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 sources 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 webservers, 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

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 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 [BCHDHR08, 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:** A 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 web service, 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


**Poster presentations and tools**


---

**F) SCIENTIFIC VISITS & EXCHANGES**

<table>
<thead>
<tr>
<th>Visitor(s)</th>
<th>Host</th>
<th>Purpose</th>
<th>Start date &amp; duration of visit</th>
</tr>
</thead>
<tbody>
<tr>
<td>P. Dasgupta &amp; P.P. Chakrabarti, IIT Kharagpur</td>
<td>T. Henzinger, EPFL</td>
<td>Kick-off meeting</td>
<td>June 2006, 1 week</td>
</tr>
<tr>
<td>D. Berwanger, EPFL</td>
<td>P. Dasgupta, IIT Kharagpur</td>
<td>Coordination, presentation</td>
<td>January 2007, 1 week</td>
</tr>
<tr>
<td>K. Chatterjee &amp; V. Prabhu, IIT Kharagpur</td>
<td>T. Henzinger, EPFL</td>
<td>Internship</td>
<td>November 2007, 1 month</td>
</tr>
<tr>
<td>K. Chatterjee, IIT Kharagpur</td>
<td>T. Henzinger, EPFL</td>
<td>Scientific collaboration</td>
<td>April 2008, 1 week</td>
</tr>
<tr>
<td>R. Majumdar, IIT Kharagpur</td>
<td>T. Henzinger, EPFL</td>
<td>Scientific collaboration</td>
<td>June 2008, 10 days</td>
</tr>
<tr>
<td>S. Raje &amp; A. Radhakrishna, IIT Kharagpur</td>
<td>T. Henzinger, EPFL</td>
<td>Internship</td>
<td>May 2008, 7 weeks</td>
</tr>
</tbody>
</table>