CSSE3100 Study Notes

Brae

June 4, 2018

Semester 1, 2018

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.

Composition Rule

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

JML Constructors

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

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.

JML Visibility

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

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

JML Invariants

Invariants are always true properties of a class which are:

- ensured by a constructor
- maintained by each method

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

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() {}
```

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]