Verification of Polynomial Interrupt Timed Automata

Béatrice Bérard¹,²,⁴,⁵, Serge Haddad²,⁴,⁵, Claudine Picaronny²,⁴,⁵, Mohab Safey El Din¹,⁴,⁵, Mathieu Sassolas³,⁵

¹Université P. & M. Curie, LIP6
²ENS Cachan, LSV
³Université Paris-Est, LACL
⁴CNRS, ⁵INRIA

SynCoP + PV, ETAPS, Uppsala, April 22nd, 2017
Landing a rocket

- First stage (lasting $x_1$) in state $q_0$:
  From distance $d$, the rocket approaches the land under gravitation $g$;

- Second stage (lasting $x_2$, while $x_1$ is frozen) in $q_1$:
  The rocket approaches the land with constant deceleration $h < 0$;

- Third stage: The rocket must reach the land with small positive speed (less than $\varepsilon$).

\[ \frac{1}{2}g x_1^2 + g x_1 x_2 + \frac{1}{2} h x_2^2 = d \land 0 \leq g x_1 + h x_2 < \varepsilon \]

For all $g \in [7, 10]$ does there exist an $h \in [-3, -1]$ such that the rocket is landing?
Hybrid automata

Hybrid automaton = finite automaton + variables

Variables evolve in states and can be tested and updated on transitions.

- Clocks are variables with slope 1 in all states
- Stopwatches are variables with slope 0 or 1

Verification problems are mostly undecidable

- Decidability requires restricting:
  - either the flows [Henzinger et al. 1998]
  - or the jumps [Alur et al. 2000] for flows \( \dot{x} = Ax \)
  - or both like in Timed Automata = finite automaton + clocks with guards \( x \preceq c \) and reset [Alur, Dill 1990]

- Other approaches exist like bounded delay reachability or approximations by discrete transition systems.
Interrupt clocks

Many real-time systems include interruption mechanisms (as in processors).

Several levels with exactly one active clock at each level

Level 4
Level 3
Level 2
Level 1

\[
\begin{bmatrix}
  x_1 \\
  x_2 \\
  x_3 \\
  x_4
\end{bmatrix}
\]

Exec:
\[
\begin{bmatrix}
  0 \\
  0 \\
  0 \\
  0
\end{bmatrix}
\]
\[
\begin{bmatrix}
  1.5 \\
  0 \\
  0 \\
  0
\end{bmatrix}
\]
\[
\begin{bmatrix}
  1.5 \\
  0 \\
  2.1 \\
  0
\end{bmatrix}
\]
\[
\begin{bmatrix}
  1.5 \\
  0 \\
  2.1 \\
  0
\end{bmatrix}
\]
\[
\begin{bmatrix}
  1.5 \\
  0 \\
  0 \\
  0
\end{bmatrix}
\]
\[
\begin{bmatrix}
  3.7 \\
  0 \\
  0 \\
  0
\end{bmatrix}
\]
The model of PolITA

In Polynomial Interrupt Timed Automata (PolITA)

- variables are interrupt clocks acting as stopwatches ordered along hierarchical levels,
- guards are polynomial constraints and variables can be updated by polynomials.

Results

- Reachability is decidable in 2EXPTIME.
- The result still holds for several extensions.
- A restricted form of quantitative model checking is also decidable.
- The class PolITA is incomparable with the class SWA of Stopwatch Automata.
Outline

Polynomial Interrupt Timed Automata

Reachability using cylindrical decomposition

Algorithmic issues
PolITA: syntax

\[ A = (\Sigma, Q, q_0, X, \lambda, \Delta) \]

- Alphabet \( \Sigma \), finite set of states \( Q \), initial state \( q_0 \),
- set of clocks \( X = \{x_1, \ldots, x_n\} \), with \( x_k \) for level \( k \),
- \( \lambda : Q \rightarrow \{1, \ldots, n\} \) state level, with \( x_{\lambda(q)} \) the active clock in state \( q \),
- Transitions in \( \Delta \):

\[
\begin{array}{c}
q, k \quad \overset{g, a, u}{\longrightarrow} \quad q', k'
\end{array}
\]

- Guards: conjunctions of polynomial constraints in \( \mathbb{Q}[x_1, \ldots, x_n] \)
  \( P \succ 0 \) with \( \succ \) in \( \{<, \leq, =, \geq, >\} \), and \( P \in \mathbb{Q}[x_1, \ldots, x_k] \) at level \( k \).
PolITA: updates

From level $k$ to $k'$

**increasing level $k \leq k'$**

Level $i > k$: reset
Level $k$: unchanged or polynomial update $x_k := P$ for some $P \in \mathbb{Q}[x_1, \ldots, x_{k-1}]$
Level $i < k$: unchanged.

$x_2 > 2x_1^2$,

\[
\begin{align*}
(x_1 &:= x_1) \\
x_2 &:= x_1^2 - x_1 \\
x_3 &:= 0 \\
x_4 &:= 0
\end{align*}
\]

$q_1, 2 \rightarrow q_2, 4$
**PollTA: updates**

From level $k$ to $k'$

**increasing level $k \leq k'$**

Level $i > k$: reset
Level $k$: unchanged or polynomial update $x_k := P$ for some $P \in \mathbb{Q}[x_1, \ldots, x_{k-1}]$
Level $i < k$: unchanged.

Decreasing level

Level $i > k'$: reset
Otherwise: unchanged.
Examples

$A_2$ in dimension 2

\[ (2x_1 - 1)x_2^2 > 1, \quad b \]

\[ x_2 \leq 5 - x_1^2, \quad c \]

\[ x_1^2 \leq x_1 + 1, \quad a \]

$A_3$ in dimension 3

\[ x_1^2 + x_2^2 < 1 \]

\[ 0 < x_1 < 1 \]

\[ x_1 := 0 \]

\[ x_1^2 + x_2^2 + x_3^2 \geq 1 \]
**PollTA: semantics**

### Clock valuation

\[ \nu = (\nu(x_1), \ldots, \nu(x_n)) \in \mathbb{R}^n \]

### A transition system \( T_A = (S, s_0, \rightarrow) \) for \( A = (\Sigma, Q, q_0, X, \lambda, \Delta) \)

- **Configurations** \( S = Q \times \mathbb{R}^n \), initial configuration \( s_0 = (q_0, \nu_0) \) with \( \nu_0 = 0 \)
- **Time steps** from \( q \) at level \( k \): \( (q, \nu) \xrightarrow{d} (q, \nu + k \cdot d) \), only \( x_k \) is active, with all clock values in \( \nu + k \cdot d \) unchanged except \( (\nu + k \cdot d)(x_k) = \nu(x_k) + d \)
- **Discrete steps** \( (q, \nu) \xrightarrow{e} (q', \nu') \) for a transition \( e : q \xrightarrow{g,a,u} q' \) if \( \nu \) satisfies the guard \( g \) and \( \nu' = \nu[u] \)

### An execution

Alternates time and discrete steps

\[
(q_0, \nu_0) \xrightarrow{d_0} (q_0, \nu_0 + \lambda(q_0) \cdot d_0) \xrightarrow{e_0} (q_1, \nu_1) \xrightarrow{d_1} (q_1, \nu_1 + \lambda(q_1) \cdot d_1) \xrightarrow{e_1} \ldots
\]
The image contains a graph and text related to a formal semantics example. The graph represents a transition system with states $q_0, q_1,$ and $q_2$, and transitions labeled with conditions.

1. $x_1^2 > x_1 + 1, \quad a', \quad x_1 := 0$
2. $x_1^2 \leq x_1 + 1, \quad a$
3. $(2x_1 - 1)x_2^2 > 1, \quad b$
4. $x_2 \leq 5 - x_1^2, \quad c$

The graph has transitions labeled $a, b, c$ with corresponding conditions.

The text includes equations and inequalities:

\[
\begin{align*}
x_1^2 & > x_1 + 1, \\
x_1^2 & \leq x_1 + 1, \\
(2x_1 - 1)x_2^2 & > 1, \\
x_2 & \leq 5 - x_1^2,
\end{align*}
\]

The conditions are checked by regions on the graph.

Blue and green curves meet at real roots of $-2x^5 + x_1^4 + 20x_1^3 - 10x_1^2 - 50x_1 + 26$.

Additional conditions and states are given:

\[
\begin{align*}
a & : \quad x_1 = 1.2 \\
b & : \quad x_2^2 > \frac{1}{1.4} \\
c & : \quad x_2 \leq 3.56
\end{align*}
\]
Reachability problem for PolITA

Given $\mathcal{A} = (\Sigma, Q, q_0, X, \lambda, \Delta)$ and $q_f \in Q$

is there an execution from initial configuration $s_0 = (q_0, 0)$ to $(q_f, v)$ for some valuation $v$?

Build a finite quotient automaton $\mathcal{R}_A$

time-abstract bisimilar to $\mathcal{T}_A$:

- **states**: $(q, C)$ for suitable sets of valuations $C \subseteq \mathbb{R}^n$, where polynomials of $\mathcal{A}$ have constant sign (and number of roots),

- **time abstract transitions**: $(q, C) \rightarrow (q, \text{succ}(C))$ where $\text{succ}(C)$ is the time successor of $C$, consistent with time elapsing in $\mathcal{T}_A$,

- **discrete transitions**: $(q, C) \xrightarrow{e} (q', C')$ for $e : q \xrightarrow{g,a,u} q'$ in $\Delta$ if $C$ satisfies the guard $g$ and $C' = C[u]$, consistent with discrete steps in $\mathcal{T}_A$.

The sets $C$ will be cells from a cylindrical decomposition adapted to the polynomials in $\mathcal{A}$. 

Cylindrical decomposition: basic example

The decomposition starts from a set of polynomials and proceeds in two phases: **Elimination phase** and **Lifting phase**.

Starting from single polynomial $P_3 = x_1^2 + x_2^2 + x_3^2 - 1 \in \mathbb{Q}[x_1, x_2][x_3]$

**Elimination phase**

Produces polynomials in $\mathbb{Q}[x_1, x_2]$ and $\mathbb{Q}[x_1]$ required to determine the sign of $P_3$.

- First polynomial $P_2 = x_1^2 + x_2^2 - 1$ is produced.
  - If $P_2 > 0$ then $P_3$ has no real root.
  - If $P_2 = 0$ then $P_3$ has 0 as single root.
  - If $P_2 < 0$ then $P_3$ has two real roots.

- In turn the sign of $P_2 \in \mathbb{Q}[x_1][x_2]$ depends on $P_1 = x_1^2 - 1$.

**Lifting phase**

Produces partitions of $\mathbb{R}$, $\mathbb{R}^2$ and $\mathbb{R}^3$ organized in a tree of cells where the signs of these polynomials (in $\{-1, 0, 1\}$) are constant.
Lifting phase

Level 1: partition of $\mathbb{R}$ in 5 cells
$C_{-\infty} = ]-\infty, -1[ \cup C_{-1} = \{-1\}, C_0 = ]-1, 1[ \cup C_1 = \{1\}, C_{+\infty} = ]1, +\infty[$
Lifting phase

Level 2: partition of $\mathbb{R}^2$
Above $C_{-\infty}$: a single cell $C_{-\infty} \times \mathbb{R}$
Above $C_{-1}$: three cells
$\{-1\} \times ]-\infty, 0[ , \{(-1,0)\} , \{-1\} \times ]0, +\infty[ $

Level 1: partition of $\mathbb{R}$ in 5 cells
$C_{-\infty} = ]-\infty, -1[ , C_{-1} = \{-1\} , C_0 = ]-1, 1[ , 
C_1 = \{1\} , C_{+\infty} = ]1, +\infty[ $
Level 2 above $C_0$
Level 2 above $C_0$

\[ -1 < x_1 < 1 \]
\[ -\sqrt{1 - x_1^2} < x_2 < \sqrt{1 - x_1^2} \]
Level 2 above $C_0$

\[ C_{0,1} \quad \begin{cases} 
-1 < x_1 < 1 \\
 x_2 = \sqrt{1 - x_1^2} 
\end{cases} \]

\[ C_{0,0} \quad \begin{cases} 
-1 < x_1 < 1 \\
 -\sqrt{1 - x_1^2} < x_2 < \sqrt{1 - x_1^2} 
\end{cases} \]

\[ C_{0,-1} \quad \begin{cases} 
-1 < x_1 < 1 \\
 x_2 = -\sqrt{1 - x_1^2} 
\end{cases} \]
Level 2 above $C_0$

\[ C_{0,\infty} \quad \{ \begin{align*} -1 < x_1 < 1 \\ x_2 > \sqrt{1 - x_1^2} \end{align*} \]

\[ C_{0,1} \quad \{ \begin{align*} -1 < x_1 < 1 \\ x_2 = \sqrt{1 - x_1^2} \end{align*} \]

\[ C_{0,0} \quad \{ \begin{align*} -1 < x_1 < 1 \\ -\sqrt{1 - x_1^2} < x_2 < \sqrt{1 - x_1^2} \end{align*} \]

\[ C_{0,-1} \quad \{ \begin{align*} -1 < x_1 < 1 \\ x_2 = -\sqrt{1 - x_1^2} \end{align*} \]

\[ C_{0,-\infty} \quad \{ \begin{align*} -1 < x_1 < 1 \\ x_2 < -\sqrt{1 - x_1^2} \end{align*} \]
The tree of cells

\[\mathbb{R}^0\]

\[C_{-\infty} \quad C_{-1} \quad C_0 \quad C_1 \quad C_{+\infty}\]

\[\{\{-1\} \times \] -\infty, 0[\}

\[\{(-1, 0)\}\]

\[\{\{-1\} \times 0, +\infty[\]

\[\vdots\]

\[\{\{-1\} \times \)0, +\infty[ \times \mathbb{R}\]

\[C_{-\infty} \times \mathbb{R}^2\]

\[\vdots\]

\[C_{+\infty} \times \mathbb{R}^2\]
Building the quotient

partially, for $A_3$, using the sphere case with some refinements:

\[ x_1^2 + x_2^2 < 1 \]

\[ 0 < x_1 < 1 \]
\[ x_1 := 0 \]

\[ 0 < x_1 < 1 \]

\[ x_1^2 + x_2^2 + x_3^2 \geq 1 \]
Building the quotient

partially, for $A_3$, using the sphere case with some refinements:

\[ q_0, 0 < x_1 < 1, \]
\[ 0 < x_1 < 1, \]
\[ x_1^2 + x_2^2 + x_3^2 \geq 1, \]
\[ x_1^2 + x_2^2 < 1, \]
\[ q_0, R_0 = (x_1 = 0), R_1 = (0 < x_1 < 1), \]
Building the quotient

partially, for $A_3$, using the sphere case with some refinements:

level 1: $R_0 = (x_1 = 0)$, $R_1 = (0 < x_1 < 1)$,

level 2 above $R_1$: $R_{10} = (R_1, x_2 = 0)$, $R_{11} = (R_1, 0 < x_2 < \sqrt{1 - x_1^2})$,
Building the quotient

partially, for $A_3$, using the sphere case with some refinements:

level 1: $R_0 = \left( x_1 = 0 \right)$, $R_1 = \left( 0 < x_1 < 1 \right)$,
level 2 above $R_1$: $R_{10} = \left( R_1, x_2 = 0 \right)$, $R_{11} = \left( R_1, 0 < x_2 < \sqrt{1 - x_1^2} \right)$,
level 3 above $R_{11}$: $R_{110} = \left( R_{11}, x_3 = 0 \right)$, $R_{111} = \left( R_{11}, 0 < x_3 < \sqrt{1 - x_1^2 - x_2^2} \right)$,
$R_{112} = \left( R_{11}, x_3 = \sqrt{1 - x_1^2 - x_2^2} \right)$, $R_{113} = \left( R_{11}, x_3 > \sqrt{1 - x_1^2 - x_2^2} \right)$,
Building the quotient partially, for $A_3$, using the sphere case with some refinements:

\[ q_0 < x_1 < 1 \]
\[ x_1 := 0 \]
\[ 0 < x_1 < 1 \]
\[ x_1^2 + x_2^2 + x_3^2 \geq 1 \]
\[ x_1^2 + x_2^2 < 1 \]

Level 1: $R_0 = (x_1 = 0)$, $R_1 = (0 < x_1 < 1)$,
Level 2 above $R_1$: $R_{10} = (R_1, x_2 = 0)$, $R_{11} = (R_1, 0 < x_2 < \sqrt{1 - x_1^2})$,
Level 3 above $R_{11}$: $R_{110} = (R_{11}, x_3 = 0)$, $R_{111} = (R_{11}, 0 < x_3 < \sqrt{1 - x_1^2 - x_2^2})$,
$R_{112} = (R_{11}, x_3 = \sqrt{1 - x_1^2 - x_2^2})$, $R_{113} = (R_{11}, x_3 > \sqrt{1 - x_1^2 - x_2^2})$,
and back to level 1
Effective construction: Elimination

From an initial set of polynomials, the elimination phase produces in 2EXPTIME a family of polynomials $\mathcal{P} = \{\mathcal{P}_k\}_{k \leq n}$ with $\mathcal{P}_k \subseteq \mathbb{Q}[x_1, \ldots, x_k]$ for level $k$.

Some polynomials do not have always the same degree and roots. For instance, $B = (2x_1 - 1)x_2^2 - 1$ is of degree 2 in $x_2$ if and only if $x_1 \neq \frac{1}{2}$.

For $A_2$

Starting from $\{x_1, A\}$ and $\{x_2, B, C\}$ with $A = x_1^2 - x_1 - 1$ and $C = x_2 + x_1^2 - 5$ results in

- $\mathcal{P}_1 = \{x_1, A, D, E, F, G\}$,
- $\mathcal{P}_2 = \{x_2, B, C\}$,

with $D = 2x_1 - 1$, $E = x_1^2 - 5$, $F = -2x_1^5 + x_1^4 + 20x_1^3 - 10x_1^2 - 50x_1 + 26$, $G = 4(2x_1 - 1)^2$.
Effective construction: Lifting

To build the tree of cells in the lifting phase, we need a suitable representation of the roots of these polynomials (and the intervals between them), obtained by iteratively increasing the level.

A description like \( x_3 > \sqrt{1 - x_1^2 - x_2^2} \) cannot be obtained in general.

- A point is coded by “the \( n^{th} \) root of \( P \)”.
- The interval \([n, P), (m, Q)\] is coded by a root of \((PQ)'\).

This lifting phase can be performed on-the-fly, producing only the reachable part of the quotient automaton \( R_A \).
Conclusion

In the class PolITA

- Reachability is decidable in 2EXPTIME.
- Parameters can be included as ordinary variables!

Experiments

were produced by Rémi Garnier and Mathieu Huot (L3 students of ENS Cachan) who developed a prototype.

Future work

Extension to o-minimal decidable theories.
Conclusion

In the class PolITA

- Reachability is decidable in 2EXPTIME.
- Parameters can be included as ordinary variables!

Experiments

were produced by Rémi Garnier and Mathieu Huot (L3 students of ENS Cachan) who developed a prototype.

Future work

Extension to o-minimal decidable theories.

Thank you