Math 601 Homework Assignment #11 Due Wednesday, April 18, 2018

Write up and hand in solutions to the following exercises. You must give complete justification for all answers. Assume all polynomials are in $\mathbf{F}[x]$.

1. Table 1 shows the elements of the field $\mathbf{F}[x]/(1+x+x^3)$. Make a similar table for the field $\mathbf{F}[x]/(1+x^2+x^3)$.

2. Find the minimal polynomials for all the elements of $\mathbf{F}[x]/(1+x^2+x^3)$.

3. Table 2 shows the elements of the field $K = \mathbf{F}[x]/(1+x^3+x^4)$, except with some entries left out.

   (a) Fill in the rest of Table 2.

   (b) Find the minimal polynomials for β and β^3 in K.

   (c) Find a (transposed) parity-check matrix for the 2-error-correcting BCH code of length 15 using this field.

   (d) What is the generator polynomial for the code in (c)?

4. Table 3 shows the elements of the field $K = \mathbf{F}[x]/(1+x+x^4)$. Let C be the 2-error-correcting BCH code of length 15 using this field. C has generator polynomial $m_\beta(x)m_{\beta^3}(x) = (1+x+x^4)(1+x+x^2+x^3+x^4) = 1+x^4+x^6+x^7+x^8$. A (transposed) parity-check matrix for C is given in Figure 1 below. Decode the following received words.

   (a) 01000 10101 00000

   (b) 11011 11010 11000

Extra credit:

1. Let $g(x)$ be the generator polynomial for a cyclic Hamming code with parameters $[2^r-1, 2^r-r-1, 3]_2$. Prove that $(x+1)g(x)$ is the generator polynomial for a linear cyclic code with parameters $[2^r-1, 2^r-r-2, d]_2$ for some $d \geq 4$. (Can you prove $d = 4$?)

2. Prove: Let $K = \mathbf{F}[x]/(g(x))$ and $\alpha \in K$. $m_\alpha(x)$ is a primitive polynomial if and only if α is a primitive element of K.

power of β		polynomial in x	word
-		0	000
β^0		1	100
β^1		x	010
β^2		x^2	001
β^3	$(x^3 \bmod g(x) = 1 + x)$	$1 + x$	110
β^4	$(x^4 \bmod g(x) = x + x^2)$	$x + x^2$	011
β^5	$(x^5 \bmod g(x) = 1 + x + x^2)$	$1 + x + x^2$	111
β^6	$(x^6 \bmod g(x) = 1 + x^2)$	$1 + x^2$	101

Table 1: $\mathbf{F}[x]/(1 + x + x^3)$

power of β	polynomial in x	word
-	0	0000
β^0	1	1000
β^1	x	0100
β^2	x^2	0010
β^3	x^3	0001
β^4		
β^5	$1 + x + x^3$	1101
β^6	$1 + x + x^2 + x^3$	1111
β^7	$1 + x + x^2$	1110
β^8		
β^9	$1 + x^2$	1010
β^{10}	$x + x^3$	0101
β^{11}	$1 + x^2 + x^3$	1011
β^{12}		
β^{13}		
β^{14}	$x^2 + x^3$	0011

Table 2: $\mathbf{F}[x]/(1 + x^3 + x^4)$

power of β	polynomial in x	word
-	0	0000
β^0	1	1000
β^1	x	0100
β^2	x^2	0010
β^3	x^3	0001
β^4	$1+x$	1100
β^5	$x+x^2$	0110
β^6	x^2+x^3	0011
β^7	$1+x+x^3$	1101
β^8	$1+x^2$	1010
β^9	$x+x^3$	0101
β^{10}	$1+x+x^2$	1110
β^{11}	$x+x^2+x^3$	0111
β^{12}	$1+x+x^2+x^3$	1111
β^{13}	$1+x^2+x^3$	1011
β^{14}	$1+x^3$	1001

Table 3: $\mathbf{F}[x]/(1+x+x^4)$

$$H^T = \begin{bmatrix} 1000 & 1000 \\ 0100 & 0001 \\ 0010 & 0011 \\ 0001 & 0101 \\ 1100 & 1111 \\ 0110 & 1000 \\ 0011 & 0001 \\ 1101 & 0011 \\ 1010 & 0101 \\ 0101 & 1111 \\ 1110 & 1000 \\ 0111 & 0001 \\ 1111 & 0011 \\ 1011 & 0101 \\ 1001 & 1111 \end{bmatrix}$$

Figure 1: Transposed parity-check matrix for the BCH 2-error-correcting code constructed from the field in Table 3.