Internship Proposal (M2): Diagnosing Controller Synthesis

Place: Inria - Irisa, Rennes – SUMO team (http://www.irisa.fr/sumo/)

In discrete-event systems, *diagnosis* consists in determining in bounded time and with certainty whether a fault has occurred given a sequence of observations [4]. In fact, if some events internal to the system are not observable from outside, then a given observation sequence can correspond to several executions, some of which are faulty and other non-faulty. The simplest formalism for this problem is finite automata, and algorithms were given to check if a given model is diagnosable. However some systems carry an intrinsic ambiguity and the observations are not sufficient for diagnosing faults. *Active diagnosis* was suggested to overcome this issue [3, 2]. It consists in controlling the system by activating some events, and disabling some others, so that all induced executions can be diagnosed: whether a fault has occurred in the controlled system can be determined by looking at observations.

The only objective in the active diagnosis problem is to control the system to make sure that any fault is diagnosed. But the computed controller does not guarantee any other property on the controlled system; for instance, a controller that makes sure that a fault always occurs is a possible solution to active diagnosis since it guarantees diagnosability. Some partial solutions were given, *e.g.* in [1], where it is required that the controller guarantees non-faulty behaviors with positive probability.

In this internship, we suggest improving the active diagnosis problem to address this issue. We will consider diagnosability as an additional and secondary objective to be taken into account in controller synthesis with a given primary objective. Roughly, the controller should try to satisfy its primary objective, such as trying to avoid faults, and give additional diagnosability guarantees if this is not possible. The proper formalization of this idea is one of the objectives of this internship. For instance, what does it mean for a controller to *try to* avoid a fault? There are several directions that can be followed. One can explore the possibility of computing controllers that make sure that no fault occurs for a maximal subset of states, while ensuring diagnosability for the rest of the states. One can also formulate the problem in a quantitative way and look for controllers that minimize the time to fault. A third possibility is to use game theoretic notions to compare control strategies: for instance, a controller that ensures a fault immediately is worse than a controller that avoids any fault for k steps, and then possibly allow a fault without forcing it. Several classical notions from game theory, such as rationality, dominance, and regret, can be applied here to capture *reasonable* controllers.

The direction to be explored can be chosen according to the intern's interests.

Keywords: Automata theory, formal languages, discrete-event systems, game theory, partial-information games, quantitative graph games, probabilistic automata

Related courses (Rennes): Parcours 1, Techniques de Vérification Avancées

Supervisors: Nathalie Bertrand (`http://people.rennes.inria.fr/Nathalie.Bertrand`), Hervé Marchand (`http://people.rennes.inria.fr/Herve.Marchand/`), Ocan Sankur (`http://www.ulb.ac.be/di/verif/sankur`)

Contact: osankur@ulb.ac.be, {nathalie.bertrand,herve.marchand}@inria.fr

References

[1] N. Bertrand, É. Fabre, S. Haar, S. Haddad, and L. Hélouët. Active diagnosis for probabilistic systems. In A. Muscholl, editor, *FoSSaCS'14*, volume 8412 of *Lecture Notes in Computer Science*, pages 29–42, Grenoble, France, Apr. 2014. Springer.

[2] S. Haar, S. Haddad, T. Melliti, and S. Schwoon. Optimal constructions for active diagnosis. In A. Seth and N. Vishnoi, editors, *FSTTCS'13*, volume 24 of *Leibniz International Proceedings in Informatics*, pages 527–539, Guwahati, India, Dec. 2013. Leibniz-Zentrum für Informatik.

[3] M. Sampath, S. Lafortune, and D. Teneketzis. Active diagnosis of discrete-event systems. *Automatic Control, IEEE Transactions on*, 43(7):908–929, 1998.

[4] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis. Diagnosability of discrete-event systems. *Automatic Control, IEEE Transactions on*, 40(9):1555–1575, 1995.