BCH Codes

Yunghsiang S. Han

Graduate Institute of Communication Engineering,
National Taipei University
Taiwan

E-mail: yshan@mail.ntpu.edu.tw

Description of BCH Codes

- 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 code for multiple-error correction.
- We only consider binary BCH codes in this lecture note. Non-binary BCH codes such as Reed-Solomon codes will be discussed in next lecture note.
- For any positive integers $m \geq 3$ and $t < 2^{m-1}$, there exists a binary BCH code with the following parameters:

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

- We call this code a *t-error-correcting* BCH code.
- Let α be a primitive element in $GF(2^m)$. The generator polynomial $\boldsymbol{g}(x)$ of the t-error-correcting BCH code of length $2^m - 1$ is the *lowest-degree polynomial* over $GF(2)$ which has

$$\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{2t}$$

as its roots.

- $\boldsymbol{g}(\alpha^i) = 0$ for $1 \leq i \leq 2t$ and $\boldsymbol{g}(x)$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ and their conjugates as all its roots.
- Let $\boldsymbol{\phi}_i(x)$ be the minimal polynomial of α^i. Then $\boldsymbol{g}(x)$ must be the *least common multiple* of $\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_2(x), \ldots, \boldsymbol{\phi}_{2t}(x)$, i.e.,

$$\boldsymbol{g}(x) = \mathrm{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_2(x), \ldots, \boldsymbol{\phi}(x)_{2t}\}.$$

- If i is an even integer, it can be expressed as $i = i'2^\ell$, where i' is odd and $\ell > 1$. Then $\alpha^i = \left(\alpha^{i'}\right)^{2\ell}$ is a conjugate of $\alpha^{i'}$. Hence, $\boldsymbol{\phi}_i(x) = \boldsymbol{\phi}_{i'}(x)$.

- $\boldsymbol{g}(x) = \text{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_3(x), \ldots, \boldsymbol{\phi}_{2t-1}(x)\}$.
- The degree of $\boldsymbol{g}(x)$ is at most mt. That is, the number of parity-check digits, $n-k$, of the code is at most equal to mt.
- If t is small, $n-k$ is exactly equal to mt.
- Since α is a primitive element, the BCH codes defined are usually called *primitive* (or *narrow-sense*) BCH codes.

Example

- Let α be a primitive element of $GF(2^4)$ such that $1+\alpha+\alpha^4=0$. The minimal polynomials of α, α^3, and α^5 are

$$\begin{aligned}\boldsymbol{\phi}_1(x) &= 1+x+x^4,\\ \boldsymbol{\phi}_3(x) &= 1+x+x^2+x^3+x^4,\\ \boldsymbol{\phi}_5(x) &= 1+x+x^2,\end{aligned}$$

respectively. The double-error-correcting BCH code of length $n=2^4-1=15$ is generated by

$$\begin{aligned}\boldsymbol{g}(x) &= \mathrm{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_3(x)\}\\ &= (1+x+x^4)(1+x+x^2+x^3+x^4)\\ &= 1+x^4+x^6+x^7+x^8.\end{aligned}$$

$n-k=8$ such that this is a $(15, 7, \geq 5)$ code. Since the weight of the generator polynomial is 5, it is a $(15, 7, 5)$ code.

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

$$\begin{aligned} \boldsymbol{g}(x) &= \mathrm{LCM}\{\boldsymbol{\phi}_1(x), \boldsymbol{\phi}_3(x), \boldsymbol{\phi}_5(x)\} \\ &= (1 + x + x^4)(1 + x + x^2 + x^3 + x^4)(1 + x + x^2) \\ &= 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}. \end{aligned}$$

  $n - k = 10$ such that this is a $(15, 5, \geq 7)$ code. Since the weight of the generator polynomial is 7, it is a $(15, 5, 7)$ code.

- The single-error-correcting BCH code of length $2^m - 1$ is a Hamming code.

$\alpha\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16} \equiv \alpha$

$\alpha^3\ \alpha^6\ \alpha^{12}\ \underline{\alpha}^{24}\ \alpha^{48} \equiv \alpha^3$

$\equiv \alpha^9$

Representations of $GF(2^4)$. $p(z) = z^4 + z + 1$

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	0000	0	x
α^0	1	0001	1	$x + 1$
α^1	z	0010	2	$x^4 + x + 1$
α^2	z^2	0100	4	$x^4 + x + 1$
α^3	z^3	1000	8	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^4	$z + 1$	0011	3	$x^4 + x + 1$
α^5	$z^2 + z$	0110	6	$x^2 + x + 1$
α^6	$z^3 + z^2$	1100	12	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^7	$z^3 + z + 1$	1011	11	$x^4 + x^3 + 1$
α^8	$z^2 + 1$	0101	5	$x^4 + x + 1$
α^9	$z^3 + z$	1010	10	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{10}	$z^2 + z + 1$	0111	7	$x^2 + x + 1$
α^{11}	$z^3 + z^2 + z + 1$	1110	14	$x^4 + x^3 + 1$
α^{12}	$z^3 + z^2 + z + 1$	1111	15	$\underline{x^4 + x^3 + x^2 + x + 1}$
α^{13}	$z^3 + z^2 + 1$	1101	13	$x^4 + x^3 + 1$
α^{14}	$z^3 + 1$	1001	9	$x^4 + x^3 + 1$

Examples of Finite Fields

GF(4) →

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

0	0	0	0
1	0	1	1
2	1	0	α
3	1	1	$\alpha+1$

$\equiv \mathrm{GF}(2)[\alpha] / \alpha^2+\alpha+1$

$\mathrm{GF}(4^2) \equiv \mathrm{GF}(4)[z]/z^2+z+2$, $p(z) = z^2+z+2$

Primitive polynomial over GF(4)

Exponential Notation	Polynomial Notation	Binary Notation	Decimal Notation	Minimal Polynomial
0	0	00	0	
α^0	1	01	1	$x + 1$
α^1	z	10	4	$x^2 + x + 2$
α^2	$z + 2$	12	6	$x^2 + x + 3$
α^3	$3z + 2$	32	14	$x^2 + 3x + 1$
α^4	$z + 1$	11	5	$x^2 + x + 2$
α^5	2	02	2	$x + 2$
α^6	$2z$	20	8	$x^2 + 2x + 1$
α^7	$2z + 3$	23	11	$x^2 + 2x + 2$
α^8	$z + 3$	13	7	$x^2 + x + 3$
α^9	$2z + 2$	22	10	$x^2 + 2x + 1$
α^{10}	3	03	3	$x + 3$
α^{11}	$3z$	30	12	$x^2 + 3x + 3$
α^{12}	$3z + 1$	31	13	$x^2 + 3x + 1$
α^{13}	$2z + 1$	21	9	$x^2 + 2x + 2$
α^{14}	$3z + 3$	33	15	$x^2 + 3x + 3$

Operate on GF(4)

$\alpha = z$
$\alpha^{15} = 1$

BCH Codes of Lengths Less than $2^{10} - 1$ (1)

m	n	k	t	m	n	k	t	m	n	k	t	n	k	t	n	k	t
3	7	4	1		63	24	7		127	50	13	255	187	9	255	71	29
4	15	11	1			18	10			43	14		179	10		63	30
		7	2			16	11			36	15		171	11		55	31
		5	3			~~10~~	~~13~~			29	21		163	12		47	42
5	31	26	1			7	15			22	23		155	13		45	43
		21	2	7	127	120	1			15	27		147	14		37	45
		16	3			113	2			8	31		139	15		29	47
		11	5			106	3	8	255	247	1		131	18		21	55
		6	7			99	4			239	2		123	19		13	59
6	63	57	1			92	5			231	3		115	21		9	63
		~~51~~	~~2~~			85	6			223	4		107	22	511	502	1
		45	3			78	7			215	5		99	23		493	2
		39	4			71	9			207	6		91	25		484	3
		36	5			64	10			199	7		87	26		475	4
		30	6			57	11			191	8		79	27		466	5

For t small
$n - k = mt$

BCH Codes of Lengths Less than $2^{10} - 1$ (2)

n	k	t	n	k	t	n	k	t	n	k	t	n	k	t
511	457	6	511	322	22	511	193	43	511	58	91	1023	933	9
	448	7		313	23		184	45		49	93		923	10
	439	8		304	25		175	46		40	95		913	11
	430	9		295	26		166	47		31	109		903	12
	421	10		286	27		157	51		28	111		893	13
	412	11		277	28		148	53		19	119		883	14
	403	12		268	29		139	54		10	121		873	15
	394	13		259	30		130	55		1013	1		863	16
	385	14		250	31		121	58	1023	1003	2		858	17
	376	15		241	36		112	59		993	3			
	367	16		238	37		103	61		983	4			
	358	18		229	38		94	62		973	5			
	349	19		220	39		85	63		963	6			
	340	20		211	41		76	85		953	7			
	331	21		202	42		67	87		943	8			

GALOIS FIELD GF(2^6) WITH $\rho(\alpha) = 1 + \alpha + \alpha^6 = 0$

0	0	(0 0 0 0 0 0)	α^{15}	$\alpha^3 + \alpha^5$	(0 0 0 1 0 1)
1	1	(1 0 0 0 0 0)	α^{16}	$1 + \alpha + \alpha^4$	(1 1 0 0 1 0)
α	α		α^{17}	$\alpha + \alpha^2 + \alpha^5$	(0 1 1 0 0 1)
α^2	α^2	(0 1 0 0 0 0)	α^{18}	$1+\alpha+\alpha^2+\alpha^3$	(1 1 1 1 0 0)
α^3	α^3	(0 0 1 0 0 0)	α^{19}	$\alpha+\alpha^2+\alpha^3+\alpha^4$	(0 1 1 1 1 0)
α^4	α^4	(0 0 0 1 0 0)	α^{20}	$\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(0 0 1 1 1 1)
α^5	α^5	(0 0 0 0 0 1)	α^{21}	$1+\alpha+\alpha^3+\alpha^4+\alpha^5$	(1 1 0 1 1 1)
α^6	$1+\alpha$	(1 1 0 0 0 0)	α^{22}	$1+\alpha^2+\alpha^4+\alpha^5$	(1 0 1 0 1 1)
α^7	$\alpha+\alpha^2$	(0 1 1 0 0 0)	α^{23}	$1+\alpha^3+\alpha^5$	(1 0 0 1 0 1)
α^8	$\alpha^2+\alpha^3$	(0 0 1 1 0 0)	α^{24}	$1+\alpha^4$	(1 0 0 0 1 0)
α^9	$\alpha^3+\alpha^4$	(0 0 0 1 1 0)	α^{25}	$\alpha+\alpha^5$	(0 1 0 0 0 1)
α^{10}	$\alpha^4+\alpha^5$	(0 0 0 0 1 1)	α^{26}	$1+\alpha+\alpha^2$	(1 1 1 0 0 0)
α^{11}	$1+\alpha$	(1 1 0 0 0 1)	α^{27}	$\alpha+\alpha^2+\alpha^3$	(0 1 1 1 0 0)
α^{12}	$1+\alpha^2$	(1 0 1 0 0 0)	α^{28}	$\alpha^2+\alpha^3+\alpha^4$	(0 0 1 1 1 0)
α^{13}	$\alpha+\alpha^3$	(0 1 0 1 0 0)	α^{29}	$\alpha^3+\alpha^4+\alpha^5$	(0 0 0 1 1 1)
α^{14}	$\alpha^2+\alpha^4$	(0 0 1 0 1 0)	α^{30}	$1+\alpha+\alpha^4+\alpha^5$	(1 1 0 0 1 1)

α^{31}	$1+\alpha^2+\alpha^5$	(1 0 1 0 0 1)	α^{47}	$1+\alpha+\alpha^2+\alpha^5$	(1 1 1 0 0 1)
α^{32}	$1+\alpha^3$	(1 0 0 1 0 0)	α^{48}	$1+\alpha^2+\alpha^3$	(1 0 1 1 0 0)
α^{33}	$\alpha+\alpha^4$	(0 1 0 0 1 0)	α^{49}	$\alpha+\alpha^3+\alpha^4$	(0 1 0 1 1 0)
α^{34}	$\alpha^2+\alpha^5$	(0 0 1 0 0 1)	α^{50}	$\alpha^2+\alpha^4+\alpha^5$	(0 0 1 0 1 1)
α^{35}	$1+\alpha+\alpha^3$	(1 1 0 1 0 0)	α^{51}	$1+\alpha+\alpha^3+\alpha^5$	(1 1 0 1 0 1)
α^{36}	$\alpha+\alpha^2+\alpha^4$	(0 1 1 0 1 0)	α^{52}	$1+\alpha^2+\alpha^4$	(1 0 1 0 1 0)
α^{37}	$\alpha^2+\alpha^3+\alpha^5$	(0 0 1 1 0 1)	α^{53}	$\alpha+\alpha^3+\alpha^5$	(0 1 0 1 0 1)
α^{38}	$1+\alpha+\alpha^3+\alpha^4$	(1 1 0 1 1 0)	α^{54}	$1+\alpha+\alpha^2+\alpha^4$	(1 1 1 0 1 0)
α^{39}	$\alpha+\alpha^2+\alpha^4+\alpha^5$	(0 1 1 0 1 1)	α^{55}	$\alpha+\alpha^2+\alpha^3+\alpha^5$	(0 1 1 1 0 1)
α^{40}	$1+\alpha+\alpha^2+\alpha^3+\alpha^5$	(1 1 1 1 0 1)	α^{56}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4$	(1 1 1 1 1 0)
α^{41}	$1+\alpha^2+\alpha^3+\alpha^4$	(1 0 1 1 1 0)	α^{57}	$\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(0 1 1 1 1 1)
α^{42}	$\alpha+\alpha^3+\alpha^4+\alpha^5$	(0 1 0 1 1 1)	α^{58}	$1+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(1 1 1 1 1 1)
α^{43}	$1+\alpha+\alpha^2+\alpha^4+\alpha^5$	(1 1 1 0 1 1)	α^{59}	$1+\alpha^2+\alpha^3+\alpha^4+\alpha^5$	(1 0 1 1 1 1)
α^{44}	$1+\alpha^2+\alpha^3+\alpha^5$	(1 0 1 1 0 1)	α^{60}	$1+\alpha^3+\alpha^4+\alpha^5$	(1 0 0 1 1 1)
α^{45}	$1+\alpha^3+\alpha^4$	(1 0 0 1 1 0)	α^{61}	$1+\alpha^4+\alpha^5$	(1 0 0 0 1 1)
α^{46}	$\alpha+\alpha^4+\alpha^5$	(0 1 0 0 1 1)	α^{62}	$1+\alpha^5$	(1 0 0 0 0 1)

$\boxed{\alpha^{63} = 1}$

Minimal Polynomials of the Elements in $GF(2^6)$

Elements	Minimal polynomials
$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}$	$1 + X + X^6$
$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{33}$	$1 + X + X^2 + X^4 + X^6$
$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{17}, \alpha^{34}$	$1 + X + X^2 + X^5 + X^6$
$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{49}, \alpha^{35}$	$1 + X^3 + X^6$
$\alpha^9, \alpha^{18}, \alpha^{36}$	$1 + X^2 + X^3$
$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{25}, \alpha^{50}, \alpha^{37}$	$1 + X^2 + X^3 + X^5 + X^6$
$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{41}, \alpha^{19}, \alpha^{38}$	$1 + X + X^3 + X^4 + X^6$
$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{57}, \alpha^{51}, \alpha^{39}$	$1 + X^2 + X^4 + X^5 + X^6$
α^{21}, α^{42}	$1 + X + X^2$
$\alpha^{23}, \alpha^{46}, \alpha^{29}, \alpha^{58}, \alpha^{53}, \alpha^{43}$	$1 + X + X^4 + X^5 + X^6$
$\alpha^{27}, \alpha^{54}, \alpha^{45}$	$1 + X + X^6$
$\alpha^{31}, \alpha^{62}, \alpha^{61}, \alpha^{59}, \alpha^{55}, \alpha^{47}$	$1 + X^5 + X^6$

Generator Polynomials of All BCH Codes of Length 63

n	k	t	g(X)
63	57	1	$g_1(X) = 1 + X + X^6$
	51	2	$g_2(X) = (1 + X + X^6)(1 + X + X^2 + X^4 + X^6)$
	45	3	$g_3(X) = (1 + X + X^2 + X^5 + X^6)g_2(X)$
	39	4	$g_4(X) = (1 + X^3 + X^6)g_3(X)$
	36	5	$g_5(X) = (1 + X^2 + X^3)g_4(X)$
	30	6	$g_6(X) = (1 + X^2 + X^3 + X^5 + X^6)g_5(X)$
	24	7	$g_7(X) = (1 + X + X^3 + X^4 + X^6)g_6(X)$
	18	10	$g_{10}(X) = (1 + X^2 + X^4 + X^5 + X^6)g_7(X)$
	16	11	$g_{11}(X) = (1 + X + X^2)g_{10}(X)$
	10	13	$g_{13}(X) = (1 + X + X^4 + X^5 + X^6)g_{11}(X)$
	7	15	$g_{15}(X) = (1 + X + X^3)g_{13}(X)$

Parity-Check Matrix of a BCH Code

- We can define a t-error-correcting BCH code of length $n = 2^m - 1$ in the following manner: A binary n-tuple $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ is a code word if and only if the polynomial $\boldsymbol{v}(x) = v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}$ has $\alpha, \alpha^2, \ldots, \alpha^{2t}$ as roots.
- Since α^i is a root of $\boldsymbol{v}(x)$ for $1 \leq i \leq 2t$, then

$$\boldsymbol{v}(\alpha^i) = v_0 + v_1 \alpha^i + v_2 \alpha^{2i} + \cdots + v_{n-1} \alpha^{(n-1)i} = 0.$$

- This equality can be written as a matrix product as follows:

$$(v_0, v_1, \ldots, v_{n-1}) \begin{bmatrix} 1 \\ \alpha^i \\ \alpha^{2i} \\ \vdots \\ \alpha^{(n-1)i} \end{bmatrix} = 0 \tag{1}$$

for $1 \leq i \leq 2t$.

- Let

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

- From (1), if $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1})$ is a code word in the t-error-correcting BCH code, then

$$\boldsymbol{v} \cdot \boldsymbol{H}^T = \boldsymbol{0}.$$

- If an n-tuple $\boldsymbol{v}$ satisfies the above condition, α^i is a root of the polynomial $\boldsymbol{v}(x)$. Therefore, $\boldsymbol{v}$ must be a code word in the t-error-correcting BCH code.

- $\boldsymbol{H}$ is a parity-check matrix of the code.
- If for some i and j, α^j is a conjugate of α^i, then $\boldsymbol{v}(\alpha^j) = 0$ if and only if $\boldsymbol{v}(\alpha^i) = 0$.
- The $\boldsymbol{H}$ matrix can be reduced to

$$\boldsymbol{H} = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & (\alpha^3) & (\alpha^3)^2 & (\alpha^3)^3 & \cdots & (\alpha^3)^{n-1} \\ 1 & (\alpha^5) & (\alpha^5)^2 & (\alpha^5)^3 & \cdots & (\alpha^5)^{n-1} \\ \vdots & & & & & \vdots \\ 1 & (\alpha^{2t-1}) & (\alpha^{2t-1})^2 & (\alpha^{2t-1})^3 & \cdots & (\alpha^{2t-1})^{n-1} \end{bmatrix}.$$

- If each entry of $\boldsymbol{H}$ is replaced by its corresponding m-tuple over $GF(2)$ arranged in column form, we obtain a binary parity-check matrix for the code.

BCH Bound

- The t-error-correcting BCH code defined has minimum distance at least $2t+1$.

  Proof: We need to show that no $2t$ of fewer columns of $\boldsymbol{H}$ sum to zero. Suppose that there exists a nonzero code vector $\boldsymbol{v}$ with weight $\delta \leq 2t$. Let $v_{j_1}, v_{j_2}, \ldots, v_{j_\delta}$ be the nonzero components of $\boldsymbol{v}$. Then

$$
\begin{aligned}
\mathbf{0} &= \boldsymbol{v} \cdot \boldsymbol{H}^T \\
&= (v_{j_1}, v_{j_2}, \ldots, v_{j_\delta}) \cdot \begin{bmatrix} \alpha^{j_1} & (\alpha^2)^{j_1} & \cdots & (\alpha^{2t})^{j_1} \\ \alpha^{j_2} & (\alpha^2)^{j_2} & \cdots & (\alpha^{2t})^{j_2} \\ \alpha^{j_3} & (\alpha^2)^{j_3} & \cdots & (\alpha^{2t})^{j_3} \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^2)^{j_\delta} & \cdots & (\alpha^{2t})^{j_\delta} \end{bmatrix}
\end{aligned}
$$

$$= \quad (1,1,\ldots,1)\cdot\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^{2t} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^{2t} \\ \alpha^{j_3} & (\alpha^{j_3})^2 & \cdots & (\alpha^{j_3})^{2t} \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^{2t} \end{bmatrix}.$$

The equality above implies the following equality:

$$(1,1,\ldots,1)\cdot\begin{bmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^{\delta} \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^{\delta} \\ \alpha^{j_3} & (\alpha^{j_3})^2 & \cdots & (\alpha^{j_3})^{\delta} \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^{\delta} \end{bmatrix} = \mathbf{0},$$

which the second matrix on the left is a $\delta \times \delta$ square matrix. To satisfy the above equality, the determinant of the $\delta \times \delta$ matrix must be zero. That is,

$$\begin{vmatrix} \alpha^{j_1} & (\alpha^{j_1})^2 & \cdots & (\alpha^{j_1})^\delta \\ \alpha^{j_2} & (\alpha^{j_2})^2 & \cdots & (\alpha^{j_2})^\delta \\ \alpha^{j_3} & (\alpha^{j_3})^2 & \cdots & (\alpha^{j_3})^\delta \\ \vdots & \vdots & & \vdots \\ \alpha^{j_\delta} & (\alpha^{j_\delta})^2 & \cdots & (\alpha^{j_\delta})^\delta \end{vmatrix} = 0.$$

Then

$$\alpha^{j_1+j_2+\cdots+j_\delta} \cdot \begin{vmatrix} 1 & \alpha^{j_1} & \cdots & \alpha^{j_1(\delta-1)} \\ 1 & \alpha^{j_2} & \cdots & \alpha^{j_2(\delta-1)} \\ 1 & \alpha^{j_3} & \cdots & \alpha^{j_3(\delta-1)} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha^{j_\delta} & \cdots & \alpha^{j_\delta(\delta-1)} \end{vmatrix} = 0.$$

The determinant in the equality above is a *Vandermonde determinant* which is *nonzero*. Contradiction!

- The parameter $2t+1$ is usually called the *designed distance* of the t-error-correcting BCH code.
- The true minimum distance of the code might be larger than $2t+1$.

Syndrome Calculation

- Let
$$\boldsymbol{r}(x) = r_0 + r_1 x + r_2 x^2 + \cdots + r_{n-1} x^{n-1}$$
be the received vector and $\boldsymbol{e}(x)$ the error pattern. Then
$$\boldsymbol{r}(x) = \boldsymbol{v}(x) + \boldsymbol{e}(x).$$

- The syndrome is a $2t$-tuple,
$$\boldsymbol{S} = (S_1, S_2, \ldots, S_{2t}) = \boldsymbol{r} \cdot \boldsymbol{H}^T,$$
where $\boldsymbol{H}$ is given by (2).

- $$S_i = \boldsymbol{r}(\alpha^i) = r_0 + r_1 \alpha^i + r_2 \alpha^{2i} + \cdots + r_{n-1} \alpha^{(n-1)i}$$
for $1 \le i \le 2t$.

- Dividing $\boldsymbol{r}(x)$ by the minimal polynomial $\boldsymbol{\phi}_i(x)$ of α_i, we have

$$\boldsymbol{r}(x) = \boldsymbol{a}_i(x)\boldsymbol{\phi}_i(x) + \boldsymbol{b}_i(x),$$

  where $\boldsymbol{b}_i(x)$ is the remainder with degree less than that of $\boldsymbol{\phi}_i(x)$.

- Since $\boldsymbol{\phi}_i(\alpha^i) = 0$, we have

$$S_i = \boldsymbol{r}(\alpha^i) = \boldsymbol{b}_i(\alpha^i).$$

- Since $\alpha^1, \alpha^2, \ldots, \alpha^{2t}$ are roots of each code polynomial, $\boldsymbol{v}(\alpha^i) = 0$ for $1 \leq i \leq 2t$.
- Then $S_i = \boldsymbol{e}(\alpha^i)$ for $1 \leq i \leq 2t$.
- We now consider a general case that is also good for non-binary case.
- Suppose that the error pattern $\boldsymbol{e}(x)$ has v errors at locations

$0 \le j_1 < j_2 < \cdots < j_v \le n$. That is,

$$\boldsymbol{e}(x) = e_{j_1}x^{j_1} + e_{j_2}x^{j_2} + \cdots + e_{j_v}x^{j_v}.$$

- $$\begin{aligned} S_1 &= e_{j_1}\alpha^{j_1} + e_{j_2}\alpha^{j_2} + \cdots + e_{j_v}\alpha^{j_v} \\ S_2 &= e_{j_1}(\alpha^{j_1})^2 + e_{j_2}(\alpha^{j_2})^2 + \cdots + e_{j_v}(\alpha^{j_v})^2 \\ S_3 &= e_{j_1}(\alpha^{j_1})^3 + e_{j_2}(\alpha^{j_2})^3 + \cdots + e_{j_v}(\alpha^{j_v})^3 \\ &\vdots \\ S_{2t} &= e_{j_1}(\alpha^{j_1})^{2t} + e_{j_2}(\alpha^{j_2})^{2t} + \cdots + e_{j_v}(\alpha^{j_v})^{2t}, \qquad (3) \end{aligned}$$

  where $e_{j_1}, e_{j_2}, \ldots, e_{j_v}$, and $\alpha^{j_1}, \alpha^{j_2}, \ldots, \alpha^{j_v}$ are unknown.
- Any method for solving these equations is a decoding algorithm for the BCH codes.
- Let $Y_i = e_{j_i}$, $X_i = \alpha^{j_i}$, $1 \le i \le v$.

- (3) can be rewritten as follows:

$$\begin{aligned} S_1 &= Y_1X_1 + Y_2X_2 + \cdots + Y_vX_v \\ S_2 &= Y_1X_1^2 + Y_2X_2^2 + \cdots + Y_vX_v^2 \\ S_3 &= Y_1X_1^3 + Y_2X_2^3 + \cdots + Y_vX_v^3 \\ &\vdots \\ S_{2t} &= Y_1X_1^{2t} + Y_2X_2^{2t} + \cdots + Y_vX_v^{2t}. \end{aligned} \tag{4}$$

- We need to transfer the above set of non-linear equations into a set of linear equations.
- Consider the error-locator polynomial

$$\begin{aligned} \Lambda(x) &= (1 - X_1x)(1 - X_2x)\cdots(1 - X_vx) \\ &= 1 + \Lambda_1x + \Lambda_2x^2 + \cdots + \Lambda_vx^v. \end{aligned} \tag{5}$$

- Multiplying (5) by $Y_iX_i^{j+v}$, where $1 \le j \le v$, and set $x = X_i^{-1}$

we have

$$0 = Y_i X_i^{j+v} \left(1 + \Lambda_1 X_i^{-1} + \Lambda_2 X_i^{-2} + \cdots + \Lambda_v X_i^{-v}\right).$$

for $1 \leq i \leq v$.

- Summing all above v equations, we have

$$\begin{aligned} 0 &= \sum_{i=1}^{v} Y_i \left(X_i^{j+v} + \Lambda_1 X_i^{j+v-1} + \cdots + \Lambda_v X_i^{j}\right) \\ &= \sum_{i=1}^{v} Y_i X_i^{j+v} + \Lambda_1 \sum_{i=1}^{v} Y_i X_i^{j+v-1} + \cdots + \Lambda_v \sum_{i=1}^{v} Y_i X_i^{j} \\ &= S_{j+v} + \Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \cdots + \Lambda_v S_j. \end{aligned}$$

- We have

$$\Lambda_1 S_{j+v-1} + \Lambda_2 S_{j+v-2} + \cdots + \Lambda_v S_j = -S_{j+v}$$

for $1 \leq j \leq v$.

- Putting the above equations into matrix form we have

$$\begin{bmatrix} S_1 & S_2 & \cdots & S_{v-1} & S_v \\ S_2 & S_3 & \cdots & S_v & S_{v+1} \\ \vdots & & & & \\ S_v & S_{v+1} & \cdots & S_{2v-2} & S_{2v-1} \end{bmatrix} \begin{bmatrix} \Lambda_v \\ \Lambda_{v-1} \\ \vdots \\ \Lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{2v} \end{bmatrix}. \quad (6)$$

- Since $v \leq t$, $S_1, S_2, \ldots, S_{2v}$ are all known. Then we can solve for $\Lambda_1, \Lambda_2, \ldots, \Lambda_v$.
- We still need to find the smallest v such that the above system of equations has a unique solution.

- Let the matrix of syndromes, M, be defined as follows:

$$M = \begin{bmatrix} S_1 & S_2 & \cdots & S_u \\ S_2 & S_3 & \cdots & S_{u+1} \\ \vdots & \vdots & & \vdots \\ S_u & S_{u+1} & \cdots & S_{2u-1} \end{bmatrix}.$$

- M is nonsingular if u is equal to v, the number of errors that actually occurred. M is singular if $u > v$.

  Proof: Let

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ X_1 & X_2 & \cdots & X_u \\ \vdots & \vdots & & \vdots \\ X_1^{u-1} & X_2^{u-1} & \cdots & X_u^{u-1} \end{bmatrix}$$

with $A_{ij} = X_j^{i-1}$ and

$$B = \begin{bmatrix} Y_1X_1 & 0 & \cdots & 0 \\ 0 & Y_2X_2 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & Y_uX_u \end{bmatrix}$$

with $B_{ij} = Y_iX_i\delta_{ij}$, where

$$\delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

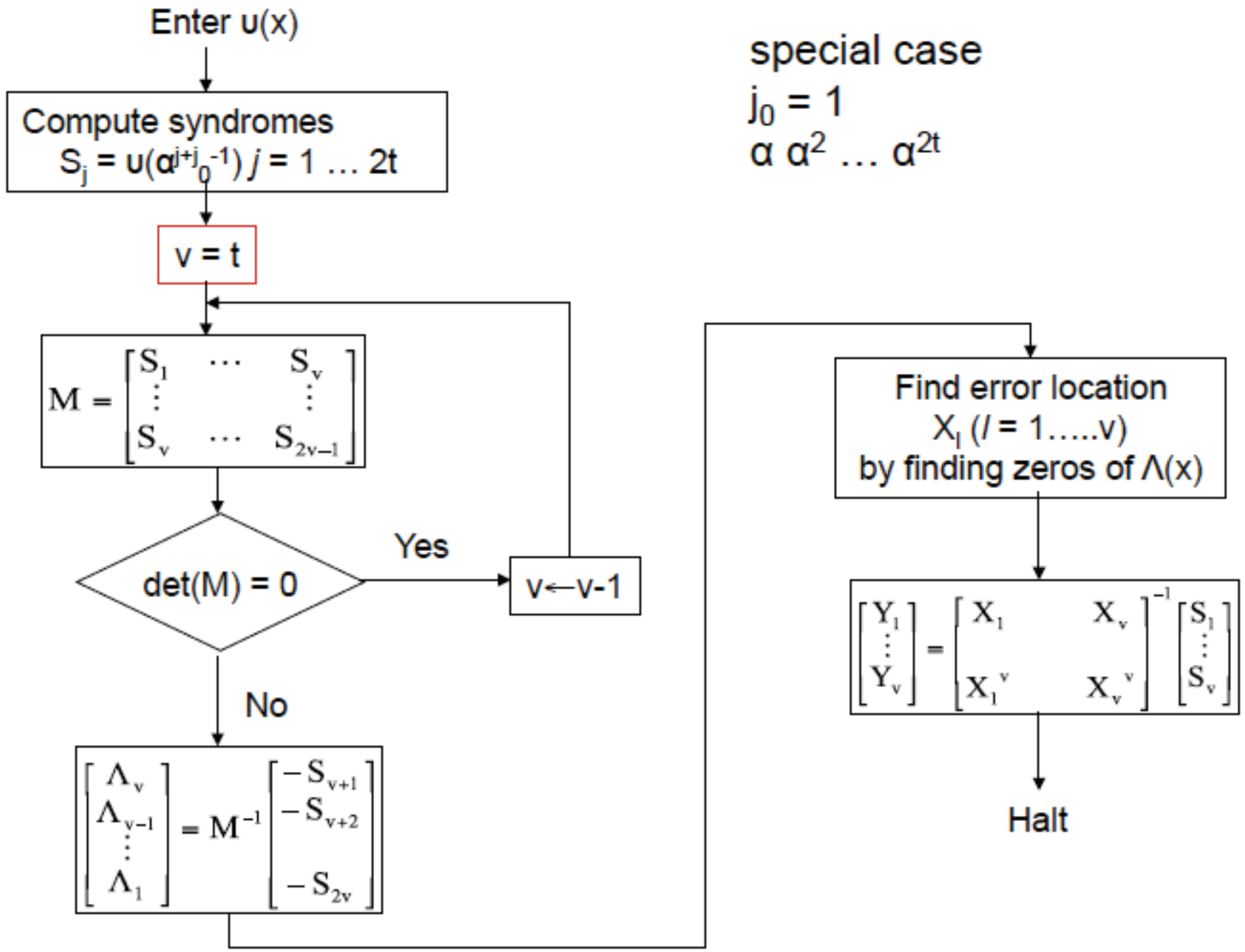
We have

$$\left(ABA^T\right)_{ij} = \sum_{\ell=1}^{u} X_\ell^{i-1} \sum_{k=1}^{u} Y_\ell X_\ell \delta_{\ell k} X_k^{j-1}$$

$$\begin{aligned} &= \sum_{\ell=1}^{u} X_\ell^{i-1} Y_\ell X_\ell X_\ell^{j-1} \\ &= \sum_{\ell=1}^{u} Y_\ell X_\ell^{i+j-1} = M_{ij}. \end{aligned}$$

Hence, $M = ABA^T$. If $u > v$, then $\det(B) = 0$ and then $\det(M) = \det(A)\det(B)\det(A^T) = 0$. If $u = v$, then $\det(B) \neq 0$. Since A is a Vandermonde matrix with $X_i \neq X_j$, $i \neq j$, $\det(A) \neq 0$. Hence, $\det(M) \neq 0$.

The Peterson-Gorenstein-Zierler Algorithm



Example

Consider the triple-error-correcting $(15, 5)$ BCH code with $\boldsymbol{g}(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Assume that the received vector is $\boldsymbol{r}(x) = x^2 + x^7$. The operating finite field is $GF(2^4)$. Then the syndromes can be calculated as follows:

$$
\begin{aligned}
S_1 &= \alpha^7 + \alpha^2 = \alpha^{12} \\
S_2 &= \alpha^{14} + \alpha^4 = \alpha^9 \\
S_3 &= \alpha^{21} + \alpha^6 = 0 \\
S_4 &= \alpha^{28} + \alpha^8 = \alpha^3 \\
S_5 &= \alpha^{35} + \alpha^{10} = \alpha^0 = 1 \\
S_6 &= \alpha^{42} + \alpha^{12} = 0.
\end{aligned}
$$

Set $v = 3$, we have

$$\begin{aligned}\det(M) &= \begin{vmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{vmatrix} \\ &= \begin{vmatrix} \alpha^{12} & \alpha^9 & 0 \\ \alpha^9 & 0 & \alpha^3 \\ 0 & \alpha^3 & 1 \end{vmatrix} = 0.\end{aligned}$$

Set $v = 2$, we have

$$\det(M) = \begin{vmatrix} S_1 & S_2 \\ S_2 & S_3 \end{vmatrix} = \begin{vmatrix} \alpha^{12} & \alpha^9 \\ \alpha^9 & 0 \end{vmatrix} \neq 0.$$

We then calculate

$$M^{-1} = \begin{bmatrix} 0 & \alpha^6 \\ \alpha^6 & \alpha^9 \end{bmatrix}.$$

Hence,

$$\begin{bmatrix} \Lambda_2 \\ \Lambda_1 \end{bmatrix} = M^{-1} \begin{bmatrix} 0 \\ \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^9 \\ \alpha^{12} \end{bmatrix}$$

and

$$\begin{aligned} \Lambda(x) &= 1 + \alpha^{12}x + \alpha^9 x^2 \\ &= \left(1 + \alpha^2 x\right)\left(1 + \alpha^7 x\right) \\ &= \alpha^9 \left(x - \alpha^8\right)\left(x - \alpha^{13}\right). \end{aligned}$$

Since $1/\alpha^8 = \alpha^7$ and $1/\alpha^{13} = \alpha^2$, we found the error locations.