On the Reaction Time of Some Synchronous Systems

Ilias Garnier, Christophe Aussagès, Vincent David, Guy Vidal-Naquet

June 9, 2011

Plan

- Context
- Formal model
- Reaction time
- Compositionality of reaction time
- Applications to refinement

© CEA. All rights reserved

Context: real-time embedded systems

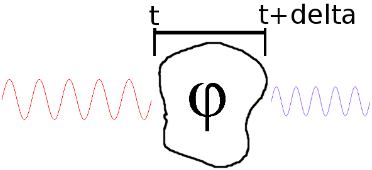
Real-time embedded systems: computer systems interacting with the physical environment under strong timing constraints.

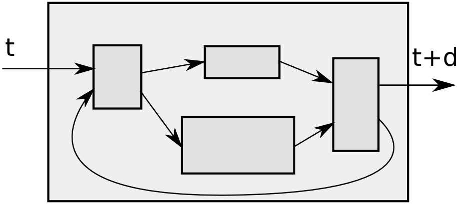
- Studied systems: synchronous system
- Study of delay of significant reaction time, called here **reaction time**

© CEA. All rights reserved

Motivation: introducing reaction time

Analogy: wave through a physical medium





Reaction time ≈ delay between input and **functionally dependent** output.

© CEA. All rights reserved

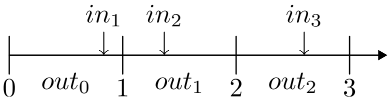
Introducing synchronous systems

Our study concentrates on the Moore model of **synchronous** computation.

Synchronous round of computation

- Observable output part of the state
- Next state depends on input and current state

Synchronous computation = (possibly infinite) succession of rounds. When state space is finite, defines a *Moore machine*.



© CEA. All rights reserved

Investigating reaction time

- What does it *mean* to **react** to an input ?
  - existence of an "observable effect"
  - observable state is a function of the input
  - $\Rightarrow$ **need a formal notion of observational equivalence**
- What is a reaction **time** ?
  - in our case, number of transitions until observable effect
- Is it **compositional** ?
  - in this presentation, study of sequential composition

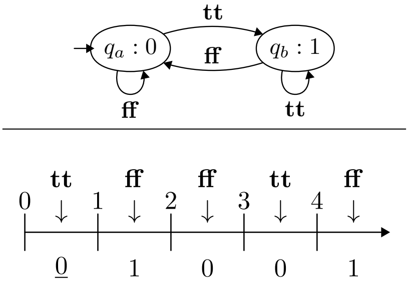
© CEA. All rights reserved

Moore machines

Moore machine = FSM where states are labelled with output. Let **In** set of inputs, **Out** set of outputs, $\mathcal{M} = \langle \mathbf{In}, \mathbf{Out}, Q, E, \mathbf{out} \rangle$.

- Q finite set of states,
- $E \subseteq Q \times \mathbf{In} \times Q$ edges, <u>Input-enabled</u>
- $\mathbf{out} : Q \to \mathbf{Out}$ outputs.

Quick example: outputs 0 on **ff**, outputs 1 on **tt**:

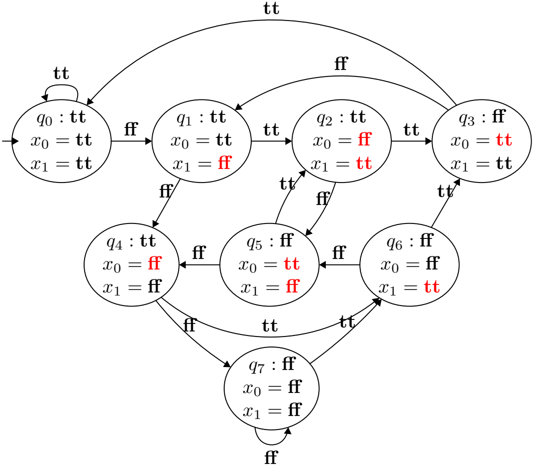


© CEA. All rights reserved

Bigger example

A synchronous program and its corresponding machine

x_0 := **true**;
x_1 := **true**;
next(**true**);
while true do
    next(x_0);
    x_0 := x_1;
    x_1 := **input**
done



© CEA. All rights reserved

Observational equivalence

In order to define observational **difference**, we need to define observational **equivalence**. We choose bisimilarity (finest-grained). Let p, q be two states.

$$
\begin{aligned}
p \sim q \quad \leftrightarrow \quad & \mathbf{out}(p) = \mathbf{out}(q) \ \wedge \\
& \forall a, \forall p \xrightarrow{a} p', \exists q \xrightarrow{a} q', p' \sim q' \ \wedge \\
& \forall a, \forall q \xrightarrow{a} q', \exists p \xrightarrow{a} p', p' \sim q'
\end{aligned}
$$

Intuitive view: $p \sim q$ is simply equality on **infinite unfoldings** starting from p and q.

© CEA. All rights reserved

Reaction time: case of total functions

Recall that reaction time $\approx$ delay between input and **related** output. "Related" means **functional dependency** between input and output.

$f : D \to E$ a total function. We have:

$$f \text{ constant} \leftrightarrow f(D) = \{e\}$$

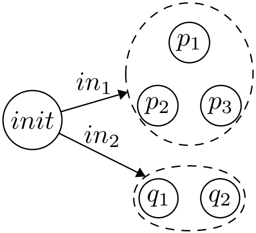
$$f \text{ non-constant} \leftrightarrow \exists d_1, d_2, d_1 \neq d_2 \wedge f(d_1) \neq f(d_2)$$

(d_1, d_2) allows to prove f non-constant: **separating pair**.

© CEA. All rights reserved

Reaction time: states of Moore machines

state = function from inputs to set of states



reached sets P, Q not equivalent when $\exists\ p_i \in P$ s.t. $\forall q_j \in Q$, $p_i \not\sim q_j$ (or the other way around).

Reaction time

Given $p \not\sim q$, we want to study how many transitions are needed to have an *observable effect*.

© CEA. All rights reserved

Observable effects

Observable effects extracted from proofs of **non-bisimilarity**
Inductive definition of $p \nsim q$:

$$\text{BASE}\ \frac{}{\mathbf{out}(p) \neq \mathbf{out}(q) \to p \nsim q}$$

$$\text{IND}\ \frac{\exists p \xrightarrow{a} p', \forall q \xrightarrow{a} q', p' \nsim q' \ \vee\ \exists q \xrightarrow{a} q', \forall p \xrightarrow{a} p', p' \nsim q'}{p \nsim q}$$

$$\left.\begin{array}{l} p = p_0 \xrightarrow{a_0} p_1 \xrightarrow{a_1} p_2 \dots p_n \\ q = q_0 \xrightarrow{a_0} q_1 \xrightarrow{a_1} q_2 \dots q_n \end{array}\right| \text{ s.t. } \mathbf{out}(p_n) \neq \mathbf{out}(q_n).$$

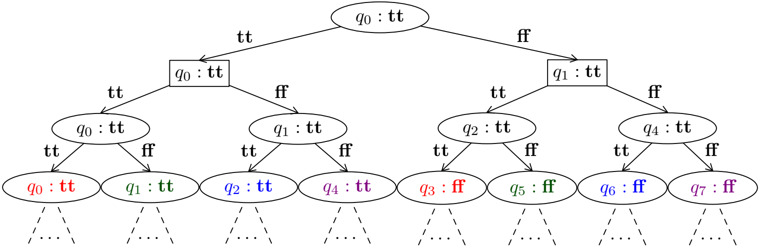
Observable effect, separator

The pair $(\mathbf{out}(p_n), \mathbf{out}(q_n))$ is an *observable effect*. The word $a_0.a_1 \dots a_{n-1}$ is called a *separator*.

© CEA. All rights reserved

Observable effects example

Unfolding of state q_0 of delay program.

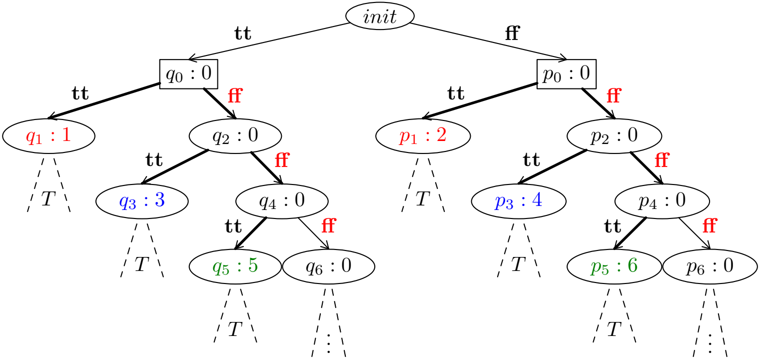


In this case, every word of length 2 is a separator.

© CEA. All rights reserved

Observable effects example (cont.)

An unfolding where **ff*** does not contain separators.



© CEA. All rights reserved

From obs. effects to reaction time

1. Reactivity of a state q ($\equiv$ non-constantness) $\leftrightarrow$ $\exists$ **separating pair** of inputs $in_1 \neq in_2$ s.t. $q \xrightarrow{in_1} Q_1, q \xrightarrow{in_2} Q_2$ and set Q_1 not equivalent to set Q_2
2. Any proof of $q_i \nsim q_j$ yields an **observable effect** triggered by a particular input word called **separator**;
   - in a non-deterministic fashion: **may**-separator
   - for all runs of the separator: **must**-separator

Reaction time

Exists **iff** all infinite input words are prefixed by a must-separator. It is the worst-case number of transitions necessary to obtain the **first** observable effect.

© CEA. All rights reserved

Compositionality

Computing separators and observable effects in order to obtain reaction time is costly.

Compositionality property

Given machines M_1, M_2 and binary composition operation $\mathcal{C}$, can we compute the observable effects of the composed machine $\mathcal{C}(M_1, M_2)$ without performing the whole state-space exploration ?

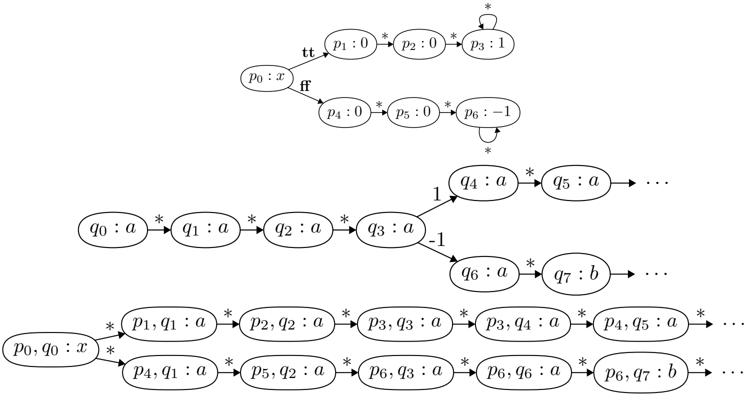
I.e. how easily can we compute the observable effects of $\mathcal{C}(M_1, M_2)$ given those of M_1 and M_2 ?
In our case, $\mathcal{C} = \circ$, the sequential composition.

© CEA. All rights reserved

Sequential composition of states

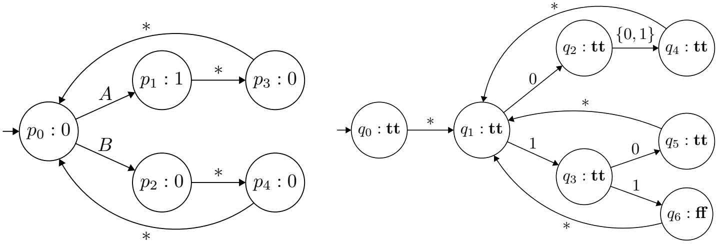
Compound state space = cartesian product. Compound transition exists iff receiving transition labelled by output of sending state.

$$\frac{q_f \xrightarrow{in_f} q_f' \qquad q_g \xrightarrow{\textbf{out}(q_f)} q_g'}{(q_f, q_g) \xrightarrow{in_f} (q_f', q_g')} \qquad \frac{}{\textbf{out}(q_g \circ q_f) = \textbf{out}(q_g)}$$

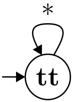


© CEA. All rights reserved

Necessity of a well-behaved composition



States q_6 becomes unreachable in composition, states q_2 and q_3 no more separable. Sequential composition yields



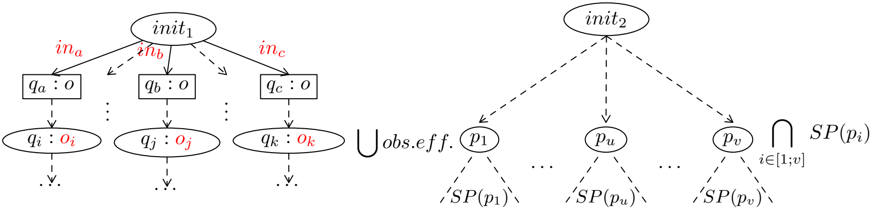
Moore machines: to compute all compound obs. effects, full state space search necessary.

Possible solution: under-approximate obs. effects until they are compositional.

© CEA. All rights reserved

Approximating obs. effects

Core idea: reduce branching property to a linear one.



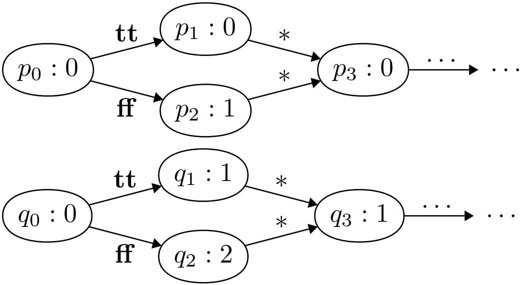
linear time criterion: $init_2 \circ init_1$ reactive if $\bigcup obs.effects \subseteq \bigcap SP(q_i)$

Problem: sets of separating pairs and obs. effects can be complex.

© CEA. All rights reserved

Determinism and separability

Solution 2: restriction to sep. pairs and obs. effects present for all input words, i.e. **deterministic sep. pairs and obs. effects**.



context **tt**.**bool***, obs. effect $\emptyset.(0,1).(0,1)\dots$

context **ff**.**bool***, obs. effect $\emptyset.(1,2).(0,1)\dots$

deterministic obs. effect: $\emptyset.\emptyset.(0,1)\dots$

© CEA. All rights reserved

Refinement

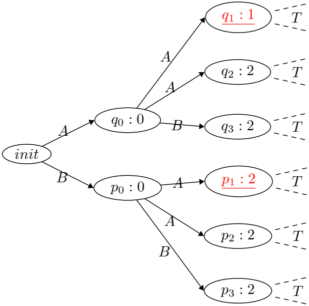
We aim at developing real-time embedded systems by *validated* stepwise refinement, s.t. the refinement step i) preserves reaction time and ii) is a congruence.

- Simulation as refinement, i.e. p refines $q \leftrightarrow p$ has less possible behaviours than q ($=$ tree inclusion)
- Problem: does simulation preserve observable effects ? Is it compositional ?

© CEA. All rights reserved

Observable effect preservation

Simulation doesn't preserve non-deterministic separators.



Corollary: observable effects and reaction time not preserved in general. Solution: consider a subset of observable effects generated by proofs of non-bisimulation which do not rely on non-determinism. I.e. Deterministic obs. effects are preserved by refinement.

© CEA. All rights reserved

Conclusion

- Reaction time can be defined in terms of observable effects, which correspond to proofs of non-bisimulation
- In general,
  - not preserved by sequential composition
  - not preserved by refinement.
- Det. obs. effects preserved

© CEA. All rights reserved