Assignment 10
Semantics, WS 2009/10

Prof. Dr. Gert Smolka, Dr. Jan Schwinghammer, Christian Doczkal
www.ps.uni-sb.de/courses/sem-ws09/

Hand in by 11.59am, Tuesday, January 19

Send your solutions to Exercise 10.2 in a file named `lastname.v` to `doczkal@ps.uni-sb.de`. Make sure that the entire file compiles without errors. You can find a template file on the course webpage.

Recommended reading: Chapter 5 of the lecture notes.

Exercise 10.1 (Hoare logic)

a) Make sure that you can state the evaluation rules and Hoare rules for IMP.

b) Show that the following variant of the rule for assignment is *not* correct:

$$\frac{}{\{p\}\,X := a\,\{\lambda\sigma.\,p(\sigma[X := [\![a]\!]\sigma])\}}$$

Exercise 10.2 (Hoare logic in Coq)

a) State and prove the conjunction rule in Coq.

$$\frac{\{p\}\,c\,\{q\} \qquad \{p'\}\,c\,\{q'\}}{\{\lambda\sigma.\,p\,\sigma \wedge p'\,\sigma\}\,c\,\{\lambda\sigma.\,q\,\sigma \wedge q'\,\sigma\}}$$

b) State and prove the disjunction rule in Coq.

$$\frac{\{p\}\,c\,\{q\} \qquad \{p'\}\,c\,\{q'\}}{\{\lambda\sigma.\,p\,\sigma \vee p'\,\sigma\}\,c\,\{\lambda\sigma.\,q\,\sigma \vee q'\,\sigma\}}$$

Exercise 10.3 (Product) Consider the following annotated IMP program *mult* that multiplies X and Y by iterated addition:

$\{\lambda\sigma.\ \sigma\,X = x \ \wedge\ \sigma\,Y = y\}$
```
P := 0;
N := 1;
```
$\{Inv\}$
```
while (N<=X) do
  P := P+Y; N := N+1
```
$\{\lambda\sigma.\sigma\,P = x{\cdot}y\}$

Give a suitable loop invariant *Inv*, and use the Hoare rules to prove the triple

$$\{\lambda\sigma.\ \sigma\,X = x \wedge \sigma\,Y = y\}\mathit{mult}\{\lambda\sigma.\sigma\,P = x{\cdot}y\}$$

for any $x, y \in \mathbb{N}$.

Exercise 10.4 (Factorial) Consider the following annotated IMP program *fact* that computes the factorial of X:

$\{\lambda\sigma.\ \sigma\, X = n \wedge \sigma\, Y = 1\}$
$\{Inv\}$
```
while (X>0) do
  Y := X*Y;
  X := X-1
```
$\{\lambda\sigma.\sigma\, Y = n!\}$

Give a suitable loop invariant *Inv*, and use the Hoare rules to prove the triple

$$\{\lambda\sigma.\ \sigma\, X = n \wedge \sigma\, Y = 1\}\mathit{fact}\{\lambda\sigma.\sigma\, Y = n!\}$$

for any $n \in \mathbb{N}$.

Exercise 10.5 (Euclid) Consider the following annotated IMP program *euclid* that computes the greatest common divisor (*gcd*) of N and M:

$\{\lambda\sigma.\ \sigma\, M = m \ \wedge\ \sigma\, N = n\}$
$\{Inv\}$
```
while not(M=N) do
  if (M<=N)
    then N := N-M
  else M := M-N
```
$\{\lambda\sigma.\sigma\, M = gcd(n, m)\}$

Give a suitable loop invariant *Inv*, and use the Hoare rules to prove the triple

$$\{\lambda\sigma.\ \sigma\, M = m \wedge \sigma\, N = n\}\ \mathit{euclid}\ \{\lambda\sigma.\sigma\, M = gcd(n, m)\}$$

for all $n, m \in \mathbb{N}$ with $n > 0$ and $m > 0$.

You may use the following facts for positive numbers n and m:

- $gcd(n, m) = gcd(m, n)$,
- $gcd(n, m) = gcd(n - m, m)$ if $n > m$,
- $gcd(n, n) = n$.