidable if negative rates are allowed
  - This motivates the Gap Domination Problem, where we include a slack paramter ϵ

Problems

Definition

Given L, the set of finite locations, let $R : L \to \mathbb{Z}^{\mathcal{Y}}$ be the rate function, where $\mathcal{Y}$ is a finite set of observers.
The value of a run ρ is defined to be $\mathrm{val}(\rho) = \sum_{i=0}^{m-1}(t_{i+1} - t_i)R(l_i)$.

- Given an MPTA and a target $\gamma \in \mathbb{R}^{\mathcal{Y}}$, the Domination Problem is to decide whether there is an accepting run ρ such that $\mathrm{val}(\rho) \leq \gamma$ pointwise
  - This is PSPACE-complete for MPTA with positive rates only, undecidable if negative rates are allowed
  - This motivates the Gap Domination Problem, where we include a slack paramter ϵ
  - If there is some run ρ such that $\mathrm{val}(\rho) \leq \gamma - \epsilon$, the output should be "dominated", and if there is no run such that $\mathrm{val}(\rho) \leq \gamma$ the output should be "not dominated"

Reduction to a bilinear problem

Definition

A semilinear set is the finite union of linear sets

Lemma

Let $\mathcal{A}$ be an MPTA with set of observers $\mathcal{Y}$ of cardinality $d+1$. Then there is a semilinear set $\mathcal{S}_{\mathcal{A}} \subset (\mathbb{Z}^{\mathcal{Y}})^{d+1}$, such that for every accepting run ρ of $\mathcal{A}$ there exists $(\gamma_1, \ldots, \gamma_{d+1}) \in \mathcal{S}_{\mathcal{A}}$, for which the val$(\rho)$ lies in the convex hull of these vectors.

Moreover, $\mathcal{S}_{\mathcal{A}}$ can be written as a collection of linear sets that can be computed in time exponential in $||\mathcal{A}||$, each of which has a description length polynomial in $||\mathcal{A}||$

Reduction to a bilinear problem

Lemma

Given $\gamma \in \mathbb{R}^x$, where x depends on $\mathcal{A}$, there exists a run ρ on $\mathcal{A}$ with $val(\rho) \leq \gamma$ if and only if the following mixed integer-real system of non-linear inequalities has a solution:

$$\lambda_1\gamma_1 + \cdots + \lambda_{d+1}\gamma_{d+1} \leq \gamma,\ 1 = \sum_{i=1}^{d+1} \lambda_i$$

$$(\gamma_1, \ldots, \gamma_{d+1}) \in \mathcal{S}_{\mathcal{A}},\ 0 \leq \lambda_i$$

$$\gamma_i \in \mathbb{Z}^x,\ \lambda_i \in \mathbb{R}$$

What we actually think about

Definition

A mixed-integer bilinear (MIB) system is a collection of constraints in integer variables $\mathbf{x}$ and real variables $\mathbf{y}$ of the form

$$\begin{aligned}
&\mathbf{x}^T A_i \mathbf{y} < b_i,\ i = 1, \ldots, l,\\
&C\mathbf{x} \leq \mathbf{d},\\
&E\mathbf{y} \leq \mathbf{f},\\
&\mathbf{x} \in \mathbb{Z}^m,\ \mathbf{y} \in \mathbb{R}^n.
\end{aligned}$$

What we actually think about

Definition

A mixed-integer bilinear (MIB) system is a collection of constraints in integer variables $\mathbf{x}$ and real variables $\mathbf{y}$ of the form

$$\begin{aligned}
&\mathbf{x}^T A_i \mathbf{y} < b_i,\ i = 1, \ldots, l,\\
&C\mathbf{x} \leq \mathbf{d},\\
&E\mathbf{y} \leq \mathbf{f},\\
&\mathbf{x} \in \mathbb{Z}^m,\ \mathbf{y} \in \mathbb{R}^n.
\end{aligned}$$

We say the system is bounded if the polyhedron

$$\{\mathbf{y} \in \mathbb{R}^n \ :\ E\mathbf{y} \leq \mathbf{f}\}$$

is bounded, i.e. a polytope.

An initial problem

Theorem

The satisfiability problem for bounded MIB systems is undecidable.

An initial problem

Theorem

The satisfiability problem for bounded MIB systems is undecidable.

Proof.

Reduce from Hilbert's 10th problem. □

An initial problem

Theorem

The satisfiability problem for bounded MIB systems is undecidable.

Proof.

Reduce from Hilbert's 10th problem. □

Add slack: A satisfying requirement has slack $\epsilon > 0$ if

$$\mathbf{x}^T A_i \mathbf{y} < b_i - \epsilon$$

An initial problem

Theorem

The satisfiability problem for bounded MIB systems is undecidable.

Proof.

Reduce from Hilbert's 10th problem. □

Add slack: A satisfying requirement has slack $\epsilon > 0$ if

$$\mathbf{x}^T A_i \mathbf{y} < b_i - \epsilon$$

Gap satisfiability problem: given $\epsilon > 0$ and MIB system $\mathcal{S}$, find procedure that returns SAT if $\mathcal{S}$ has a satisfying assignment with slack ϵ, and UNSAT if $\mathcal{S}$ is unsatisfiable.

An initial problem

Theorem

The satisfiability problem for bounded MIB systems is undecidable.

Proof.

Reduce from Hilbert's 10th problem. □

Add slack: A satisfying requirement has slack $\epsilon > 0$ if

$$\mathbf{x}^T A_i \mathbf{y} < b_i - \epsilon$$

Gap satisfiability problem: given $\epsilon > 0$ and MIB system $\mathcal{S}$, find procedure that returns SAT if $\mathcal{S}$ has a satisfying assignment with slack ϵ, and UNSAT if $\mathcal{S}$ is unsatisfiable.
No requirement on output if $\mathcal{S}$ is satisfiable, but with no satisfying assignment with slack ϵ.

Gap Satisfiablilty

Theorem

The Gap Satisfiability Problem is undecidable for (unbounded) MIB systems.

Gap Satisfiablilty

Theorem

The Gap Satisfiability Problem is undecidable for (unbounded) MIB systems.

Proof.

Reduce from Hilbert's 10th Problem. □

Gap Satisfiablilty

Theorem

The Gap Satisfiability Problem is undecidable for (unbounded) MIB systems.

Proof.

Reduce from Hilbert's 10th Problem. □

Theorem

The Gap Satisfiability Problem is decidable for bounded MIB systems

Gap Satisfiablilty

Theorem

The Gap Satisfiability Problem is undecidable for (unbounded) MIB systems.

Proof.

Reduce from Hilbert's 10th Problem. □

Theorem

The Gap Satisfiability Problem is decidable for bounded MIB systems

Theorem

The Gap Domination Problem for MPTA is decidable in non-deterministic exponential time

Proof Ideas

- The proof of the above essentially comes down to “relaxation and rounding”

Proof Ideas

- The proof of the above essentially comes down to “relaxation and rounding”
  - we relax and work over the reals rather than integers

Proof Ideas

- The proof of the above essentially comes down to “relaxation and rounding”
  - we relax and work over the reals rather than integers
  - the use the flatness theorem from Diophantine Approximation to round these solutions to integers

Proof Ideas

- The proof of the above essentially comes down to “relaxation and rounding”
  - we relax and work over the reals rather than integers
  - the use the flatness theorem from Diophantine Approximation to round these solutions to integers
- Loosely, the flatness theorem is like Minkowski’s theorem on lattices

Proof Ideas

- The proof of the above essentially comes down to “relaxation and rounding”
  - we relax and work over the reals rather than integers
  - the use the flatness theorem from Diophantine Approximation to round these solutions to integers
- Loosely, the flatness theorem is like Minkowski’s theorem on lattices
- Essentially, it shows if a convex polyhedron is “wide” enough it contains an integer point

Diophantine Approximation

- Using Diophantine Approximation ideas, there are some subcases of the unbounded version we can hope to tackle

Diophantine Approximation

- Using Diophantine Approximation ideas, there are some subcases of the unbounded version we can hope to tackle
- Assume the condition, $\mathbf{x} \geq 0$

Diophantine Approximation

- Using Diophantine Approximation ideas, there are some subcases of the unbounded version we can hope to tackle
- Assume the condition, $\mathbf{x} \geq 0$
- We can use the multidimensional version of Dirichlet's Theorem for a similar "relax and round" strategy

Diophantine Approximation

- Using Diophantine Approximation ideas, there are some subcases of the unbounded version we can hope to tackle
- Assume the condition, $\mathbf{x} \geq 0$
- We can use the multidimensional version of Dirichlet's Theorem for a similar "relax and round" strategy

Theorem (Multidimensional Dirichlet)

Let $(i_1, \ldots, i_m)$ be an m-tuple of real numbers satisfying

$$0 < i_1, \ldots, i_m < 1 \text{ and } \sum_{t=1}^{m} i_t = 1.$$

Then, for any $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$ and $N \in \mathbb{N}$, there exists a $q \in \mathbb{Z}$ such that $1 \leq q \leq N$ and

$$\max \left\{ \|qx_1\|^{1/i_1}, \ldots, \|qx_m\|^{1/i_m} \right\} < N^{-1},$$

where by $\|x\|$ we mean the distance to the integer closest to x.

Broad Idea

- Again, relax and round

Broad Idea

- Again, relax and round
- Find solutions $\mathbf{x}^*, \mathbf{y}^* \in \mathbb{R}$ that satisfy the constraints

Broad Idea

- Again, relax and round
- Find solutions $\mathbf{x}^*, \mathbf{y}^* \in \mathbb{R}$ that satisfy the constraints
- Use Dirichlet to approximate $\mathbf{x}^*$ by $\mathbf{p}/q$

Broad Idea

- Again, relax and round
- Find solutions $\mathbf{x}^*, \mathbf{y}^* \in \mathbb{R}$ that satisfy the constraints
- Use Dirichlet to approximate $\mathbf{x}^*$ by $\mathbf{p}/q$
    - Given our ϵ, we can pick a sufficiently large N which from which we know $\mathbf{p}$, q exist that satisfy the inequalities we need.

Broad Idea

- Again, relax and round
- Find solutions $\mathbf{x}^*, \mathbf{y}^* \in \mathbb{R}$ that satisfy the constraints
- Use Dirichlet to approximate $\mathbf{x}^*$ by $\mathbf{p}/q$
  - Given our ϵ, we can pick a sufficiently large N which from which we know $\mathbf{p}$, q exist that satisfy the inequalities we need.
- We then use bilinearity to move the $1/q$ to $\mathbf{y}$

Broad Idea

- Again, relax and round
- Find solutions $\mathbf{x}^*, \mathbf{y}^* \in \mathbb{R}$ that satisfy the constraints
- Use Dirichlet to approximate $\mathbf{x}^*$ by $\mathbf{p}/q$
  - Given our ϵ, we can pick a sufficiently large N which from which we know $\mathbf{p}$, q exist that satisfy the inequalities we need.
- We then use bilinearity to move the $1/q$ to $\mathbf{y}$
  - WARNING! When does $\frac{\mathbf{y}^*}{q}$ still satisfy

$$E\mathbf{y} < \mathbf{f}?$$

Another Idea?

Theorem (Minkowski's Theorem for Systems of Linear Forms)

Let $\beta_{i,j} \in \mathbb{R}$*, where* $1 \leq i, j \leq q$ *and let* $C_1, \ldots, C_k > 0$*. If*

$$|\det(\beta_{i,j})| \leq \prod_{i=1}^{k} C_i,$$

then there exists a non-zero integer point $x = (x_1, \ldots, x_k)$ *such that*

$$\begin{aligned} |x_1\beta_{i,1} + \cdots + x_k\beta_{i,k}| &< C_i, \qquad 1 \leq i \leq k-1 \\ |x_1\beta_{k,1} + \cdots + x_k\beta_{k,k}| &\leq C_k. \end{aligned}$$