First order logic and fix-point: Modeling opacity control problems in terms of logic

Encadrants

Hervé Marchand (Contact)
Mail : herve.marchand@inria.fr
Téléphone : 0299847509

Sophie Pinchinat
Mail : sophie.pinchinat@irisa.fr

Structure d'accueil

Ville : Rennes
Désignation de l'établissement : Laboratoire
Nom de l'établissement : IRISA
Équipe : LogicA

Keywords : Security, Opacity, Control Theory, Logic.

Description :

Security is one of the most important and challenging aspect in designing services deployed on large open networks, like Internet or mobile phones, e-voting systems etc., that is nowadays a very active area in the research community in formal methods. We focused here on the particular case of the notion of *opacity* [1] that expresses the inability of an inquisitive attacker to infer some given information given its observation capabilities. This information can be a particular pattern in the executed sequence of events, or the fact that the system is in some distinguished configuration.

Opacity has been extensively investigated in the literature, mostly in an abstract formal-language centric setting, where the two main concerns are its verification and the ability to control the system so that, for the remaining behavior, the opacity property holds [2,3,4,5]. In order to obtain deeper results and/or to answer questions left open, we advocate the use of logic to capture essential features of opacity properties. For example, we recently made use of First-order Logic (FOL) to specify the property of opacity for systems with synchronous observations, and use the extension of FOL with fix-points [6,9] to characterize the maximal sub-behavior of a system where opacity holds.

The main purpose of the internship is to promote the logical approach as a powerful tool to solve part of the many relevant questions left in the literature, and to derive related algorithms. For example, it is currently not established whether the maximal sub-behavior of a system where opacity holds is a regular language or not, since FOL with fix-point may, in its full generality, describe non-regular languages. The challenge here consists in identifying fragments of FOL with fix-point that give rise to regular languages only. A promising approach is a combination of the automatic structure setting [7-8] and a fine-grained restriction on observational equivalence [10.11].
Needless to say that the investigations of the internship encompass an accurate study of the problems' complexity, and their companion algorithms.

Web : http://www-logica.irisa.fr/

http://people.rennes.inria.fr/Herve.Marchand/

http://people.irisa.fr/Sophie.Pinchinat/

Bibliography

[1] J.W. Bryans, M. Koutny, L. Mazaré, P.Y.A. Ryan: Opacity Generalized to Transition Systems. Int. Journal of Computer Security, vol. 7(6), 2008, pp 421-435.

[2] J. Dubreil, Ph. Darondeau, H. Marchand. Supervisory Control for Opacity. IEEE Transactions on Automatic Control, 55(5):1089-1100, May 2010.

[3] J., Romain, J.-J. Lesage, and J.-M. Faure. "Overview of discrete event systems opacity: Models, validation, and quantification." *Annual reviews in control* 41 (2016): 135-146.

[4] S. Lafortune, F. Lin, and C. N. Hadjicostis. "On the history of diagnosability and opacity in discrete event systems." *Annual Reviews in Control* 45 (2018): 257-266.

[5] B. Maubert, S. Pinchinat and L. Bozzelli. Opacity Issues in Games with Imperfect Information. Gandalf 2011, 2nd International Symposium on Games, Automata, Logics and Formal Verification, Minori, Italy, 15-17 June 2011.

[6] Y. Gurevich and S. Shelah. Fixed-point extensions of first-order logic. Annals of Pure and Applied Logic, 32:265–280, January 1986.

[7] A. Blumensath and E. Grädel: Automatic Structure. in LICS'00, 2000

[8] S. Rubin. Automata Presenting Structures: A Survey of the Finite String Case. Bulletin of Symbolic Logic, 14(2):169–209, June 2008. Publisher: Cambridge University Press.

[9] *Lectures in game theory for computer scientists*. Apt, Krzysztof R., and Erich Grädel, eds. Cambridge University press, 2011.

[10] E. Kieronski and A. Kuusisto. Uniform One-Dimensional Fragments with One Equivalence Relation, 24th EACSL Annual Conference on Computer Science Logic (CSL 2015), pp 597—615, 2015

[11] D. Figueira and L. Libkin. Synchronizing Relations on Words. 31st International Symposium on Theoretical Aspects of Computer Science (STACS 2014, pp 518—529, 2014