Math 601 Homework Assignment #12 Due Wednesday, April 25, 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. Consider the field $K = \mathbf{F}[x]/(1+x+x^4)$, shown in Table 3 of Homework #11.
   (a) On Homework #11, I identified the following minimal polynomials for this field: $m_\beta(y) = (1+y+y^4)$ and $m_{\beta^3}(y) = (1+y+y^2+y^3+y^4)$. Find the mimimal polynomial of β^5. (Hint: first determine its degree—then it is easy.)
   (b) Write a transposed parity-check matrix for a 3-error-correcting BCH code of length 15.

2. Let C be the cyclic code of length 7 with generator polynomial $g(x) = 1 + x + x^2 + x^4$.
   (a) Give a (transposed) parity check matrix for C. (Recommended: use the matrix with entries $x^k \bmod g(x)$.)
   (b) From H^T in (a), find a codeword of weight 4.
   (c) Use your answer in (b) to find two vectors v and w in $\mathbf{F}^7$ such that
      i. v and w are in the same coset (have the same syndrome).
      ii. v has weight 2 and cyclic burst length 2.
      iii. w has weight 2 but cyclic burst length greater than 2.

      Note: This shows C is not 2-error-correcting.
   (d) Find the syndromes of all words in $\mathbf{F}^7$ of cyclic burst length at most 2. Conclude that C is 2-cyclic-burst-error-correcting.

3. Show that if C is a 3-cyclic-burst-error-correcting code of length 8, then $\dim(C) \leq 5$.

4. $g(x) = 1 + x + x^2 + x^3 + x^6$ generates a 3-cyclic-burst-error-correcting linear cyclic code C of length 15. Decode the received word $w = 00000\ 01111\ 10000$.

Extra credit:

1. Prove: Let $g(x)$ be a primitive polynomial of degree $r \geq 3$, and let $\beta = x \bmod g(x)$. Prove the minimal polynomial m_{β^3} of β^3 has degree r. (I said part of why this is true in class; here I am asking you to supply the details.).

2. Prove: If C is an ℓ-burst-error-correcting linear code of length n and dimension k, then $\ell \leq (n-k)/2$. Hint: Show that any error pattern with burst length 2ℓ can be written as the sum of two error patterns e_1 and e_2, each with burst length at most ℓ. Show that $e_1 + e_2$ is not a codeword, and argue from there.