Indo Swiss Joint Research Programme (ISJRP)

Project IT01
Games in system design and verification

Final report submitted by the Swiss project partners:

Dr. Barbara Jobstmann & Prof. Thomas Henzinger
Models and Theory of Computation Laboratory (MTC)
Swiss Federal Institute of Technology Lausanne (EPFL), 1015 Lausanne

Project duration: December 1st, 2006 – September 30th, 2009
Keywords: Formal verification, model checking

INDIAN PROJECT PARTNER

Prof. Pallab Dasgupta
Dept. of Computer Science & Engineering
Indian Institute of Technology (IIT) Kharagpur
Kharagpur - 721 302, INDIA

A) SYNTHESIS OF THE PROJECT

In this project, we use games played on graphs as a unifying framework to design, validate, and synthesize state-event systems. Games provide an intuitive way to capture conflicting behaviors. Modern computer systems exhibit several source of conflict, e.g., several computers want to access the same printer, or two different programs have to share processor time.

Traditionally, games studied in computer science are two-player zero-sum games. In these games, two players compete against each other by pushing a token along edges in a graph structure. A play is then evaluated based on the vertices of the graph the token has visited. Zero-sum refers to the fact that the sum of the rewards the two players get in a play is zero.

In this project, we have developed and analyzed several generalizations of this basic model to describe and solve fundamental problems arising in the areas of specification and validation of safety-critical systems, software verification and synthesis, interface design and verification for webservices, etc.

We obtained new theoretical as well as practical results published in international conferences and journals. The results can be classified in four categories:

1. Synthesis

2. Imperfect information and concurrent games

3. New complexity results for stochastic and omega regular games

4. Applications and evaluation of algorithms

B) RESULTS

Synthesis: The synthesis problem asks, given a specification, to construct a system that satisfies the specification. If the specification is temporal, then synthesis amounts to finding a winning strategy in a game played against an adversarial environment that attempts to violate the specification.

For multi-component systems, the two-player zero-sum model is no longer suitable. We initiated a fundamental study of games with two or more players that are not necessarily in conflict. Based on assume-guarantee principles, we defined and studied secure equilibria [CHJ06] and iteratively admissible strategies [B07] as solution concepts for games with infinitary objectives. In this framework, we refined the classical synthesis problem to assume-guarantee synthesis [CH07] for components that consist themselves of independent processes and showed that this problem can be solved by computing secure equilibria.

We solved the synthesis problem when the system has to be constructed under a limited budget [CMH08a]. We also showed how to compute weakest possible assumptions on the environment that make successful synthesis possible [CHJ08, GIST09]. In [BCHJ09], we showed that quantitative objectives can be used to measure the «goodness» of an implementation. Using games with corresponding quantitative objectives, we can synthesize «optimal» implementations, which are preferred among the set of possible implementations

that satisfy a given specification. This approach has been implemented in [qSynth09] and extended to measuring system under a probabilistic environment [CHJS09].

Using our quantitative synthesis framework [BCGHJ09], we provided a notion of robustness based on error functions. Error function maps all possible behaviors of a system to values representing the number of defaults of the system or its environment. We provide algorithms to check if a system is robust and to construct robust systems.

Imperfect information and concurrent games: We developed a solution for minimum-time reachability in concurrent timed games [BHPR07]. We developed and implemented the first practical algorithms for solving two important generalizations of classical graph games, namely, graph games where the players have imperfect information about the state of the game [BCDHR08, BCDDH09], and graph games where the players move simultaneously and independently [CdAH09]. In the latter case, optimal strategies can be only approximated.

New complexity results for stochastic and omega regular games: If the system or environment can behave probabilistically, then the appropriate model for synthesis is the setting of stochastic games. We analyzed the exact computational complexity of stochastic graph games with parity objectives [CH08], which are a canonical form of qualitative objectives, and with mean-payoff objectives [CMH08a], which are a canonical form of quantitative objectives. We also investigated stochastic games with limit-average payoffs and settled the complexity of computing their value [CMH08b]. A significant complexity improvement resulted from our analysis of generalized parity games [CHP07]. These are special instances of Rabin and Streett games that arise naturally in verification and that can be solved much easier than the generic games.

Applications and Evaluation of Algorithms: An fundamental concern of our investigation was to develop algorithms that are scalable. We conducted a comparative analysis of different approaches to interface synthesis [BHS07]. To illustrate the formalism for specification and verification of webservice, we developed a case study based on the Amazon.com E-Commerce Services platform [BCHS07]. Synergy is a new algorithm for property checking over implicitly specified systems with infinite state space [GHKNR06]. A prototype of this algorithm which combines techniques from testing and from verification has been implemented.

C) OVERALL ASSESSMENT

The project was successful in the sense that we obtained many interesting new scientific results.

D) SWISS PERSONNEL EMPLOYED

Dr. Dietmar Berwanger (1.1.2007-15.7.2007)
Dr. Barbara Jobstmann (1.11.2007-30.9.2009)

E) LIST OF PUBLICATIONS

Publications in reviewed venues

[HP06] Thomas A. Henzinger and Vinayak S. Prabhu. Timed alternating-time temporal logic. In Proc. of the 4th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS), volume 4202 of LNCS, pages 1–17. Springer, 2006.

[CHJ06] Krishnendu Chatterjee, Thomas A. Henzinger, and Marcin Jurdzinski. Games with secure equilibria. Theor. Comput. Sci., 365(1-2):67–82, 2006.

[B07] Dietmar Berwanger. Admissibility in infinite games. In Proc. of the 24th Annual Symposium on Theoretical Aspects of Computer Science (STACS), volume 4393 of LNCS, pages 188–199. Springer, 2007.

[BCHS07] Dirk Beyer, Arindam Chakrabarti, Thomas A. Henzinger, and Sanjit A. Seshia. An application of web-service interfaces. In Proc. of the International Conference on Web Services (ICWS). IEEE Computer Society Press, 2007.

[BHS07] Dirk Beyer, Thomas A. Henzinger, and Vasu Singh. Algorithms for interface synthesis. In Proc. of the 19th International Conference on Computer-Aided Verification (CAV), volume 4590 of LNCS, pages 4–19. Springer, 2007.

[BHPR07] Thomas Brihaye, Thomas A. Henzinger, Vinayak Prabhu, and Jean-François Raskin. Minimum-time reachability in timed games. In Proc. of the 34th International Colloquium on Automata, Languages, and Programming (ICALP), LNCS. Springer, 2007.

[CH07] Krishnendu Chatterjee and Thomas A. Henzinger. Assume-guarantee synthesis. In Proc. of the 13th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), number 4424 in LNCS, pages 261–275. Springer, 2007.

[CHP07] Krishnendu Chatterjee, Thomas A. Henzinger, and Nir Piterman. Generalized parity games. In Proc. of the Tenth International Conference on Foundations of Software Science and Computation Structures (FOSSACS), number 4423 in LNCS, pages 153–167. Springer, 2007.

[CMH08a] Krishnendu Chatterjee, Rupak Majumdar, and Thomas A. Henzinger, Controller Synthesis with Budget Constraints. In proceedings of the 11th International Workshop on Hybrid Systems: Computation

and Control (HSCC), LNCS 4981, Springer, pp. 72-86, 2008.

[CMH08b] Krishnendu Chatterjee, Rupak Majumdar, and Thomas A. Henzinger, Stochastic Limit-Average Games are in EXPTIME. In International Journal of Game Theory 37:219-234, 2008.

[CHJ08] Krishnendu Chatterjee, Thomas A. Henzinger, and Barbara Jobstmann. Environment Assumptions for Synthesis. In Proceedings of the 19th International Conference on Concurrency Theory (CONCUR), LNCS 5201, Springer, 2008, pp. 147-161.

[BCDHR08] Dietmar Berwanger, Krishnendu Chatterjee, Laurent Doyen, Thomas A. Henzinger, and Sangram Raje, Strategy Construction for Parity Games with Imperfect Information. In proceedings of the 19th International Conference on Concurrency Theory (CONCUR), LNCS 5201, Springer, 2008, pp. 325-339.

[CH08] Krishnendu Chatterjee and Thomas A. Henzinger, Reduction of Stochastic Parity to Stochastic Mean-Payoff Games. In Information Processing Letters 106:1-7, 2008.

[CdAH09] Krishnendu Chatterjee, Luca de Alfaro, and Thomas A. Henzinger, Termination Criteria for Solving Concurrent Safety and Reachability Games. In proceedings of the 20th Annual Symposium on Discrete Algorithms (SODA), ACM Press, January 2009.

[BCHJ09] Roderick Bloem and Krishnendu Chatterjee and Thomas Henzinger and Barbara Jobstmann, Better Quality in Synthesis through Quantitative Objectives. In Computer Aided Verification (CAV)'09, Grenoble, France, 2009.

[BGHJ09] Roderick Bloem, Karin Greimel, Thomas Henzinger, and Barbara Jobstmann, Synthesizing Robust Systems. In Conference on Formal Methods in Computer Aided Design (FMCAD'09), Austin, Texas, 2009.

[BCDDH09] Dietmar Berwanger, Krishnendu Chatterjee, Martin De Wulf, Laurent Doyen, and Thomas A. Henzinger, Alpaga: A tool for solving parity games with imperfect information. In proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS), pp. 58-61, 2009.

Poster presentations and tools

[BCGHJ09] Roderick Bloem, Krishnendu Chatterjee, Karin Greimel, Thomas Henzinger and Barbara Jobstmann, Quality through Quantity. In International Conference on Formal Methods and Models for Codesign (MEMOCODE'09), Boston, Massachusetts, 2009.

[GIST09] Arjun Radhakrishna, GIST - a tool for solving probabilistic games with ω-regular objectives qualitatively. http://pub.ist.ac.at/gist/

[qSynth09] Rohit Singh, qSynth - a tool for quantitative synthesis. http://www.cse.iitb.ac.in/~rohitsingh/qsynth/

[CHJS09] Krishnendu Chatterjee, Thomas Henzinger, Barbara Jobstmann, and Rohit Singh, Measuring Systems under Probabilistic Environments. Report.

F) SCIENTIFIC VISITS & EXCHANGES

Visitor(s)	Host	Purpose	Start date & duration of visit
P. Dasgupta & P.P. Chakrabarti, IIT Khragpur	T. Henzinger, EPFL	Kick-off meeting	June 2006, 1 week
D. Berwanger, EPFL	P. Dasgupta, IIT Kharagpur	Coordination, presentation	January 2007, 1 week
K. Chatterjee & V. Prabhu, IIT Kharagpur	T. Henzinger, EPFL	Internship	November 2007, 1 month
K. Chatterjee, IIT Kharagpur	T. Henzinger, EPFL	Scientific collaboration	April 2008, 1 week
R. Majumdar, IIT Kharagpur	T. Henzinger, EPFL	Scientific collaboration	June 2008, 10 days
S. Raje & A. Radhakrishna, IIT Kharagpur	T. Henzinger, EPFL	Internship	May 2008, 7 weeks
R. Gupta & R. Singh, IIT Kharagpur	T. Henzinger, EPFL	Internship	May 2009, 11 weeks