Generalized Synchronization Trees

James Ferlez†, Rance Cleaveland§ and Steve Marcus†

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

UNIVERSITY OF MARYLAND

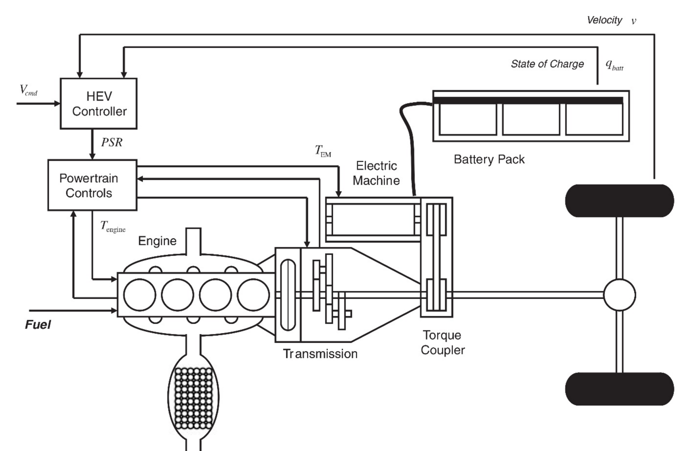
The Institute for Systems Research

CPS Program Information

- CPS Breakthrough: ***Compositional Modeling of Cyber-Physical Systems*** *(NSF Grant: CNS-1446665)*
- PIs: Rance Cleaveland and Steve Marcus

Cyber-Physical Systems are Compositional

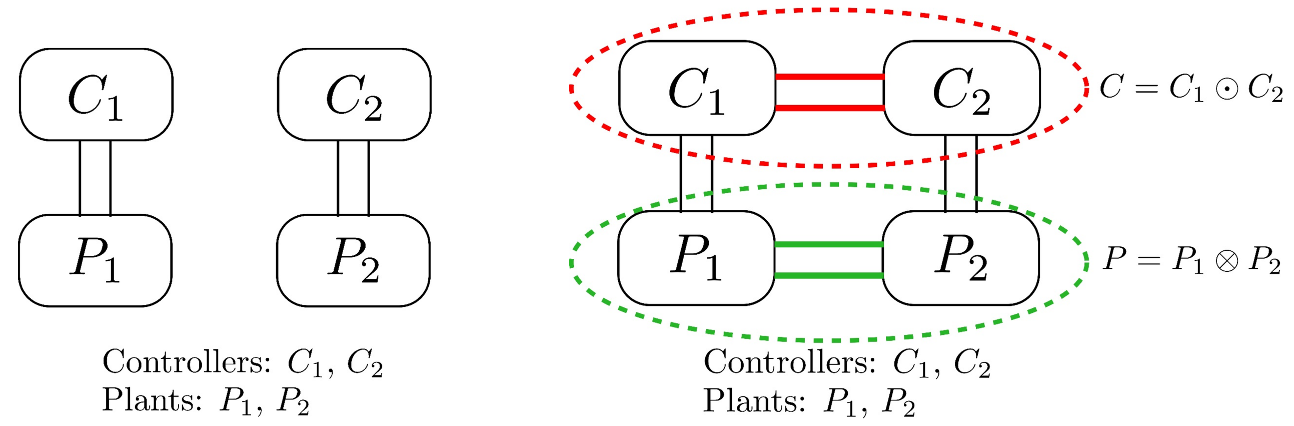
- For example, hybrid powertrains (see e.g. [6]):



(Diagram taken from [6])

Compositional Reasoning for CPSs

We need to reason about a complicated system based on models/behaviors of components:



- Can the composed system be analyzed in a rigorous way?

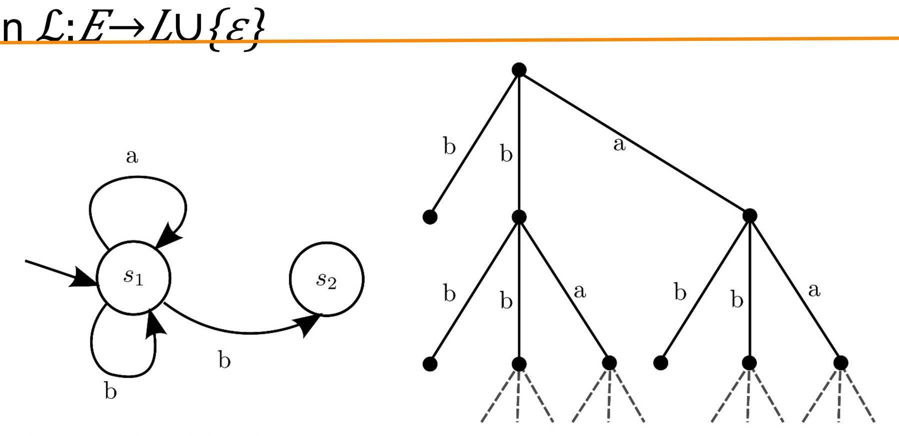
Algebraic Composition of Transitions Systems

Famously, Milner [4] devised synchronization trees for labeled transition systems (subsequently known as 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 $\mathcal{L}: E \to L \cup \{\varepsilon\}$



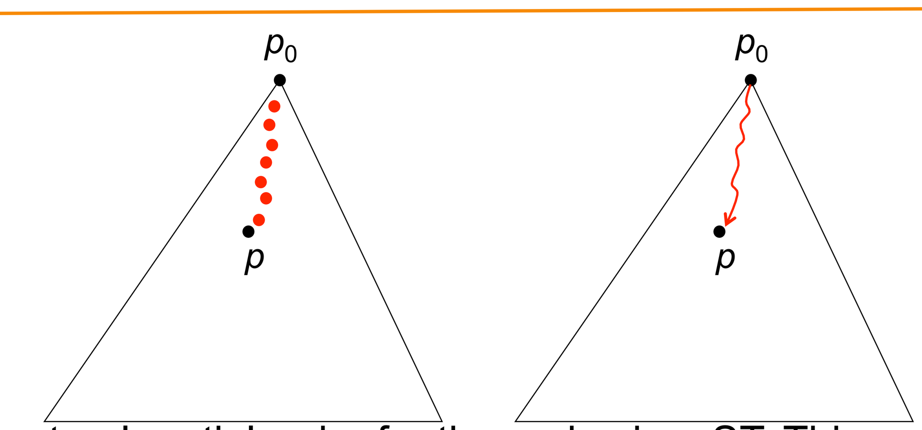
- Each path in the tree is an execution of the transition system.
- Nondeterminism: multiple children with the same label.
- Composition: algebraic operations on synchronization trees

Generalizing Trees

Definition:

A **tree** [3] is a partially ordered set $(P,\le)$ with the following two properties:

1) There is a $p_0 \in P$ s.t. $p_0 \le p$ for all $p \in P$. p_0 is the root of the tree.
2) For each $p \in P$, the set $\{p' \in P \mid p' \le p\}$ is linearly ordered by $\le$.



- There is a natural partial order for the nodes in a ST. This partial order labels each node with the list of its predecessors (on the path connecting it to the root); then the nodes are partially ordered according to sequence prefixes.

Generalized Synchronization Trees (GSTs)

Definition:

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

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

Research: Composition and Congruence

Goal: an algebraic theory of composition for CPSs.

- Semantically different notions of bisimulation: strong and weak.
  - Different substitutivity with respect to different notions of bisimulation
- Composition Operators on GSTs
  - CSP parallel composition

Weak and Strong Bisimulation

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

Definition:

Weak and Strong Bisimulation (cont.)

Proposition:

If G_P and G_Q are STs, then G_P strongly simulates G_Q iff 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.

CSP Parallel Composition

- SOS rules for processes P and Q (S is a set of labels):

$$\frac{P \xrightarrow{a} P' \quad a \notin S}{P|S|Q \xrightarrow{a} P'|S|Q} \qquad \frac{Q \xrightarrow{a} Q' \quad a \notin S}{P|S|Q \xrightarrow{a} P|S|Q'} \qquad \frac{P \xrightarrow{a} P' \quad Q \xrightarrow{a} Q' \quad a \in S}{P|S|Q \xrightarrow{a} P'|S|Q'}$$

Definition:

Let $(P,\le)$ be a partial order. A linearization of $(P,\le)$ is a total order $(P,\le')$ s.t. if $p_1 \le p_2$, then $p_1 \le' p_2$.

Definition:

Let $G_1 = (P_1, p_1, \le_1, \mathcal{L}_1)$ and $G_2 = (P_2, p_2, \le_2, \mathcal{L}_2)$ be two GSTs with $P_1 \cap P_2 = \emptyset$, and let $T_1 = (p_1, p_1']$ and $T_2 = (p_2, p_2']$ be two bounded trajectories. Also, let $S \subseteq L$. A total order $(Q, \le_Q)$ is an ***S-synchronized interleaving*** of T_1 and T_2 iff there exists a monotonic bijection $\lambda: \{p \in T_1 \mid \mathcal{L}_1(p) \in S\} \to \{p \in T_2 \mid \mathcal{L}_2(p) \in S\}$ s.t.

1. $\mathcal{L}_1(p) = \mathcal{L}_2(\lambda(p))$ for all $p \in T_1$ s.t. $\mathcal{L}_1(p) \in S$.
2. $Q = \{p \in T_1 \mid \mathcal{L}_1(p) \notin S\} \cup \{p \in T_2 \mid \mathcal{L}_2(p) \notin S\} \cup \{(p, \lambda(p)) \mid \mathcal{L}_1(p) \in S\}$.
3. Let $\pi_1: Q \to (T_1 \cup T_2)$ where $\pi_1: p \mapsto p$ for $p \in T_1 \cup T_2$ and $\pi_1: (p_1', p_2') \mapsto p_1'$ otherwise, and similarly for π_2. Then $\pi_1(q) \le_1 \pi_1(q')$ or $\pi_2(q) \le_2 \pi_2(q')$ implies $q \le_Q q'$.

Let $I_S(T_1, T_2)$ denote the set of all S-synchronized interleavings of T_1 and T_2.

Definition:

Let $G_1 = (P_1, p_1, \le_1, \mathcal{L}_1)$ and $G_2 = (P_2, p_2, \le_2, \mathcal{L}_2)$ be two GSTs with $P_1 \cap P_2 = \emptyset$. Then the GST $G_1 |S| G_2 = (Q, q_0, \le_Q, \mathcal{L}_Q)$ is given by:

1. $Q = \{(p_1, p_2)\} \cup \{T \mid T \in I_S(T_1, T_2)$ *for trajectories* $T_1 = (p_1, p_1']$ *and* $T_1 = (p_2, p_2']\}$.
2. $q \le_Q q'$ iff $q = (p_1, p_2)$, or $q = (r, \le_r)$, $q' = (r', \le_{r'})$, and $r \subseteq r' \wedge (\forall (s,t) \in r \times r' \setminus r.\ (s,t) \in \le_{r'})$.
3. $q_0 = (p_1, p_2)$.
4. Let $q \in Q$ and $p' = \sup(q)$. Then define $\mathcal{L}_Q: Q \to L$ such that: $\mathcal{L}_Q: q \mapsto \mathcal{L}_1(p')$ *if* $p' \in P_1$; $\mathcal{L}_Q: q \mapsto \mathcal{L}_2(p')$ *if* $p' \in P_2$; and $\mathcal{L}_Q: q \mapsto \mathcal{L}_1(p_1')$ *if* $p' = (p_1', p_2')$.

$G_1 |S| G_2$ is a generalization of the CSP parallel composition operator.

References

[1] J. Ferlez, R. Cleaveland, and S. Marcus. *Generalized synchronization trees*. In FOSSACS 2014, vol. 8412 of LNCS, pages 304–319, Grenoble, France, 2014. Springer-Verlag.

[2] M. Hennessy and R. Milner. *Algebraic laws for nondeterminism and concurrency*. J. ACM, 32(1):137–161, January 1985.

[3] T. Jech. *Set Theory*. Academic Press, 1978.

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

[5] G.D. Plotkin. *A structural approach to operational semantics*. Technical Report DAIMI- FN-19, Computer Science Department, Aarhus University, Aarhus, Denmark.

[6] E. D. Tate Jr, J. W. Grizzle, and H. Peng. *Shortest path stochastic control for hybrid electric vehicles*. Int. J. Robust Nonlinear Control, 18(14):1409-1429, December 2007.