Unification and Anti-unification modulo Equational Theories

Santiago Escobar[1]*

Departamento de Sistemas Informáticos y Computación,
Universitat Politècnica de València, Spain
sescobar@dsic.upv.es

Automated reasoning modulo an equational theory E is a fundamental technique in many applications. If E can be split as a disjoint union $R \cup Ax$ in such a way that R is a set of rewrite rules that are confluent, terminating, sort-decreasing, and coherent modulo a set of equational axioms Ax, it is well-known that narrowing with R modulo Ax provides a complete E-unification algorithm. However, narrowing did not receive much attention in unification theory due to being hopelessly inefficient in the case of using unrestricted narrowing (also called full narrowing). Little has been studied on effective narrowing strategies for equational unification beyond the case of *basic narrowing*, which is a sound and complete narrowing strategy effective for equational unification when there are no axioms. Indeed, there are very few studies on termination of basic narrowing. In the general modulo case, the decisive observation is that basic narrowing is incomplete modulo AC, so some narrowing strategy beyond basic narrowing must be defined.

Narrowing with rules R modulo axioms Ax can be turned into a practical automated reasoning technique by systematically exploiting the notion of R, Ax-variants of a term. A variant-based equational unification algorithm was defined and it is publicly available in the Maude programming language. A relevant point is that variant-based unification is defined by means of two narrowing strategies: *variant narrowing* and *folding variant narrowing*. Variant narrowing restricts the number of narrowing steps at a local level by taking profit of R being confluent, terminating, and coherent modulo Ax. Folding variant narrowing restricts the number of narrowing steps at a global level by taking profit of a theory $R \cup Ax$ that has the *finite variant property*, i.e., a finite number of most general variants can be computed for any term. Theories with a presentation satisfying the finite variant property are quite common in protocol specification, including cancellation of encryption and decryption, exclusive-or, Diffie-Hellmann, or abelian groups. An interesting observation is that folding variant narrowing is optimally variant-terminating, i.e., there is no other possible narrowing strategy better for computing variants.

We are also interested in equational generalization, also called anti-unification, which is the dual of unification. Given terms t and t', a generalizer is a term t'' of which t and t' are substitution instances. The dual of a most general unifier (mgu) is that of least general generalizer (lgg). As a long-term project for providing anti-unification for an equational theory $E = R \cup Ax$, we have extended the known untyped generalization algorithm to, first, an order-sorted typed setting with sorts, subsorts, and sub- type polymorphism; second, to work modulo equational theories, where function symbols can obey any combination of associativity, commutativity, and identity axioms (including the empty set of such axioms); and third, to the combination of both, which results in a modular, order-sorted equational generalization algorithm.

*This work has been partially supported by the EU (FEDER) and the Spanish MEC/MICINN under grant TIN 2010-21062-C02-02, and by Generalitat Valenciana PROMETEO2011/052.