Analysis and Tools: Control Synthesis Algorithms

VERIMAG

May 3, 2004

AMETIST DELIVERABLE 2.2.1

Project acronym: AMETIST
Project full title: Advanced Methods for Timed Systems
Project no.: IST-2001-35304
Project Co-ordinator: Frits Vaandrager
Project Start Date: 1 April 02
Duration: 36 months
Project home page: http://ametist.cs.utwente.nl/

While verification is concerned with proving that a system is correct with respect to all external disturbances, synthesis attempts to mechanize the choice between design options for the system in order to produce a system which is provably correct with respect to all disturbances. Clearly this problem is more difficult than verification although the underlying algorithmic principles are similar.

This report summarizes the progress in understanding, development and implementation of control synthesis algorithms. This topic is closely related to deliverable 1.5 of the first year *modeling: control synthesis*, and in order to avoid redundancy we will not repeat here most of what has been said there. The reader may consult deliverable 1.5 to complete the picture.

The work on synthesis algorithms within the project can be roughly classified into the following categories:

- Application specific synthesis.
- Application oriented algorithms.
- General algorithms for new classes of problems.
- Algorithmic specialization.
- A unifying framework.

Application Specific Synthesis

Under this title we group works that attempt to solve a single specific problem. The outcome of this work is typically not a general theorem but rather an acceptable solution to a real problem. The solution is not always obtained by a complete semantic model that covers all the system's modes of functioning but rather using a "piecewise-formal" model. For example, scheduling for production plants over long time durations, can be done by ignoring uncertainty, solving short term problems using deterministic models, and coping with uncertainty, for example, by re-scheduling. Some examples of work in this style are [28, 29, 31, 14], which are oriented toward optimization of operations in chemical plants.

Other work that falls in this category is related, of course, to the case-studies. For the Cybernetix case-study [15] show that synthesis can be achieved for this problem using standard verification tools. For the Terma case-study, an optimal scheduler was synthesized by hand in [36].

Application Oriented Algorithms

Here we mention work intended to solve a whole class of problems whose primary motivation comes form a particular concrete application domain (rather starting from a mathematical model). One line of research is oriented toward the application of timed automata synthesis technology to scheduling-aware compilation of real-time embedded systems. This framework is put forward in [4, 30] and one of its concrete realization is the system defined in [17, 18] for synthesizing schedules with guaranteed quality of service for Java threads. Being constrained by the application, this tool has the cope with additional aspects that are absent from idealized problems such as interfacing with the compiler and implementing the scheduler with *bounded resources*. Another related work is that of [13], dealing with code generation from Simulink models, although "synthesis" is taken here in a more narrow sense. See also [11] which is related to the same application domain.

General Algorithms for New Problems

This class contains algorithms that extend the scope of synthesis to richer models and performance criteria. Controller synthesis for timed automata for safety, reachability and time optimality criteria has been known to be decidable since several years. A large part of the activity in this domain is to check whether the same holds for other models. A lot of work has been invested in enriching the model with *non uniform costs*, rather than time. In [8] the difficult problem of optimal synthesis with respect to linear costs (in the presence of adversary) has been solved. The problem of cost optimality of infinite schedules was

solved with respect to two concurrent performance criteria (safety and cost optimality), while [27] was concerned with related implementation aspects of synthesis algorithms for cost optimality. The extension of the synthesis framework to partial observability was addressed in [9]. The tool Smart-Playout which connects the specification formalisms of live sequence charts to the model-checker SMV has been adapted and used for controller synthesis in [37, 20]. Other works were concerned with synthesis algorithms for systems defined by linear hybrid automata and even richer models of dynamical systems [32, 23, 33, 34, 6].

Algorithmic Specialization

Proving that a general problem is solvable still does not mean that it is practically feasible, and much effort was invested in finding specialized algorithms and data-structure to solve specific instances of controller synthesis, especially those arising in scheduling problems. In [26] an attempt was made to improve performance by combining reachability analysis and linear programming. The work of [3, 1] finds efficient synthesis algorithms for the special case of scheduling under temporal uncertainty in task durations, while in [2] some ideas coming from partial order methods are explored. The idea of using forward search, first proposed in [5] was elaborated and implemented in [10] to deal with scheduling problems with discrete uncertainty. The integration of cost optimality into the UPPAAL tool is the subject of [7].

A Unifying Framework

The synthesis paper [22], prepared in collaboration with the project CC (Control and Computation), attempts to put many controller synthesis problems under the unified model of two-players dynamic game. It shows that this model captures "classical" synthesis for automata, optimal control for discrete time continuous systems as well as optimal scheduling problems viewed as a special type of a discrete game played on continuous time. The paper identifies three classes of algorithms for solving such problems, static optimization for bounded horizon problems, backward value iteration (dynamic programming) and heuristic forward search on alternating graphs.

Other Work

In addition to the above we mention other work which is not specific for synthesis but deals with other aspects of validation, in particular the hot topic of real-time testing and its foundations [12, 16, 21, 19, 35, 24, 25].

To summarize, the project continues to advance the state-of-the-art and the understanding of the issue of automatic controller synthesis for discrete and timed systems, and, during the second year, significant contributions to the algorithmic aspects of controller synthesis have been made.

References

[1] Y. Abdeddaïm, E. Asarin, and O. Maler. Scheduling with timed automata. In *Theoretical Computer Science (to appear)*, 2004. Available from World Wide Web: `http://www-verimag.imag.fr/~maler/Papers/schedule-tcs.ps`.

[2] Y. Abdeddaïm and P. Niebert. On the use of partial order methods in scheduling. In *Ninth International Conference on Project Management and Scheduling (PMS 04)*, 2004. Available from World Wide Web: `http://www.cmi.univ-mrs.fr/~niebert/docs/pms04.pdf`. to be published as online abstract.

[3] Yasmina Abdeddaïm. *Scheduling with Timed Automata*. PhD thesis, INPG Grenoble, November 2002. Available from World Wide Web: `http://www-verimag.imag.fr/~maler/Papers/thesis-yasmina.ps`.

[4] K. Altisen, G. Goessler, and J. Sifakis. Scheduler modeling based on the controller synthesis paradigm. *Journal of Real-Time Systems, special issue on Control Approaches to Real-Time Computing*, 23:55–84, 2002. Available from World Wide Web: `http://www-verimag.imag.fr/~sifakis/paper_final.pdf`.

[5] K. Altisen and S. Tripakis. Tools for controller synthesis of timed systems. In *RT-TOOLS*, 2002. Available from World Wide Web: `http://www-verimag.imag.fr/~tripakis/final-rttools02.pdf`.

[6] Zvi Artstein and Gera Weiss. State nullification by memoryless output feedback. *MCSS*, 2004. In print.

[7] G. Behrmann. Guiding and cost optimizing uppaal. Web-page, 2002. Available from World Wide Web: `http://www.cs.auc.dk/~behrmann/_guiding/`.

[8] P. Bouyer, F. Cassez, E. Fleury, and K. G. Larsen. Optimal strategies in priced timed game automata. BRICS Report Series RS-04-4, Basic Research In Computer Science, 2004. Available from World Wide Web: `http://www.brics.dk/RS/04/4/BRICS-RS-04-4.ps.gz`.

[9] P. Bouyer, D. D'Souza, P. Madhusudan, and A. Petit. Timed control with partial observability. In *Proc. of 15th Int. Conf. Computer Aided Verification (CAV'2003)*, volume 2725 of *Lecture Notes in Computer Science*, pages 180–192. Springer-Verlag, 2003. Available from World Wide Web: `http://www.lsv.ens-cachan.fr/Publis/PAPERS/BDMP-cav-2003.ps`.

[10] M. Bozga, A. Kerbaa, and O. Maler. Optimal scheduling of acyclic branching programs on parallel machines. 2004. Submitted for publication.

[11] E. Brinksma and A. Mader. Model checking embedded system designs (invited). In *6th Int. Workshop on Discrete Event Systems (WODES)*, pages 151–158, Zaragoza, Spain, 2002. IEEE Computer Society Press, Los Alamitos, California. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/UTpublications/WODESexabs.pdf`.

[12] Laura Brand'an Briones and Ed Brinksma. A test generation framework for quiescent real-time systems, 2004. Submitted to FACS.

[13] P. Caspi, A. Curic, A. Maignan, C. Sofronis, S. Tripakis, and P. Niebert. From Simulink to SCADE/Lustre to TTA: a layered approach for distributed embedded applications. In *Languages, Compilers, and Tools for Embedded Systems (LCTES'03)*. ACM, 2003.

[14] S. Engell, A. Maerkert, G. Sand, and R. Schultz. Aggregated scheduling of a multiproduct batch plant by two-stage stochastic integer programming. *Optimization and Engineering*, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/OE04.pdf`. (accepted).

[15] B. Gebremichael and F.W. Vaandrager. Control synthesis for a smart card personalization system using symbolic model checking. In *Proceedings First International Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS 2003), m September 6-7 2003, Marseille, France*, volume 2791 of *LNCS*. Springer Verlag, 2003. Available from World Wide Web: `http://www.cs.kun.nl/ita/publications/papers/fvaan/smart.html`.

[16] A. Hessel, K. G. Larsen, B. Nielsen, P. Pettersson, and A. Skou. Time-optimal test cases for real-time systems. In *Proc. of 1st Int. Workshop on Formal Modeling and Analysis of Timed Systems (FORMATS'2003)*, Lecture Notes in Computer Science. Springer-Verlag, 2003. Available from World Wide Web: `http://www.docs.uu.se/docs/rtmv/papers/hlnps-formats03.pdf`. To appear.

[17] Ch. Kloukinas and S. Yovine. Synthesis of safe, qos extendible, application specific schedulers for heterogeneous real-time systems. In *Proceedings of '5th Euromicro Conference on Real-Time Systems (ECRTS'03)'*, Porto, Portugal, July 2003. Available from World

Wide Web: `http://www-verimag.imag.fr/PEOPLE/Christos.Kloukinas/IN2P3/kloukinas_yovine.pdf`.

[18] Christos Kloukinas, Chaker Nakhli, and Sergio Yovine. A methodology and tool support for generating scheduled native code for real-time Java applications. In Rajeev Alur and Insup Lee, editors, *EMSOFT 2003*, volume 2855 of *Lecture Notes in Computer Science*, pages 274–289, Philadelphia, Pennsylvania, USA, 2003. Springer-Verlag.

[19] M. Krichen and S. Tripakis. Black-box conformance testing for real-time systems. In *11th International SPIN Workshop on Model Checking of Software (SPIN'04)*, volume 2989 of *LNCS*. Springer, 2004.

[20] Hillel Kugler and Gera Weiss. Planning a production line with LSCs. Research report, Weizmann, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/WISPublications/cybernetix.zip`.

[21] K. G. Larsen, M. Mikucionis, and B. Nielsen. Real-time system testing on-the-fly. Brics report series, Basic Research In Computer Science, 2003. Available from World Wide Web: `http://www.brics.dk/RS/03/49/BRICS-RS-03-49.pdf`.

[22] O. Maler. On optimal and sub-optimal control in the presence of adversaries. 2004. Available from World Wide Web: `http://www-verimag.imag.fr/~maler/Papers/wodes.ps`. Invited talk at WODES'04.

[23] O. Maler, B. Krogh, and M. Mahfoudh. On control with bounded computational resources. In W. Damm and E-R Olderog, editors, *FTRTFT'02*, volume 2469 of *LNCS*, pages 147–164. Springer. Available from World Wide Web: `http://www-verimag.imag.fr/PEOPLE/Oded.Maler/Papers/resources.ps`.

[24] O. Maler and D. Nickovic. Monitoring temporal properties of continuous signals. 2004. Submitted for publication.

[25] Oded Maler and Amir Pnueli. On Recognizable Timed Languages. In Igor Walukiewicz, editor, *Proceedings FOSSACS 2004, Barcelona, Spain, March 29 - April 2, 2004*, volume 2987 of *Lecture Notes in Computer Science*, pages 348–362. Springer, 2004. Available from World Wide Web: `http://www.informatik.uni-trier.de/~ley/db/conf/fossacs/fossacs2004.html#MalerP04`.

[26] S. Panek, O. Stursberg, and S. Engell. Job-shop scheduling by combining reachability analysis with linear programming. In *Proc. 7th Int. Workshop on Discrete Event Systems*, 2004. (submitted).

[27] J. Rasmussen, K. G. Larsen, and K. Subramani. Scheduling using priced timed automata. In *Proc. 10th Int. Conf. of Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2004)*, volume 2988 of *Lecture Notes in Computer Science*, pages 220–235. Springer-Verlag, 2004. Available from World Wide Web: `http://www.springerlink.com/app/home/contribution.asp?wasp=9a0qbvyyrjdjt6rvmewp&referrer=parent&back`.

[28] G. Sand and S. Engell. Aggregated batch scheduling in a feedback structure. In J. v. Schijndel and J. Grievink, editors, *European Symp. on Computer Aided Process Engineering-12*, volume 10 of *Computer-Aided Chemical Engineering*, pages 775–780. Elsevier Science, 2002. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/cp2_sand+_02.ps`.

[29] G. Sand and S. Engell. Risk conscious scheduling of batch processes. In *Proc. Computer-Aided Chemical Engineering*, pages 588–593, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/CACE04.pdf`.

[30] J. Sifakis, S. Tripakis, and S. Yovine. Building models of real-time systems from application software. In *Proceedings of the IEEE Special issue on modeling and design of embedded*, pages 91(1):100–111, January 2003. Available from World Wide Web: `http://ieeexplore.ieee.org/xpls/abs_all.jsp?isNumber=26369?=JNL&arnumber=1173199&arSt=+100&ared=+111&arAuthor=Sifakis%2C+J.%3B+Tripakis%2C+S.%3B+Yovine%2C+S.&arNumber=1173199&a_id0=1173177&a_id1=1173180&a_id2=1173184&a_id3=1173187&a_id4=1173191&a_id5=1173196&a_id6=1173199&a_id7=1173202&a_id8=1173203&a_id9=1173205&a_id10=1173207&a_id11=1173210&a_id12=1173213&a_id13=1173215&a_id14=1173229&count=15`.

[31] O. Stursberg. Dynamic optimization of processing systems with mixed degrees of freedom. In *Proc. 7th Int. Symposium on Dynamics and Control of Process Systems*, 2004. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/DYCOPS04.pdf`. (to appear).

[32] O. Stursberg. A graph search algorithm for optimal control of hybrid systems. In *Proc. 43rd IEEE Conf. on Decision and Control*, 2004. (submitted).

[33] Olaf Stursberg and Sebastian Engell. Optimal control of switched continuous systems using mixed-integer programming. In *15th IFAC World Congress of Automatic Control*, Barcelona, Spain, 2002. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/IFAC_WC_02.pdf`.

[34] Olaf Stursberg and Sebastian Panek. Control of switched hybrid systems based on disjunctive formulations. In *Hybrid Systems: Computation and Control, LNCS 2289*, pages 421–435. Springer, 2002. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/DORTMUNDPublications/78hscc02.pdf`.

[35] S. Tripakis. Folk theorems on the determinization and minimization of timed automata. In *Formal Modeling and Analysis of Timed Systems (FORMATS'03)*, LNCS. Springer, 2003.

[36] Gera Weiss. Optimal Scheduler for a Memory Card. Research report, Weizmann, 2002. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/WISPublications/Optimal_Schedule_for_a_Memory_Card`.

[37] Gera Weiss. Modeling smart-card personalization machine with LSCs. Research report, Weizmann, 2003. Available from World Wide Web: `http://ametist.cs.utwente.nl/INTERNAL/PUBLICATIONS/WISPublications/cybernetix.zip`.