Karlsruher Institut für Technologie

Institut für Theoretische Informatik (ITI)
Anwendungsorientierte Formale Verifikation
**Prof. Dr. Bernhard Beckert**

# Bachelor's Thesis

## Using SDGs to Generate Frame Conditions

**The Frame Problem.** An important aspect of formal verification (as done for e.g. by the KeY tool) is modularity. Each method is verified in isolation, and any method call inside a body is abstracted by its method specification. To achieve this, it is not enough to specify what a method does; it is also required to specify what a method does *not* do. This is known as the *frame problem*. Basically, for modular verification one needs to know what is the *frame* of a method, i.e., what are the variables that may be changed at most by the method, and what is the *antiframe*, i.e., which variables must not be changed by the method.

**System Dependence Graphs.** System dependence graphs (SDGs) are directed graphs that represent dependencies between parts of a program. Nodes in the SDG represent program statements, conditions, or input parameters, and edges represent dependencies between the nodes; i.e., an edge between nodes exists if the execution of one node may depend on the outcome of the other node. There are roughly two types of edges in an SDG: data dependence edges, representing possible direct dependencies and control dependencies which represent possible indirect dependencies. The dependencies represented by the SDG are, however, over-approximations of the actual dependencies in the program. The *JOANA* tool, developed at the group of Prof. Snelting is based on an SDG analysis approach.

**Task.** The idea is to use the SDGs provided by the JOANA tool to generate (over-approximated) frame conditions that can then be used by KeY. The main tasks for this thesis are:

- Implementation of an approach for frame condition generation based on SDGs
- Evaluation of this implementation with respect to the precision of the generated frame conditions. Examples from the KeY example collection can be used for this purpose.

**Your profile.** You are a serious and competent student. Programing in Java poses no challenge to you. You are interested in formal methods and, ideally, have already some knowledge about formal verification with the KeY system (e.g. from the *Formale Systeme* lecture).

**Kontakt**
Mihai Herda herda@kit.edu 50.34 R227