Cơ sở lí thuyết thông tin

Chương 4: Mã vòng CRC

TS. Phạm Hải Đăng

Phần 1: Khái niệm cơ bản

- Định nghĩa Mã vòng
  - Mã vòng là mã khối tuyến tính *C(n,k)*.
  - Nếu *c* là từ mã của mã vòng *C(n,k)*, các dịch vòng của từ mã *c* cũng là từ mã của mã vòng *C(n,k)*.

$$c = (c_0, c_1, \ldots, c_{n-1})$$

$$c^{(1)} = (c_{n-1}, c_0, c_1, \ldots, c_{n-2}$$

- Cấu trúc dịch vòng giúp cho việc tính toán mã hóa và giải mã, tính toán vector syndrome trở nên dễ dàng.

Phần 1: Khái niệm cơ bản

- Biểu diễn mã vòng dưới dạng đa thức

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$$

$$c^{(1)}(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1}$$

  - Mỗi từ mã *c(x)* đều có bậc lớn hơn hoặc bằng *n-k*, nhỏ hơn hoặc bằng *n-1*

$$(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \leftrightarrow xc(x)$$

$$(c_{n-2}, c_{n-1}, c_0, \ldots, c_{n-3}) \leftrightarrow x^2 c(x)$$

$$\vdots$$

$$(c_1, c_2, \ldots, c_{n-1}, c_0) \leftrightarrow x^{n-1} c(x)$$

Phần 1: Khái niệm cơ bản

- Đa thức sinh *g(x)*
  - Chỉ có duy nhất một đa thức sinh *g(x)* với mỗi mã vòng.
  - Bậc của đa thức sinh *g(x)* phải nhỏ hơn hoặc bằng *n-k*.
  - Đa thức từ mã *c(x)* phải chia hết cho đa thức sinh *g(x)*.

$$\mathrm{g}(x) = g_0 + g_1 x + g_2 x^2 + \ldots + g_{n-k} x^{n-k}$$

$$g_0 = g_{n-k} = 1$$

- Đa thức từ mã đều có thể biểu diễn dưới dạng

$$c(x) = m(x) g(x)$$

trong đó $m(x) = m_0 + m_1 x + m_2 x^2 + \ldots + m_{k-1} x^{k-1}$ là đa thức bản tin

- Tính chất của đa thức sinh
  - Đa thức sinh g(x) luôn được là đa thức con của đa thức $x^n - 1$
  - Tất cả các đa thức con của đa thức $x^n - 1$ với bậc *(n-k)* đều có thể sử dụng làm đa thức sinh.
  - Do $x^n - 1$ chia hết cho *g(x)*

$$x^n - 1 = h(x)g(x)$$

trong đó
$$h(x) = h_0 + h_1 x + h_2 x^2 + \ldots + h_k x^k$$
$$h_0 = h_k = 1$$

h(x) là đa thức kiểm tra của đa thức sinh *g(x)* của mã vòng (n,k).

Phần 1: Khái niệm cơ bản

- Ví dụ:

$$x^{15}-1=(1+x)(1+x+x^2)(1+x+x^4)(1+x+x^2+x^3+x^4)(1+x^3+x^4)$$

  - Các đa thức con có bậc 1, 2, 4, 4, 4.
  - Đa thức $g(x)=(1+x+x^2)(1+x+x^4)(1+x+x^2+x^3+x^4)$. được sử dụng cho mã vòng (15,5)
  - Đa thức $g(x)=(1+x)(1+x+x^4)$ có thể sử dụng cho mã vòng (15, 10)

Bảng mã chuẩn CRC

Table 4.6: CRC Generators

CRC Code	Generator Polynomial
CRC-4	$g(x) = x^4 + x^3 + x^2 + x + 1$
CRC-7	$g(x) = x^7 + x^6 + x^4 + 1$
CRC-8	$g(x) = x^8 + x^7 + x^6 + x^4 + x^2 + 1$
CRC-12	$g(x) = x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-ANSI	$g(x) = x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	$g(x) = x^{16} + x^{12} + x^5 + 1$
CRC-SDLC	$g(x) = x^{16} + x^{15} + x^{13} + x^7 + x^4 + x^2 + x + 1$
CRC-24	$g(x) = x^{24} + x^{23} + x^{14} + x^{12} + x^8 + 1$
CRC-32a	$g(x) = x^{32} + x^{30} + x^{22} + x^{15} + x^{12} + x^{11} + x^7 + x^6 + x^5 + x$
CRC-32b	$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

Phần 2: Mã hóa và giải mã không hệ thống

- Vector bản tin $\mathbf{m} = [m_0 \quad m_1 \quad \ldots \quad m_{k-1}]$

  biểu diễn dạng đa thức $m(x) = m_0 + \cdots + m_{k-1}x^{k-1}$

- Từ mã dạng không hệ thống (nonsystematic)

$$\begin{aligned} c(x) &= m(x)g(x) \\ &= (m_0 g(x) + m_1 x g(x) + \cdots m_{k-1} x^{k-1} g(x)) \end{aligned}$$

- Quá trình mã hóa không hệ thống biểu diễn dạng ma trận

$$c(x) = [m_0 \quad m_1 \quad m_2 \quad \cdots \quad m_{k-1}] \begin{bmatrix} g(x) \\ x g(x) \\ x^2 g(x) \\ \vdots \\ x^{k-1} g(x) \end{bmatrix}$$

Phần 2: Mã hóa và giải mã không hệ thống

- Biểu diễn dạng ma trận

$$c(x) = \begin{bmatrix} m_0 & m_1 & m_2 & \cdots & m_{k-1} \end{bmatrix} \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \\ \vdots \\ x^{k-1} g(x) \end{bmatrix}$$

$$\mathbf{c}_m = [m_0, m_1, \ldots, m_{k-1}] \begin{bmatrix} g_0 & g_1 & \cdots & g_r & & & & \\ & g_0 & g_1 & \cdots & g_r & & & \\ & & g_0 & g_1 & \cdots & g_r & & \\ & & & \ddots & \ddots & & \ddots & \\ & & & & g_0 & g_1 & \cdots & g_r & \\ & & & & & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

Phần 2: Mã hóa và giải mã không hệ thống

- Ví dụ: với mã vòng *n=7*

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

Ma trận sinh ***G*** dạng không hệ thống được biểu diễn

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

- Bảng quan hệ giữa bản tin và từ mã (dạng vector và dạng đa thức)

m	$m(x)g(x)$	code polynomial	codeword
(0,0,0)	$0g(x)$	0	0000000
(1,0,0)	$1g(x)$	$1+x^2+x^3+x^4$	1011100
(0,1,0)	$xg(x)$	$x+x^3+x^4+x^5$	0101110
(1,1,0)	$(x+1)g(x)$	$1+x+x^2+x^5$	1110010
(0,0,1)	$x^2g(x)$	$x^2+x^4+x^5+x^6$	0010111
(1,0,1)	$(x^2+1)g(x)$	$1+x^3+x^5+x^6$	1001011
(0,1,1)	$(x^2+x)g(x)$	$x+x^2+x^3+x^6$	0111001
(1,1,1)	$(x^2+x+1)g(x)$	$1+x+x^4+x^6$	1100101

Giải mã vòng dạng không hệ thống

$$
\begin{aligned}
c(x)h(x) &= m(x)g(x)h(x) \\
&= \mathrm{m(x)}\left(x^n - 1\right) \\
&\equiv 0
\end{aligned}
$$

- Đa thức thu được phía thu *r(x)*. Để kiểm tra *r(x)*

$$s(x) = r(x)h(x) \quad (\mathrm{mod}\ x^n - 1)$$

- *s(x)* là đa thức syndrome. *s(x)*=0 khi và chỉ khi *r(x)* là từ mã.

Phần 2: Mã hóa và giải mã không hệ thống

Xây dựng ma trận kiểm tra dạng không hệ thống

$$c(x)h(x) = m(x)g(x)h(x) = m(x)(x^n - 1) = m(x) - m(x)x^n$$

- Do bậc của *m(x)* nhỏ hơn *k*, do đó các hệ số $x^k, x^{k+1}, \ldots, x^{n-1}$ bằng 0 trong đa thức $m(x) - m(x)x^n$

  Do đó, $x^k, x^{k+1}, \ldots, x^{n-1}$ có hệ số bằng 0 trong đa thức $c(x)\bar{h}(x)$

$$\sum_{i=0}^{k} h_i c_{l-i} = 0 \text{ for } l = k, k+1, \ldots, n-1$$

- Ma trận kiểm tra dạng không hệ thống được biểu diễn dạng

$$\begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & & \\ & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & \\ & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & \\ & & & \ddots & & & & \ddots & \\ & & & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} = \mathbf{0}$$

Phần 2: Mã hóa và giải mã không hệ thống

Xây dựng ma trận kiểm tra dạng không hệ thống

$$c(x)h(x) = m(x)g(x)h(x) = m(x)(x^n - 1) = m(x) - m(x)x^n$$

- Do bậc của *m(x)* nhỏ hơn *k*, do đó các hệ số $x^k, x^{k+1}, \ldots, x^{n-1}$ bằng 0 trong đa thức $m(x) - m(x)x^n$

  Do đó, $x^k, x^{k+1}, \ldots, x^{n-1}$ có hệ số bằng 0 trong đa thức $c(x)\bar{h}(x)$

$$\sum_{i=0}^{k} h_i c_{l-i} = 0 \text{ for } l = k, k+1, \ldots, n-1.$$

- Ma trận kiểm tra dạng không hệ thống được biểu diễn dạng

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & & \\ & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & & \\ & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & & \\ & & & \ddots & & & & \ddots & \\ & & & & h_k & h_{k-1} & h_{k-2} & \cdots & h_0 \end{bmatrix}$$

Phần 2: Mã hóa và giải mã không hệ thống

- Ví dụ: Cho mã vòng (7,3) với đa thức sinh $g(x) = x^4 + x^3 + x^2 + 1$

Xây dựng ma trận sinh và ma trận kiểm tra dạng không hệ thống.

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

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & & & \\ & 1 & 1 & 0 & 1 & & \\ & & 1 & 1 & 0 & 1 & \\ & & & 1 & 1 & 0 & 1 \end{bmatrix}$$

Phần 3: Mã hóa và giải mã dạng hệ thống

Cho đa thức bản tin *m(x)* và đa thức sinh *g(x)*.

Từ mã dạng hệ thống được xây dựng theo công thức sau:

- Thực hiện phép chia đa thức lấy phần dư *d(x)*

$$x^{n-k}m(x) = q(x)g(x) + d(x)$$

- Từ mã dạng hệ thống của bản tin *m(x)* được tính như sau

$$c(x) = x^{n-k}m(x) - d(x)$$

  - Từ mã *c(x)* thỏa mãn điều kiện chia hết cho đa thức sinh *g(x)*, có bậc lớn hơn *(n-k)* và nhỏ hơn *n*.
  - Từ mã được biểu diễn dạng vector

$$c = [-d_0, -d_1, \ldots, -d_{n-k-1}, m_0, m_1, \ldots, m_{k-1}]$$

- Biểu diễn ma trận sinh và ma trận kiểm tra dạng hệ thống

$$
\begin{array}{cl}
\begin{bmatrix}
g_0 & g_1 & \cdots & g_r & & & & & \\
 & g_0 & g_1 & \cdots & g_r & & & & \\
 & & g_0 & g_1 & \cdots & g_r & & & \\
 & & & \ddots & \ddots & & \ddots & & \\
 & & & & g_0 & g_1 & \cdots & g_r & \\
 & & & & & g_0 & g_1 & \cdots & g_r
\end{bmatrix}
&
\begin{array}{l}
\longrightarrow \mathrm{mod}(x^{n-k}) \\
\longrightarrow \mathrm{mod}(x^{n-k+1}) \\
\longrightarrow \mathrm{mod}(x^{n-k+2}) \\
\\
\\
\longrightarrow \mathrm{mod}(x^{n-1})
\end{array}
\end{array}
$$

Tương đương với việc thực hiện phép chia lấy phần dư với các hàng trong ma trận G

$$x^{n-k+i} = q_i(x)g(x) + b_i(x), \qquad i = 0, 1, \ldots, k-1$$

Thu được ma trận sinh dạng hệ thống

$$
G = \begin{bmatrix}
-b_{0,0} & -b_{0,1} & \cdots & -b_{0,n-k-1} & 1 & 0 & 0 & \cdots & 0 \\
-b_{1,0} & -b_{1,1} & \cdots & -b_{1,n-k-1} & 0 & 1 & 0 & \cdots & 0 \\
-b_{2,0} & -b_{2,1} & \cdots & -b_{2,n-k-1} & 0 & 0 & 1 & \cdots & 0 \\
\vdots & & & & & & & & \\
-b_{k-1,0} & -b_{k-1,1} & \cdots & -b_{k-1,n-k-1} & 0 & 0 & 0 & \cdots & 1
\end{bmatrix} = [P \mid I]
$$

Phần 3: Mã hóa và giải mã dạng hệ thống

- Ma trận kiểm tra dạng hệ thống

$$H = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & b_{0,0} & b_{1,0} & b_{2,0} & \cdots & b_{k-1,0} \\ 0 & 1 & 0 & \cdots & 0 & b_{0,1} & b_{1,1} & b_{2,1} & \cdots & b_{k-1,1} \\ 0 & 0 & 1 & \cdots & 0 & b_{0,2} & b_{1,2} & b_{2,2} & \cdots & b_{k-1,2} \\ \vdots & & & & & & & & & \\ 0 & 0 & 0 & \cdots & 1 & b_{0,n-k-1} & b_{1,n-k-1} & b_{2,n-k-1} & \cdots & b_{k-1,n-k-1} \end{bmatrix} = \left[I \mid P^T \right]$$

Phần 3: Mã hóa và giải mã dạng hệ thống

- Ví dụ: Cho đa thức sinh $g(x) = 1 + x + x^3$

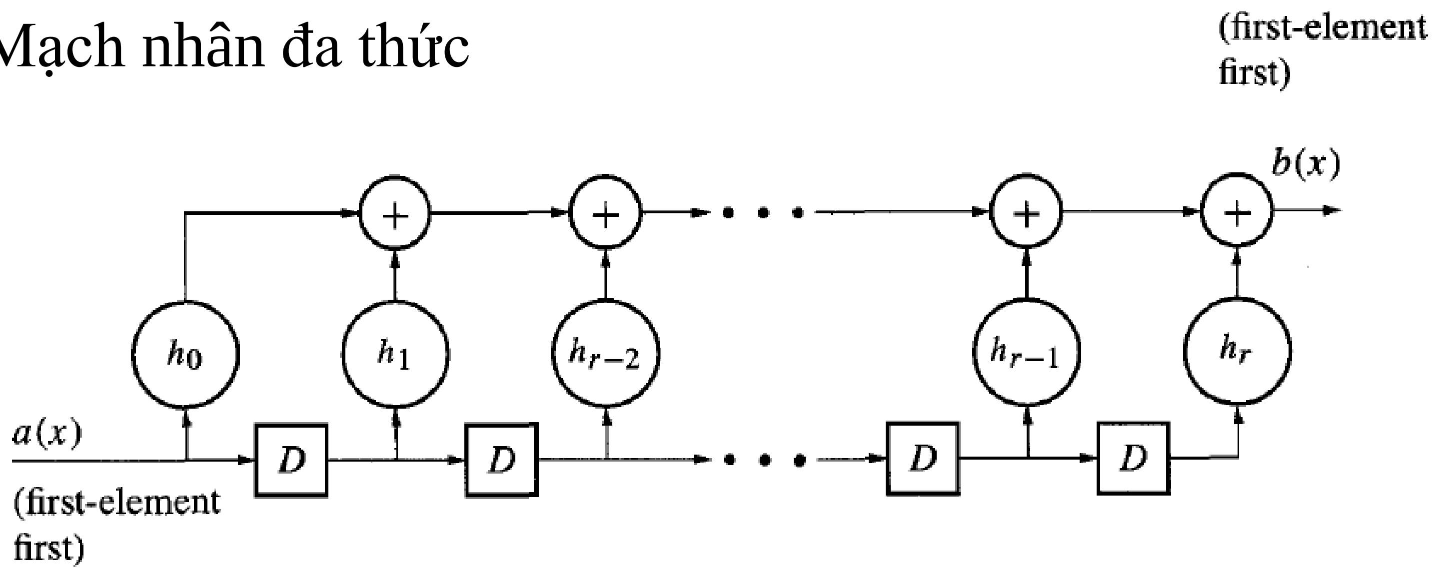
Biểu diễn ma trận sinh và ma trận kiểm tra dạng hệ thống.

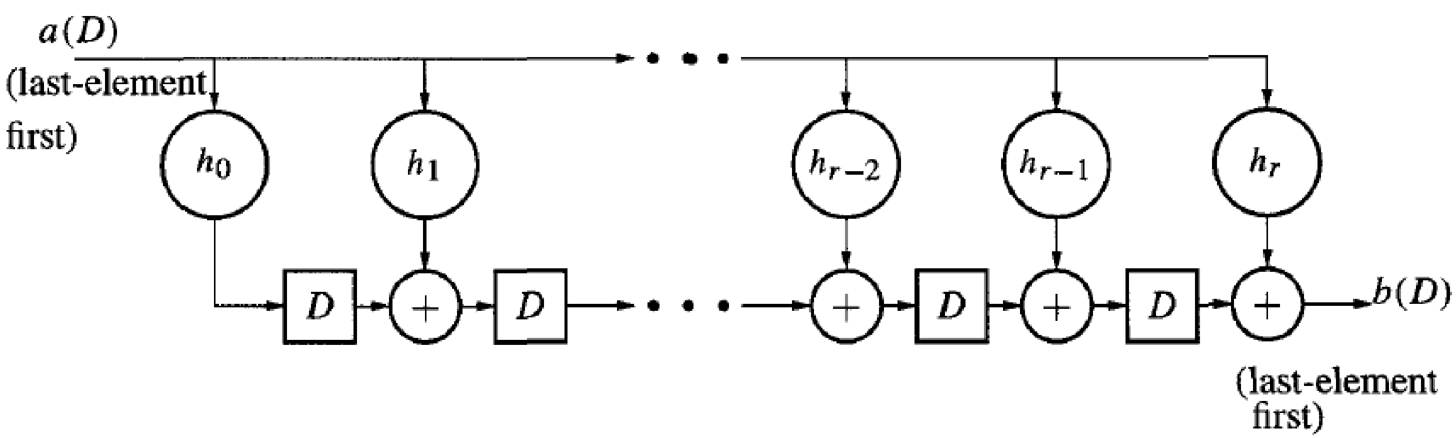
$$
\begin{aligned}
i = 0:&\quad x^3 &&= g(x) + (1 + x) &\qquad b_0(x) &= 1 + x \\
i = 1:&\quad x^4 &&= xg(x) + (x + x^2) &\qquad b_1(x) &= x + x^2 \\
i = 2:&\quad x^5 &&= (x^2 + 1)g(x) + (1 + x + x^2) &\qquad b_2(x) &= 1 + x + x^2 \\
i = 3:&\quad x^6 &&= (x^3 + x + 1)g(x) + (1 + x^2) &\qquad b_3(x) &= 1 + x^2
\end{aligned}
$$

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

Phần 4: Thực hiện phần cứng mã hóa giải mã vòng CRC

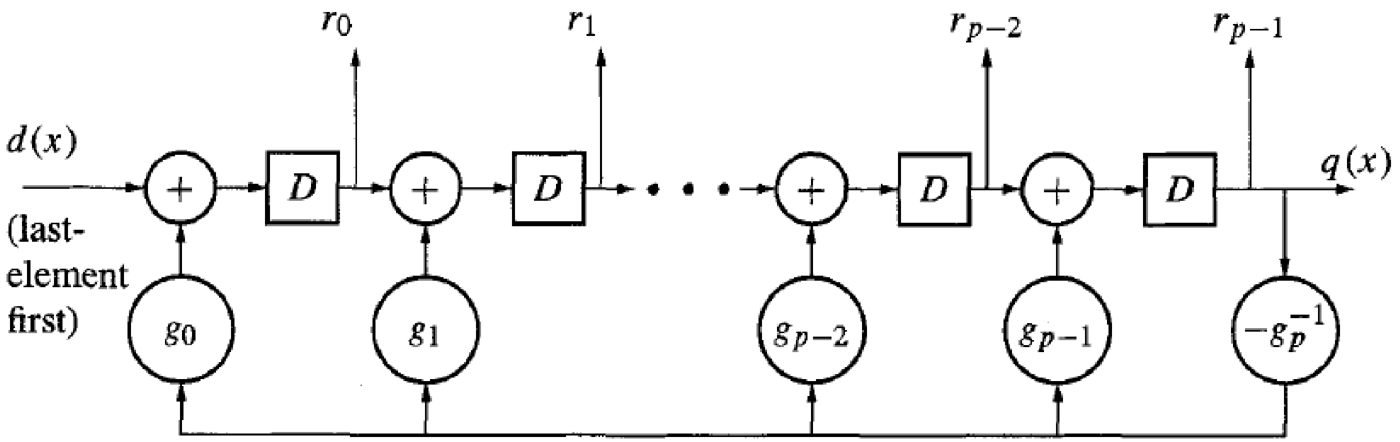
- Mạch nhân đa thức



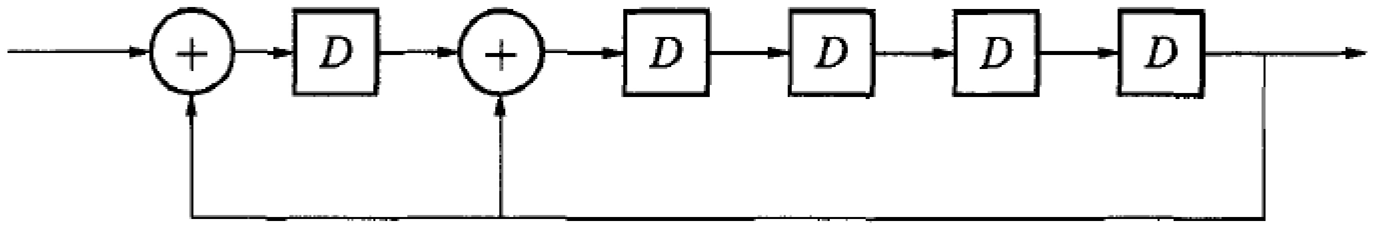


Phần 4: Thực hiện phần cứng mã hóa giải mã vòng CRC

- Mạch chia đa thức



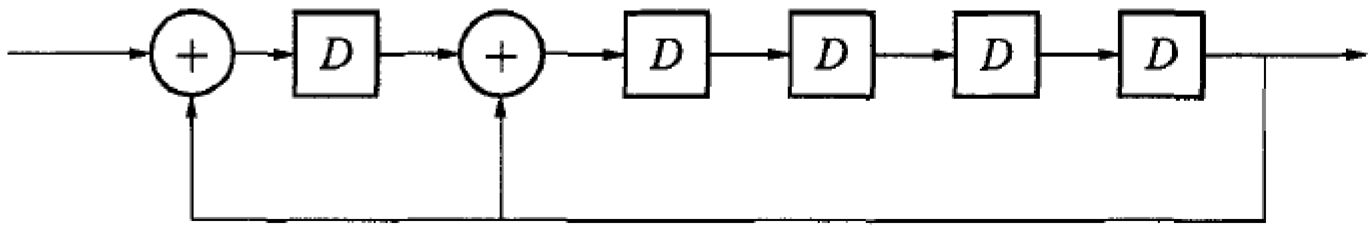
- Ví dụ: Mạch chia đa thức $g(x) = x^5 + x + 1$



Giá trị khởi tạo của các FF-D là ‘0’.

Phần 4: Thực hiện phần cứng mã hóa giải mã vòng CRC

- Ví dụ: Mạch chia đa thức $g(x) = x^5 + x + 1$



Bảng quan hệ đầu vào – đầu ra mạch chia $a(x) = x^8 + x^7 + x^5 + x + 1$

	Input Symbol on jth Shift		Shift Register Contents After j Shifts		Output Symbol on jth Shift	
j	bit	polynomial term	bits	polynomial representation	bit	polynomial term
0	–	–	0 0 0 0 0			
1	1	(x^8)	1 0 0 0 0			
2	1	(x^7)	1 1 0 0 0			
3	0	(x^6)	0 1 1 0 0			
4	1	(x^5)	1 0 1 1 0			
5	0	(x^4)	0 1 0 1 1	A: $x^5 + x^7 + x^8$	1	x^3
6	0	(x^3)	1 1 1 0 1	B: $x^3 + x^4 + x^5 + x^7$	1	x^2
7	0	(x^2)	1 0 1 1 0	C: $x^2 + x^4 + x^5$	0	x^1
8	1	(x^1)	1 1 0 1 1	$x + x^2 + x^4 + x^5$	1	x^0
9	1	1	0 0 1 0 1	D: $x^2 + x^4$		