BCH Codes

Outline

- Binary Primitive BCH Codes
- Decoding of the BCH Codes
- Implementation of Galois Field Arithmetic
- Implementation of Error Correction
- Nonbinary BCH Codes and Reed-Solomon Codes

Preface

- The Bose, Chaudhuri, and Hocquenghem (BCH) codes form a large class of powerful random error-correcting cyclic codes.
- This class of codes is a remarkable generalization of the Hamming codes for multiple-error correction.
- Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960.
- Generalization of the binary BCH codes to codes in p^m symbols (where p is a prime) was obtained by Gorenstein and Zierler.
- Among the nonbinary BCH codes, the most important subclass is the class of Reed-Solomon (RS) codes.
- Among all the decoding algorithms for BCH codes, Berlekamp's iterative algorithm, and Chien's search algorithm are the most efficient ones.

Description of the BCH Codes

Binary Primitive BCH Codes

- $\forall$ integer $m \geq 3, \ \ t < 2^{m-1}, \exists$ a binary BCH codes with

$$n = 2^m - 1 \rightarrow \text{ Block length}$$
$$n - k \leq mt \rightarrow \text{ Number of parity-check digits}$$
$$d_{\min} \geq 2t + 1 \rightarrow \text{ Minimum distance}$$

- Clearly, this code is capable of correcting any combination of t or fewer errors in a block of $n = 2^m - 1$ digits. We call this code a *t-error-correcting* BCH code. The generator polynomial of this code is specified in terms of its roots from the Galois field $GF(2^m)$
- Let α be a primitive element of $GF(2^m)$. The generator poly. $g(x)$ of the t-error-correcting BCH code of length $2^m - 1$ is the lowest-degree poly. over $GF(2)$ which has

$$\alpha.\alpha^2.\alpha^3....\alpha^{2t} \text{ as its roots.}$$

Binary Primitive BCH Codes

- It follows from Theorem 2.11 that $g(x)$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ and their conjugates as all its roots. Let $\phi_i(x)$ be the minimal poly. of α^i. Then $g(x)$ must be the *least common multiple* (LCM) of $\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)$, that is,

$$g(x) = \mathrm{LCM}\{\phi_1(x), \phi_2(x), \ldots \phi_{2t}(x)\}$$

- If i is an even integer, it can be expressed as a product of the following form :

$$i = i'2^l,$$

where i' is an odd number and $l \geq 1$. Then $\alpha^i = (\alpha^{i'})^{2^l}$ is a conjugate of $\alpha^{i'}$ and therefore α^i and $\alpha^{i'}$ have the same minimal poly., that is,

$$\phi_i(x) = \phi_{i'}(x).$$

Binary Primitive BCH Codes

- Hence, even power of α has the same minimal poly. as some preceding odd power of α.

$$g(x) = \text{LCM}\ \{\phi_1(x), \phi_3(x), \ldots \phi_{2t-1}(x)\}$$

- $\deg\ [\phi_i(x)] \leq m$ (Theorem 2.18 & 2.19)

$$\therefore\ \deg\ [g(x)] \leq mt \quad \therefore n - k \leq mt$$

- The BCH codes defined above are usually called primitive (or narrow-sense) BCH codes.

Binary Primitive BCH Codes

- The single-error-correcting BCH codes of length $2^m - 1$ is generated by $g(x) = \phi_1(x)$ since $t = 1$.

  $\because \alpha$ is a primitive element of $GF(2^m)$

  $\therefore \phi_1(x)$ is a primitive poly. of degree m

  $$(\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2} \ldots, \alpha^{2^m} = 1)$$

  $\therefore$ the single-error-correcting BCH codes of length $2^m - 1$ is a Hamming code

- Ex 6.1

  α is a primitive element of $GF(2^4)$ given by Table 2.8 such that $1 + \alpha + \alpha^4 = 0$. The minimal polynomials of $\alpha, \alpha^3, \alpha^5$ are

Binary Primitive BCH Codes

TABLE 2.8: Three representations for the elements of $GF(2^4)$ generated by $p(X) = 1 + X + X^4$.

Power representation	Polynomial representation	4-Tuple representation
0	0	$(0\,0\,0\,0)$
1	1	$(1\,0\,0\,0)$
α	α	$(0\,1\,0\,0)$
α^2	α^2	$(0\,0\,1\,0)$
α^3	α^3	$(0\,0\,0\,1)$
α^4	$1 + \alpha$	$(1\,1\,0\,0)$
α^5	$\alpha + \alpha^2$	$(0\,1\,1\,0)$
α^6	$\alpha^2 + \alpha^3$	$(0\,0\,1\,1)$
α^7	$1 + \alpha + \alpha^3$	$(1\,1\,0\,1)$
α^8	$1 + \alpha^2$	$(1\,0\,1\,0)$
α^9	$\alpha + \alpha^3$	$(0\,1\,0\,1)$
α^{10}	$1 + \alpha + \alpha^2$	$(1\,1\,1\,0)$
α^{11}	$\alpha + \alpha^2 + \alpha^3$	$(0\,1\,1\,1)$
α^{12}	$1 + \alpha + \alpha^2 + \alpha^3$	$(1\,1\,1\,1)$
α^{13}	$1 + \alpha^2 + \alpha^3$	$(1\,0\,1\,1)$
α^{14}	$1 + \alpha^3$	$(1\,0\,0\,1)$

9

Binary Primitive BCH Codes

$$\therefore \phi_1(x) = 1 + x + x^4$$

$$\phi_3(x) = 1 + x + x^2 + x^3 + x^4$$

$$\phi_5(x) = 1 + x + x^2$$

- The double-error-correcting BCH code of length $n = 2^4 - 1 = 15$ is generated by $g(x) = \text{LCM}\,\{\phi_1(x), \phi_3(x)\}$
  Since $\phi_1(x)$ and $\phi_3(x)$ are two distinct irreducible polynomials,

$$g(x) = (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)$$

$$= 1 + x^4 + x^6 + x^7 + x^8$$

$$\therefore (15, 7) \text{ cyclic code with } d_{\min} \geq 5$$

$$\because W(g(x)) = 5 \qquad \therefore d_{\min} = 5$$

Binary Primitive BCH Codes

- The triple-error-correcting BCH code of length 15 is generated by

$$g(x) = \text{LCM } \{\phi_1(x), \phi_3(x), \phi_5(x)\}$$
$$= (1+x+x^4)(1+x+x^2+x^3+x^4)(1+x+x^2)$$
$$= 1+x+x^2+x^4+x^5+x^8+x^{10}$$

  It's a (15,5) cyclic code with $d_{\min} \geq 7$. Since $W(g(x)) = 7, d_{\min} = 7.$

- Let $v(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$ be a poly. with $v_i \in GF(2)$

  If v(x) has roots $\alpha, \alpha^2, \ldots, \alpha^{2t}$, then v($x$) is divisible by $\phi_1(x), \phi_2(x), \ldots, \phi_{2t}(x)$. (Theorem 2.14)

- **v**(x) is a code poly., g(x)|v(x), $\mathrm{g}(x) = \text{LCM}\{\varphi_1(x), \varphi_2(x), \ldots, \varphi_{2t}(x)\}$

Binary Primitive BCH Codes

- We have a new definition for *t*-error-correcting BCH code: A binary *n*-tuple $\mathbf{v} = (v_0, v_1, v_2, \ldots, v_{n-1})$ is a code word if and only if the poly. $\mathrm{v}(x) = v_0 + v_1 x + \ldots + v_{n-1} x^{n-1}$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ as roots, i.e.

$$\mathrm{v}(\alpha^i) = v_0 + v_1 \alpha^i + v_2 \alpha^{2i} + \ldots + v_{n-1} \alpha^{(n-1)i}$$

$$(v_0, v_1, v_2, \ldots, v_{n-1}) \cdot \begin{bmatrix} 1 \\ \alpha^i \\ \cdot \\ \cdot \\ \cdot \\ \alpha^{(n-1)i} \end{bmatrix} = 0 \ \text{ for } 1 \le i \le 2t.$$

Binary Primitive BCH Codes

- Let

$$\mathrm{H} = \begin{bmatrix} 1 & \alpha & . & . & . & \alpha^{n-1} \\ 1 & (\alpha^2) & . & . & . & (\alpha^2)^{n-1} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 1 & (\alpha^{2t}) & . & . & . & (\alpha^{2t})^{n-1} \end{bmatrix}$$

If **v** is a code word in the *t*-error-correcting BCH code, then $\mathrm{v} \cdot \mathrm{H}^T = 0$

The code is the null space of the matrix **H** and **H** is the parity-check matrix of the code.

Binary Primitive BCH Codes

- α^j is a conjugate of α^i, then $v(\alpha^j)=0$ iff $v(\alpha^i)=0$ (Thm. 2.11)
  j-th row of **H** can be omitted. As a result **H** can be reduced to the following form :

$$H=\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & (\alpha^3)^2 & \cdots & (\alpha^3)^{n-1} \\ & & & & \\ 1 & \alpha^{(2t-1)} & (\alpha^{2t-1})^2 & \cdots & (\alpha^{2t-1})^{n-1} \end{bmatrix}$$

只剩下奇數的Row

- EX 6.2
  double-error-correcting BCH code of length $n=2^4-1=15$, (15,7) code. Let α be a primitive element in $GF(2^4)$

Binary Primitive BCH Codes

- The parity-check matrix is

(Note that the parity check matrix is not binary anymore.)

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \ldots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \ldots & \alpha^{42} \end{bmatrix}$$

Using $\alpha^{15} = 1$, and representing each entry of **H** by its 4-tuple,

$$H = \begin{bmatrix} 100010011010111 \\ 010011010111100 \\ 001001101011110 \\ 000100110101111 \\ \hdashline 100011000110001 \\ 000110001100011 \\ 001010010100101 \\ 011110111101111 \end{bmatrix}$$

Binary Primitive BCH Codes

- FACT:
  The t-error-correcting BCH code indeed has $d_{\min} \geq 2t+1$
  (pf): Suppose $\exists$ $\underline{v} \neq \underline{0}$ such that $\mathrm{W(v)} = \delta \leq 2t$
  Let $v_{j_1}, v_{j_2}, \ldots v_{j_\delta}$ be the nonzero components of $\underline{v}$ (i.e. all ones)

$$\Rightarrow \underline{0} = \underline{v}H^T = (v_{j_1} v_{j_2} .. v_{j_\delta}) \begin{bmatrix} \alpha^{j_1} & (\alpha^2)^{j_1} \cdots (\alpha^{2t})^{j_1} \\ \alpha^{j_2} & (\alpha^2)^{j_2} \cdots (\alpha^{2t})^{j_2} \\ \vdots & \vdots \\ \alpha^{j_\delta} & (\alpha^2)^{j_\delta} \cdots (\alpha^{2t})^{j_\delta} \end{bmatrix}$$

$$\Rightarrow (1,1\ldots,1) \begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 \cdots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 \cdots & (\alpha^{j_2})^{2t} \\ \vdots & \vdots & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 \cdots & (\alpha^{j_\delta})^{2t} \end{bmatrix} = \underline{0} \ldots\ldots\ldots \otimes$$

Binary Primitive BCH Codes

$$(1,1\ldots,1)\underbrace{\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots (\alpha^{j_1})^{\delta} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots (\alpha^{j_2})^{\delta} \\ \vdots & \vdots & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots (\alpha^{j_\delta})^{\delta} \end{bmatrix}} = 0$$

A, a $\delta \times \delta$ square matrix $\quad (\delta \le 2t)$

$$\Rightarrow |A| = 0$$

Taking out the common factor from each row of the determinant.

$$\Rightarrow \alpha^{(j_1 + j_2 + \ldots + j_\delta)} \begin{vmatrix} 1 & \alpha^{j_1} & \cdots \alpha^{(\delta-1) j_1} \\ 1 & \alpha^{j_2} & \cdots \alpha^{(\delta-1) j_2} \\ \vdots & \vdots & \vdots \\ 1 & \alpha^{j_\delta} & \cdots \alpha^{(\delta-1) j_\delta} \end{vmatrix} = 0\ldots\ldots \otimes\otimes$$

Binary Primitive BCH Codes

- The determinant in the equality above is a Vandermonde determinant which is nonzero. The product on the left-hand side of

  $\otimes\otimes$ can not be zero. This is a contradiction and hence our assumption that there exists a nonzero code vector v of $\mathrm{W(v)} = \delta \leq 2t$ is invalid.

$$\therefore d_{\min} \geq 2t+1$$

- $2t+1$ is the designed distance of the t-error-correcting BCH code. The true minimum distance of a BCH code may or may not be equal to its designed distance.

- Binary BCH code with length $n \neq 2^m - 1$ can be constructed in the same manner as for the case $n = 2^m - 1$. (Theorem 2.9)
  Let β be an element of order n in $GF(2^m)$, $n \mid 2^m - 1$ and **g**(x) be the binary polynomial of minimum degree that has $\beta, \beta^2, \ldots, \beta^{2t}$ as roots.

Binary Primitive BCH Codes

- Let $\psi_1(x), \psi_2(x), \ldots, \psi_{2t}(x)$ be the minimal poly. of $\beta, \beta^2, \ldots \beta^{2t}$ respectively then $g(x) = \text{LCM}\{\psi_1(x), \psi_2(x), \ldots, \psi_{2t}(x)\}$

- $\because \beta^n = 1, \therefore \beta, \beta^2, \ldots, \beta^{2t}$ are roots of $x^n + 1$

  $\Rightarrow g(x) \big| (x^n + 1)$
- We see that g(x) is a factor of $X^n + 1$.
  - The cyclic code generated by **g**(x) is a *t*-error-correcting BCH code of length *n*.
  - The number of parity-check digits $\leq mt$
  - $d_{\min} \geq 2t + 1$.
- If β is not a primitive element of GF(2^m), the code is called a nonprimitive BCH code.

General Definition of Binary BCH Codes

- General definition of binary BCH codes.

  $\beta \in GF(2^m), \ell_0$ be any nonnegative integer and consider $\beta^{l_0}, \beta^{l_0+1}, \ldots, \beta^{l_0+d_0-2}$. For $0 \le i < d_0 - 1$, let $\psi_i(x), n_i$ be the minimal poly. and order of β^{ℓ_0+i} , respectively.

$$g(x) = \mathrm{LCM}\{\psi_0(x), \psi_1(x), \ldots, \psi_{d_0-2}(x)\}$$

and the length of the code is

$$n = \mathrm{LCM}\left\{n_0, n_1, \ldots n_{d_0-2}\right\}$$

<u>Note that</u>: $d_{\min} \ge d_0$ (Proof is omitted and left as an exercise.)

parity-check digits $\le m(d_0 - 1)$

is capable of correcting $\lfloor (d_0 - 1)/2 \rfloor$ or fewer errors

General Definition of Binary BCH Codes

- If we let $l_0 = 1$, $d_0 = 2t+1$ and β be a primitive element of $GF(2^m)$, the code becomes a t-error-correcting primitive BCH code of length $2^m - 1$.

- If we let $l_0 = 1$, $d_0 = 2t+1$ and β be not a primitive element of $GF(2^m)$, the code is a nonprimitive t-error-correcting BCH code of length n, which is the order of β .

- For a BCH code with designed distance d_0, we require g(x) has d_0 -1 consecutive powers of a field element β as roots. This guarantees that the code has $d_{\min} \geq d_0$. This lower bound on the minimum distance is called the BCH bound.

- In the rest of this chapter, we consider only the primitive BCH codes.

Decoding of the BCH Codes

Decoding of the BCH Codes

- Suppose that a code word $\mathbf{v}(\mathrm{x}) = v_0 + v_1 x + v_2 x^2 + \ldots + v_{n-1} x^{n-1}$ is transmitted and the transmission errors result :

  $$\mathbf{r}(\mathrm{x}) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$$

  Let $\mathbf{e}(\mathrm{x})$ be the error pattern. Then

  $$\mathrm{r(x) = v(x) + e(x)}$$

- For decoding, remember

$$\mathrm{H} = \begin{bmatrix} 1 & \alpha & . & . & . & \alpha^{n-1} \\ 1 & (\alpha^2) & . & . & . & (\alpha^2)^{n-1} \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ 1 & (\alpha^{2t}) & . & . & . & (\alpha^{2t})^{n-1} \end{bmatrix}$$

Decoding of the BCH Codes

- The syndrome is $2t$-tuple,

$$\mathrm{S} = (S_1, S_2, \ldots S_{2t}) = \mathrm{r} \cdot \mathrm{H}^{\mathrm{T}}$$

Let $s_i = r(\alpha^i) = r_0 + r_1\alpha^i + \ldots + r_{n-1}(\alpha^i)^{n-1}$ for $1 \le i \le 2t$

s_i can be evaluated by $b_i(x) = R_{\phi_i(x)}[r(x)]$

$\phi_i(x)$ is the minimal poly. of α^i

$\because r(x) = a_i(x)\phi_i(x) + b_i(x)$

$\therefore s_i = r(\alpha^i) = b_i(\alpha^i)$

Decoding of the BCH Codes

- EX6.4
  Consider the double-error-correcting (15, 7) BCH code given in (from Ex6.1) .

$$\text{If } \underline{r} = (100000001000000) \Rightarrow r(x) = 1 + x^8$$

$$\because \phi_1(x) = \phi_2(x) = \phi_4(x) = 1 + x + x^4 \qquad \therefore s_1 = b_1(\alpha) = \alpha^2, s_2 = b_1(\alpha^2) = \alpha^4$$

$$\phi_3(x) = 1 + x + x^2 + x^3 + x^4 \qquad s_3 = b_3(\alpha^3) = 1 + \alpha^9$$

$$b_1(x) = R_{\phi_1(x)}[r(x)] = x^2 \qquad = 1 + \alpha + \alpha^3 = \alpha^7$$

$$b_3(x) = R_{\phi_3(x)}[r(x)] = 1 + x^3 \qquad s_4 = b_1(\alpha^4) = \alpha^8$$

$$\therefore \underline{s} = (\alpha^2, \alpha^4, \alpha^7, \alpha^8)$$

(Note that syndrome is not binary anymore.)

Decoding of the BCH Codes

- $\because v(\alpha^i) = 0$ for $1 \le i \le 2t \rightarrow s_i = r(\alpha^i) = e(\alpha^i)$

Suppose $e(x) = x^{j_1} + x^{j_2} + \ldots + x^{j_v} \quad 0 \le j_1 < j_2 < \ldots j_v < n$

$$\Rightarrow s_1 = \alpha^{j_1} + \alpha^{j_2} + \ldots + \alpha^{j_v}$$

$$s_2 = (\alpha^{j_1})^2 + (\alpha^{j_2})^2 + \ldots + (\alpha^{j_v})^2$$

$$\vdots$$

$$s_{2t} = (\alpha^{j_1})^{2t} + \ldots + (\alpha^{jv})^{2t}$$

where $\alpha^{j_1}, \alpha^{j_2}, \ldots \alpha^{j_v}$ are unknown.

Any method for solving these equations is a decoding algorithm for the BCH codes.

Decoding of the BCH Codes

- Once $\alpha^{j_1}, \alpha^{j_2}, \ldots \alpha^{j_v}$ have been found, the powers $j_1, j_2, \ldots j_v$ tell us the error locations in $e(x)$
- If the number of errors in **e**(x) is t or less, the solution that yields an error pattern with the smallest number of errors is the right solution.
- For convenience, let $\beta_\ell = \alpha^{j_\ell}$, $1 \le \ell \le v$ be the error location numbers.

$$\left.\begin{aligned} s_1 &= \beta_1 + \beta_2 + \ldots + \beta_v \\ s_2 &= \beta_1^2 + \beta_2^2 + \ldots + \beta_v^2 \\ &\vdots \\ s_{2t} &= \beta_1^{2t} + \beta_2^{2t} + \ldots. + \beta_v^{2t} \end{aligned}\right\} \text{Power-sum Symmetric function}$$

Decoding of the BCH Codes

- Define $\sigma(x) = (1+\beta_1 x)(1+\beta_2 x)....(1+\beta_v x)$

  $= \sigma_0 + \sigma_1 x + \sigma_2 x^2 + ... + \sigma_v x^v$

  : error-location poly.

- The roots of $\sigma(x)$ are $\beta_1^{-1}, \beta_2^{-1}, ...\beta_v^{-1}$, which are the inverses of the error location numbers.

$$\sigma_0 = 1$$

$$\sigma_1 = \beta_1 + \beta_2 + ...\beta_v$$

$$\sigma_2 = \beta_1\beta_2 + \beta_2\beta_3 + ... + \beta_{v-1}\beta_v$$

$$\vdots$$

$$\sigma_v = \beta_1\beta_2 ... \beta_v$$

Decoding of the BCH Codes

These coefficients are known as elementary symmetric functions. σ_i 's are related to s_j 's by Newton's identities

$$
\begin{aligned}
&s_1 + \sigma_1 = 0 \\
&s_2 + \sigma_1 s_1 + 2\sigma_2 = 0 \\
&s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0 \\
&\qquad\quad \vdots \\
&s_v + \sigma_1 s_{v-1} + \ldots + \sigma_{v-1} s_1 + v\sigma_v = 0 \\
&s_{v+1} + \sigma_1 s_v + \ldots + \sigma_{v-1} s_2 + \sigma_v s_1 = 0
\end{aligned}
$$

Note that, for binary case, $\because\ 1+1=2=0$, we have

$$
i\sigma_i = \begin{cases} \sigma_i & \text{for odd } i \\ 0 & \text{for even } i \end{cases}
$$

Decoding of the BCH Codes

Consequently, if $\beta_1, \beta_2, ..., \beta_v \in GF(2^m)$, then

$$(\beta_1 + \beta_2 + ... + \beta_v)^{2^r} = \beta_1^{2^r} + \binom{2^r}{1} \beta_1^{2^r - 1} \beta_2 + \cdots + \beta_v^{2^r}$$

$$= \beta_1^{2^r} + \beta_2^{2^r} + \cdots + \beta_v^{2^r}$$

Since $\binom{2^r}{1} = \binom{2^r}{2} = \cdots \binom{2^r}{2^r - 1} \equiv 0 \mod 2,$

$$s_{2j} = \sum_{i=1}^{v} \beta_i^{2j} = \left(\sum_{i=1}^{v} \beta_i^{j} \right)^2 = s_j^2$$

Decoding of the BCH Codes

Consequently, the Newton's Identities can be simplified into t equations:

$$
\begin{aligned}
&s_1 + \sigma_1 = 0 \\
&s_3 + \sigma_1 s_2 + \sigma_2 s_1 + \sigma_3 = 0 \\
&s_5 + \sigma_1 s_4 + \sigma_2 s_3 + \sigma_3 s_2 + \sigma_4 s_1 + \sigma_5 = 0 \\
&\qquad\vdots \\
&s_{2t-1} + \sigma_1 s_{2t-2} + \sigma_2 s_{2t-3} + \cdots + \sigma_t s_{t-1} = 0
\end{aligned}
$$

Decoding of the BCH Codes

- The equations may have many solutions.
- We want to find the solution that yields a σ(X) of minimal degree. This σ(X) would produce an error pattern with minimum number of errors.
- Decoding Procedure

step 1. Compute $\underline{s} = (s_1, s_2, \ldots s_{2t})$ from $r(x)$

step 2. Determine $\sigma(x)$ from $\underline{s}$

step 3. Determine the error-location number

$\beta_1, \beta_2, \ldots \beta_v$ by finding the roots of $\sigma(x)$

and correct the errors in $r(x)$

Decoding of the BCH Codes

- The first method for determing $\sigma(x)$ from $\underline{s}$

$\rightarrow$ Peterson's Algorithm

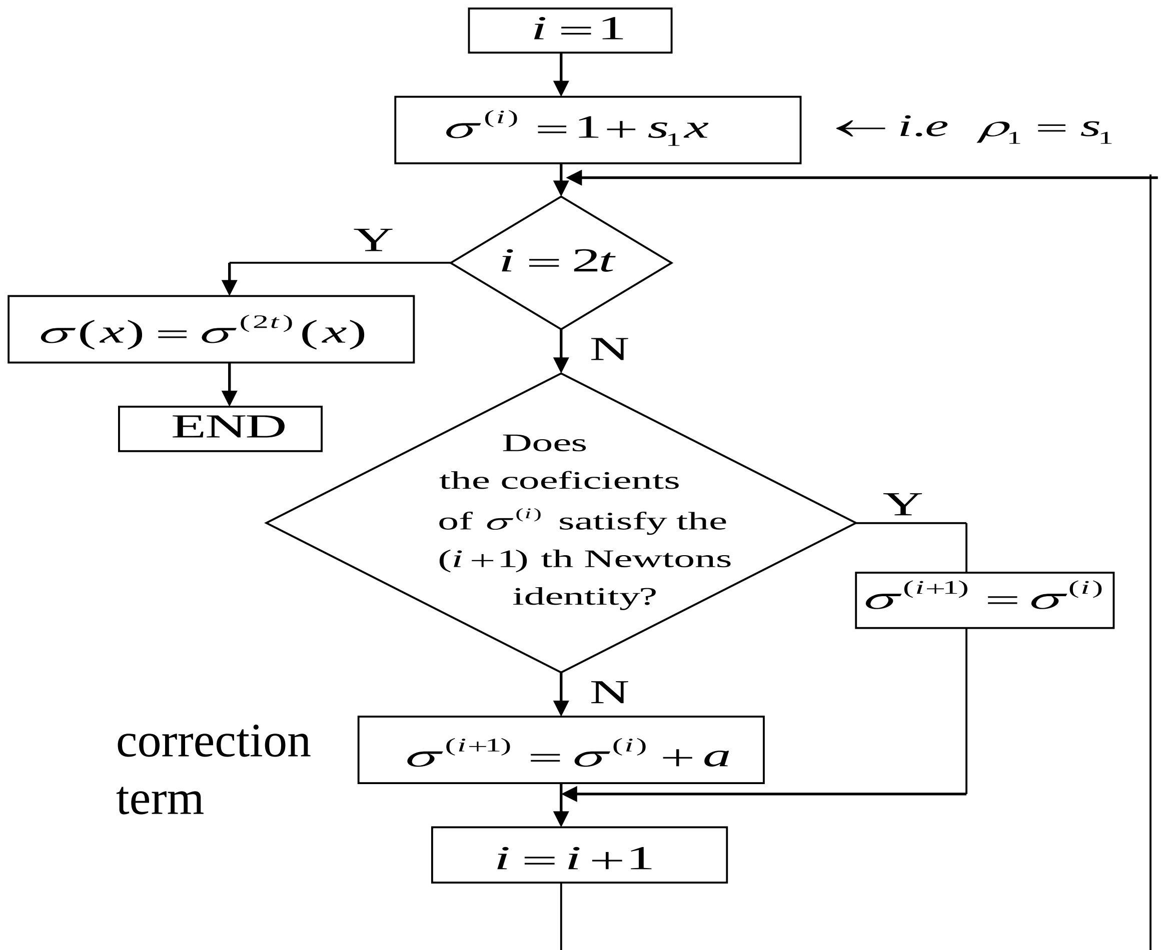
$$\mathbf{A\sigma} \triangleq \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ s_2 & s_1 & 1 & 0 & \cdots & 0 & 0 \\ s_4 & s_3 & s_2 & s_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ s_{2t-4} & s_{2t-5} & s_{2t-6} & s_{2t-7} & \cdots & s_{t-2} & s_{t-3} \\ s_{2t-2} & s_{2t-3} & s_{2t-4} & s_{2t-5} & \cdots & s_t & s_{t-1} \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \vdots \\ \sigma_{t-1} \\ \sigma_t \end{bmatrix} = \begin{bmatrix} s_1 \\ s_3 \\ s_5 \\ \vdots \\ s_{2t-3} \\ s_{2t-1} \end{bmatrix}$$

$$\Rightarrow \sigma_1 = s_1, \sigma_2 = \frac{s_3 + s_1^3}{s_1}, \cdots$$

Decoding of the BCH Codes

- The second method: Berlekamps iterative algorithm

  $\Rightarrow$ Iterative Algorithm for finding $\sigma(x)$



Decoding of the BCH Codes

- How to add a correction term to $\sigma^{(i)}$?

  Let $\sigma^{(\mu)} = 1 + \sigma_1^{(\mu)} x + \sigma_2^{(\mu)} x^2 + \ldots + \sigma_{\ell_\mu}^{(\mu)} x^{\ell_\mu}$

  be the minimum-degree poly. determined at the μth step.

  To determine $\sigma^{(\mu+1)}(x)$ => compute μth discrepancy

  $$d_\mu = s_{\mu+1} + \sigma_1^{(\mu)} s_\mu + \sigma_2^{(\mu)} s_{\mu-1} + \ldots + \sigma_{\ell_\mu}^{(\mu)} s_{\mu+1-\ell_\mu}$$

  If $d_\mu = 0 \Rightarrow \sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x)$

  If $d_\mu \neq 0$, go back to the steps prior to the μth step and determine $\sigma^{(\rho)}(x)$ s.t. ρth discrepancy $d_\rho \neq 0$, and $\rho - \ell_\rho$ has the largest value. ($\ell_\rho = \deg\ [\sigma^{(\rho)}(x)]$) . Then

  $$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) + d_\mu d_\rho^{-1} x^{(\mu-\rho)} \sigma^{(\rho)}(x)$$

  is the minimum-degree poly. whose coefficients satisfy the first Newton's identities

Decoding of the BCH Codes

- To carry out the iteration of finding σ(X) , we begin with the following table:

μ	$\sigma^{(\mu)}(x)$	d_μ	ℓ_μ	$\mu-\ell_\mu$
–1	1	1	0	-1
0	1	S_1	0	0
1				
2				
$\vdots$				
$2t$				

Decoding of the BCH Codes

- l_μ is the degree of $\sigma^{(\mu)}(X)$.
- If $d_\mu = 0$, then $\sigma_\mu^{(\mu+1)}(X) = \sigma^{(\mu)}(X)$ and $l_{\mu+1} = l_\mu$.
- If $d_\mu \neq 0$, find another row ρ prior to the μth row such that $d_\rho \neq 0$ and the number $\rho - l_\rho$ in the last column of the table has the largest value. Then $\sigma^{(\mu+1)}(X)$ is given by

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) + d_\mu d_\rho^{-1} x^{(\mu-\rho)} \sigma^{(\rho)}(x)$$

  and $l_{\mu+1} = \max(l_\mu, l_\rho + \mu - \rho)$.
- In either case, $d_{\mu+1} = s_{\mu+2} + \sigma_1^{(\mu+1)} s_{\mu+1} + \ldots + \sigma_{\ell_{\mu+1}}^{(\mu+1)} s_{\mu+2-\ell_{\mu+1}}$
- The polynomial $\sigma^{(2t)}(X)$ in the last row should be the required $\sigma(X)$.

Decoding of the BCH Codes

- Ex 6.5
  Consider (15.5) triple-error-correcting BCH codes given in ex 6.1

  $(t=3)$

$$p(x) = 1 + x + x^4$$

$$\underline{v} = 0 \rightarrow \oplus \xleftarrow{} \underline{e} \qquad \underline{v} = 0 \rightarrow \oplus \rightarrow r = x^3 + x^5 + x^{12}$$

$$\phi_1(x) = \phi_2(x) = \phi_4(x) = 1 + x + x^4$$

$$\phi_3(x) = \phi_6(x) = 1 + x + x^2 + x^3 + x^4$$

$$\phi_5(x) = 1 + x + x^2$$

Decoding of the BCH Codes

$$b_1(x) = R_{\phi_1(x)}[r(x)] = 1$$

$$b_3(x) = R_{\phi_3(x)}[r(x)] = 1 + x^2 + x^3$$

$$b_5(x) = R_{\phi_5(x)}[r(x)] = x^2$$

$$s_1 = s_2 = s_4 = 1$$

$$s_3 = 1 + \alpha^6 + \alpha^9 = \alpha^{10}$$

$$s_6 = 1 + \alpha^{12} + \alpha^{18} = \alpha^5$$

$$s_5 = \alpha^{10}$$

$$\therefore \underline{s} = (1, 1, \alpha^{10}, 1, \alpha^{10}, \alpha^5)$$

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) + d_\mu d_\rho^{-1} x^{(\mu-\rho)} \sigma^{(\rho)}(x)$$

Decoding of the BCH Codes

$$d_\mu = s_{\mu+1} + \sigma_1^{(\mu)} s_\mu + \sigma_2^{(\mu)} s_{\mu-1} + \ldots + \sigma_{\ell_\mu}^{(\mu)} s_{\mu+1-\ell_\mu}$$

$$\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x) + d_\mu d_\rho^{-1} x^{(\mu-\rho)} \sigma^{(\rho)}(x)$$

$$l_{\mu+1} = \max(l_\mu\,,\ l_\rho + \mu - \rho).$$

- $S_1=1$
- $\mu=0$; $d_0=S_1=1\neq 0$
- $\rho=-1$
- $\sigma^{(1)}(X)= \sigma^{(0)}(X)+d_0 d_{-1}^{-1} X^{(0+1)}\sigma^{(-1)}(X)=1+1\cdot 1\cdot X\cdot 1=1+X$
- $l_1=\max(l_0,l_{-1}+\mu-\rho))=\max(0,0+0+1)=1$
- $\mu-l_\mu=1-l_1=1-1=0$
- $d_1=S_2+\sigma_1^{(1)}S_1=1+1\cdot 1=0$
- $\sigma^{(2)}(X)= \sigma^{(1)}(X)=1+X$
- $l_2=l_1=1$
- $\mu-l_\mu=2-l_2=2-1=1$
- $d_2=S_3+\sigma_1^{(2)}S_2 =\alpha^{10}+1\cdot 1=(1+\alpha+\alpha^2)+1= \alpha^5$

Decoding of the BCH Codes

- $d_2=\alpha^5\neq 0$
- $\rho=0$
- $\sigma^{(3)}(X)=\sigma^{(2)}(X)+d_2 d_0^{-1}X^{(2-0)}\sigma^{(0)}(X)=1+X+\alpha^5\cdot 1\cdot X^2\cdot 1=1+X+\alpha^5X^2$
- $l_3=\max(l_2,l_0+\mu-\rho))=\max(1,0+2-0)=2$
- $\mu-l_\mu=3-l_3=3-2=1$
- $d_3=S_4+\sigma_1^{(3)}S_3+\sigma_2^{(3)}S_2+\sigma_3^{(3)}S_1=1+1\cdot\alpha^{10}+\alpha^5\cdot 1+0\cdot 1$
  $=1+(1+\alpha+\alpha^2)+(\alpha+\alpha^2)=0$

Decoding of the BCH Codes

μ	$\sigma^{(\mu)}(x)$	d_μ	ℓ_μ	$\mu-\ell_\mu$
-1	1	1	0	-1
0	1	1	0	0
1	$1+x$	0	1	0
2	$1+x$	α^5	1	1
3	$1+x+\alpha^5x^2$	0	2	1
4	$1+x+\alpha^5x^2$	α^{10}	2	2
5	$1+x+\alpha^5x^3$	0	3	2
6	$1+x+\alpha^5x^3$	-	-	-

$$\therefore \sigma(x)=\sigma^{(6)}(x)=1+x+\alpha^5x^3$$
$$=(1+\alpha^{-3}x)(1+\alpha^{-10}x)(1+\alpha^{-12}x)$$

$$\therefore x=\alpha^3,\alpha^{10},\alpha^{12}$$

Decoding of the BCH Codes

error location numbers

$$\beta_1 = \alpha^{-3} = \alpha^{12}, \beta_2 = \alpha^{-10} = \alpha^{5}, \beta_3 = \alpha^{-12} = \alpha^{3}$$

$$\therefore e(x) = x^3 + x^5 + x^{12}$$

$$\therefore r(x) = r(x) + e(x) = 0$$

- If the number of errors in the received polynomial $\mathbf{r}(X)$ is less than the designed error-correcting capability t of the code, it is not necessary to carry out the $2t$ steps of iteration to find the error-location polynomial $\sigma(X)$.
- It has been shown that if d_μ and the discrepancies at the next t-l_μ-1 steps are all zeros (i.e. successive t-l_μ zeros), $\sigma^{(\mu)}(X)$ is the error-location polynomial.
- If $v(v \leq t)$ errors occur, only $v+t$ steps of iteration are needed.
- The iterative algorithm described above not only applies to binary BCH codes but also nonbinary BCH codes.

Decoding of the BCH Codes

Simplified Algorithm for finding $\sigma(x)$

- For a binary BCH code, it is only required to fill out a table with t empty rows. Such a table is presented below.

μ	$\sigma^{(\mu)}(x)$	d_μ	ℓ_μ	$2\mu-\ell_\mu$
-1/2	1	1	0	-1
0	1	S_1	0	0
1				
2				
.				
.				
t				

Decoding of the BCH Codes

1. If $d_\mu = 0,$ then $\sigma^{(\mu+1)}(x) = \sigma^{(\mu)}(x)$

2. If $d_\mu \neq 0,$ find another row ρ proceding the μth row, s.t. $2\rho - \ell_\rho$ is as large as possible and $d_\rho \neq 0$

Then $\sigma^{(\mu+1)}(X) = \sigma^{(\mu)}(X) + d_\mu d_\rho^{-1} X^{2(\mu-\rho)} \sigma^{(\rho)}(X)$

note that $d_{\mu+1} = s_{2\mu+3} + \sigma_1^{(\mu+1)} s_{2\mu+2} + \sigma_2^{(\mu+1)} s_{2\mu+1}$

$$+ \ldots + \sigma_{\ell_{\mu+1}}^{(\mu+1)} s_{2\mu+3-\ell_{\mu+1}}$$

$$\ell_{\mu+1} = \deg\ [\sigma^{(\mu+1)}(x)]$$

Decoding of the BCH Codes

- The polynomial $\sigma^{(t)}(X)$ in the last row should be the required $\sigma(X)$.
- If it has degree greater than t, there were more than t errors, and generally it is not possible to locate them.
- The computation required in this simplified algorithm is one-half of the computation required in the general algorithm.
- The simplified algorithm applies only to binary BCH codes.
- If the number of errors in the received polynomial $\mathbf{r}(X)$ is less than the designed error-correcting capability t of the code, it is not necessary to carry out the t steps of iteration to find the error-location polynomial $\sigma(X)$ for a t-error-correcting binary BCH code.

Decoding of the BCH Codes

- Remarks:
  - If $v \le t$ errors occur, only $\lceil (t+v)/2 \rceil$ steps needed.
  - If, for some μ, d_μ and the discrepancies at the next $(t-l_\mu-1)/2$ steps are zero, then $\sigma(X)$ is the error-location poly.
- EX6.6

  The simplified table for finding $\sigma(x)$ for the code in ex6.5 is given below. Thus, $\sigma(x) = \sigma^{(3)}(x) = 1 + x + \alpha^5 x^3$.

μ	$\sigma^{(\mu)}(x)$	d_μ	l_μ	$2\mu - l_\mu$
-1/2	1	1	0	-1
0	1	$S_1=1$	0	0
1	$1+S_1x=1+x$	$S_3+S_2S_1== \alpha^5$	1	1(take ρ= -1/2)
2	$1+x+\alpha^5x^2$	α^{10}	2	2(take ρ= 0)
3	$1+x+\alpha^5x^3$	----	3	3(take ρ= 1)

Decoding of the BCH Codes

Finding the Error-Location Numbers and Error Correction.

- Consider ex6.6. The error-location poly. has been found to be

$$\sigma(x) = 1 + x + \alpha^5 x^3$$

  By substituting $1, \alpha, \alpha^2, \ldots, \alpha^{14}$ into it, we find that $\alpha^3, \alpha^{10}, \alpha^{12}$ are the roots of $\sigma(x)$. Therefore, the error location numbers are $\alpha^{12}, \alpha^5, \alpha^3$ => $e(x) = x^3 + x^5 + x^{12}$

- Chien's procedure: The received vector

$$r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$$

  is decoded on a bit-by-bit basis. The high-order bits are decoded first. To decode r_{n-1}, the decoder test whether α^{n-1} is an error-location number; this is equivalent to test whether its inverse α is a root of $\sigma(x)$. If α is a root, then

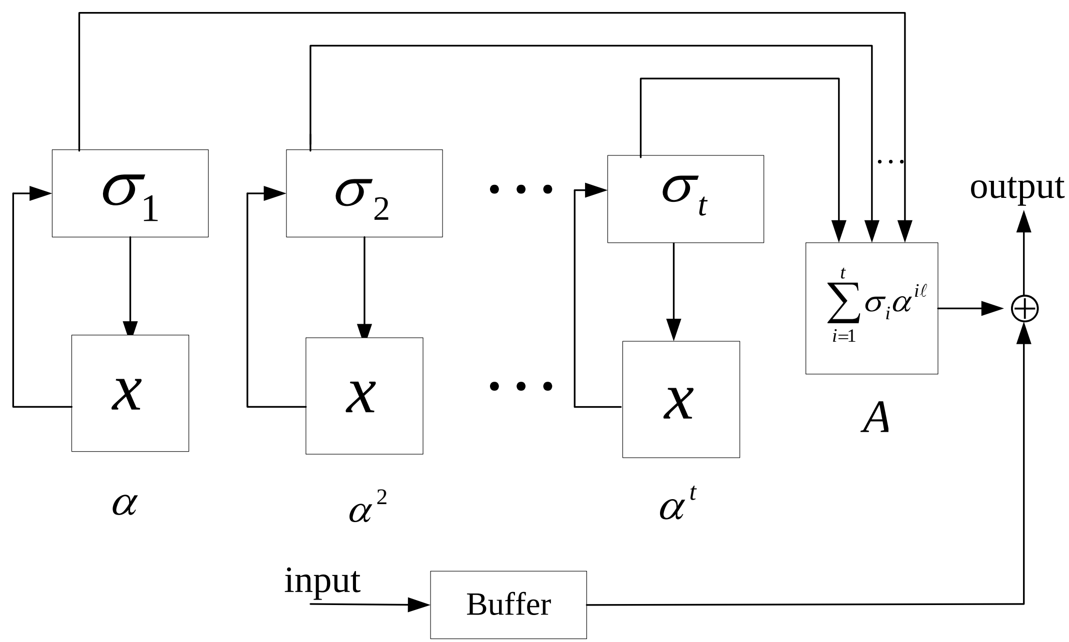
$$1 + \sigma_1 \alpha + \sigma_2 \alpha^2 + \ldots + \sigma_v \alpha^v = 0$$

Decoding of the BCH Codes

- To decode r_{n-l}, the decoder forms $\sigma_1\alpha^l, \sigma_2\alpha^{2l}, \ldots, \sigma_v\alpha^{vl}$ and tests the sum $1+\sigma_1\alpha^l+\sigma_2\alpha^{2l}+\ldots+\sigma_v\alpha^{vl}$

  If the sum is zero, then α^{n-l} is an error-location number and r_{n-l} is an erroneous digit; otherwise, r_{n-l} is a correct digit.

Cyclic error location search unit



Decoding of the BCH Codes

- The $t\sigma$-registers are initial stored with $\sigma_1, \sigma_2, ..., \sigma_t$ calculated in step 2 of the decoding ($\sigma_{v+1} = \sigma_{v+2} = ... = \sigma_t = 0$ for $v < t$). Immediately before r_{n-1} is read out of the buffer, the t multiplier are pulsed once. The multiplications are performed and $\sigma_1\alpha, \sigma_2\alpha^2, \ldots, \sigma_v\alpha^v$ are stored in the σ-registers. The output of the logic circuit A is 1 if and only if the sum $1+\sigma_1\alpha+\sigma_2\alpha^2+\ldots+\sigma_v\alpha^v=0$; otherwise, the output of A is 0. The digit r_{n-1} is read out of the buffer and corrected by the output of A. Having decoded r_{n-1} ,the t multipliers are pulsed again. Now $\sigma_1\alpha^2, \sigma_2\alpha^4, \ldots, \sigma_v\alpha^{2v}$ are stored in the σ-registers. The sum

$$1+\sigma_1\alpha^2+\sigma_2\alpha^4+\ldots+\sigma_v\alpha^{2v}$$

  is tested for 0. The digit r_{n-2} is read out of the buffer and corrected in the same manner as r_{n-1} is corrected.