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

WS 2005/2006

17. November 2005

Übungen zur Vorlesung
Rechnergestütztes Beweisen

Blatt 5

Aufgabe 14: [Papier, 6 Punkte] Zur Erinnerung: Ein Ring (mit Einselement) ist eine Menge R mit zwei Operationen $+$ und $*$ und zwei Konstanten $0, 1$, derart dass gilt:

- $R, +, 0$ ist eine Gruppe, und $R, *, 1$ ist ein Monoid.
- $+$ ist kommutativ.
- $*$ ist distributiv über $+$.

Beweisen Sie, dass in Ringen die Gesetze (1) $0 * x = x * 0 = 0$, (2) $-(-x) = x$, und (3) $(-x) * y = x * (-y) = -(x * y)$ gelten.

Ein Ring R heisst Boolesch, falls für alle $x \in R$ gilt $x^2 = x$. (Ein Beispiel ist der Restklassenring $\mathbb{Z}/2\mathbb{Z}$ der ganzen Zahlen modulo 2.)

Beweisen Sie, dass in Booleschen Ringen außerdem (4) $-x = x$ und (5) $x * y = y * x$ gelten, d.h., der Ring ist kommutativ.

Hinweis zu (5): Betrachten Sie $(x + y)^2$.

Aufgabe 15: [PVS, 14 Punkte]

Axiomatisieren Sie den Begriff eines Ringes in PVS und beweisen Sie obige Aussagen (1)–(5) in PVS.

Hinweis: Mit (`replace-name` *name subterm*) kann Subterme durch neue Namen ersetzen lassen. Damit kann man Terme verstecken, die von `rewrite-lemma` nicht berührt werden sollen. Näheres zu den Kommandos im PVS Prover Guide.

Abgabe: bis **Dienstag, 22.11., 18.00 Uhr** im Sekretariat (**Z1.05**) oder bei Andreas Abel im Büro (**D1.09**). Elektronische Lösungsteile per Mail an `abel@informatik.uni-muenchen.de`.