Towards Hilbertian Formal Methods

(Extended abstract)

Marius C. Bujorianu
University of Kent
Computing Laboratory
Canterbury, Kent, UK
Bujorianu@yahoo.com

Manuela L. Bujorianu
University of Twente
Faculty of Electronics, Mathematics
and Computer Science -EWI
Enschede, The Netherlands
L.M.Bujorianu@cs.utwente.nl

In this work, we address the issue of handling complex continuous evolutions of the environment of embedded systems. There is now an impressive amount of research in the area of intelligent embedded controllers, and thus we do not need to argue about the importance of this subject. Our contribution is twofold:

1. Define a new problem, that of using complex mathematical information about continuous environments; and

2. Propose an initial solution in the form of a new logic defined using Hilbertian methods. This represents the first step towards using abstract continuous mathematics in formal methods, a program that we have called *Hilbertian Formal Methods*.

Usually, the information about the environment is obtained via a set of sensors, that is a process of discretizations. In this case, the controller synthesis can be carried out efficiently using discrete mathematics. We remark that the controller uses only little information about its environment.

In some cases, the differential equation governing the environment evolution is studied enough to make available efficient algorithms for computing/approximating the solutions. This mixed discrete/continuous mathematics form the basis of the well-developed theory of hybrid systems [5]. In the deterministic case, formal methods are now mature for specification and verification of a large class of safety properties. However, the complexity of hybrid automata models or the idealistic representations of the continuous environments require to randomize these models. The result, called stochastic hybrid systems (SHS) [2], has the advantage of being more compact and expressive. The major problem, then, is that the formal specification and verification are still in their infant days. Despite that, there is a spectacularly increase of research applying SHS to system modelling, and that includes air traffic control, automotive systems, bioengineering and medicine. This trend suggests that there is a real need to make more information about the environment available at the controller design stage.

Moreover, there are many situations when the continuous mathematical models of the environment are such that:

- the equations do not admit computable solutions,

- or, these solutions are computable in exponential time (or algorithmically inefficient),

- or, they are so complex (because of some mathematical features like nonlinearity, stochasticity, etc) such that only very little about solutions is known.

Such situations are typical, for example, in weather [4] and disease modelling. For instance, the nonlinearity effects and random factors, like global warming, can make a storm to have catastrophical consequences (sudden and massive floods, hurricanes, etc). The evaluation methods in hybrid systems and weather forecasting computing, often, fail to compute numerical approximations in real time if not at all. However, the mathematicians can make predictions using known mathematical properties of the solutions. These properties may not produce directly numerical estimations but they still do offer plenty of valuable information. A typical example is the cadlag property (right continuous with left limits) of the process trajectories.

We address this timely problem of tailoring formal methods for employing the mathematical knowledge when the numerical approximations are not available. Our approach is inspired from the research in continuous mathematics. The mathematicians have introduced an abstract framework, called the theory of distributions [3], to study complex continuous phenomena. Roughly speaking, in this framework, every important differential operator admits solutions, called weak solutions [3] (or solutions in sense of distributions). As the main scope of this theory is not computability, the benefits of these mathematical efforts are counted in mathematical properties. The main idea is that these properties remain true for the solutions in the clas-

Seventh International Conference on Application of Concurrency to System Design (ACSD 2007)
0-7695-2902-X/07 $25.00 © 2007 IEEE

sical sense (like in mathematical physics [3]). Then it is necessary to have a suitable logic for representing the weak solutions and their analytic properties. Such a logic is difficult to design because understanding distributions requires a very advance level in continuous mathematics. Our main contribution consists in a way of defining logically the weak solutions with no use of the theory of distribution at all.

We call the new logic *Hilbertian logic*. We interpret this logic in the class of semi-dynamical systems, a functional analysis based formalization of continuous phenomena.

Consider a generic collection of types, called *Hilbertian types*. Each type models a (partial) differential operator or the generator of a Markov process.

The terms of a given type T are generated by the following grammar

$f := 1|\bot|\top| < \wp > f|f \odot f|f : f|f - c|\inf(f,f)|\sup(f,f)$

To each type T we attach two supertyped $\wp_T$ and E_T and the terms of type $\wp_T$ are of the form $< \wp > f$ with f ranging the terms of type T. The terms of type E_T are of the form $\sup_{n\in\mathbb{N}} p_n$ with p ranging the terms of type $\wp_T$.

The formulas are defined as equalities or inequalities between terms.

Let X be a Polish space, equipped with its Borel σ-algebra $\mathcal{B}$, and $X_\Delta = X \cup \{\Delta\}$. The set of all bounded measurable numerical functions on X is denoted by $\mathcal{B}^b(X)$.

A semi-dynamical system is given by a state space X and a map $\phi : \mathbb{R}_+ \times X_\Delta \to X_\Delta$ such that

1. ϕ is a measurable map; 2. $\phi(o,x) = x$;
3. $\phi(t_1+t_2,x) = \phi(t_1,\phi(t_2,x))$
4. $\phi(t,x) = \Delta \Rightarrow \phi(s,x) = \Delta, \forall s \geq t$;
5. $\phi(t,x) = \phi(t,y), \forall t > 0 \Rightarrow x = y$.

The *kernel operator* V is defined by
$Vf(\cdot) = \int_0^\infty f(\phi(t,x))dt$, $f \in \mathcal{B}^b(X)$.

Now consider a fixed semi-dynamical system $M = (X,\phi)$. The interpretation of a term f is a function $f : X \to \mathbb{R}$. Then
$1(x) := 1, \forall x \in X$; $\bot(x) := 0$
$\top(x) := M$ where M is a constant large enough
$(f \odot g)(x) := f(x) + g(x)$
$(f : g)(x) := f(x) - g(x)$ if $f(x) \geq g(x)$ and 0 otherwise.
$(f - c)(x) := f(x) - c$ if $f(x) \geq c$ and 0 otherwise.

The infimum and supremum are defined pointwise. The action of $\wp$ to a formula f is given by $(\wp.f)(\cdot) = Vf(\cdot)$

The global properties of weak solutions of partial differential equations can be traced back to the Poincare's sweeping method. In each system state x a weak solution is characterized by a potential, in our approach given by $Vf(x)$.

The elements of $\mathcal{B}^b(X)$ can be thought of as *terms* in a Hilbertian logic associated to M. The interpretation of Hil formulas are the obvious predicates associated with the (in)equalities.

It is also possible to interpret the Hil specifications over stochastic models. In this case, the terms of the form $< \wp > f$ are excessive functions [3] associated to a Markov process. These characterize the Markov process up to a time change and are defined axiomatically on the stochastic paths.

In modern control engineering the problems are formulated in a global manner. For example, engineers and applied mathematicians often use measurable sets of system trajectories (often of continuum power). The trajectories themselves are dense and thus it is impossible to use specifications involving concepts like 'next state' and 'after k steps the system...'. The trajectories form very rich algebraic and functional structures. System properties are often defined in terms of possible trajectories using advanced concepts of topology, functional analysis and probability theory. In contrast, probabilistic methods in computer science are based on explicit state changes, where the concept of next state is fundamental. These methods, from an engineering (whether this is financial, medical or safety critical systems) point of view, could be characterized as been local (the vicinity given by the possible next states) or observational (the system behaviour is given by observing the state changes). Probabilistic specification and verification (using model checking) are now mature and rapidly growing. A severe limitation of these methods is that they are strictly local (which means a clear underlying transitional structure).

This work is part of a series of papers [2, 1] where we have shown that formal methods can be soundly founded on Hilbertian mathematics and therefore we have introduced the term *Hilbertian formal methods*.

The full version of this paper is available on www [1]

Acknowledgments
We thank Rom Langerak and the editors for many useful remarks. This work was funded by the NWO project Aisha[2].

References

[1] M. Bujorianu and C. Bujorianu. A model checking strategy for a class of performance properties of fluid stochastic models. *Proc. of 3rd European Performance Engineering Workshop*, pages 198–216, Springer-Verlag, LNCS 4054 2006.

[2] M. Bujorianu and J. Lygeros. Bisimulation for general stochastic hybrid systems. *in [5]*, pages 198–216, 2005.

[3] J. Doob. *Classical Potential Theory and Its Probabilistic Counterpart*. Springer- Verlag, New York, 1984.

[4] V. Gordin. *Mathematical Problems and Methods of Hydrodynamic Weather Forecasting*. CRC, 680 pages, 2000.

[5] M. Morari and L. Thiele. *Hybrid Systems: Computation and Control. Proc. of 8th International Workshop*. Springer-Verlag, LNCS 3414, 2005.

[1] http://wwwhome.cs.utwente.nl/ manuela/aisha/Hilbert.pdf
[2] http://wwwhome.cs.utwente.nl/ manuela/aisha/index.html