Titel: Automated Analysis of Probabilistic Programs

Abstract:
The problem to ascertain whether a computer program is correct is fundamental in computer science. This project studies the correctness of probabilistic programs. Such programs are pivotal for cryptography, privacy and quantum programming, are typically small, but very hard to understand and analyse. It is a true challenge to automate their correctness proof. The main causes for their complexity are randomness, variables with infinite domains, and the occurrence of parameters. Parameters can range over concrete probabilities but can also encompass various aspects of the program, such as number of participants, size of certain variables etc. This project aims at pushing the limits of automating the correctness analysis of probabilistic programs. Our approach is to seek for semi-automated means for synthesizing loop invariants, integrate the analysis of rich data structures (lists and arrays), and to investigate the borders of which verification steps can be automated and which ones cannot.
(End of abstract.)