Robust compositions of embedded systems

George J. Pappas
Departments of ESE and CIS
University of Pennsylvania
pappasg@ee.upenn.edu
Component-based modeling and synthesis

The main (controller) synthesis equation

\[ A \parallel X \cong B \]

or a more relaxed version...

\[ A \parallel X \leq B \]

<table>
<thead>
<tr>
<th>Discrete</th>
<th>Continuous</th>
<th>Embedded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Models</td>
<td>Finite state automata</td>
<td>Dynamical</td>
</tr>
<tr>
<td>Composition</td>
<td>( L(A \parallel B) = L(A) \cap L(X) )</td>
<td>Feedback</td>
</tr>
<tr>
<td>Equivalence</td>
<td>( A \cong B \iff L(A) = L(X) )</td>
<td>Asymptotic</td>
</tr>
<tr>
<td>Order</td>
<td>( A \leq B \iff L(A) \subseteq L(X) )</td>
<td>?</td>
</tr>
</tbody>
</table>
From exact to robust

Exact relationships useful but fragile for binary answers
   Asymptotic relationships are useless for interacting embedded systems

When dealing with the physical world, we need approximations
   Labeled Markov processes (Desharnais et. al., TCS 2004)
   Quantitative transition systems (de Alfaro et. al., ICALP 2004)
   Metric transition systems (Girard and Pappas, 2005)

From exact towards approximate embedded system relationships
   Enable larger system “compression”
   Quantify error/complexity tradeoffs
   Provide measures of robustness

Challenges
   What are the right metrics (industry help is needed)? Can we compute them?
   Are approximate relationships compositional?
Define metrics for (metric) transition systems:

\[
\begin{align*}
    d_L(S_1, S_2) &= 0 \quad \text{iff} \quad L(S_1) \subseteq L(S_2) \\
    d_L(S_1, S_2) &= 0 \quad \text{iff} \quad L(S_1) = L(S_2) \\
    d_S(S_1, S_2) &= 0 \quad \text{iff} \quad S_1 \leq S_2 \\
    d_B(S_1, S_2) &= 0 \quad \text{iff} \quad S_1 \equiv S_2
\end{align*}
\]

How can we define such metrics and how are they related?

\[
\begin{align*}
    A \parallel X &\equiv B \\
    \text{Compute} \quad d(A \parallel X, B)
\end{align*}
\]

\[
\begin{align*}
    S_1 \equiv S_2 \Rightarrow S \parallel S_1 &\equiv S \parallel S_2 \\
    d(S_1, S_2) < \varepsilon \Rightarrow d(S \parallel S_1, S \parallel S_2) < \varepsilon
\end{align*}
\]