Specification, Design and Verification of Distributed Embedded Systems

MURI Kickoff

Eric Klavins, Assistant Professor

Electrical Engineering
University of Washington
Seattle, WA
The UW MURI Team

Eric Klavins, co-PI

J.M. McNew, Graduate Student
   Works on embedded graph grammars

David Thorsley, Postdoctoral Scholar
   Ph.D. in 2006 from U. Michigan
   Fault Diagnosis in Stochastic DES
   Starts at UW in September 2006

Other UW graduate students: Josh Bishop, Crystal Flores,
Nils Napp and Fayette Shaw.
Bottom Up Design

Product description

• Correct by construction methods for factory design.

• Low level continuous behaviors are verified and have well-defined interfaces.

• Results in a complex, interconnected system of systems.


Klavins, HSCC 2000
Embedded Systems

- Broadly construed, an *embedded system*, is any programmable part of a larger interconnected dynamical system.

- The *context* into which a system is embedded may be natural, artificial, deterministic, non-deterministic, stochastic, dynamic, friendly or adversarial.

- In a complex and networked environment, interactions may be *intentional* or *induced* by the environment.

UW programmable parts embedded in an uncertain, stochastic, networked environment.
Challenges

- Build systems without program/environment duality
- Understand the dynamic locality of subsystems
- Bottom up: Verify locally, synthesize globally
- Build scalable algorithms and proof methods

UW programmable parts embedded in an uncertain, stochastic, networked environment.
Graph Grammars: A Modeling Formalism

Program, $\Phi$

$$i \ x \ w \ \rightarrow \ i_1 - c$$

Klavins, Ghrist, Lipsky. TAC 2006.
Graph Grammars: A Modeling Formalism

Program, $\Phi$

$i \ w \rightarrow i_1 - c$

Environment, $\Psi$

$i \ l \rightarrow i - a$

Klavins, Ghrist, Lipsky. TAC 2006.
Graph Grammars: A Modeling Formalism

Program, $\Phi$

\[
i \, w \rightarrow i_1 - c
\]

\[
\cdot
\]

\[
\cdot
\]

Environment, $\Psi$

\[
i \, l \rightarrow i - a
\]

\[
\cdot
\]

\[
\cdot
\]

For what $\Psi$ is $\Phi$ [ $\Psi$ correct, robust, etc.?]

Klavins, Ghrist, Lipsky. TAC 2006.
Expressibility

Graph rewrite systems are Turing complete.

Graph rewrite systems model

• Communications protocols
• Distributed databases
• Reconfigurable networks

We are working on the following extensions

• **Stochastic** Graph Grammars
• **Embedded** Graph Grammars with continuous control modes
• **Optimization-based** methods for behavior synthesis
• **Model-checking** as a compliment to bottom up verification

The Nondeterministic Setting

The reachability graph

Klavins, Ghrist & Lipsky, TAC 2006.

Model checking

McNew & Klavins, ACC 2006.
- Graph Grammar Specific Collapses
- Canonical Initial Graphs

Composition of grammars

Bishop & Klavins, CDC 2006.
- Correct by construction!
Hierarchical Composition of Communication Protocols

\( \Phi_1, \Phi_2 : \) Grammars describing different output behaviors

\( \Phi_1 \mathcal{E}_q \Phi_2 : \) Composed grammar

\[ q(G(t)) \] behave like \( \Phi_1 \)
\[ : q(G(t)) \] behave like \( \Phi_2 \)

value of \( q(G(t)) \) is locally estimated

“glue” rules perform estimation and consensus

Can be further interconnected via properties \( q_i \) of \( \Phi_i \).

Bishop & Klavins, CDC 2006
Stochasticity

Self-Assembling Robots

Optimal Rules for Self-Assembly
Klavins, Burden and Napp, RSS 2006.

Optimization of Individual Behaviors
Klavins et al, in preparation.

Programmable DNA Motors
Bishop, Shaw and Klavins in preparation.
Geometry and Dynamics

Extend the idea of rewrite to include local continuous state.

\[ g(x_{i_1}, \ldots, x_{i_k}) : L \rightarrow R \]

Add continuous dynamics that depend on local geometry.

\[ u : \Gamma_i(x, G) \rightarrow U_i \]

The underlying hybrid automaton is vast, but has a regular structure.

\[ ||x_a - x_b|| < r : i \ w \rightarrow i_1 - c \]

What are the proof techniques?

- McNew & Klavins, Embedded Graph Grammars
- McNew, Egerstedt & Klavins, in Progress
Example: Distributed Rendezvous
Uses Lexicographic Composition of Lyapunov Functions!

Goal
Distribute Robots among rendezvous points

Constraints
Limited communication range
Must maintain connectivity

Motion control
Maintain connectivity
Move toward goals

Communication Protocols
Cycle removal
Distribute robots
Research Directions

Build a **palette** of verified low-level behaviors
- Low level protocols
- Continuous Control Modes

Build a high-level **behavior specification language** with
(embedded, stochastic, etc) graph grammatical semantics

Build tools that allow
- **Model checking** and testing of proposed grammars
- Automated search for (sub) **Lyapunov** functions
- **Robustness** analysis of $\Phi \ [ \Psi(\epsilon) $

Test on
- **Programmable Parts**
- MVWT
- Alice/Bob