Optimization-Based Verification: An Overview

Stephen Prajna
California Institute of Technology

(Joint with A. Jadbabaie, G. J. Pappas, A. Rantzer)
Technological Disasters

Major power outage hits New York, other large cities

NEW YORK (CNN) -- Power began to flicker on late Thursday evening, hours after a major power outage struck simultaneously across dozens of cities in the eastern United States and Canada.

By 11 p.m. in New Jersey, power had been restored to all but 250,922 of the nearly 1 million customers who had been in the dark since just after 4 p.m., a spokesperson for Public Service Energy and Gas said.

Power was being restored in Pennsylvania and Ohio, too.

In New York City, however, Con Edison backed off previous predictions that

Ariane 5 Explosion

Foundational challenges and questions

1. What can we learn about complex biological networks from their technological counterparts, and vice versa?

2. What are the prospects for a deep and rigorous theoretical foundation for complex, embedded, networked systems of systems (SOS)?

• Biology and technology have deeply intertwined challenges
• Enormous progress is being made, but is poorly understood
• Start with the simplest, most familiar settings that we still don't understand (cell biology and Internet)
Properties of Interest

Focus today is on properties that are expressed in terms of reachability / temporal specifications.

- Some bad states are never reached (safety)
- Some good states will be reached (reachability/eventuality)
- Some states will be reached before some other states, etc.

In many cases, more natural than stability and optimality.
Status

- Many results from computer science, for discrete transition systems. Much less for continuous or hybrid systems.

- Standard tools in systems and control (e.g., Lyapunov functions) can handle only some special cases.

- Various methods have been recently proposed:
  - Continuous systems: quantifier elimination, set propagation, ....
  - Hybrid systems: abstraction, ....
  - Stochastic systems: discretization, randomization, ...
Some Challenges

- Common framework
- Automated computation
- Easily checkable proofs
- Scalability
Our Approach

- Use **algebraic proofs** and **deductive inference** to prove temporal properties.

- Framework is applicable to a very large class of systems:
  - Nonlinear
  - Hybrid
  - Uncertain
  - Constrained
  - Stochastic
  - Time-delay, etc.

- **Efficient computation** of proofs using convex optimization.
Outline of the Talk

- Background
- **Safety Verification**
- Reachability Verification
- Other Results (Hybrid, Stochastic, etc)
- Future Directions
Safety Verification – Barrier Certificate

Unsafe Set

\[ B(x) = 0 \]

\[ x(0) \in X_0 \]

\[ \dot{x} = f(x, d) \]

\[ d \in D \]

Find differentiable \( B(x) \) s.t.

\[ B(x) \leq 0 \quad \forall x \in X_0 \]

\[ B(x) > 0 \quad \forall x \in X_u \]

\[ \frac{\partial B}{\partial x} f(x, d) \leq 0 \quad \forall (x, d) \in X \times D \]
Computation of Barrier Certificate

- For polynomial systems, a polynomial barrier certificate $B(x)$, can be searched using sum of squares (SOS) programming.

- SOS polynomials:

  $p(x)$ is an SOS, if $\exists$ polynomials $f_1(x), \ldots, f_N(x)$, s.t.

  $$p(x) = \sum_{i=1}^{N} f_i^2(x).$$

  Equivalently, if $\exists$ monomial vector $Z(x)$ and p.s.d. matrix $Q$, s.t.

  $$p(x) = Z^T(x)QZ(x).$$

  (sufficient condition for non-negativity).

- Software: SOSTOOLS (http://www.cds.caltech.edu/sostools)
Example

\[ \dot{x}_1 = x_2 \]
\[ \dot{x}_2 = -x_1 + \frac{1}{3} x_1^3 - x_2 \]
\[ X = \square^2 \]
\[ X_0 = \{(x_1 - 1)^2 + x_2^2 \leq 0.5^2\} \]
\[ X_u = \{(x_1 + 1)^2 + (x_2 + 1)^2 \leq 0.4^2\} \]

Computation using SOS programming yields (after some rounding and re-check):

\[ B(x) = -13 + 7x_1^2 + 16x_2^2 - 6x_1^2x_2^2 - \frac{7}{6} x_1^4 - 3x_1x_2^3 + 12x_1x_2 - \frac{12}{3} x_1^3x_2 \]
Proof Correctness

For example, to check that $\frac{\partial B}{\partial x} f(x) \leq 0$, use the quadratic form

$$
-\frac{\partial B}{\partial x} f(x) = 30x_1 x_2 + 3x_1 x_2^3 - 22x_1^3 x_2 + 3x_2^4 + 20x_2^2 - 9x_1^2 x_2^2 + 4x_2 x_1^5 + 3x_1^4 x_2^2 + 12x_1^2 - 8x_1^4 + \frac{4}{3} x_1^6
$$

\[
\begin{bmatrix}
    x_2 \\
x_2^2 \\
x_1 \\
x_1 x_2 \\
x_1^2 x_2 \\
x_1^3
\end{bmatrix}^T
\begin{bmatrix}
    20 & 0 & 15 & 0 & -7.5 & -5 \\
    0 & 3 & 0 & 1.5 & 0 & 0 \\
    15 & 0 & 12 & 0 & -6 & -4 \\
    0 & 1.5 & 0 & 6 & 0 & 0 \\
    -7.5 & 0 & -6 & 0 & 3 & 2 \\
    -5 & 0 & -4 & 0 & 2 & 4/3
\end{bmatrix}
\begin{bmatrix}
    x_2 \\
x_2^2 \\
x_1 \\
x_1 x_2 \\
x_1^2 x_2 \\
x_1^3
\end{bmatrix} \geq 0
\]
Outline of the Talk

- Background
- Safety Verification
- Reachability Verification
- Some Other Results
- Future Directions
Lesson from Finite State Systems

Barrier:

Maximize $B_{14} - B_0$, subject to

\[
\begin{align*}
B_1 - B_0 &\leq 0 \\
B_2 - B_0 &\leq 0 \\
\vdots \\
B_{14} - B_{13} &\leq 0
\end{align*}
\]

Safe if obj $> 0$.

Compare to:

\[
\begin{align*}
B(x) &\leq 0 \quad \forall x \in X_0 \\
B(x) &> 0 \quad \forall x \in X_u \\
\frac{\partial B}{\partial x} f(x,d) &\leq 0 \quad \forall (x,d) \in X \times D
\end{align*}
\]
Lesson from Finite State Systems

Barrier:
Maximize $B_{14} - B_0$, subject to

$B_1 - B_0 \leq 0$
$B_2 - B_0 \leq 0$
...
$B_{14} - B_{13} \leq 0$

Safe if obj > 0.

Flow:
Minimize 0, subject to

$$LP \text{ duality}$$

$$1 = \rho_{0,1} + \rho_{0,2} + \rho_{0,3}$$
$$\rho_{11,14} + \rho_{11,12} + \rho_{13,14} = 1$$
$$\rho_{0,1} = \rho_{1,4}, \quad \text{and so on}$$

Reachable if LP is feasible.
Assume $X$ is bounded, and $X_0$ has non-empty interior.
Let $\varepsilon$ be a positive number.

Find cont. diff. $\rho(x)$ s.t.

$$\int_{X_0} \rho(x)dx \geq 0,$$

$$\rho(x) \leq -\varepsilon \quad \forall x \in \partial X \setminus \partial X_r,$$

$$\nabla \cdot (\rho f)(x) \geq \varepsilon \quad \forall x \in X \setminus X_r.$$
Outline of the Talk

- Background
- Safety Verification
- Reachability Verification
- Other Results (Hybrid, Stochastic, etc)
- Future Directions
Hybrid Systems

Mode 1
Inv(1)

Mode 2
Inv(2)

Mode 3
Init(1)

\[ \frac{dx}{dt} = f_1(x, d) \]
\[ d \in D(1) \]

Guard(1,2)

\[ \frac{dx}{dt} = f_2(x, d) \]
\[ d \in D(2) \]

Guard(2,3)

Reset(1,2)
Find a collection \( \{ B_l(x) : l = 1, \ldots, L \} \) s.t.

\[
B_l(x) \leq 0 \quad \forall x \in Init(l)
\]

\[
B_l(x) > 0 \quad \forall x \in Unsafe(l)
\]

\[
\frac{\partial B_l}{\partial x} f_l(x, d) \leq 0 \quad \forall (x, d) \in Inv(l) \times D(l)
\]

\[
B_{l'}(x') - B_l(x) \leq 0 \quad \forall x' \in Reset(l, l')(x), \quad x \in Guard(l, l')
\]
Stochastic Systems

What is the reach probability???

\[ dx = f(x)dt + g(x)dw_t \]

Prajna, Jadbabaie, Pappas (CDC 2004)
Stochastic Systems

\[ B(x) = 1 \]

\[ B(x) = \gamma < 1 \]

\[ x(0) \in X_0 \]

\[ dx = f(x)dt + g(x)d\omega_t \]

Unsafe Set \( X_u \)

Find non-negative \( B(x) \) s.t.

\[ B(x) \leq \gamma \quad \forall x \in X_0 \]

\[ B(x) \geq 1 \quad \forall x \in X_u \]

\[ \frac{\partial B}{\partial x} f(x) + g^T(x) \frac{\partial^2 B}{\partial x^2} g(x) \leq 0 \quad \forall x \in X \]

\[ \Rightarrow \text{Prob(Reach)} \leq \gamma \]

Prajna, Jadbabaie, Pappas (CDC 2004)
Networked control systems:

\[
\dot{x}(t) = f(x(t), x(t - r))
\]

Infinite dimensional state space!!

Prajna & Jadbabaie, (CDC 2005)
Networked control systems:

\[ \dot{x}(t) = f(x(t), x(t - r)) \]

Infinite dimensional state space!!

Use *functional* of state:

\[
B(x_t) = B_0(x(t)) + \int_{-r}^{0} B_1(\theta, x(t), x(t + \theta))d\theta + \int_{-r}^{0} \int_{t}^{t} B_2(x(\eta))d\eta d\theta
\]

Conditions for safety can be derived.

Prajna & Jadbabaie, (CDC 2005)
Existence (Converse) Theorem

There is $B(x)$ s.t.

- $B(x) \leq 0 \quad \forall x \in X_0$
- $B(x) > 0 \quad \forall x \in X_u$
- $\frac{\partial B}{\partial x} f(x) \leq 0 \quad \forall x \in X$

Safety property holds for system $\dot{x} = f(x)$, sets $X_0, X_u, X$

Yes, under some reasonable technical conditions.

Proof: Use strong duality between convex programs for safety and reachability.

Prajna & Rantzer, (IFAC 2005)
Outline of the Talk

- Background
- Safety Verification
- Reachability Verification
- Other Results (Hybrid, Stochastic, etc)
- Future Directions
Hierarchical Large-Scale Verification

Subsystem verification: (conform to protocols???)

• Automated verification using SOS programming.
Hierarchical Large-Scale Verification

System-wide verification

- Possibility for symbolic and structured proof

(Lesson from the stability analysis of internet congestion control)
From Control Algorithm to Implementation

**Control Algorithm**

- Differential equations, difference equations, logic-based control, etc.

**Control Implementation**

- Embedded controllers, C++ code, DSP, etc.

**Certificates/Proofs**

- Barrier certificates, density functions, Lyapunov functions, etc.

**Should carry over!!**
## Conclusions

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Our Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common framework</td>
<td>Encompasses a very large class of systems.</td>
</tr>
<tr>
<td>Automated computation</td>
<td>SOS programming, software tools are available.</td>
</tr>
<tr>
<td>Easily checkable proofs</td>
<td>Algebraic proofs, easy to check.</td>
</tr>
<tr>
<td>Scalability</td>
<td>Potential both at small – medium scale (numerical) and large scale (symbolic, structured).</td>
</tr>
</tbody>
</table>