EE 605: Error Correcting Codes

Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay
Autumn 2011

Solution to Assignment 4

---

1. Let $\mathbb{F}_{16}$ be the field generated by $p(X) = 1 + X + X^4$. Let α be a primitive element of $\mathbb{F}_{16}$ which is a root of $p(X)$. Devise a circuit which is capable of multiplying any element in $\mathbf{F}_{16}$ by α^7.

   Solution: Any element in the field $\mathbb{F}_{16}$ can be represented as $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$. If we multiply this element by α^7, we get the element $a_0\alpha^7 + a_1\alpha^8 + a_2\alpha^9 + a_3\alpha^{10}$. We have the following identities.

   - $\alpha^7 = \alpha^3 + \alpha + 1$
   - $\alpha^8 = \alpha^2 + 1$
   - $\alpha^9 = \alpha^3 + \alpha$
   - $\alpha^{10} = \alpha^2 + \alpha + 1$

   Using these identities, the product can be written as

$$\begin{aligned} a_0\alpha^7 + a_1\alpha^8 + a_2\alpha^9 + a_3\alpha^{10} &= a_0(\alpha^3 + \alpha + 1) + a_1(\alpha^2 + 1) + a_2(\alpha^3 + \alpha) + a_3(\alpha^2 + \alpha + 1) \\ &= a_0 + a_1 + a_3 + (a_0 + a_2 + a_3)\alpha + (a_1 + a_3)\alpha^2 + (a_0 + a_2)\alpha^3 \end{aligned}$$

   The circuit for multiplication by α^7 can be now obtained by taking a register containing a_0, a_1, a_2, a_3 and using XOR gates to obtain $a_0 + a_1 + a_3, a_0 + a_2 + a_3, a_1 + a_3$ and $a_0 + a_2$.

2. Consider a t-error-correcting binary BCH code of length $n = 2^m - 1$. If $2t+1$ is a factor of n, prove that the minimum distance of the code is exactly$2t + 1$. You can assume the BCH bound in your solution ($d_{min} \geq 2t + 1$). (*Hint:* Let $n = l(2t + 1)$. Show that $\frac{X^n+1}{X^l+1}$ is a code polynomial of weight $2t + 1$. Remember that a code polynomial has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ as roots where α is a primitive element of $\mathbb{F}_{2^m}$ which has order $n = 2^m - 1$.)

   Solution: Since the BCH bound gives us $d_{min} \geq 2t + 1$, we will be done if we can show the existence of a codeword whose weight is equal to $2t + 1$. Let $Y = X^l$. The we have the following identities.

$$\begin{aligned} \frac{X^n + 1}{X^l + 1} &= \frac{X^{l(2t+1)} + 1}{X^l + 1} = \frac{Y^{2t+1} + 1}{Y + 1} = 1 + Y + Y^2 + \cdots + Y^{2t} \\ &= 1 + X^l + X^{2l} + \cdots + X^{2tl} \end{aligned}$$

   So we can see that $c(X) = \frac{X^n+1}{X^l+1}$ is a polynomial of weight $2t + 1$. We have

$$c(\alpha) = \frac{\alpha^n + 1}{\alpha^l + 1} = \frac{1 + 1}{\alpha^l + 1} = 0.$$

The above calculation is valid since the denominator $\alpha^l + 1 \neq 0$ due to the fact that $l < n = 2^m - 1$ and α has order $2^m - 1$ (note that $t \geq 1$). Similarly, we get

$$c(\alpha^i) = \frac{\alpha^{ni} + 1}{\alpha^{li} + 1} = \frac{1 + 1}{\alpha^{li} + 1} = 0$$

for $i = 2, 3, \ldots, 2t$ since $2tl < n$. Hence $c(X)$ is a codeword of weight $2t + 1$.

3. Prove that the dual of a Reed-Solomon code is a Reed-Solomon code. (*Hint*: The dual code of an (n, k) cyclic code with generator polynomial $g(X)$ has generator polynomial $X^k h(X^{-1})$ where $h(X) = \frac{X^n - 1}{g(X)}$.)

   Solution: Consider a t-error correcting Reed-Solomon code over a field $\mathbb{F}_q$. Then the length of the codewords is $n = q-1$. It has a generator polynomial $g(X) = \prod_{i=1}^{2t}(X - \alpha^i)$ where α is a primitive element of $\mathbb{F}_q$. In any field $X^{q-1} - 1 = \prod_{i=0}^{q-2}(X - \alpha^i)$ and consequently we have

$$h(X) = \frac{X^n - 1}{g(X)} = \frac{X^{q-1} - 1}{g(X)} = (X - 1) \prod_{i=2t+1}^{q-2} (X - \alpha^i) = \prod_{i=2t+1}^{q-1} (X - \alpha^i)$$

   since $\alpha^{q-1} = 1$. Here the degree of $h(X)$ is k (remember that the degree of the generator polynomial of an (n, k) cyclic code is $n-k$). Then the generator polynomial of the dual code is given by

$$X^k h(X^{-1}) = \prod_{i=2t+1}^{q-1} (1 - \alpha^i X).$$

   Since $\alpha^{q-1} = 1$, the generator polynomial of the dual code has roots α^{q-2t-2}, α^{q-2t-1}, …, α^{q-1}. Thus the dual code is a Reed-Solomon code (see comment in Moodle for the definition of a general RS code).

4. Consider a $(2, 1)$ convolutional code with encoder matrix $G(D) = \begin{bmatrix} 1 + D^2 & 1 + D + D^2 + D^3 \end{bmatrix}$.

   (a) Draw the encoder circuit.

   (b) Draw the encoder state diagram.

   (c) Is this encoder catastrophic? If yes, find an infinite weight information sequence which generates a codeword of finite weight.

   Solution: The encoder is catastrophic since the greatest common divisor of the polynomials is $1 + D^2$ which is not of the form D^l. Consider the all ones infinite length information sequence whose polynomial representation is given by $1 + D + D^2 + D^3 + \cdots = \frac{1}{1+D}$. The output corresponding to this input is $v(D) = \frac{1}{1+D} G(D) = \begin{bmatrix} 1 + D & 1 + D^2 \end{bmatrix}$.