Workshop on Formal Verification of Proofs and Programs

Tuesday October 6th 2015

InCo (Room to be confirmed)

14:00 **Joshua Guttman (The MITRE Corporation, Worcester Polytechnic Institute, USA)**, *A Cut Principle for Information Flow*

We view a distributed system as a graph of active locations with unidirectional channels between them, through which they pass messages. In this context, the graph structure of a system constrains the propagation of information through it. Suppose a set of channels is a cut set between an information source and a potential sink. We prove that, if there is no disclosure from the source to the cut set, then there can be no disclosure to the sink. We introduce a new formalization of partial disclosure, called blur operators, and show that the same cut property is preserved for disclosure to within a blur operator. A related compositional principle ensures limited disclosure for a class of systems that differ only beyond the cut.

14:45 **Gilles Barthe (IMDEA Software, Spain)**, *Relational verification of probabilistic programs*

In this talk, I will outline a general method for verifying probabilistic programs, and discuss applications to cryptography, privacy, and randomized algorithms.

15:30 Coffee Break

16:00 **Maximiliano Cristiá (CIFASIS-CONICET, Universidad de Rosario, Argentina)**, *Adding partial functions to constraint logic programming with sets*

Partial functions are common abstractions in formal specification notations such as Z, B and Alloy. Conversely, executable programming languages usually provide little or no support for them. In this talk I'll show how Gianfranco Rossi and me added partial functions as a primitive feature to a Constraint Logic Programming (CLP) language, namely {log}. Although partial functions could be programmed on top of {log}, providing them as first-class citizens adds valuable flexibility and generality to the form of the set-theoretic formulas that the language can safely deal with. In particular, I'll show how {log} is naturally extended in order to accommodate for the new primitive constraints dealing with partial functions.

16:45 **Álvaro Tasistro (Universidad ORT, Uruguay)**, *Alpha-Structural Induction and Recursion for the Lambda Calculus in Constructive Type Theory*

We formulate principles of induction and recursion for a variant of lambda calculus in its original syntax (i.e., with only one sort of names for both free and bound variables) where alpha-conversion is based upon name swapping as in nominal abstract syntax. The principles allow to work modulo alpha-conversion and implement the Barendregt variable convention. We derive them all from the simple structural induction principle on concrete terms and work out applications to some fundamental meta-theoretical results, such as the substitution lemma for conversion and the lemma on substitution composition. The whole work is implemented in Agda.