Tutorial Letter 203/0/2020

Formal Program Verification

COS4892

Year module

School of Computing

This tutorial letter contains the solutions to Assignment 3.

Dear Student

Hope you are well. This tutorial letter contains the solutions to the third and final assignment for COS4892.

Question 1 – **RB** Chapter 14	10 marks

The problem: Given an array with *n* objects colored red, white or blue, sort them **in-place** so that objects of the same color are adjacent, with the colors in the order *red*, *white* and *blue*.

The question: Discuss the solution presented in **RB**.

The rubric used to assess this question is as follows:

Issues that needed to be addressed	Marks
• Introduce and discuss 4 partitions	3
• Iterative process	1
• Variables and specification	1
• Initialisation of variables	1
• Discussion of how to progress towards termination condition	1
○ white	1
○ red	1
○ blue	1

Question 2 – **RB** Chapter 15	15 marks

Write a well-planned essay in which you show how the principles developed in the earlier chapters of **RB** are used to develop an algorithm for Remainder Computation.

Build your essay around the following:

- a formal specification of the problem involving a remainder and quotient
- a development of an elementary version of the algorithm
- extending the development to include a discussion of the **mod** and **div** functions.

Remember that a good essay starts with an **Introduction**, followed by the **Body** of the essay and ends with a sensible **Conclusion**.

The rubric used to assess this question is as follows:

Issues that needed to be addressed	Marks
Introduction	
• Addressing the concept of a remainder	2
• Used for coding of data (encryption and error resilient coding)	
Body	
• Formal specification	2
• Discussion of algorithm	3
• Discussion of mod (definition and example)	2

• Discussion of div (definition and example) • Discussion of difference	2 2
Conclusion	2

Question 3 – **RB** Chapter 16	25 marks

(a) Define and describe Boolean Polynomials by addressing *generator* polynomials and the addition and multiplication operators on coefficients. Give examples besides those used in **RB**. (10)

The rubric used to assess this question is as follows:

Issues that needed to be addressed	Marks
• Define (Boolean) polynomials and discuss example	3
• Iterative process	1
• Discuss concept of degree + example	1
• Discuss concept of coefficient + example	1
• Adding of Boolean polynomials	1
• Multiplication of Boolean polynomials	1
• Define generator polynomials	1
• Example	1

(b) Use the generator polynomial $x^8 + x^7 + x^6 + x^4 + 1$ to encode the message 0110110. (5)

The generator polynomial is given as $Q = x^8 + x^7 + x^6 + x^4 + 1$ and it corresponds to 111010001
The message 0110110 is presented as the input polynomial $P = x^5 + x^4 + x^2 + x^1$

The encoded message will be the original message concatenated with the remainder r of

$$\frac{Px^8}{Q}$$

$$\begin{aligned} Px^8 &= (x^5 + x^4 + x^2 + x^1)\, x^8 \\ &= x^{13} + x^{12} + x^{10} + x^9 \end{aligned}$$

$$\frac{Px^8}{Q} = \frac{x^{13} + x^{12} + x^{10} + x^9}{x^8 + x^7 + x^6 + x^4 + 1}$$

Using long division, add 8 zero bits to P (0110110) to become 0110110 00000000

```
                                                0 1 0 1 0 1 1
111010001   ) 0  1  1  0  1  1  0  0  0  0  0  0  0  0  0
                0  0  0  0  0  0  0  0  0
                ---------------------------------------------
                   1  1  0  1  1  0  0  0  0  0  0  0  0  0
                   1  1  1  0  1  0  0  0  1
                   ---------------------------------------
                      0  1  1  0  0  0  0  1  0  0  0  0  0
                      0  0  0  0  0  0  0  0  0
                      ------------------------------------
                         1  1  0  0  0  0  1  0  0  0  0  0
                         1  1  1  0  1  0  0  0  1
                         ---------------------------------
                            0  1  0  1  0  1  0  1  0  0  0
                            0  0  0  0  0  0  0  0  0
                            ---------------------------
                               1  0  1  0  1  0  1  0  0
                               1  1  1  0  1  0  0  0  1
                               ------------------------
                                  1  0  0  0  0  1  0  1  0
                                  1  1  1  0  1  0  0  0  1
                                  ---------------------
                                     1  0  0  0  0  1  0  1
                                     1  1  1  0  1  0  0  0
                                     ------------------
                                        1  1  0  1  1  0  1
```

Another way to do long division is using a table:

									1	0	1	0	1	1
	x^{13}	x^{12}	x^{11}	x^{10}	x^9	x^8	x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
Px^8	1	1	0	1	1	0	0	0	0	0	0	0	0	0
x^5Q	1	1	1	0	1	0	0	0	1	0	0	0	0	0
remainder			1	1	0	0	0	0	1	0	0	0	0	0
x^3Q			1	1	1	0	1	0	0	0	1	0	0	0
remainder					1	0	1	0	1	0	1	0	0	0
x^1Q					1	1	1	0	1	0	0	0	1	0
remainder						1	0	0	0	0	1	0	1	0
x^1Q						1	1	1	0	1	0	0	0	1
remainder							1	1	0	1	1	0	1	1

The remainder is: 11011011 and therefore, $r = x^7 + x^6 + x^4 + x^3 + x + 1$

As the encoded message is the original message concatenated with the remainder r, the encoded message becomes: 011011011011011

(c) Determine an appropriate generator polynomial to encode the message 110010. Give the encoded message. (10)

You have to determine an appropriate generator polynomial (Q) which will allow for the number of parity bits. The degree of the generator polynomial will give the number of parity bits. E.g. Q = $x^4 + x^2 + 1$ has a degree of 4 and will allow for 4 parity bits.

Assume $Q = x^3 + x + 1$, with $degree.Q = 3$

The input polynomial is given as $P = x^5 + x^4 + x$

The check bits are defined to be the coefficients of the remainder polynomial after the division of the input polynomial $P \times x^{degree.Q}$ by Q.

$$\begin{aligned} P \times x^{degree.Q} &= P \times x^3 \\ &= (x^5 + x^4 + x)\, x^3 \\ &= x^8 + x^7 + x^3 \end{aligned}$$

Calculate the remainder by dividing Px^3 by Q

$$\frac{Px^3}{Q} = \frac{x^8 + x^7 + x^3}{x^3 + x + 1}$$

```
                    1  1  1  0  1  1
          ---------------------------
1011    ) 1  1  0  0  1  0  0  0  0

     1  0  1  1
     ----------
        1  1  1  1  0  0  0  0
        1  0  1  1
        ----------
           1  0  0  0  0  0  0
           1  0  1  1
           ----------
              0  1  1  0  0  0
              0  0  0  0
              ----------
                 1  1  0  0  0
                 1  0  1  1
                 ----------
                    1  1  1  0
                    1  0  1  1
                    ----------
                       1  0  1
```

The final remainde $r = 101$

Since the encoded message is the original message concatenated with the remainder r, the encoded message becomes: 110010101