CISC 5835—Algorithms for Data Analytics
Fall, 2019

Chapter 1 Addendum (Hoare Axiomatics) Homework

Here's an iterative version of the peasant multiplication algorithm:

$$
\begin{array}{l}
\{x_0 \geq 0\} \\
x \leftarrow x_0 \\
y \leftarrow y_0 \\
z \leftarrow 0 \\
\{P\} \\
\textbf{while } (x > 0) \textbf{ do} \\
\quad \{P \wedge (x > 0)\} \\
\quad \textbf{if } \mathrm{odd}(x) \textbf{ then } z \leftarrow z + y \\
\quad x \leftarrow \lfloor x/2 \rfloor \\
\quad y \leftarrow 2 * y \\
\{z = x_0 \cdot y_0\}
\end{array}
$$

(All variables are integers.) Here P is defined to be

$$P \iff (z + x \cdot y = x_0 \cdot y_0) \wedge (x \geq 0)$$

The goal of this homework set is to develop a correctness proof for this algorithm, the main job being to show that the algorithm is correctly annotated.

We'll break this into parts.

1. [5 points] Show that

$$\{x_0 \geq 0\}\ x \leftarrow x_0;\ y \leftarrow y_0;\ z \leftarrow 0\ \{P\}$$

2. [5 points] Show that

$$
\begin{array}{l}
\{(z + \lfloor x/2 \rfloor \cdot 2y = x_0 \cdot y_0) \wedge x > 0\} \\
x \leftarrow \lfloor x/2 \rfloor \\
y \leftarrow 2 * y \\
\{P\}
\end{array}
$$

3. [5 points] Show that

$$
\begin{array}{l}
\{P \wedge (x > 0)\} \\
\textbf{if } \mathrm{odd}(x) \textbf{ then } z \leftarrow z + y \\
\{(z + \lfloor x/2 \rfloor \cdot 2y = x_0 \cdot y_0) \wedge x > 0\}
\end{array}
$$

Hint: Note that

$$\lfloor x/2 \rfloor = \begin{cases} x/2 & \text{if } x \text{ is even,} \\ (x-1)/2 & \text{if } x \text{ is odd.} \end{cases}$$

4. [5 points] Show that

$$
\begin{array}{l}
\{P \wedge (x > 0)\} \\
\textbf{if } \mathrm{odd}(x) \textbf{ then } z \leftarrow z + y \\
\{(z + \lfloor x/2 \rfloor \cdot 2y = x_0 \cdot y_0) \wedge x > 0\} \\
x \leftarrow \lfloor x/2 \rfloor \\
y \leftarrow 2 * y \\
\{P\}
\end{array}
$$

Hint: This is a "one-liner"; don't over-complicate it! There's a reason I'm giving the subproblems in this particular order!

5. [5 points] Show that

$$
\begin{array}{l}
\{P\} \\
\textbf{while } (x > 0) \textbf{ do} \\
\quad \textbf{if } \mathrm{odd}(x) \textbf{ then } z \leftarrow z + y \\
\quad x \leftarrow \lfloor x/2 \rfloor \\
\quad y \leftarrow 2 * y \\
\{z = x_0 \cdot y_0\}
\end{array}
$$

and that the loop terminates after finitely-many iterations.

Hint: There's a reason I gave this problem after Problem 4.

6. [5 points] Show that the full algorithm (on the previous page) is correct, as annotated. That is, show that if $x_0 \geq 0$, then the algorithm terminates, with $z = x_0 \cdot y_0$.