

Intuitionistic modal logics: efficient fragments and parameterized complexity

R. Ramanujam¹ and S.P. Suresh²

¹ The Institute of Mathematical Sciences Chennai, India. jam@imsc.res.in

² Chennai Mathematical Institute, Chennai, India. spsuresh@cmi.ac.in

A basic problem of logical inference systems is that of *derivability*: given a set of formulas X and a formula α , can α be derived from X using the inference rules? When the logical language is designed to express computational properties, the complexity of derivability assumes importance, and for most reasoning systems of even the propositional kind, the problem is hard. It is in this context that parameterized complexity offers hope for coping with hardness.

While classical propositional and modal logics are hard to reason about, finding efficient positive fragments with controlled use of negation can be one way out. Hence fragments of intuitionistic propositional modal logics have gained attention in recent times, especially with hope for applications to computer security. In systems like DKAL [5], security policies are formulated as inference rules, while access rights and permissions encoded as sets of formulas. The query, whether a principal may be granted access to an object, is a matter of derivability. Typical logical languages used have the power to express *delegation* (using modalities) and *conditional rights* (using implication).

Similarly, in reasoning about cryptographic security protocols, the verification problem of security with respect to the passive intruder has the same flavour. In Dolev-Yao theories [4], inference rules describe the process of building and deconstructing encrypted terms, and facts about which secrets (nonces) and keys a principal possesses are encoded as sets of formulas. The query, whether the intruder can learn an unintended secret, is again a matter of derivability. Typically the problem is in polynomial time [3, 4] but when cryptographic primitives like blind pairing (that distribute over encryption) are considered, it can be as bad as DEXPTIME-complete [2]. In general, when we extend Dolev-Yao theories to talk about properties as well as terms, the problem can be co-NP-hard. The complexity is because of the power to express *partial secrecy* (using disjunction), and holds even for a positive intuitionistic logic with a very restricted indirect atomic negation [7].

It is well-known [8] that the derivability problem for basic intuitionistic logic, even for the fragment consisting only of implication, is PSPACE-complete. This motivates the search for efficient algorithms for (fragments of) intuitionistic modal logic. Fortunately, modalities do not increase the complexity, as can be seen from the algorithm in [6] (based on the semantics of the logic) or the more direct, proof-theoretic algorithms in [1] and [7]. The main reasons for the complexity of the logic are the rules for implication introduction and disjunction

elimination (displayed below):

$$\frac{X \cup \{\alpha\} \vdash \beta}{X \vdash \alpha \rightarrow \beta} \rightarrow i \qquad \frac{X \vdash \alpha_1 \vee \alpha_2 \quad X \cup \{\alpha_1\} \vdash \beta \quad X \cup \{\alpha_2\} \vdash \beta}{X \vdash \beta} \vee e$$

Some sequents in the premises have more formulas on the left hand side than the sequents in the conclusion. This has the effect that the set of formulas derivable from X cannot be computed by fixing the context (X , in this case). One needs to solve the problem for many different contexts, and obtaining bounds on these contexts is non-trivial. This sort of behaviour also manifests in the case of rules for modalities.

We identify *context change* as a resource, and a *natural parameter* in the study of these inference systems. We explore various means by which the number of context changes may be bounded: bounding the number of disjunctions, the number of implications, the number of modalities etc. in assumptions. Some of these ideas have already been explored in [6, 7]. For instance, in [7] we show that the derivability problem becomes fixed-parameter tractable by controlling the use of disjunctions.

In this talk, we wish to expand on these ideas and present a research programme for efficient algorithms for fragments of intuitionistic modal logics, and the parametrized complexity of these logics.

References

1. A. Baskar, P. Naldurg, K.R. Raghavendra, and S.P. Suresh. Primal infon logic: derivability in polynomial time. In *Proceedings of FSTTCS 2013*, LIPIcs, vol. 24, pages 163–174, 2013.
2. A. Baskar, R. Ramanujam, and S.P. Suresh. A DEXPTIME-complete Dolev-Yao theory with distributive encryption. In *Proceedings of MFCS 2010*, LNCS 6281, pages 102–113, 2010.
3. Y. Chevalier, R. Küsters, M. Rusinowitch, and M. Turuani. An NP decision procedure for protocol insecurity with XOR. *Theoretical Computer Science*, 338(1–3):247–274, 2005.
4. H. Comon-Lundh and R. Treinen. Easy intruder deductions. In *Verification: Theory and Practice*, LNCS 2772, pages 225–242, 2003.
5. Y. Gurevich and I. Neeman. DKAL: Distributed-knowledge authorization language. In *Proceedings of CSF 2008*, pages 149–162, 2008.
6. Y. Gurevich and I. Neeman. Infon logic: the propositional case. *ACM Transactions on Computational Logic*, 12(2):9:1–9:28, 2011.
7. R. Ramanujam, V. Sundararajan, and S.P. Suresh. Extending Dolev-Yao with assertions. Technical Report, April 2014. <http://www.cmi.ac.in/~spsuresh/pdffiles/dyassert.pdf>.
8. R. Statman. Intuitionistic propositional logic is polynomial-space complete. *Theoretical Computer Science*, 9:67–72, 1979.