Error-Correcting Codes: Solutions #5

Alfred Menezes (cryptography101.ca)

---

1. Since $\alpha \in GF(q^m)^*$, we have $\alpha^{q^m-1} = 1$ (by Fermat's Little Theorem for finite fields). Thus, α is a root of the polynomial $y^{q^m-1} - 1 \in GF(q)[y]$. It follows from Property 4) of minimal polynomials (slide 139) that $m_\alpha(y)$ divides $y^{q^m-1} - 1$.

2. (a) The order of $GF(4)^*$ is 3, which is prime. Since $\alpha = x \in GF(4)^*$, and since $\alpha \neq 1$, the order of α is 3. Hence α is a generator of $GF(4)^*$.
   Alternate solution: Computing powers of α, we see that $\alpha^1 = x$, $\alpha^2 = x^2 = x + 1$, and $\alpha^3 = x^2 + x = 1$; so the order of α is 3.

   (b) We check that $u(z) = z^2 + \alpha z + 1$ has no roots in $GF(4)$:

$$\begin{aligned} u(0) &= 1 \neq 0 \\ u(1) &= \alpha \neq 0 \\ u(\alpha) &= \alpha^2 + \alpha^2 + 1 = 1 \neq 0 \\ u(\alpha^2) &= \alpha^4 + \alpha^3 + 1 = \alpha + 1 + 1 = \alpha \neq 0. \end{aligned}$$

   Hence, by the Factor Theorem, $u(z)$ is irreducible over $GF(4)$.

   (c) We compute powers of $\beta = \alpha z$ to confirm that the order of β is 15. (After confirming that $\beta \neq 1$, $\beta^3 \neq 1$ and $\beta^5 \neq 1$, we can conclude that the order of β is 15. Nevertheless, we compute all 15 powers of β because these powers are useful in (d).)

$$\begin{aligned} \beta^1 &= \alpha z \\ \beta^2 &= \alpha^2 z^2 = z + \alpha^2 \\ \beta^3 &= \alpha z^2 + z = \alpha^2 z + \alpha + z = \alpha z + \alpha \\ \beta^4 &= \alpha z + \alpha^2 \\ \beta^5 &= \alpha^2 z^2 + z = \alpha^2 \\ \beta^6 &= z \\ \beta^7 &= \alpha^2 z + z \\ \beta^8 &= z + 1 \\ \beta^9 &= z + \alpha \\ \beta^{10} &= \alpha \\ \beta^{11} &= \alpha^2 z \\ \beta^{12} &= \alpha z + 1 \\ \beta^{13} &= \alpha^2 z + \alpha^2 \\ \beta^{14} &= \alpha^2 z + 1 \\ \beta^{15} &= 1. \end{aligned}$$

   Hence the order of β is 15.

   (d) We have $\gamma = \alpha z + \alpha = \beta^3$. The conjugates of γ with respect to $GF(4)$ are β^3, $(\beta^3)^4 = \beta^{12}$, $(\beta^{12})^4 = \beta^{48} = \beta^3$. So, there are two distinct conjugates, namely β^3 and β^{12}. Hence, the

minimal polynomial of γ over $GF(4)$ is

$$\begin{aligned} m_\gamma(y) &= (y-\beta^3)(y-\beta^{12}) \\ &= y^2+(\beta^3+\beta^{12})y+\beta^{15} \\ &= y^2+(\alpha+1)y+1. \end{aligned}$$

3. (a) Here are the powers of β: $\beta^1 = x^2$, $\beta^2 = x^2+x-1$, $\beta^3 = -x^2+x$, $\beta^4 = x^2-x-1$, $\beta^5 = x^2+x+1$, $\beta^6 = x^2+x$, $\beta^7 = x$, $\beta^8 = -x^2+1$, $\beta^9 = -x+1$, $\beta^{10} = -x^2-1$, $\beta^{11} = x^2-x+1$, $\beta^{12} = x+1$, $\beta^{13} = 1$, which confirms that the order of β is 13.

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

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

Thus, $y^{13}-1$ is a product of five irreducible polynomials over $GF(3)$, one of degree 1, and four of degree 3. We have $m_0(y) = y-1$. We then compute

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

We next compute $m_{\beta^2}(y) = (y-\beta^2)(y-\beta^5)(y-\beta^6) = y^3-y-1$. Similarly, we compute $m_{\beta^4}(y) = y^3+y^2+y-1$ and $m_{\beta^7}(y) = y^3+y^2-1$. Thus,

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

4. The characteristic of $GF(7^2)$ is 7, which divides 735. So, $x^{735}-1 = (x^{15}-1)^{49}$ over $GF(7^2)$ by the Frosh's dream. Let $q = 49$ and $n = 15$. Then the cyclotomic cosets of q modulo n are:

$$C_0 = \{0\} \quad C_1 = \{1,4\} \quad C_2 = \{2,8\} \quad C_3 = \{3,12\} \quad C_5 = \{5\}$$

$$C_6 = \{6,9\} \quad C_7 = \{7,13\} \quad C_{10} = \{10\} \quad C_{11} = \{11,14\}.$$

Thus, $x^{735}-1$ factors over $GF(7^2)$ as $(f_0f_1f_2f_3f_5f_6f_7f_{10}f_{11})^{49}$, where f_0, f_5, f_{10} have degree one, and f_1, f_2, f_3 f_6, f_7, f_{11} are irreducible quadratics. Hence, the number of cyclic subspaces of $V_{735}(GF(7^2))$ is 50^9.

5. Let's look for a BCH code with parameters $q = 7$, $n = 29$, $k = 15$, $\delta = 6$. The cyclotomic cosets of q modulo n are:

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1,7,16,20,23,24,25\} \\ C_2 &= \{2,3,11,14,17,19,21\} \\ C_4 &= \{4,5,6,9,13,22,28\} \\ C_8 &= \{8,10,12,15,18,26,27\}. \end{aligned}$$

The cosets C_1 and C_8 contain $\delta-1 = 5$ consecutive integers, namely 23, 24, 25, 26, 27. Also, the union of C_1 and C_8 has size 14. Thus, the product of the minimal polynomials of β and β^8 over $\mathbb{Z}_7$ (where β is an element of order $n = 29$ in $GF(7^7)$) has degree 14, and generates a $(29,15)$-cyclic code over $\mathbb{Z}_7$ with designed distance 6 (and hence distance at least 6, by the BCH bound).
(The cosets C_2 and C_4 yield the same conclusion.)