Probabilistic Logic over Equations and Domain Restrictions

Andreia Mordido, Carlos Caleiro

SQIG – Instituto de Telecomunicações
Dep. Mathematics, IST – Universidade de Lisboa

We propose and study a probabilistic logic built on top of an equational base with domain constraints. The logic is motivated by the reasoning used in the analysis of cryptographic protocols, namely in the analysis of so-called *offline guessing attacks* [1] in a setting where the usual Dolev-Yao intruder [4] is extended with some cryptanalytic power [2]. The logic combines aspects from classical logic and equational logic with an exogenous approach to quantitative probabilistic reasoning. It is an extension of the equation-based classical logic of [6] with domain restrictions and probabilities.

We provide a sound and (weakly) complete axiomatization for the logic, parameterized by an equational specification of the algebraic basis coupled with the intended domain restrictions. We also show that the satisfiability problem for the logic is decidable, under the assumption that its algebraic basis is given by means of a convergent rewriting system and, additionally, that the axiomatization of domain restrictions enjoys a suitable subterm property. Our satisfiability proof is actually more informative, as we develop a satisfiability algorithm for our logic by means of a reduction to the satisfiability problems for classical propositional logic, namely to the well-known problem SAT [3], and to a variant of the lesser-known problem PSAT [5]. As a consequence, we get that validity in the logic is also decidable. Furthermore, under the assumption that the rewriting system that defines the equational basis underlying the logic is also subterm convergent, we show that the resulting satisfiability problem is NP-complete, and thus the validity problem is coNP-complete.

As an application, we explore meaningful examples on the analysis of cryptographic protocols and, further, on the estimation of the probability of offline guessing attacks to simple security protocols.

References

[1] M. Baudet. Deciding security of protocols against off-line guessing attacks. In *Proceedings of the 12th ACM Conf. on Computer and Communications Security*, CCS '05, pages 16–25, 2005.

[2] B. Conchinha, D. A. Basin, and C. Caleiro. Symbolic probabilistic analysis of off-line guessing. In *ESORICS*, volume 8134 of *Lecture Notes in Computer Science*, pages 363–380. Springer, 2013.

[3] S. A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, STOC '71, pages 151–158. ACM, 1971.

[4] D. Dolev and A. C. Yao. On the security of public key protocols. In *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*, SFCS '81, pages 350–357. IEEE Computer Society, 1981.

[5] M. Finger and G.D. Bona. Probabilistic satisfiability: Logic-based algorithms and phase transition. In *IJCAI*, pages 528–533. IJCAI/AAAI, 2011.

[6] A. Mordido and C. Caleiro. An equation-based classical logic. In *Logic, Language, Information, and Computation - 22nd International Workshop, WoLLIC 2015, Proceedings*, volume 9160 of *Lecture Notes in Computer Science*, pages 38–52. Springer, 2015.