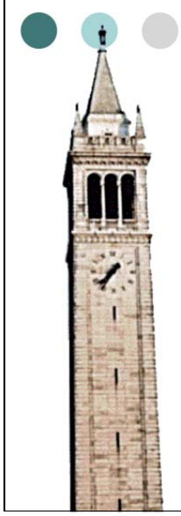


Concurrent Models of Computation for Embedded Software

Edward A. Lee

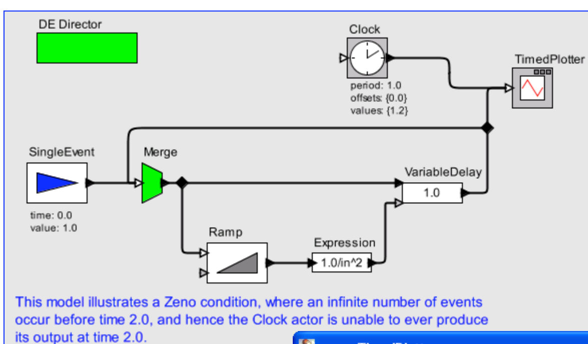
Professor, UC Berkeley

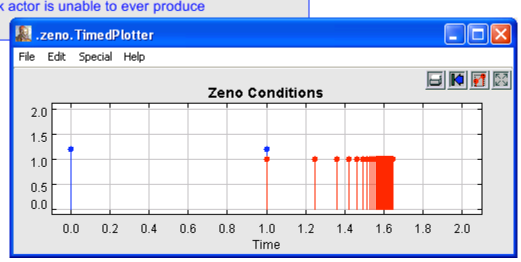
EECS 290n – Advanced Topics in Systems Theory

Fall, 2004

Lecture 13: Semantics of Discrete Event Systems

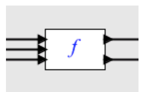
We Seek Semantics that Give Meaning to Feedback and Help Rule Out Zeno





Mathematical Framework

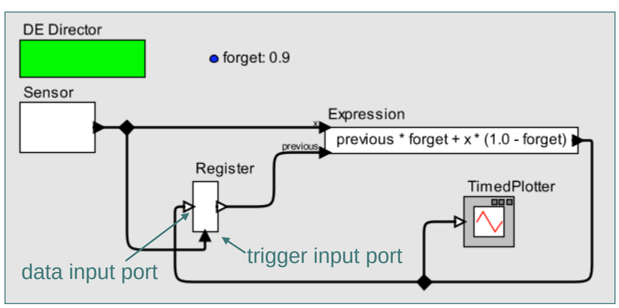
Let the set of all signals be $A = [T \to V]$ where T is a totally ordered set and V is a set of values. Let an actor



be a function $f : A^n \to A^m$. What are the constraints on these functions such that:

1. Compositions of actors are determinate.
2. Feedback compositions have a meaning.
3. We can rule out Zeno behavior.

A Feedback Design Pattern



In this model, a sensor produces measurements that are combined with previous measurements using an exponential forgetting function.

The feedback loop makes it impossible to present the Register actor with all its inputs at any tag before firing it.

Solving Feedback Loops

Possible solutions:

1. Find algebraic solution
2. All actors have time delay
3. Some actors have time delay,
   and every directed loop must have an actor with time delay.
4. All actors have delta delay
5. Some actors have delta delay
   and every directed loop must have an actor with delta delay.

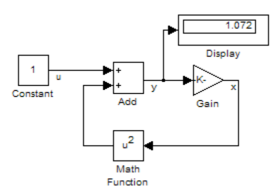
Although each of these solutions is used, all are problematic.

The root of the problem is simultaneous events.

Consider “Find Algebraic Solution”

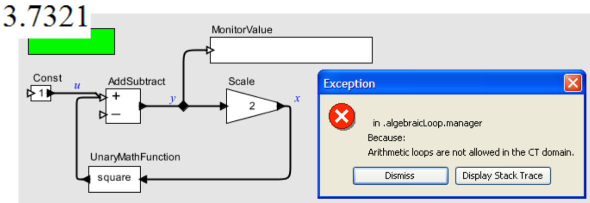
This solution is used by Simulink, but is ill posed. Consider:

$$y(t) = x^2(t) + u(t)$$
$$x(t) = K\,y(t)$$

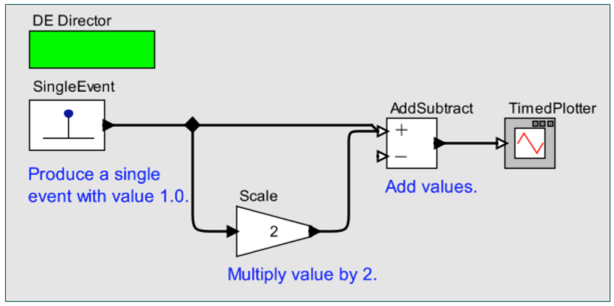


This has two solutions:

$$y(t) = 1.072, \quad x(t) = 0.268, \text{ or}$$
$$y(t) = 14.9282, \quad x(t) = 3.7321$$



Consider “All Actors Have Time Delay”



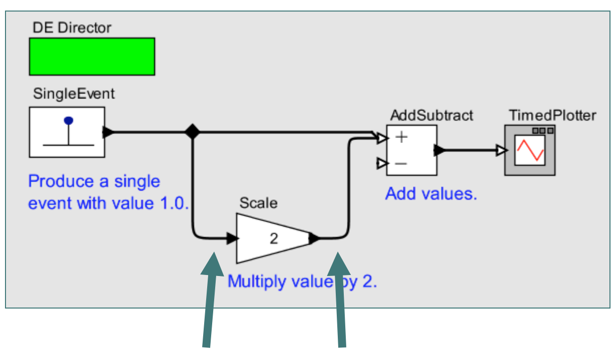
If all actors have time delay, this produces either:

- Event with value 1 followed by event with value 2, or
- Event with value 1 followed by event with value 3.

(the latter if signal values are persistent).

Neither of these is likely what we want.

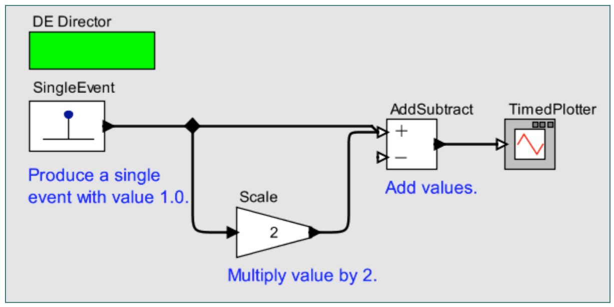
Consider “All Actors Have Delta Delay”



With delta delays, if an input event is ((t, n), v), the corresponding output event is ((t, n+1), v’). Every actor is assumed to give a delta delay.

This style of solution is used in VHDL.

Consider "All Actors Have Delta Delay"



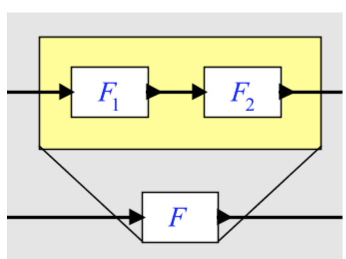
If all actors have a delta delay, this produces either:

- Event with value 1 followed by event with value 2, or
- Event with value 1 followed by event with value 3

(the latter if signal values are persistent, as in VHDL).

Again, neither of these is likely what we want.

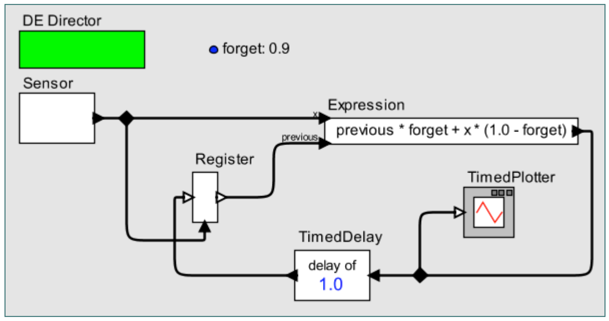
More Fundamental Problem: Delta Delay Semantics is Not Compositional



The top composition of two actors will have a two delta delays, whereas the bottom abstraction has only a single delta delay.

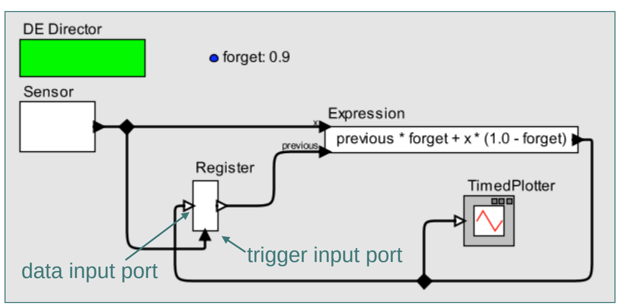
Under delta delay semantics, a composition of two actors cannot have the semantics of a single actor.

Consider "Some actors have time delay,
and every directed loop must have an actor with
time delay."



Any non-zero time delay imposes an upper bound on the rate at which sensor data can be accepted. Exceeding this rate will produce erroneous results.

Consider "Some actors have delta delay,
and every directed loop must have an actor with
delta delay."

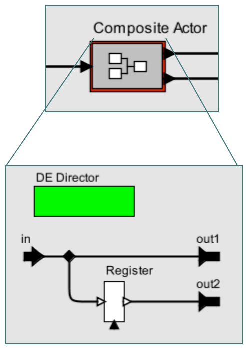


The output of the Register actor must be at least one index later than the data input, hence this actor has at least a delta delay.

To schedule this, could break the feedback loop at actors with delta delay, then do a topological sort.

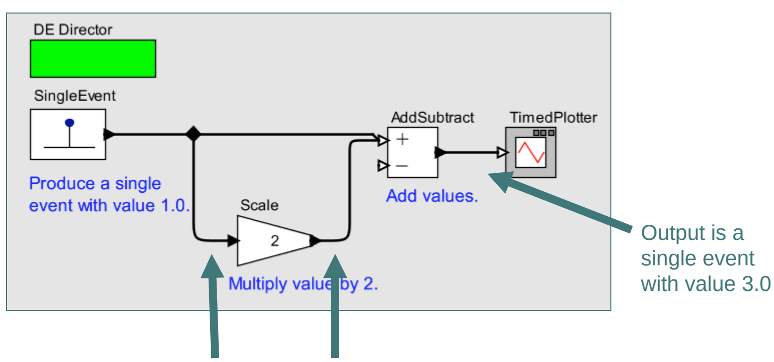
Naïve Topological Sort is not Compositional

Breaking loops where an actor has a delta delay and performing a topological sort is not a compositional solution:



Does this composite actor have a delta delay or not?

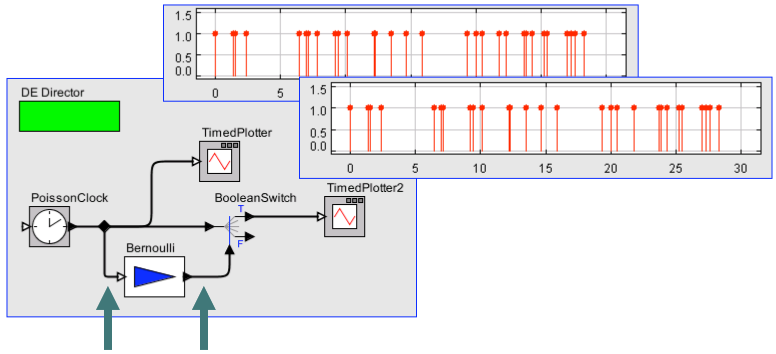
Ptolemy Solution: No Required Delay, and Feedback Loops Have (Unique) Least Fixed Points Semantics



Given an input event ((t, n), v), the corresponding output event is ((t, n), v'). The actor has no delay.

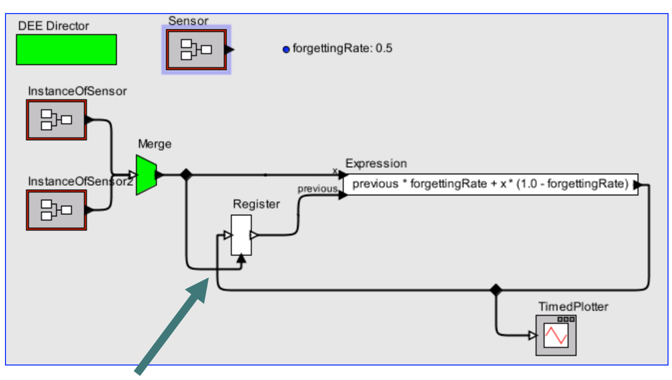
The challenge now is to establish a determinate semantics and a scheduling policy for execution.

Fixed-Point Semantics at a Tag Handles Simultaneous Events



By default, an actor produces events with the same time as the input event. But in this example, we expect (and need) for the BooleanSwitch to “see” the output of the Bernoulli in the same “firing” where it sees the event from the PoissonClock. Events with identical time stamps are also ordered, and reactions to such events follow data precedence order.

Fixed-Point Semantics at a Tag Handles Feedback



Data precedence analysis has to take into account the non-strictness of this actor (that an output can be produced despite the lack of an input).

Semantics of DE

At a particular tag value, we assume SR semantics (least fixed point on a flat CPO).

What about across tags? Two alternatives for a semantics of the dynamics of DE:

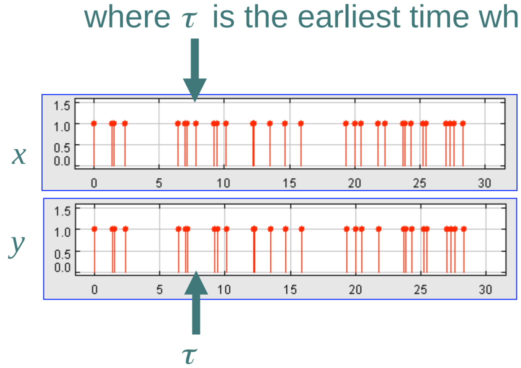
- Metric spaces
- Fixed points on a CPO

Discrete-Event Semantics
First Approach: Metric Spaces

Cantor metric:

$$d(x, y) = 1/2^{\tau}$$

where τ is the earliest time where x and y differ.



Metric

A *metric* on a set A is a function $d : A \times A \to R$ where for all $a, b, c \in A$

1. $d(a, b) = d(b, a)$
2. $d(a, b) = 0 \Leftrightarrow a = b$
3. $d(a, b) + d(b, c) \geq d(a, c)$

Exercise: Show that these properties imply that for all $a, b \in A, \quad d(a, b) \geq 0$

Metric space: (A, d)

Lee 13: 19

Variations on Metrics

Ultrametric: Replace property 3 with:

3. $\max(d(a, b), d(b, c)) \geq d(a, c)$

Exercise: Prove that an ultrametric is a metric.

Partial Metric: Replace properties 2 and 3 with:

2. $d(a, a) \leq d(a, b)$
3. $d(a, b) + d(b, c) - d(b, b) \geq d(a, c)$

In a partial metric, a is the “closest” object to itself.

Lee 13: 20

The Cantor Metric

Given the tag set $T = R \times N$ use only the time stamps. Let

$$d : [T \to V] \times [T \to V] \to R$$

such that for all $s, s' \in [T \to V]$,

$$d(s, s') = 1/2^{\tau}$$

where τ is the time stamp of the least tag t where $s(t) \neq s'(t)$. That is, either one is defined and the other not at t or both are defined but are not equal.

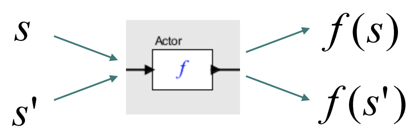
The Cantor Metric is an Ultrametric

Need to show that for all signals $a, b, c \in [T \to V]$,

1. $d(a, b) = d(b, a)$
2. $d(a, b) = 0 \Leftrightarrow a = b$
3. $\max(d(a, b), d(b, c)) \geq d(a, c)$

(1) and (2) are obvious. To show (3), assume without loss of generality that $d(a, b) \geq d(b, c)$. This means that a and b differ earlier than b and c. Suppose that a and b differ first at time τ. Since a and b differ earlier than b and c, then prior to τ, b and c are identical. Thus, a and c must be identical prior to τ so $d(a, c)$ must be smaller than or equal to $d(a, b)$. QED

Causality



Causal: For all signals s and s'

$$d\,(\,f\,(s)\,,f\,(s'\,))\leq d\,(\,s\,,s'\,)$$

Strictly causal: For all signals s and s'

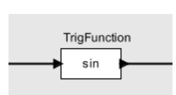
$$s \neq s' \quad \Rightarrow \quad d\,(\,f\,(s)\,,f\,(s'\,)) < d\,(\,s\,,s'\,)$$

Delta causal: There exists a real number $\delta < 1$ such that for all signals s and s'

$$s \neq s' \quad \Rightarrow \quad d\,(\,f\,(s)\,,f\,(s'\,)) \leq \delta\, d\,(\,s\,,s'\,)$$

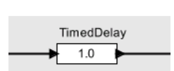
Examples

Simple functional actor:



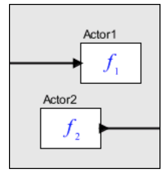
This actor is causal but not strictly causal or delta causal.

Time delay with non-zero delay:



This actor is delta causal.

Source and Sink Actors

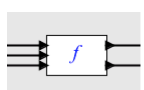


Consider Actor1. Its function is $f_1 \colon A^1 \to A^0$ where A^0 is a *singleton set* (a set with one element). Such a function is always delta causal with $\delta = 0$.

Consider Actor2. Its function is $f_1 \colon A^0 \to A^1$. Such a function is again always delta causal with $\delta = 0$.
In fact, the function can only yield one possible output signal, since its domain has size 1.

Extending to Multiple Inputs/Outputs

Consider a function $f \colon A^n \to A^m$, where $A = [T \to V]$



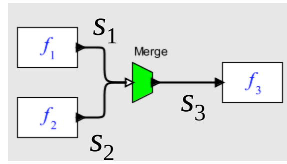
The input is a tuple of signals $(a_1, a_2, \ldots, a_n)$.

Extend the Cantor metric to handle tuples:

$$d((a_1, a_2, \ldots, a_n),(b_1, b_2, \ldots, b_n))$$
$$= \min(d(a_1, b_1), \ldots, d(a_n, b_n))$$

The resulting function is still an ultrametric.

Example: Merge Actor



Recall that for input

$$s_1 = \{\ldots ((t, 0), v_1), ((t, 1), v_2), \ldots)$$
$$s_2 = \{\ldots ((t, 0), q_1), ((t, 1), q_2), \ldots)$$

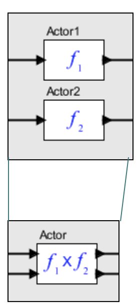
the output is:

$$s_3 = \{\ldots ((t, 0), v_1), ((t, 1), q_1), ((t, 2), v_2), ((t, 3), q_2), \ldots)$$

This actor is causal but not strictly causal, and the operations on indexes do not appear in the semantics.

Parallel Composition of Actors

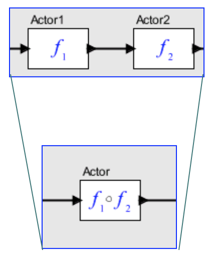
If f_1 and f_2 are causal (strictly causal, delta causal), then so is $f_1 \times f_2$.



What if f_1 is causal and f_2 is delta causal?

Cascade Composition of Actors

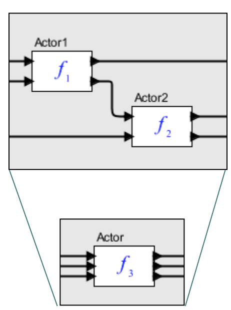
If f_1 and f_2 are causal (strictly causal, delta causal), then so is $f_1 \circ f_2$.



What if f_1 is causal and f_2 is delta causal?

More Interesting Composition

If f_1 and f_2 are causal (strictly causal, delta causal), then so is the following composition:



Question: What if f_1 is causal and f_2 is delta causal?

Technicality

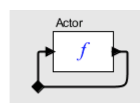
In the set $S = [T \to V]$, we could have a signal s that has, for example, an event at all integer time stamps (positive and negative), and we could compare it against a signal s' that has no events at all.

$$d(s, s') = \infty$$

This is problematic. We can avoid these problems by excluding from the set S all signals that have infinite distance from the empty signal. All such signals have an earliest event.

Lee 13: 31

Fixed Point Theorem 3



Let $(S^n = [T \to V]^n, d)$ be a metric space and $f : S^n \to S^n$ be a strictly causal function. Then f has at most one fixed point.

Proof: It is enough to show that

$$s \neq s' \Rightarrow f(s) \neq s \text{ or } f(s') \neq s'.$$

Suppose to the contrary that

$$s \neq s' \text{ and } f(s) = s \text{ and } f(s') = s'$$

But this is not possible because it would imply that

$$d(s, s') = d(f(s), f(s')) < d(s, s').$$

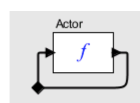
Lee 13: 32

Determinacy

Fixed-Point Theorem 3 takes care of determinacy. There can be no more than one behavior.

Can we find that behavior?

Fixed Point Theorem 4 (Banach Fixed Point Theorem)



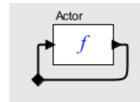
Let $(S^n = [T \to V]^n, d)$ be a *complete* metric space and $f : S^n \to S^n$ be a delta causal function. Then f has a unique fixed point, and for any point $s \in S^n$, the following sequence converges to that fixed point:

$$s_1 = s,\ s_2 = f(s_1),\ s_3 = f(s_2),\ \ldots$$

This means no Zeno! Two issues:

- Any starting point?
- Complete metric space?

Construction of a Fixed Point: Example



Suppose f is a delay by one time unit, such that

$$s' = f(s)$$

where for each event $e = (t, v) \in s$ where $t = (\tau, n)$, there is an event $e' = (t', v) \in s'$ where $t' = (\tau + 1, n)$.

Suppose we start with a "lucky guess" $s = \varnothing$. This is the only fixed point, so we converge immediately.

Suppose we start with an "unlucky guess" $s = \{((0,0), 0)\}$. As we iterate f, the event gets further out in the future, and the signal "converges" to $s = \varnothing$.

Complete Metric Spaces

A *Cauchy sequence* $\{s_1, s_2, \ldots\}$ is an infinite sequence where

$$d(s_n, s_m) \to 0 \text{ as } n, m \to \infty$$

A *complete metric space* (X, d) is one where every Cauchy sequence has a limit in X.

Example 1

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((n, 0), v)\}$$

Is this sequence Cauchy?

Does the sequence converge? To what?

Example 1

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((n, 0), v)\}$$

Is this sequence Cauchy? Yes

$$d(s_n, s_m) = 1/2^{\min(m, n)} \rightarrow 0$$

Does the sequence converge? To what? Yes. To $\emptyset$

$$\lim(s_n) = \emptyset$$

Example 2

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((i, 0), v) \mid i \in \{1, 2, \ldots, n\}\}$$

Is this sequence Cauchy?

Does the sequence converge? To what?

Example 2

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((i, 0), v) \mid i \in \{1, 2, \ldots, n\}\}$$

Is this sequence Cauchy? Yes

$$d(s_n, s_m) = 1/2^{\min(m, n) + 1} \to 0$$

Does the sequence converge? To what? Yes. To

$$\{((i, 0), v) \mid i \in \{1, 2, \ldots\}\}$$

Example 3

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((\tau_i, 0), v) \mid i \in \{1, 2, \ldots, n\}, \tau_i = 1 - 1/i\}$$

Is this sequence Cauchy?

Does the sequence converge? To what?

Lee 13: 41

Example 3

Consider a sequence $\{s_1, s_2, \ldots\}$ where

$$s_n = \{((\tau_i, 0), v) \mid i \in \{1, 2, \ldots, n\}, \tau_i = 1 - 1/i\}$$

Is this sequence Cauchy? No

$$d(s_n, s_m) > 1/2$$

Does the sequence converge? To what? No. Exercise.

Lee 13: 42

Completeness of DE Signals

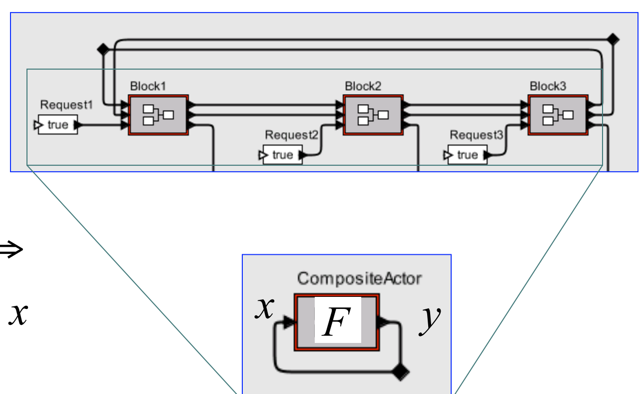
The set of n-tuples of discrete-event signals under the Cantor metric is a complete metric space.

Proof (sketch): We need to show that every Cauchy sequence converges. Given a Cauchy sequence $\{s_1, s_2, \ldots\}$, for any tag t with time stamp $\tau > 0$, there is a subsequence $\{s_n, s_{n+1}, \ldots\}$, for some $n > 0$, of signals that are identical up to and including tag t. Let s be the sequence obtained by letting its value at each tag t be that identical value (or absence, if all signals in the subsequence have no event at t). This is clearly a signal (or tuple of signals). Then it is easy to show that the Cauchy sequence converges to s.

Thanks to Adam Cataldo for this proof.

Summary: Semantics of Composition

If the components are deterministic, the composition is deterministic.

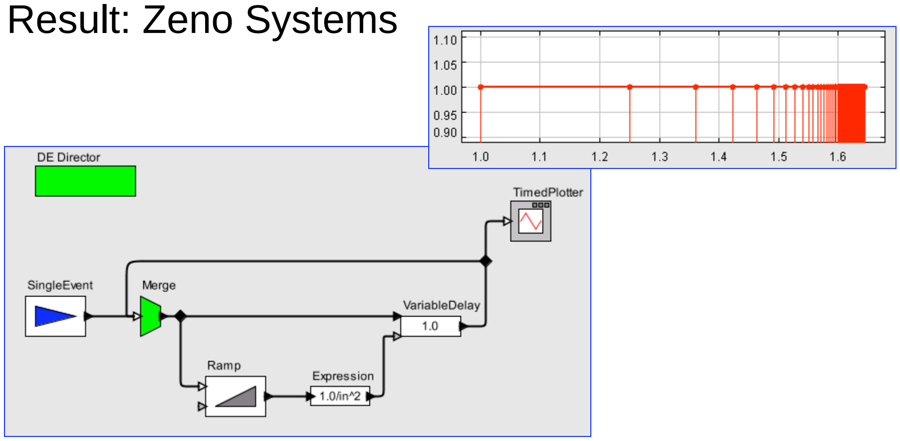


$$x = y \Rightarrow$$
$$F(x) = x$$

Banach fixed point theorem:

- Contraction map has a unique fixed point
- Execution procedure for finding that fixed point
- Successive approximations to the fixed point

Result: Zeno Systems



Theorem: If every directed cycle contains a delta-causal component, then the system is non-Zeno.

Semantics of DE

At a particular tag value, we assume SR semantics (least fixed point on a flat CPO).

What about across tags? Two alternatives for a semantics of the dynamics of DE:

- Metric spaces
- Fixed points on a CPO

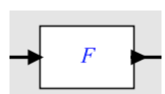
Second Approach (X. Liu): Prefix Order

- Recall that a signal s is a partial function: defined on an initial segment of T. Such a function can be given by its *graph*, $s \subset T \times V_\varepsilon$.
- A signal s_1 is a *prefix* of a signal s_2 if $s_1 \subseteq s_2$. The prefix relation is a partial order on the set S of signals.
- Fact: S with the prefix order is a complete semilattice (and hence also a CPO).
- Generalizes easily to tuples of signals S^N.

Monotonic and Continuous Functions

A function $F\colon S \to S$ is *monotonic* if it is order-preserving,

$$\forall s_1, s_2 \in S, \quad s_1 \subseteq s_2 \implies F(s_1) \subseteq F(s_2).$$



The same function is (Scott) *continuous* if for all directed sets $S' \subseteq S$, $F(S')$ is a directed set and

$$F(\bigvee S') = \bigvee F(S').$$

Here, $F(S')$ is defined in the natural way as $\{F(s) \mid s \in S'\}$, and $\vee X$ denotes the least upper bound of the set X.

Every continuous function is monotonic, and behaves as follows: Extending the input (in time or tags) can only extend the output.

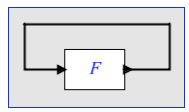
Recall Fixed-Point Theorem

A classic fixed point theorem states that if F is continuous, then it has a least fixed point, and that least fixed point is

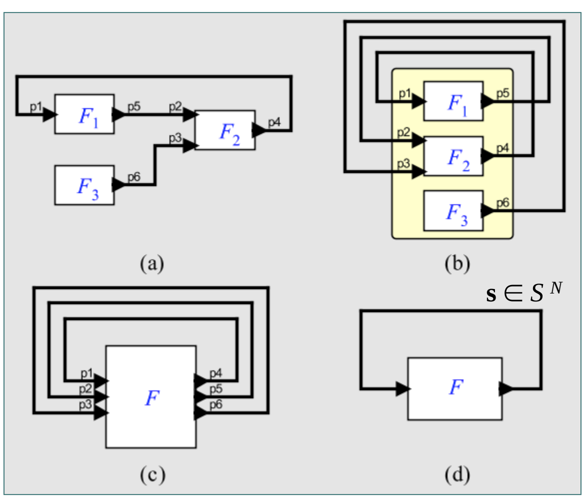
$$\bigvee\{F^n(\perp_S) \mid n \in \mathbb{N}\},$$

where $\perp_S$ is the least element of S (the empty signal) and $\mathbb{N}$ is the natural numbers.

Start with empty signals.
Iteratively apply function *F*.
Converge to the unique solution.



Summary: Existence and Uniqueness of the Least Fixed Point Solution.

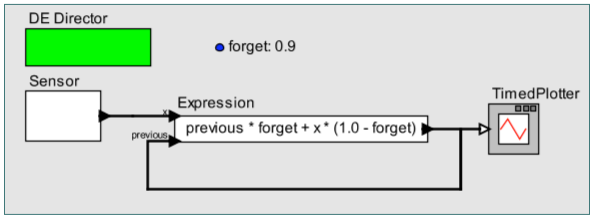


- Signal: $s\colon \mathbb{R}_+ \times \mathbb{N} \rightharpoonup V_\varepsilon$
- Set of signals: S
- Tuples of signals: $\mathbf{s} \in S^N$
- Actor: $F\colon S^N \to S^M$

A unique least fixed point, $\mathbf{s} \in S^N$ such that $F(\mathbf{s}) = \mathbf{s}$, exists and be constructively found if S^N is a CPO and F is (Scott) continuous.

Under our execution policy, actors are usually (Scott) continuous.

But: Need to Worry About Liveness: Deadlocked Systems

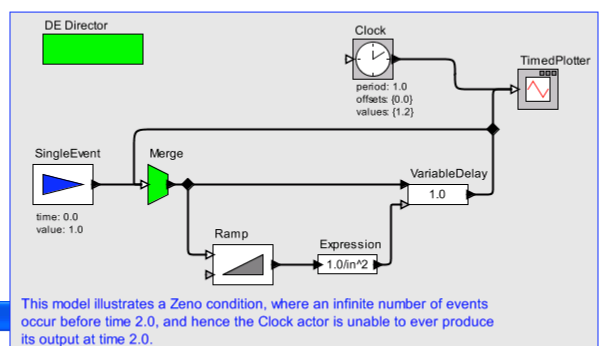


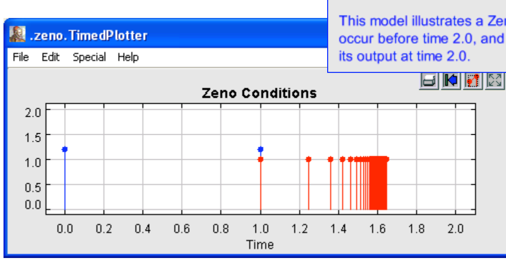
Existence and uniqueness of a solution is not enough.

The least fixed point of this system consists of empty signals. It is deadlocked!

Another Liveness Concern: Zeno Systems

DE systems may have an infinite number of events in a finite amount of time. These “Zeno systems” can prevent time from advancing.





In this case, our execution policy fails to implement the Knaster-Tarski constructive procedure because some of the signals are not total.

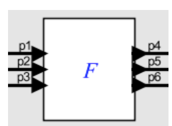
Liveness

A signal is *total* if it is defined for all tags in T.
A model with no inputs is *live* if all signals are total.
A model with inputs is *live* if all input signals are total implies all signals are total.

Liveness ensures freedom from deadlock and Zeno.

Whether a model is live is, in general, undecidable.
We have developed a useful sufficient condition based on *causality* that ensures liveness.

Causality Ensures Liveness of an Actor



A monotonic actor F is *causal* if for all sets of input signals S_i, the corresponding set of output signals $S_o = F(S_i)$ satisfy

$$\bigcap_{s \in S_i} \mathrm{dom}(s) \subseteq \bigcap_{s \in S_o} \mathrm{dom}(s) \,.$$

An immediate consequence of this definition is that a causal actor is live. Thus, whether a composition of actors is causal will tell us whether it is live.

Causality does not imply continuity and continuity does not imply causality. Continuity ensures existence and uniqueness of a least fixed point, whereas causality ensures liveness.

Strict Causality Ensures Liveness of a Feedback Composition

A composition of causal actors without directed cycles is itself a causal actor. With cycles, we need:

- A monotonic actor F is *strictly causal* if for all sets of input signals S_i, the corresponding set of output signals $S_o = F(S_i)$ either consists only of total signals (defined over all T) or

$$\bigcap_{s \in S_i} \mathrm{dom}(s) \subset \bigcap_{s \in S_o} \mathrm{dom}(s)\,.$$

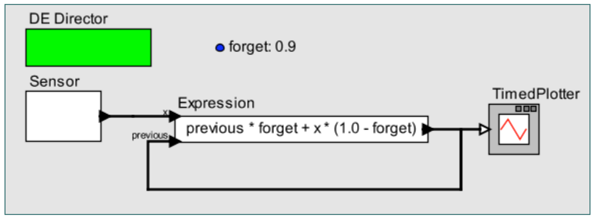
($\subset$ denotes strict subset). If F is a strictly causal actor with one input and one output, then $F(s_\perp) \neq s_\perp$. F must "come up with something from nothing."

Continuity, Liveness, and Causality

Theorem: Given a totally ordered tag set and a network of causal and continuous actors where in every dependency loop in the network there is at least one strictly causal actor, then the network is a causal and continuous actor.

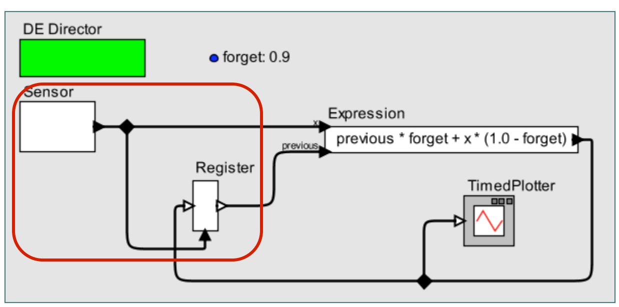
This gives us sufficient, but not necessary condition for freedom deadlock and Zeno.

Recall Deadlocked System



The feedback loop has no strictly causal actor.

Feedback Loop that is Not Deadlocked



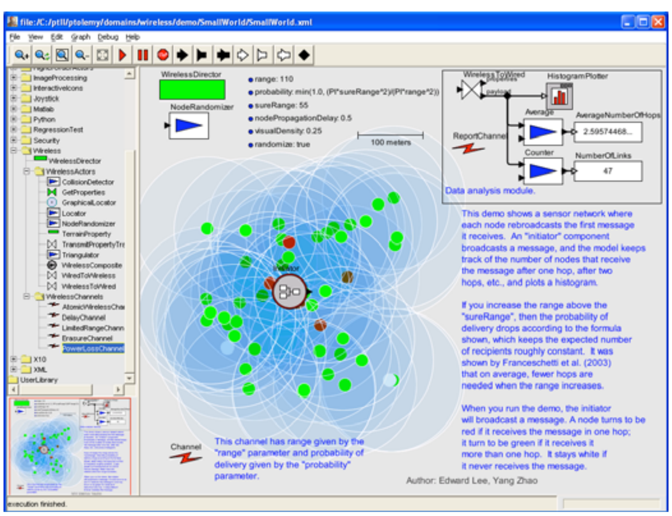
This feedback loop also has no strictly causal actor, unless…

We aggregate the two actors as shown into one.

Operational Semantics

1. Topologically sort actors according to paths that do not increment tags.
2. Start with a set of events on signals taken from the event queue that all have the same tag.
3. Iterate to find a fixed-point value for all signals at that tag (absent or having a value).
4. Continue with the next smallest tag in the event queue.

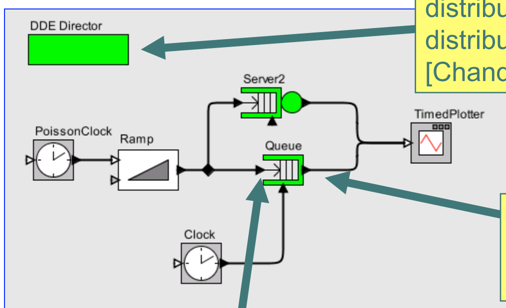
Extension of Discrete-Event Modeling for Wireless Sensor Nets



VisualSense extends the Ptolemy II discrete-event domain with communication between actors representing sensor nodes being mediated by a *channel*, which is another actor.

The example at the left shows a grid of nodes that relay messages from an *initiator* (center) via a channel that models a low (but non-zero) probability of long range links being viable.

Distributed Discrete Event (DDE) Models (Chandy/Misra style)



DDE Director supports distributed execution and a distributed notion of time [Chandy & Misra 1979]

Local notion of time in each actor, advancing only when input is received

Blocking read at input ports prevents time from locally advancing without “permission” from a source

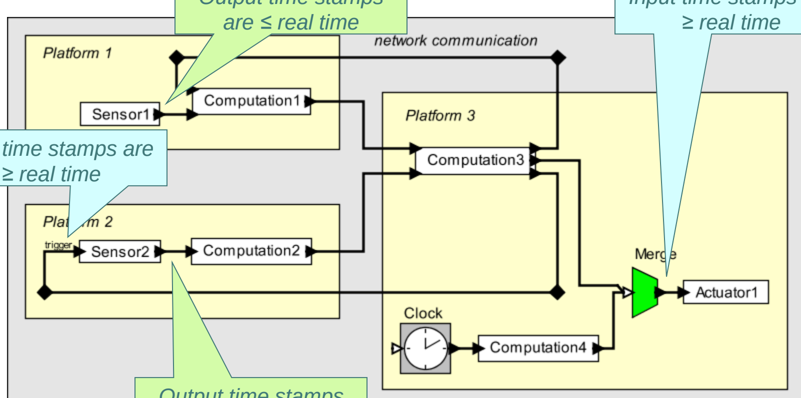
This is the “Chandy and Misra” style of distributed discrete events [1979], which compared to Croquet and Time Warp [Jefferson, 1985], is “conservative.”

Example: PTIDES: Programming Temporally Integrated Distributed Embedded Systems

Distributed execution under DE semantics, with “model time” and “real time” bound at sensors and actuators.

Output time stamps are ≤ real time

Input time stamps are ≥ real time



Input time stamps are ≥ real time

Output time stamps are ≤ real time

Other Interesting Possibilities for Distributed Discrete Events

- Time-Warp (Jefferson)
  - Optimistic computation
  - Backtracking
- Croquet (Reed)
  - Optimistic computation
  - Replication of computation
  - Voting algorithm (Lamport)

Summary

- Superdense time defines a tag to be a time and an index.
- Fixed point semantics on a flat CPO (like SR) at each tag.
- Discrete systems require execution at a subset of tags that is order isomorphic with an initial segment of the natural numbers.
- Operational semantics: Choose the next tag in the event queue and find a fixed point.
- Denotational semantics: Metric space and CPO approaches both available, and yield proofs of liveness for different subsets of models.