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

Salar Moarref

Joint work with Rajeev Alur and Ufuk Topcu

Formal Methods in Computer-Aided Design

October 2013
Example
Example
Example

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Robot" /></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>

2
Example
Example
Example

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image" alt="Robot" /></td>
<td><img src="image" alt="Devil" /></td>
</tr>
<tr>
<td><img src="image" alt="Apple" /></td>
<td></td>
<td></td>
</tr>
<tr>
<td><img src="image" alt="Basket" /></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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>
</tbody>
</table>

- A robot
- A basket
- An apple
- A devil
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="Apple" /></td>
</tr>
<tr>
<td><img src="image" alt="Basket" /></td>
<td><img src="image" alt="Robot" /></td>
<td><img src="image" alt="Devil" /></td>
</tr>
</tbody>
</table>
Realizable?
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 specification
- 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..
Counter-Strategy Guided Refinement

1. Specification
2. Generating candidates
3. Counter-strategy
4. Patterns synthesis
5. Subset of variables
6. Realizable

Flow:
- Choose & add
- Yes → Done
- No → Realizable
- Realizable
- Realizable → Done
- Realizable → Choose & add
- Choose & add
- Choose & add → Realizable
- Realizable → Yes or No
Counter-Strategy

- A winning strategy for the environment
- Represented as Moore machine
Candidate Assumptions

- Infer LTL formulas which hold over all runs of the counter-strategy
- Choose one and add its complement as assumption to the specification
  - Strengthen the environment assumptions
- Remove the counter-strategy from admissible environment behaviors
Example: Candidate Assumptions

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

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

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

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

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

- **Candidate assumption**
  - \( \Box \Diamond (\text{Loc}_{obj} \neq \text{Loc}_{apple}) \)
Patterns

- LTL formulas of the form
  - $\Diamond \Box \psi$, $\Diamond \psi$, and $\Diamond (\psi \rightarrow \Box \psi')$
  - Hold over *all* runs of the *abstraction* of counter-strategy
  - Synthesized using graph search algorithms
Generalized Reactivity (1)

- Specifications of the form $\varphi = \varphi_{env} \rightarrow \varphi_{sys}$
- Safety: $\square \varphi$
- Transition: $\square (\varphi \rightarrow \bigcirc \varphi')$
- Fairness/liveness: $\square \Diamond \varphi$
- Efficient algorithms for realizability and synthesis [Piterman 06]
- Expressive [Bloem 12]
Eventually Always Patterns

- Complement of liveness/fairness formulas
Eventually Always Patterns

* Complement of liveness/fairness formulas

\[ q_0 \to q_1 \to q_2 \to q_3 \to q_0 \]

- Strongly connected components including cycle
Eventually Always Patterns

- Complement of liveness/fairness formulas

\[ \Diamond \square (q_1 \lor q_2 \lor q_3) \]

Strongly connected components including cycle
Synthesizing Candidate Assumptions

$q_1 \iff S_1 \iff c \land r$

State predicate: a truth assignment to the variables in the state
Synthesizing Candidate Assumptions

* Replace states in patterns with state predicates

* $\Diamond \Box (q_1 \lor q_2 \lor q_3)$ leads to

* $\Diamond \Box ((c \land r) \lor (c \land \neg r) \lor (c \land r)) = \Diamond \Box c$

* Complement the formula

$\Box \Diamond \neg c$
Example

- Suggested refinement
  - $\psi_1 = \Box \Diamond (\text{Loc}_{obj} \neq \text{Loc}_{apple})$
  - $\psi_2 = \Box \Diamond (\text{Loc}_{obj} \neq \text{Loc}_{basket})$

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

- Realizable
Case Study

* Suggested refinement

  * \( \psi_1 = \Box \Diamond (\text{Loc}_{\text{obj}} \neq \text{Loc}_{\text{apple}}) \)

  * \( \psi_2 = \Box \Diamond (\text{Loc}_{\text{obj}} \neq \text{Loc}_{\text{basket}}) \)

  * \( \psi_3 = \Box \Diamond (\text{Loc}_{\text{obj}} \notin \text{second column}) \)

  * \( \psi_4 = \Box \Diamond (\text{Loc}_{\text{obj}} \notin \text{gray cells}) \)

* Refined specification

  * Realizable
More Case Studies

- Lift controller
  - Refinement found by processing one counter-strategy
  - Three candidate assumptions generated
  - Generating candidates: 0.6% of total time

- ARM’s advanced bus architecture
  - Refinement found by processing one counter-strategy
  - Five candidate assumptions generated
  - Generating candidates: 28.6% of total time
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
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
  - Simple GR(1) formulas
  - Easy to understand and validate by the user
- As weak as possible in the specified structure
References


Generating candidates

Subset of variables

Choose & add

Patterns synthesis

Counter-strategy

Realizable

Yes

Done

No
Resources

- http://2.bp.blogspot.com/-z_OUSIm3jwo/UiXSAMnLz0I/AAAAAAAAYeY/U4HNps51S_U/s1600/basket_1.gif
- http://www.mayjesushchristbepraised.com/pictures/02/devil-icon.png