POP Seminar

Linear Dependent Types for Differential Privacy

Marco Gaboardi

University of Pennsylvania

Dept. of Computer & Information Science

Abstract:

Differential privacy offers a way to answer queries about sensitive information while offering strong, provable privacy guarantees. Several tools have been developed for certifying that a given query is differentially private. In one approach, Reed and Pierce [31] proposed a functional programming language, Fuzz, for writing differentially private queries. Fuzz uses linear types to track sensitivity, as well as a probability monad to express randomized computation; it guarantees that any program that has a certain type is differentially private. Fuzz can successfully verify many useful queries. However, it fails when the analysis depends on values that are not known statically. We present DFuzz, an extension of Fuzz with a combination of linear indexed types and lightweight dependent types. This combination allows a richer sensitivity analysis that is able to analyze a larger class of queries, including queries whose sensitivity depends on runtime information. As in Fuzz, the differential privacy guarantees follows directly from the soundness theorem for the type system. We demonstrate the enhanced expressivity of DFuzz by certifying differential privacy a broad class of iterative algorithms that could not be typed previously.

Monday, October 29, 2012

Gates Hillman Center Rm# 6115

2:30 PM – 4:00 PM