Using HyTech to synthesize control parameters for a steam boiler*

Thomas A. Henzinger[1] and Howard Wong-Toi[2]

[1] Dept. of Electrical Engineering and Computer Sciences
University of California, Berkeley, CA, USA
[2] Cadence Berkeley Labs, Berkeley, CA, USA

Abstract. We model a steam-boiler control system using hybrid automata. We provide several abstracted models of the nonlinear behavior of the boiler. For each model, we describe a controller and demonstrate how the tool HyTech can be used to automatically synthesize control parameter constraints that guarantee safe operation of the boiler.

1 Evaluation and Comparison

Hybrid automata enable a relatively natural, yet mathematically formal, modeling of the steam boiler system. We model continuous behaviors directly. This provides a formal framework in which safety properties proven automatically for abstractions are also true for the originally specified continuous system. Because our modeling language includes information about continuous behaviors, we are able to discover nontrivial information about constants governing the physical behavior of the boiler, *e.g.* a lower bound on the safe lengths for the delay between rounds of communication, bounds on the water level achieved during operation, parametric correctness criteria for a variety of control scenarios. The advantage of an expressive model comes at a cost of computationally expensive automated analysis which restricts the size of the model HyTech can currently handle.

Here, we have modeled fault-free components as well as a simple fault-tolerant system. Designing the nonlinear hybrid automata was reasonably straightforward, although slightly tedious. We would expect an average programmer with some background in a state-machine formalism to have little difficulty understanding our model, and to be able to produce a similar solution after a couple of weeks' training. The majority of time developing the solution was spent in the iterative process of abstracting the nonlinear model to linear models, testing whether HyTech was able to produce useful results, and then redesigning our abstractions. The simplest abstractions were easy to derive, but produced coarse

* This research was supported in part by the ONR YIP award N00014-95-1-0520, by the NSF CAREER award CCR-9501708, by the NSF grants CCR-9200794 and CCR-9504469, by the AFOSR contract F49620-93-1-0056, and by the ARPA grant NAG2-892.

results, and were sometimes too conservative to establish system correctness for safe parameter combinations. However we found that more accurate approximations sometimes caused HyTech's semidecision procedures to fail, due to either memory overflow, arithmetic overflow in solving linear constraints, or a nonterminating sequence of iterations. Finding the balance between detail and abstraction, and modeling the system to optimize use of HyTech's analysis algorithms, is still somewhat of an art.

Our goal is automated analysis of the combined discrete and continuous components of the steam boiler. Among the papers in this volume, many abstract the continuous behavior into a discrete system (*e.g.* [7, 10, 21]) or a simple timed system (*e.g.* [20, 23]) which may then be subjected to automated analysis. Others analyze the continuous behavior deductively with the possible assistance of a mechanical proof-checker (*e.g.* [6, 11, 19, 22]). This paper is unique in that we largely retain continuous information about the boiler's physical quantities during automated analysis. While state-explosion forces us to keep the models simpler and smaller compared to discrete-state based methods, our approach allows the automated synthesis of constraints on the parameters controlling the continuous behavior.

References

1. J.-R. Abrial, E. Börger, and H. Langmaack. Additional information concerning the physical behaviour of the steam boiler. Note sent to participants in the Dagstuhl seminar, 1995.
2. Jean-Raymond Abrial. Steam-boiler control specification problem. In *Dagstuhl Meeting: Method for Semantics and Specification*, August 1995.
3. R. Alur, C. Courcoubetis, N. Halbwachs, T.A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138:3–34, 1995.
4. R. Alur, T.A. Henzinger, and P.-H. Ho. Automatic symbolic verification of embedded systems. In *Proceedings of the 14th Annual Real-time Systems Symposium*, pages 2–11. IEEE Computer Society Press, 1993.
5. R. Alur, T.A. Henzinger, and M.Y. Vardi. Parametric real-time reasoning. In *Proceedings of the 25th Annual Symposium on Theory of Computing*, pages 592–601. ACM Press, 1993.
6. Robert Buessow and Matthias Weber. A steam-boiler control specification with Statecharts and Z. This volume.
7. Thierry Cattel and Gregory Duval. The steam-boiler problem in Lustre. This volume.
8. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for the static analysis of programs by construction or approximation of fixpoints. In *Proceedings of the Fourth Annual Symposium on Principles of Programming Languages*. ACM Press, 1977.
9. P. Cousot and N. Halbwachs. Automatic discovery of linear restraints among variables of a program. In *Proceedings of the Fifth Annual Symposium on Principles of Programming Languages*. ACM Press, 1978.
10. Gregory Duval and Thierry Cattel. Specifying and verifying the steam-boiler problem with SPIN. This volume.

11. G.Leeb and N.Lynch. Proving safety properties of the steam boiler controller. This volume.
12. T.A. Henzinger and P.-H. Ho. Algorithmic analysis of nonlinear hybrid systems. In P. Wolper, editor, *CAV 95: Computer-aided Verification*, Lecture Notes in Computer Science 939, pages 225–238. Springer-Verlag, 1995.
13. T.A. Henzinger and P.-H. Ho. HyTech: The Cornell Hybrid Technology Tool. In P. Antsaklis, A. Nerode, W. Kohn, and S. Sastry, editors, *Hybrid Systems II*, Lecture Notes in Computer Science 999, pages 265–293. Springer-Verlag, 1995.
14. T.A. Henzinger, P.-H. Ho, and H. Wong-Toi. HyTech: The next generation. To appear at RTSS, 1995.
15. T.A. Henzinger, P.-H. Ho, and H. Wong-Toi . A user guide to HyTech. In E. Brinksma, W.R. Cleaveland, K.G. Larsen, T. Margaria, and B. Steffen, editors, *TACAS 95: Tools and Algorithms for the Construction and Analysis of Systems*, Lecture Notes in Computer Science 1019, pages 41–71. Springer-Verlag, 1995. Full version available as Technical Report CSD-TR-95-1532, Cornell University.
16. T.A. Henzinger, X. Nicollin, J. Sifakis, and S. Yovine. Symbolic model checking for real-time systems. *Information and Computation*, 111(2):193–244, 1994.
17. T.A. Henzinger and H. Wong-Toi. Linear phase-portrait approximations for nonlinear hybrid systems. In R. Alur and Thomas A. Henzinger, editors, *Hybrid Systems III*, Lecture Notes in Computer Science 1066, pages 377–388. Springer-Verlag, 1995.
18. P.-H. Ho and H. Wong-Toi. Automated analysis of an audio control protocol. In P. Wolper, editor, *CAV 95: Computer-aided Verification*, Lecture Notes in Computer Science 939, pages 381–394. Springer-Verlag, 1995.
19. XiaoShan Li and Juan Wang. Specifying optimal design of a steam-boiler system. This volume.
20. P.C. Olveczky, P. Kosiuczenko, and M. Wirsing. An object-oriented algebraic steam-boiler control specification. This volume.
21. Christian Schinagl. VDM specification of the steam-boiler control using RSL notation. This volume.
22. Jan Vitt and Jozef Hooman. Assertional specification and verification using PVS of the steam boiler control system. This volume.
23. Andreas Willig and Ina Schieferdecker. Specifying and verifying the steam-boiler control system with time extended LOTOS. This volume.