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 in the computational model to define a computationally complete symbolic attacker for S4 (S4 is a version of modal logic). For any first-order formula $\theta$, Fitting defined a transformation $\theta \mapsto \theta^*$, where $\theta^*$ is a formula of first-order S4, and (for the case when the Barcan formula and its converse, $\forall x \square \theta \leftrightarrow \square \forall x \theta$ are assumed) is given recursively as follows:

- For any atomic formula $\theta$, let $\theta^* \equiv \square \neg \theta$;
- $(\neg \theta)^* \equiv \square \neg \theta^*$; $(\theta_1 \rightarrow \theta_2)^* \equiv \square (\theta_1^* \rightarrow \theta_2^*)$;
- $(\forall x \theta)^* \equiv \square \forall x \theta^*$; $(\forall x \theta)^* \equiv \forall x \theta^*$.

Fitting’s theorem says that any formula $\theta$ is deducible in first-order logic if and only if $\theta^*$ is deducible in first-order S4 with the Barcan formulas. (Without the Barcan formulas, $(\forall x \theta)^* \equiv \square \forall x \theta^*$ 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 $\theta$ that Bana and Comon considered, $\theta^*$ would give its Fitting embedding, which then can be given a standard Kripke semantics in the computational model: $M^c \models \theta^*$. Then $M^c \models \theta$ holds if and only if $M^c \models \theta^*$ holds. Because of Fitting’s theorem and as S4 deduction is sound with respect to $\models^4$, first-order deduction is also sound with respect to $\models$.

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

