Error-Correcting Codes: Solutions #2

Alfred Menezes (cryptography101.ca)

---

1. (a) $q = 7^4$.
   (b) The polynomials in $\mathbb{Z}_7[x]$ of degree less than 4.
   (c) 7.
   (d) $5x^3 + 2x^2 + 5$.
   (e) By the Frosh's dream, $(x+1)^7 = x^7 + 1 = 6x^3 + x^2 + 4x + 3$. Since $2400 = q - 1$, it follows from Fermat's Little Theorem (slide 48) that $(4x^3 + 5x^2 + 6x + 4)^{2400} = 1$. Hence the answer is $6x^3 + x^2 + 4x + 3$.

2. (a) We have $f(x) = 2(x^2 + x + 2)(x^2 + 1)$, so $f(x)$ is reducible over $\mathbb{Z}_3$.
   (b) We have $g(0) = 2$, $g(1) = 1$ and $g(2) = 2$, so $g(x)$ has no linear factors. Now, the monic irreducible quadratics over $\mathbb{Z}_3$ are $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$, neither of which divides $g(x)$. Thus, $g(x)$ has no linear or quadratic factors and so must be irreducible over $\mathbb{Z}_3$.
   Remark. A polynomial $f(x)$ of degree n over a field F is irreducible over F if and only if f has no monic irreducible factors in $F[x]$ of degree at most $n/2$.

3. Since $GF(2^6)$ has order $q = 64$, we need to show that x has order $q - 1 = 63$. We know that the order of a nonzero element in $GF(2^6)^*$ must divide 63, so the order is either 1, 3, 7, 9, 21 or 63.
   Since $x \neq 1$, the order of x is not 1.
   Since $x^3 \neq 1$, the order of x is not 3.
   Since $x^7 = x(x^6 + x + 1) + x^2 + x = x^2 + x \neq 1$, the order of x is not 7.
   Since $x^9 = x^7 \cdot x^2 = x^4 + x^3 \neq 1$, the order of x is not 9.
   Finally, since $x^{21} = (x^7)^3 = (x^2 + x)^3 = x^6 + x^5 + x^4 + x^3 = x^5 + x^4 + x^3 + x + 1 \neq 1$, the order of x is not 21.
   Thus, we can conclude that the order of x is 63.

4. (a) Assume that $\alpha^i = \alpha^j$ for $0 \leq i < j \leq t - 1$. Then $\alpha^{j-i} = 1$. But $0 < j - i \leq t - 1$, which contradicts $\text{ord}(\alpha) = t$. Hence $\alpha^0, \alpha^1, \ldots, \alpha^{t-1}$ are pairwise distinct.
   (b) Let $t = \text{ord}(\alpha)$ and $s = \text{ord}(\alpha^{-1})$. Now,

$$\alpha^s = (\alpha^{-1})^{-s} = \frac{1}{(\alpha^{-1})^s} = \frac{1}{1} = 1.$$

   Hence $t \mid s$. Similarly, $(\alpha^{-1})^t = \alpha^{-t} = 1/\alpha^t = 1/1 = 1$; hence $s \mid t$. We conclude that $t = s$.

5. (a) G is a 4×7 matrix and has rank 4. Hence $n = 7$ and $k = 4$.
   (b) $c = mG = (1101010)$.
   (c) $C^\perp$ has length 7 and dimension 3.
   (d) A generator matrix for C in standard form is:

$$G' = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Hence a parity-check matrix for C is

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

(e) G is a parity-check matrix for $C^{\perp}$.

(f) The columns of H are nonzero, and so $d(C) \geq 2$. Since columns 4 and 5 of H are equal, we have $d(C) = 2$.

(g) C is a 0-error correcting code.

(h) C is a 1-error detecting code.