Chapter 6: Algebraic Coding

Lecture 27

BCH codes

- Hamming codes
- Reed-Solomon codes DVD, DTV, satellites, mobile phones...
- Cyclic codes
- Golay codes

BCH codes allow fast decoding and can correct any t errors.

BCH CODES (single-error)

Let $f(x) \in \mathbb{Z}_p[x]$ be a primitive polynomial of degree m with root α.
Let $n = p^m - 1$ 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 (single-error)

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

$$S(\mathbf{c}) = H\mathbf{c}^T = (1\ \alpha\ \cdots\ \alpha^{n-1}) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$= c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = C(\alpha)$$

where $C(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ is the codeword polynomial of $\mathbf{c}$.

BCH codes (single-error)

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

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

The syndrome of $\mathbf{c}$ is

$$S(\mathbf{c}) = H\mathbf{c}^T = (1\ \alpha\ \cdots\ \alpha^{n-1}) \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$= c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = C(\alpha)$$

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 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 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 $S(\mathbf{d}) = \alpha^j$

If $D(\alpha) = 0$, then there is no error.

BCH decoding

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

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

BCH CODES (double-error)

For each 1-error correcting BCH code C,
$\mathbf{c}$ is a codeword of C if and only if $C(\alpha) = 0$.
Here, $C(x) = (1 \; x \; \cdots \; x^{n-1})\mathbf{c}^T$
and α is a primitive element of $GF(p^k)$.

To correct 1 error, we used 1 root of the minimal polynomial $M_1(x)$ of α.
To correct 2 errors (or more), we must use 2 roots (or more).

For each index s, define cyclotomic coset containing s as

$$K_s = \{s, ps, p^2 s, p^3 s, \ldots \pmod{p^k - 1}\}$$

Theorem

If β is a root of $g(x) \in \mathbb{Z}_p[x]$, then so is β^{p^i} for all i.

Corollary

The minimal polynomial $M_s(x)$ of α^s has roots $\{\alpha^k : k \in K_s\}$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
Here, $p = 2$ and

$$\begin{aligned}
K_1 &= \{1, 2, 4, 8, 16, \ldots \pmod{15}\} = \{1, 2, 4, 8\} \\
K_3 &= \{3, 6, 12, 9\} \\
K_5 &= \{5, 10\} \\
K_7 &= \{7, 14, 13, 11\}
\end{aligned}$$

Let α be a primitive root of $x^4 + x + 1$.
The minimum polynomials of $\alpha = \alpha^1$ and α^3 are

$$\begin{aligned}
M_1(x) &= x^4 + x + 1 \\
M_3(x) &= (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9) \\
&= \cdots \\
&= x^4 + x^3 + x^2 + x + 1
\end{aligned}$$

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
Let α be a primitive root of $x^4 + x + 1$.
The minimal polynomials of $\alpha = \alpha^1$ and α^3 are

$$\begin{aligned} M_1(x) &= x^4 + x + 1 \\ M_3(x) &= x^4 + x^3 + x^2 + x + 1 \end{aligned}$$

Define the polynomial

$$\begin{aligned} M(x) &= M_1(x)M_3(x) \\ &= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) \\ &= x^8 + x^7 + x^6 + x^4 + 1 \end{aligned}$$

Note that α and α^3 are both roots of $M(x)$.

BCH codes (double-error)

Construction

① Find a primitive root $\alpha = \alpha_1$ of polynomial $m(x)$ with degree n in some field $\mathbb{F} = \mathbb{Z}_p / \langle m(x) \rangle$

② Find the cyclotomic coset K_1 of $\alpha = \alpha^1$

③ Find an index $i \in \{1, \ldots, p^m - 1\} - K_1$

④ Find the minimal polynomial $M_i(x)$ for α^i

⑤ Define $M(x) = M_1(x) M_i(x)$ where $M_1(x) = m(x)$

⑥ Define the check matrix

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^i & \cdots & (\alpha^i)^{n-1} \end{pmatrix}$$

⑦ Define the syndrome $S(\mathbf{c}) = H\mathbf{c}^T$

⑧ Define $C = \{\mathbf{c} \in \mathbb{R}^n \ : \ S(\mathbf{c}) = \mathbf{0}\}$

BCH codes (double-error)

⑥ Define the check matrix

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^i & \cdots & (\alpha^i)^{n-1} \end{pmatrix}$$

⑦ Define the syndrome $S(\mathbf{c}) = H\mathbf{c}^T$

⑧ Define $C = \{\mathbf{c} \in \mathbb{R}^n \ : \ S(\mathbf{c}) = \mathbf{0}\}$

The syndrome of a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ is

$$S(\mathbf{c}) = H\mathbf{c}^T = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^i & \cdots & (\alpha^i)^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} \\ c_0 + c_1\alpha^i + \cdots + c_{n-1}(\alpha^i)^{n-1} \end{pmatrix} = \begin{pmatrix} C(\alpha) \\ C(\alpha^i) \end{pmatrix}$$

BCH codes (double-error)

⑥ Define the check matrix

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{n-1} \\ 1 & \alpha^i & \cdots & (\alpha^i)^{n-1} \end{pmatrix}$$

⑦ Define the syndrome $S(\mathbf{c}) = H\mathbf{c}^T$

⑧ Define $C = \{\mathbf{c} \in \mathbb{R}^n \ : \ S(\mathbf{c}) = \mathbf{0}\}$

The syndrome of a codeword $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ is

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

We see that $\mathbf{c} \in \mathbb{R}$ is a codeword in C if and only if $C(\alpha) = C(\alpha^i) = 0$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$.
Let α be a primitive root of $x^4 + x + 1$.
The minimal polynomials of $\alpha = \alpha^1$ and α^3 are

$$M_1(x) = x^4 + x + 1$$
$$M_3(x) = x^4 + x^3 + x^2 + x + 1$$

Define the polynomial

$$M(x) = M_1(x)M_3(x) = x^8 + x^7 + x^6 + x^4 + 1$$

Note that α and α^3 are both roots of $M(x)$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
Let α be a primitive root of $x^4 + x + 1$.
The minimal polynomials of $\alpha = \alpha^1$ and α^3 are

$$M_1(x) = x^4 + x + 1$$
$$M_3(x) = x^4 + x^3 + x^2 + x + 1$$

Define the check matrix

$$H = \begin{pmatrix} 1 & \alpha & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \cdots & (\alpha^3)^{14} \end{pmatrix} = \begin{bmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ \hline 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \end{bmatrix}$$

This BCH code has parametres has $n = 15$, $m = 8$, and $k = 7$.

BCH codes (double-error)

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 $R(x) = I(x) \pmod{M(x)}$
3. Calculate the codeword polynomial $C(x) = I(x) + R(x)$

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

Decoding

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

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

Error-Correcting

This is more complicated than in the single-error case.

BCH codes (double-error)

Error-Correcting

Input: $\mathbf{d} = \mathbf{c} + \mathbf{e}_j + \mathbf{e}_\ell$ where 2 errors are given by unit vectors $\mathbf{e}_j, \mathbf{e}_\ell$.

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

$$S(\mathbf{d}) = \begin{pmatrix} D(\alpha) \\ D(\alpha^i) \end{pmatrix} = \begin{pmatrix} C(\alpha) + \alpha^j + \alpha^\ell \\ C(\alpha^i) + (\alpha^i)^j + (\alpha^i)^\ell \end{pmatrix} = \begin{pmatrix} \alpha^j + \alpha^\ell \\ \alpha^{ij} + \alpha^{i\ell} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_i \end{pmatrix}$$

3. Determine α^j and α^ℓ from S_1 and S_i.

Output: The errors lie in columns α^j and α^ℓ.

Note that

- if there are no errors, then $\mathbf{d} = \mathbf{c}$ and $S(\mathbf{d}) = \mathbf{0}$;
- if there is 1 error, then $\mathbf{d} = \mathbf{c} + \mathbf{e}_j$ and $D(\alpha) = C(\alpha) + \alpha^j = \alpha^j$.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
Let α be a primitive root of $x^4 + x + 1$.
Suppose that $\mathbf{d} = \mathbf{c} + \mathbf{e}_j + \mathbf{e}_\ell$ has 2 errors, given by unit vectors $\mathbf{e}_j, \mathbf{e}_\ell$.
To correct these errors, we calculate the syndrome:

$$S(\mathbf{d}) = \begin{pmatrix} D(\alpha) \\ D(\alpha^3) \end{pmatrix} = \begin{pmatrix} C(\alpha) + \alpha^j + \alpha^\ell \\ C(\alpha^i) + (\alpha^3)^j + (\alpha^3)^\ell \end{pmatrix} = \begin{pmatrix} \alpha^j + \alpha^\ell \\ \alpha^{3j} + \alpha^{3\ell} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix}$$

Then
$$\begin{aligned} S_1^3 &= \alpha^{3j} + 3\alpha^{2j+\ell} + 3\alpha^{j+2\ell} + \alpha^{3\ell} \\ &= (\alpha^{3j} + \alpha^{3\ell}) + 3\alpha^j\alpha^\ell(\alpha^j + \alpha^\ell) \\ &= S_3 + 3\alpha^j\alpha^\ell S_1 \end{aligned}$$

so $\alpha^j + \alpha^\ell = S_1$ and $\alpha^j\alpha^\ell = \frac{S_3}{S_1} + S_1^2$.
Therefore, α^j and α^ℓ are the roots of

$$z^2 + S_1 z + \left(\frac{S_3}{S_1} + S_1^2\right) = 0 \quad \text{over} \quad \mathbb{Z}_2(\alpha)$$

Testing $z = \alpha^r$ for $r = 0, 1, \ldots, n-1$ gives the answers.

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$.
Let α be a primitive root of $x^4 + x + 1$.

Now suppose that $\mathbf{d} = 01111101 \big| 1001011$ has 2 errors, in positions α^j, α^ℓ.
Then

$$D(x) = x + x^2 + x^3 + x^4 + x^5 + x^7 + x^8 + x^{11} + x^{13} + x^{14}$$

so

$$\begin{aligned} S(\mathbf{d}) = \begin{pmatrix} D(\alpha) \\ D(\alpha^3) \end{pmatrix} &= \begin{pmatrix} \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^7 + \alpha^7 + \alpha^{11} + \alpha^{13} + \alpha^{14} \\ \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} + \alpha^{15} + \alpha^{21} + \alpha^{24} + \alpha^{33} + \alpha^{39} + \alpha^{42} \end{pmatrix} \\ &= \begin{pmatrix} \alpha^{12} \\ \alpha^7 \end{pmatrix} = \begin{pmatrix} S_1 \\ S_3 \end{pmatrix} = \begin{pmatrix} \alpha^j + \alpha^\ell \\ \alpha^{3j} + \alpha^{3\ell} \end{pmatrix} \end{aligned}$$

Now, $\dfrac{S_3}{S_1} + S_1^2 = \dfrac{\alpha^7}{\alpha^{13}} + (\alpha^{12})^2 = \alpha^{13}$, so we must solve $x^2 + \alpha^{12}x + \alpha^{13} = 0$.
By trial and error testing, we find the solutions α^3, α^{10}.
We correct these bits to get $\mathbf{c} = 01101101 \big| 1011011$.

BCH codes (general binary case)

Let α be a primitive element of $GF(2^r)$ and let $M(x)$ be the least common multiple of the minimal polynomials of $\alpha, \alpha^2, \ldots, \alpha^{2t}$ where $2t < 2^r$.
If $\deg M(x) = 2^r - k$, then a BCH $(2^r - 1,\ k)$-code C is the set of polynomials $C(x) \in \mathbb{Z}_2[x]$ divisible by $M(x)$ and of degree at most $2^r - 2$.

Theorem

- C can correct up to t errors
- If $D(x)$ has $u \leq t$ errors and $\mathbf{S} = \begin{pmatrix} S_1 & \cdots & S_t \\ \vdots & & \vdots \\ S_t & \cdots & S_{2t-1} \end{pmatrix}$ for $S_i = D(\alpha^i)$, then $u = \operatorname{rank} \mathbf{S}$.

Let α be a primitive element of $GF(2^r)$ and let $M(x)$ be the least common multiple of the minimal polynomials of $\alpha, \alpha^2, \dots, \alpha^{2t}$ where $2t < 2^r$.
If $\deg M(x) = 2^r - k$, then a BCH $(2^r - 1,\ k)$-code C is the set of polynomials $C(x) \in \mathbb{Z}_2[x]$ divisible by $M(x)$ and of degree at most $2^r - 2$.

Theorem

- C can correct up to t errors
- If $D(x)$ has $u \leq t$ errors and $\mathbf{S} = \begin{pmatrix} S_1 & \cdots & S_t \\ \vdots & & \vdots \\ S_t & \cdots & S_{2t-1} \end{pmatrix}$ for $S_i = D(\alpha^i)$, then $u = \operatorname{rank} \mathbf{S}$.
- $D(x) = C(x) + E(X)$ where $E(x) = x^{j_1} + x^{j_2} + \cdots + x^{j_u}$ and $\alpha^{j_1}, \dots, \alpha^{j_u}$ are the roots of the polynomial

$$z^u + \sigma_1 z^{u-1} + \cdots + \sigma_{u-1} z + \sigma_u$$

and

$$\begin{pmatrix} S_1 & \cdots & S_u \\ \vdots & & \vdots \\ S_u & \cdots & S_{2u-1} \end{pmatrix} \begin{pmatrix} \sigma_u \\ \vdots \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} S_{u+1} \\ \vdots \\ S_{2u} \end{pmatrix}$$

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$.
Let α be a primitive root of $x^4 + x + 1$.
The cyclotomic sets are

$$K_1 = \{1, 2, 4, 8\}$$
$$K_3 = \{3, 6, 12, 9\}$$
$$K_5 = \{5, 10\}$$
$$K_7 = \{7, 14, 13, 11\}$$

The minimum polynomials of $\alpha = \alpha^1$, α^3, and α^5 are

$$M_1(x) = x^4 + x + 1$$
$$M_3(x) = x^4 + x^3 + x^2 + x + 1$$
$$M_5(x) = x^2 + x + 1$$

Define the polynomial

$$M(x) = M_1(x)M_3(x)M_5(x) = \cdots = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

Example

Consider the field $\mathbb{F} = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$.
Let α be a primitive root of $x^4 + x + 1$.
The minimum polynomials of $\alpha = \alpha^1$, α^3, and α^5 are

$$\begin{aligned} M_1(x) &= x^4 + x + 1 \\ M_3(x) &= x^4 + x^3 + x^2 + x + 1 \\ M_5(x) &= x^2 + x + 1 \end{aligned}$$

Define the polynomial

$$M(x) = M_1(x)M_3(x)M_5(x) = \cdots = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

By the theorem, $M(x)$ defines a $t = 3$ error correcting (15,5) BCH code.

Chapter 6: Algebraic Coding

Lecture 27