Controller Synthesis for Hybrid Systems using SMT Solving

Ulrich Loup

AlgoSyn (GRK 1298)
Hybrid Systems Group
Prof. Dr. Erika Ábrahám

GRK Workshop 2009, Schloss Dagstuhl
Our model: hybrid system

- Discrete controller in a continuous setting
- Simple example:

\[ \dot{v} \in [0, 2] \]
Our model: hybrid system

- **Discrete** controller in a **continuous** setting
- Simple example:

\[ \dot{x} = v \]
\[ \dot{v} \in [0, 2] \]
\[ v \leq v_{\text{max}} \]

\[ \ell_0 \]

\[ v = 0 \]
\[ x = 0 \]

"accelerate"

\[ \dot{x} = v \]
\[ \dot{v} \in [-2, 0] \]
\[ v \geq 0 \]

\[ \ell_1 \]

"brake"
Our model: hybrid system

- Discrete controller in a continuous setting
- Simple example:

\[
\begin{align*}
\ell_0 & \quad \dot{x} = v \\
& \quad \dot{v} \in [0, 2] \\
& \quad v \leq v_{\text{max}} \\
\ell_1 & \quad \dot{x} = v \\
& \quad \dot{v} \in [-2, 0] \\
& \quad v \geq 0
\end{align*}
\]

“accelerate”

Parameter synthesis:

How is $v_{\text{max}}$ to be chosen such that the car can always be stopped in $\leq 0.2$ meters?
Our model: hybrid system

- **Discrete controller in a continuous setting**
- **Simple example:**

\[
\ell_0 \\
\begin{aligned}
\dot{x} &= v \\
v &\in [0, 2] \\
v &\leq v_{\text{max}}
\end{aligned}
\]

"accelerate"

\[
\ell_1 \\
\begin{aligned}
\dot{x} &= v \\
v &\in [-2, 0] \\
v &\geq 0
\end{aligned}
\]

"brake"

Parameter synthesis:

\[\exists v_{\text{max}} \exists v_0 \ldots \exists v_4 \ldots \left( \ldots \land x_4 - x_3 \leq 0.2 \land v_4 = 0 \land \ldots \right)\]
Satisfiability checking over the reals

<table>
<thead>
<tr>
<th>Given:</th>
<th>First-order formula $\varphi$ over $(\mathbb{R}, +, \cdot, &lt;)$.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question:</td>
<td>Is $\varphi$ satisfiable?</td>
</tr>
</tbody>
</table>

Theoretical results

- decidable [Tarski1948]
- upper bound for time complexity $2^{2^n}$ where $n$ is the number of variables [BrownDavenport2007]
Satisfiability checking over the reals

Given: First-order formula \( \varphi \) over \((\mathbb{R}, +, \cdot, <)\).
Question: Is \( \varphi \) satisfiable?

Theoretical results
- decidable [Tarski1948]
- upper bound for time complexity \( 2^{2^n} \) where \( n \) is the number of variables [BrownDavenport2007]

Approach
- exploit practical experience in satisfiability checking in propositional logic (SAT solving)
Satisfiability modulo theories (SMT)

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land \left( x - y + 1 = 0 \lor x + y - 1 = 0 \right) \right) \]
Satisfiability modulo theories (SMT)

\[ a \land b \land c \land (d \lor e) \]

SAT solver

Theory solver

\[ \exists x \ \exists y \ (x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land \left( x - y + 1 = 0 \lor x + y - 1 = 0 \right) ) \]
Satisfiability modulo theories (SMT)

∃x ∃y (x^2 - 1 = 0 ∧ y^2 - 1 = 0 ∧ x - 1 = 0 ∧ (x - y + 1 = 0 ∨ x + y - 1 = 0))?

a ∧ b ∧ c ∧ (d ∨ e)?

SAT solver

Theory solver

∃x ∃y (x^2 - 1 = 0 ∧ y^2 - 1 = 0 ∧ x - 1 = 0 ∧ (x - y + 1 = 0 ∨ x + y - 1 = 0))?
Satisfiability modulo theories (SMT)

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land (x - y + 1 = 0 \lor x + y - 1 = 0) \right) ? \]

SAT solver

\[ a \land b \land c \land (d \lor e) ? \]

Theory solver

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land (x - y + 1 = 0 \lor x + y - 1 = 0) \right) ? \]

- incremental
- minimal infeasible subset
Satisfiability modulo theories (SMT)

∃x ∃y ( x^2 - 1 = 0 ∧ y^2 - 1 = 0 ∧ x - 1 = 0 ∧ (x - y + 1 = 0 ∨ x + y - 1 = 0 ) )?

SAT solver

a ∧ b ∧ c ∧ (d ∨ e)?

Theory solver

∃x ∃y ( x^2 - 1 = 0 ∧ y^2 - 1 = 0 ∧ x - 1 = 0 ∧ x + y - 1 = 0 )

unsat

b ∧ c ∧ e

▷ incremental
▷ minimal infeasible subset
▷ backtracking
Satisfiability modulo theories (SMT)

\[
\exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land (x - y + 1 = 0 \lor x + y - 1 = 0) \right)
\]

- SAT solver
- Theory solver
- incremental
- minimal infeasible subset
- backtracking

unsat, unsatisfiability proof
Theory solver: existing implementations

Cylindrical algebraic decomposition (CAD)

- QEPCAD, Reduce, ...

Gröbner bases

- Maple, Mathematica, Singular, Maxima, CoCoA, Reduce, ...

Other methods

- Virtual substitution (Reduce)
- Interval arithmetic (Ariadne)

More on computer algebra: [Kaplan2005]
Theory solver: CAD

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \right) \]
Theory solver: CAD

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x - y + 1 = 0 \right) ? \]

- incremental
Theory solver: CAD

\[ \exists x \exists y \ ( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x + y - 1 = 0 )? \]

- incremental
- minimal infeasible subset
- backtracking
Theory solver: CAD

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x + y - 1 = 0 \right) ? \]

- incremental ∨
- minimal infeasible subset ?
- backtracking ∨
Theory solver: \textit{Gröbner} bases

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \]

has no solution \iff \[ q_1 p_1 + \cdots + q_k p_k = 1 \text{ for some polynomials } q_1, \ldots, q_k \]
Theory solver: **Gröbner bases**

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \quad \text{has no solution} \iff q_1 p_1 + \cdots + q_k p_k = 1 \quad \text{for some polynomials } q_1, \ldots, q_k \]

\[ \exists x \exists y \left( x^2 - 1 = 0 \land \{ x^2 - 1 \} \right) ? \]
Theory solver: *Gröbner* bases

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \]

has no solution \iff

\[ q_1 p_1 + \cdots + q_k p_k = 1 \]

for some polynomials \( q_1, \ldots, q_k \)

\[ \exists x \exists y \; (x^2 - 1 = 0 \land y^2 - 1 = 0) \]

\{\( x^2 - 1, y^2 - 1 \)\}

\[ \text{incremental } \checkmark \]
Theory solver: \textsc{Gröbner} bases

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \ \text{has no solution} \iff q_1 p_1 + \cdots + q_k p_k = 1 \text{ for some polynomials } q_1, \ldots, q_k \]

\[ \exists x \ \exists y \ ( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land \ )? \]

\[
\begin{align*}
\{x - 1, y^2 - 1\} \\
x^2 - 1 = (x + 1)(x - 1)
\end{align*}
\]

\[ \text{incremental } \checkmark \]
Theory solver: GRÖBNER bases

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \]
has no solution \(\iff \) \( q_1 p_1 + \cdots + q_k p_k = 1 \) for some polynomials \( q_1, \ldots, q_k \)

\[ \exists x \exists y \ ( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x - y + 1 = 0 )? \]

- incremental ✓
- minimal infeasible subset · ·

\[
1 = \frac{1}{3}(y^2 - 1) - \frac{1}{3}(y + 2)(x - 1) + \frac{1}{3}(y + 2)(x - y + 1)
\]

\{1\}
Theory solver: \texttt{GRÖBNER} bases

Mathematical background

\begin{align*}
& p_1 = 0 \land \ldots \land p_k = 0 \\
& \text{has no solution} \iff q_1 p_1 + \cdots + q_k p_k = 1 \text{ for some polynomials } q_1, \ldots, q_k
\end{align*}

\[ \exists x \exists y \ (x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x + y - 1 = 0) \]

\begin{itemize}
  \item incremental \checkmark
  \item minimal infeasible subset \checkmark
  \item backtracking \checkmark
\end{itemize}

\{x - 1, y^2 - 1\}
Theory solver: Gröbner bases

Mathematical background

\[ p_1 = 0 \land \ldots \land p_k = 0 \text{ has no solution} \iff q_1 p_1 + \cdots + q_k p_k = 1 \text{ for some polynomials } q_1, \ldots, q_k \]

\[ \exists x \exists y \left( x^2 - 1 = 0 \land y^2 - 1 = 0 \land x - 1 = 0 \land x + y - 1 = 0 \right) ? \]

- incremental ✓
- minimal infeasible subset · ·
- backtracking · ·

\[ 1 = -(y^2 - 1) - y(x - 1) + y(x + y - 1) \]
Future work

- Enhance theory solver:
  - Adjust the methods to the SMT framework (Redlog, Thomas Sturm, Universidad de Cantabria; Singular, Viktor Levandovskyy, RWTH Aachen).
  - Manage differential equations.
  - Generate unsatisfiability proofs.
  - Integrate interval arithmetic (Ariadne, Pieter Collins, CWI Amsterdam).

- Work on the applications:
  - Termination analysis (Computer science 2, RWTH Aachen)
  - SFB 686 “Niedertemperaturverbrennung”
References

