Quiz 8
Algebraic Coding Theory
Math 525
Stephen Giang RedID: 823184070

Problem 1: Consider the Galois field $GF(2^4)$ constructed from the primitive polynomial $p(x) = x^4 + x^3 + 1$. Let β be a root of $p(x)$, that is, $p(\beta) = 0$. The table below displays the word and respective power of β representations of each field element except for four of them. The entries in red, namely, (a), (b), (c), and (d) are missing and you are asked to determine them.

word	power of β
0000	
1000	β^0
0100	β^1
0010	β^2
0001	β^3
(a)	β^4
1101	β^5
1111	β^6
1110	β^7
0111	β^8
(b)	β^9
0101	β^{10}
1011	β^{11}
(c)	β^{12}
0110	β^{13}
(d)	β^{14}

(1) Determine the missing entries of the table, that is, the word rep-resentations of $\beta^4, \beta^9, \beta^{12}$, and β^{14}.

(a) Notice the following for β^4:

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

Thus we get $\boldsymbol{(a) = 1001}$

(b) Notice the following for β^9:

$$(1 + x^2) \bmod p(x) = x^9 \bmod p(x)$$

Thus we get $\boldsymbol{(b) = 1010}$

(c) Notice the following for β^{12}:

$$(1 + x) \bmod p(x) = x^{12} \bmod p(x)$$

Thus we get $\boldsymbol{(c) = 1100}$

(d) Notice the following for β^{14}:

$$(x^2 + x^3) \bmod p(x) = x^{14} \bmod p(x)$$

Thus we get $\boldsymbol{(d) = 0011}$

(2) Calculate the minimal polynomials of β^7 and β^{13}. Express each answer as a polynomial with binary coefficients.

Notice the following:

$$\boldsymbol{\beta^7} \quad \Rightarrow \quad (\beta^7)^2 = \boldsymbol{\beta^{14}} \quad \Rightarrow \quad (\beta^1 4)^2 = \beta^{28} = \boldsymbol{\beta^{13}} \quad \Rightarrow \quad (\beta^{13})^2 = \beta^{26} = \boldsymbol{\beta^{11}}$$
$$\Rightarrow \quad (\beta^{11})^2 = \beta^{22} = \beta^7$$

Now we can calculate the minimal polynomial:

$$\begin{aligned} m_\alpha(x) &= (x + \beta^7)(x + \beta^{14})(x + \beta^{13})(x + \beta^{11}) \\ &= \left(x^2 + (\beta^7 + \beta^{14})x + \beta^{21}\right)\left(x^2 + (\beta^{13} + \beta^{11})x + \beta^{24}\right) \\ &= \left(x^2 + \beta^5 x + \beta^6\right)\left(x^2 + \beta^5 x + \beta^9\right) \\ &= x^4 + (\beta^5 + \beta^5)x^3 + (\beta^9 + \beta^{10} + \beta^6)x^2 + (\beta^{14} + \beta^{11})x + \beta^{15} \\ &= \boldsymbol{x^4 + x + 1} \end{aligned}$$

(3) Calculate $r(\beta^{12})$ where $r(x) = x^5 + x^4 + x^3 + 1$. Your answer must be represented as either 0 or a power of β(e.g.,β^5, β^9, etc.).

Notice the following:

$$\begin{aligned} r(\beta^{12}) &= (\beta^{12})^5 + (\beta^{12})^4 + (\beta^{12})^3 + 1 \\ &= \beta^{60} + \beta^{48} + \beta^{36} + 1 \\ &= \beta^3 + \beta^6 + 1 \\ &= \boldsymbol{\beta^{13}} \end{aligned}$$