C&O 331: Assignment #5 solutions

---

1. (a) Let $x^i + x^{i+1}$ and $x^j + x^{j+1}$ be two double-adjacent error patterns with $i < j$. If these are in the same coset of C, then $g(x) \mid (x^i + x^{i+1} + x^j + x^{j+1})$. But

$$x^i + x^{i+1} + x^j + x^{j+1} \;=\; x^i(1+x) + x^j(1+x) \;=\; (1+x)x^i(1+x^{j-i}).$$

Since $g(x) \mid (x^n - 1)$, then $\gcd(g(x), x) = 1$, and hence $\gcd(p(x), x) = 1$. If $g(x) \mid (1+x)x^i(1+x^{j-i})$, then $p(x) \mid (1+x^{j-i})$, which contradicts the hypothesis that $p(x)$ does not divide $x^t - 1$ for any t, $1 \le t \le n-1$. Hence, no two distinct double-adjacent error patterns are in the same coset of C.

(b) We need to prove (i) that no two single error patterns are in the same coset; and (ii) that no single and double-adjacent error patterns are in the same coset.
For (i), observe that if $g(x) \mid (x^i + x^j)$ (where $i < j$), then $g(x) \mid x^i(1 + x^{j-i})$. This implies that $p(x) \mid (1 + x^{j-i})$, which is false.
For (ii), observe that if $g(x) \mid (x^i + x^j + x^{j+1})$, then $(1+x) \mid (x^i + x^j(x+1))$, whence $(1+x) \mid x^i$, which is impossible.

(c) $g(x) = (1+x)(1+x+x^4)$. Also, $g(x) = (1+x)(1+x^3+x^4)$.

2. (a) Some positive powers of β are:

$\beta = x^2$	$\beta^9 = 1 - x + x^2$
$\beta^2 = -x + x^2$	$\beta^{10} = 1 + x - x^2$
$\beta^4 = -1 - x^2$	$\beta^{12} = 1 - x - x^2$
$\beta^8 = 1 - x$	$\beta^{13} = 1.$

Since the divisors of 26 are 1, 2, 13 and 26, and $\beta \neq 1$, $\beta^2 \neq 1$, but $\beta^{13} = 1$, the order of β is 13.

(b) The cyclotomic cosets of 3 modulo 13 are:

$$\{0\}, \quad \{1,3,9\}, \quad \{2,6,5\}, \quad \{4,12,10\}, \quad \{7,8,11\}.$$

(c) The cyclotomic cosets $\{1,3,9\}$ and $\{4,12,10\}$ correspond to cubic irreducible polynomials over $GF(3)$ that are reciprocals of each other. A similar statement holds for the cosets $\{2,6,5\}$ and $\{7,8,11\}$.
We first compute

$$\begin{aligned} g_1(y) &= (y-\beta)(y-\beta^3)(y-\beta^9) \\ &= y^3 - (\beta + \beta^3 + \beta^9)y^2 + (\beta^4 + \beta^{10} + \beta^{12})y - \beta^{13} \\ &= y^3 + y^2 + y - 1. \end{aligned}$$

We next compute $g_2(y) = (y-\beta^2)(y-\beta^5)(y-\beta^6) = y^3 - y - 1$. Thus

$$y^{13} - 1 = (y-1)(y^3+y^2+y-1)(y^3-y^2-y-1)(y^3+y^2-1)(y^3-y-1).$$

3. The cyclotomic cosets of 2 modulo 31 are:

$$C_0 = \{0\}, \quad C_1 = \{1,2,4,8,16\}, \quad C_3 = \{3,6,12,24,17\}, \quad C_5 = \{5,10,20,9,18\}$$

$$C_7 = \{7, 14, 28, 25, 19\}, \quad C_{11} = \{11, 22, 13, 26, 21\}, \quad C_{15} = \{15, 30, 29, 27, 23\}.$$

The set $C_1 \cup C_3 \cup C_5 \cup C_7$ contains the elements 1 to 10, and has cardinality 20. Hence

$$\begin{aligned} g(x) &= m_\alpha(x) m_{\alpha^3}(x) m_{\alpha^5}(x) m_{\alpha^7}(x) \\ &= 1 + x^2 + x^4 + x^6 + x^7 + x^9 + x^{10} + x^{13} + x^{17} + x^{18} + x^{20} \end{aligned}$$

is a generator polynomial for the required code.

4. We have $r(x) = x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11} + x^{12} + x^{14}$.

   - We compute
   $$s_1 = r(\beta) = \beta^2 + \beta^4 + \beta^5 + \beta^6 + \beta^{10} + \beta^{11} + \beta^{12} + \beta^{14} = \beta$$
   $$s_3 = r(\beta^3) = \beta^6 + \beta^{12} + 1 + \beta^3 + 1 + \beta^3 + \beta^6 + \beta^{12} = 0.$$
   - We compute the error locator polynomial
   $$\sigma(z) = z^2 + s_1 z + \frac{s_3}{s_1} + s_1^2 = z^2 + \beta z + \beta^2.$$
   Since the roots are β^i and β^j with $\beta^i \beta^j = \beta^2$, we have $i + j \equiv 2 \pmod{15}$. So, check if $\beta^i + \beta^j = \beta$ for $(i, j) \in \{(0, 2), (3, 14), (4, 13), (5, 12), (6, 11), (7, 10), (8, 9)\}$. We find that $\beta^6 + \beta^{11} = \beta$. Thus
   - Thus $e = (00000\ 01000\ 01000)$, and r is corrected to $c = (00101\ 10000\ 10101)$.