Universität Bremen

Korrekte Software: Grundlagen und Methoden SoSe 2021

Serge Autexier
Christoph Lüth

5. Übungsblatt

Ausgabe: 27.05.21
Abgabe: 01.06.21 10:00

Dieses Übungsblatt ist ein PDF-Formular. Bitte in einem PDF-Viewer Ihrer Wahl ausfüllen, abspeichern und in Ihrem Gitlab-Abgabe-Repository committen. Alternativ können Sie die Lösungen in der Markdown-Datei `uebung-XX.md` eintragen und diese committen.

Gruppe:

Name: Matrikelnummer:
Name: Matrikelnummer:
Name: Matrikelnummer:

5.1 *Binärprodukte*

Im letzten Übungsblatt haben Sie ein Programm zur Multiplikation zweier Zahlen durch wiederholte Addition verifiziert. Ihr Kollege sagt, folgendes Program sei wesentlich effizienter:[1]

```
/* Binary multiplication of n and m */
// {M = m ∧ N = n ∧ n > 0}
x= 0;
while (n != 0) {
  x= x+m*(n % 2);
  m= 2* m;
  n= n/2;
  }
// (POST)
```

Als ad-hoc-Erweiterung unserer Sprache benutzt das Programm den Modulo-Operator (%) in C, der den Rest bei der Division berechnet. Die mathematische Notation dafür ist x mod y.

(i) Geben Sie die Nachbedingung an.

POST =

[1] Richtig schnell wird dieses Programm, wenn wir den Modulo-Operator und die Multiplikation und Division mit 2 durch entsprechende Operationen auf Bitebene (in C &, >>, <<) ersetzen, aber semantisch passiert da nichts, deshalb ist dieses Programm hier effizient genug.

(ii) Finden Sie eine Invariante, und beweisen Sie die Korrektheit des Programmes.

Hinweise:

- Denkt daran, dass / die *ganzzahlige Division* (geschrieben $\div$) berechnet. Es ist im Allgemeinen *nicht* das Inverse zur Multiplikation (d.h. es gilt *nicht*, dass $a = b \cdot (a \div b)$). Aber es gilt:

$$a = b \cdot (a \div b) + a \bmod b \tag{1}$$

  und in diesem Fall spezialisiert mit $b = 2$:

$$a = 2 \cdot (a \div 2) + a \bmod 2 \tag{2}$$

- Die Invariante ist nicht ganz einfach. Um eine Idee zu bekommen, schreibt euch für verschiedene konkrete Belegungen von n und m deren Werte während der Berechnung der Schleife jeweils am Anfang und am Ende auf. Wer trotzdem keine findet, kann die Veranstalter um Hilfe fragen.