C&O 331: Assignment #5

Due date: Not to be handed in

---

1. Let C be a binary (n,k)-cyclic code with generator polynomial $g(x) = (x+1)p(x)$, where $p(x)$ does not divide $x^t - 1$ for any t, $1 \le t \le n-1$. An error pattern of the form $e(x) = x^i + x^{i+1}$ $(0 \le i \le n-1)$ is called a *double-adjacent* error pattern.

   (a) Prove that no two double-adjacent error patterns can be in the same coset of a standard array for C.

   (b) Prove that C corrects all single errors and all double-adjacent errors.

   (c) Construct a generator polynomial for a binary $(15,10)$-cyclic code which corrects all single errors and all double-adjacent error patterns.

2. Consider $GF(3^3)$ generated by $f(x) = 1 - x + x^3$ over $GF(3)$.

   (a) Prove that $\beta = x^2$ has order 13 in $GF(3^3)$.

   (b) Determine the cyclotomic cosets of 3 modulo 13.

   (c) Use (a) and (b) to factor $y^{13} - 1$ into irreducible monic polynomials over GF(3).

3. Consider the finite field $GF(2^5) = \mathbb{Z}_2[x]/(x^5 + x^2 + 1)$. Then $\alpha = x$ is a generator of $GF(2^5)$. We have the following minimal polynomials:

   $m_0(y) = y$ $\qquad m_{\alpha^5}(y) = 1 + y + y^2 + y^4 + y^5$

   $m_1(y) = 1 + y$ $\qquad m_{\alpha^7}(y) = 1 + y + y^2 + y^3 + y^5$

   $m_\alpha(y) = 1 + y^2 + y^5$ $\qquad m_{\alpha^{11}}(y) = 1 + y + y^3 + y^4 + y^5$

   $m_{\alpha^3}(y) = 1 + y^2 + y^3 + y^4 + y^5$ $\qquad m_{\alpha^{15}}(y) = 1 + y^3 + y^5.$

   Construct a generator polynomial for a binary $(31,11)$-cyclic code which has designed distance 11.

4. Recall that C_{15} is a (15,7)-BCH code over $GF(2)$ with designed distance 5 generated by $g(x) = m_\beta(x)m_{\beta^3}(x)$, where $\beta = y$ is an element of order 15 in $GF(2^4) = \mathbb{Z}_2[y]/(y^4 + y + 1)$. Decode the received word $r = (00101\ 11000\ 11101)$ using C_{15}.

Solutions will be available on the course web site on April 2.