Lutz Schröder und Till Mossakowski

Spezifikation und Verifikation von Java-Programmen
Übungsblatt 1

Beweise die folgenden partiellen Korrektheitsaussagen:

a)

$$\{i = Y \wedge X = 1\} \text{ while } \neg(Y = 0) \text{ do } Y := Y - 1; X := 2 \times X \; \{X = 2^i\};$$

b)

$$\{X = m \wedge Y = n \wedge Z = 1\} \; \mathit{fastexp} \; \{Z = m^n\};$$

c)

$$\{N = n \wedge M = m \wedge 1 \leq n \wedge 1 \leq m\} \; \mathit{euclid} \; \{M = \mathrm{gcd}(n, m)\}.$$

Hierbei ist *fastexp* das Programm

$$\begin{array}{l}
\text{while } \neg(Y = 0) \text{ do} \\
\{\text{while } \mathit{even}(Y) \text{ do } \{X := X \times X; Y := Y/2\}; \\
Z := Z \times X; Y := Y - 1 \\
\}
\end{array}$$

($Y/2$ ist die größte ganze Zahl k mit $2 * k \leq Y$), und *euclid* ist das Programm

$$\begin{array}{l}
\text{while } \neg(M = N) \text{ do } \{ \\
\quad \text{if } M \leq N \\
\quad \text{then } N := N - M \\
\quad \text{else } M := M - N \\
\quad \}.
\end{array}$$

Hinweis: verwende in der Invarianten für *fastexp* die Formel $Z * X^Y = m^n$.