



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.

Contents

Acknowledgments	xi
1 Introduction	1
1.1 Background	2
1.2 Overview of the Dissertation	6
1.3 Origins of the Material	8
2 Preliminaries	9
2.1 Finite Automata and Regular Expressions	9
2.2 Kripke Models and Bisimulation	10
2.3 Three Logics	13
2.3.1 Propositional Dynamic Logic	13
2.3.2 Epistemic Temporal Logic	15
2.3.3 Dynamic Epistemic Logic	15
I Logics of Epistemic Protocols	19
3 Meta-knowledge Matters	21
3.1 Introduction	21
3.2 Preliminaries	22
3.3 Announcement Protocol and Verification	24
3.4 Deterministic Protocols for $RCP_{3.3.1}$	29
3.5 Conclusion and Discussion	34
4 Logics of Knowledge and Protocol Change	37
4.1 Introduction	37
4.2 Basic Logic PDL^1	39
4.3 Public Event Logic $PDL^{1?b}$	43
4.4 Update Logic PDL^{\boxplus}	49
4.5 Conclusion and Future Work	55

II	Dynamic Epistemic Modelling	57
5	Composing Models	59
5.1	Introduction	59
5.2	Composing Static Models	61
5.2.1	Merging Composition	61
5.2.2	Expansion	65
5.2.3	Preservation	67
5.3	Decomposition	69
5.4	Composing Updates	73
5.5	Discussion and Future Work	80
6	Counting Models	83
6.1	Introduction	83
6.2	Preliminaries	85
6.3	Cardinality of the Tree Languages	88
6.4	Normal Form of the Countable Languages	95
6.5	Discussion and Future Work	98
III	Model Checking	101
7	Making Models Smaller	103
7.1	Introduction	103
7.2	Preliminaries	104
7.2.1	Kripke Modal Labelled Transition System	104
7.2.2	Three-valued Public Announcement Logic	105
7.3	Abstraction and Logical Characterization	109
7.3.1	Abstraction	109
7.3.2	Logical Characterization	110
7.4	The Muddy Children and Abstraction	114
7.5	Conclusion and Future work	117
8	Accelerating the Transitions	119
8.1	Introduction	119
8.2	Preliminaries	121
8.2.1	PDL on AKM	121
8.2.2	Regular Expression Rewriting	123
8.3	Model Checking	124
8.3.1	A Reduction to Standard PDL _Σ Model Checking	124
8.3.2	A Direct Algorithm	125
8.3.3	Complexity Analysis	128
8.4	Axiomatization	130
8.5	Satisfiability	133
8.6	Conclusion and Future Work	136

IV	Modelling Security Protocols	137
9	Epistemic Approaches to Security Protocol Verification	139
9.1	Knowledge in Security Protocols	139
9.1.1	Different Aspects of Knowledge	140
9.1.2	Tension Between Epistemic and Temporal Structure	141
9.2	Epistemic Approaches: A Brief Survey	142
9.2.1	BAN logic	142
9.2.2	Basics of Epistemic Approaches	144
9.2.3	Epistemic Temporal Approaches	146
9.2.4	Dynamic Epistemic Logic Approaches	148
9.2.5	Tools	149
9.3	Comparisons	149
9.3.1	On Equivalences	149
9.3.2	ETL vs. DEL in Modelling	151
9.4	To Know or Not, Towards a Technical Answer	155
9.4.1	On Expressivity of ETL	155
9.4.2	Model Checking ETL	157
9.5	Conclusion	158
A	Alloy Code for Russian Cards Problem (3.3.1)	159
	Bibliography	161
	Abstract	177
	Samenvatting	179
	Index	181