Departamento de Matemática
Universidade de Aveiro

CIDMA | CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

Seminário do Grupo de Álgebra e Geometria

A KAT-like approach for union-bound reasoning

on probabilistic programs

Leandro Gomes

Resumo

Kleene Algebra with Tests (KAT) provides a framework for algebraic equational reasoning on imperative programs. The recent variant Guarded KAT (GKAT) allows to reason on non-probabilistic properties of probabilistic programs. Here we introduce an extension of this framework called aGKAT (approximate GKAT), a form of graded GKAT over a partially ordered monoid (real numbers) which enables to express satisfaction of (deterministic) properties except with a probability up to a certain bound. This allows to represent in equational reasoning 'à la KAT' proofs of probabilistic programs based on the union bound, a technique from basic probability theory. We show how a propositional variant of approximate Hoare Logic (aHL), a program logic for union bound, can be soundly encoded in our system aGKAT. We then illustrate the use of aGKAT on an example of accuracy analysis from the field of differential privacy.

Sala 11.1.28, 29 de novembro de 2024, 15:00

fct Fundação
para a Ciência
e a Tecnologia

REPÚBLICA
PORTUGUESA