Formal methods for robot planning

Jana Tumova
Associate Professor
Division of Robotics, Perception and Learning
Why formal methods?

Rigorous techniques for

specification

development, verification, analysis of systems

How do we tell robots what to do?

How do we ensure that they behave as expected?

Jana Tumova, tumova@kth.se
Why temporal logics and formal synthesis?

Temporal logics
- rich
- rigorous
- resemblance to natural language

Formal synthesis

How do we tell robots what to do?

How do we ensure that they behave as expected?
Temporal logic for mission and motion objectives

- Keep patrolling the three offices.
  \[ GF(A) \land GF(B) \land GF(C) \]
- Whenever you spot danger, go directly to the staircase and wait for “all clear” signal before continuing.
  \[ G(danger \Rightarrow X(staircase \cup all\_clear)) \]
- Make sure to recharge at least every 10 minutes.
  \[ GF_{[0,10]}recharge \]
- At all times, stay within 5 meters from the wi-fi router.
  \[ G(Dist(robot, router) \leq 5) \]
Why temporal logics and formal synthesis?

Temporal logics
• rich
• rigorous
• resemblance to natural language

Formal synthesis
• correct-by-design plan

How do we tell robots what to do?
How do we ensure that they behave as expected?
Formal synthesis

System

Model \( \dot{p}(t) = u(t) \)

Abstraction

Formal synthesis

Objective

Patrol offices A and B.

Temporal logic specification

A correct-by-design plan

There is no correct-by-design plan

Jana Tumova, tumova@kth.se
**Formal synthesis (2009)**

System

Model

Abstraction

DTS, NTS, Petri nets

Temporal logic specification

LTL, GR(1)

Objective

Patrol offices A and B.

Formal synthesis

A correct-by-design plan

There is no correct-by-design plan

Some seminal works:
[Kress-Gazit et al, TRO 2009, Kloetzer and Belta, TAC 2008]
Formal synthesis (2013)

System

Model

Abstraction

multi-agent, partially unknown and dynamic environments,…

Non-linear, with disturbance,…

DTS, NTS, Petri nets, roadmaps, trees, WTS, MDPs,…

Formal synthesis

Objective

temporal goals, additional optimization criteria, deadlines

User-friendly interface

Linguistic, graphical

Temporal logic specification

LTL, GR(1), sc-LTL, PCTL, MTL,…

A correct-by-design plan

There is no correct-by-design plan

Jana Tumova, tumova@kth.se
Formal synthesis (today)

System
- Non-linear, with disturbance,…

Model
- Abstraction
  - DTS, NTS, Petri nets, roadmaps, trees, WTS, MDPs,…

Objective
- multi-agent, partially unknown and dynamic environments,…
- temporal goals,
- additional optimization criteria, deadlines
- spatio-temporal goals and constraints,…

User-friendly interface
- Linguistic, graphical

Temporal logic specification
- LTL, GR(1), sc-LTL, PCTL, MTL, STL,…

Formal synthesis
- A correct-by-design plan
- There is no correct-by-design plan

Jana Tumova, tumova@kth.se
Formal synthesis, integrated

Multi-robot coordination for dynamic production assistance
Three challenges of formal synthesis

1. "The no-plan challenge"

2. "The no-good-model challenge"

3. "The interaction challenge"

System

Model

Abstraction

Formal synthesis

A correct-by-design plan

Objective

User-friendly interface

Temporal logic specification

There is no correct-by-design plan

Jana Tumova, tumova@kth.se
1. The no-plan challenge

Objective
Obey the traffic rules:
- Do not cross the full lane
- Stay in the right lane
- Do not enter the construction zone
- Do not enter sidewalk
...

Temporal logic specification
LTL over finite traces

There is no correct-by-design plan
All the traffic rules cannot be obeyed simultaneously
1. The no-plan challenge

**Objective**
Obey the traffic rules:
- Do not cross the full lane
- Stay in the right lane
- Do not enter the construction zone
- Do not enter sidewalk
...

**Model, abstraction**

**System**

**Temporal logic specification**
LTL over finite traces

**A plan as correct as possible**

The traffic rules are violated only for the absolutely necessary, for the necessary time
Quantitative evaluation of LTL

Assume a transition system from RRT* or other abstraction

Level of violation $\lambda(\text{trace, LTL formula})$: the time duration associated with the discrete transitions that need to be removed to make the trace satisfy the LTL formula, weighted by the penalty

[Tumova et al HSCC 2013]

Jana Tumova, tumova@kth.se
Minimum-violation automata-based FS

Abstraction (TS)

\[ \psi_1 \quad \ldots \quad \psi_N \]

FA

\[ \text{Enhance} \]

Weighted FA

Weighted product automaton

The shortest accepting run

The minimally violating plan

The runs of the product automaton map to the traces of the transition system.
The weights along the run of the product automaton determine the level of violation.
The shortest run of the product maps onto the minimally violating trace of the model.

[Tumova et al HSCC 2013]

Jana Tumova, tumova@kth.se
MV-RRT*

- Incrementally build
- Incrementally update
- Optimality criterion

RRT*

- weighted tree
- shortest path
- distance

MV-RRT*

- weighted product automaton
- minimally violating path
- primarily level of violation, then distance

[Reyes-Castro et al CDC 2013]

Jana Tumova, tumova@kth.se
MV-RRT* in autonomous driving

Limited sensing:

Violation of $\theta$, for time duration $d$ results in penalty $P = p_1 \cdot d$

Multi-vehicle settings:

Critical Area

Sensing area of green vehicle

The no plan challenge under uncertainty

Objective
Common sense/RSS:
• Keep a safe distance $\Delta(v_e, v_l)$
• ...

Temporal logic specification
$G(\Delta(v_e, v_l) - (p_l - p_e) > 0)$

The severity of violation, the probability of violation, and the level of uncertainty are taken into account
Risk-aware planning in autonomous driving

- Safety specification: $G(h(x(t)) > 0)$
- Severity function: $\ell_h(x) = \begin{cases} \ell(h(x(t))), & h(x(t)) > 0 \\ 0, & \text{otherwise} \end{cases}$
- Severity of violation: $L = l_h(\hat{x})$
- Risk: $E[L]$
- Risk-aware planning

[Nyberg et al IV 2021]
Signal Temporal Logic spatial robustness

\[ G(1 - \text{dist}(\sigma, M) > 0) \]

See [Donze and Maler, LNCS, 2013]
STL as a preference specification
STL-guided autonomous exploration

AEP

AEP + STL \( G(\text{dist}(\sigma, M) - 1 > 0) \)

Guiding Autonomous Exploration with Signal Temporal Logic

Fernando S. Barbosa, Daniel Duberg, Patric Jensfelt and Jana Tumova

[Barbosa et al RA-L 2019]

Jana Tumova, tumova@kth.se
2. The no-good-model challenge
Safe multi-step feedback motion primitives for non-holonomic system with bounded disturbance

- Divide the input space into regions & linearize
- Linearization introduces error
- The error can be corrected in $k$ steps
- The motion primitives can be chained and refined

[Tajvar et al. ISSR 2019, CASE 2020, IROS 2021]
LTL planning with motion primitives

System

Motion primitives

Objective

LTL specification

BA

Backward reachability tree

Modified A* refine

heuristics

A correct-by-design plan

[Tajvar et al. CASE 2020]

Jana Tumova, tumova@kth.se
Towards safe data-driven contact-rich manipulation

[Mitsioni et al Humanoids 2021]

Jana Tumova, tumova@kth.se
The interaction challenge
Correct-by-design and socially acceptable plan

System → Model, Abstraction → Formal synthesis → A plan

Objective

Social acceptability, perceived safety

Goals, constraints, preferences

Temporal logic specification
Correct-by-design and socially acceptable plan

System
  \[\xrightarrow{\text{Interactions}}\]
  \[\xrightarrow{\text{Model, Abstraction}}\]
  \[\xrightarrow{\text{Formal synthesis}}\]
  A plan

Objective
  Social acceptability, perceived safety
  \[\xrightarrow{\text{STL with probabilistic predicates}}\]
  Temporal logic specification

Linard et al CASE 2020, IROS 2021
I wish I had time to talk also about

• Provable safety vs. perceived safety

• Assumption-guarantee synthesis

• Decentralized multi-agent coordination with temporal logic specifications
Take-aways

• Temporal logics and formal synthesis to address
  – How do we tell robots what to do?
  – How do we ensure that they behave as expected?

• Rigorous, but not rigid:
  – Can be used to provide guarantees if that is desired and possible
  – No need to freeze if a correct-by-design plan does not exist
  – Support for preferences, not just mission/safety-critical goals
The future: Moving forward to the wild

• Well-defined mathematical objectives → “Soft” objectives
• Guarantees → Risk-awareness
• Manually created models and specifications → Data-driven models and specifications
• FS or learning → FS and learning
  RL with TL goals, RL with TL constraints,
• Component-view → System-view

Jana Tumova, tumova@kth.se
Thanks!

Pouria Tajvar, Truls Nyberg, Fernando Barbosa, Wei Wang, Albin Larsson Forsberg, Georg Schuppe, Alexis Linard, Christian Pek, Jesper Karlsson