Localizing Inconsistencies in Unsynthesizable Specifications

Vasu Raman
Cornell University

Joint work with Cameron Finucane, Gangyuan Jing and Hadas Kress-Gazit
Synthesizable

Unsynthesizable

? 

Hybrid Controller
• **Patrol the aisles.**
• If you find a missing item, call the manager.
• Avoid aisles with spills.

*Jing, Finucane, Raman and KG, ICRA 2012*
• **Patrol the aisles.**

group Corners is r1, r2, r3, r4
if you are not activating call_manager then visit all Corners
do look_leftright if and only if
  you are not activating call_manager and
  you were in (between r1 and r2 or between r3 and r4)

• **If you find a missing item, call the manager.**

call_manager is set on see_missingitem and reset on head_tapped
if you are activating call_manager then stay there

• **Avoid aisles with spills.**

spill_top is set on (r1 or r2) and see_spill and reset on false
spill_bottom is set on (r3 or r4) and see_spill and reset on false

if you are activating spill_top then always not between r1 and r2
if you are activating spill_bottom then always not between r3 and r4
**TYPES OF PROBLEMS**

\[ \varphi = \varphi_e \Rightarrow \varphi_s \]

- Specification Unsatisfiable:

  "Start in Deck. Always stay there. Go to kitchen."

- Specification Unrealizable:

  \[ \exists \text{Environment} \models \varphi_e \text{ s.t. } \text{Robot} \not\models \varphi_s \]

  "Start in Deck. If you see person stay there. Go to kitchen."

- Trivial solution:

  \[ \forall \text{Robot} \models \varphi \]

  "Always person and not person."

*Raman and Kress-Gazit, CAV 2011, ICRA 12, T-RO 12*
## Cases of (Un)synthesizability

\[ \varphi = \varphi_e \Rightarrow \varphi_s \]

### ROBOT \( (\varphi_s) \)

<table>
<thead>
<tr>
<th>Unsatisfiable</th>
<th>Unrealizable</th>
<th>Realizable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsatisfiable</td>
<td>Trivial automaton/ Unexpected behaviour</td>
<td>Trivial automaton/ Unexpected behaviour</td>
</tr>
<tr>
<td>Unrealizable</td>
<td>No automaton</td>
<td>Unexpected behaviour</td>
</tr>
<tr>
<td>Realizable</td>
<td>No automaton</td>
<td>No automaton</td>
</tr>
</tbody>
</table>

---

*Raman and Kress-Gazit, CAV 2011, ICRA 12, T-RO 12*
**Unrealizability**

The environment can force the robot into:

- **deadlock** (a state with no next robot move)

\[

\square(\pi_e \Rightarrow \neg \bigcirc \pi_s) \\
\land \quad \square(\pi_e \Rightarrow \bigcirc \pi_s)
\]

- **livelock** (trapped in states that do not satisfy the goals)

\[

\square(\pi_e \Rightarrow \neg \bigcirc \pi_s) \\
\land \quad \square \Diamond \pi_s
\]
Two Cases

Unsatisfiability/unrealizability can be:

- **Single-step** (involving current and next time steps only)

  \[ \Box(p_e \Rightarrow \neg \bigcirc \pi_s) \]
  \[ \land \Box(p_e \Rightarrow \bigcirc \pi_s) \]

  - Easy to detect from transition relation

- **Multi-step** (over multiple time steps)
  - Requires looking at environment counterstrategy

Raman and Kress-Gazit, CAV 2011, ICRA 12, T-RO 12
ENVIRONMENT COUNTERSTRATEGY

• Environment winning strategy
  • First proposed for debugging hardware designs
    [Konighofer, Hofferek and Bloem, 2009]

• At every time step, provides inputs to force the robot into deadlock or livelock.

• *If the environment winning strategy is “TRUE”, the robot is unsatisfiable.

Raman and Kress-Gazit, CAV 2011, ICRA 12, T-RO 12
Feedback to the User

• Distinguish between unsatisfiable, unrealizable and trivial
• Highlight subset of sentences
• Unrealizable spec: Playing a game with the user; tool is the environment, user is the robot
# Initial conditions
2 Env starts with false
3 Robot starts with false
4 Robot starts in porch
5
6 # Assumptions about the environment
7 If you were in porch then do not hazardous_item and do not person
8
9 # Define robot safety including how to pick up
10 Do pick_up if and only if you are sensing hazardous_item and you are not activating carrying_item
11 If you did not activate carrying_item then always not porch
12
13 # Define when and how to radio
14 Do radio if and only if you are sensing person
15 If you are activating radio or you were activating radio then stay there
16
17 # Patrol goals
18 If you are not activating carrying_item and you are not activating radio then visit dining
19 Visit porch

**ERROR:** Specification was unrealizable.

**RESULT**
System highlighted goal(s) unrealizable

No automaton synthesized.
Interactive Game for System Unrealizability

Allows the user to explore the cause of unrealizability

User (robot) vs. tool (environment)

Example

Start in the deck, go to the porch. If you see fire, avoid the kitchen. If you see a person, avoid the living room. fire and person cannot be seen together.
Interactive Game for System Unrealizability

<table>
<thead>
<tr>
<th></th>
<th>fire</th>
<th>person</th>
<th>Region</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>False</td>
<td>False</td>
<td>p8 (deck)</td>
</tr>
</tbody>
</table>

Current environment state:
- Fire
- Person

Please choose your response:
- Stay in region p8 (deck)

Actuator states:

Internal propositions:
Specification Analysis

Boolean Satisfiability

Counterstrategy

Identify deadlock/livelock

Highlight spec. sentences

Interactive game

LTL Synthesis

Synthesizable

Unsynthesizable

Feedback to the user

Change the specification

(FSA)

Hybrid Controller

- Boolean Satisfiability
- Counterstrategy
- Identify deadlock/livelock
- Highlight spec. sentences
- Interactive game

Raman and Kress-Gazit, CAV 2011, ICRA 12, T-RO 12
BUT...What We Get (extreme case)

- **Patrol the aisles.**

  group Corners is r1, r2, r3, r4
  if you are not activating call_manager then visit all Corners
  do look_leftright if and only if
  you are not activating call_manager and
  you were in (between r1 and r2 or between r3 and r4)

- **If you find a missing item, call the manager.**

  call_manager is set on see_missingitem and reset on head_tapped
  if you are activating call_manager then stay there

- **Avoid aisles with spills.**

  spill_top is set on (r1 or r2) and see_spill and reset on false
  spill_bottom is set on (r3 or r4) and see_spill and reset on false

  if you are activating spill_top then always not between r1 and r2
  if you are activating spill_bottom then always not between r3 and r4
BUT...What We Want

- Patrol the aisles.

  group Corners is r1, r2, r3, r4
  if you are not activating call_manager then visit all Corners
  do look_leftright if and only if
    you are not activating call_manager and
    you were in (between r1 and r2 or between r3 and r4)

- If you find a missing item, call the manager.

  call_manager is set on see_missingitem and reset on head_tapped
  if you are activating call_manager then stay there

- Avoid aisles with spills.

  spill_top is set on (r1 or r2) and see_spill and reset on false
  spill_bottom is set on (r3 or r4) and see_spill and reset on false

  if you are activating spill_top then always not between r1 and r2
  if you are activating spill_bottom then always not between r3 and r4
**Granularity of Feedback**

\[ \varphi = (\varphi_e \Rightarrow \varphi_s) \]

\[ = (\varphi^i_e \land \varphi^t_e \land \varphi^g_e \Rightarrow \varphi^i_s \land \varphi^t_s \land \varphi^g_s) \]

Analysis will highlight ENTIRE subformula if it contributes
**GOAL:**
Highlight the MINIMAL cause of unsynthesizability

- Find the smallest subset of formulas that cause unsynthesizability
  - a minimal unsynthesizable “core”
Tools for finding the “core”

UNSATISFIABLE SPECIFICATIONS

• SAT solvers (for single-step unsatisfiability)
  • Encode as SAT problem, find unsatisfiable core

• Bounded Model Checking (multi-step)
  • Gives counterexample of shortest possible length
  • Use this depth to “unroll” LTL into a SAT formula, then find unsatisfiable core
  • Map it back to original specification

HOW CAN WE DO BETTER?

Work in progress!
HOW CAN WE DO BETTER?

*Work in progress!*

Tools for finding the "core"

UNREALIZABLE SPECIFICATIONS

- efficient searching for minimal subset
- search all subsets (e.g. delta debugging)
OTHER CAUSES OF UNSYNTHESIZABILITY

Continuous execution in the physical domain
- Automaton OK, execution not OK
- More on this later today