Seminar/Talk

Towards Theory AB

Justin Hsu
University of Pennsylvania

Host:

Since the inception of computer science, rigorous mathematical proofs have played a major role in analyzing and understanding computation. Fields like algorithms, datastructures, and complexity theory---commonly known as "Theory A" or simply "Theory"---seek to understand how efficiently problems can be solved by a computer, if they can be solved at all. In contrast, disciplines like programming languages, denotational semantics, and verification---commonly known as "Theory B" or simply "Formal Methods"---explore how to represent computation, and how to reason about its correctness.

While these two broad areas share a theoretical perspective on computer science, in recent years they have diverged substantially. In this talk, I will present a confluence of ideas from the two theories. First, I will show how coupling proofs, used to analyze random walks and Markov chains, correspond to proofs in the program logic pRHL. This connection enables formal verification of novel probabilistic properties, and provides an structured understanding of proofs by coupling. Then, I will show how an approximate version of pRHL, called apRHL, points to a new, approximate version of couplings closely related to differential privacy, and a new kind of proof by approximate coupling. This proof technique enables cleaner proofs of differential privacy, both for humans and for formal verification. Finally, I will discuss some potential directions towards a possible "Theory AB", blending ideas from both worlds.

Thursday, January 26, 2017 09:45am - 10:45am
Mondi Seminar Room 2, Central Building

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station.
Please find a schedule of the ISTA Shuttle on our webpage:
https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.