Verifying the Leakage of Information in Concurrent Systems

by Kostantinos Chatzikokolakis.
Joint work with Daniel Gebler, Catuscia Palamidessi and Lili Xu.

Abstract

We consider the problem of measuring the leakage of information in probabilistic concurrent systems, focusing in particular on the quantitative information flow and differential privacy properties. We show that the bisimulation metrics based on the Kantorovich lifting, which have proved quite successful in probabilistic verification, are not suited for our needs. This is due, essentially, to the additive nature of the lifting. We then propose an extension of the Kantorovich construction, which brings to a much more general notion of bisimulation metric. We show that this new notion provides a solution to our problem, in the sense that it allows to compute a bound for the information leakage, even when there is no bound on the length of the execution.