Generalized Synchronization Trees

James Ferlez†, Rance Cleaveland§ and Steve Marcus†

§Department of Computer Science †Department of Electrical and Computer Engineering

THIRTY YEARS OF SYSTEMS RESEARCH EXCELLENCE

INSTITUTE FOR SYSTEMS RESEARCH
A. JAMES CLARK SCHOOL OF ENGINEERING

Past: Algebraic Reasoning about Computing Processes

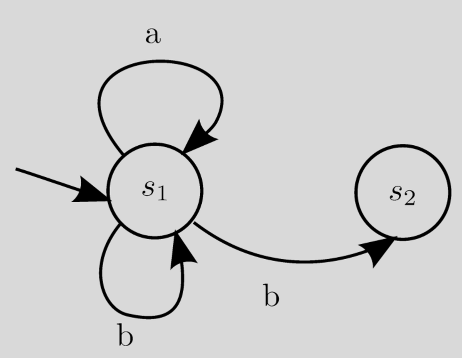
Milner [2] devised synchronization trees for labeled transition systems (Process Algebra):

Definition:

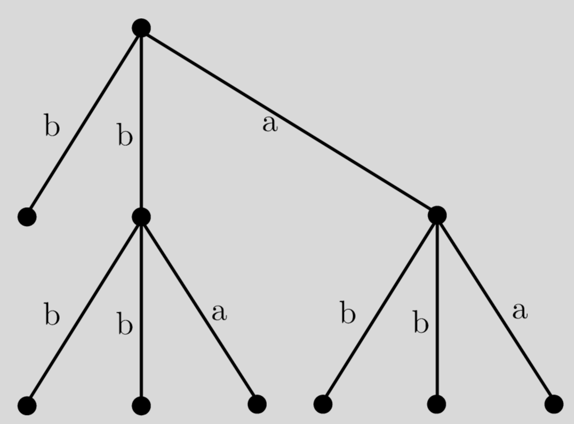
A **Synchronization Tree** (ST) over a set of labels L is a tuple $(V, E, \mathcal{L})$ where:

- (V, E) is an undirected, connected, acyclic graph (V, E) with a specially identified root node r *and*
- $\mathcal{L}$ is a function $\mathcal{L}: E \rightarrow L \cup \{\varepsilon\}$.

- Each path in the tree is an execution of the transition system.
- Nondeterminism: multiple children with the same label.
- In a synchronization tree, every execution leads to another synchronization tree (self-similarity).
- Composition: algebraic operations on synchronization trees.



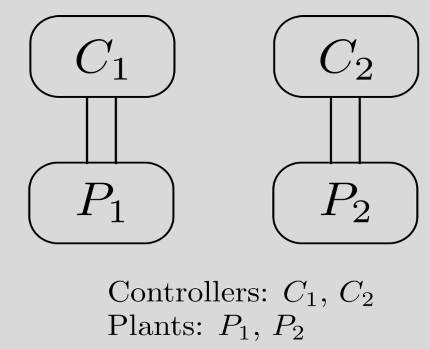
Labeled Transition System

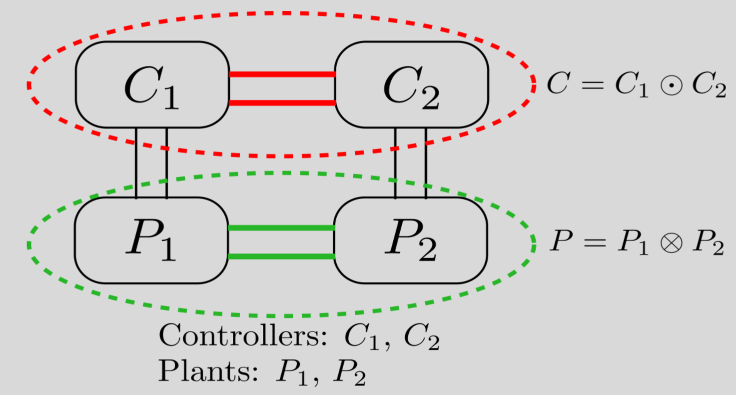


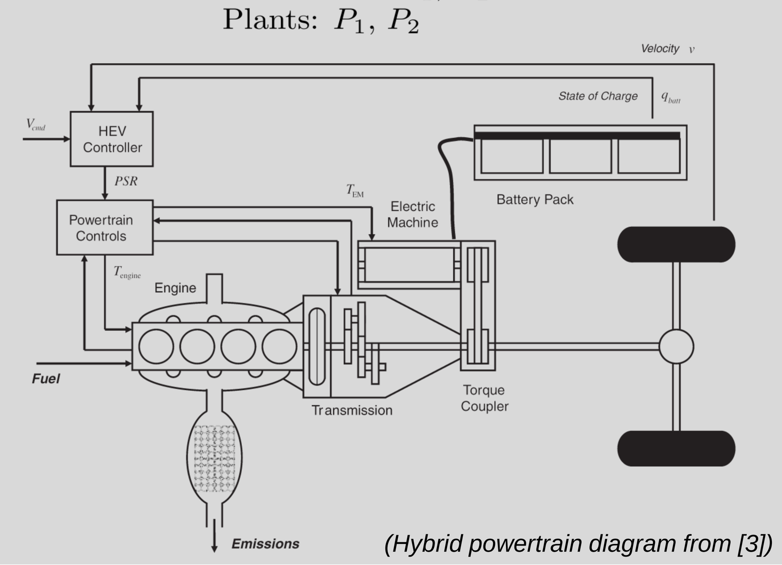
Synchronization Tree

Future: Compositional Design of Control Systems

Reason about complicated systems based on the models/behaviors of components:







(Hybrid powertrain diagram from [3])

Whole-system analysis

Current Research: Generalized Synchronization Trees

Extending Process Algebra

Goal: extend Process Algebra to model cyber-physical systems (CPSs).

Common restrictions in CPS modelling frameworks:

- transitions (choices) are **discretized** *or*
- composition is **synchronous**.

Generalizing the process algebraic approach promises a rich CPS-modelling framework in which:

- choice can be **continuous** *and*
- rich, **asynchronous composition** operations are natural.

This research is a new point of contact between the disciplines of computer science and control theory.

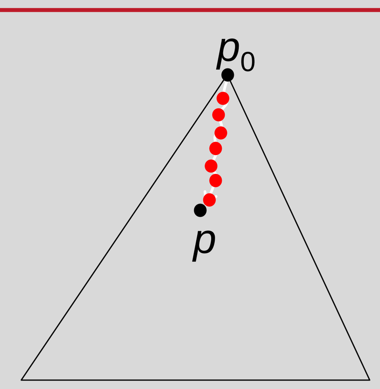
Generalizing Trees

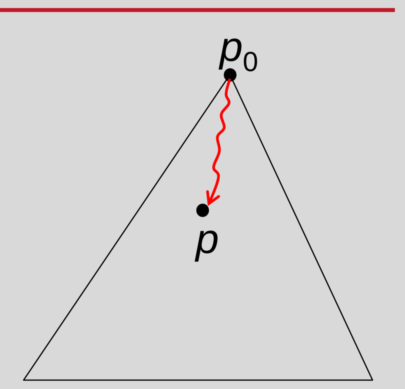
Definition:

A **tree** is a partially ordered set $(P, \leq)$ with the following properties:

1) There is a $p_0 \in P$ such that $p_0 \leq p$ for all $p \in P$. p_0 is the *root* of the tree;
2) For each $p \in P$, the set $\{p' \in P \mid p' \leq p\}$ is linearly ordered by $\leq$.

The nodes in a ST have a natural tree partial order: each node can be associated with a sequence of transitions, and two nodes are ordered if one's sequence of transitions is a prefix of the other's.





Generalized Synchronization Trees (GSTs)

Definition:

A **Generalized Synchronization Tree** [1] over a set of labels L is a tree $(P, \leq)$ along with a labeling function $\mathcal{L}: P \backslash \{p_0\} \rightarrow L$.

- In a synchronization tree, the nodes form a discrete GST tree with the canonical partial order.

Simulation for GSTs

In the following, let $G_P = (P, p_0, \leq_P, \mathcal{L}_P)$ and $G_Q = (Q, q_0, \leq_Q, \mathcal{L}_Q)$ be two GSTs.

Definition:

A **trajectory** (of G_P) starting from $p \in P$ and ending at $p' \in P$ is the set $(p, p'] \stackrel{\text{def}}{=} \{r \in P | p \leq r \leq p'\}$.

Definition:

A trajectory $(p, p']$ of G_P is **order equivalent** to a trajectory $(q, q']$ of G_Q if there exists an order preserving bijection $\lambda: (p, p'] \rightarrow (q, q']$ such that $\mathcal{L}_Q(\lambda(r)) = \mathcal{L}_P(r)$ for all $r \in (p, p']$. λ is called an **order equivalence** between $(p, p']$ and $(q, q']$.

Definition:

G_P **weakly simulates** G_Q if there is a relation $R \subseteq P \times Q$ such that $(p_0, q_0) \in R$ and

- For any $(p, q) \in R$ and $q' \geq q$, there exists a $p' \geq p$ such that $(p', q') \in R$, and there is an order equivalence between $(p, p']$ and $(q, q']$.

Simulation for GSTs (continued)

A new, semantically different kind of simulation for GSTs:

Definition:

G_P **strongly simulates** G_Q if there is a relation $R \subseteq P \times Q$ such that $(p_0, q_0) \in R$ and

- For any $(p, q) \in R$ and $q' \geq q$, there exists a $p' \geq p$ such that $(p', q') \in R$, and there is an order equivalence λ between $(p, p']$ and $(q, q']$ such that $(r, \lambda(r)) \in R$ for each $r \in (p, p']$.

Proposition:

If G_P and G_Q are STs, then G_P strongly simulates G_Q if and only if it weakly simulates G_Q.

Theorem:

There exist GSTs G_P and G_Q such that G_P weakly simulates G_Q but G_P doesn't strongly simulate G_Q.

References and Funding Information

NSF Grant: CNS-1446665. CPS Breakthrough Grant: "Compositional Modeling of Cyber-Physical Systems."

NSF Grant: CCF-0926194. "RECOVERY: Collaborative Research: Next-Generation Model Checking and Abstract Interpretation with a Focus on Embedded Control and Systems Biology." (CMACS)

[1] J. Ferlez, R. Cleaveland, and S. Marcus. *Generalized synchronization trees*. In FOSSACS 2014, volume 8412 of Lecture Notes in Computer Science, pages 304–319, Grenoble, France, 2014. Springer-Verlag.

[2] Robin Milner. *A Calculus of Communicating Systems*. Number 92 in Lecture Notes in Computer Science. Springer-Verlag, 1980.

[3] Edward Dean Tate Jr, Jessy W. Grizzle, and Huei Peng. *Shortest path stochastic control for hybrid electric vehicles*. Int. J. Robust Nonlinear Control, 18(14):1409-1429, December 2007.

NSF Grants CNS-1446665 and CCF-0926194