LIBRARY-ORIENTED SYSTEM DESIGN USING LTL-BASED ASSUME-GUARANTEE CONTRACTS

Antonio Iannopollo

ExCAPE Annual Meeting, 10-11 June 2013
A Framework for Contract Based Design

• Contract Based Design gives formal keys to compositional design

• LTL-based Assume/Guarantee contracts can express both system requirements and system component interfaces

• Lots of tools for dealing with LTL, we need to coordinate all of them in a coherent design flow
A/G Contracts

• A contract is characterized by
  • Set P of ports, \( P = I \cup O \)
  • Set A of assumptions
  • Set G of guarantees

• A/G contract theory specifies
  • Composition of contracts
  • Refinement relations
  • Compatibility and Consistency

• An assume-guarantee LTL formula \( (\varphi_A \rightarrow \varphi_G) \), used in synthesis, can be seen as a contract

\[
C = (\varphi_A, \varphi_G)
\]
Design Flow

Contract Library Design

Map contracts to system plant

Connect & Compose contracts

Check refinements (properties)

Synthesize automata
Key Points

- Library of contracts is tightly related to a given platform
  - Each contract specifies a component or a subset of components
- Library is hierarchically organized, according to the refinement partial order
  - More abstract contracts can be used to improve performance of some design steps
- System requirements are expressed as contracts
  - The designed system meets a requirement if the final composite contract is a refinement of that requirement
- Interface with external tools for LTL-sat check and synthesis
Collaboration

• User-friendly library definition process
  • Structured English-to-LTL work from Cornell
Collaborations

- User-friendly library definition process
- Structured English-to-LTL work from Cornell

Antonio Iannopollo
6/10/13
Collaboration

- User-friendly library definition process
- Structured English-to-LTL work from Cornell
Collaboration

- User-friendly library definition process
  - Structured English-to-LTL work from Cornell

- Application to the robotic scenario
  - Interfacing existing tools and techniques
THANK YOU