HW3

November 14, 2024

1 Homework 3 - Naiara Alonso Montes

1.1 Problem 1

1.1.1 Write down the generator polynomial and its corresponding check polynomial.

Acording to the matrix:

$$g(x) = 1 + x^2 + x^3$$

The check polynomial is:

$$h(x) = \frac{x^n - 1}{g(x)}$$

Where n is equal to 7, so

$$h(x) = \frac{x^7 - 1}{x^3 + x^2 + 1} = x^4 + x^3 + x^2 + 1$$

1.1.2 Find the code rate, length and minimum distance

Code rate: $\frac{k}{n} = \frac{4}{7}$

Code legth is $n = 2^{deg(g(x))} - 1 = 2^3 - 1 = 7$

Minimum distance, as $g(x)$ has 3 terms, $d \leq 3$

1.1.3 Write down the parity check matrix of the code

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \tag{1}$$

1.1.4 Compare the code parameters with the Griesmer bound

$d_G \rightarrow n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil$

d	d_G
0	0

d	d_G
1	4
2	5
3	7
4	8

$d_G = 7$ (on the original solution I missmatched concepts)

1.2 Problem 2

1.2.1 For the extension field $GF(2^5)$ constructed by using primitive polynomial $x^5 + x^2+1$ (see Homework assigment 2) find minimal polynomial for α^3 and α^5, where α is primitive element.

Case α^3

$$(x+\alpha^3)(x+\alpha^6)(x+\alpha^{12})(x+\alpha^{24})(x+\alpha^{17})$$
$$(x^2+\alpha^1 x+\alpha^9)(x^2+\alpha^4 x+\alpha^5)(x+\alpha^{17})$$
$$x^5+x^4+x^3+x^2+1$$

Case α^5

$$(x+\alpha^5)(x+\alpha^{10})(x+\alpha^{20})(x+\alpha^9)(x+\alpha^{18})$$
$$(x^2+\alpha^7 x+\alpha^{15})(x^2+\alpha^{28} x+\alpha^{29})(x+\alpha^{18})$$
$$x^5+x^4+x^2+x+1$$

1.3 Problem 3

1.3.1 A BCH code of length 31 correcting 2 errors is used for transmitting messages. The primitive polynomial $p(x) = x^5 + x^2 + 1$ was used for constructing the code. At the output we observe the sequence $y = 0101000001110101010011001111000$ (the smallest degree is the first). Find the decoded codeword.

$GF(2^5), t = 2$

$g(x) = m_1(x)m_{2t-1}(x) = m_1(x)m_3(x)$

$b(x) = x + x^3 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} + x^{17} + x^{20} + x^{21} + x^{24} + x^{25} + x^{26} + x^{27}$

$s_1 = \alpha + \alpha^3 + \alpha^9 + \alpha^{10} + \alpha^{11} + \alpha^{13} + \alpha^{15} + \alpha^{17} + \alpha^{20} + \alpha^{21} + \alpha^{24} + \alpha^{25} + \alpha^{26} + \alpha^{27} = \alpha^25$

$s_3 = \alpha^3 + \alpha^9 + \alpha^{27} + \alpha^{30} + \alpha^2 + \alpha^8 + \alpha^{14} + \alpha^{20} + \alpha^{29} + \alpha + \alpha^{10} + \alpha^{13} + \alpha^{16} + \alpha^{19} = \alpha^3$

$$\begin{cases} s_1 = \alpha^i + \alpha^j \\ s_3 = \alpha^{3i} + \alpha^{3j} \end{cases}$$

$\alpha^i = x_1, a^j = x_2$

$$\begin{cases} x_1 + x_2 = \alpha^{25} \\ x_1^3 + x_2^3 = \alpha^3 \end{cases}$$

$(x_1 + x_2)^2 = S_1^2$

$(x_1^3 + x_2^3)/(x_1 + x_2) = x_1^2 + x_2^2 + x_1x_2 = s_2^2 + x_1x_2$

$$\begin{cases} x_1 + x_2 = \alpha^{25} \\ x_1x_2 = s_3/s_1 - s_1^2 \end{cases}$$

$$\begin{cases} x_1 + x_2 = \alpha^{25} \\ x_1x_2 = \alpha^3/\alpha^{25} + \alpha^{19} = \alpha^{13} \end{cases}$$

$x^2 + \alpha^{25}x + \alpha^{13} = 0$

Now I will substitue x with α^0 to α^{30} to find the roots of the polynomial.

The roots are α^{21} and α^{23} and its inversese α^{10} and α^8 respectively. The errors are in position 10 and 8, the decoded codeword is then:

$c = 01010000110101010100011001111000$

1.4 Problem 4

1.4.1 Find the generator polynomial of the length $n = 31$ of primitive BCH code correcting 3 errors.

$t = d - 1 \Rightarrow 3 = d - 1 \Rightarrow d = 4$

Find primitive of field:

$2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 16, 2^5 = 1$

$3^1 = 3, 3^2 = 9, 3^3 = 27, 3^4 = 19, 3^5 = 26, 3^6 = 16, 3^7 = 17, 3^8 = 20, 3^9 = 29, 3^{10} = 25,$

$3^{11} = 13, 3^{12} = 8, 3^{13} = 24, 3^{14} = 10, 3^{15} = 30, 3^{16} = 28, 3^{17} = 22, 3^{18} = 4, 3^{19} = 12, 3^{20} = 5,$

$3^{21} = 15, 3^{22} = 14, 3^{23} = 11, 3^{24} = 2, 3^{25} = 6, 3^{26} = 18, 3^{27} = 23, 3^{28} = 7, 3^{29} = 21, 3^{30} = 1$

3 is primitive of field

$g(x) = (x - \alpha^3)(x - \alpha^9)(x - \alpha^{27}) = x^3 + \alpha^{25}x^2 + \alpha^{25}x + \alpha^8$

1.4.2 The number $2^m - 1, m = 10$ can be factorized as 1023=33$\times$31. Let $n = 33$, find cyclotonic classes of modulo n

$C_0 = \{0\}, m = 10$

$C_1 = \{1, 2, 4, 8, 16, 32, 31, 29, 25, 17\}, m = 10$

$C_2 = \{3, 6, 12, 24, 15, 30, 27, 21, 9, 18\}, m = 10$

$C_5 = \{5, 10, 20, 7, 14, 28, 23, 13, 26, 19\}, m = 10$

$C_{11} = \{11, 22\}, m = 2$

1.4.3 Find parameters of BCH code of length $n = 33$ (dimesion, design distance) with generator polynomial $g(x) = m_1(x)m_3(x)$, where $m_i(x)$ is minimal polynomial of $\beta = \alpha^{31}$ in GF(2^{10}), α is a primitive element of GF(2^{10})

Powers	$g(x)$	$k = n - deg(g(x))$	Distance
1, 2, 3, 4 // 29, 30, 31, 32	$m_1(x)m_3(x)$	33 - 20 = 13	5

1.5 Problem 5

1.5.1 Construct a generator polynomial of the RS-code over GF(2^3) modulo $p(x) = x^3 + x + 1$ correcting 2 errors

Length $n = q - 1 = 8 - 1 = 7$

Distance $d = 2t + 1 = 2 \times 2 + 1 = 5$

$b = 1$

$g(x) = m_b(x)m_{b+1}()...m_{b+d-2}(x) =$

$m_1(x)m_2(x)m_3(x)m_4(x) =$

$(x - ^1)(x - ^2)(x - ^3)(x - ^4) =$

$(x^2 + ^4x + ^{3)(x}2 + ^6x + ^0) =$

$g(x) = x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$

1.5.2 Find the code rate, length, and minimum distance of the RS code

Length: 7

$k = -d + n + 1 = -5 + 7 + 1 = 3$

Code rate: $\frac{k}{n} = \frac{3}{7}$

Distance $ d = 5$

1.5.3 Write down the parity-check matrix of the RS code

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \end{pmatrix} \tag{2}$$

1.5.4 Write down the generator matrix of the RS code

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{3}$$

[1]:
```
!jupyter nbconvert --to pdf HW3.ipynb
```

```
[NbConvertApp] Converting notebook HW3.ipynb to pdf
[NbConvertApp] Writing 31237 bytes to notebook.tex
[NbConvertApp] Building PDF
[NbConvertApp] Running xelatex 3 times: ['xelatex', 'notebook.tex', '-quiet']
[NbConvertApp] CRITICAL | xelatex failed: ['xelatex', 'notebook.tex', '-quiet']
b"This is XeTeX, Version 3.141592653-2.6-0.999995 (TeX Live 2023/Debian)
```