Worshhop on Verification of Autonomous Systems
Techniques for Practical Verification

Jana Tumova
Research interests

• Past
  • Parallel and distributed probabilistic model checking
  • Quantitative model checking of systems with degradation
  • Temporal logic analysis and control of piecewise affine systems

• Ongoing
  • Model checking-based robot motion and action planning
  • Model checking-based multi-agent control
Model checking-based planning

System

\[ \dot{x} = f(x, u) \quad x(0) = x_{\text{init}} \]

Abstraction

Model

\[ \mathcal{T} = (Q, Q_0, \text{Act}, \rightarrow) \]

Behavior specification

Temporal logic formula

Which of the model executions satisfy the formula?

Projection

Here is one

\[ Q^* \rightarrow \text{Act} \]

There is none
Model checking-based robot mission and motion planning

System
\[
\dot{p}(t) = u(t) \quad p(t) \in P \subseteq \mathbb{R}^2 \quad u(t) \in U \subseteq \mathbb{R}^2 \\
p(0) = P_1
\]

Behavior specification
Periodically visit \( P_1, P_4, P_8 \) and never enter \( P_{10} \)

Model checking-based robot mission and motion planning

System
\[ \dot{p}(t) = u(t) \quad p(t) \in P \subseteq \mathbb{R}^2 \quad u(t) \in U \subseteq \mathbb{R}^2 \]
\[ p(0) = P_1 \]

Behavior specification
Periodically visit \( P_1, P_4, P_8 \) and never enter \( P_{10} \)

Linear Temporal Logic (LTL) formula
\[ \Diamond \varphi P_1 \land \Diamond \varphi P_4 \land \Diamond \varphi P_8 \land \Box \neg P_{10} \]

Model checking-based robot mission and motion planning

**System**

\[
\dot{p}(t) = u(t) \quad p(t) \in P \subseteq \mathbb{R}^2 \quad u(t) \in U \subseteq \mathbb{R}^2
\]

\[p(0) = P_1\]

**Behavior specification**

Periodically visit \(P_1, P_4, P_8\) and never enter \(P_{10}\)

**Linear Temporal Logic (LTL) formula**

\[\mathcal{GF} P_1 \land \mathcal{GF} P_4 \land \mathcal{GF} P_8 \land \mathcal{G} \neg P_{10}\]

Research challenges

- Input user-friendliness
  - structured English, graphical representation
- Computational complexity and scalability
  - receding horizon, fragments of logics
- Dynamic environments and imprecisions of sensors and actuators
  - nondeterministic, probabilistic, partial observable models
  - reactive re-planning
- Multi-agent systems
  - task decomposition, decentralized planning
- Optimality
  - weighted models
- Specification infeasibility
  - least-violating planning, model repair, analysis of reasons
1 Highlight: Least violating sampling-based motion planning algorithm

Least-violating Control Strategy Synthesis with Safety Rules in HSCC 2013, with Gavin Hall, Sertac Karaman, Emilio Frazzoli, Daniela Rus
Incremental Sampling-based Algorithm for Minimum-violation Motion Planning in CDC 2013, with Luis Reyes-Castro, Pratik Chaudhari, Sertac Karaman, Emilio Frazzoli, Daniela Rus