Equational Unification modulo Non-disjoint Union of Theories

Serdar Erbatur[*]
Department of Computer Science
University of Texas at Dallas (UT Dallas)

Abstract

Unification and its applications to verification of cryptographic protocols have been explored extensively. The main idea is that it is possible to reduce verification of protocols to solving symbolic equations between terms exchanged between Alice and Bob who follow a protocol for secure communication. This approach is further extended so that the terms are interpreted by taking into account algebraic properties of function symbols that occur in them. For instance, properties such as associativity (A) and commutativity (C) occur frequently and AC-unification is used to verify protocols that employ AC function symbols. The underlying logical formalism for this whole approach is first-order logic with equality (i.e., equational logic). In this logic, the algebraic properties possessed by the function symbols are axioms of equational theories.

In this talk, I will present an overview of recent results of our group. In particular, I will explain non-trivial modularity results when an equational theory is a non-disjoint union of other theories.

[*] e-mail: serdar.erbatur@gmail.com