Ghostbusting JML with CATs (automatically)

Master Thesis Proposal

TECHNISCHE
UNIVERSITÄT
DARMSTADT

Software Engineering Group

Context

Context-aware trace contracts (CATs) [1] are a program logic for specifying global behaviors of asynchronous programs, and are based on the trace logic introduced in [2]. A trace formulas describes what happens during the execution of a program by specifying the occurrence of events and the assertions about the program state. A CAT specifies the internal behavior and the context of execution of procedures. It consists of three trace formulas that describe (i) what must have happened before the procedure's execution (ii) the procedure's internal behavior, and (iii) what the procedure expects to happen after its termination. CATs are shown to be a highly expressive specification language that can describe complex behaviors, such as system/temporal properties, intuitively and independently of an underlying programming language [3]. For these reasons, in [4], the authors candidate CATs as a lingua franca for behavioral specification. They demonstrate how target language-specific formalisms, such as the Java Modeling Language (JML), can be desugared into CATs, resulting in intuitive, comparable specifications, that are independent of the target code.

A crucial part of the desugaring process is the *ghostbusting*, i.e. the desugaring of *ghost code*. Ghost code is a specification pattern consisting in introducing (non interfering) data and computation to the original program. Ghost code is essential when specifying complex properties in language-specific formalisms, such as JML, but it usually results in awkward specification, not easy to understand, maintain or reuse.

Thesis

The goal of the thesis is to provide an automatic mechanism to desugar JML to CATs.

This involves identifying a meaningful subset of JML that is possible to desugar to CATs automatically, with a focus on complex properties such as system and temporal properties. The final goal is to developing a correct and automatic desugaring mechanism, with a focus on how *ghostbusting* can be achieved.

Approximate Work Distribution

Analysis	■■■■□
Programming	■■■■■
Literature	■■□□□

Contact

M.Sc. Marco Scaletta
Software Engineering Group
`scaletta@cs.tu-darmstadt.de`

References

[1] R. Hähnle, E. Kamburjan, and M. Scaletta, "Context-aware trace contracts," in *Active Object Languages: Current Research Trends*, 2024.

[2] R. Bubel, D. Gurov, R. Hähnle, and M. Scaletta, "Trace-based deductive verification," LPAR 2023.

[3] R. Hähnle, M. Scaletta, and E. Kamburjan, "Herding cats," SEFM 2023.

[4] M. Scaletta and R. Hähnle, "Context-aware contracts as a lingua franca for behavioral specification," ISOLA 2024.