

AUFGABE 3: WP-KALKÜL – FRAMA-C

In dieser Aufgabe werden Sie die Korrektheit zweier Programme mit Hilfe von Frama-C und des WP-Kalküls nachweisen. Ab dieser Aufgabe steht Ihnen die Möglichkeit, direkt in den master-Zweig Ihres Gerrit-Repositories einzuchecken nicht mehr zur Verfügung. Stattdessen sollen Sie, wie in der Tafelübung beschrieben das Gerrit-Review-System verwenden. Ihr Änderungen gelangen nun erst nachdem sie von uns genehmigt worden sind in den master-Zweig.

Aufgabenstellung

a. Annotieren Sie die Schnittstelle Ihres Ampel-Programms aus Aufgabe 1 mit je mindestens einer `assigns`-, `ensures`- und `requires`-Aussage. *Fassen Sie diese Aussagen so streng wie möglich.* Sofern sinnvoll, benutzen Sie wiederverwendbare Prädikate. Weisen Sie die Korrektheit der Implementierung mit Hilfe des Jessie- bzw. des WP-Plugins von Frama-C nach.

b. Bestimmen Sie den Vertrag, die Schleifeninvarianten und die Schleifenvariante der Funktion `lower_bound()` und weisen Sie die Korrektheit der Implementierung in Frama-C nach. Die Implementierung und die Annotationsrumpfe finden Sie in der aktuellen Vorgabe.

```
1 unsigned int lower_bound(const int *a,
2                           unsigned int n,
3                           int val) {
4     unsigned int left = 0;
5     unsigned int right = n;
6     unsigned int middle = 0;
7
8     while (left < right) {
9         middle = left + (right - left) / 2;
10        if (a[middle] < val) {
11            /*@ assert \forall integer i; 0 <= i < middle + 1
12                           ==> a[i] < val;
13            */
14            left = middle + 1;
15        } else {
16            right = middle;
17        }
}
```

```
18 }  
19     return left;  
20 }  
21 }
```

Hinweise

- Erforderliche Dateien: keine Einschränkungen.
- Bearbeitung: Gruppe mit je zwei bis drei Teilnehmern.
- Abgabezeit: 13.06.2012
- Fragen bitte an i4ezs@lists.informatik.uni-erlangen.de