Runtime Composition Of Systems of Interacting Cyber-Physical Components

Benjamin Lion, Farhad Arbab, and Carolyn Talcott

Cyber-physical system

Cyber:

- discrete actions;
- experiments are repeatable;
- do not miss any observations.

Physics:

- continuous changes;
- behavior may depend on time;
- eventually sampling losses.

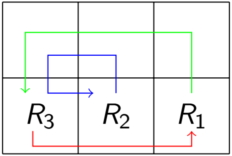
Running Example

R_3	R_2	R_1

Context:

- robots exhibit discrete sequences of moves as a *cyber* system;
- field changes its state continuously as a *physical* system;
- reachability query on the state of the field.

Running Example



Modeling challenges:

- actions between robots may interleave;
- interactions with the physical field may lead to interferences;
- robots may not observe all possible events of other robots;

Will the robots eventually get sorted?

Content

1. Algebra of Components
   - component
   - products and division
2. Specification of components
   - transition system
   - compositionality
   - compatibility
3. Analysis
   - scenario
   - results

Discrete event framework

Preliminaries

Ingredients for our model:

- set of discrete events E;
- observation as a pair of a set of events O and a time stamp t, i.e., $(O, t) \in \mathcal{P}(E) \times \mathbb{R}_+$.
- timed-event sequences (TES) as an infinite sequence of observations, i.e., $\sigma : \mathbb{N} \to (\mathcal{P}(E) \times \mathbb{R}_+)$ with time increasing for consecutive observations.

For a TES σ, we write $\sigma(t) = O$ if there exists $i \in \mathbb{N}$ such that $\sigma(i) = (O, t)$, and $\sigma(t) = \emptyset$ otherwise.

Discrete event framework

Preliminaries

Ingredients for our model:

- set of discrete events E;
- observation as a pair of a set of events O and a time stamp t, i.e., $(O, t) \in \mathcal{P}(E) \times \mathbb{R}_+$.
- timed-event sequences (TES) as an infinite sequence of observations, i.e., $\sigma : \mathbb{N} \to (\mathcal{P}(E) \times \mathbb{R}_+)$
  with time increasing for consecutive observations.

For a TES σ, we write $\sigma(t) = O$ if there exists $i \in \mathbb{N}$ such that $\sigma(i) = (O, t)$, and $\sigma(t) = \emptyset$ otherwise.

Similar semantic model as in (Fiadeiro and Lopes, 2017) and (Arbab and Rutten, 2002)

Component

A *component* $C = (E, L)$ is a pair of

- an interface E is a set of observable events
  - position readings $r(i, (x, y))$ with $x, y \in \mathbb{N}$ for a robot;
  - move $E(i)$ as robot i moves East;
  - position display $(x, y)_i$ with $x, y \in \mathbb{R}$ for a field with obstacle i;

Component

A *component* $C = (E, L)$ is a pair of

- an interface E is a set of observable events
  - position readings $r(i,(x,y))$ with $x, y \in \mathbb{N}$ for a robot;
  - move $E(i)$ as robot i moves East;
  - position display $(x,y)_i$ with $x, y \in \mathbb{R}$ for a field with obstacle i;
- a behavior L is a set of Timed Events Streams over E ($L \subseteq$ TES(E)), e.g.,

t	$\sigma \in L$	$\eta \in L$
t_1	$\{N(1)\}$	$\{N(2)\}$
t_2	$\{W(1)\}$	$\{E(2)\}$
t_3	$\{r(i,(n;m))\}$	$-$
$\dots$	$\dots$	$\dots$

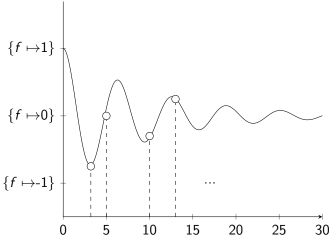
  with $t_1, t_2, t_3, \dots$ increasing and Non-Zeno.

Component

Physical example

A function $f : \mathbb{R}_+ \to D$ as a component $C = (E_f, L_f)$ where:

- its interface E_f is the set of events D;
- its behavior L_f is the set of sequences of images $f(x)$ sampled at monotonically increasing, non-Zeno sequences of values of x.



Component

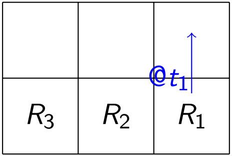
Example sequence

R_3	R_2	R_1

t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$

Component

Example sequence



t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$
t_1	$N(1)$	$-$	v_1

Component

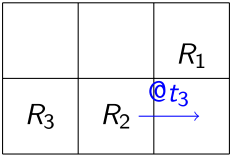
Example sequence

		R_1
R_3	R_2	

t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$
t_1	$N(1)$	$-$	v_1
t_2	$r(1, (\lfloor x \rfloor; \lfloor y \rfloor))$	$-$	$(x; y)_1$

Component

Example sequence



t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$
t_1	$N(1)$	$-$	v_1
t_2	$r(1, (\lfloor x \rfloor; \lfloor y \rfloor))$	$-$	$(x; y)_1$
t_3	$-$	$E(2)$	v_2

Component

Example sequence

		R_1
R_3		R_2

t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$
t_1	$N(1)$	$-$	v_1
t_2	$r(1, (\lfloor x \rfloor ; \lfloor y \rfloor))$	$-$	$(x; y)_1$
t_3	$-$	$E(2)$	v_2
t_4	$-$	$r(2, (\lfloor x \rfloor ; \lfloor y \rfloor))$	$(x; y)_2$

Component

Example sequence

		R_1
R_3		R_2

t	$\sigma : R_1$	$\eta : R_2$	$\tau : F$
t_1	$N(1)$	$-$	v_1
t_2	$r(1, (\lfloor x \rfloor; \lfloor y \rfloor))$	$-$	$(x; y)_1$
t_3	$-$	$E(2)$	v_2
t_4	$-$	$r(2, (\lfloor x \rfloor; \lfloor y \rfloor))$	$(x; y)_2$
$\cdots$	$\cdots$	$\cdots$	$\cdots$

Composition

Goal

Composite components as a *product* of components.

Products must capture:

- dependence between events (e.g., synchrony);
- merge of two observations (e.g., union).

Those two features define an interaction signature.

Algebra of Components

Interaction signature

L_1 and L_2 be two sets of TESs.

Composability: R is a relation that says *which* pair $(\sigma_1, \sigma_2) \in L_1 \times L_2$ can compose

Composition: $\oplus$ is a function that says *how* a pair $(\sigma_1, \sigma_2) \in L_1 \times L_2$ compose to an element $\sigma_1 \oplus \sigma_2 \in L$.

An interaction signature Σ is a pair $\Sigma = (R, \oplus)$.

Algebra of Components

Interaction signature (examples)

Let $(\sigma \cup \tau)(t) = \sigma(t) \cup \tau(t)$ for any TESs σ and τ.

Synchronous interaction signature $\Sigma_{sync} = (R_{sync}(E_1, E_2), \cup)$ has

- $(\sigma, \tau) \in R_{sync}(E_1, E_2)$ if and only if $\sigma(t) \cap E_2 = \tau(t) \cap E_1$;

Algebra of Components

Interaction signature (examples)

Let $(\sigma \cup \tau)(t) = \sigma(t) \cup \tau(t)$ for any TESs σ and τ.

Synchronous interaction signature $\Sigma_{sync} = (R_{sync}(E_1, E_2), \cup)$ has

- $(\sigma, \tau) \in R_{sync}(E_1, E_2)$ if and only if $\sigma(t) \cap E_2 = \tau(t) \cap E_1$;

Asynchronous interaction signature $\Sigma_{async} = (R_{async}, \cup)$ has

- $(\sigma, \tau) \in R_{async}$ if and only if $\sigma(t) \cap \tau(t) = \emptyset$;

Algebra of Components

Interaction signature (examples)

Let $(\sigma \cup \tau)(t) = \sigma(t) \cup \tau(t)$ for any TESs σ and τ.

Synchronous interaction signature $\Sigma_{sync} = (R_{sync}(E_1, E_2), \cup)$ has

- $(\sigma, \tau) \in R_{sync}(E_1, E_2)$ if and only if $\sigma(t) \cap E_2 = \tau(t) \cap E_1$;

Asynchronous interaction signature $\Sigma_{async} = (R_{async}, \cup)$ has

- $(\sigma, \tau) \in R_{async}$ if and only if $\sigma(t) \cap \tau(t) = \emptyset$;

Free interaction signature $\Sigma_{free} = (R_{free}, \cup)$ has

- $(\sigma, \tau) \in R_{free}$ for all (σ, τ);

Algebra of Components

Greatest fixed point

Construct Σ co-inductively, given a relation on observations κ.

Algebra of Components

Greatest fixed point

Construct Σ co-inductively, given a relation on observations κ.

The function ϕ_κ takes a set S of pairs of TESs and returns the set:

$$\phi_\kappa(S) = \{(\sigma, \tau) \mid (\sigma(0), \tau(0)) \in \kappa, \ \textit{and}\ (\sigma, \tau)' \in S\}$$

where $(\sigma, \tau)'$ drops the first observation(s).

The greatest post fixed point of ϕ_κ defines the set of composable pairs, i.e.,

$$[\kappa] = \bigcup \{S \mid S \subseteq \phi_\kappa(S)\}$$

Algebra of Components

Greatest fixed point

Construct Σ co-inductively, given a relation on observations κ.

The function ϕ_κ takes a set S of pairs of TESs and returns the set:

$$\phi_\kappa(S) = \{(\sigma, \tau) \mid (\sigma(0), \tau(0)) \in \kappa, \text{ and } (\sigma, \tau)' \in S\}$$

where $(\sigma, \tau)'$ drops the first observation(s).

The greatest post fixed point of ϕ_κ defines the set of composable pairs, i.e.,

$$[\kappa] = \bigcup \{S \mid S \subseteq \phi_\kappa(S)\}$$

$\Sigma = ([\kappa], \cup)$ is an interaction signature.

Algebra of Components

Interaction signature (example)

Interaction signature $\Sigma_{FR} = ([\kappa_{FR}], \cup)$ between the Field and Robot is such that:

- an event (x, y) on the field is related to an approximated position event $(\lfloor x \rfloor, \lfloor y \rfloor)$ in a robot observation;
- a move event $d(i)$ of robot i in direction d is related to a speed event $\mathbf{v}_i$ on the field.

Σ_{FR} is co-inductively defined.

Algebra of Components

Product

We fix two components $C_1 = (E_1, L_1)$ and $C_2 = (E_2, L_2)$.
We fix an interaction signature $\Sigma = (R, \oplus)$.

A product $C_1 \times_\Sigma C_2$ is a component (E, L) with

- $E = E_1 \cup E_2$, and
- for all $\sigma_1 \in L_1$ and $\sigma_2 \in L_2$, $(\sigma_1, \sigma_2) \in R$ implies $\sigma_1 \oplus \sigma_2 \in L$.

Component

Example sequence

		R_1
R_3		R_2

t	$\sigma : (R_1 \times_{\Sigma_{free}} R_2 \times_{\Sigma_{free}} R_3) \times_{\Sigma_{RF}} F$
t_1	$\{N(1), v_1\}$
t_2	$\{r(1, (\lfloor x \rfloor; \lfloor y \rfloor)), (x; y)_1\}$
t_3	$\{E(2), v_2\}$
t_4	$\{r(2, (\lfloor x \rfloor; \lfloor y \rfloor)), (x; y)_2\}$
$\dots$	$\dots$

Specification

Construction of components

Given C_1 and C_2 two components, and Σ an interaction signature, we search for a step-by-step construction of a behavior in the composition $C_1 \times_\Sigma C_2$.

Challenge for a sound runtime composition:

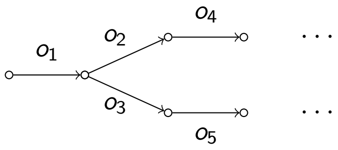
- Let C^* be the component whose behavior contains every prefixes of $\sigma : C$, completed with empty observations.
- In general, there exist some components C_1 and C_2 such that:

$$C_1^* \times_\Sigma C_2^* \neq (C_1 \times_\Sigma C_2)^*$$

Specification

TES transition system

We define a TES transition system $\mathcal{T} = (E, Q, \rightarrow)$ where transitions are labeled with observations (set of events with a time stamp):



Given a state $q \in Q$ of $\mathcal{T}$, we give two equivalent semantics of $\mathcal{T}$ as component $[\![\mathcal{T}(q)]\!]$ using:

- infinite paths on $\mathcal{T}$ whose sequence of labels form a TES;
- greatest post fix point.

Specification

Composition

We define a family of products $\star_\kappa$ on TES transition systems and we show compositionality:

$$[\![\mathcal{T}_1(q_1) \star_\kappa \mathcal{T}_2(q_2)]\!] = [\![\mathcal{T}_1(q_1)]\!] \times_\Sigma [\![\mathcal{T}_2(q_2)]\!]$$

where $\Sigma = ([\kappa], \cup)$.

Moreover, we show condition for two $\mathcal{T}_1$ and $\mathcal{T}_2$ such that:

$$[\![\mathcal{T}_1 \star_\kappa \mathcal{T}_2]\!]^* = [\![\mathcal{T}_1]\!]^* \times_\Sigma [\![\mathcal{T}_2]\!]^*$$

In which case, we say that $\mathcal{T}_1$ and $\mathcal{T}_2$ are κ-compatible.

Specification

Towards an implementation

Two restrictions:

- we restrict to a fragment of TES transition systems with integer time and arbitrary shift:

$$\textit{if} \;\; q \xrightarrow{(O,n)} q', \; \textit{then} \;\; q \xrightarrow{(O,n+k)} q'$$

  for all $k \in \mathbb{N}$.

- we assume TES transition systems to be κ-compatible.

Simulation

Scenario

We implemented the framework in Maude.
We specify the following system:

R_3	R_2	R_1

where:

- each R_i can go in any direction at any step;
- the field is a grid that excludes two robots to move on the same location;
- a protocol $S(R_i, R_j)$ may swap R_i with R_j if R_i is on the adjacent east position of R_j.

Properties:

$$P_{sorted}\text{: eventually } R_i \text{ is on position } (i;0).$$
$$P_b\text{: eventually } B_i \text{ has energy } 0.$$

System:

$$\underset{1\leq i\leq 3}{\times_{\Sigma_{free}}}(R_i \times_{\Sigma_{RB}} B_i) \times_{\Sigma_{RF}} F$$

Results:

- P_{sorted} is verified: 12.10^3 states, 25s, 31.10^6 rewrites
- P_b is true

Simulation
Results

Properties:

$$P_{sorted}\text{: eventually } R_i \text{ is on position } (i;0).$$
$$P_b\text{: eventually } B_i \text{ has energy } 0.$$

System:

$$\Big(\mathop{\times_{\Sigma_{sync}}}_{1 \le i < j \le 3} S(R_i, R_j)\Big) \times_{\Sigma_{SR}} \Big(\mathop{\times_{\Sigma_{free}}}_{1 \le i \le 3} (R_i \times_{\Sigma_{RB}} B_i)\Big) \times_{\Sigma_{RF}} F$$

Results:

- P_{sorted} is verified: 8250 states, 71s, 83.10^6 rewrites
- P_b is false

Conclusion

We proposes an algebra of components with parametrized products to model interaction in cyber-physical systems.

We give a semantics for labeled transition systems as components, and prove its compositionality.

We exposed some conditions for a sound step-by-step composition at runtime.