Fitting's Embedding of Classical Logic in S4 and Trace Properties in the Computational Model (Extended Abstract)

Gergei Bana
INRIA
Paris, France
bana@math.upenn.edu

Mitsuhiro Okada
Department of Philosophy, Keio University
Tokyo, Japan
mitsu@abelard.flet.keio.ac.jp

When Bana and Comon (BC) proposed a technique [1] to define a computationally complete symbolic attacker for the verification of trace properties of security protocols, they faced with the difficulty of interpreting first-order formulas in the computational model in a non-Tarskian manner. This was necessary in order to receive a semantics that is closest to the intuition. A single computational model $\mathcal{M}^c$ according to BC is defined by fixing a protocol and an attacker algorithm. Then, $\mathcal{M}^c$ contains all (for the various outcomes of coin tosses) computational execution traces for all possible values of the security parameter. That is, different protocols or different attackers result different models, but changing the security parameter or the outcomes of coin tosses does not change the model. BC considered first-order formulas θ, and defined their computational satisfaction $\mathcal{M}^c \overset{c}{\models} \theta$.

In a usual Tarskian semantics, $\mathcal{M} \models \theta_1 \vee \theta_2$ iff $\mathcal{M} \models \theta_1$ or $\mathcal{M} \models \theta_2$. However, this is not how BC defined their interpretation. For example, a statement such as "the key is leaked or the nonce cannot be computed by the adversary" should mean that (having fixed a protocol and an attacker algorithm) on *some part* of the computational model (i.e. for certain values of the security parameter and certain random outcomes) the key may be leaked, but on the rest of the model (where the key is not leaked) the nonce cannot be computed. This is different from the Tarskian way above. Negation is also defined differently from Tarski by BC: "cannot be computed by the adversary" means that the nonce in question cannot be computed *anywhere* on that part of the execution, which also contradicts the usual interpretation of negation (as computable means computable *everywhere* on that part). The exact definitions BC gave were even more complex, and – for technical reasons to be explained in the talk – followed the pattern that "for every non-negligible subset, there exists a further non-negligible subset, such that...". Bana and Comon proved, that although the semantics is not the usual first-order semantics, first order deduction is still sound with respect to their semantics.

As it turns out, what they proved with brute force, is actually a special case of Fitting's theorem about his embedding of (first-order) classical logic in (first-order) S4 [3] (S4 is a version of modal logic). For any first-order formula θ, Fitting defined a transformation $\theta \mapsto \theta^*$, where θ^* is a formula of first-order S4, and (for the case when the Barcan formula and its converse, $\forall x \Box \theta \leftrightarrow \Box \forall x \theta$ are assumed) is given recursively as follows:

- For any atomic formula θ, let $\theta^* \equiv \Box\Diamond\theta$;
- $(\neg\theta)^* \equiv \Box\neg\theta^*$; $(\theta_1 \to \theta_2)^* \equiv \Box(\theta_1^* \to \theta_2^*)$;
- $(\theta_1 \vee \theta_2)^* \equiv \Box\Diamond(\theta_1^* \vee \theta_2^*)$; $(\theta_1 \wedge \theta_2)^* \equiv (\theta_1^* \wedge \theta_2^*)$;
- $(\exists x\theta)^* \equiv \Box\Diamond\exists x\theta^*$; $(\forall x\theta)^* \equiv \forall x\theta^*$.

Fitting's theorem says that any formula θ is deducible in first-order logic if and only if θ^* is deducible in first-order S4 with the Barcan formulas. (Without the Barcan formulas, $(\forall x\theta)^* \equiv \Box\Diamond\forall x\theta^*$ has to be written above).

The semantics of Bana and Comon is then the composition of Fitting's embedding with a computational Kripke-semantics, in which the possible worlds are the non-negligible sets of the computational execution. More precisely, for any first-order formula θ that Bana and Comon considered, θ^* would give its Fitting embedding, which then can be given a standard Kripke semantics in the computational model: $\mathcal{M}^c \overset{s4}{\models} \theta^*$. Then $\mathcal{M}^c \overset{c}{\models} \theta$ holds if and only if $\mathcal{M}^c \overset{s4}{\models} \theta^*$ holds. Because of Fitting's theorem and as S4 deduction is sound with respect to $\overset{s4}{\models}$, first-order deduction is also sound with respect to $\overset{c}{\models}$.

In this presentation we detail how the semantics that Bana and Comon defined emerge naturally, unavoidably in the computational model, and we describe the above Fitting connection in detail.

This connection was included in [2], but it has never actually been presented at a workshop or conference.

References

[1] G. Bana and H. Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *POST'12*, LNCS, pages 189–208. Springer, 2012.

[2] G. Bana, K. Hasebe, and M. Okada. Computationally complete symbolic attacker and key exchange. In *CCS '13*, pages 1231–1246. ACM, 2013.

[3] Melvin Fitting. An embedding of classical logic in s4. *The Journal of Symbolic Logic*, 35(4):529–534, 1970.