Galculator: A program calculus based on Galois connections

Paulo Silva

February 2007

Abstract

Formal proofs about the properties of programs are necessary in order to ensure their correctness. However, these proofs are usually difficult to derive. In the traditional approach, this requires to write down a description of the problem in some kind of logic (first order, higher order, ...) and using inference rules, derive the conjectures about the program from the axioms of the system. This usually leads to proofs by induction over the structure of the problem and to some complex case analysis. With simple problems this may not be an issue, but with complex systems with large descriptions this approach does not scale.

Automatic theorem proving was developed as a solution to handle with complex proofs with computer assistance. Theorem provers are software programs that help in the process of deriving proofs from the logical description of problems. Sometimes, the proofs are automatically generated by the program; more often, the theorem prover assists a human user in the process by suggesting the applicable rules and ensuring that their application is correct. Some interesting problems have been solved with the aid of theorem provers under human guidance.

An alternative way for describing and solving problems has been made, some year ago. Instead of using logics, relations were purposed because of their properties: they have an algebraic nature, form a complete lattice, and have many Galois connections which provide many useful calculation rules and properties "for free". Moreover, relations are well-suited for modelling partiality, non-determinism, under-specification and for development by refinement. The relation calculus operators make the logic quantifiers and connectors implicit, thus offering more structure and being able to scale better. Variables are also omitted making the calculus pointfree, with a solid connection to the theory of categories and allegories.

Relation calculus leads to an algebraic style of reasoning with expressions being manipulated with algebraic rules. This usually makes the proof much

more syntatic in its nature: the symbols unfold the path. Moreover, since small steps are used when applying the algebraic rules, it is easier to follow the correctness of the proof. However, this kind of reasoning has been used in proofs with pencil-and-paper but its power has not been used in automated tools.

The *Galculator* is a tool that aims to explore and apply the power of relation calculus in the automatic deriving of proofs, using the algebraic properties of relations and Galois connections. Since relation properties are usually equational or inequational, the *Galculator* should be mostly suited to derive proofs by indirect equality and possibly by mutual inclusion. However, the tool should be generic and useful on a large sort of fields since relations are ubiquitous.