Assignment 2 CSSE3100/7100 Reasoning about Programs

Due: 5pm on 23 April, 2020

Instructions: Answer all questions below and submit a single pdf file with your solutions to 1(a) and 2(a), and a single Dafny file with your solutions to 1(b) and 2(b) to Blackboard by the due date and time.

Question 1 [6 marks]

(a) Your friend (yes, the same one!) claims that the method below always terminates and returns X * Y, provided X and Y are non-negative. Prove that your friend is either right or wrong. To do so, complete the specification below and use weakest precondition reasoning to show whether or not the implementation satisfies the specification.

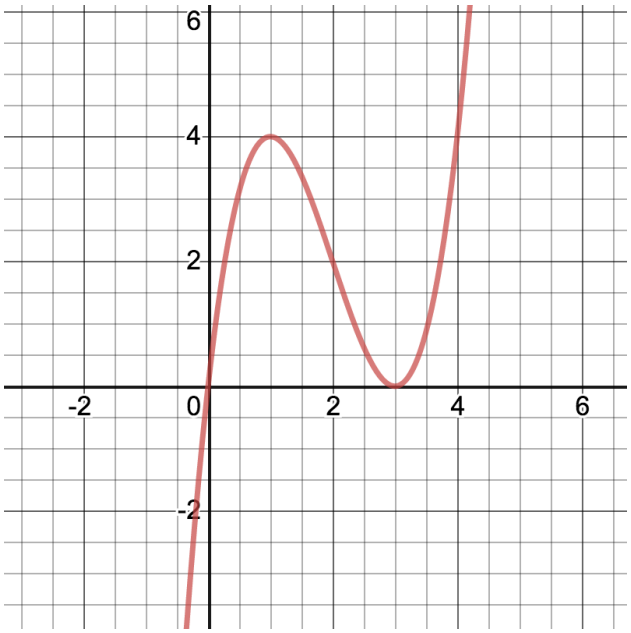
If the specification is not correct, explain the cases when it will fail to compute X * Y and provide a precondition for which it is correct.

```
method mult2(X: int, Y: int)  returns (r: int)
    requires …
    ensures …
{
    var x, y, c := X, Y, 0;
    while y > 1
        invariant …
        decreases …
    {
        if y % 2 == 0 {
            y := y/2;
        } else {
            y := (y-1)/2;
            c := c + x;
        }
        x := 2*x;
    }
    r := x + c;
}
```

(b) Encode the method (with corrected precondition, if necessary) along with your invariant and decreases clause in Dafny. Unfortunately, Dafny doesn't know everything you do about integer and modulo division. Provide lemmas so that Dafny can verify the code. If Dafny can't prove your lemmas automatically, provide a proof by induction.

Question 2 [9 marks]

The graph below plots the equation $y = x^3 - 6x^2 + 9x$.



(a) Derive an iterative method which, for a given $N \geq 0$, computes the smallest integer x that satisfies $x^3 - 6x^2 + 9x \geq N$. Your program must satisfy the following requirements for efficiency:

1. No loop iterations for values which (given the graph above) cannot correspond to the return value.
2. No multiplication in loop iterations. You must use the "wishing" method from lectures to achieve this.

Your derivation must be based on a pre/postcondition specification and use weakest precondition reasoning.

(b) Encode your method in Dafny to check your working. Include calc statements to check the predicate simplifications you made when deriving the loop body.

Marking

A detailed breakdown of the marks is given below.

Q1	loop invariant	1 mark
	termination metric	0.5 marks
	weakest precondition proof [1]	3 marks
	lemmas in Dafny	1.5 marks
Q2	precondition	0.5 marks
	postcondition	1 mark
	loop invariant	1 mark
	termination metric	0.5 marks
	derivation	5 marks
	calc statements in Dafny	1 mark

[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