Question 1

Show that $\vdash_{tot} \{T\}\, P\, \{z = \max(x, y)\}$ is valid, where $\max(x, y)$ is the largest number of x and y. [3 marks]

$\{\top\}$

```
if (x > y){
```

$\{\top \wedge x > y\}$ If-statement

$\{x = \max(x,y)\}$ Implied

```
    z = x;
```

$\{z = \max(x,y)\}$ Assignment

```
} else {
```

$\{\top \wedge \neg(x < y)\}$ If-statement

$\{y = \max(x,y)\}$ Implied

```
    z = y;
```

$\{z = \max(x,y)\}$ Assignment

```
}
```

Explanation:

First, If branch, by the Assignment rule we can prove

$$\{y = \max(x, y)\}\, z = y\, \{z = \max(x, y)\}$$

From $\vdash x > y \rightarrow y = \max(x, y)$ by the Implied rule we can prove

$$\{x > y\}\, z = y\, \{z = \max(x, y)$$

the else branch is similar, so we can show

$$\frac{\{\top \wedge x > y\} z = y \{z = \max(x, y)\} \{\top \wedge \neg(x > y)\} z = x \{z = \max(x, y)\}}{\{\top\} \text{ if } x > y \text{ then } z = y \text{ else } z = x \{z = \max(x, y)\}}$$

Question 2

Show that $\vdash_{tot} \{x \geq 0\}\ Fac1(x)\ \{y = x!\}$ is valid

1. Write down a proper loop invariant which is useful for constructing the correctness proof. [2 marks]
2. Write down a proper variant which is useful for proving the termination of the program. [1 mark]
3. Provide the full proof using proof rules. [4 marks]
4. Justify the correct uses of the implied rule in three places of the proof in English. [3 marks]

1. $y * a! = x!$
2. a
3.

(1). If a > 0

{0 ≤ x}

{ 1*x!= x! ∧ 0 ≤ x}   Imply

```
a = x;
```

{ 1*a! = x! ∧ 0 ≤ a}   Assignment

```
y = 1;
```

{ y*a! = x! ∧ 0 ≤ a}   Assignment

```
while (a > 0){
```

$\{y*a! = x! \wedge a > 0 \wedge 0 \leq a = E_0\}$ Invariant Hyp. and guard

$\{y * a *(a-1)! = x! \wedge 0 \leq a -1 < E_0\}$ Implied

```
    y = y * a;
```

$\{y*(a-1)! = x! \wedge 0 \leq a -1 < E_0\}$ Assignment

```
    a = a - 1;
```

$\{y*a! = x! \wedge 0 \leq a < E_0\}$ Assignment

```
}
```

$\{y*a! = x! \wedge \neg(a > 0)\}$ Total-while

$\{y = x!\}$ Implied

(2). If a = 0

$\{0 \leq x\}$ Implied

```
a = x = 0;

y = 1;

while (a > 0){

    y = y * a;

    a = a - 1;

}
```

$\{y = 0! = x!\}$ Implied

If a = x = 0, so that we can imply x is greater than or equal to 0. Also, it will not enter the while loop, so it will always terminate. Thus, we can imply y = 1 = 0! = x!.

4. (1) First, from the Invariant Hyp. and guard $\{y * a! = x! \wedge a > 0 \wedge 0 \leq a = E0\}$, as a! equals to $a * (a - 1)!$, so that y*a! = x! can imply $y * a * (a - 1)! = x!$.

Also, as a is greater than 0, known from the condition of the while loop, and $0 \leq a = E_0$, so that a – 1 is greater than or equal to 0 and also less than E_0.

Thus, $\{y * a! = x! \wedge a > 0 \wedge 0 \leq a = E0\}$ can imply $\{y * a * (a - 1)! = x! \wedge 0 \leq a - 1 < E0\}$

(2) From $\{1 * x! = x! \wedge 0 \leq x\}$, as $1 * x! = x!$ is a tautology, so that $T \wedge 0 \leq x$ can imply the pre-condition $\{0 \leq x\}$.

(3) From $\{y * a! = x! \wedge \neg(a > 0)\}$, as $0 \leq$ a and $\neg(a > 0)$, so that a is equal to 0. Because 0! is equal to 1, so that $y * 1 = x!$. Thus, $\{y * a! = x! \wedge \neg(a > 0)\}$ can imply $\{y = x!\}$.