Strategy & Counter-Strategy
Guided Refinement of GR(1)
Temporal Logic Specifications

Salar Moarref

Joint work with Rajeev Alur and Ufuk Topcu

ExCape Meeting

March 2014
Example
Example
Reactive Synthesis

- Specification
  - Formal Language: LTL, CTL, ...
- Game
- System
- Environment
- Realizable?
  - Yes: strategy
  - No: counter-strategy
Realizable?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Apple
- Robot
- Basket
- Devil
Realizable?

<table>
<thead>
<tr>
<th>No!</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Apple
- Robot
- Basket
- Devil emoji
Realizable?

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="No!" /></td>
<td><img src="image" alt="Robot" /></td>
<td><img src="image" alt="Devil" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Motivation

- Developing correct and complete formal specification
  - Challenging and tedious
  - Initial specifications often unrealizable
- Unrealizable specification
  - Often due to inadequate environment assumptions
  - Cannot be executed or simulated
  - Counter-strategies?
Motivation

- Developing correct and complete formal specification
  - Challenging and tedious
  - Initial specifications often unrealizable
- Unrealizable specification
  - Often due to inadequate environment assumptions
  - Cannot be executed or simulated
  - Counter-strategies?
Motivation

• Developing correct and complete formal specifications
  • Challenging and tedious
  • Initial specifications often unrealizable
• Unrealizable specification

Goal: automatically refining the constraints over the environment by adding assumptions in order to achieve realizability

• Counter-strategies?
Applications

- Constructing an environment model
- Giving the user an insight into the specification
- Correcting the specification
- Constructing the interface specification
- And more..
Refining Interface Specifications

- Global realizable specification
  \[ \phi = \phi_e \rightarrow \phi_s \]

- Decomposed specifications
  \[ \phi_1 = \phi_{e_1} \rightarrow \phi_{s_1} \]
  \[ \phi_2 = \phi_{e_2} \rightarrow \phi_{s_2} \]

- Find refinements such that
  \[ \text{Refined specification are both realizable} \]
Specification Refinement

- Unrealizable specifications
  - Inferring LTL formulas from counter-strategy
  - Refining environment assumptions
- Realizable specifications
  - Inferring LTL formulas from strategy
  - Refining system guarantees
Counter-Strategy Guided Refinement

1. Specification
2. Generating candidates
3. Infer LTL formulas
4. Realizable
5. Counter-strategy
6. Choose & add
7. Subset of variables

流程图如下：
- 从 Specification 到 Realizable
- 从 Realizable 到 Done
- 从 Realizable 到 Counter-strategy
- 从 Counter-strategy 到 Infer LTL formulas
- 从 Infer LTL formulas 到 Choose & add
- 从 Choose & add 到 Specification

条件：
- $\neg \varphi$
- $\mathcal{M}_{cs} \models \varphi$
- $\mathcal{M}_{cs}$
Example: Candidate Assumptions

- Inferred Formula
  \[ \Diamond \Box (\text{Loc}_{obj} = \text{Loc}_{apple}) \]

- Candidate assumption
  \[ \Box \Diamond (\text{Loc}_{obj} \neq \text{Loc}_{apple}) \]
Example: Candidate Assumptions

- Inferred Formula
  - $\diamondsuit \Box (\text{Loc}_{\text{obj}} = \text{Loc}_{\text{apple}})$

- Candidate assumption
  - $\Box \diamondsuit (\text{Loc}_{\text{obj}} \neq \text{Loc}_{\text{apple}})$
Example: Candidate Assumptions

- Inferred Formula
  - $\Diamond \Box (Loc_{obj} = Loc_{apple})$

- Candidate assumption
  - $\Box \Diamond (Loc_{obj} \neq Loc_{apple})$
Inferring LTL formulas

Abstract

Abstraction

Patterns Synthesis

Instantiation
Inferring LTL formulas

Strongly connected components including cycle

$\Diamond \Box (q_1 \lor q_2)$

Abstraction

Patterns Synthesis

Instantiation
Inferring LTL formulas

\[ \Diamond \Box (q_1 \lor q_2) \Rightarrow \Diamond \Box ((r \land c) \lor (\neg r \land c)) = \Diamond \Box c \]
Specification Refinement Example

- Suggested refinement
  - $\psi_1 = \square \Diamond (Loc_{obj} \neq Loc_{apple})$
  - $\psi_2 = \square \Diamond (Loc_{obj} \neq Loc_{basket})$

- Refined specification
  - $(\varphi_e \land \psi_1 \land \psi_2) \rightarrow \varphi_s$

- Realizable
Refining Interface Specification

<table>
<thead>
<tr>
<th></th>
<th>R1</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>R2</td>
</tr>
</tbody>
</table>

Diagram showing a grid with arrows connecting R1 and R2.
Refining Interface Specification

- Refine the specifications

\[
\psi = \Box \Diamond (\text{Loc}_{R_1} \neq \text{Loc}_{apple}) \\
\phi_{e_1} \rightarrow (\phi_{s_1} \land \psi) \\
(\phi_{e_2} \land \psi) \rightarrow \phi_{s_2}
\]
Current and Future Work

- Taking advantage of multiplicity of generated candidates
- Improving the scalability
- Automatically finding good subset of variables
- Extension to more general subsets of LTL
- Synthesizing the interface specification between components
Conclusion

• Counter-strategy guided refinement of GR(1) specifications

• Refining the unrealizable specification by adding assumptions

• Refining the realizable specification by adding guarantees

• Simple GR(1) formulas

  • Easy to understand and validate by the user

• As weak as possible in the specified structure
References


Generating candidates

Choose & add

\neg \varphi

Subset of variables

Infer LTL formulas

\mathcal{M}_{cs} \models \varphi

Counter-strategy

Realizable

Yes → Done

No → Generating candidates

\mathcal{M}_{cs}
Resources

- http://2.bp.blogspot.com/-z_QUSIm3jwo/UiXSAMnLz0I/AAAAAAAYeY/U4HNps5l5sU/s1600/basket_1.gif
- http://www.mayjesuschristbepraised.com/pictures/02/devil-icon.png
Inferring Behaviors as LTL formulas

- LTL formulas of special form which hold over all runs of the (counter)-strategy

- $\Box\Diamond \psi, \Box \psi$ and $\Box(\psi \rightarrow \bigcirc \psi')$

- Discovering implicit guarantees of a strategy

- $\Diamond \Box \psi, \Diamond \psi$ and $\Diamond(\psi \land \bigcirc \psi')$

- Restricting the system or environment by adding their complement
User Input

- A subset of variables for each pattern type
- may contribute to unrealizability problem
- are underspecified

- Smaller subset of variables

- Simpler formulas

- More restrictive

- $\square (c \lor r)$ vs. $\square c$
Properties of Patterns and Assumptions

- Synthesized patterns are
  - Minimal
    - Removing any state leads to unsatisfiable formulas
    - Strongest formulas of the specified form
- Synthesized assumptions
  - Rule out the counter-strategy
  - Restricts the environment as weakly as possible