ProMoVer: A Tool for Modular Verification of Temporal Safety Properties

Siavash Soleimanifard
Royal Institute of Technology, KTH
Stockholm, Sweden
siavashs@csc.kth.se

I will talk about ProMoVer, a tool for fully automated procedure-modular verification of Java programs equipped with method-local and global assertions that specify safety properties of sequences of method invocations. Modularity at the procedure-level is a natural instantiation of the modular verification paradigm, where correctness of global properties is relativized on the local properties of the methods rather than on their implementations. In our approach, the relativization is accomplished by the construction of maximal models for a program model that abstracts away from program data, where a maximal model is a model that represents all models satisfying a specification; maximal models of methods are constructed form the provided specifications by assertions, then composed and model checked against the global control flow safety property. This approach allows global properties to be verified in the presence of different forms of variability, e.g., code evolution, multiple method implementations (as arising from software product lines), or even unknown method implementations (as in mobile code for open platforms). ProMoVer automates a typical verification scenario for a previously developed tool set for compositional verification of control flow safety properties, and provides appropriate pre- and post-processing. Modularity is exploited by a mechanism for proof reuse that detects and minimizes the verification tasks resulting from changes in the code and the specifications. The verification task is light-weight due to support for abstraction from private methods and automatic extraction of candidate specifications from method implementations.

In this talk, I will first introduce ProMoVer and then I will show how it can be used for the different variability forms both from theoretical and practical aspects.