Assignment-03

Hrudaya
TA40935

① Let
$p(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x + 1$
and $q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$

ⓐ compute by hand GCD((p(x), q(x)) over the ring GF(2)[x]

sol where we have
$p(x) = x^{12} + x^9 + x^8 + x^6 + x^4 + x + 1$
= 1001101010011

$q(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^3 + 1$
= 110001111001

```
                11  = (x+1)
110001111001 | 1001101010011
               110001111001
               -------------
               0101110100001
                110001111001
               -------------
               0111110111000
elim
x^10 + x^9 + x^8 + x^7 + x^6 + x^4 + x^3
```

so $p(x) = q(x)(x+1) + (x^{10} + x^9 + x^8 + x^7 + x^6 + x^4 + x^3)$

1

11111011000) 11000111001
11111011000
00111 11001001

x^9

$q(x) = (x^{10}+x^9+x^8+x^7+x^6+x^4+x^3).1 + (x^9+x^8+x^7+x^6+x^3+1)$

And again

1

1111001001) 11111011000
1111001001
00001001010

x^6+x^3+x

Hence

$x^{10}+x^9+x^8+x^7+x^6+x^4+x^3$

$= (x^9+x^8+x^7+x^6+x^3+1).1 + (x^6+x^3+x)$

$111 = x^2+x+1$

1001010) 1111001001
1001010
0110011001
1001010
010110001
1001010
00100101

$x^5\ x^4\ x^3\ x^2\ x\ 1$

$= x^5+x^2+1$

Hence

$(x^9+x^8+x^7+x^6+x^3+1) = (x^6+x^3+x) \cdot (x^2+x+1) + x^5+x^2+1$

$$
\begin{array}{r|l}
 & \quad 1 \\
100101 & 1001010 \\
x^5\,x^4\,x^3\,x^2\,x\,1 & 100101 \\
\hline
 & \quad 0
\end{array}
$$

$(x^6+x^3+x) = (x^5+x^2+1) \cdot 1 + 0$

Hence GCD of given $p(x)$ and $q(x)$ is x^5+x^2+1

(2) (b) Implement in Mathematica

Sol

We utilized polynomial GCD function inorder to get GCD of two polynomials

$x^{12}+x^{9}+x^{8}+x^{6}+x^{4}+x+1$

$x^{11}+x^{10}+x^{6}+x^{5}+x^{4}+x^{3}+1$

with modulus 2 to verify the solution

$\Downarrow$

as $GF(2)(x)$ is given

Scanned with CamScanner

hrudayajinna.nb - Wolfram Cloud | hrudaya.nb - Wolfram Cloud

wolframcloud.com/env/hrudayj1/hrudaya.nb

WOLFRAM MATHEMATICA | *Plan:* University of Maryland at Baltimore County | Documentation | Language Intro | Quick Links | Cloud Files

hrudaya.nb | File | Edit | Format | Insert | Evaluation | View | Help | Share | Publish

In[10]:= x^12+x^9+x^8+x^6+x^4+x+1

Out[10]= $1+x+x^4+x^6+x^8+x^9+x^{12}$

In[11]:= x^11+x^10+x^6+x^5+x^4+x^3+1

Out[11]= $1+x^3+x^4+x^5+x^6+x^{10}+x^{11}$

In[12]:=

PolynomialGCD[$1+x+x^4+x^6+x^8+x^9+x^{12}$, $1+x^3+x^4+x^5+x^6+x^{10}+x^{11}$, Modulus → 2]

Out[12]= $1+x^2+x^5$

plot | x derivative | x integral | zeros | *more...*

Quick Links

GETTING STARTED

Five Minute Hands-On Intro

Some Things to Try

USING NOTEBOOKS

1-Minute Video

MATHEMATICA + WOLFRAM LANGUAGE

Fast Intro for Math Students

Fast Intro for Programmers

Full Documentation

Language Home Page

An Introduction to the Wolfram Language

Online book » | Open Course »

EDUCATION & TRAINING

Wolfram U Course Catalog

RESOURCES

Function Repository

45°F Clear | Search | 9:27 PM 3/9/2023

② Create a log|Antilog table for $GF(2^4)$ using the primitive (hence irreducible) polynomial

$$p(x) = x^4 + x^3 + 1$$

sol Given

$$p(x) = x^4 + x^3 + 1$$

$$x^4 = x^3 + 1$$

$\therefore$ $\xi^{-\infty} = 0 \quad = 0000$

$\xi^0 = 1 \quad = 0001$

$\xi^1 = \xi \quad = 00110$

$\xi^2 = \xi^2 \quad = 0100$

$\xi^3 = \xi^3 \quad = 1000$

$\xi^4 = \xi^3 + 1 = 1001$

$\xi^5 = \xi^4 + \xi = \xi^3 + \xi + 1 = 1011$

$\xi^6 = \xi^5 + \xi^2 = \xi^4 + \xi^2 + \xi = \xi^3 + \xi^2 + \xi + 1 = 1111$

$\xi^7 = \xi^4 + \xi^3 + \xi^2 + \xi = \xi^3 + 1 + \xi^3 + \xi^2 + \xi = \xi^2 + \xi + 1 = 0111$

$\xi^8 = \xi^3 + \xi^2 + \xi = 1110$

$\xi^9 = \xi^4 + \xi^3 + \xi^2 = \xi^3 + 1 + \xi^3 + \xi^2 = 1 + \xi^2 = 0101$

$\xi^{10} = \xi^3 + \xi = 1010$

$\xi^{11} = \xi^4 + \xi^2 = \xi^3 + \xi^2 + 1 = 1101$

$\xi^{12} = \xi^4 + \xi^3 + \xi = \xi^3 + 1 + \xi^3 + \xi = 1 + \xi = 0011$

$\xi_1^{13} = \xi_1^2 + \xi_1 = 0110$

$\xi_1^{14} = \xi_1^3 + \xi_1^2 = 1100$

$\xi_1^{15} = \xi_1^4 + \xi_1^3 = \xi_1^3 + 1 + \xi_1^3 = \underline{1} = 0001$

Log & Antilog table for $GF(2^4)$ where $p(x) = x^4 + x^3 + 1$

log	Antilog a_3 a_2 a_1 a_0
$-\infty$	0 0 0 0
0	0 0 0 1
1	0 0 1 0
2	0 1 0 0
3	1 0 0 0
4	1 0 0 1
5	1 0 1 1
6	1 1 1 1
7	0 1 1 1
8	1 1 1 0
9	0 1 0 1
10	1 0 1 0
11	1 1 0 1
12	0 0 1 1
13	0 1 1 0
14	1 1 0 0

③ Create a log/Antilog table for GF(3^2) using the primitive (hence, irreducible) polynomial

$p(x) = x^2+x+2$

Sol

$p(x) = x^2+x+2$

$x^2 = -(x+2) = -x-2$

Hence GF(3) $\quad -1=2$

$x^2 = 2x+1$

$\xi^2 = 2\xi+1$

$\therefore \quad \xi^{-\infty} = 0 \longrightarrow 00$

$\xi^0 = 1 \longrightarrow 01$

$\xi^1 = \xi \longrightarrow 10$

$\xi^2 = 2\xi+1$

$\xi^3 = 2\xi^2+\xi$

$= 2(2\xi+1)+\xi$ $\qquad$ $5\%3=2$

$= 4\xi+2+\xi = 5\xi+2$

$= 2\xi+2 \longrightarrow 22$

$\xi^4 = 2\xi^2+2\xi$

$= 2(2\xi+1)+2\xi$ $\qquad$ $6\%3=0$

$= 4\xi+2+2\xi = 6\xi+2 = 2$

$\longrightarrow 02$

$\xi^5 = 2\xi \longrightarrow 20$

$\xi^6 = 2\xi^2$

$= 2(2\xi+1)$

$= 4\xi+2$ / $4\%3=\underline{1}$

$= \xi+2 \longrightarrow 12$

$\xi^7 = \xi^2+2\xi$

$=2\xi+1+2\xi$ $4\%3=\underline{1}$

$= 4\xi+1 = \xi+1 \longrightarrow 11$

$\xi^8 = \xi^2+\xi$ $3\%3=0$

$=2\xi+1+\xi = 3\xi+1$

$=\underline{1}$

From above deduction log/Antilog table for $GF(3^2)$

$p(x) = x^2+x+2$

log	Antilog a_1 a_0
$-\infty$	0 0
0	0 1
1	1 0
2	2 1
3	2 2
4	0 2
5	2 0
6	1 2
7	1 1

④ Put the following matrix into reduced echlon canonical form over GF(3)

$$\begin{bmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 \\ 1 & 1 & 2 & 0 & 2 & 2 \\ 1 & 1 & 0 & 1 & 2 & 1 \end{bmatrix}$$

Nonzero element to be in 1st row

So interchange R_1 & R_3

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 1 & 1 & 0 & 1 & 2 & 1 \end{bmatrix}$$

second row first element is zero

$R_2 \leftrightarrow R_2 + R_1$

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 1 & 1 & 0 & 1 & 2 & 1 \end{bmatrix}$$

By making the last row to zero,

so $R_4 \leftrightarrow R_4 + 2R_1$

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}$$

$R_3 \leftrightarrow R_3 + 2R_2$ we have to reduce R_3 by using R_2

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}$$

4th row 3rd column has to be zero

We have to reduce R_4 by using R_2

$R_4 \leftrightarrow R_4 + R_2$

$$\begin{bmatrix} 1 & 1 & 2 & 0 & 2 & 2 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we have to reduce R_1 by using R_2

$R_1 \leftrightarrow R_1 + 2R_2$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we have to reduce R_1 by using R_3

$R_1 \leftrightarrow R_1 + 2R_3$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 2 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$R_2 \leftrightarrow R_2 + 2R_3$ we have to reduce R_2 by using R_3

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Now eliminating 2 in second row by multiplying 2

$R_2 \leftrightarrow 2R_2$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Hence the matrix is reduced to Echelon cononial form.

All the rows are lineary independent

Scanned with CamScanner

(5) Put the following matrix into reduced echlon canonical form over GF(11)

$$\begin{bmatrix} 0 & 0 & 2 & 2 & 0 & 2 \\ 2 & 2 & 6 & 8 & 4 & 8 \\ 1 & 1 & 5 & 6 & 2 & 5 \\ 1 & 1 & 3 & 4 & 2 & 7 \end{bmatrix}$$

First we have to interchange R_1 as there should be non zero elements in the 1st row

$R_1 \leftrightarrow R_3$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 2 & 2 & 6 & 8 & 4 & 8 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 1 & 1 & 3 & 4 & 2 & 7 \end{bmatrix}$$

We have to reduce R_2 by R_1 $11 \% 11 = 0$

So $R_2 \leftrightarrow R_2 + 9R_1$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 1 & 1 & 3 & 4 & 2 & 7 \end{bmatrix}$$

we have to reduce R_4 using R_1

$R_4 \leftrightarrow R_4 + 10R_1$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 9 & 9 & 0 & 4 \end{bmatrix}$$

we have to reduce R_4 using R_3

$R_4 \leftrightarrow R_4 + R_3$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 2 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{bmatrix}$$

we have to reduce R_3 using R_2

$R_3 \leftrightarrow 2R_3 + R_2$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{bmatrix}$$

we can reduce R_3 by multiplying with 6 which gives $12 \% 11 = 1$

$R_3 \leftrightarrow 6R_3$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 4 \end{bmatrix}$$

We can reduce R_4 using R_3

$R_4 \longleftrightarrow R_4 + 7R_3$

$$\begin{bmatrix} 1 & 1 & 5 & 6 & 2 & 5 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we can reduce R_1 using R_2

$R_1 \longleftrightarrow R_1 + R_2$

$$\begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 3 \\ 0 & 0 & 7 & 7 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we can reduce R_2 by using R_3

$R_2 \longleftrightarrow R_2 + 2R_3$

$$\begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 3 \\ 0 & 0 & 7 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we can reduce R_1 by using R_3

$R_1 \longleftrightarrow R_1 + 8R_3$

$$\begin{bmatrix} 1 & 1 & 1 & 2 & 2 & 0 \\ 0 & 0 & 7 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

we can reduce R_1 using R_2

$$R_1 \leftrightarrow R_1 + 3R_2$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 7 & 7 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Now we can reduce R_2 by multiplying with

$8 = 8 \times 7 = 56 \% 11 = 1$

$$R_2 \leftrightarrow 8R_2$$

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

the above matrix is in reduced echelon canonical form.

Hence the non zero rows in this form is linearly independent