Institut für Informatik
der Universität München
Prof. M. Hofmann
A. Abel

WS 2005/2006

22. Dezember 2005

Übungen zur Vorlesung
Rechnergestütztes Beweisen

Blatt 10

Aufgabe 26: [PVS] Definieren Sie eine PVS Funktion, die einen Bitvektor der Länge I mit einem der Länge J multipliziert und das Ergebnis als Bitvektor der Länge I+J zurückgibt. Dazu benötigen Sie folgende Hilfsfunktionen: den Ripple-Addierer aus der Vorlesung, Multiplikation mit 2 (Linksverschiebung), Division durch 2 (Rechtsverschiebung), Erweiterung eines Vektors um führende Nullen. Stellen Sie Lemmata über diese Hilfsfunktionen auf (mit Hilfe von `bv2nat`) und verfizieren Sie diese. Charakterisieren Sie auch `bv2nat` durch Gleichungen unabhängig von `bv2nat_rec`.

Stellen Sie ein Korrektheitstheorem für den Multiplizierer auf. Testen Sie konkrete Instanzen Theorems (z. B. $7 \times 11 = 77$) mit `grind`.

Beweisen Sie die Korrektheit. Dabei dürfen Sie auch einige Lemmata unbewiesen lassen (insofern die Korrektheit nicht eine triviale Folgerung eines solchen Lemmas ist).

Aufgabe 27: [PVS] Aufbauend auf die Vorlesung am 22. Dezember 2005: Das Korrektheitstheorem fuer den Pipelined Prozessor macht nur eine Aussage fuer den Fall, dass `stall` nicht gesetzt ist. Formulieren Sie auch eine Korrektheitsaussage fuer den Fall, dass `stall` gesetzt ist und versuchen Sie sie zu beweisen.

Zu den Aufgaben befindet sich Material auf der Homepage!

Abgabe: bis **Dienstag, 10.01.2006, 18.00 Uhr** per Mail an `abel@informatik.uni-muenchen.de`.