Specifying Protocols Using Scenarios and Requirements

Christos Stergiou
with Rajeev Alur, Milo Martin, Mukund Raghothaman, Stavros Tripakis, Abhishek Udupa
Problem

• Specify distributed protocols in intuitive ways
• Traditionally used communicating FSMs
• Scenarios or MSCs are more intuitive
• Describe different behaviors of the protocol
• Can we use scenarios to specify protocols?
Scenario Example

- Two processes: Sender and Receiver
- Sequence of message exchanges
Methodology

• Protocol skeleton
  – Processes to synthesize, their interfaces

• Environment
  – Known processes

• Specification
  – Set of formal requirements

• Scenarios
  – Example behaviors of the system, type of MSCs
Alternating-Bit Protocol

• Protocol skeleton
  – Sender and receiver
• Environment
  – Forward and backward channels, timer
• Specification
  – Absence of deadlocks, safety and liveness
• Scenarios
  – Four behaviors
ABP Scenarios
ABP Requirements

Safety monitor

Liveness monitor
From Scenarios to Automata

Process

S0: empty message history
S1: a!
S2: a! b?

S0 = S2

S0 initial
S1 a!
S1 initial
S2 b?
S2 initial
Automata Completion

Partial automata using first scenario

Correct implementation
Synthesis from Scenarios

• Representative set of scenarios
• Cover all states of implementation
• Complete partial automata using requirements
• ABP
  – First scenario is sufficient
  – All scenarios need smaller set of requirements
Conclusion

• New methodology for describing distributed protocols
• Synthesis problem as automata completion
• Two preliminary techniques
• Cache-coherence protocols
• Questions?