Assignment 1 CSSE3100/7100 Reasoning about Programs

Due: 4pm on 19 March, 2021

The aim of this assignment is to consolidate your learning of the course's introductory material. Specifically, it aims to provide you with experience with specifying and verifying programs involving control flow and recursion.

Instructions: Submit a single pdf file with your solution to the following question to Blackboard by the due date and time.

The greatest common divisor of two positive integers is the largest number which divides into them both evenly, i.e., with a remainder of 0. For example, the greatest common divisor of 9 and 12 is 3, and the greatest common divisor of 15 and 30 is 15.

Let gcd(a, b) denote the greatest common divisor of positive integers a and b, i.e., a >= 0 and b >= 0. The following are properties of gcd(a,b):

i. gcd(a, 0) = a
ii. gcd(a, a) == a
iii. gcd(a, b) == gcd(b, a)
iv. b > 0 ==> gcd(a, b) == gcd(b, a % b)

Your colleague Andy claims the following is a simple way to implement gcd(a, b), provided a and b are not 0.

```
method GCD1(a: int, b: int) returns (r: int) {
     if a < b {
          r := GCD1(b, a);
     } else if (a % b == 0) {
          r := b;
     } else {
          r := GCD1(b, a % b);
     }
}
```

Your other colleague Candy says it can be implemented much more simply as follows. And, she claims, in this program we can allow a and b to be 0!

```
method GCD2(a: int, b: int) returns (r: int) {
     if b == 0 {
          r := a;
     } else {
          r := GCD2(b, a % b);
     }
}
```

Which of your colleagues is right? Andy, Candy, or both? Justify your answer by providing a specification and a formal (weakest precondition) proof of total correctness for each of the programs. Your specifications may refer to gcd(a, b), e.g., you may have a

predicate such as r == gcd(a,b); there is no need to expand the definition of gcd(a, b) further. Instead, your proofs may use any of the 4 properties of gcd(a, b) above to simplify predicates, e.g., a step of your proof may change r == gcd(a,b) to r == gcd(b,a) using rule (iii). Non-trivial simplifications of predicates need to be justified, i.e., if you're not sure whether the marker will understand your simplification, add some text to explain why it is true.

Marking

You will get marks for the application of the appropriate rules for each line of code (do not skip the application of a rule), and for correct and, where necessary, justified simplifications. A breakdown of the marks is given below.

GCD1	pre and postcondition	1 mark
	termination metric	0.5 marks
	weakest precondition proof [1]	4 marks
GCD2	pre and postcondition	1 marks
	termination metric	0.5 mark
	weakest precondition proof [1]	3 marks

[1] Including explanation of program failure if necessary.

School Policy on Student Misconduct

This assignment is to be completed individually. You are required to read and understand the School Statement on Misconduct, available on the Schools website at: http://www.itee.uq.edu.au/itee-student-misconduct-including-plagiarism