A Robust Interpretation of Duration Calculus

Martin Fränzle* and Michael R. Hansen**

Informatics and Mathematical Modelling
Technical University of Denmark
Richard Petersens Plads, Bldg. 322
DK-2800 Kgs. Lyngby, Denmark

As embedded systems become more and more complex, early availability of unambiguous specification of their intended behaviour has become an important factor for quality and timely delivery. Consequently, the quest for automatic analysis methods for specifications arises. This quest becomes even more pronounced if specifications are to be formal, because formal specifications are often found to be particularly hard to write and maintain, such that decision procedures for entailment between specifications, satisfiability of specifications, etc., may be extremely helpful in their design process. The price to be paid for such procedures is, however, a firmly constrained expressiveness of the specification formalisms: one has to sacrifice all elements that could give rise to undecidability.

However, the logically motivated notions of entailment between specifications, satisfiability of specifications, etc., have often been criticized from an engineering standpoint, as their validity or invalidity may well depend on the *exact* values of certain constants (e.g., the exact length of a steering rod relative to the exact distance of two joints), while any technical realization of these constants can only be approximate. In system design, the role of any decision problem prone to changing its truth value under arbitrarily small variations of constants may be considered questionable. Based on this insight, research has in recent years addressed more "robust" notions of property satisfaction, where a property is considered to be "robustly (in-)valid" iff it does not change its validity under small variation of constants and/or values of variables [GHJ97,Pur98,Frä99,AB01,Frä01,Rat02a,Rat02b]. The ultimate hope is that, besides being more relevant to engineering problems, such robust notions enhance decidability as, e.g., existence of non-computable reals cannot influence their validity.

With respect to embedded system design, such robust properties have by now mainly been investigated in the automata-based modeling context. Starting with Gupta's, Henzinger's, and Jagadeesan's [GHJ97] as well as Puri's [Pur98] investigation of timed automata, the idea has been to exploit topological properties of systems in order to obtain robust answers. Asarin and Bouajjani [AB01] have applied this approach to reach set computation of, a.o., hybrid automata and Turing machines. Fränzle introduced a variant thereof in [Frä99] by applying the concept to decision problems about hybrid automata instead of reach-set computation, e.g. invariance of a first-order property over hybrid states [Frä99]

* Email: mf@imm.dtu.dk; Phone: +45-4525 7512; Fax: +45-4593 0074.
** Email: mrh@imm.dtu.dk; Phone: +45-4525 3727; Fax: +45-4593 0074.

or progress [Frä01], thereby obtaining decision procedures that succeed in all robust cases, even such which are undecidable wrt. non-robust notions of property satisfaction.

Independently, constraint solving technology for numerical constraints over the real numbers was developed that has perfectly corresponding properties: one can solve otherwise undecidable constraints (containing functions over the real numbers other than polynomials) , provided they are robust, in the sense that their solvability does not change under small perturbations of the constants the constraints contain [Rat02a,Rat02b,Rat02c]. Even in cases where constraints are decidable, robust constraints can generally be solved much more efficiently.

In this talk, we unite above two lines of research by addressing logical models of embedded systems. We provide a robust interpretation of a very expressive metric-time temporal logic, Duration Calculus (DC) [ZHR91,ZH04], and show its equivalence to a multi-valued interpretation that uses the real numbers as semantic domain and assigns Lipschitz-continuous interpretations to all operators of DC.

We define a formula ϕ to be *robustly valid* iff not only ϕ itself is valid (in the classical sense of DC), but there additionally is a real number $\delta > 0$ such that all formulae ϕ' that differ from ϕ only in a change of constants of up to $\pm\delta$ are valid (again in the classical sense of DC). The fundamental idea of the *multi-valued semantics*, on the other hand, is to assign to each (sub-)formula ϕ and each valuation σ of its free variables a real number $\mathcal{MV}[\![\phi]\!](\sigma)$, where

- the sign of $\mathcal{MV}[\![\phi]\!](\sigma)$ signifies whether ϕ is satisfied by σ or not, and
- the magnitude of $\mathcal{MV}[\![\phi]\!](\sigma)$ corresponds to the maximum permissible change of the constants occurring in ϕ that keeps ϕ's satisfaction properties over σ unchanged.

I.e., if $|\mathcal{MV}[\![\phi]\!](\sigma)| = c$ then all formulae ϕ' that differ from ϕ only in a change of constants of up to $\pm c$ correspond to ϕ wrt. σ in so far as either both ϕ and ϕ' are satisfied by σ, or both are not. Intuitively, $|\mathcal{MV}[\![\phi]\!](\sigma)|$ is the *robustness margin* of ϕ wrt. σ, such that the multi-valued semantics and the notion of robust validity are in direct correspondence.

An analysis of $\mathcal{MV}[\![\phi]\!]$ reveals that the multi-valued semantics assigns Lipschitz-continuous interpretations to all operators of DC. This Lipschitz-continuity provides a handle for a plethora of approximability results. I.e., unlike the classical two-valued interpretation, truth values in the multi-valued interpretation can be approximated in various ways, some of which are algorithmic. In particular, there is a discrete-time approximation of the multi-valued dense-time interpretation of a formula. As interesting subsets of DC are decidable over discrete time [Han94], yet undecidable over dense time [ZHS93,ZH04,Frä04], this can provide novel approaches towards tool support for dense-time DC.

References

[AB01] E. Asarin and A. Bouajjani. Perturbed turing machines and hybrid systems. In *Proceedings of the Sixteenth Annual IEEE Symposium on Logic in*

Computer Science (LICS 2001). IEEE, 2001.

[Frä99] M. Fränzle. Analysis of hybrid systems: An ounce of realism can save an infinity of states. In J. Flum and M. Rodríguez-Artalejo, eds., *Computer Science Logic (CSL'99)*, volume 1683 of *Lecture Notes in Computer Science*, pages 126–140. Springer-Verlag, 1999.

[Frä01] ———. What will be eventually true of polynomial hybrid automata. In N. Kobayashi and B. C. Pierce, eds., *Theoretical Aspects of Computer Software (TACS 2001)*, volume 2215 of *Lecture Notes in Computer Science*, pages 340–359. Springer-Verlag, 2001.

[Frä04] ———. Model-checking dense-time duration calculus. *Formal Aspects of Computing*, 16(2):121–139, 2004.

[GHJ97] V. Gupta, T. A. Henzinger, and R. Jagadeesan. Robust timed automata. In O. Maler, ed., *Proceedings of the First International Workshop on Hybrid and Real-Time Systems (HART 97)*, volume 1201 of *Lecture Notes in Computer Science*, pages 331–345. Springer-Verlag, 1997.

[Han94] M. R. Hansen. Model-checking discrete duration calculus. *Formal Aspects of Computing*, 6(6A):826–845, 1994.

[Pur98] A. Puri. Dynamical properties of timed automata. In A. P. Ravn and H. Rischel, eds., *Formal Techniques in Real-Time and Fault-Tolerant Systems (FTRTFT'98)*, volume 1486 of *Lecture Notes in Computer Science*, pages 210–227. Springer-Verlag, 1998.

[Rat02a] S. Ratschan. Continuous first-order constraint satisfaction. In J. Calmet, B. Benhamou, O. Caprotti, L. Henocque, and V. Sorge, eds., *Artificial Intelligence, Automated Reasoning, and Symbolic Computation*, number 2385 in LNCS, pages 181–195. Springer, 2002.

[Rat02b] ———. Quantified constraints under perturbations. *Journal of Symbolic Computation*, 33(4):493–505, 2002.

[Rat02c] ———. Search heuristics for box decomposition methods. *Journal of Global Optimization*, 24(1):51–60, 2002.

[ZH04] Zhou Chaochen and M. R. Hansen. *Duration Calculus — A Formal Approach to Real-Time Systems*. EATCS monographs on theoretical computer science. Springer-Verlag, 2004.

[ZHR91] Zhou Chaochen, C. A. R. Hoare, and A. P. Ravn. A calculus of durations. *Information Processing Letters*, 40(5):269–276, 1991.

[ZHS93] Zhou Chaochen, M. R. Hansen, and P. Sestoft. Decidability and undecidability results for duration calculus. In P. Enjalbert, A. Finkel, and K. W. Wagner, eds., *Symposium on Theoretical Aspects of Computer Science (STACS 93)*, volume 665 of *Lecture Notes in Computer Science*, pages 58–68. Springer-Verlag, 1993.