



UvA-DARE (Digital Academic Repository)

Epistemic modelling and protocol dynamics

Wang, Y.

Publication date
2010

[Link to publication](#)

Citation for published version (APA):

Wang, Y. (2010). *Epistemic modelling and protocol dynamics*. [Thesis, fully internal, Universiteit van Amsterdam]. Institute for Logic, Language and Computation.

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

Abstract

This dissertation presents a logical investigation of epistemic protocols, focussing on protocol-dynamics, epistemic modelling, and epistemic model checking.

In Part I, we introduce logics for specifying epistemic protocols including their goals and their dynamics. Chapter 3 departs from the existing discussions about protocols in the field of Dynamic Epistemic Logic by introducing a logic which can specify both the epistemic protocols and their goals *within the language*. We formalize the verification problem of epistemic protocols under the assumption of meta knowledge about the intended goal. The subtlety of this verification problem is discussed in theory and examples. In Chapter 4, we address the question: “How can people get to know a protocol?” For this, we develop logics which are convenient for reasoning about knowledge change and protocol change. With various protocol-changing operators we can handle the dynamics of protocols and formalize how actions acquire new meanings as a result of protocol change. We show that all the three logics we introduced can be translated back to Propositional Dynamic Logic (PDL) on standard Kripke models, thus the techniques of modelling and model checking we develop in the other parts of the dissertation can be applied to these logics.

In Part II we address the issue of epistemic modelling, in order to study model checking for the logics introduced in Part I. In Chapter 5 we propose new composition operations on static and event models with arbitrary vocabularies, aiming at a compositional method for generating initial epistemic models. We prove decomposition theorems w.r.t. our new operator and demonstrate the use of our methods by various examples. Chapter 6 reports results on counting the number of different models given a finite set of initial assumptions. Restricted to image-finite models, we show that if a modal μ -calculus formula has an infinite model modulo bisimulation then it has 2^{\aleph_0} (cardinality of the continuum) different models modulo bisimulation. On the other hand, if it does not have any infinite models modulo bisimulation then all its models can be represented in a normal form.

Part III introduces abstraction techniques that are particularly useful on making

the model checking more efficient. A 3-valued semantics for Public Announcement Logic is defined and studied in Chapter 7 to facilitate abstractions of models. We define a relation with vocabulary and agent mappings between concrete models and their abstractions, thus making it possible to also abstract the signatures of models. We then give a logical characterization of this abstraction relation thus showing it is safe to check properties on the abstract model instead of the original concrete model. Chapter 8 studies the PDL on so-called *accelerated Kripke models* where the transitions in the models are labelled by regular expressions in order to obtain informative abstractions. By making use of a technique of regular expression rewriting, we analyse the complexity of the model checking and satisfiability problems of this logic and give a complete axiomatization.

In Part IV (Chapter 9) we survey the epistemic approaches to security protocol verification. We summarize the most important techniques in the Epistemic Temporal Logic and Dynamic Epistemic Logic approaches to security protocol verification, and compare these two approaches in term of convenience. We argue that some security properties can only be faithfully formalized by temporal logic with knowledge operators, but are not expressible by standard temporal logic. However, we need to pay some cost in model checking complexity, in exchange to the expressiveness we gain.