Internship Master 2: Qualitative probabilistic hyperproperties and application to security

Advisors: Benjamin Monmege and Jean-Marc Talbot
prenom.nom@univ-amu.fr

Laboratoire d'Informatique et Systèmes (LIS) – Équipe MOVE

Software security has become a crucial issue. Hence, guaranteeing the absence of security vulnerabilities in applications becomes an important area of the verification process. Among other security flaws, due to incorrect software developments, applications through exchanges with other applications may reveal (partial) information intended to remain secret. A possible model of such a phenomenon is formalized in the notion of non-interference: data are classified according to their private or public nature and only the public values are observable. The correction then states that private data do not interfere with public data: observation of the processing of public data (input and output in particular) does not make possible to extract information concerning private data [6]. This property of non-interference is not a property of each of the traces of execution taken individually but of each of the pairs of traces by specifying that any pair of traces sharing the same public inputs also shares the same public outputs.

We can specify this in terms of hyperproperties (instead of properties) which express properties of sets of traces and not individual traces. An extension of CTL* called HyperCTL* [3] provides a specification formalism for hyperproperties, by adding to CTL* quantifiers on traces. Some other hyperlogics have been proposed, with a hierarchy studied in [4].

Temporal logics have been extended to model properties of probabilistic systems, like Markov chains (instead of Kripke structures). For instance, the logic PCTL [9] trades the operators A and E of CTL, to a new probabilistic operator P that follows the probability distribution over paths in the Markov chain.

Later, hyper-versions of the logic PCTL has been introduced, called HyperPCTL [1], that allows one to model probabilistic hyperproperties of Markov chains: this enables the specification of probabilistic non-interference [8], or even differential privacy [5].

Non-interference, even probabilistic, as worded is very coarse and cannot, for example, distinguish the disclosure of a plaintext password and that of a password *hashed* using a random value. However, it is obvious that knowing the clear version of a password or its hashed version does not give the same

amount of information. Therefore, non-interference has been extended with quantitative aspects to distinguish these two situations [10]. Independently, extensions of LTL logics have been consider to reason about quality [2]: instead of associating a formula with the truth value 0 (false) or 1 (true), a formula is now associated with a quality in the interval $[0, 1]$. Last year, Samuel Graepler has considered an extension of HyperLTL with such qualitative reasonings [7].

The objective of this internship is thus to study qualitative extensions of HyperPCTL, merging techniques used in the articles [1, 2]. Apart from a study of the literature, the internship will consist in the definition of a qualitative extension of HyperPCTL, and a study of the model-checking problem of this logic, which consists in checking whether a given Markov chain fulfils a formula. The goal is also to apply this model-checking algorithm to the problem of quantitative non-interference, or other security measures.

Keywords: security, non-interference, information flow, temporal logic, quantitative logic, Markov chains, differential privacy

References

[1] E. Ábrahám and B. Bonakdarpour. HyperPCTL: A temporal logic for probabilistic hyperproperties. In *International Conference on Quantitative Evaluation of Systems*, 2018.

[2] S. Almagor, U. Boker, and O. Kupferman. Formally reasoning about quality. *Journal of the ACM*, 63(3):1–56, 2016.

[3] M. R. Clarkson, B. Finkbeiner, M. Koleini, K. K. Micinski, M. N. Rabe, and C. Sánchez. Temporal logics for hyperproperties. In *POST'14*, pages 265–284, 2014.

[4] N. Coenen, B. Finkbeiner, C. Hahn, and J. Hofmann. The hierarchy of hyperlogics. In *34th Annual ACM/IEEE Symposium on Logic in Computer Science*, 2019.

[5] C. Dwork and A. Roth. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 9(3-4):211–407, 2014.

[6] J. A. Goguen and J. Meseguer. Security policies and security models. In *IEEE Symposium on Security and Privacy*, pages 11–20, 1982.

[7] S. Graepler. Quantitative hyperltl and application to security. Master's thesis, Aix-Marseille Université, 2023.

[8] J. W. Gray III. Toward a mathematical foundation for information flow security. *Journal of Computer Security*, 1(3-4):255–294, 1992.

[9] H. Hansson and B. Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6(5):512–535, 1994.

[10] G. Smith. On the foundations of quantitative information flow. In *FOSSACS'09*, pages 288–302, 2009.