EECS 340: Assignment 1

Shaochen (Henry) ZHONG, sxz517
Zhitao (Bobby) CHEN, zxc325

Due on 01/27/2020, submitted on 01/26/2020
EECS 340, Dr. Koyuturk

1 Problem 1

1.1 (a)

Without loss of generality, assume $x > y$ for $x, y \in \mathbb{Z}^+$. The loop invariant is:

$$Euclidean(x, y) = Euclidean(x - y, y) \tag{1}$$

1.2 (b)

Without loss of generality, assume $x > y$ for $x, y \in \mathbb{Z}^+$.

Let d for $d \in \mathbb{Z}^+$ being the greatest common divisor of x and y, a.k.a $d = gcd(x, y)$. As d being a divisor of both x and y, we may therefore have $x = kd$ and $y = jd$ for $k, j \in \mathbb{Z}^+$. Then we may infer:

$$x - y = dk - dj = d(k - j) \tag{2}$$

From *Equation 2* and the known fact that $y = jd$, we may say that d is also a common divisor of $x - y$ and y. By the defination of gcd, this means the upper bond of d cannot be greater than $gcd(x - y, y)$. Thus we may conclude:

$$\begin{aligned} &gcd(x, y) = d \leq gcd(x - y, y) \\ &\Rightarrow gcd(x, y) \leq gcd(x - y, y) \end{aligned} \tag{3}$$

Now similarly, Let e for $e \in \mathbb{Z}^+$ being the greatest common divisor of $x - y$ and y. We may therefore have $x - y = le$ and $y = me$ for $l, m \in \mathbb{Z}^+$. Then we may infer:

$$x = (x - y) + y = le + me = e(l + m) \tag{4}$$

From *Equation 4* and the known fact that $y = me$, we may say that e is also a common divisor of x and y. By the defination of gcd, this means the upper bond of e cannot be greater than $gcd(x, y)$. Thus we may conclude:

$$\begin{aligned} gcd(x-y, y) &= e \leq gcd(x, y) \\ \Rightarrow gcd(x-y, y) &\leq gcd(x, y) \end{aligned} \tag{5}$$

By observing *Equation 3* and *Equation 5*, we may have a constraint of $gcd(x, y) = gcd(x-y, y)$. As the given method $Euclidean()$ is a gcd finder, we may promote such constraint to $Euclidean(x, y) = Euclidean(x-y, y)$ due to the equivalency of $Euclidean(a, b)$ and $gcd(a, b)$.

1.3 (c)

The `while` loop always terminates as the condition $x = y$ will eventually be reached. Due to the fact that we have x and y for $x, y \in \mathbb{Z}^+$; without loss of generality, we assume $x > y$, therefore we must have $x' = x - y$ for $x' \in \mathbb{Z}^+$.

As we have only a finte amount of x', x'', x'''... to decrease for x', x'', and $x''' \in \mathbb{Z}^+$, the decremental calculation of $x_{k+1} = x_k - y_k$[1] will eventually reaches a condition where $x = y$ due to the "well ordering" nature of the natural numbers. Thus, the `while` loop always terminates.

1.4 (d)

In **Section 1.2**, we have proven that $gcd(x, y) = gcd(x-y, y) \Rightarrow Euclidean(x, y) = Euclidean(x-y, y)$ assuming $x > y$ for $x, y \in \mathbb{Z}^+$. Following the principle of induction, we can generalize it as:

$$Euclidean(x, y) = Euclidean(x_{k+1}, y_{k+1}) \tag{6}$$

$$\text{for } x', y' \in \mathbb{Z}^+ \text{ while}$$

$$x_{k+1} = x_k - y_k \text{ if } x_k > y_k \text{ and } y_{k+1} = y_k - x_k \text{ if } y_k > x_k$$

Where $Euclidean(x_{k+1}, y_{k+1})$ is the greatest common divisor of (x, y).

As we haven proven in **Section 1.2**, that the `while` loop within the $Euclidean()$ method must terminate. Combined such finding with *Equation 6*, we must have a:

$$Euclidean(a, b) = Euclidean(a_{k+1}, b_{k+1}) = Euclidean(a_{k+2}, a_{k+2}) \tag{7}$$

[1] for k being the numbers of iteration went through in the `while` loop.

As we know by calculation that $Euclidean(a_{k+2}, a_{k+2}) = a_{k+2}$, a_{k+2} will be the greatest common divisor of $Euclidean(a, b)$.

2 Problem 2

2.1 (a)

2.2 (b)

2.3 (c)

2.4 (d)

3 Problem 3