Problem 1

Determine the value of the following determinant over GF(4) $\det\begin{bmatrix}2&1&2\\1&3&2\\1&0&1\end{bmatrix}=?$

Solution:

Every number in *GF(4)* can be represented as a polynomial of degree q^m-1 helyett m. Then for the multiplication to fulfill the axioms we can use an irreducible polynomial to perform the "mod" arithmetic in the big field.

If $a,b\in\{0,1,\dots q^m-1\}$ are in the big field, we can uniquely represent these numbers as polynomials

$$a\mapsto a(x)=a_0+a_1x+a_2x^2+\dots+a_{q^m-1}x^{q^m-1}$$

as: $b\mapsto b(x)=b_0+b_1x+b_2x^2+\dots+b_{q^m-1}x^{q^m-1}$ in this case:

$b_i,a_i\in\{0,\dots,q-1\}$, the little field

a	*poly*	*bin*
0	$0\cdot x^1+0$	00
1	$0\cdot x^1+1$	01
2	$1\cdot x^1+0$	10
3	$1\cdot x^1+1$	11

To have operations called multiplication and addition in the big field which satisfy the axioms, we need an irreducible polynomial of degree $\deg=m$, if $GF(q^m)$.

For this problem the irreducible polynomial's deg=2 .

If we have such a polynomial, the addition and multiplication can be defined to fulfill the axioms.

The operations of two elements in $GF(q^m)$ are equivalent to the operations on their polynomials and perform the "mod" operation with the irreducible polynomial

$$a,b,c\in GF(q^m),a_i,b_i\in\{0,\dots,q-1\},\text{ the little field}$$

$$a\cdot b=c \qquad \text{such that}$$

$$c(x)=\{a(x)\cdot b(x)\}\bmod P(x)$$

$$a+b=c \qquad \text{such that}$$

$$c(x)=\{a(x)+b(x)\}\bmod P(x)=a(x)+b(x)$$

We know that an irreducible polynomial with degree 2 is $P(x)=x^2+x+1$

If we know the irreducible polynomial, we can construct the addition, multiplication and power table.

+	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

=

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

*	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

=

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

a	*poly*	*bin*	x^i	
0	$0\cdot x^1+0$	00	$x^{-\infty}$	
1	$0\cdot x^1+1$	01	x^0	x^3
2	$1\cdot x^1+0$	10	x^1	x^4
3	$1\cdot x^1+1$	11	x^2	x^5

$$x^2\bmod P(x)=\text{remainder}(x^2:x^2+x+1)=x+1$$

$$x^3\bmod P(x)=\text{remainder}(x^3:x^2+x+1)=x\cdot x^2=x(x+1)=x^2+x=x+1+x=1$$

$$x^4\bmod P(x)=\text{remainder}(x^4:x^2+x+1)=x^2\cdot x^2=(x+1)(x+1)=x^2+x+x+1=x+1+1=x$$

$$x^5\bmod P(x)=\text{remainder}(x^5:x^2+x+1)=x^3\cdot x^2=1(x+1)=x+1$$

$$\det\begin{bmatrix}2&1&2\\1&3&2\\1&0&1\end{bmatrix}=2\cdot3\cdot1-2\cdot0\cdot2-(1\cdot1\cdot1-1\cdot1\cdot2)+2\cdot1\cdot0-2\cdot1\cdot3=$$

Since $\quad =1 \quad -0 \quad -(1-2) \quad +0 \quad -1=$

$\quad =1 \quad +3 \quad +1=3$

Problem 2

Perform the operation $x = 4 \cdot 7$ over $GF(8)$ with the help of shift registers if the irreducible polynomial is $P(y) = y^3 + y + 1$

Solution:
First we do it generally with an arbitrary element of the field in GF(8) using the power table:

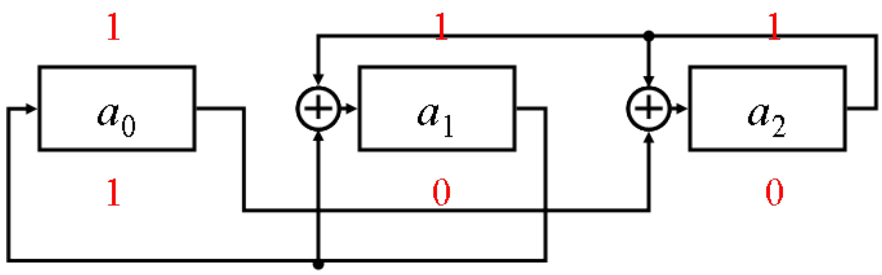
poly	binary	decimal	power			
1	001	1	1	7	14	21
y	010	2	y	8	15	22
y^2	100	4	y^2	9	16	23
$y+1$	011	3	y^3	10	17	24
y^2+y	110	6	y^4	11	18	25
y^2+y+1	111	7	y^5	12	19	26
y^2+1	101	5	y^6	13	20	27

$\alpha \in Q = \{0,1,\ldots,7\}$

4 in polynomial reprezentation is y^2

$$4 \cdot \alpha = y^2\left(a_0 + a_1 y + a_2 y^2\right) = a_0 y^2 + a_1 y^3 + a_2 y^4 = a_0 y^2 + a_1(y+1) + a_2\left(y^2 + y\right) =$$
$$= a_1 + \left(a_1 + a_2\right)y + \left(a_0 + a_2\right)y^2$$

From this the SR implementation looks as follows:



7 can be represented with the coefficients: $a_0 = 1, a_1 = 1, a_2 = 1$
Sot the output is 100 = 1.

Problem 3

Given a cyclic RS code over GF(8) correcting every double errors.
Give the parameters of the code.
Give the parity check polynomial in the standard form

Help for the arithmetic (the power table over $GF(2^3)$):

1	1	7	14	21
y	y	8	15	22
y^2	y^2	9	16	23
$y+1$	y^3	10	17	24
y^2+y	y^4	11	18	25
y^2+y+1	y^5	12	19	26
y^2+1	y^6	13	20	27

Solution:

C(7,3)

because $t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$, and RS codes are MDS, so $d_{\min} = n-k+1$

furthermore we know that with RS codes $n = q-1$

thus $n = 8-1 = 7$

we know that we must correct every double error, so $2 = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor \rightarrow d_{\min} = 5$

from n and $d_{\min}$ we can compute *k:* $5 = 7-k+1 \rightarrow k = 3$

the parity check polynomial can be constructed as follows:

$$h(x) = \prod_{i=n-k+1}^{n} \left(x - y^i\right) = \prod_{i=5}^{7} \left(x - y^i\right) = \left(x - y^5\right)\left(x - y^6\right)\left(x - y^7\right) =$$

$$= \left(x^2 + yx + y^4\right)\left(x+1\right) = x^3 + yx^2 + xy^4 + x^2 + yx + y^4 = x^3 + y^3x^2 + y^2x + y^4$$

Problem 4

Given a cyclic RS code over GF(8).

a.) What are the parameters of the code (n,k) if two errors are to be corrected.

b.) Give the parity check polynomials (the power primitive element y are used as roots)

c.) What is the received vector if the corresponding polynomial is

$$v(x) = y^5x^6 + y^5x^5 + y^5x^4 + y^5x^3 + y^5x^2 + y^5x^1 + y^5$$

d.) What is the degree of the generator polynomial of the code and what is the coefficient of its largest power?

Solution:

a.) $n=q\text{-}1=7$ $\quad t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = 2 \quad d_{\min} = n - k + 1 = 5 \quad k=3$

b.) The parity check polynomial is given as

$$h(x) = \prod_{i=n-k+1}^{n} \left(x - y^i\right) = \left(x - y^5\right)(x - y^6)(x - y^7) =$$

$$= \left(x - y^5\right)(x - y^6)(x-1) = \left(x - y^5\right)\left(x^2 + y^2x + y^6\right) =$$

$$= x^3 + y^5x^2 + y^2x^2 + x + y^6x + y^4 = x^3 + y^3x^2 + y^2x + y^4$$

c.) If he received polynomial is

$v(x) = y^5x^6 + y^5x^5 + y^5x^4 + y^5x^3 + y^5x^2 + y^5x + y^5$ then the received vector is all one $\mathbf{v} = \left(111\ \ 111\ \ 111\ \ 111\ \ 111\ \ 111\ \ 111\right)$.

d.) The degree of the generator polynomial is $n\text{-}k$=4,
since it is a main polynomial therefore the coefficient of the largest power is 1.

Problem 5

Give the generator polynomial of the cyclic RS code capable of correcting every single error!

Solution:
the code parameters:

$$t = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor = 1 \rightarrow n-k=2; n = 2^m - 1 \rightarrow n = 3; k = 1; m = 2$$

Over GF(4) the irreducible polynomial is $P(y) = y^2 + y + 1$,
and the power table is:

$y^0 \rightarrow 1;$

$y^1 \rightarrow y$

$y^2 \rightarrow y+1$

The generator polynomial is the following:

$$g(x) = \prod_{i=1}^{n-k} \left(x - y^i\right) = \left(x-y\right)\left(x-y^2\right) = \left(x+y\right)\left(x+y^2\right) = x^2 + \left(y+y^2\right)x + y^3 = x^2 + x + 1$$

Problem 6

Given a cyclic code over GF(8) with the generator polynomial: $g(x)=x^3+y^6x^2+yx+y^6$

a) What are the code parameters?

b) Give the code word belonging to the message vector. The components of the code word are all 1-s in binary form (the code word is supposed to be given also in binary form)

c) Can this code be an RS code?

Solution:

a) $n=q-1=7,\quad \deg\left(g(x)\right)=n-k=3 \quad \to C(7,4)$

b)

$$c(x)=g(x)u(x)=\left(x^3+y^6x^2+yx+y^6\right)\left(y^5x^3+y^5x^2+y^5x+y^5\right)=$$

$$=y^5x^6+y^4x^5+y^6x^4+y^4x^3++y^5x^5+y^4x^4+y^6x^3+y^4x^2++y^5x^4+y^4x^3+y^6x^2+y^4x++y^5x^3+y^4x^2+y^6x+y^4=$$

$$=y^5x^6+x^5+y^2x^4+yx^3+y^6x^2+y^3x+y^4$$

Using the power table:

poly	binary	decimal	power			
1	001	1	1	7	14	21
y	010	2	y	8	15	22
y^2	100	4	y^2	9	16	23
$y+1$	011	3	y^3	10	17	24
y^2+y	110	6	y^4	11	18	25
y^2+y+1	111	7	y^5	12	19	26
y^2+1	101	5	y^6	13	20	27

$$c(x)=\ y^5x^6+1\cdot x^5+y^2x^4+yx^3+y^6x^2+y^3x+y^4$$

$$\downarrow\quad\downarrow\quad\downarrow\quad\downarrow\quad\downarrow\quad\downarrow\quad\downarrow\quad\downarrow$$

$$\mathbf{c}\ =(111,\ 001,\ 100,\ 010,\ 101,\ 011,\ 110)$$

c) it can be, because:

$$g(x)=(x-y)\left(x-y^2\right)\left(x-y^3\right)=\left(x^2+y^4x+y^3\right)\left(x-y^3\right)=x^3+y^4x^2+y^3x+y^3x^2+x+y^6=$$

$$=x^3+y^6x^2+yx+y^6$$

Problem 7

We have a cyclic RS code with parameters C(7,2)

a) Give the appropriate field parameter $GF(p)$
b) How many errors can we detect and correct with this code?
c) Give the generator polynomial $g(x)$
d) Give the parity check polynomial $h(x)$
e) We observe a received vector represented in the decimal form $\mathbf{v} = (0,1,4,3,5,6,2)$ can this be a codeword?
f) We observe a received vector represented in the decimal form $\mathbf{v} = (0,1,4,2,5,6,2)$ what is the detected error vector?

Solution

a) $p = n+1 = 7+1 = 8 = 2^3$ we are in $GF(8)$
b) We know that an RS code is MDS, so $n-k+1 = d_{\min}$ we can detect $l = d_{\min} - 1$ errors, and $t = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor$ errors can be corrected $d_{\min} = 7-2+1 = 6$, $l = 5, t = 2$
c) the power table over $GF(8)$ if $P(y) = y^3 + y + 1$ is

poly	binary	decimal	power			
1	001	1	1	7	14	21
y	010	2	y	8	15	22
y^2	100	4	y^2	9	16	23
$y+1$	011	3	y^3	10	17	24
y^2+y	110	6	y^4	11	18	25
y^2+y+1	111	7	y^5	12	19	26
y^2+1	101	5	y^6	13	20	27

$$g(x) = \prod_{i=1}^{n-k} (x - y^i) = (x-1)(x-y^2)(x-y^3)(x-y^4)(x-y^5) =$$

since we are in $GF(2^3)$ the subtraction and the addition is the same, because the small field has $\bmod 2$ arithmetic

$$g(x) = \prod_{i=1}^{n-k} (x - y^i) = (x-1)(x-y^2)(x-y^3)(x-y^4)(x-y^5) =$$

$$= (x^2 + y^2x + x + y^2)(x^2 + y^4x + y^3x + y^7)(x + y^5) =$$

$$= (x^2 + y^6x + y^2)(x^2 + y^6x + 1)(x + y^5) =$$

$$= (x^4 + y^6x^3 + x^2 + y^6x^3 + y^{12}x^2 + y^6x + y^2x^2 + y^8x + y^2)(x + y^5) =$$

$$= (x^4 + (y^6 + y^6)x^3 + (1 + y^{12} + y^2)x^2 + y^6x + y^2)(x + y^5) =$$

$$= \ldots$$

d) $h(x)=\prod_{i=n-k+1}^{n}(x-y^i)=(x-y^6)(x-y^7)=x^2+(y^6+1)x+y^6y^7=x^2+y^2x+y^6$

e) If the received vector in decimal form is $\mathbf{v}=(0,1,4,3,5,6,2)$

then it is in binary form and polynomial form is:

$\mathbf{v}=(000,001,100,011,101,110,010)$

$v(x)=0x^6+1x^5+y^2x^4+y^3x^3+y^6x^2+y^4x+y$

or

$v(x)=0+1x+y^2x^2+y^3x^3+y^6x^4+y^4x^5+yx^6$

it depends on how we define the 0^{th} component of $\mathbf{v}$

We know that both $g(x),h(x)$ divided x^n-1 without a remainder so if

$h(x)v(x)\bmod(x^n-1)=0$ then $v(x)$ is a codeword polynomial

this is true, because $g(x)h(x)=x^n-1$

$v(x)=g(x)u(x)+e(x),$

$h(x)v(x)\bmod x^n-1=$

$(h(x)g(x)u(x)+h(x)e(x))\bmod x^n-1=$

$((x^n-1)u(x)+h(x)e(x))\bmod x^n-1=$

$\underbrace{(x^n-1)u(x)\bmod(x^n-1)}_{0}+h(x)e(x)\bmod(x^n-1)=$

$=h(x)e(x)\bmod(x^n-1)$

if $v(x)$ is a codeword polynomial, then this should be 0 as well.

We test this equality:

$h(x)v(x)=(x^2+y^2x+y^6)(0x^6+1x^5+y^2x^4+y^3x^3+y^6x^2+y^4x+y)=$

$=0x^8+1x^7+y^2x^6+y^3x^5+y^6x^4+y^4x^3+yx^2+$

$+(0\cdot y^2)x^7+(1\cdot y^2)x^6+(y^2\cdot y^2)x^5+(y^3\cdot y^2)x^4+(y^6\cdot y^2)x^3+(y^4\cdot y^2)x^2+(y\cdot y^2)x+$

$+(0\cdot y^6)x^6+(1\cdot y^6)x^5+(y^2\cdot y^6)x^4+(y^3\cdot y^6)x^3+(y^6\cdot y^6)x^2+(y^4\cdot y^6)x+(y\cdot y^6)=$

$=0x^8+(1+0y^2)x^7+(y^2+y^2+0y^6)x^6+(y^3+y^4+y^6)x^5+$

$+(y^6+y^5+y^8)x^4+(y^4+y^8+y^9)x^3+(y+y^6+y^{12})x^2+(y^3+y^{10})x+y^7=$

$=x^7+1=x^7-1$

$x^7-1\bmod x^7-1=0$

or it can be computer for the other direction as well

$h(x)v(x)=(x^2+y^2x+y^6)(0+1x+y^2x^2+y^3x^3+y^6x^4+y^4x^5+yx^6)$