Logic in Computer Science Assignment 6

10185101210 陈俊潼

January 2021

1 Prove

1.1 Prove the following progam `MAX` is partial correctness.

$$\{n > 0 \land dom(f) = [0 \ldots n-1] \land ran(f) \in N\}$$
$$Max$$
$$\{y = max\Big(ran(f)\Big)\}$$

Proof:

First we add an empty else statement and a pair of brace for the original code to make it more clear in the process of proving. So the refined version of the `MAX` program would be:

```
y = f[0]
i = 1
while (i < n)
{
    if (y < f[i])
    {
        y = f[i])
    }
    else
    {
    }
    i = i + 1
}
```

Then analysing the algorithm, we assume the loop invariant to be `y = max(ran(f[0:i]))`. Now we can proof its partial correctness as follows:

$(\!\|\ \top\ \|\!)$	
$(\!\|\ f[0] = \max(f[0])\ \|\!)$	Implied
$(\!\|\ f[0] = \max(\mathrm{ran}(f[0:1]))\ \|\!)$	Implied
`y = f[0]`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:1]))\ \|\!)$	Assignment
`i = 1`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i]))\ \|\!)$	Assignment
`while (i < n)`	
`{`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i])) \land i < n\ \|\!)$	Invariant Hyp. ∧ Guard
$(\!\|\ y = \max(\mathrm{ran}(f[0:i]))\ \|\!)$	Implied
$(\!\|\ \left(y < f[i] \to \max(\mathrm{ran}(f[0:i])) < f[i]\right) \land$	
$\neg(y < f[i]) \to y = \max(\mathrm{ran}(f[0:i]))\ \|\!)$	Implied
`if (y < f[i])`	
`{`	
$(\!\|\ \max(\mathrm{ran}(f[0:i])) < f[i]\ \|\!)$	If-Statement
$(\!\|\ f[i] = \max(\mathrm{ran}(f[0:i]),\ f[i])\ \|\!)$	Implied
`y = f[i]`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i]),\ f[i])\ \|\!)$	Assignment
$(\!\|\ y = \max(\mathrm{ran}(f[0:i+1]))\ \|\!)$	Implied
`}`	
`else`	
`{`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i]))\ \|\!)$	If-Statement
$(\!\|\ y = \max(\mathrm{ran}(f[0:i+1]))\ \|\!)$	Implied
`}`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i+1]))\ \|\!)$	If-Statement
`i = i + 1`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i]))\ \|\!)$	Assignment
`}`	
$(\!\|\ y = \max(\mathrm{ran}(f[0:i])) \land \neg(i < n)\ \|\!)$	Partial-While
$(\!\|\ y = \max(\mathrm{ran}(f[0:i])) \land i \geq n\ \|\!)$	Implied
$(\!\|\ y = \max(\mathrm{ran}(f[0:n]))\ \|\!)$	Implied
$(\!\|\ y = \max(\mathrm{ran}(f))\ \|\!)$	Implied