Karlsruher Institut für Technologie

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

Bachelor-/Masterarbeit

Abhängige Eigenschaftstypen in Java

Hintergrund.
Eigenschaftstypen in Java sind ein an unserem Lehrstuhl entwickelter Ansatz zur Spezifikation von Java-Programmen. Ein Eigenschaftstyp besteht aus einem Java-Typ und einer Annotation, die mit einer booleschen Eigenschaft versehen ist. In dem Beispiel rechts hat die Annotation `Interval` die Eigenschaft `min <= subject && subject <= max`.

```
@Interval(min=1, max=3) int f;
public void foo() {
    f = 3; // OK
    f = 4; // Error!
}
```

Wir haben einen Typprüfer entwickelt, der für (fast) beliebige Eigenschaftstypen überprüft, ob jede Variable in einem gegebenen Programm immer ihre Eigenschaft erfüllt. Die Teile des Programms, deren Korrektheit der Typprüfer nicht beweisen kann, übersetzt er nach JML (*Java Modeling Language*) und übergibt sie an KeY, ein am KIT mitentwickeltes Verifikationswerkzeug für Java.

Aufgabe. *Abhängige Typen* sind Typen, die von Variablen im Programm abhängen dürfen. Eine Funktion mit dem Rückgabetyp `@Interval(min="1",max="arg") int`, der vom Argument `arg` abhängt, darf z.B. nur Zahlen zwischen 1 und dem Wert von `arg` zurückgeben. Ihre Aufgabe ist es, die Theorie der Eigenschaftstypen um abhängige Typen zu erweiten, und diese Erweiterung sowohl in dem Typprüfer als auch in der oben erwähnten JML-Übersetzung zu implementieren.

Vorraussetzungen. Sie sind erfahren in der Programmierung mit Java und haben Grundkenntnisse in Logik und formaler Verifikation, wie sie z.B. in der Vorlesung *Formale Systeme* vermittelt werden. Kenntnisse über Typtheorie und abhängige Typen sind hilfreich aber nicht erforderlich.

Kontakt
Florian Lanzinger lanzinger@kit.edu Büro 50.34R203