Software Specifications
Intro to Specification

Cain Susko

Queen's University
School of Computing

March 4, 2022

Specification

a specification is what a program should *do.* the implementation is what the program *does.* In specific terms, specifications include:

- what the input are
- what the outputs should be
- the environment in which the program should run

Formalization a given specification has a corresponding formulation which will include:

- assertion on input values (pre-condition)
- assertion on onput values in validation to input values (post condition)
- declaration interface: static properties of identifiers

Specification as a Contract if the program is started in a state satisfying the pre-conditions, then it terminates in a state satisfying the post condition (aka: total correctness). if the preconditions do not hold, then the program can do anything without violating the specifications.
a weaker notion of total correctness is partial correctness; which says that if the program is started in a state satisfying the precondition then if it terminates at the end the state satisfies the postcondition.
Specifications use locigcal formulas like from cisc204. the characters used can be made using standard keyboard characters (as they are intended to be written in comments in code etc.)

Boolean Operations	$\&\&, \|\|,$
Implies	$implies$
if	if, iff
equality	$==, !=$

The quantifiers are represented as $\forall = ForAll(inti)$ and $\exists = Exists(inti)$. an example of an expression in this notation is:

$$P\&\&Q\ implies\ P||Q$$

Note: the above equation is generally true.

Example

consider the following expressions:

$$ForAll(inti)Exists(intj)j == i + 1$$

$$Exists(intj)ForALL(inti)j == i + 1$$

the first equation is true. there is also a shorthand for a range used by the textbook:

$$ForAll(i = a; i < b)P$$

which stands for $ForAll(inti)a = i < b \; implies \; P$. this can also be done for $Exists$ which has the same function. Additionally, the notation uses alot of programming conventions, for example:$A[i] \; ! = \; A[j]$