CSSE3100 Study Notes

Brae

Semester 1, 2018

1 Derivation

Programs can be derived from specifications statements.

This allows programs to be proved correct when the program is being developed rather than after development.

2 Assignment Rule

3 Skip Rule

4 Composition Rule

A specification statement can be separated into two statements by the composition rule.

5 JML Constructors

```
/*@ requires c >= 0;
  @ ensures getCredits == c;
  @*/
public Constructor(int c) {
    this.c = c;
}
```

> Constructors can only reference parameters not instance variables as they have not yet been initialized.

6 JML Visibility

Specifications obey visibility of java access modifieres unless overriden by above syntax

```
/*@ spec_public */ private int status;
```

7 JML Invariants

Invariants are always true properties of a class which are:

- ensured by a constructor
- maintained by each method

```
/*@ invariant x;
  @ invariant y;
  @*/
```

> Helper methods do not need to maintain the invariant
>
> ```
> private /*@ helper @*/ helperMethod() {}
> ```

8 Weakest Precondition

$$Q \Rightarrow P$$

w:[P, Q] $\sqsubseteq w : [\,P, M\,]\,; w : [\,M, Q\,]$

w:[P, Q] $\sqsubseteq w : [\,P, M\,]\,; w : [\,M, Q\,]$

w:[P, Q]

$\sqsubseteq (Composition : chooseMasM)$

$w : [\,P, M\,]\,; w : [\,M, Q\,]$