i	$\tilde{R}^{(i)}(x)$	$s^{(i)}(x)$	Error?
0	$1+x^2+x^3+x^5+x^6$	x^2	No
1	$1+x+x^3+x^4+x^6$	$1+x$	No
2	$1+x+x^2+x^4+x^5$	$x+x^2$	No
3	$x+x^2+x^3+x^5+x^6$	$1+x+x^2$	No
4	$1+x^2+x^3+x^4+\cancel{x^6}$	$1+x^2$	Yes
5	$x+x^3+x^4+x^5$	1	No
6	$x^2+x^4+x^5+x^6$	x	No
7	$1+x^3+x^5+x^6$		

check this is a codeword.

Decoding BCH Codes

Euclid's Algorithm

Suppose we want the greatest common divisor of

28 and 6

$28 = 4 \cdot 6 + 4$

$6 = 1 \cdot 4 + 2$ ← take last remainder

$4 = 2 \cdot 2 + 0$ stop

Unraveling,

$$2 = 6 - 4 \cdot 1$$
$$= 6 - (28 - 4 \cdot 6)$$
$$= 5 \cdot 6 - 28 \cdot 1$$

Extended Euclid's Algorithm

Input: integers $a \geq b \geq 0$ **Output:** $d = \gcd(a,b)$ and x, y s.t. $ax + by = d$

Initialize:

$r_{-1} = a \qquad r_0 = b$

$s_{-1} = 1 \qquad s_0 = 0$

$t_{-1} = 0 \qquad t_0 = 1$

i^{th} step: divide r_{i-2} by r_{i-1}

$$r_{i-2} = q_i r_{i-1} + r_i$$

then $$t_i = t_{i-2} - q_i t_{i-1}$$
$$s_i = s_{i-2} - q_i s_{i-1}$$

Stop at $r_{n+1} = 0$

Then $$r_n = \gcd(a,b)$$
$$s_n a + t_n b = r_n$$

Example

$a = 23 \qquad b = 5$

	i	r_i	s_i	t_i	q_i
	-1	23	1	0	
	0	5	0	1	
	1	3	1	-4	4
	2	2	-1	5	1
n	3	1	2	-9	1
$n+1$	4	0			2

$\gcd = 1$

$1 = s_n a + t_n b$

$= 2 \cdot 23 - 9 \cdot 5$

Do $\tilde{S}(x)$ first.

Method

① Find $\tilde{S}(x)$

② Apply Extended Euclid's Algorithm with $a(x) = X^{2t}$ and $b(x) = \tilde{S}(x) \Rightarrow$ stop when degree of $r_i(x)$ is less than t. Read off $\sigma(x) = t_n(x)$.

③ Find roots of $\sigma(x)$. These powers of α correspond to error locations.

Examples ($n = 15$, $t = 3$ BCH code)

$$g(x) = m_\alpha(x)\, m_{\alpha^3}(x)\, m_{\alpha^5}(x)$$

$$\deg(g(x)) = 10 \quad \Rightarrow \quad k = 5 \quad \Rightarrow \quad (15, 5) \text{ TEC}$$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{14} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{13} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \cdots & \alpha^{12} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \cdots & \alpha^{11} \\ 1 & \alpha^5 & \alpha^{10} & 1 & \cdots & \alpha^{10} \\ 1 & \alpha^6 & \alpha^{12} & \alpha^3 & \cdots & \alpha^9 \end{pmatrix} \Bigg\} 10$$

Note: $\tilde{S}(x) = \tilde{S}_1 + \tilde{S}_2 X + \tilde{S}_3 X^2 + \cdots + \tilde{S}_{2t} X^{2t-1}$

where $\tilde{S}_i = r(\alpha^i) = [\,1 \;\; \alpha^i \;\; \alpha^{2i} \cdots \alpha^{(n-1)i}\,]^T \underline{r}$

Suppose

$$\underline{r} = (1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0)$$

$\tilde{S}_i = r(\alpha^i)$

$\tilde{S}_1 = r(\alpha)$

$= 0\ 0\ 0\ 1$ (0)
$0\ 0\ 1\ 0$ (1)
$0\ 1\ 0\ 0$ (2)
$1\ 1\ 0\ 0$ (6)
$1\ 0\ 1\ 1$ (7)
$0\ 1\ 1\ 1$ (10)
$1\ 1\ 1\ 0$ (11)
$1\ 1\ 1\ 1$ (12)
$1\ 1\ 0\ 1$ (13)

$1\ 0\ 1\ 1 = \alpha^7$

$\tilde{S}_3 = r(\alpha^3)$

cubed

~~0 0 0 1~~
~~1 0 0 0~~
~~1 1 0 0~~
$1\ 0\ 0\ 0$
$1\ 1\ 0\ 0$
~~0 0 0 1~~
~~1 0 0 0~~
~~1 1 0 0~~
$1\ 0\ 1\ 0$

$1\ 1\ 1\ 0 = \alpha^{11}$

$\tilde{S}_5 = r(\alpha^5)$

~~0 0 0 1~~
~~0 1 1 0~~
~~0 1 1 1~~
~~0 0 0 1~~
~~0 1 1 0~~
~~0 1 1 0~~
~~0 1 1 1~~
$0\ 0\ 0\ 1$
~~0 1 1 0~~

$0\ 0\ 0\ 1 = \alpha^0$

$\tilde{S}_2 = r(\alpha^2)$

$= [r(\alpha)]^2 = \alpha^{14}$

$\tilde{S}_4 = r(\alpha^4)$

$= [r(\alpha)]^4 = \alpha^{13}$

$\tilde{S}_6 = r(\alpha^6)$

$= [r(\alpha^3)]^2$

$= \alpha^7$

$s(x) = \alpha^7 x^5 + x^4 + \alpha^{13} x^3 + \alpha^{11} x^2 + \alpha^{14} x + \alpha^7$

Use exponent notation: $0 : \alpha^0 = 1$

$* : \alpha^{-\infty} = 0$

i	r_i	t_i	q_i
-1	$[0, *, *, *, *, *, *]$	$[*]$	–
0	$[7, 0, 13, 11, 14, 7]$	$[0]$	–
1	$[11, 9, 2, *, 8]$	$[8, 1]$	$[8, 1]$
2	$[8, 6, 9, *]$	$[4, 2, *]$	$[11, 14]$
stop → 3	$[7, *, 8]$	$[7, 5, 8, 1]$	$[3, *]$

deg $(r_i) < t$

$$
\begin{array}{r}
 & & & & & & & [8,\ 1] \\
\hline
7,0,13,11,14,7 & \big) & 0, & * & , & * & , & * & , & * & , & * \\
 & & \underline{0,} & \underline{8,} & \underline{6,} & \underline{4,} & \underline{7,} & \underline{0} \\
 & & 8, & 6, & 4, & 7, & 0, & * \\
 & & \underline{8,} & \underline{1,} & \underline{14,} & \underline{12,} & \underline{0,} & \underline{8} \\
 & & 11, & 9, & 2, & *, & 8 &
\end{array}
$$

$$
\begin{array}{r}
 & & & & & & [11,\ 14] \\
\hline
11,9,2,*,8 & \big) & 7, & 0, & 13, & 11, & 14, & 7
\end{array}
$$

remainder $[8, 6, 9, *]$

$$t_2 = [0] - [8, 1]\,[11, 14]$$

$$= [0] - [4, 12 + 7, 0]$$

$$= [0] - [4, 2, 0]$$

$$= [4, 2, *]$$

Thus, need to find roots of

$$\sigma(x) = \alpha^7 x^3 + \alpha^5 x^2 + \alpha^6 x + \alpha$$

$$= (x^3 + \alpha^{13} x^2 + \alpha x + \alpha^9)\alpha^7$$

Start plugging in elements:

	α^0	α	...	α^3
x^3	0001	1000		1010
$\alpha^{13} x^2$	1101	0001		0011
αx	0010	0100		0011
α^9	1010	1010		1010
	$0100 \neq 0$	$0111 \neq 0$		0000 $\Leftarrow \alpha^3$ is a root.

So are α^9 and α^{12}. Thus, correct errors in locations $\alpha^3, \alpha^9, \alpha^{12}$:

$r = (1\ 1\ 1\ \overset{1}{\underset{\uparrow}{\cancel{0}}}\ 0\ 0\ \overset{0}{\underset{\uparrow}{\cancel{1}}}\ 0\ 0\ 1\ 1\ \overset{0}{\underset{\uparrow}{\cancel{0}}}\ 1\ 0)$

$\alpha^3 \quad\quad \alpha^9 \quad\quad \alpha^{12}$

$\hat{c} = (1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0)$

(Check: show $\hat{c}$ satisfies all of the parity checks $\Rightarrow$

$$c(\alpha) = c(\alpha^2) = c(\alpha^3) = c(\alpha^4) = c(\alpha^5) = c(\alpha^6) = 0,$$