Hybrid Systems

Paul Caspi

Verimag/CNRS

- Why?
- Problems
- A proposal

Why?

- The implemention of continous control systems on computers has found a mature theory (previous lecture)

  Sampling theory, numerical analysis, stability

  $\Rightarrow$ Periodic and multi-periodic sampling, Simulink, synchronous languages, time-triggered systems, . . .)

Why?

- There is also a mature theory of discrete-event control:

  $\Rightarrow$ Stateflow, synchronous languages, event-triggered systems

- But most complex control systems are mixed continuous and discrete-event ones:
  - continuous control
  - modes
  - alarms,
  - fault-tolerance

  How to deal with these mixed cases ?

How to deal with these mixed cases ?

Two possible answers:

- Extend the discrete event approach to the continuous case?
  - variable step solvers ???
  - complex scheduling ???

- Extend the sampling approach to the discrete event case ?

  This is by now the most popular approach

  But it raises the question of a satisfactory theory for sampling discrete event systems

  Practitioners rely on “in-house” recipes which lack of theoretical background

⇒ “in-house” continous education, no textbooks, few research

Sampling Problems

Sampling discrete-event systems raise questions of asynchrony

- Sampling inputs is not deterministic

- Holding outputs is not deterministic

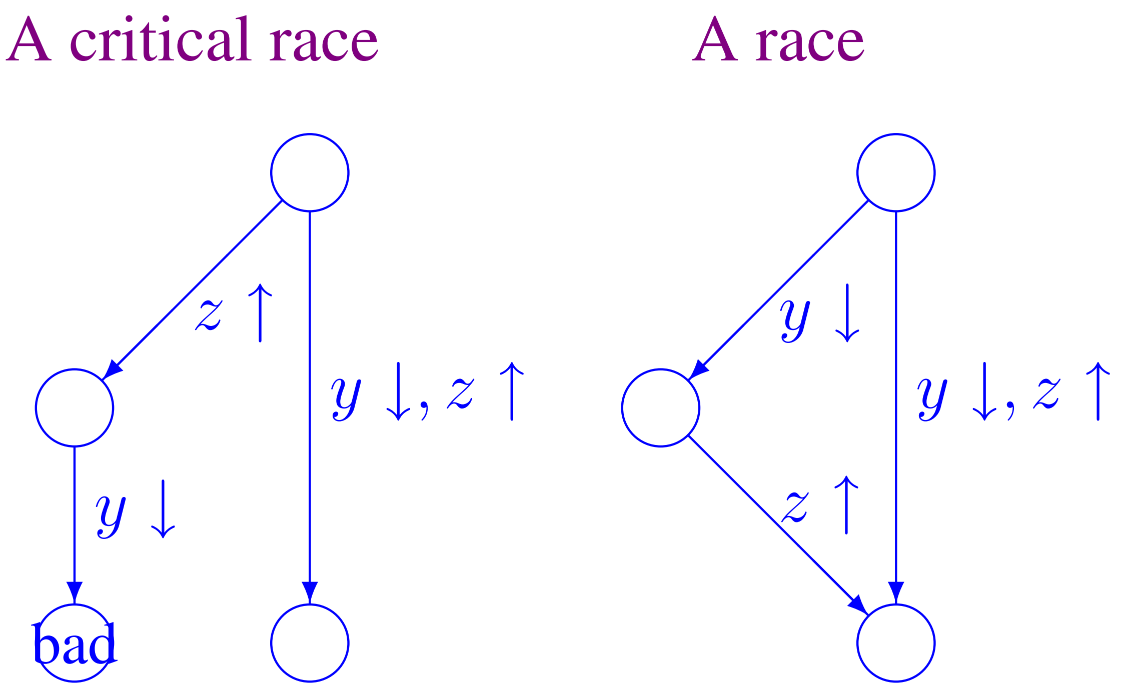
$\Rightarrow$ Possible races

Usual design and simulation tools like Simulink/Stateflow don't allow the designer to investigate it

Races

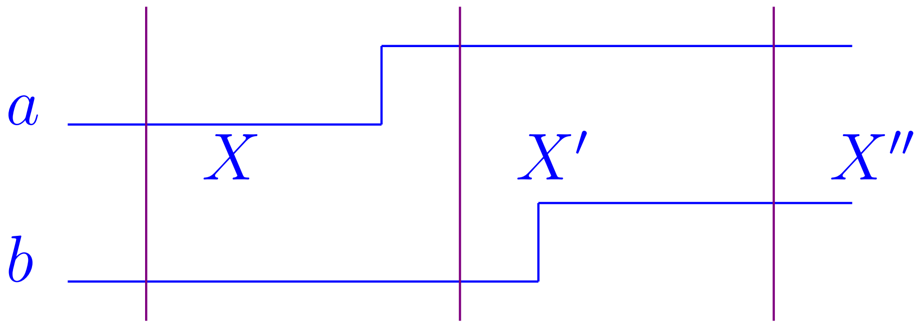
A race takes place when two discrete signals can vary either at the same time or not according to several hasards

A race becomes critical if different states can be reached according to which signal wins the race



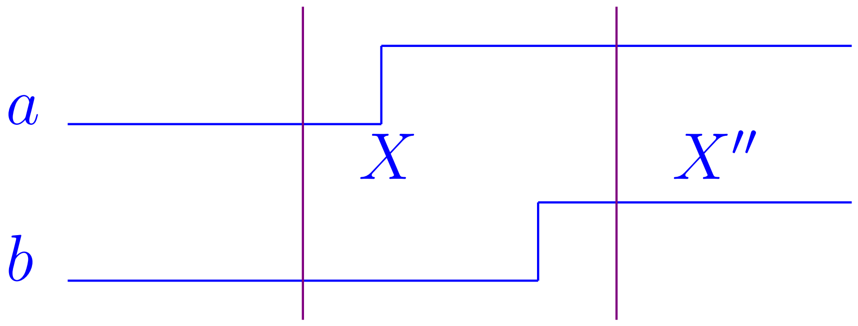
Sampling Tuples

A possible sampling



Sampling Tuples

Another possible sampling



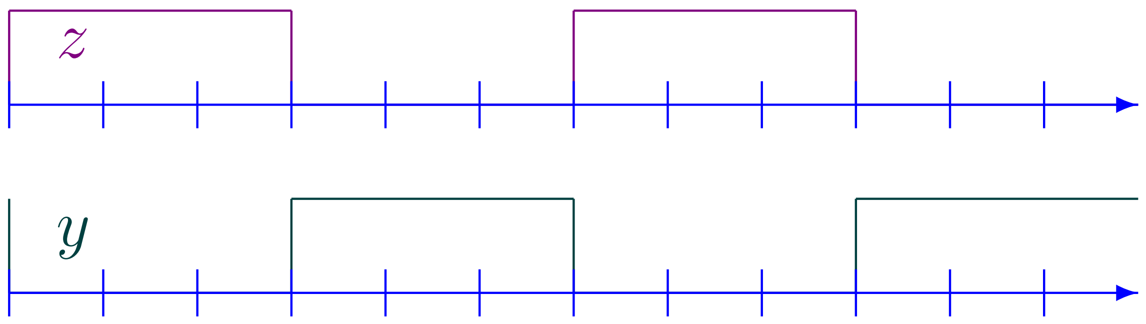
Possible race

Holding Outputs

Example : Mutual exclusion

```
always not (y and z)
```

A non robust solution :

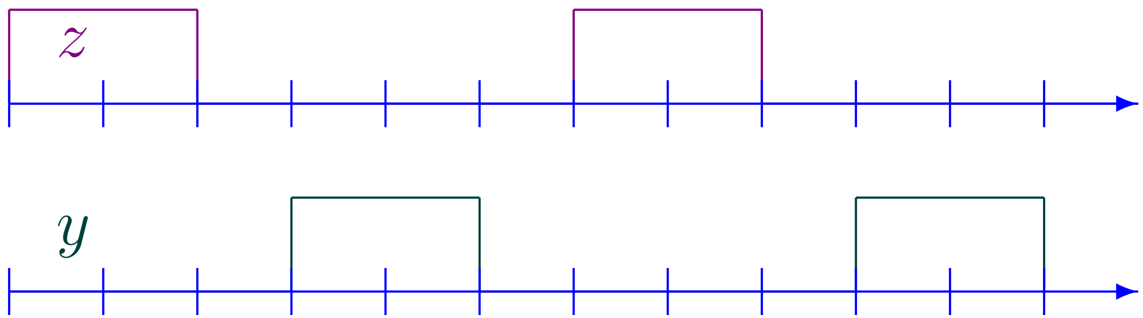


Asynchronous Recipes

Insert delays

Insert causality chains forbidding races

- z waits for y to go down before rising and conversely



Other Motivations

- Model-based development in control

  What is a model in control ?

  What is a refinement ?

- Fault-tolerance problems

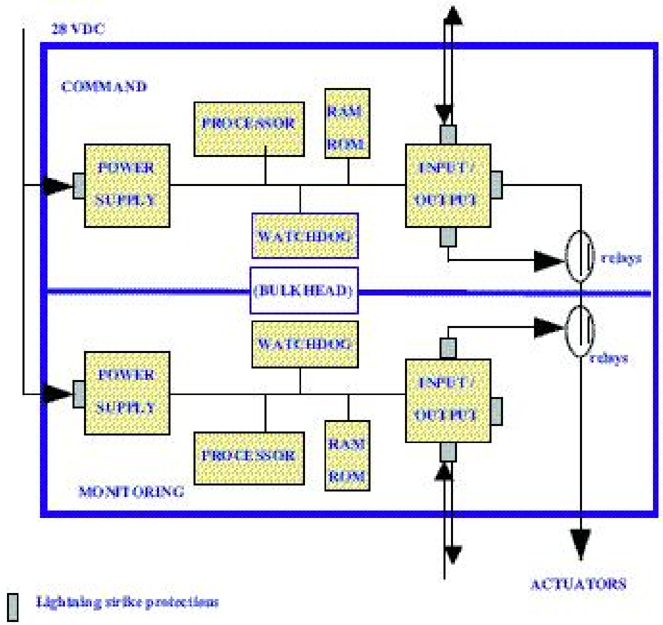
Fault-tolerance Problems

Understand voting methods used in industry (AIRBUS, and many more...)

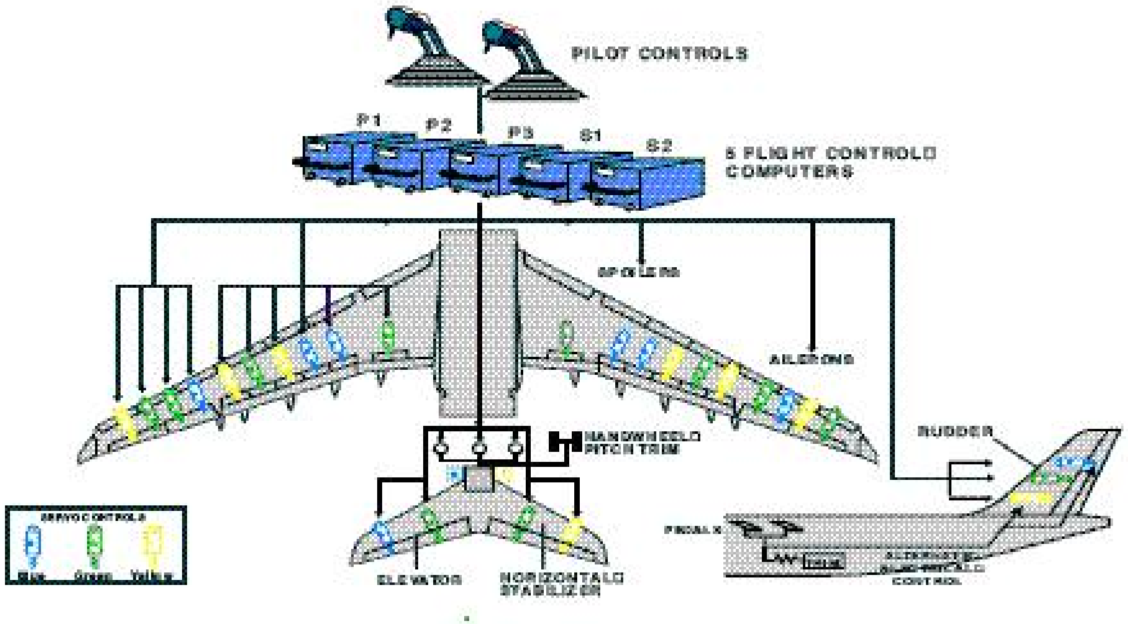
- Threshold voting
- Delay voting
- Mixed threshold-delay voting

Airbus Architecture (continued)

fault detection redondancy

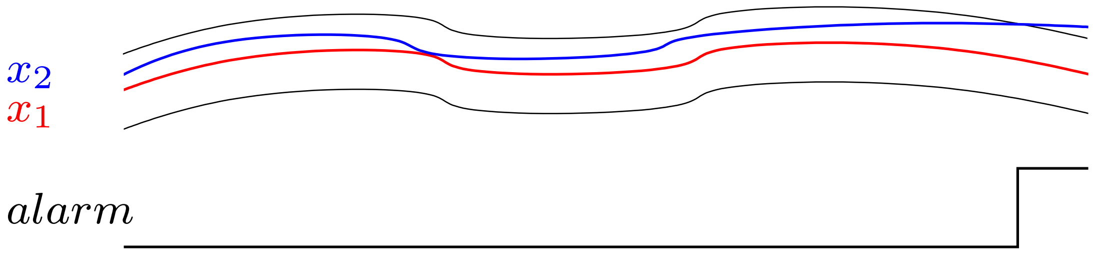


fault masking redondancy



Redundant computers have their own clocks

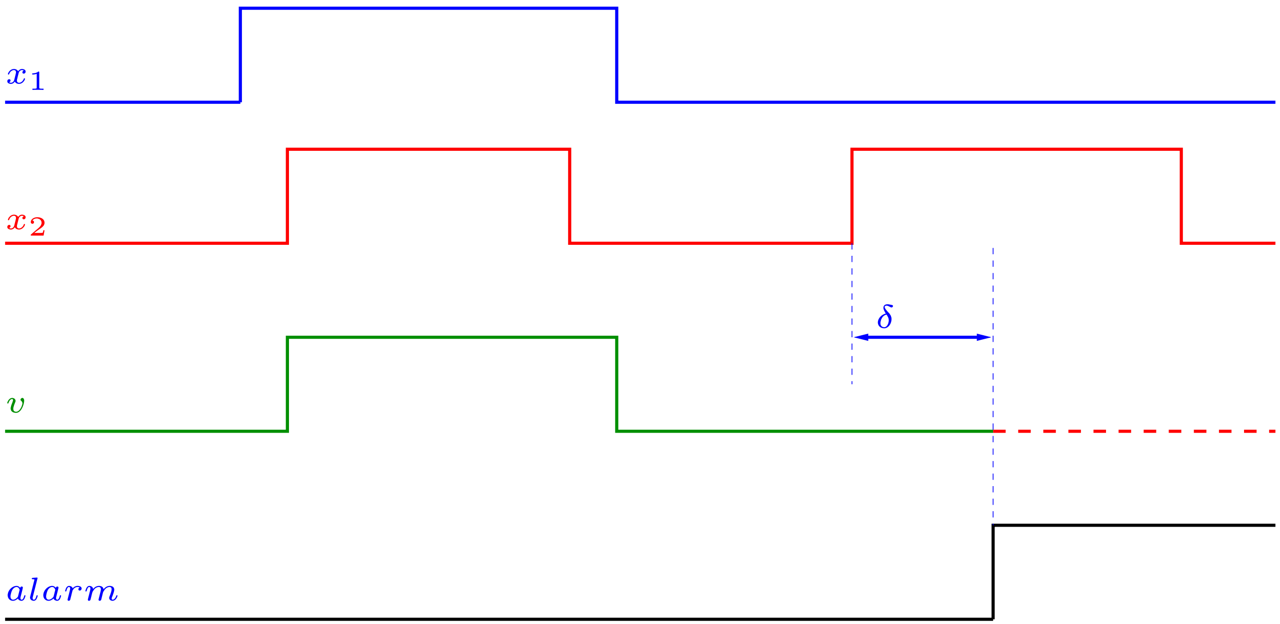
Threshold Voting



$\Rightarrow$ Based on $||.||_\infty$ norm.

This technique allows software diversity and alleviates Byzantine problems

Delay voting



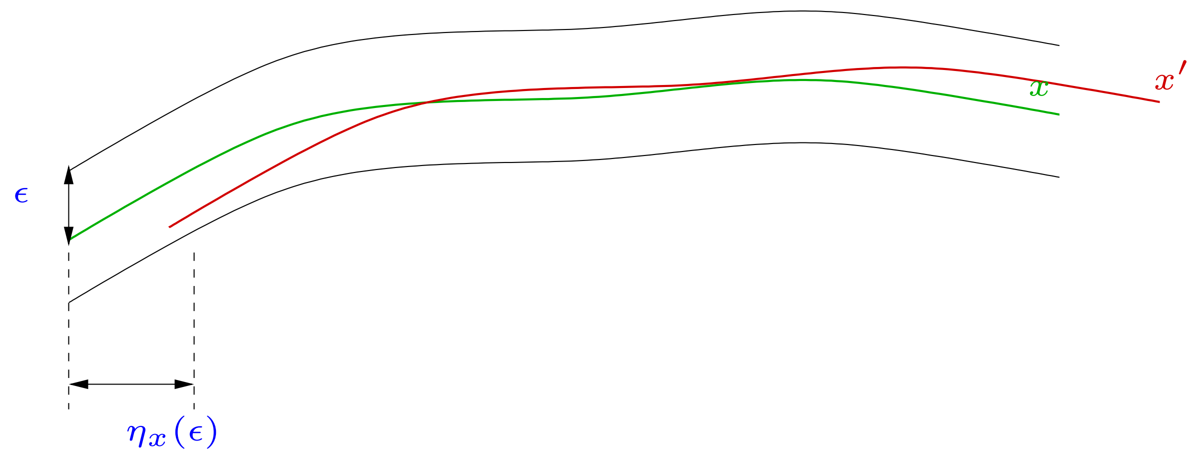
$\Rightarrow$ Based on uniform bounded variability and bounded delays

What is Lacking?

An approximation, sampling and voting theory for discrete-event and hybrid systems

Sampling Continuous Signals

A signal x is samplable if it is uniformly continuous



$$\forall \epsilon > 0, \exists \eta_x > 0, \forall t, t', |t - t'| \leq \eta_x \Rightarrow |x(t) - x(t')| \leq \epsilon$$

Retiming

Time distorsion :

- $r : T \rightarrow T$
- r non decreasing

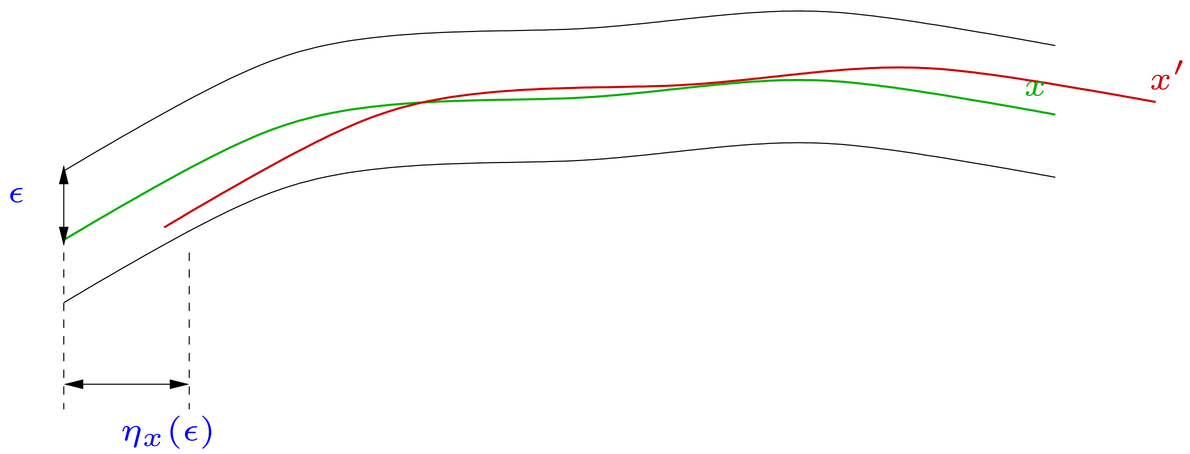
Examples:

- bounded retiming: $||r - id||_\infty \leq \delta$
- bijective retiming $=>$ continuous

- T periodic sampling: $r(t) = \left\lfloor \frac{t}{T} \right\rfloor T$
- time delay : $r(t) = t - \delta$

Sampling Continuous Signals

A signal x is samplable if it is uniformly continuous



$$\forall \epsilon > 0, \exists \eta_x > 0, \forall t, t', |t - t'| \leq \eta_x \Rightarrow |x(t) - x(t')| \leq \epsilon$$

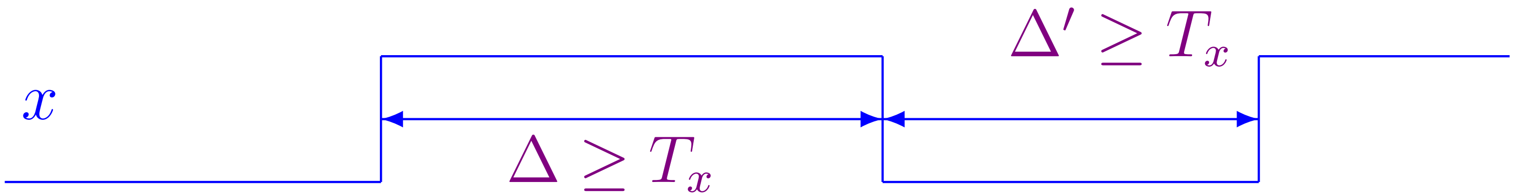
which can be restated as:

$$\exists \eta_x > 0, \forall \epsilon > 0, \forall \; retiming \; r, ||r - id||_\infty \leq \eta_x(\epsilon) \Rightarrow ||x - x \circ r||_\infty \leq \epsilon$$

A First Attempt

Samplable boolean signals are bounded variability signals :

There exists a minimal stable time $T_x > 0$ associated with signal x.



These signals are also those uniformly continuous with respect to the Skorokhod distance(Caspi Benveniste 02)

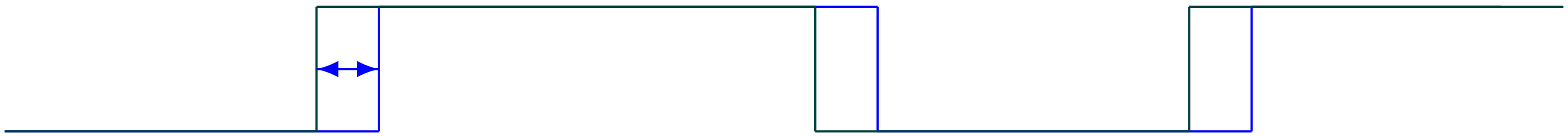
Allows a natural extension to hybrid signals

Skorokhod distance

Based on bijective retiming :

$$d_S(x,y) = \inf_{r \in BR} ||r - id||_\infty + ||x \circ r - y||_\infty$$

Boolean example : the worst shift between corresponding edges



Problem : combinational boolean functions are not UC: too fine topology

Same problem with the Tube distance of Henzinger et al.

A new approach

Topology based on a family of open balls:

$$B(x;T,\epsilon) = \{\ y \mid \sup_t \int_t^{t+T} \frac{|x-y|}{T} < \epsilon\ \}$$

Properties:

- Defines indeed a topology
- Generalises the $||\ ||_\infty$ distance

$$\lim_{T \to 0} \sup_t \int_t^{t+T} \frac{|x-y|}{T} = ||x-y||_\infty$$

It is a topology

It suffices to show that any point of a ball is the center of another ball which is a subset of the former.

Let $x' \in B(x;T,\epsilon)$. It yields: $\sup_t \int_t^{t+T} \frac{|x'-x|}{T} = d < \epsilon$

Let us take

$$T' = T \qquad \epsilon' = (\epsilon - d)$$

Let $x'' \in B(x';T',\epsilon')$ and let us show that x'' belongs to $B(x;T,\epsilon)$: for any t,

$$\int_t^{t+T} |x''-x| \leq \int_t^{t+T} |x''-x'| + \int_t^{t+T} |x'-x|$$

$$\int_t^{t+T} |x''-x| < \epsilon' T + dT$$

It is a topology

It suffices to show that any point of a ball is the center of another ball which is a subset of the former.

Let $x' \in B(x; T, \epsilon)$. It yields: $\sup_t \int_t^{t+T} \frac{|x' - x|}{T} = d < \epsilon$

Let us take

$$T' = T \qquad \epsilon' = (\epsilon - d)$$

Let $x'' \in B(x'; T', \epsilon')$ and let us show that x'' belongs to $B(x; T, \epsilon)$: for any t,

$$\int_t^{t+T} |x'' - x| < \epsilon' T + dT$$

$$\int_t^{t+T} |x'' - x| < (\epsilon - d)T + dT$$

It is a topology

It suffices to show that any point of a ball is the center of another ball which is a subset of the former.

Let $x' \in B(x; T, \epsilon)$. It yields: $\sup_t \int_t^{t+T} \frac{|x' - x|}{T} = d < \epsilon$

Let us take

$$T' = T \qquad \epsilon' = (\epsilon - d)$$

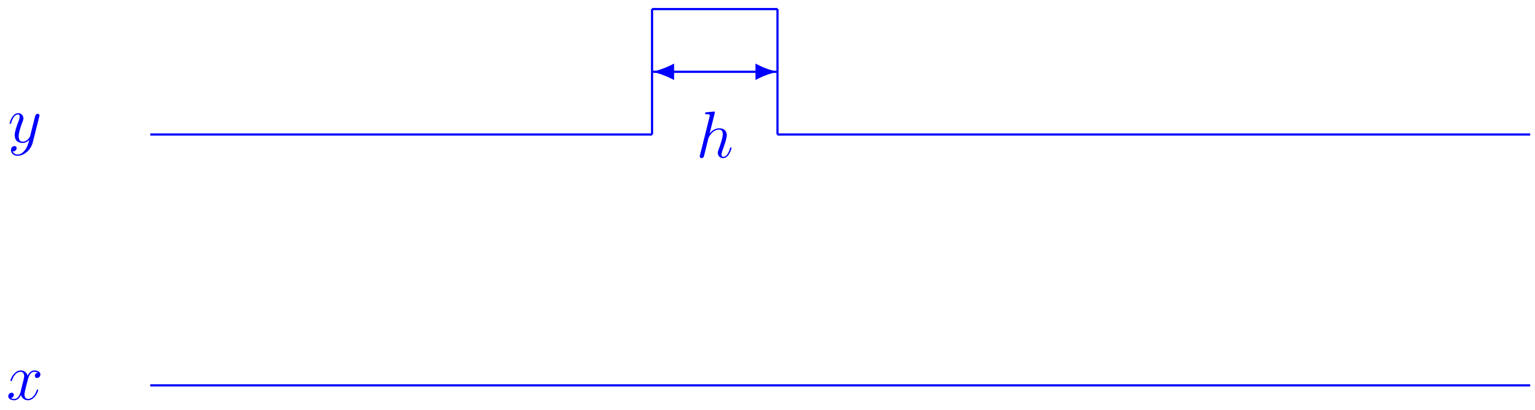
Let $x'' \in B(x'; T', \epsilon')$ and let us show that x'' belongs to $B(x; T, \epsilon)$: for any t,

$$\int_t^{t+T} |x'' - x| < (\epsilon - d)T + dT$$

$$\int_t^{t+T} |x'' - x| < \epsilon T$$

Interest

Filters short transients



x and y are neighbours when h gets small, which is the case neither with Skorokhod nor with Tube

Uniformly continuous signals

Signal x is UC if there exists a positive function $\eta_x(T, \epsilon)$ such that

- for all $\epsilon, T > 0$,
- for all r with $||r - id||_\infty \leq \eta_x(T, \epsilon)$

$x \circ r$ belongs to $\bar{B}(x; T, \epsilon)$

Examples :

- Uniformly continuous signals in the usual sense
- Uniform bounded variability boolean signals

Uniformly continuous signals

Fundamental property

Let x UC with $\eta_x(T, \epsilon)$

For any ϵ, T, there exists in any time interval of duration T a sub-interval of duration $\eta_x(T, \epsilon)$ such that for all t, t' in this sub-interval,

$$|x(t) - x(t')| \leq 2\epsilon$$

We can see the deviation with respect to usual UC

Allows designing UC checkers and voters (Airbus)

Uniformly continuous signals

Fundamental property

Let x UC with $\eta_x(T, \epsilon)$

For any ϵ, T, there exists in any time interval of duration T a sub-interval of duration $\eta_x(T, \epsilon)$ such that for all t, t' in this sub-interval,

$$|x(t) - x(t')| \leq 2\epsilon$$

Compare with ordinary UC:

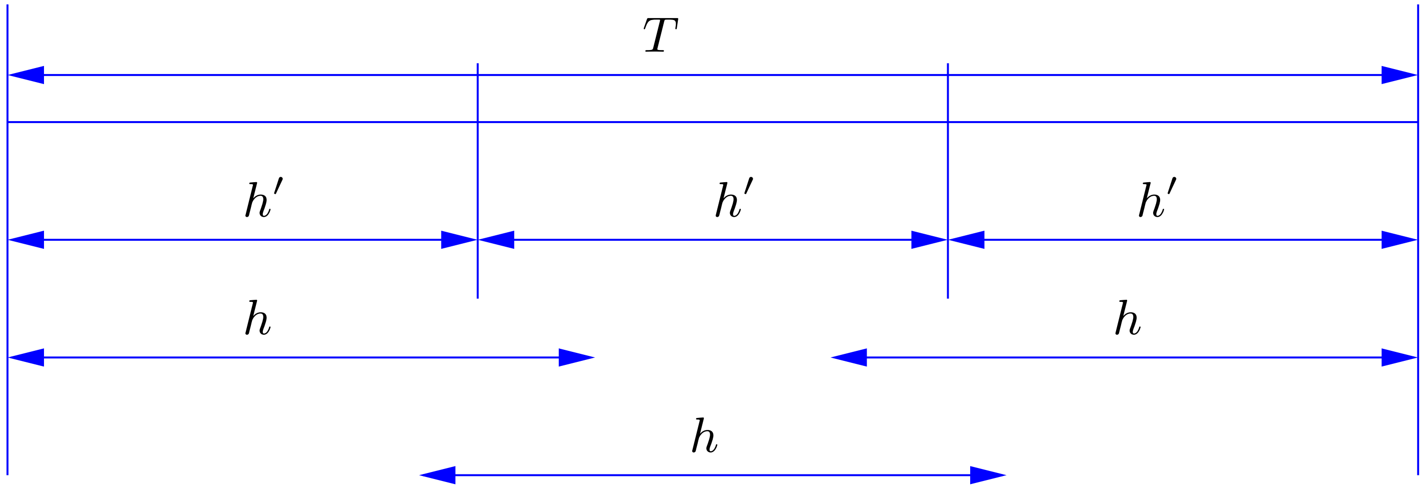
Let x ordinary UC with $\eta_x(\epsilon)$

For any ϵ, in any time interval of duration $\eta_x(\epsilon)$, for all t, t' in this interval,

$$|x(t) - x(t')| \leq \epsilon$$

Proof

Let us divide an arbitrary interval I of duration T into n equal sub-intervals $I_i, i = 1, n$ of duration h.



Proof

Let us divide an arbitrary interval I of duration T into n equal sub-intervals $I_i, i = 1, n$ of duration h.

Let: $x_i^M = \sup_{t \in I_i} x(t) \quad x_i^m = \inf_{t \in I_i} x(t) \quad e_i = x_i^M - x_i^m$

It is easy to design two retimings r^M et r^m such that forall $t \in I_i$,

$$x \circ r^M(t) = x_i^M \quad , \quad x \circ r^m(t) = x_i^m$$

We have moreover:

$$\sup_t |r^M(t) - t| \leq \eta_x(T, \epsilon) \quad , \quad \sup_t |r^m(t) - t| \leq \eta_x(T, \epsilon)$$

Thus,

$$\int_I \frac{|x - x \circ r^M|}{T} \leq \epsilon \quad , \quad \int_I \frac{|x - x \circ r^m|}{T} \leq \epsilon$$

Proof

Let us divide an arbitrary interval I of duration T into n equal sub-intervals $I_i, i = 1, n$ of duration h.

Let: $x_i^M = \sup_{t \in I_i} x(t) \quad x_i^m = \inf_{t \in I_i} x(t) \quad e_i = x_i^M - x_i^m$

It is easy to design two retimings r^M et r^m such that forall $t \in I_i$,

$$x \circ r^M(t) = x_i^M \quad , \quad x \circ r^m(t) = x_i^m$$

$$\int_I \frac{|x - x \circ r^M|}{T} \leq \epsilon \quad , \quad \int_I \frac{|x - x \circ r^m|}{T} \leq \epsilon$$

By triangular inequality, we get:

$$\int_I \frac{|x \circ r^M - x \circ r^m|}{T} \;\leq\; 2\epsilon$$

Proof

Let us divide an arbitrary interval I of duration T into n equal sub-intervals $I_i, i = 1, n$ of duration h.

Let: $x_i^M = \sup_{t \in I_i} x(t) \quad x_i^m = \inf_{t \in I_i} x(t) \quad e_i = x_i^M - x_i^m$

It is easy to design two retimings r^M et r^m such that forall $t \in I_i$,

$$x \circ r^M(t) = x_i^M \quad , \quad x \circ r^m(t) = x_i^m$$

$$\int_I \frac{|x \circ r^M - x \circ r^m|}{T} \leq 2\epsilon$$

Finally,

$$\sum_1^n \frac{h}{T} e_i \leq 2\epsilon$$

Proof

Let us divide an arbitrary interval I of duration T into n equal sub-intervals $I_i, i = 1, n$ of duration h.

Let: $x_i^M = \sup_{t \in I_i} x(t) \quad x_i^m = \inf_{t \in I_i} x(t) \quad e_i = x_i^M - x_i^m$

It is easy to design two retimings r^M et r^m such that forall $t \in I_i$,

$$x \circ r^M(t) = x_i^M \quad , \quad x \circ r^m(t) = x_i^m$$

Finally,

$$\sum_1^n \frac{h}{T} e_i \leq 2\epsilon$$

If all e_i were larger than 2ϵ, this would be also true for their mean value. Thus, at least one e_i is smaller than or equal to 2ϵ.

Mixed threshold delay voters

If x and x' are UC and if

$$x' \in \bar{B}(x; T, \epsilon)$$

then, there exists T' such that, in any time interval of duration T there exists a sub-interval of duration T' such that for all t, t' in this sub-interval,

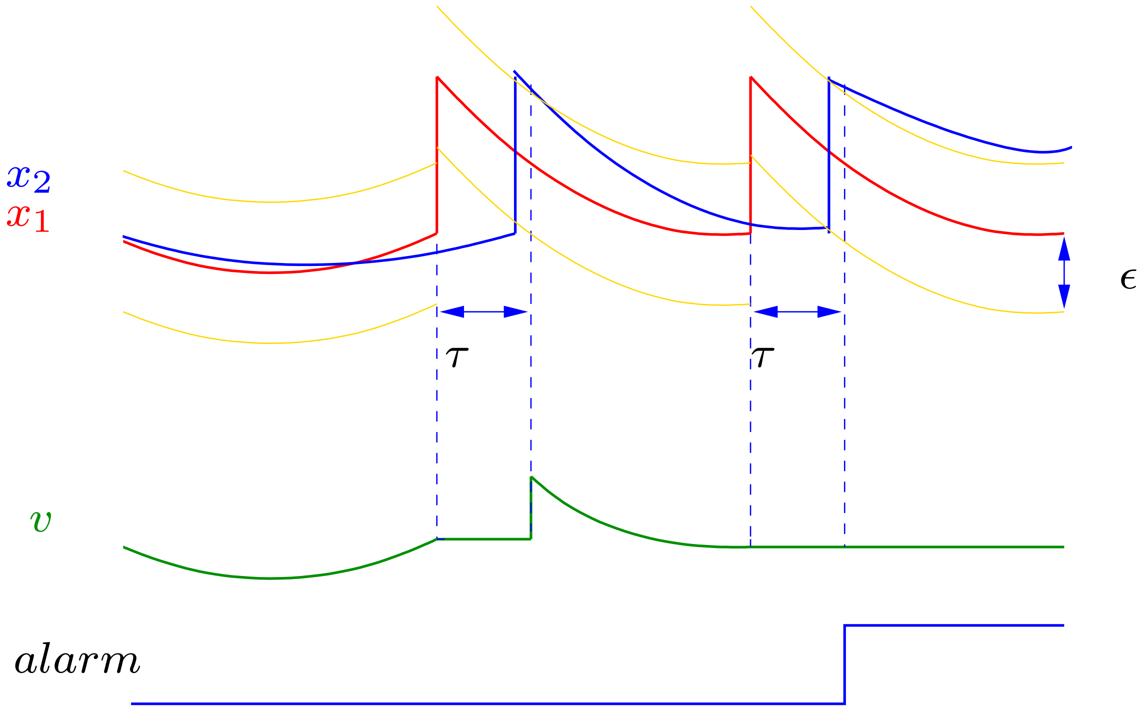
$$|x(t) - x(t')| \leq 3\epsilon$$

Corollary :

If the sampling period is smaller than T', two fault-free replicas cannot differ of more than 3ϵ for longer than $T - T'$

This is exactly the principle of Airbus $2/2$ voters

Mixed threshold delay voters



Uniformly continuous systems

System S is UC if there exists a positive function $\eta_S(T, \epsilon)$ such that

- for all $T, \epsilon > 0$,
- for all x, x' with x' in $\bar{B}(x; \eta_S(T, \epsilon))$

$S(x')$ belongs to $\bar{B}(S(x); T, \epsilon)$

Examples:

- LTI asymptotically stable systems
- Combinational boolean systems

LTI assymptotically stable systems

An asymptotically stable LTI system S is such that there exists a an impulse response h_S with:

$$S(x)(t) = \int_{-\infty}^{\infty} h_S(u)x(t-u) \quad , \quad \int_{-\infty}^{\infty} |h_S| = K_S < \infty$$

Thus, for any x, x', T, t,

$$\begin{aligned}
& \int_t^{t+T} |S(x'(v) - S(x)(v)|/T \\
= \; & \int_t^{t+T} | \int_{-\infty}^{\infty} h_S(u)[x'(v-u) - x(v-u)]|/T \\
\leq \; & \int_t^{t+T} \int_{-\infty}^{\infty} |h_S(u)||x'(v-u) - x(v-u)|/T \\
\leq \; & \int_{-\infty}^{\infty} |h_S(u)| \int_t^{t+T} |x'(v-u) - x(v-u)|/T
\end{aligned}$$

LTI assymptotically stable systems

Thus, for any x, x', T, t,

$$
\begin{aligned}
& \int_t^{t+T} |S(x'(v) - S(x)(v)|/T \\
\leq \;& \int_{-\infty}^{\infty} |h_S(u)| \int_t^{t+T} |x'(v-u) - x(v-u)|/T \\
\leq \;& \int_{-\infty}^{\infty} |h_S(u)| \sup_t \int_t^{t+T} |x'(v-u) - x(v-u)|/T \\
\leq \;& K_S \sup_t \int_t^{t+T} |x'(v-u) - x(v-u)|/T
\end{aligned}
$$

It suffices then to choose:

$$\eta_S(T, \epsilon) = T, \frac{\epsilon}{K_S}$$

to get the announced result.

Boolean Combinational Systems

Let us show the proof for a boolean function f with two inputs. It suffices to take:

$$\eta_f(T, \epsilon) = (T, T), (\epsilon/2, \epsilon/2)$$

Let us first remark that if $\epsilon \geq 1$ the property is obvious.

Let us assume $\epsilon < 1$ and $x'_1 \in \bar{B}(x_1; T, \epsilon/2), x'_2 \in \bar{B}(x_2; T, \epsilon/2)$. This amounts to saying that in any interval of duration T, x'_1 differs from x_1 for some fraction of time $\epsilon/2 < 0.5$ and similarly for x_2, x'_2. It is then clear that the couple x'_1, x'_2 differs from couple x_1, x_2 for a fraction of time at most equal to ϵ. This is also the case for $f(x'_1, x'_2)$ and $f(x_1, x_2)$.

Conclusion

- A theory that matches some current practices
- Generalisates usual theory
- May unify several points of view (continuous control, discrete event control, computing)

Perspectives

- A numerical analysis framework : compute and combine error functions
- Stability of discrete event and hybrid closed loop systems ?
  needs contracting operators : Airbus confirmation functions?