

# COS 4892 Assignment 3

Adriaan Louw (53031377)

September 13, 2019

## 1 The Integer Remainder Computation Algorithm

The concept of a remainder is a very important concept in computing. It is used in fields like encryption and error checking. This essay will discuss how the principles developed in “Program Construction” by Roland Backhouse was used to develop an algorithm for Remainder Computation in Chapter 15 of said book.

For integers, the remainder can be defined as what is left over after one number is divided by another. For instance, when we divide 10 by 3 we get a quotient of 3 and a remainder of 1. Or when we divide 4 by 2 we get a quotient of 2 and a remainder of 0.

Given an integer  $P$  divided by a positive natural number  $Q$  gives remainder  $r$  and quotient  $d$ . This can be expressed in the following way:

$$0 \leq r < Q \wedge P = Q.d + r \quad (1)$$

Where  $r$  will always be positive and less than  $Q$  by definition.

We can define the 2nd half of Formula 1 more precisely as:

$$0 \leq r < Q \wedge \langle \exists d :: P = Q.d + r \rangle \quad (2)$$

This uses the Quantifier Notation from Chapter 11. This notation has the general form

$$\langle qv : r : t \rangle \quad (3)$$

Where  $q$  is the quantifier that applies to the dummy variable  $v$ . This could be the existential quantifier  $\exists v$ , the summation quantifier  $\sum v$  or even the universal quantifier  $\forall v$ .  $r$  defines the range over which the quantifier operates. This is a boolean expression that determines the set of values the dummy variable can take. Then  $t$  is the term to which the dummy variable applies. In Formula 2 this means that there exists a value for  $d$  such that the expression  $P = Q.d + r$  is valid. Here the range is not specified. Therefore  $d$  could be any integer.

The question remains whether in Formula 1 the values of  $r$  and  $d$  are unique for some value of  $P$  and  $Q$ . To prove this we need the concept of substitution of equals for equals or Leibniz’s rule (Formula 4) for short which was discussed in Chapter 7.

$$(e = f) \equiv (e = f) \wedge (E[x := e] = E[x := f]) \quad (4)$$

This formula states that the “..application of a function to equal values gives equal results...” (From Chapter 7).

Now to prove the uniqueness of  $r$  and  $d$  we assume that 2 pairs  $(r, d)$  and  $(r', d')$  satisfy Formula 1 then we have

$$(0 \leq r < Q \wedge P = Q.d + r) \wedge (0 \leq r' < Q \wedge P = Q.d' + r') \quad (5)$$

which is equivalent to

$$(0 \leq r < Q \wedge P = Q.d + r) \wedge (Q > r' \geq 0 \wedge P = Q.d' + r') \quad (6)$$

Then to introduce  $r - r'$  and  $d - d'$  we see that by ‘subtraction’ the 2 terms, the previous statement will imply

$$-Q < r - r' < Q \wedge 0 = Q.(d - d') + (r - r') \quad (7)$$

Now using Leibniz and some arithmetic, the above statement is equivalent to

$$-Q < -(Q.(d - d')) < Q \wedge -(Q.(d - d')) = r - r' \quad (8)$$

which becomes for  $Q \neq 0$

(9)

which with some arithmetic becomes

$$d = d' \wedge r = r' \tag{10}$$