Secure and Dependable Systems
Jacobs University Bremen
Zihan Qi

Course: CO21-320203
March 8th, 2018

Homework 2

Problem 2.1 *partial correctness of the gcd algorithm*

Solution:
$\{X = x \wedge Y = y \wedge x > 0 \wedge y > 0\}$
$WHILE\ Y \neq 0\ DO\ Z := X \,\%\, Y; X := Y; Y := Z;\ OD$
$\{X = gcd(x, y)\}$

Find a loop variant P such that:
- $\{P \wedge Y \neq 0\}\ Z := X \,\%\, Y; X := Y; Y := Z\ \{P\}$ (While rule)
- $X = x \wedge Y = y \wedge x > 0 \wedge y > 0 \to P$ (Precondition strengthening)
- $P \wedge \neg(Y \neq 0) \to X = gcd(x, y)$ (Postcondition weakening)

A loop variant $gcd(X, Y) = gcd(x, y)$ is valid since:
- $gcd(X, Y) = gcd(x, y) \wedge Y \neq 0 \to gcd(Y, X \,\%\, Y) = gcd(x, y)$ (Euclid's algorithm)
- $\{gcd(Y, X \,\%\, Y) = gcd(x, y)\}\ Z := X \,\%\, Y\ \{gcd(Y, Z) = gcd(x, y)\}$ (Assignment axiom)
- $\{gcd(Y, Z) = gcd(x, y)\}\ X := Y\ \{gcd(X, Z) = gcd(x, y)\}$ (Assignment axiom)
- $\{gcd(X, Z) = gcd(x, y)\}\ Y := Z\ \{gcd(X, Y) = gcd(x, y)\}$ (Assignment axiom)

Then we have $\{gcd(X, Y) = gcd(x, y)\}\ Z := X \,\%\, Y; X := Y; Y := Z\ \{gcd(X, Y) = gcd(x, y)\}$

As well,
- $X = x \wedge Y = y \wedge x > 0 \wedge y > 0 \to gcd(X, Y) = gcd(x, y)$, which is trivial.
- $gcd(X, Y) = gcd(x, y) \wedge \neg(Y \neq 0) \to gcd(X, Y) = gcd(x, y) \wedge Y = 0$

since we assume $\vdash gcd(a, 0) = a$
Then, $gcd(X, Y) = gcd(x, y) \wedge \neg(Y \neq 0) \to X = gcd(x, y)$

Since the loop variant hold before and after the loop terminates, partial correctness of gcd algorithm is proved.

Problem 2.2 *total correctness of the gcd algorithm*

Solution:
Precondition:$\{X = x \wedge Y = y \wedge x > 0 \wedge y > 0\}$
$\{X = x \wedge Y = y \wedge x > 0 \wedge y > 0\}$
WHILE $Y \neq 0$ **DO**
$gcd(X, Y) = gcd(x, y)$
$[Y]$
$Z := X \,\%\, Y$
$X := Y$
$Y := Z$
OD
Postcondition:$\{X = gcd(x, y)\}$
(Annotations are marked with blue color)

$(X = x \wedge Y = y \wedge x > 0 \wedge y > 0) \to (X = x \wedge Y = y \wedge x > 0 \wedge y > 0)$, since we dont have initial statements.
While loop rule gives:
$(X = x \wedge Y = y \wedge x > 0 \wedge y > 0) \to (gcd(X, Y) = gcd(x, y))$
$(gcd(X, Y) = gcd(x, y) \wedge \neg(Y \neq 0)) \to (X = gcd(x, y))$
$(gcd(X, Y) = gcd(x, y) \wedge Y \neq 0) \to Y \geq 0$

Then the Verification Conditions are generated as follows:
$\{gcd(X, Y) = gcd(x, y) \wedge Y \neq 0 \wedge Y = n\}\ Z := X \,\%\, Y; X := Y; Y := Z\ \{gcd(X, Y) = gcd(x, y) \wedge Y < n\}$
$\{gcd(X, Y) = gcd(x, y) \wedge Y \neq 0 \wedge Y = n\}\ Z := X \,\%\, Y; X := Y\ \{gcd(X, Z) = gcd(x, y) \wedge Z < n\}$
$\{gcd(X, Y) = gcd(x, y) \wedge Y \neq 0 \wedge Y = n\}\ Z := X \,\%\, Y\ \{gcd(Y, Z) = gcd(x, y) \wedge Z < n\}$
$(gcd(X, Y) = gcd(x, y) \wedge Y \neq 0 \wedge Y = n) \to (gcd(Y, X \,\%\, Y) = gcd(x, y) \wedge X \,\%\, Y < n)$

Since $Y \neq 0 \wedge Y = y \wedge y > 0$, then $Y > 0$, and VC is true hence the algorithm terminates. Therefore, total correctness of gcd is proved.