New methods in verification of multi-agent systems and e-voting protocols

Wojciech Penczek

Institute of Computer Science, PAS, Warsaw
penczek@ipipan.waw.pl

1 Project Description

Multi-agent systems describe interactions of multiple entities called *agents*, often assumed to be intelligent and autonomous. *Alternating-time temporal logic* $\mathbf{ATL}^*$ and its fragment $\mathbf{ATL}$ [1] are logics which allow for reasoning about strategic interactions in such systems, by extending the framework of temporal logic with the game-theoretic notion of *strategic ability*. Hence, $\mathbf{ATL}^*$ enables to express statements about what agents (or groups of agents) can achieve. Such properties can be useful for specification, verification, and reasoning about interaction in agent systems and security and usability in e-voting protocols. They have become especially relevant due to active development of algorithms and tools for verification where the "correctness" property is given in terms of strategic ability [4]. However, there are several obstacles First, most of the tools and algorithmic solutions focus on agents with perfect information, i.e., agents who at any point of the game know exactly the global state of the game, which is clearly unrealistic in all but the simplest multi-agent scenarios. The imperfect information semantics of $\mathbf{ATL}$ does not admit alternation-free fixpoint characterizations [3], which makes incremental synthesis of strategies impossible, or at least difficult to achieve. Secondly, the semantics of strategic logics are almost exclusively based on synchronous concurrent game models. That is, one implicitly assumes the existence of a global clock that triggers subsequent global events in the system. However, many real-life systems are inherently asynchronous, and do not operate on a global clock that perfectly synchronizes the atomic steps of all the components.

The aim of the project is to develop a new methodology for verification of agents with imperfect information, using strategy logics interpreted on asynchronous models [2]. As far as the applications are concerned, the main focus will be on voting procedures and protocols, and in particular on their essential features like confidentiality, coercion-resistance, and voter-verifiability.

More specifically, the verification methods will include:

- Symbolic model checking using BDD's, SAT-solvers, or SMT-solvers,
- Nature inspired algorithms such as Genetic Algorithm, Simulated Annealing, or Generalized Optimization Algorithm,
- Hybrid algorithms combining symbolic and nature inspired methods,
- Model abstractions based on data and state abstractions,
- Model reductions such as partial order reductions or symmetry reductions.

2 Candidate's Profile

The candidate is required to have a strong background in mathematical logics, including modal logics, as well as programming skills (C, Java). Some knowledge of formal methods and verification techniques is expected. The candidate should also have good communication skills and good skills in oral and written English.

References

1. R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time Temporal Logic. *Journal of the ACM*, 49:672–713, 2002.
2. P. Dembinski, W. Jamroga, A. Mazurkiewicz, and W. Penczek. Towards partial order reductions for fragments of alternating-time temporal logic. Technical report, ICS PAS Report 1036, 2016.
3. C. Dima, B. Maubert, and S. Pinchinat. Relating paths in transition systems: The fall of the modal mu-calculus. In *Proceedings of MFCS*, volume 9234 of *Lecture Notes in Computer Science*, pages 179–191. Springer, 2015.
4. A. Lomuscio, H. Qu, and F. Raimondi. MCMAS: An open-source model checker for the verification of multi-agent systems. *International Journal on Software Tools for Technology Transfer*, 2015. Availabe online.