

## PRACTICE QUESTIONS FOR AXIOMATIC SEMANTICS

1. Take the exponentiation program and give a formal proof of total correctness. The code is

```
e := 1;
t := y;
while t greater 0 do
  e := e mult x;
  t := t minus 1
end
```

and the specification is  $[y \geq 0, e = x^{**}y]$ . The proof is sketched in the class write-up, but you should write it out properly and follow the technique outlined in class.

2. Take the division example used in class and give a formal proof of total correctness. Here is the program:

```
q := 0;
r := x;
while r greater y minus 1 do
  q := q plus 1;
  r := r minus y
end
```

The proof rests on choosing the right specification and the right invariant for the loop. The specification to use is:  $[y \geq 1 \wedge x \geq 0, x = q * y + r \wedge 0 \leq r < y]$ . The Floyd expression for total correctness should map into the natural numbers, but need not reduce by one every time round the loop; as long as it reduces and never becomes negative that is enough. By using ratios and offsets, any such expression can map directly into the natural numbers.

3. Suppose the greatest common divisor of two positive integers is given by:

$$\begin{aligned} \text{gcd}(n, m) &\Leftrightarrow \\ m > 0 \wedge n > 0 \wedge \\ n > m &\Rightarrow \text{gcd}(n, m) = \text{gcd}(n - m, m) \wedge \\ \text{gcd}(n, m) &= \text{gcd}(m, n) \wedge \\ \text{gcd}(n, n) &= n \end{aligned}$$

With this definition, prove that the following program (Euclid's algorithm) is partially correct with respect to the specification  $[n > 0 \wedge m > 0, \text{gcd}(n, m) = x]$ , where  $x$  is existentially quantified.

```
N := n
M := m
while not (N = M) do
  if N > M then
    N := N - M
  else M > N then
    M := M - N
```