Emanuele D’Osualdo (University of Konstanz)

Bluebell: a modal logic to reason about probabilistic programs

Probabilistic programs are computer programs that, additionally to normal computation, can sample from probability distributions (and therefore induce a distribution of possible outputs). They can be used to model stochastic processes, cryptographic protocols (where distributions model key generation/uncertainty about the secrets from the perspective of the adversary), or algorithms for differential privacy (where controlled noise is injected into computation to achieve privacy goals). Our goal is to formally establish properties of the output distribution of a program. I will give an overview of Bluebell, a modal logic I recently proposed (jointly with J. Bao and A. Farzan) which harmonises and generalises proof techniques that were previously introduced in ad-hoc ways for probabilistic reasoning: independence, conditioning and relational lifting via couplings. Bluebell’s main insight is that probabilistic independence and conditioning in the form of a modality, can form the basis of a substructural modal logic able to represent many known and new high-level reasoning principles without exposing the low-level intricacies of probability spaces.

Link to Paper: https://arxiv.org/abs/2402.18708