Unité Mixte de Recherche 5104 CNRS - INPG - UJF
Centre Equation
2, avenue de VIGNATE
F-38610 GIERES
tel : +33 456 52 03 40
fax : +33 456 52 03 50
http://www-verimag.imag.fr

Approximation, Sampling and Voting in Hybrid Computing Systems

Chiheb Kossentini and Paul Caspi

Verimag Research Report n^o 2005-19

January 2006

Approximation, Sampling and Voting in Hybrid Computing Systems

Chiheb Kossentini and Paul Caspi

Airbus and Verimag-CNRS

January 2006

Abstract

This report addresses the question of extending the usual approximation and sampling theory of continuous signals and systems to those encompassing discontinuities, such as found in modern distributed control systems. We provide a topological framework dealing with continuous, discrete and mixed systems in a uniform manner. We show how this theoretical framework can be used for appoximating systems, sampling and voting on hybrid signals in critical real-time systems.

Keywords: approximation, sampling, voting, hybrid systems, topology

Reviewers: Oded Maler

Notes: This work has been supported by the European Network of Excellence Artist and by the Airbus-Verimag CIFRE grant 2003-2006.
Chiheb Kossentini is with Airbus : chiheb.kossentini@airbus.com
Paul Caspi is with Verimag-CNRS : caspi@imag.fr

How to cite this report:

```
@techreport { rr,
title = { Approximation, Sampling and Voting in Hybrid Computing Systems },
authors = { Chiheb Kossentini and Paul Caspi },
institution = {  Verimag Research Report },
number = {2005-19},
year = { 2005},
note = { }
}
```

Contents

1 Introduction

This work is a continuation of previous efforts ([8, 6, 13] toward building a satisfactory theory of hybrid computing system approximation. The motivations for building such a theory are the following:

1.1 Model-based design in computer science and control

Model-based design is advocated in both theories as a method of choice for efficiently and safely building systems. However these theories differ on the way of achieving this goal:

In computer science, the proposed method (see for instance [1]) is based on successive refinements: a large specification is designed first, imprecise (non deterministic) in general, but sufficient for meeting the desired properties of the system. Then implementation details are brought in progressively, making the specification more and more precise, while keeping the properties, up to a point when it can be implemented. Clearly, this is an ideal scheme which is rarely respected, but which has a paradigmatic value.

In control science, on the contrary, an exact model is built first, which allows a control system to be designed. Then the various uncertainties that may affect the system behaviour are progressively introduced and it is checked that the designed controller is robust enough to cope with them.

Clearly, these two schemes are not, in practice, too far from each other. But, as control systems are mostly implemented by now on computers, some effort is needed, if we want them to match more closely and this can be valuable in the prospect of making easier the communication between the computer and control cultures. A way to achieve this goal can be to see the initially precise control model as representing a large class of models, those models which fall into some "distance" of this model. This distance would then represent the maximal uncertainty around this model and further refinements would make this uncertainty more precise. This goal requires thus some notion of control system approximation.

1.2 Sampling discrete event and hybrid systems

Another point of interest is that large modern control systems mix very closely continuous and discrete event systems. This is due for instance, to mode changes, alarms, fault tolerance and supervisory control. From a theoretical point of view, computer implementations of these two kinds of activity are quite different. Continuous control is dealt with through periodic sampling (time-triggered computations [12]) while discrete event systems use event-triggered implementation. However, in practice, many mixed continuous control and discrete event control systems are implemented through periodic sampling. This is the case, for instance, Airbus fly-by-wire systems and many safety-critical control systems. The problem is that there is no theory for doing it and practitioners rely on in-house "ad-hoc" methods. Building a consistent sampling theory for mixed continuous control and discrete event systems would help in strengthening these practices.

1.3 Fault-tolerance in GALS systems

Though the theory of distributed fault-tolerant systems advocates the use of clock synchronisation [16, 12], still many critical real-time systems are based on the GALS (globally asynchronous, locally synchronous), and more precisely the "Quasi-Synchronous" [7] paradigm: in this framework, each computer is time-triggered but the clocks associated with each computer are not synchronised and communication is based on periodic sampling: each computer has its own clock and periodically samples its environment, *i.e.*, the physical environment but, also, the activities of the other computers with which it communicates. When such an architecture is used in critical systems, there is a need for a thorough formalisation of fault tolerance in this framework.

1.4 Previous works

In a previous paper [8] we already formalised the concepts of threshold and delay voters. However there was in this paper some lack of symmetry between the two concepts: sampling continuous signals and threshold voting were very simply based on topological notions like uniform continuity and L_∞ norm. On the contrary, sampling discrete event signals and associated delay voting were based on more *ad-hoc* notions.

Later [6], we found that the use of the Skorokhod distance [4] was a way to overcome this lack of symmetry. More precisely, we showed that the discrete signals that could be sampled were those that were uniformly continuous with respect to this distance. This opened the way toward a generalisation to hybrid (mixed continuous-discrete) signals. Moreover, we remarked that our previous study on voters was incomplete: in practice, it appears that people do not only use threshold voters and delay voters but also, and mainly, mixed threshold and delay voters. In these voters, a failure is detected if two signals differ for more than a given threshold during more than a given delay. But, when we tried to relate those two issues [13] we found unexpected difficulties linked to the fact that the Skorokhod topology is too fine and distinguishes too many systems. It should be noted that this would be also the case for another topology which has also been proposed for robust hybrid systems [10].

1.5 Report organisation

In this report, we propose a simpler topology which seems to better meet our needs in that it:

- generalises the L_∞ norm to non continuous signals and systems;
- allows us to uniformly handle errors and bounded delays;
- provides a setting where samplable signals are those uniformly continuous with respect to this topology, and where asymptotically stable systems and combinational boolean systems are uniformly continuous systems;
- provides a foundation to mixed error and delay voters.

More precisely, we show that if two signals are within a given neighbourhood and if both of them are uniformly continuous with respect to that topology, then we can design a 2x2 hybrid voter which will not raise an alarm as long as these conditions are fulfilled. In practice, this result allows us to finely tune the voter parameters as a function of the nominal (non-faulty) errors and delays resulting from:

- the numerical and delay analysis of sensors,
- the algorithms used for computing outputs[1]
- and the architecture of communication between computing locations.

The report is organised as follows: in a second section, we provide basic definitions. Section 3 addresses the classical theory of sampling continuous signals and systems. In Section 4, we define our topology and prove the report main result on the property of signals and systems which are uniformly continuous with respect to that topology. Section 5 applies this result to the sampling and approximation problem .Finally, section 6 recalls basic voting schemes, presents the mixed (hybrid) voter and applies the theory to this voting scheme.

1.6 Related Works

Several approaches seem to have been followed for addressing the question:

- The topological approach initiated by Nerode [17, 5] explicitly introduces the approximation and then tries to characterise it as a continuous mapping. This leads to equip the approximation space with an *ad-hoc* (small) topology.
- The equivalence or property preserving approaches followed for instance in [15, 2, 9, 11] tries to construct an approximation of a given system and to check whether it is equivalent to or preserves some properties of the original system expressed in some logic.
- Finally, M. Broucke [14] mixes the two approaches and uses the Skorokhod distance in order to define an approximate bisimulation between several classes of hybrid systems. In this sense, her work is quite close from ours. However, the motivations are slightly different: it doesn't seem that uniformity is addressed and that a result similar to proposition 4.3 is obtained.

[1] We can remark that this kind of method allows the use of diverse programming [3] which is one of the ways for tolerating design and software faults

2 Basic definitions

2.1 Signals and systems

We consider systems that have to operate continuously for a long time, for instance a nuclear plant control that is in operation for weeks or an aircraft control that flies for several hours. Thus, the horizon of our signals is not bounded. Hence, a *signal* x is for us simply a piece-wise continuous function from $\Re$ to $\Re$, that is to say, a function which is continuous but on a finite or diverging sequence of times $\{t_0, \ldots t_n, \ldots\}$. This means, in particular, that left and right limits exist at each point in time. Furthermore, we assume that discontinuities are only of the first kind, such that the value at a given time is always within the interval made of left and right limits:

For all t,

$$x(t) \in [\inf(x(t^-), x(t^+)), \sup(x(t^-), x(t^+))]$$

where, as usual, $x(t^-), (x(t^+))$ is the left (right) limit of x at t.

Finally, we assume that the signal remains constant before the first discontinuity time t_0.

Concerning boolean signals, the fact that the sequence of discontinuity points diverges does not prevent from getting two consecutive discontinuity points arbitrarily close. This is why, in many cases we may need a stronger restriction:

Definition 2.1 *A boolean signal x has uniform bounded variability (UBV) if the interval between two consecutive discontinuities is lower bounded. i.e., there exists a positive (stable time) T_x between any two successive discontinuities of x.*

A *system* is simply a function S causally transforming signals, that is to say, such that $S(x)(t)$ is only function of $x(t'), t' < t$.

The *delay operator* Δ^τ is such that $(\Delta^\tau\ x)(t) = x(t-\tau)$, and a system is *stationary* (or time invariant) if $\forall \tau, S(\Delta^\tau\ x) = \Delta^\tau(S\ x)$.

An even more restricted class of systems is the class of *static or combinational* systems, that is to say, systems that are the "unfolding" of a scalar function:

$$S_f(x)(t) = f(x(t))$$

3 A sampling theory for continuous signals and systems

3.1 Uniformly continuous signals

A signal x is *uniformly continuous (UC)* (figure 1) if there exists a positive function η_x from errors to delays, such that:

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

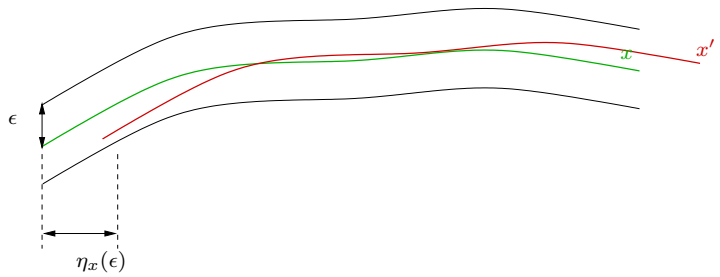

Figure 1: A uniformly continuous signal

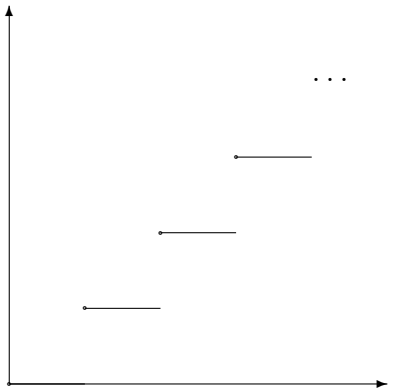

Figure 2: A periodic sampling retiming

Such a definition can be rephrased in a functional way by introducing the $||\ ||_\infty$ norm on signals, *i.e.*, for our piece-wise continuous signals with only first kind discontinuities: $||x||_\infty = \sup_t |x(t)|$,.

Then, a signal x is uniformly continuous if there exists a positive function η_x from errors to delays, such that:

$$\forall \epsilon > 0, \forall \tau, |\tau| \leq \eta_x(\epsilon) \Rightarrow ||x - \Delta^\tau\ x)||_\infty \leq \epsilon$$

3.2 Retiming and sampling

A *retiming* function $r \in Ret$ is a non decreasing function from $\Re$ to $\Re$. This is a very general definition which provides many possibilities. For instance, a piece-wise constant retiming function can be seen as a sampler: if $x' = x \circ r$, and if r is piece-wise constant, then, at each jump of r, a new value of x is taken and maintained up to the next jump. This allows us to define a periodic sampler r, of period T_r as the piece-wise constant function (see figure 2):

$$r(t) = \lfloor t/T_r \rfloor T_r$$

where $\lfloor\rfloor$ is the floor function.

A desirable property of retimings is to have a bounded deviation with respect to identity.

Definition 3.1 (Bounded retiming) *A bounded retiming is a retiming which has a deviation* $dev(r) = \sup_t |r(t) - t|$

Finally, retimings allow us to characterise static (or combinational) systems as those systems which commute with retiming:

Proposition 3.1 (Static systems) *A static system* S *is such that, for any* $r \in Ret$*,*

$$S \circ r = r \circ S$$

3.3 Sampling

Retiming allows us to restate the uniformly continuous signal definition, by saying that a signal x is uniformly continuous if there exists a positive function η_x from errors to delays, such that:

$$\begin{array}{l} \forall \epsilon > 0, \forall\ retiming\ r, \\ dev(r) \leq \eta_x(\epsilon) \Rightarrow ||x - x \circ r||_\infty \leq \epsilon \end{array}$$

where id is the identity function (neutral retiming).

We can then define a *samplable* signal as a signal such that the sampling error can be controlled by tuning the sampling period:

Definition 3.2 (Samplable Signal) *A signal* x *is samplable if there exists a positive function* η_x *from errors to sampling periods, such that:*

$$\begin{array}{l} \forall \epsilon > 0, \forall\ periodic\ sampling\ r, \\ T_r \leq \eta_x(\epsilon) \Rightarrow ||x - x \circ r||_\infty \leq \epsilon \end{array}$$

Then the following property obviously holds:

Proposition 3.2 *A signal is samplable if and only if it is uniformly continuous.*

3.4 From signals to systems

This framework extends quite straightforwardly to systems by saying that a system S is uniformly continuous (figure 3) if there exists a positive function η_S from errors to errors such that:

$$\begin{array}{l} \forall \epsilon > 0, \forall x, x', \\ ||x - x'||_\infty \leq \eta_S(\epsilon) \Rightarrow ||(S\ x) - (S\ x')||_\infty \leq \epsilon \end{array}$$

and state the following proposition:

Proposition 3.3 *A uniformly continuous stationary system, fed with a uniformly continuous signal outputs a uniformly continuous signal.*

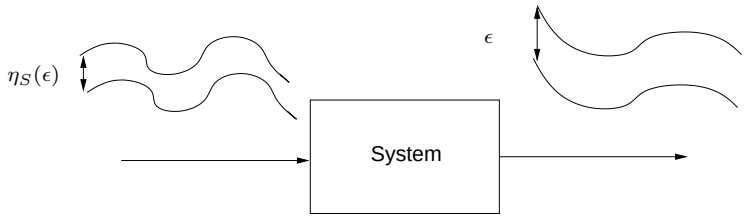

Figure 3: A uniformly continuous system

Proof:
The proof is straightforward and is repeated from [6].
Given x UC, S UC, and $\epsilon > 0$, $\forall x'$,

$$||x - x'||_\infty \leq \eta_S(\epsilon) \Rightarrow ||(S\ x) - (S\ x')||_\infty \leq \epsilon$$

and $\forall \tau$,

$$|\tau| \leq \eta_x(\eta_S(\epsilon)) \Rightarrow ||x - (\Delta^\tau\ x)||_\infty \leq \eta_S(\epsilon)$$

Thus, $\forall \tau$,

$$|\tau| \leq \eta_x(\eta_S(\epsilon)) \Rightarrow ||(S\ x) - (S\ (\Delta^\tau\ x)||_\infty \leq \epsilon$$

But $S(\Delta^\tau\ x) = \Delta^\tau(S\ x)$. We thus get

$$\eta_{Sx} = \eta_x \circ \eta_S$$

End

This property says that given an acyclic network of UC systems, one can compute maximum delays on system interconnection, sampling periods and maximum errors on input signals such that errors on output signals be lower than given bounds. This provides us thus with a nice approximation theory.

4 A hybrid topology

The difficulties met with the Skorokhod topology have led us to propose the following definition:

4.1 Topology definition

Let us consider the following family of open balls centred at arbitrary signals x, with positive parameters T, ϵ:

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

Proposition 4.1 *This family defines a topology.*

Proof:
It suffices to show that any point of a ball is the centre 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

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

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

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

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

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

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

End

Example: Figure 4 shows two boolean signals that can be made arbitrarily close in this topology by decreasing the duration h. It is easy to see conversely that this is not the case, neither with the L_∞ distance nor the Skorokhod distance nor the tube distance of [10].

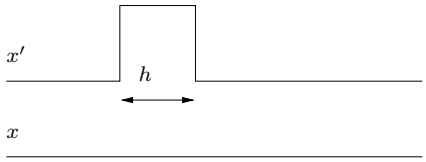

Figure 4: x and x' are close to each other when h is small in the given topology.

Closed Balls: Let us denote as $\bar{B}(x;T,\epsilon)$ the corresponding closed balls.

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

4.2 Product topology

When dealing with signal tuples, we consider product topologies. For instance, the topology associated with couples (x,y) will be defined by the balls:

$$B(x;T_x,\epsilon_x) \times B(y;T_y,\epsilon_y)$$

Yet, another solution would be to consider the two-dimension balls:

$$B(x,y;T,\epsilon) = \{x',y' \mid \sup_t \int_t^{t+T} \frac{|x-x'|+|y-y'|}{T} < \epsilon\}$$

What are the relations between the two generated topologies ?

Proposition 4.2 *These topologies are equivalent*

Proof:

It suffices to show that each ball of one family is included in one ball of the other family:

1: Assume x',y' belongs to $B(x;T_x,\epsilon_x) \times B(y;T_y,\epsilon_y)$.
Then

$$\begin{aligned} \sup_t \int_t^{t+T_x} \frac{|x-x'|}{T_x} &< \epsilon_x \\ \sup_t \int_t^{t+T_y} \frac{|y-y'|}{T_y} &< \epsilon_y \end{aligned}$$

Taking

$$\begin{aligned} T &= \inf\{T_x,T_y\} \\ \epsilon &= \frac{\epsilon_x T_x}{T} + \frac{\epsilon_y T_y}{T} \end{aligned}$$

yields

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

2: Conversely, taking

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

obviously yields

$$\begin{aligned} \sup_t \int_t^{t+T} \frac{|x-x'|}{T} &< \epsilon \\ \sup_t \int_t^{t+T} \frac{|y-y'|}{T} &< \epsilon \end{aligned}$$

End

4.3 Uniformly continuous signals

Definition 4.1 *A signal x is uniformly continuous with respect to the hybrid topology (UC_{ht}) if there exists a positive function $\eta_x(T,\epsilon)$ such that*

- *For all $\epsilon, T > 0$,*
- *For all r with $dev(r) \leq \eta_x(T,\epsilon)$*

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

Examples:

- Uniform bounded variability signals are UC_{ht}.
- Uniformly continuous signals in the usual sense are UC_{ht}.

4.4 Fundamental property of UC_{ht} signals

Proposition 4.3 *Let x be a UC_{ht} signal and let η_x be the corresponding error function.*

Then, there exists, for any positive ϵ, T, in any interval of duration T, a sub-interval of duration $h = \inf\{T, \eta_x(T,\epsilon)\}$ such that, for any t, t' in this interval

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

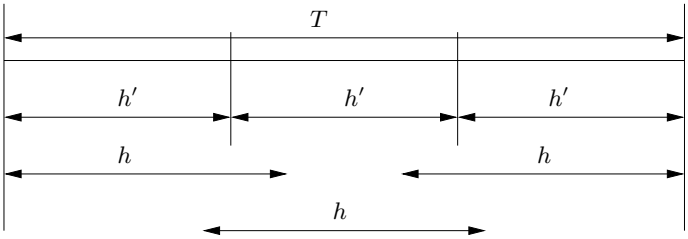

Figure 5: Interval partition

Proof:
The proof is by contradiction: let us assume that in each sub-interval of duration h the signal variation is larger than 2ϵ and show that there exists a retiming r of deviation smaller than or equal to h such that $x \circ r$ does not belong to $\bar{B}(x; T, \epsilon)$.

Let us cover an arbitrary interval I of duration T into n sub-intervals $I_i, i = 0, n-1$ of duration h where $n = \lceil T/h \rceil$. We choose these sub-intervals such that they equally overlap (unless h exactly divides T). We then partition T into n sub-intervals $I'_i, i = 0, n-1$ of duration $h' = T/n$ (see figure 5).

We can thus write:

$$T = nh' = nh - r$$

with $r < h$. More precisely,

$$\begin{aligned} I &= [t, t+T] \\ I_i &= [t + i(h - \frac{r}{n-1}), t + i(h - \frac{r}{n-1}) + h] \\ I'_i &= [t + ih', t + (i+1)h'] \end{aligned}$$

By assumption, there exists, in each sub-interval I_i, t_i and t'_i such that:

$$2\epsilon < x(t_i) - x(t'_i)$$

Furthermore,

- either t_i and t_{i+1} do not belong to $I_i \cap I_{i+1}$ and $t_i \leq t_{i+1}$
- or we can rearrange them by assigning:

$$\begin{aligned} t &:= argmax\{x(t_i), x(t_{i+1})\}; \\ t_i &:= t; \\ t_{i+1} &:= t; \end{aligned}$$

  which also yields $t_i \leq t_{i+1}$. Moreover, this rearrangement preserves the property $2\epsilon < x(t_i) - x(t'_i)$.

The same rearrangement can be performed on the (t'_i) sequence, Thus, the two sequences (t_i), (t'_i) are loosely increasing ones.

Let us consider the two retimings r et r' such that :

- for all $t \in I'_i$, $r(t) = t_i$
- for all $t \in I'_i$, $r'(t) = t'_i$

It can be seen that the corresponding deviations are less than h.

$$\begin{aligned} t + i(h - \frac{r}{n-1}) + h - (t + ih') &= h - r\frac{i}{n(n-1)} \leq h \\ t + (i+1)h' - (t + i(h - \frac{r}{n-1})) &= h - r\frac{n-i-1}{n(n-1)} \leq h \end{aligned}$$

Thus,

$$\begin{aligned} dev(r) &\leq \eta_x(T, \epsilon) \\ dev(r') &\leq \eta_x(T, \epsilon) \end{aligned}$$

Now we can see that

$$\int_I \frac{|x \circ r - x \circ r'|}{T} = \sum_1^n \frac{h'}{T}[x(t_i) - x(t'_i)] > 2\epsilon$$

By triangular inequality, we get:

$$\int_I \frac{|x - x \circ r|}{T} + \int_I \frac{|x - x \circ r'|}{T} > 2\epsilon$$

This means that at least one of the two integrals is larger than ϵ. The corresponding retiming violates the UC_{ht} assumption.

End

We clearly see now how our new topology generalises the usual one concerning uniform continuity: In the usual definition, for any ϵ, we can find η such that, in any interval of duration η, the signal variation is smaller than or equal to ϵ. In our new framework, for any T, ϵ, we can find η such that, in any interval of duration T, there exists a sub-interval of duration η where the signal variation is smaller than or equal to ϵ. This is clearly a generalisation and it is the price to be paid for tolerating the discontinuities inherent to discontinuous signals like booleans and for encompassing in the same framework continuous signals and boolean signals. Furthermore, having been able to encompass both classes of signals allows us to also deal with hybrid piece-wise continuous ones.

Moreover, we can show that this property is quite tight by considering the example of a boolean signal x with uniform bounded variability, *i.e.,* such that the interval between two discontinuities is larger than T.

It is easy to show, by taking a delay $r(t) = t - T\epsilon$, with $\epsilon < 1/2$, that

$$\eta_x(T, \epsilon) = T\epsilon$$

Now, in any interval of duration T, there truly exists an interval of duration $T\epsilon < T/2$ where the boolean signal remains constant and, thus,

$$x^M - x^m \leq 2\epsilon < 1$$

5 Sampling hybrid signals and systems

5.1 Sampling hybrid signals

The fundamental property 4.3 allows us first to find a condition on sampling periods. The idea, here, is that hybrid signals are made of stable intervals, where the signal variation is smooth, separated by intervals where discontinuous perturbations are present. Property 4.3 gives us a condition on sampling periods such that at least one sample is taken in each stable intervals. More precisely:

Definition 5.1 *An ϵ_stable interval (ϵ_SI) of a signal x is an interval I such that, for any t, t' in I, $|x(t) - x(t')| \leq \epsilon$*

Definition 5.2 *A ϵ_maximal stable interval (ϵ_MSI) of a signal x is an ϵ_SI which is not contained in a larger one.*

Proposition 5.1 *Given a UC_{ht} signal x, a sampling retiming r of deviation $dev(r) \leq \sup_T \eta_x(T, \epsilon/2)$ takes at least one sample in each ϵ_MSI.*

5.2 Checking the UC_{ht} property

Property 4.3 also gives us a way of approximatedly checking the UC_{ht} property. The idea is that, if we sample a signal in such a way that at least two samples are taken in each ϵ_MSI, we know that in each T interval, at least two consecutive samples should not vary of more than ϵ and we can rise an alarm if this is not the case. This is the basis of Airbus confirmation functions.

Definition 5.3 (Confirmation function)

$$
\begin{array}{lcl}
Confirm(x, h, nmax, \epsilon) & = & y \quad \texttt{where}\ y,\ n = \\
& & \quad \texttt{if}\ |x - \Delta^h_{x_0} x| \leq \epsilon \\
& & \quad \texttt{then}\ x,\ 0 \\
& & \quad \texttt{else}\ \ \texttt{if}\ \Delta^h_0 n < nmax - 1 \\
& & \qquad \texttt{then}\ \Delta^h_{x_0} y,\ \Delta^h_0 n + 1 \\
& & \qquad \texttt{else}\ alarm
\end{array}
$$

where $\Delta^h_{x_0}$ is the *delay operator* such that $\Delta^h_{x_0} x(t) = x(t-h)$ with initial value x_0.

Notations: In this definition and in the sequel, algorithms are expressed using a functional notation, that is to say by abstracting over time indices, in order to stay consistent with design tools like Simulink[2] or Scade[3]. Thus, a signal definition $x_1 = x_2$ means $\forall n \in N : x_1(nT) = x_2(nT)$ where T is the period of the computing unit running the algorithm.

- this function maintains a counter n with initial value 0, and its previous output, with some known initial value x_0,

[2] http://www.mathworks.com
[3] http://www.esterel-technologies.com

- whenever the input and the preceding one don't differ from more than ϵ, it outputs the input and resets the counter,
- else, if the counter has not reached $nmax - 1$, it increments it and outputs the previous output,
- else it raises an alarm.

Proposition 5.2 *If*

- x *is* UC_{ht}*,*
- $h < \eta_x(T, \epsilon/2)/2$
- $nmax = \lceil \frac{T - \eta_x(T,\epsilon/2)}{h} \rceil$

$Confirm(x, h, nmax, \epsilon)$ *never raises an alarm*

This is in fact a corollary of proposition 4.3.

We can go a bit further and improve the bound on $nmax$. As a matter of fact, the maximum interval between two consecutive ϵ_SMI may not be as large as $T - \eta_x(T, \epsilon/2)$. The idea, here, is that the property 4.3 is true for any T_interval. By sliding the interval, as soon as a SMI starts disappearing at the left side of the interval, another one should have already appeared at the right side of the interval:

Proposition 5.3 *If* x *is* UC_{ht}*, in any interval of duration* T*, the maximum interval between two consecutives* ϵ*_SMIs is smaller than or equal to* $T - 2\eta_x(T, \epsilon/2)$

Proof:
The proof is by contradiction: assume such an interval $I = [t_1, t_2]$ with $t_2 - t_1 > T - 2\eta_x(T, \epsilon/2)$. Consider the T_interval $[(t_1 + t_2 - T)/2, (t_1 + t_2 + T)/2]$ centred at the centre of I . This interval should contain at least an ϵ_SMI of duration at least $\eta_x(T, \epsilon/2)$ but there is no room for it in the space left by I.

End

5.3 Smoothing hybrid signals

Yet, confirmation functions have also additional interesting properties, in that their output is a smooth delayed version of their input: the output is freezed once not in a ϵ_SMI, and thus "jumps" from SMI to SMI.

5.4 UC_{ht} systems

This framework also allows us to provide elements of a sampling and approximation theory for hybrid systems.

Definition 5.4 *A system S is UC_{ht} if there exists a positive function $\eta_S(T,\epsilon)$ such that:*

- *for all $T,\epsilon > 0$,*
- *for all x, x' where x' belongs to $\bar{B}(x;\eta_S(T,\epsilon))$*

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

Clearly,

Proposition 5.4 *Asymptotically stable linear time-invariant systems are UC_{ht}.*

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

$$S(x)(t) = \int_{-\infty}^{\infty} h_S(u)x(t-u)$$

and

$$\int_{-\infty}^{\infty} |h_S| = K_S < \infty$$

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

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

It suffices then to choose:

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

to get the announced result.

End

But we also have this very nice property:

Proposition 5.5 *Boolean combinational systems are UC_{ht}.*

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

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

and to notice that, for a boolean function f, we have for any x, x', y, y', t:

$$|f(x, y) - f(x', y')|(t) \leq |x - x'|(t) + |y - y'|(t)$$

End

Noting that combinational functions commute with retiming, we can reuse the proof of 3.3 to state a similar property for networks of boolean functions:

Proposition 5.6 *A uniformly continuous combinational system, fed with a uniformly continuous signal outputs a uniformly continuous signal.*

This property says that given an acyclic network of UC_{ht} combinational systems, one can compute maximum delays on system interconnection, sampling periods and maximum errors on input signals such that errors on output signals, in the sense of our topology, be lower than given bounds. This provides us thus with a nice approximation theory which also nicely combines with voting, in that this "error calculus" allows voter parameters to be correctly set.

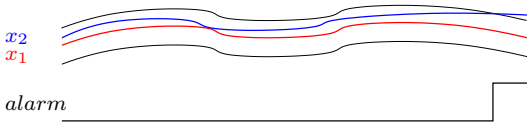

Figure 6: Threshold voting

6 Hybrid voting

In this section we recall the classical threshold and delay voting schemes. Then we propose a 2/2 hybrid voter which is a mixture of these two aspects.[4]

6.1 Threshold Voting

Threshold voting is a classical voting scheme. Assume that signals x, x' are redundantly computed signals. In theory, the two signals should be equal but, because they are not computed at the same time, in the same computer, from the same sensor values, and possibly by dissimilar algorithms, their values can be slightly different. The figure 6 shows a tolerance tube around the reference signal x. Whenever the signal x' remains within the tolerance tube, the voted value is the reference one. If the signal x' gets out the tube, an alarm is raised.

Knowing bounds on the normal deviation between values that should be equal, easily allows the design of threshold voters. For instance, if x is uniformly continuous and if

$$x' = x \circ r + e$$

with

- $||r - id||_\infty \leq \eta_x(\epsilon)$
- $||e||_\infty \leq \epsilon$

We can find a threshold $\epsilon' = 2\epsilon$ and design a $2/2$-voter:

$$\begin{array}{rl} voter2/2(x, x', \epsilon') = & \texttt{if } |x - x'| \leq \epsilon' \\ & \texttt{then } x \\ & \texttt{else } alarm \end{array}$$

such that the voter delivers a correct output in the absence of failure and, otherwise, delivers an alarm.

[4] In the usual terminology for voters, n_1/n_2 means that n_1 units out of n_2 redundant ones should operate correctly in order that the redundant system operates correctly.

6.2 Delay voting

Delay voting is the discontinuous equivalent to the threshold one. The figure 7 shows this scheme principle. Whenever the two signals are equal, the voted value is the common one. Else, the voter holds its output and waits for a new agreement during a predefined temporal window. If there is no agreement, an alarm is latched.

Let us consider boolean UBV signals x_1 and x_2 which is, in normal operation, a delayed image of x_1:

$$x_2 = x_1 \circ r$$

with a bound τ on the delay in correct operation:

$$dev(r) \quad \leq \quad \tau$$

There signals are received by some unit of period T. However, the assumption that correct computers have perfect clocks. is clearly not realistic. To be more realistic, one should consider clock drifts. A frequent assumption is that clock drifts are bounded, either because the mission time is bounded or extra mechanisms allow for detecting exceedingly large drifts. Then there exist lower (T_m) and upper (T_M) bounds for T and, in each condition involving T, it should be replaced by the bound which makes it more pessimistic. We thus assume $T_m \leq T \leq T_M$.

We also assume $\tau + T_M < T_x$. This assumption guarantees that the joint effect of the delay and the sampling at rate T (which can induce an additional delay) cannot lead to miss any change of input value (which, by assumption lasts at least T_x). Then,

- the maximum time interval during which the two signals may continuously disagree is obviously τ,
- the maximum number of samples where two correct copies continuously disagree is

$$nmax = \left\lfloor \frac{\tau}{T_m} \right\rfloor + 1$$

This allows us to design **delay voters** for delay booleans signals. For instance, a $2/2$ voter could be:

Definition 6.1 (2/2 delay voter)

$$\begin{array}{rcl} voter2/2(x_1, x_2, nmax) & = & x \quad \texttt{where}\ x,\ n = \\ & & \qquad \begin{array}{l} \texttt{if}\ x_1 = x_2 \\ \texttt{then}\ x_1,\ 0 \\ \texttt{else}\ \ \texttt{if}\ \Delta_0^T n < nmax - 1 \\ \qquad \texttt{then}\ \Delta_{x_0}^T x,\ \ \Delta_0^T n + 1 \\ \qquad \texttt{else}\ alarm \end{array} \end{array}$$

- this voter maintains a counter n with initial value 0, and its previous output, with some known initial value x_0,

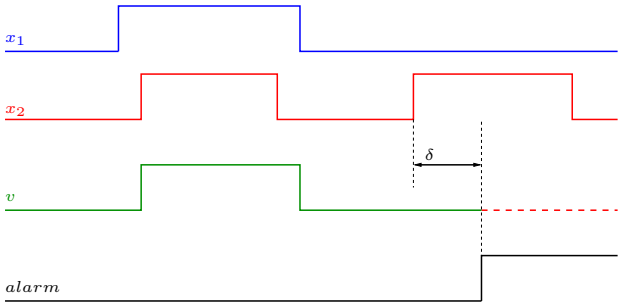

Figure 7: Bounded delay voting

- whenever the two inputs agree, it outputs one input and resets the counter,
- else, if the counter has not reached $nmax - 1$, it increments it and outputs the previous output,
- else it raises an alarm.

Proposition 6.1 *$voter2/2$ raises an alarm if the two inputs disagree for more than $nmaxT_M$ and otherwise delivers the correct value with maximum delay $(nmax + 1)T_M$.*

6.3 Hybrid delay-threshold voting

Can we mix now the two previous voters, the threshold and the delay one? This would amount to define an hybrid voter that is illustrated at figure 8:

Definition 6.2 (2/2hybrid voter)

$$hyb\_voter2/2(x, x', nmax, \epsilon') \;=\; y \;\; \texttt{where}\; y,\;\; n \;=\; \begin{array}{l}\texttt{if}\; |x - x'| \leq \epsilon' \\ \texttt{then}\; x,\;\; 0 \\ \texttt{else}\;\; \texttt{if}\; \Delta_0^T n < nmax - 1 \\ \qquad \texttt{then}\; \Delta_{x_0}^T y,\;\; \Delta_0^T n + 1 \\ \qquad \texttt{else}\; alarm\end{array}$$

- this voter maintains a counter n with initial value 0, and its previous output, with some known initial value x_0,
- whenever the two inputs threshold-agree, it outputs one input and resets the counter,
- else, if the counter has not reached $nmax - 1$, it increments it and outputs the previous output,
- else it raises an alarm.

On which condition could we state the following desirable proposition?

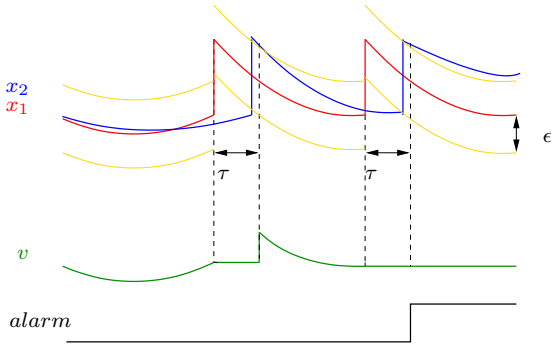

Figure 8: Hybrid threshold-delay voting

Proposition 6.2 (Hybrid voter property) *$hyb\_voter2/2$ raises an alarm if the two inputs differ for more than ϵ' during more than $nmaxT_M$ and otherwise delivers the correct value with maximum delay $(nmax + 1)T_M$.*

Answering this question is the object of the next section.

6.4 UC_{ht} signals and votes

We can now state this proposition which provides a positive answer to the question raised in 6.2:

Proposition 6.3 *If x and x' are UC_{ht} and*

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

then in any interval of duration T, there exists a sub-interval of duration $h = \inf\{T, \eta_x(T, \epsilon), \eta_{x'}(T, \epsilon)\}$ over which any t yields

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

Proof:
The proof is very similar to the one of property 4.3 and proceeds by contradiction: assume, in any sub-interval of duration h, some time t such that $|x(t) - x'(t)| > 3\epsilon$. Then some of the initial assumptions is not satisfied.

We define the cover $I_i, i = 0, n-1$ and partition $I'_i, i = 0, n-1$ as previously. Let t_i in I_i be such that $|x(t_i) - x'(t_i)| > 3\epsilon$. After some possible rearrangement, the (t_i) sequence is loosely increasing and we can define the retiming r by:

$$\forall t \in I'_i, r(t) = t_i$$

As previously we can check that this retiming has a deviation smaller than or equal to h. Thus

$$dev(r) \leq \inf\{\eta_x(T,\epsilon), \eta_{x'}(T,\epsilon)\}$$

We then get

$$\int_I \frac{|x \circ r - x' \circ r|}{T} > 3\epsilon$$

By triangular inequality,

$$\int_I \frac{|x \circ r - x}{T} + \int_I \frac{|x - x'|}{T} + \int_I \frac{|x' - x' \circ r|}{T} > 3\epsilon$$

Here also, at least one of these integrals is larger than ϵ and the corresponding assumption is violated.

End

Clearly this property provides a foundation to the use of mixed threshold and delay voters.

7 Conclusion

This report has intended to provide a satisfactory theory for merging together threshold voters adapted to continuous signals and delay voters adapted to boolean signals in order to cope with hybrid piece-wise continuous signals. One problem in performing this merge was that, while threshold voters are based on uniform continuity, delay voters are based on a more *ad-hoc* notion of uniform bounded variability. After having previously tried the Skorokhod topology, we propose here a new topology for hybrid systems which seems to better match our purpose. In particular, it allows us to merge in a very uniform way the theory of threshold voters and the theory of delay voters and to build a theory of hybrid mixed threshold and delay voters.

Moreover, this voting problem is clearly related to the more general sampling problem for hybrid systems and the results provided here may also help in defining which classes of hybrid systems can be accurately sampled. This can be a subject for future work.

Identifying uniformly continuous signals and systems enables us to handle in a safe way reconfiguration issues by using finely tuned voting schemes. These schemes guarantee recovering the overall stability of switched hybrid systems. The ”error calculus” introduced in this report is a starting point for a further work closely linking uniform continuity to the more general field of robustness.

References

[1] J.-R. Abrial. *The B-Book*. Cambridge University Press, 1995. 1.1

[2] A.Chutinan and B.H.Krogh. Computing approximating automata for a class of hybrid systems. *Mathematical and Computer Modeling of Dynamical Systems*, 6:30–50, March 2000. Special Issue on Discrete Event Models of Continuous Systems. 1.6

[3] A. Avizienis. The methodology of *n*-version programming. In M.R. Lyu, editor, *Software Fault Tolerance*, pages 23–46. John Wiley, 1995. 1

[4] P. Billingsley. *Convergence of probability measures*. John Wiley & Sons, 1999. 1.4

[5] M.S. Branicky. Topology of hybrid systems. In *32nd Conference on Decision and Control*, pages 2309–2311. IEEE, 1993. 1.6

[6] P. Caspi and A. Benveniste. Toward an approximation theory for computerised control. In A. Sangiovanni-Vincentelli and J. Sifakis, editors, *2nd International Workshop on Embedded Software, EMSOFT02*, volume 2491 of *Lecture Notes in Computer Science*, 2002. 1, 1.4, 3.4

[7] P. Caspi, C. Mazuet, R. Salem, and D. Weber. Formal design of distributed control systems with Lustre. In *Proc. Safecomp'99*, volume 1698 of *Lecture Notes in Computer Science*. Springer Verlag, September 1999. 1.3

[8] P. Caspi and R. Salem. Threshold and bounded-delay voting in critical control systems. In Mathai Joseph, editor, *Formal Techniques in Real-Time and Fault-Tolerant Systems*, volume 1926 of *Lecture Notes in Computer Science*, pages 68–81, September 2000. 1, 1.4

[9] E.Asarin, O.Maler, and A.Pnueli. On discretization of delays in timed automata and digital circuits. In R.de Simone and D.Sangiorgi, editors, *Concur'98*, volume 1466 of *Lecture Notes in Computer Science*, pages 470–484. Springer, 1998. 1.6

[10] V. Gupta, T.A. Henzinger, and R. Jagadeesan. Robust timed automata. In O. Maler, editor, *Hybrid and Real-Time Systems, HART'97*, volume 1201 of *Lecture Notes in Computer Science*, pages 331–345. Springer Verlag, 1997. 1.4, 4.1

[11] J.Ouaknine. Digitisation and full abstraction for dense-time model checking. In *TACAS 02*, volume 2280 of *Lecture Notes In Computer Science*, pages 37–51. Springer, 2002. 1.6

[12] H. Kopetz. *Real-Time Systems Design Principles for Distributed Embedded Applications*. Kluwer, 1997. 1.2, 1.3

[13] Ch. Kossentini and P. Caspi. Mixed delay and threshold voters in critical real-time systems. In S. Yovine Y. Lakhnech, editor, *Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRTFT04*, volume 3253 of *Lecture Notes in Computer Science*. Springer Verlag, 2004. 1, 1.4

[14] M.Broucke. Regularity of solutions and homotopic equivalence for hybrid systems. In *Proceedings of the 37th IEEE Conference on Decision and Control*, volume 4, pages 4283–4288, 1998. 1.6

[15] R.Alur, T.A.Henzinger, G.Lafferriere, and G.J.Pappas. Discrete abstractions of hybrid systems. *Proceedings of the IEEE*, 88:971–984, 2000. 1.6

[16] J.H. Wensley, L. Lamport, J. Goldberg, M.W. Green, K.N. Lewitt, P.M. Melliar-Smith, R.E Shostak, and Ch.B. Weinstock. SIFT: Design and analysis of a fault-tolerant computer for aircraft control. *Proceedings of the IEEE*, 66(10):1240–1255, 1978. 1.3

[17] W.Kohn and A.Nerode. Models for hybrid systems: automata, topologies, controllability and observability. In *Hybrid Systems*, volume 732 of *Lecture Notes in Computer Science*. Springer, 1993. 1.6