Project proposal
Master Informatique

Verified graph transformations with attributes

Keywords: Logic; Semantics of programming languages; Program verification; Decision procedures

Scientific Context

Within the Climt project[1], we are working on graph transformations, and in particular the verification of graph transformations.

Graph transformations have wide-spread applications, such as pointer-manipulating programs and model transformations in languages such as UML. They are also interesting for graph databases, such as those represented with RDF schemas, and the link structure of the World-Wide Web.

We are currently developing an imperative language for graph transformations, and a family of Hoare-style logics for reasoning about programs of this language. The logics are variants of Description Logics. A distinctive feature of our work is that both the programming language and the logic have been formalized in the proof assistant Isabelle[2].

Planned work

The graph transformations we have considered so far only take into account structural aspects of graphs ("node a of class A is connected to at most two nodes of class B"), but not attributes, *i.e.* numeric values, strings and the like ("for all nodes a of class A linked with a node b of class B, the attribute value $a.v$ has to be less than $b.v$"). Our graph transformation language and its associated program logic have been designed to yield decidable proof problems (with an effective proof procedure). What happens when adding numeric attributes?

The work will consist of a *conceptual phase*, in which we iterate the following points until obtaining a good compromise between expressivity and tractability:

- Enhancement of the existing graph transformation language with numeric attributes.
- Study of the impact on decision procedures for the resulting proof calculus.
- Study of availability of solvers (SMT; arithmetic decision procedures).

This phase will be followed by an *implementation phase*:

- implementation of the extension of the graph transformation language;

[1] www.irit.fr/~Martin.Strecker/CLIMT/
[2] http://isabelle.informatik.tu-muenchen.de/

- extraction of proof obligations;
- combination with selected external solvers;
- possibly: integration in the formal Isabelle development.

Prerequisites and interests

From the participating students, we expect

- interest in formal semantics of programming languages, logics, methods of correctness proofs for imperative programs (*required*)
- experience with functional (Ocaml, Haskell) or OO-functional (Scala) languages (*required*)
- experience with specialized arithmetic decision procedures and combination of decision procedures (*desirable*)
- experience with interactive proof assistants (such as Coq, Isabelle, PVS) (*would be a plus*)

Administrative Context

Interested? Then please contact us for further inquiries and for applying for the project. The internship can be carried out at either of the sites of the Climt project:

- LIG (Grenoble), contact Rachid Echahed[3]
- IRIT (Toulouse), contact Martin Strecker[4]

Funding will be provided for the duration of the project. The project is an ideal starting point for a PhD thesis.

[3] http://membres-lig.imag.fr/echahed/
[4] http://www.irit.fr/~Martin.Strecker/