Institute of Information Security and Dependability (KASTEL)
Application-oriented Formal Verification
Prof. Dr. Bernhard Beckert
https://formal.kastel.kit.edu

Bachelor Thesis, Master Thesis
Semantic Dependency Between Models and Analysis

Motivation

Model-driven development involves multiple artefacts that evolve continuously over time. Whenever a model changes, engineers often rerun all analyses, especially for safety-critical systems, even though many of them are unaffected. This leads to significant inefficiency. There is currently no formal and systematic way to explicitly capture the *semantic dependencies* between model changes and analyses.

Example

Online Ordering Service Code

```
class OrderService {
  Response placeOrder(Item item, UserToken token){
    if (!Auth.check(token)) {
      return Response.error("Unauthorized");
    }
    if (!Inventory.available(item)) {
      return Response.error("Out␣of␣stock");
    }
    Database.save(item, token.userId);
    return Response.ok();
  }
}
```

Tests / Analyses

```
// Correctness test
test_placeOrder_success(){
  // expects successful order
}

// Security test
test_placeOrder_unauthorized(){
  // rejects invalid token
}

// Performance test
test_placeOrder_latency(){
  // checks response time
}
```

Impact of Changes on Service Code

- Change comments → no tests rerun
- Change authentication → security tests
- Change database → performance + correctness tests

How can we automatically or semi-automatically synthesise these semantic dependencies, possibly with human-in-the-loop support? Even approximate solutions can significantly reduce effort while improving the soundness and completeness of reanalysis decisions.

Depending on the level (Bachelor's/Master's), the thesis may explore several research directions. Talk with me.

Contact
Dr. Tianhai Liu
tianhai.liu@kit.edu | Office: 50.34 R227