Math 525

Sections 5.3–5.5: Cyclic Hamming and BCH Codes

November 30, 2020

Hamming Codes Revisited

- Let $r \geq 2$ be an integer and let $\beta \in \mathrm{GF}(2^r)$ be primitive, i.e., $1, \beta, \beta^2, \ldots, \beta^{2^r-2}$ are all *distinct* and
$$\mathrm{GF}(2^r) = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{2^r-2}\}.$$
- Then
$$H = \begin{bmatrix} 1 \\ \beta \\ \vdots \\ \beta^{2^r-2} \end{bmatrix}$$
is a parity-check matrix of a $(2^r-1, 2^r-r-1, 3)$ Hamming code.
- Let $n = 2^r - 1$. We have:
$$c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \in C \Leftrightarrow$$
$$c_0 + c_1\beta + \cdots + c_{n-1}\beta^{n-1} = 0 \Leftrightarrow c(\beta) = 0 \Leftrightarrow m_\beta(x) \,|\, c(x).$$
- Since $m_\beta(x) \,|\, x^n + 1$, it follows that C is cyclic with $g(x) = m_\beta(x)$.

Decoding: Let $c(x)$ be the sent codeword and $e(x) = x^j$ the error pattern. Then $r(x) = c(x) + x^j$. The syndrome is equal to

$$r(\beta) = c(\beta) + \beta^j = \beta^j.$$

So we can easily determine the error location, i.e., j, from the syndrome.

Example

Consider $r = 3$ and the Hamming code of length $2^3 - 1$. Let β be a primitive element of $\mathrm{GF}(2^3)$ constructed from $x^3 + x + 1$, see the table below. Suppose $w(x) = 1 + x + x^3 + x^6$ is received. Determine the error location.

word	polynomial in x (modulo $h(x)$)	power of β
0 0 0	0	$-$
1 0 0	1	1
0 1 0	x	β
0 0 1	x^2	β^2
1 1 0	$1 + x \equiv x^3$	β^3
0 1 1	$x + x^2 \equiv x^4$	β^4
1 1 1	$1 + x + x^2 \equiv x^5$	β^5
1 0 1	$1 + x^2 \equiv x^6$	β^6

BCH Codes

- Given a primitive element $\beta \in \mathrm{GF}(2^r)$, $r \geq 2$, we saw that the generator polynomial of the Hamming code of length $n = 2^r - 1$ is equal to the minimal polynomial of β, i.e.,

$$g(x) = m_\beta(x) = m_1(x) = (x+\beta)(x+\beta^2)(x+\beta^4)(x+\beta^8)\cdots(x+\beta^{2^{r-1}}).$$

- What we really did was to select a factor of $x^{2^r-1} + 1$ in order to construct a cyclic code of length $n = 2^r - 1$:

$$\begin{aligned} x^{2^r-1} + 1 &= (x+\beta)(x+\beta^2)(x+\beta^3)(x+\beta^4)\cdots(x+\beta^{2^r-1}) \\ &= \underbrace{(x+\beta)(x+\beta^2)(x+\beta^4)\cdots(x+\beta^{2^{r-1}})}_{g(x)=m_1(x)} \cdot M(x), \end{aligned}$$

  where $M(x)$ is the product of other minimal polynomials.

- Generalizing the idea for Hamming codes, that is, by taking $g(x)$ to be

$$m_1(x) \cdot m_3(x) \cdot m_5(x)$$

  for example, leads to BCH codes.

- In this introductory chapter, we only consider $g(x) = m_1(x) \cdot m_3(x)$. Note that

$$m_3(x) = (x + \beta^3)(x + (\beta^3)^2)(x + (\beta^3)^4) \cdots (x + (\beta^3)^{2^{e-1}}),$$

where e is such that $(\beta^3)^{2^e} = \beta^3$.
- For $r > 2$, it is possible to show that, like $m_1(x)$, $m_3(x)$ has degree equal to r. In other words,

$$(\beta^3)^{2^i} \neq (\beta^3)^{2^j} \quad \text{whenever} \quad 0 \leq i < j \leq r - 1.$$

- Thus, $g(x) = m_1(x) \cdot m_3(x)$ has degree equal to $2r$, and it generates a cyclic code of length $n = 2^r - 1$ and dimension $k = 2^r - 2r - 1$.

Definition

The cyclic code C defined by $g(x)$ above is a BCH code. We will show that C corrects any error pattern of weight two, i.e., C is a double-error-correcting code.

Example

Determine the generator polynomial of a BCH code of length $n = 2^4 - 1 = 15$. Let $\beta \in \mathrm{GF}(2^4)$ be primitive and a root of $h(x) = x^4 + x + 1$.
We have

$$\begin{aligned} m_1(x) &= (x + \beta)(x + \beta^2)(x + \beta^4)(x + \beta^8) = 1 + x + x^4 \\ m_3(x) &= (x + \beta^3)(x + \beta^6)(x + \beta^{12})(x + \beta^9) = 1 + x + x^2 + x^3 + x^4. \end{aligned}$$

$$g(x) = m_1(x) \cdot m_3(x) = 1 + x^4 + x^6 + x^7 + x^8.$$

Finally, C has dimension k equal to $15 - \deg g(x) = 7$.

Parity-Check Matrix of BCH Codes

Let C be the BCH code in the last definition. Then

$$v(x) \in C \Leftrightarrow v(x) = a(x) \cdot g(x) \Leftrightarrow$$
$$v(x) = a(x)m_1(x)m_3(x) \Leftrightarrow \beta \text{ and } \beta^3 \text{ are roots of } v(x) \Leftrightarrow$$

$$\begin{cases} v_0 + v_1\beta + v_2\beta^2 + \cdots v_{n-1}\beta^{n-1} = 0 \\ v_0 + v_1\beta^3 + v_2(\beta^3)^2 + \cdots v_{n-1}(\beta^3)^{n-1} = 0 \end{cases} \Leftrightarrow$$

$$(v_0 \ v_1 \ \cdots v_{n-1}) \cdot \begin{bmatrix} 1 & 1 \\ \beta & \beta^3 \\ \beta^2 & \beta^6 \\ \vdots & \vdots \\ \beta^i & \beta^{3i} \\ \vdots & \vdots \\ \beta^{n-1} & \beta^{3(n-1)} \end{bmatrix} = [0\ 0].$$

Note that each entry of the above matrix (call it H) is a binary n-tuple. H is a parity-check matrix for C.

- Now we will show that the code C of slides #5 and 7 corrects up to two errors in a block of $n = 2^r - 1$ digits. Thus, $d(C) \geq 5$. Let $r(x)$ be the received polynomial. Then

$$s = [r(\beta), r(\beta^3)] = [s_1, s_3].$$

- If no errors occur, then $r(x) \in C$ and so

$$s = [r(\beta), r(\beta^3)] = [0, 0].$$

- If exactly one error occurs, then $r(x) = c(x) + x^j$ for some $0 \leq j \leq n-1$. Thus,

$$s = [r(\beta), r(\beta^3)] = [\beta^j, \beta^{3j}]. \text{ Hence, } s_3 = s_1^3 \neq 0.$$

- If exactly two errors occur, then $r(x) = c(x) + x^i + x^j$ for some $0 \leq i < j \leq n-1$. Thus,

$$\begin{cases} \beta^i + \beta^j &= s_1 \\ \beta^{3i} + \beta^{3j} &= s_3 \Rightarrow (\beta^i + \beta^j)(\beta^{2i} + \beta^i \cdot \beta^j + \beta^{2j}) = s_3. \end{cases}$$

Hence,

$$\begin{cases} \beta^i + \beta^j &= s_1 \\ \beta^i \cdot \beta^j &= \frac{s_3}{s_1} + s_1^2. \end{cases}$$

In conclusion, β^i and β^j are roots of

$$x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2\right) = 0. \quad (*)$$

Decoding Algorithm for 2-Error-Correcting BCH Codes

Input: The received polynomial $r(x)$.

1. Compute $s = [s_1, s_3] = [r(\beta), r(\beta^3)]$.
2. If $s_1 = s_3 = 0$, declare that no errors occurred. EXIT.
3. If $s_1 = 0$ and $s_3 \neq 0$, ask for retransmission. EXIT.
4. If $s_1 \neq 0$ and $s_3 = s_1^3$, then declare that one error occurred at position i where $s_1 = \beta^i$). EXIT.
5. If $s_1 \neq 0$ and $s_3 \neq s_1^3$, solve $(*)$ (see slide #9). If it has two distinct roots, β^i and β^j, both non-zero, declare that $e(x) = x^i + x^j$. EXIT.
6. If $(*)$ has no roots or one of the roots equals zero, ask for retransmission

Example

Consider the field $\mathrm{GF}(2^4)$ whose elements are listed on page 114. See Table 5.1. A double-error-correcting BCH code of length 15 is generated by

$$\begin{aligned} g(x) &= m_\beta(x) \cdot m_{\beta^3}(x) \\ &= (x^4 + x + 1) \cdot (x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^4 + 1. \end{aligned}$$

Decode the received polynomial $r(x) = x^9 + x^7 + x^4 + x^2 + 1$.

We have: $s_1 = r(\beta) = \beta^{10}$ and $s_3 = r(\beta^3) = 1$.

Since $s_1 \neq 0$ and $s_3 = s_1^3$, the decoder declares that $r(x)$ contains exactly one error, located in position 10, that is, $e(x) = x^{10}$.

The sent code-polynomial is estimated as

$$\widehat{c}(x) = x^{10} + x^9 + x^7 + x^4 + x^2 + 1.$$

Example

Consider the same code as in the previous example. Decode the the received polynomial $r(x) = x^{10} + x^8 + x^6 + x$.

We have: $s_1 = r(\beta) = \beta^6$ and $s_3 = r(\beta^3) = \beta^7$. Since $s_3 \neq s_1^3$, the decoder goes to Step 4 of the decoding algorithm. Note:

$$\frac{s_3}{s_1} + s_1^2 = \beta + \beta^{12} = \beta^{13}.$$

Solving the quadratic equation

$$x^2 + s_1 x + \left(\frac{s_3}{s_1} + s_1^2\right) = x^2 + \beta^6 x + \beta^{13} = 0.$$

for x gives $x_1 = 1 = \beta^0$ and $x_2 = \beta^{13}$. Therefore, $e(x) = x^{13} + 1$.

The sent code-polynomial is estimated as

$$\widehat{c}(x) = x^{13} + x^{10} + x^8 + x^6 + x + 1.$$