Chapter 6: Algebraic Coding

Lecture 26

BCH codes

Hamming codes

Reed-Solomon codes DVD, DTV, satellites, mobile phones...

Cyclic codes

Golay codes

NOTE - Check proper lecture slides for more info about this

The binary Hamming (15,11) code C has a parity check matrix H:

$$\begin{array}{c} 1 \\ \alpha \\ \alpha^2 \\ \alpha^3 \end{array} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\alpha^5$$

The columns have been ordered so as to correspond to the powers

$$\alpha^i \in \mathsf{GF}(16) = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$$

for the root α of $x^4 + x + 1$.
For instance, $\alpha^5 = \alpha + \alpha^2$.

We will represent each column by its corresponding α^i and write H as

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{14} \end{pmatrix}$$

We will represent each column by its corresponding α^i and write H as

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \cdots & \alpha^{14} \end{pmatrix}$$

The syndrome of a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{14}) \in C$ is

$$S(\mathbf{c}) = H\mathbf{c}^T = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{14}\alpha^{14} = C(\alpha)$$

where $C(x) = c_0 + c_1 x + \cdots + c_{14}x^{14}$ is the polynomial representing $\mathbf{c}$.

- This allows us to describe the code in terms of polynomials.

BCH CODES (Bose, Chaudhuri 1960 & Hocquenghem 1959)

Let $f(x) \in \mathbb{Z}_2[x]$ be a polynomial of degree m with primitive root α.
Let $n = 2^m - 1$ and $k = n - m$.

Theorem

$H = (1\,\alpha \cdots \alpha^{n-1})$ is a check matrix of a binary Hamming (n, k) code C.
Indeed, every binary Hamming (n, k) code can be obtained in this way.

Let $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in C$ be a codeword.

- $1, \alpha, \ldots, \alpha^{m-1}$ are the leading columns of H
- $c_0, \ldots, c_{m-1}$ are the check bits
- $c_m, \ldots, c_{n-1}$ are the information bits

BCH CODES (Bose, Chaudhuri 1960 & Hocquenghem 1959)

Let $f(x) \in \mathbb{Z}_2[x]$ be a polynomial of degree m with primitive root α.
Let $n = 2^m - 1$ and $k = n - m$.

Let $\mathbf{c} = (c_0, \ldots, c_{n-1}) \in C$ be a codeword.

- $1, \alpha, \ldots, \alpha^{m-1}$ are the leading columns of H
- $c_0, \ldots, c_{m-1}$ are the check bits
- $c_m, \ldots, c_{n-1}$ are the information bits

The syndrome of $\mathbf{c}$ is

$$S(\mathbf{c}) = H\mathbf{c}^T = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = C(\alpha)$$

where $C(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ is the codeword polynomial of $\mathbf{c}$.
Now, $\mathbf{c}$ is a codeword, so $C(\alpha) = S(\mathbf{c}) = 0$, and α is thus a root of $C(x)$.
The minimal polynomial $M_1(x)$ of α must divide $C(x)$ with no remainder.
Note that $M_1(x)$ is the primitive polynomial $f(x)$.

BCH coding (single-error)

- BCH encoding
- BCH error-correcting
- BCH decoding

BCH encoding

Input: message $(c_m, \ldots, c_{n-1})$

1. Form the information polynomial $I(x) = c_m x^m + \cdots + c_{n-1} x^{n-1}$
2. Calculate the check polynomial $R(x) = I(x) \pmod{M_1(x)}$
3. Calculate the codeword polynomial $C(x) = I(x) + R(x)$

Output: codeword $(c_0, \ldots, c_{n-1})$ where $C(x) = c_0 + \cdots + c_{n-1} x^{n-1}$

The first m bits are check bits and the last k bits are information bits.

BCH ENCODING

Input: message $(c_m, \ldots, c_{n-1})$

① Form the information polynomial $I(x) = c_m x^m + \cdots + c_{n-1}x^{n-1}$

② Calculate the check polynomial $R(x) = I(x) \pmod{M_1(x)}$

③ Calculate the codeword polynomial $C(x) = I(x) + R(x)$

Output: codeword $(c_0, \ldots, c_{n-1})$ where $C(x) = c_0 + \cdots + c_{n-1}x^{n-1}$

BCH ERROR-CORRECTING

Input: $\mathbf{d} = \mathbf{c} + \mathbf{e}_j$ where the error is given by jth standard unit vector $\mathbf{e}_j$.

① Represent $\mathbf{c}$ and $\mathbf{d}$ as polynomials $C(x)$ and $D(x)$.

② Calculate $S(\mathbf{d}) = D(\alpha) = C(\alpha) + \alpha^j = \alpha^j$

Output: The error lies in column $S(\mathbf{d}) = \alpha^j$

BCH DECODING

Input: $\mathbf{c} = (c_0, \ldots, c_{n-1})$

Output: $(c_m, \ldots, c_{n-1})$

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ with 8 elements.
Let β be a root of $m_1(x) = x^3 + x + 1$.
Then β is a primitive element of $\mathbb{F}$ and its powers are as follows:

$\beta^0 = 1$	$\beta^2 = \beta^2$	$\beta^4 = \beta + \beta^2$	$\beta^6 = 1 + \beta^2$
$\beta^1 = \beta$	$\beta^3 = 1 + \beta$	$\beta^5 = 1 + \beta + \beta^2$	$\beta^7 = 1$

We then have the Hamming $(7, 4)$ code check matrix

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 & \beta^5 & \beta^6 \end{pmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ with 8 elements.
Let β be a root of $m_1(x) = x^3 + x + 1$.
Then β is a primitive element of $\mathbb{F}$.

The message 0101 is encoded by the information polynomial

$$I(x) = 0x^3 + 1x^4 + 0x^5 + 1x^6 = x^4 + x^6$$

Polynomial longdivision shows that

$$I(x) = x^4 + x^6 = (x^3 + 1)(x^3 + x + 1) + (x + 1) = (x^3 + 1)m_1(x) + R(x)$$

The check polynomial is $R(x) = x + 1$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ with 8 elements.
Let β be a root of $m_1(x) = x^3 + x + 1$.
Then β is a primitive element of $\mathbb{F}$.

The message 0101 is encoded by the information polynomial

$$I(x) = 0x^3 + 1x^4 + 0x^5 + 1x^6 = x^4 + x^6$$

Polynomial longdivision shows that the check polynomial is $R(x) = x + 1$.

The codeword polynomial is

$$C(x) = I(x) + R(x) = 1 + x + x^4 + x^6$$

The message 0101 is thus encoded as $\mathbf{c} = 1100101$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ with 8 elements.
Let β be a root of $m_1(x) = x^3 + x + 1$.
Then β is a primitive element of $\mathbb{F}$ and its powers are as follows:

$\beta^0 = 1$	$\beta^2 = \beta^2$	$\beta^4 = \beta + \beta^2$	$\beta^6 = 1 + \beta^2$
$\beta^1 = \beta$	$\beta^3 = 1 + \beta$	$\beta^5 = 1 + \beta + \beta^2$	$\beta^7 = 1$

The received word $\mathbf{d} = 0011011$ has 1 error.
To correct and decode $\mathbf{d}$, find the polynomial

$$D(x) = 0x^0 + 0x^1 + 1x^2 + 1x^3 + 0x^4 + 1x^5 + 1x^6 = x^2 + x^3 + x^5 + x^6$$

and evaluate:

$$\begin{aligned} D(\beta) &= \beta^2 + \beta^3 + \beta^5 + \beta^6 \\ &= \beta^2 + (1+\beta) + (1+\beta+\beta^2) + (1+\beta^2) = 1 + \beta^2 = \beta^6 \end{aligned}$$

The error therefore lies in the entry of $\mathbf{d} = 0011011$ corresponding to β^6.
Correct to $\mathbf{c} = 0011010$ and decode to 1010.