Chapter 5:
Cyclic Codes

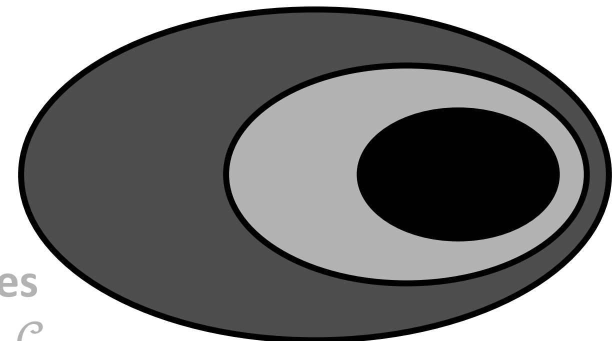
Hamid Meghdadi

Semnan University

hamid.meghdadi@gmail.com

Introduction to cyclic codes

- کدهای cyclic (چرخشی) زیر مجموعه‌ای از کدهای بلوکی خطی هستند.



Block codes
k information bits $\longrightarrow n$ coded bits

Linear Block codes
$v_1, v_2 \in \mathcal{C} \Longrightarrow (v_1 + v_2) \in \mathcal{C}$

Cyclic codes

- کد cyclic:

$$[v_0\ v_1\ v_2 \cdots v_{n-2}\ v_{n-1}] \in \mathcal{C}$$
$$\Downarrow$$
$$[v_{n-1}\ v_0\ v_1 \cdots\ v_{n-2}] \in \mathcal{C}$$

Definitions

$$\boldsymbol{v} = [v_0\ v_1\ v_2 \cdots v_{n-2}\ v_{n-1}]$$

- shift (چرخش) به راست به اندازه‌ی یک:

$$\boldsymbol{v}^{(1)} = [v_{n-1}\ v_0\ v_1 \cdots v_{n-3}\ v_{n-2}]$$

- shift (چرخش) به راست به اندازه‌ی i:

$$\boldsymbol{v}^{(i)} = [v_{n-i}\ v_{n-i+1} \cdots v_{n-1}\ v_0\ v_1 \cdots v_{n-i-2}\ v_{n-i-1}]$$

- نمایش بردارها:

$$\boldsymbol{v} = [v_0\ v_1\ v_2 \cdots v_{n-2}\ v_{n-1}]$$

$$v(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}$$

$$v_k \in \{0,1\}$$
$$X \in \{0,1\}$$

Polynomial operations in binary

- جمع:

$$(1+X)+(X+X^2)=1+0X+X^2=1+X^2=[1\ 0\ 1]$$

- ضرب:

$$(1+X)\cdot(X+X^2)=X+X^2+X^2+X^3=X+X^3=[0\ 1\ 0\ 1]$$

- تقسیم:

مقسوم

X^5+X+1 | X^2+1 مقسومٌ علیه

$+X^5+X^3$ | X^3+X خارج قسمت

X^3+X+1

$+X^3+X$

1

باقیمانده

$$\underbrace{(X^2+1)\cdot(X^3+X)}_{X^5+X^3+X^3+X=X^5+X}+1=X^5+X+1$$

Polynomial representation of cyclic shift

- شیفت چرخشی به اندازه‌ی یک واحد به راست:

$$\boldsymbol{v} = [v_0\ v_1\ v_2 \cdots v_{n-2}\ v_{n-1}]$$
$$v(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}$$

$$\boldsymbol{v}^{(1)} = [v_{n-1}\ v_0\ v_1 \cdots v_{n-3}\ v_{n-2}]$$
$$v^{(1)}(X) = v_{n-1} + v_0X + v_1X^2 + \cdots + v_{n-2}X^{n-1}$$

$$\underbrace{X.v(X)}_{\text{مقسوم}} = v_0X + v_1X^2 + v_2X^3 + \cdots + v_{n-2}X^{n-1} + v_{n-1}X^n + v_{n-1} + v_{n-1}$$
$$= \underbrace{v_{n-1} + v_0X + v_1X^2 + v_2X^3 + \cdots + v_{n-2}X^{n-1}}_{\text{باقیمانده}} + \underbrace{v_{n-1}}_{\text{خ‌ق}}\underbrace{(X^n + 1)}_{\text{م. علیه}}$$

$$\begin{array}{r|l} Xv(X) & X^n+1 \\ \hline & v_{n-1} \\ \overline{v^{(1)}(X)} & \end{array}$$

- شیفت چرخشی به اندازه‌ی i واحد به راست:

$$\begin{array}{r|l} X^iv(X) & X^n+1 \\ \hline & v_{n-i} + v_{n-i+1}X + \cdots + v_{n-1}X^i \\ \overline{v^{(i)}(X)} & \end{array}$$

Definition of cyclic codes

- کد cyclic یک کد بلوکی خطی است که در آن، شیفت یافته‌ی هرکلمه‌ی کد، خود یک کلمه‌ی کد معتبر باشد:

$$v(X) \in \mathcal{C} \Longrightarrow v^{(i)}(X) \in \mathcal{C}$$

- کدهای cyclic را معمولاً به صورت یک چند جمله‌ای باینری نمایش می‌دهیم:

$$\boldsymbol{v} = [v_0\ v_1\ v_2 \cdots v_{n-2}\ v_{n-1}] \Longrightarrow v(X) = v_0 + v_1X + v_2X^2 + \cdots + v_{n-1}X^{n-1}$$

- در یک کد (n,k) cyclic هر codeword یک چند جمله‌ای از درجه‌ی حداکثر $n-1$ است.

Example of a cyclic code

$$v(X) \in \mathcal{C} \Longrightarrow v^{(i)}(X) \in \mathcal{C}$$

message	codeword	Polynomial
u	v	v(X)
0000	0000000	$\mathbf{0}$
1000	1101000	$1+X+X^3$
0100	0110100	$X+X^2+X^4$
1100	1011100	$1+X^2+X^3+X^4$
0010	0011010	$X^2+X^3+X^5$
1010	1110010	$1+X+X^2+X^5$
0110	0101110	$X+X^3+X^4+X^5$
1110	1000110	$1+X^4+X^5$

message	codeword	Polynomial
u	v	v(X)
0001	0001101	$X^3+X^4+X^6$
1001	1100101	$1+X+X^4+X^6$
0101	0111001	$X+X^2+X^3+X^6$
1101	1010001	$1+X^2+X^6$
0011	0010111	$X^2+X^4+X^5+X^6$
1011	1111111	$1+X+X^2+X^3+X^4+X^5+X^6$
0111	0100011	$X+X^5+X^6$
1111	1001011	$1+X^3+X^5+X^6$

Code polynomial of minimum degree

- قضیه: در هر کد cyclic کلمه‌ی کد غیر صفر با حداقل درجه فقط یکی است.
  - مثلاً در کد مثال قبل، فقط یک کلمه‌ی کد با درجه‌ی۳ وجود دارد.

- اثبات: در غیر این‌صورت اگر دو کلمه‌ی کد با حداقل درجه (۳ در مثال قبل) وجود د اشته باشد با جمع آن دو می‌توان به یک کلمه‌ی کد با درجه‌ی کمتر رسید:

$$\boldsymbol{g} = [g_0\ g_1 \cdots g_{r-1}\ 1\ 0\ 0 \cdots 0]$$
$$g(X) = g_0 + g_1X + \cdots + g_{r-1}X^{r-1} + X^r$$

$$\boldsymbol{g}' = [g'_0\ g'_1 \cdots g'_{r-1}\ 1\ 0\ 0 \cdots 0]$$
$$g'(X) = g'_0 + g'_1X + \cdots + g'_{r-1}X^{r-1} + X^r$$

$$\Downarrow$$

$$g(X) + g'(X) \in \mathcal{C}$$

$$\boldsymbol{g} + \boldsymbol{g}' = [(g_0+g'_0)\ \ (g_1 + g'_1) \cdots (g_{r-1}+g'_{r-1})\ 0\ 0\ 0 \cdots 0]$$

Code polynomial of minimum degree starts with ‘1’

- قضیه: در هر کد cyclic اولین بیت کلمه‌ی کد با درجه‌ی حداقل حتماً ‘1’ است.
  - مثلاً در مثال قبل داشتیم: $[1101000] = 1 + X + X^3$

- اثبات: در غیر این صورت با یک شیفت چرخشی به اندازه‌ی یک واحد به یک کلمه‌ی کد با درجه‌ی کمتر می‌رسیم:

$$\begin{aligned} \boldsymbol{g} &= [0\ g_1 \cdots g_{r-1}\ 1\ 0\ 0 \cdots 0] \\ g(X) &= g_1 X + \cdots + g_{r-1} X^{r-1} + X^r \\ &= X(g_1 + g_2 X + \cdots + g_{r-1} X^{r-2} + X^{r-1}) \end{aligned} \quad \Longrightarrow \quad \begin{aligned} \boldsymbol{g}' &= [g_1 \cdots g_{r-1}\ 1\ 0\ 0 \cdots 0\ 0] \\ g'(X) &= g_1 + g_2 X + \cdots + g_{r-1} X^{r-2} + X^{r-1} \end{aligned}$$

از درجه‌ی r

از درجه‌ی $r-1$

تناقض

Codewords: multiples of code polynomial of minimum degree

- قضیه: در هر کد (n,k) cyclic، که در آن کلمه‌ی کد با درجه‌ی حد اقل به صورت زیر داده می‌شود:

$$g(X) = 1 + g_1 X + \cdots + g_{r-1} X^{r-1} + X^r$$

- هر چندجمله‌ای باینری با درجه‌ی حداکثر $n-1$ یک کلمه‌ی کد معتبر است اگر و تنها اگر مضرب $g(X)$ باشد.

- اثبات:
  - $v(X) = a(X)g(X)$ حتماً کلمه‌ی کد است چون یک ترکیب خطی از کلمه‌های کد $g(X)$، $Xg(X)$، ... و $X^{n-r-1}g(X)$ است.
  - اگر $v(x)$ یک کلمه‌ی کد معتبر باشد، با تقسیم آن بر $g(X)$ داریم: $v(X) = a(X)g(X) + b(X)$ که در آن $b(X)$ یا صفر است و یا دارای درجه‌ی کمتر از $g(X)$ است. با دوباره نوشتن رابطه‌ی فوق داریم: $b(X) = v(X) + a(X)g(X)$ که در آن $v(X)$ یک کلمه‌ی کد معتبر است و $a(X)g(X)$ هم بنا به قسمت اول قضیه، یک کلمه‌ی کد معتبر است، پس $b(X)$ که مجموع دو codeword است هم حتماً باید خود یک codeword باشد با درجه‌ی کمتر از $g(X)$ که امکان ندارد.

Codewords: multiples of code polynomial of minimum degree

$$g(X) = 1 + X + X^3$$

Polynomial	Multiple of g(X)
v(X)	a(X)g(X)
$\mathbf{0}$	$\mathbf{0} \cdot \boldsymbol{g(X)}$
$\mathbf{1 + X + X^3}$	$\mathbf{1} \cdot \boldsymbol{g(X)}$
$\boldsymbol{X + X^2 + X^4}$	$\boldsymbol{X \cdot g(X)}$
$\boldsymbol{1 + X^2 + X^3 + X^4}$	$\boldsymbol{(1 + X) \cdot g(X)}$
$\boldsymbol{X^2 + X^3 + X^5}$	$\boldsymbol{X^2 \cdot g(X)}$
$\boldsymbol{1 + X + X^2 + X^5}$	$\boldsymbol{(1 + X^2) \cdot g(X)}$
$\boldsymbol{X + X^3 + X^4 + X^5}$	$\boldsymbol{(X + X^2) \cdot g(X)}$
$\boldsymbol{1 + X^4 + X^5}$	$\boldsymbol{(1 + X + X^2) \cdot g(X)}$

Polynomial	Multiple of g(X)
v(X)	a(X)g(X)
$\boldsymbol{X^3 + X^4 + X^6}$	$\boldsymbol{X^3 \cdot g(X)}$
$\boldsymbol{1 + X + X^4 + X^6}$	$\boldsymbol{(1 + X^3) \cdot g(X)}$
$\boldsymbol{X + X^2 + X^3 + X^6}$	$\boldsymbol{(X + X^3) \cdot g(X)}$
$\boldsymbol{1 + X^2 + X^6}$	$\boldsymbol{(1 + X + X^3) \cdot g(X)}$
$\boldsymbol{X^2 + X^4 + X^5 + X^6}$	$\boldsymbol{(X^2 + X^3) \cdot g(X)}$
$\boldsymbol{1 + X + X^2 + X^3 + X^4 + X^5 + X^6}$	$\boldsymbol{(1 + X^2 + X^3) \cdot g(X)}$
$\boldsymbol{X + X^5 + X^6}$	$\boldsymbol{(X + X^2 + X^3) \cdot g(X)}$
$\boldsymbol{1 + X^3 + X^5 + X^6}$	$\boldsymbol{(1 + X + X^2 + X^3) \cdot g(X)}$

Code polynomial of minimum degree is of degree $n-k$

- قضیه: در هر کد (n,k) cyclic چندجمله‌ای کد با درجه‌ی حداقل حتماً از درجه‌ی $n-k$ است.
  - در مثال قبل داشتیم: $\left.\begin{matrix} n=7 \\ k=4 \end{matrix}\right\} \Longrightarrow g(X)=1+X+X^3$

- اثبات:

تمام codeword ها
حداکثر از درجه‌ی $\boldsymbol{n-1}$

$$v(X)=g(X)\cdot a(X)$$

$g(X)$: **از درجه‌ی $\boldsymbol{r}$**

$a(X)$: **حداکثر از درجه‌ی $\boldsymbol{n-r-1}$**

توان 0	توان 1	...	توان $n-r-1$
$\{0,1\}$	$\{0,1\}$		$\{0,1\}$

تعداد کل حالات = **تعداد کل codeword ها** = $\boldsymbol{2^{n-r}}$

تعداد کل کلمه‌های پیام = $\boldsymbol{2^{k}}$

$$k=n-r \Longrightarrow \boldsymbol{r=n-k}$$

Generator polynomial

- در هر کد (n,k) cyclic دقیقاً یک چندجمله‌ای از درجه‌ی $n-k$ به صورت زیر وجود دارد:

$$g(X) = 1 + g_1 X + g_2 X^2 + \cdots + g_{n-k1} X^{n-k-1} + X^{n-k}$$

- این چندجمله‌ای چند جمله‌ای مولد (generator) نامیده می‌شود به طوری که:
  - هر چندجمله‌ای کد معتبر، مضربی از $g(X)$ است، و
  - هر چند جمله‌ای از درجه‌ی $n-1$ یا کمتر که مضربی از $g(X)$ باشد، یک چندجمله‌ای کد معتبر است.

$g(X)$ is a factor of $X^n + 1$

- قضیه: در هر کد (n,k) cyclic چندجمله‌ای مولد حتماً فاکتوری از $x^n + 1$ است.
  - مثلاً در مثال قبل:

$$
\begin{array}{rl|l}
 & X^7 + 1 & X^3 + X + 1 \\ \cline{3-3}
+ & \underline{X^7 + X^5 + X^4} & X^4 + X^2 + X + 1 \\
 & X^5 + X^4 + 1 & \\
+ & \underline{X^5 + X^3 + X^2} & \\
 & X^4 + X^3 + X^2 + 1 & \\
+ & \underline{X^4 + X^2 + X} & \\
 & X^3 + X + 1 & \\
+ & \underline{X^3 + X + 1} & \\
 & 0 &
\end{array}
$$

$g(X)$ is a factor of $X^n + 1$

Generator matrix of cyclic codes

- قبلاً دیدیم که هر چندجمله‌ای کد مضربی از $g(X)$ است: $v(X) = a(X)g(X)$ که در آن $a(X)$ یک چندجمله‌ای از درجه‌ی حداکثر $k-1$ است:

$$a(X) = a_0 + a_1 X + \cdots + a_{k-1} X^{k-1}$$

- می‌توانیم فرض کنیم $a(X) = u(X) = \text{message}$. در این صورت:

$$\begin{aligned} v(X) &= u(X)g(X) \\ &= \left(u_0 + u_1 X + \cdots + u_{k-1} X^{k-1}\right) g(X) \\ &= u_0 g(X) + u_1 X g(X) + \cdots + u_{k-1} X^{k-1} g(X) \\ &= [u_0\, u_1 \cdots u_{k-1}] \begin{bmatrix} g(X) \\ Xg(X) \\ \vdots \\ X^{k-1} g(X) \end{bmatrix} \Rightarrow v = [u_0\, u_1 \cdots u_{k-1}] \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{n-k} \end{bmatrix} \end{aligned}$$

ماتریس مولد

- مثلاً برای مثال قبل داریم:

$$\boldsymbol{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Parity-check Matrix of cyclic codes

- می‌دانیم $g(X)$ فاکتوری از X^n+1 است: $X^n+1=g(X)h(X)$

$$h(X)=h_0+h_1X+h_2X^n+\cdots+h_kX^k$$

- اگر $v(X)$ یک چندجمله‌ای کد معتبر باشد، باقی‌مانده‌ی تقسیم $v(X)h(X)$ بر X^n+1 برابر صفر است:

$$\boxed{v(x)h(X)} = a(X)g(X)h(X) = \boxed{a(X)}[X^n+1]$$

ضرایب X^k تا X^{n-1} باید صفر باشند

ضرایب X^k تا X^{n-1} صفر هستند

حداکثر از درجه‌ی $k-1$

$$\sum_{i=0}^{k} h_i v_{n-i-j}=0 \quad 1\le j\le n-k$$

معادلات parity

- ماتریس H به صورت زیر به دست می‌آید:

$$\boldsymbol{H}=\begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0\\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & \dots & 0 & h_k & h_{k-1} & \dots & h_0\end{bmatrix}$$

- برای مثال قبل داریم (چرا؟):

$$\boldsymbol{H}=\begin{bmatrix}1&0&1&1&1&0&0\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix} \Rightarrow \boldsymbol{GH}^T=\boldsymbol{0}$$

Systematic cyclic codes

➢ با تعویض هریک از سطرهای با این روش . رسید می‌توان به یک کد معادل $\boldsymbol{G}$ با یک ترکیب خطی از سطرهای $\boldsymbol{G}$ می‌توان ماتریس $\boldsymbol{G}$ را به شکل سیستماتیک در آورد:

$$\boldsymbol{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

باید به ماتریس $\boldsymbol{I_{4\times4}}$ تبدیل شود

$$\boldsymbol{G_1} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{G_2} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$\boldsymbol{G}_{\text{sys}} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \longrightarrow \boldsymbol{I_{4\times4}}$$

$\text{row}_4 = \text{row}_2 + \text{row}_4$

Generating systematic cyclic codes

- ساختار یک codeword سیستماتیک:

Codeword:	Parity bits	Systematic part
n بیت	$n-k$ بیت	k بیت

$$a(X)g(X) = v(X) \quad = \quad b(X) \quad + \quad X^{n-k}u(X)$$

- برای encode کردن یک پیام:

  - ابتدا چندجمله‌ای پیام $u(X)$ را در X^{n-k} ضرب می‌کنیم.
  - چندجمله‌ای حاصل را بر $g(X)$ تقسیم می‌کنیم. باقیمانده‌ی حاصل را $b(X)$ می‌نامیم.
  - از ترکیب $u(X)$ و $b(X)$ چندجمله‌ای کد به دست می‌آید: $v(X) = b(X) + x^{n-k}u(X)$

Example: Encoding of a cyclic systematic code

$$g(X) = 1 + X + X^3$$

message	mult.	remaider	codeword
u	**$X^{n-k}u(X)$**	**b(X)**	**v**
0000	0	0	000 0000
1000	X^3	$1+X$	110 1000
0100			
1100			
0010			
1010			
0110			
1110			

message	mult.	remaider	codeword
u	**$X^{n-k}u(X)$**	**b(X)**	**v**
000			
1			
1			
1			
1			
1011			
0111			
1111			

$$X^3u(X) = X^3(1) = X^3$$

$$\begin{array}{rl|l} & X^3 & X^3+X+1 \\ \cline{3-3} + & X^3+X+1 & 1 \\ \cline{2-2} & X+1 & \end{array}$$

$$\begin{array}{cc} [1\ 1\ 0] & [1\ 0\ 0\ 0] \\ \Uparrow & \Uparrow \\ 1+X & \text{پیام} \end{array}$$

Example: Encoding of a cyclic systematic code

$$g(X) = 1 + X + X^3$$

message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v
0000	0	0	000 0000
1000	X^3	$1+X$	110 1000
0100	X^4	$X+X^2$	011 0100
1100	X^3+X^4	$1+X^2$	101 1100
0010			
1010			
0110			
1110			

message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v
0001			
1001			
0101			
1101			
0011			
1011			
0111			
1111			

$$
\begin{array}{rl|l}
 & X^4 + X^3 & X^3 + X + 1 \\ \cline{3-3}
+ & X^4 + X^2 + X & X + 1 \\ \cline{2-2}
 & X^3 + X^2 + X & \\
+ & X^3 + X + 1 & \\ \cline{2-2}
 & X^2 + 1 &
\end{array}
$$

Example: Encoding of a cyclic systematic code

$$g(X) = 1 + X + X^3$$

message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v
0000	0	0	000 0000
1000	X^3	$1+X$	110 1000
0100	X^4	$X+X^2$	011 0100
1100	X^3+X^4	$1+X^2$	101 1100
0010	X^5	$1+X+X^2$	[illegible]
1010	X^3+X^5	X^2	[illegible]
0110	X^4+X^5	1	100 0110
1110	$X^3+X^4+X^5$	X	010 1110

message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v
0001	X^6	[illegible]	[illegible]01
1001	X^3+X^6	[illegible]	[illegible]01
0101	X^4+X^6	[illegible]	[illegible]101
1101	$X^3+X^4+X^6$	0	000 1101
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
0111			
1111			

0 ⇓ [0 0 0]   پیام ⇓ [1101]

$$X^3u(X) = X^3(1+X+X^3) = X^3+X^4+X^6$$

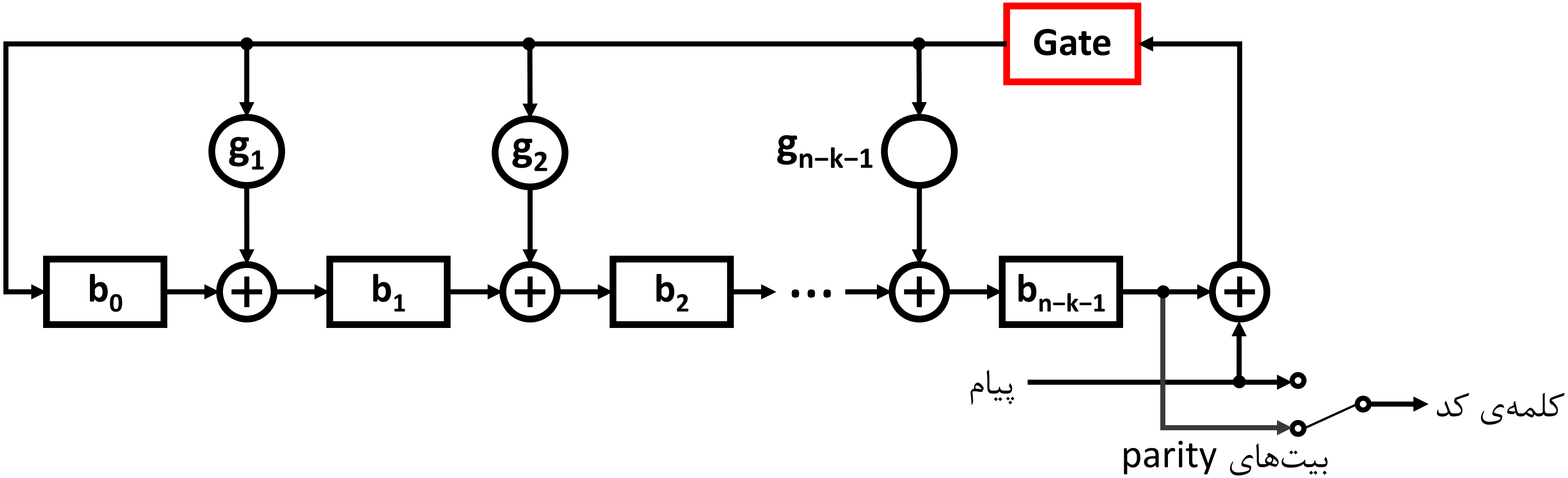
$$\begin{array}{r|l} X^6+X^4+X^3 & X^3+X+1 \\ \hline + \; X^6+X^4+X^3 & X^3+1 \\ \hline 0 & \end{array}$$

Example: Encoding of a cyclic systematic code

$$g(X) = 1 + X + X^3$$

message	mult.	remaider	codeword	message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v	u	$X^{n-k}u(X)$	b(X)	v
0000	0	0	000 0000	0001	X^6	$1+X^2$	101 0001
1000	X^3	$1+X$	110 1000	1001	X^3+X^6	$X+X^2$	011 1001
0100	X^4	$X+X^2$	011 0100	010			
1100	X^3+X^4	$1+X^2$	101 1100	110			
0010	X^5	$1+X+X^2$	111 0010	001			
1010	X^3+X^5	X^2	001 1010	1011	$X^3+X^5+X^6$	1	100 1011
0110	X^4+X^5	1	100 0110	0111	$X^4+X^5+X^6$	X^2	001 0111
1110	$X^3+X^4+X^5$	X	010 1110	1111	$X^3+X^4+X^5+X^6$	$1+X+X^2$	111 1111

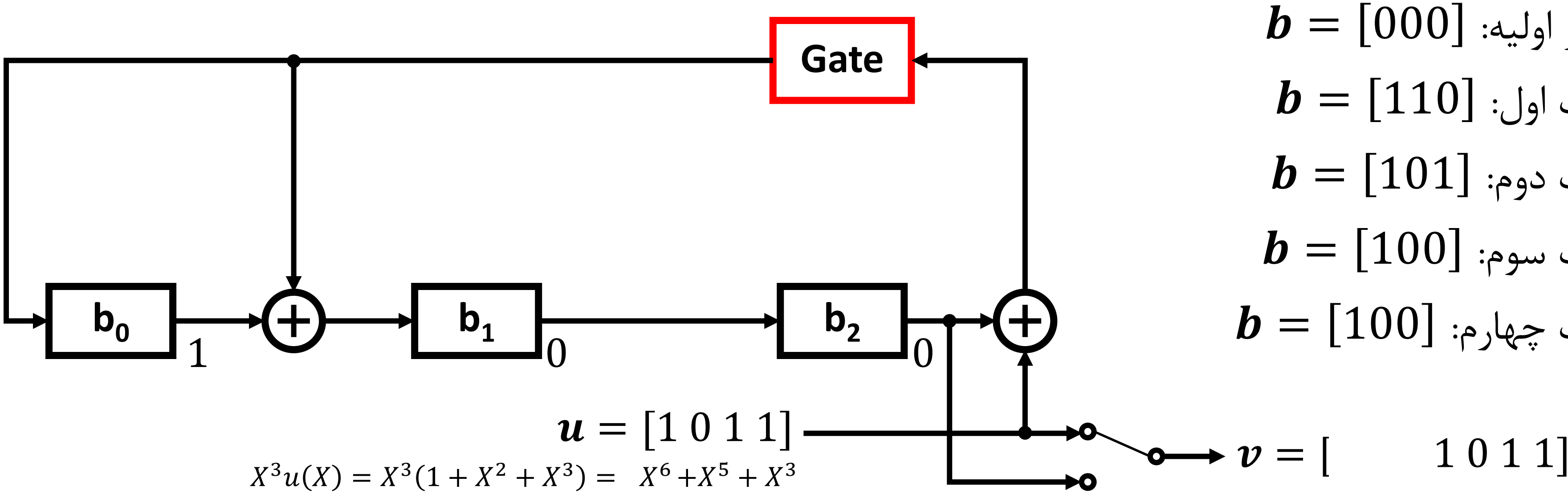
Encoder circuit for systematic cyclic codes



- gate روشن است: تعداد k بیت اطلاعات وارد مدار می‌شوند و به طور همزمان به خروجی ارسال می‌شوند.
- پس از ورود k بیت، مقادیر موجود در فلیپ فلاپ‌ها، حاصل باقی‌مانده‌ی تقسیم است.
- فیدبک مدار با خاموش کردن gate قطع می‌شود.
- تعداد n−k رقم بیت‌های parity به خروجی مدار شیفت داده می‌شود.
- بیت‌های پیام و بیت‌های parity در مجموع کلمه‌ی کد را تشکیل می‌دهند.

Example: Encoder circuit for (7,4) systematic cyclic code

- مقدار اولیه: $\boldsymbol{b} = [000]$
- کلاک اول: $\boldsymbol{b} = [110]$
- کلاک دوم: $\boldsymbol{b} = [101]$
- کلاک سوم: $\boldsymbol{b} = [100]$
- کلاک چهارم: $\boldsymbol{b} = [100]$



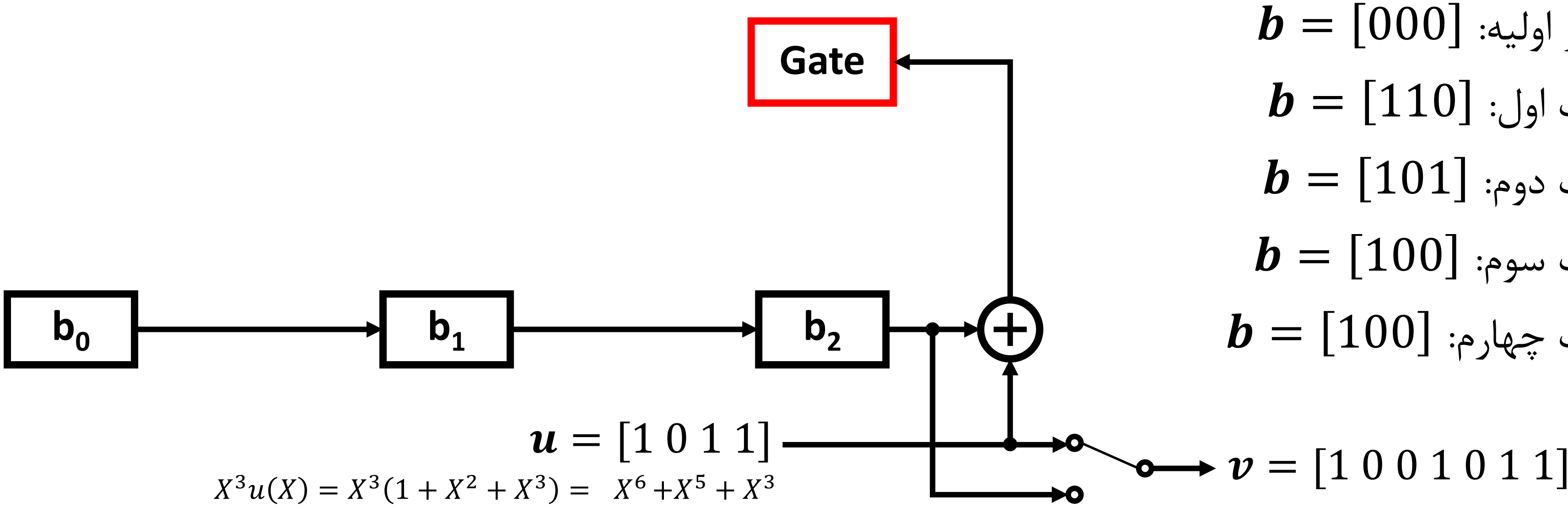
$X^3u(X) = X^3(1 + X^2 + X^3) = \ X^6 + X^5 + X^3$

$$
\begin{array}{l|l}
X^6 + X^5 + X^3 & X^3 + X + 1 \\
\hline
X^6 + X^4 + X^3 & X^3 + X^2 + X + 1 \\
\hline
X^5 + X^4 & \\
X^5 + X^3 + X^2 & \\
\hline
X^4 + X^3 + X^2 & \\
X^4 + X^2 + X & \\
\hline
X^3 + X & \\
X^3 + X + 1 & \\
\hline
1 &
\end{array}
$$

- در پایان ورود k بیت اطلاعات مقدار موجود در رجیسترها برابر حاصل باقی‌مانده‌ی تقسیم است:
- از این لحظه به بعد gate خاموش می‌شود.

Example: Encoder circuit for (7,4) systematic cyclic code

- مقدار اولیه: $\boldsymbol{b} = [000]$
- کلاک اول: $\boldsymbol{b} = [110]$
- کلاک دوم: $\boldsymbol{b} = [101]$
- کلاک سوم: $\boldsymbol{b} = [100]$
- کلاک چهارم: $\boldsymbol{b} = [100]$



$X^3u(X) = X^3(1 + X^2 + X^3) = \; X^6 + X^5 + X^3$

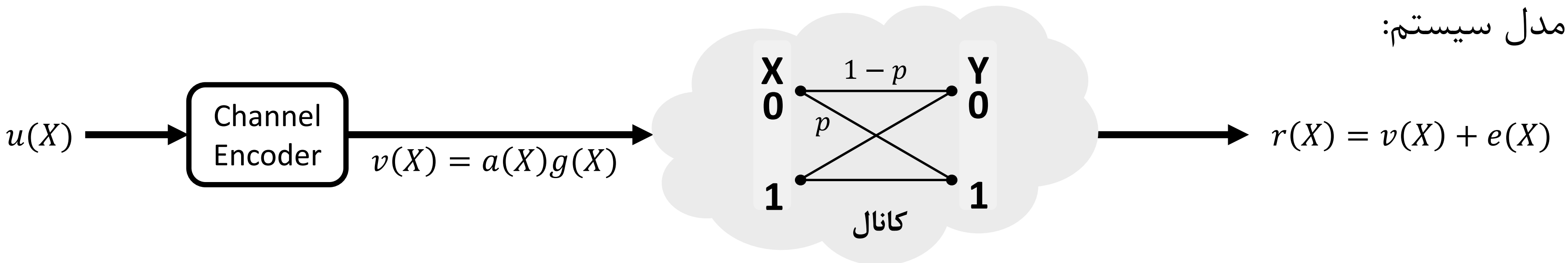
- در پایان ورود k بیت اطلاعات مقدار موجود در رجیسترها برابر حاصل باقی‌مانده‌ی تقسیم است:

$$
\begin{array}{l|l}
X^6 + X^5 + X^3 & X^3 + X + 1 \\ \cline{2-2}
\underline{X^6 + X^4 + X^3} & X^3 + X^2 + X + 1 \\
X^5 + X^4 & \\
\underline{X^5 + X^3 + X^2} & \\
X^4 + X^3 + X^2 & \\
\underline{X^4 + X^2 + X} & \\
X^3 + X & \\
\underline{X^3 + X + 1} & \\
1 &
\end{array}
$$

- از این لحظه به بعد gate خاموش می‌شود.
- با هر کلاک یک بیت از بیت‌های parity به خروجی منتقل می‌شود:
- کلاک پنجم: $\boldsymbol{b} = [010]$
- کلاک ششم: $\boldsymbol{b} = [001]$
- کلاک هفتم: $\boldsymbol{b} = [000]$

Error detection

➢ مدل سیستم:



➢ $r(X)$ یک کلمه‌ی کد معتبر است، اگر و تنها اگر $\mathbf{s} \triangleq \boldsymbol{rH}^T = \mathbf{0}$

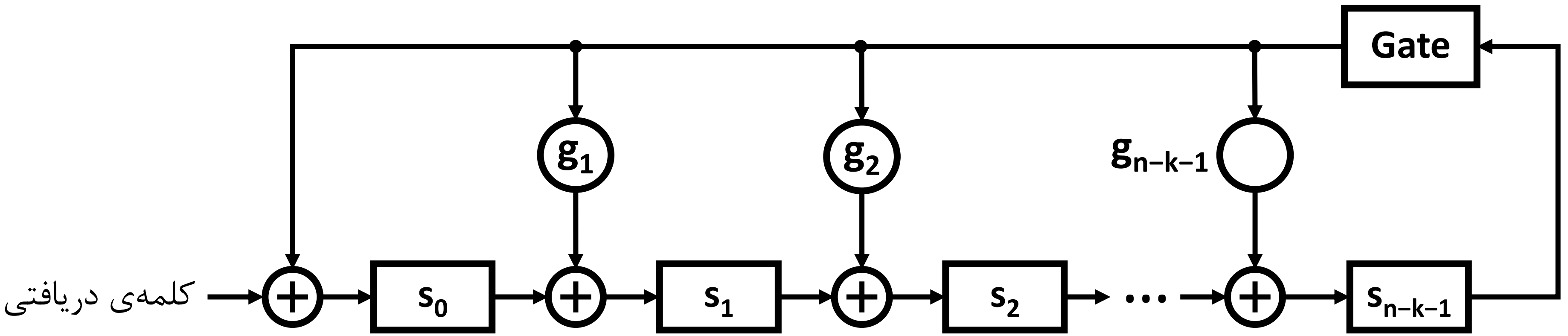
➢ تقسیم $r(X)$ بر $g(X)$:

$$\underbrace{r(X)}_{\text{حداکثر از درجه‌ی } n-1} = a'(X)\underbrace{g(X)}_{\text{از درجه‌ی } n-k} + \underbrace{s(X)}_{\text{حداکثر از درجه‌ی } n-k-1}$$

➢ برای تشخیص خطا کافیست چندجمله‌ای دریافتی را بر $g(X)$ تقسیم کنیم:

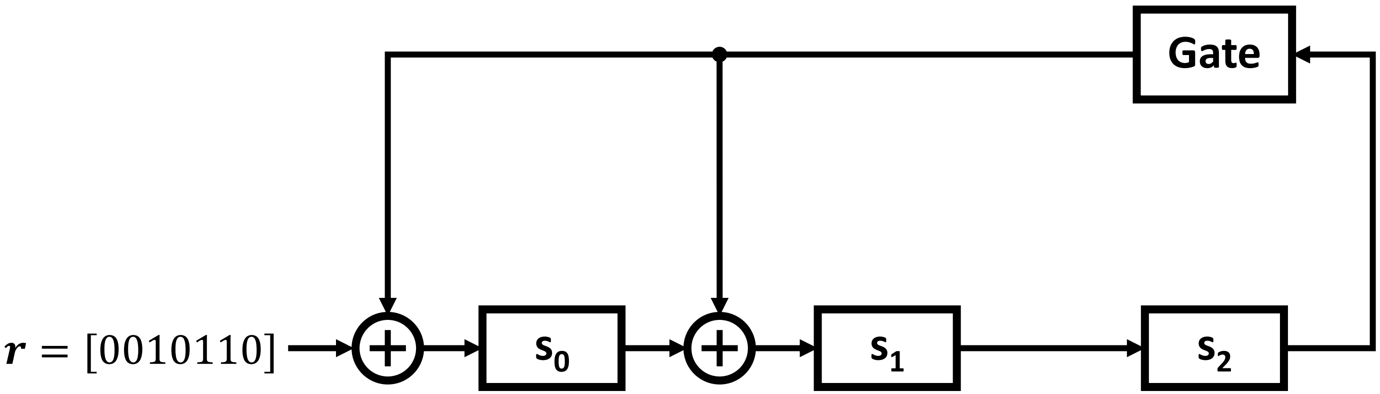
- اگر $r(X)$ چندجمله‌ای کد باشد $s(X) = 0$، در این صورت:
  - یا $e(X) = 0$: خطا اتفاق نیافتاده است.
  - یا $e(X) = b(X)g(X)$: خطا قابل تشخیص نیست.
- اگر $s(X) \neq 0$: خطا اتفاق افتاده و قابل تشخیص است.

Syndrome computation circuit



- پس از این‌که کلمه‌ی دریافتی کاملاً وارد رجیستر شد (n پالس کلاک)، مقادیر موجود در فلیپ فلاپ‌ها سندروم محاسبه شده هستند.
- کافیست در این لحظه خروجی فلیپ فلاپ‌ها با هم OR شوند تا بروز خطا تشخیص داده شود.
- gate در تمام مدت انجام عملیات روشن است.

Example: Syndrome computation circuit for (7,4) cyclic code

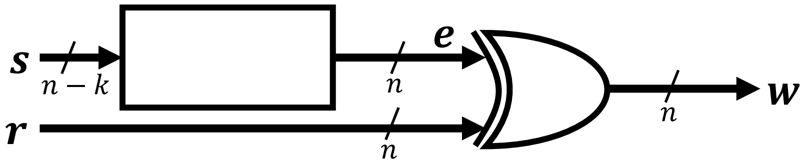


$$
\begin{array}{rl|l}
 & X^5 + X^4 + X^2 & X^3 + X + 1 \\ \cline{3-3}
+ & X^5 + X^3 + X^2 & X^2 + X + 1 \\ \cline{2-2}
 & X^4 + X^3 & \\
+ & X^4 + X^2 + X & \\ \cline{2-2}
 & X^3 + X^2 + X & \\
+ & X^3 + X + 1 & \\ \cline{2-2}
 & X^2 + 1 &
\end{array}
$$

- حالت اولیه: $\boldsymbol{s} = [000]$
- کلاک اول: $\boldsymbol{s} = [000]$
- کلاک دوم: $\boldsymbol{s} = [100]$
- کلاک سوم: $\boldsymbol{s} = [110]$
- کلاک چهارم: $\boldsymbol{s} = [011]$
- کلاک پنجم: $\boldsymbol{s} = [011]$
- کلاک ششم: $\boldsymbol{s} = [111]$
- کلاک هفتم: $\boldsymbol{s} = [101]$

Error correction in cyclic codes

- برای اصلاح خطا مانند قبل عمل می‌کنیم:
  - هر سندروم ← یک error pattern
  - به یک look-up table احتیاج داریم
  - مداری (با منطق ترکیبی) که سندروم را بگیرد و error pattern را تولید کند:



- در Matlab:

```
v = encode(u,n,k,'cyclic',poly)
```

```
v = encode([1 0 0 1],7,4,'cyclic',[1 1 0 1])
```

```
w = decode(r,n,k,'cyclic',poly)
```

```
w = decode([1 1 0 0 1 0 1],7,4,'cyclic',[1 1 0 1])
```

Error correction capability of cyclic codes

- قابلیت تشخیص خطا: $d_{min} - 1$
- ویژگی مهم کدهای cyclic: قابلیت بالای تشخیص error burst

v (codeword):	1	1	0	1	0	0	1	0	1	0	1	0	0	1	1
r (received word):	1	1	0	0	0	1	0	0	1	1	1	0	0	1	1
e (error pattern):	0	0	0	1	0	1	1	0	0	1	0	0	0	0	0
Error burst:															

- بسیاری از خطاها در سیستم‌های مخابراتی از نوع burst هستند.

- نوع خاص خطای burst: end-around error burst

v (codeword):	1	1	0	1	0	0	1	0	1	0	1	0	0	1	1
r (received word):	1	0	1	1	0	0	1	0	1	0	1	1	0	0	1
e (error pattern):	0	1	1	0	0	0	0	0	0	0	0	1	0	1	0
Error burst:															

Cyclic codes and error bursts

- فرض کنید که error pattern یک burst به طول $n-k$ یا کمتر باشد:
  - مثال:

Error pattern:

X^0	X^1	X^2	X^3	X^4	X^5	X^6	X^7	X^8	X^9	X^{10}	X^{11}	X^{12}	X^{13}	X^{14}
0	0	0	0	0	1	0	1	1	0	0	0	0	0	0

$$e(X) = X^8 + X^7 + X^5 = X^5(1 + X^2 + X^3)$$

- در این صورت داریم:

$$e(X) = X^i B(X)$$

به $g(X)$ بخش پذیر نیست

حداکثر از درجه‌ی $n-k-1$
نمی‌تواند به $g(X)$ که از درجه‌ی $n-k$ است بخش پذیر باشد

نسبت به $g(X)$ اول است

- هر کد cyclic (n,k) می‌تواند تمام error burst های به طول $n-k$ یا کمتر را تشخیص دهد.
- بسیاری از error burst های به طول $n-k+1$ و بیشتر هم قابل تشخیص هستند.

Cyclic codes and error bursts

➢ فرض کنید که error pattern یک burst به طول $n-k+1$ باشد:

Error pattern:	X^0	X^1	$\cdots$	X^{i-1}	X^i	X^{i+1}	$\cdots$	X^{i+n-k}	$X^{i+n-k+1}$	$\cdots$	X^{n-1}
	0	0	$\cdots$	0	1	?	?	1	0	$\cdots$	0
					تعداد 2^{n-k-1} حالت مختلف						

- چه تعدادی از این error burst ها قابل تشخیص نیستند؟
- چه تعدادی از این error pattern ها خود یک چندجمله‌ای کد هستند؟
- چه تعدادی از این error pattern ها بر $g(X)$ بخش پذیر هستند؟

$$e(X) = X^i\, B(X)$$

از درجه‌ی $n-k$
$g(X)$ از درجه‌ی $n-k$ است

نسبت به $g(X)$ اول است

- فقط یکی: $B(X) = g(X)$

➢ در هر کد (n,k) cyclic فقط کسر $\frac{1}{2^{n-k-1}}$ از error burst های به طول $n-k+1$ قابل تشخیص نیستند.

Cyclic codes and error bursts

➢ فرض کنید که error pattern یک burst به طول $l > n - k + 1$ باشد:

Error pattern:	X^0	X^1	$\cdots$	X^{i-1}	X^i	X^{i+1}	$\cdots$	X^{i+l}	X^{i+l+1}	$\cdots$	X^{n-1}
	0	0	$\cdots$	0	1	?	?	1	0	$\cdots$	0
					تعداد 2^{l-2} حالت مختلف						

- چه تعدادی از این error burst ها قابل تشخیص نیستند؟
- چه تعدادی از این error pattern ها خود یک چندجمله‌ای کد هستند؟
- چه تعدادی از این error pattern ها بر $g(X)$ بخش پذیر هستند؟

نسبت به $g(X)$ اول است

$$e(X) = X^i \, B(X)$$

از درجه‌ی $l - 1$
$g(X)$ از درجه‌ی $n - k$ است

- برای چه تعدادی از این error pattern ها، $B(X)$ بر $g(X)$ بخش پذیر است؟

$$e(X) = X^i a(X) g(X)$$

- تعداد: $2^{l-(n-k)-2}$

➢ در هر کد (n,k) cyclic فقط کسر $\frac{1}{2^{n-k}}$ از tsrub rorre های به طول $l > n - k + 1$ قابل تشخیص نیستند.

Shortened cyclic codes

- هدف: به دست آوردن یک کد $(n-l, k-l)$ از یک کد (n, k) cyclic
- چگونه؟
  - انتخاب کلمه‌های کدی که در آن l بیت سمت راست برابر صفر هستند
    - چند تا؟
  - استفاده از این کدها (بدون صفرهای انتهایی) به عنوان یک کد جدید.
    - $(n-l, k-l)$
- قابلیت تشخیص خطا: حداقل به اندازه‌ی کد اصلی
  - چرا؟
- کد دیگر cyclic نیست.
  - چرا؟
- مدار encoder مانند مدار کد اصلی.
  - چرا؟
- مدار decoder؟

Example: Shortened cyclic codes

➢ کد اصلی:

message	mult.	remaider	codeword	message	mult.	remaider	codeword
u	$X^{n-k}u(X)$	b(X)	v	u	$X^{n-k}u(X)$	b(X)	v
0000	$\mathbf{0}$	$\mathbf{0}$	**000 0000**	0001	X^6	$1+X^2$	101 0001
1000	$\boldsymbol{X^3}$	$\boldsymbol{1+X}$	**110 1000**	1001	X^3+X^6	$X+X^2$	011 1001
0100	$\boldsymbol{X^4}$	$\boldsymbol{X+X^2}$	**011 0100**	0101	X^4+X^6	$1+X$	110 0101
1100	$\boldsymbol{X^3+X^4}$	$\boldsymbol{1+X^2}$	**101 1100**	1101	$X^3+X^4+X^6$	0	000 1101
0010	X^5	$1+X+X^2$	111 0010	0011	X^5+X^6	X	010 0011
1010	X^3+X^5	X^2	001 1010	1011	$X^3+X^5+X^6$	1	100 1011
0110	X^4+X^5	1	100 0110	0111	$X^4+X^5+X^6$	X^2	001 0111
1110	$X^3+X^4+X^5$	X	010 1110	1111	$X^3+X^4+X^5+X^6$	$1+X+X^2$	111 1111

Example: Shortened cyclic codes

- کد جدید:

message			codeword
u			v
00			000 00
10			110 10
01			011 01
11			101 11