Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2018-03-01
Due: 2018-03-08

SADS 2018 Problem Sheet #2

Problem 2.1: *partial correctness of the gcd algorithm* (4 points)

Prove step-by-step the partial correctness of the following program using Hoare Logic. The program calculates the greatest common divisor (gcd). You can assume $\vdash gcd(a, 0) = a$ and $\vdash gcd(a, b) = gcd(b, a)$.

Precondition: $\{X = x \wedge Y = y \wedge x > 0 \wedge y > 0\}$

while $Y \neq 0$ **do**
  $Z := X \,\%\, Y$
  $X := Y$
  $Y := Z$
od

Postcondition: $\{X = gcd(x, y)\}$

Problem 2.2: *total correctness of the gcd algorithm* (1+4+1 = 6 points)

Prove the total corretness of the following program by annotating the program and deriving the verification conditions (prove goals). The program calculates the greatest common divisor (gcd). You can assume $\vdash gcd(a, 0) = a$ and $\vdash gcd(a, b) = gcd(b, a)$.

Precondition: $\{X = x \wedge Y = y \wedge x > 0 \wedge y > 0\}$

while $Y \neq 0$ **do**
  $Z := X \,\%\, Y$
  $X := Y$
  $Y := Z$
od

Postcondition: $\{X = gcd(x, y)\}$

---

a) Provide the annotated program.

b) Derive the verification conditions.

c) Prove the verification conditions.