

# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**MỘT SỐ ĐỊNH NGHĨA VÀ  
KHÁI NIỆM CƠ BẢN**

# NỘI DUNG

---

- ▶ **Các định nghĩa cơ bản:**
  - Mã hóa
  - Mã (bộ mã)
  - Các yếu tố của từ mã
- ▶ **Các khái niệm cơ bản**
  - Độ thừa của một bộ mã đều (D)
  - Khoảng cách mã
  - Trọng số của một từ mã
- ▶ **Khả năng không chế sai của một bộ mã đều nhị phân**
  - Khả năng phát hiện sai
  - Khả năng sửa sai



# Các định nghĩa cơ bản (1)

---

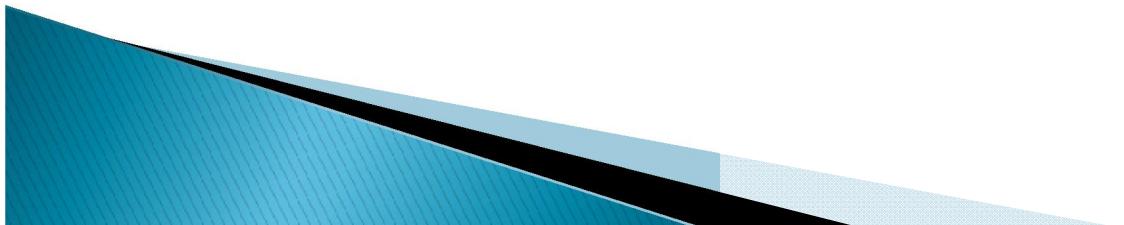
## ▶ Mã hóa

Mã hóa là một ánh xạ 1–1 từ tập các tin rời rạc  $a_i$  lên tập các từ mã  $\alpha_i^{n_i}$

$$f : a_i \rightarrow \alpha_i^{n_i}$$

## ▶ Mã (bộ mã)

Mã (hay bộ mã) là sản phẩm của phép mã hóa, hay nói cách khác mã là một tập các từ mã được lập nên theo một luật đã định trước



# Các định nghĩa cơ bản (2)

---

## ▶ Các yếu tố của từ mã:

- **Độ dài từ mã**  $n_i$  là số các dấu mã cần thiết dùng để mã hóa cho tin  $a_i$
- **Bộ mã đều**: là bộ mã mà các từ mã có độ dài như nhau.
- **Bộ mã không đều**: là bộ mã mà các từ mã có độ dài khác nhau.
- **Cơ số mã**: là số các giá trị khác nhau mà một dấu mã có thể nhận được.



# Các khái niệm cơ bản (1)

---

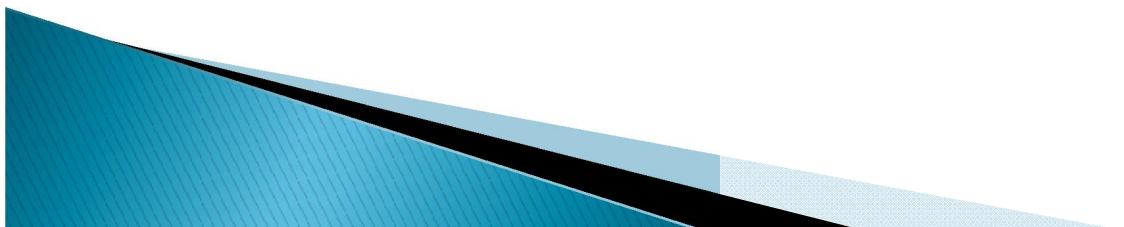
## ▶ Độ thừa của một bộ mã đều (D)

Xét phép mã hoá sau với cơ số mã là m:

$$f : A = \{a_i; i = \overline{1, s}\} \rightarrow V = \{\alpha_i^n\}$$

## ▶ Định nghĩa: Độ thừa của một bộ mã đều được xác định theo công thức sau:

$$D = \frac{\max H(V) - \max H(A)}{\max H(V)}$$



# Các khái niệm cơ bản (2)

- ▶ **Khoảng cách mã:** Khoảng cách giữa hai từ mã bất kỳ là số các dấu mã khác nhau tính theo cùng một từ mã giữa hai từ mã này ký hiệu

$$d(\alpha_i^n, \alpha_j^n)$$

- ▶ Ví dụ:  $\alpha_i^n = 0110101; \alpha_j^n = 1100100$

$$d(\alpha_i^n, \alpha_j^n) = 3$$

- ▶ **Khoảng cách Hamming**  $d_0$  của một bộ mã được xác định theo biểu thức sau:

$$d_0 = \min_{\forall \alpha_i^n, \alpha_j^n} d(\alpha_i^n, \alpha_j^n)$$

# Các khái niệm cơ bản (3)

---

▶ Trọng số của một từ mã:

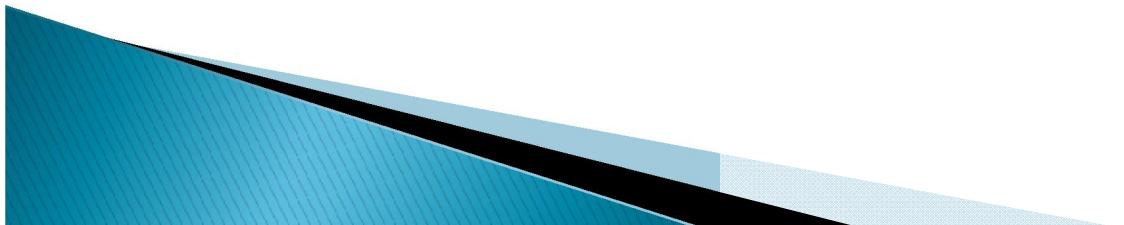
$w(\alpha_i^n)$  là số các dấu mã khác không trong từ mã.

▶ Tính chất:

$$\alpha_i^n = 0110101; \alpha_j^n = 1100100$$

$$\alpha_i^n + \alpha_j^n = 1010001$$

$$W(\alpha_i^n + \alpha_j^n) = 3 = d(\alpha_i^n, \alpha_j^n)$$



# Ví dụ

- ▶ Xét bộ mã khối tuyến tính nhị phân  $(n,k)=(6,3)$

$m_1 \ m_2 \ m_3 \rightarrow c_1 \ c_2 \ c_3 \ c_4 \ c_5 \ c_6$  với

000 - 000000

$$c_1 = m_1$$

001 - 001011

$$c_2 = m_2$$

010 - 010111

$$c_3 = m_3$$

011 - 011100

$$c_4 = m_1 + m_2$$

100 - 100101

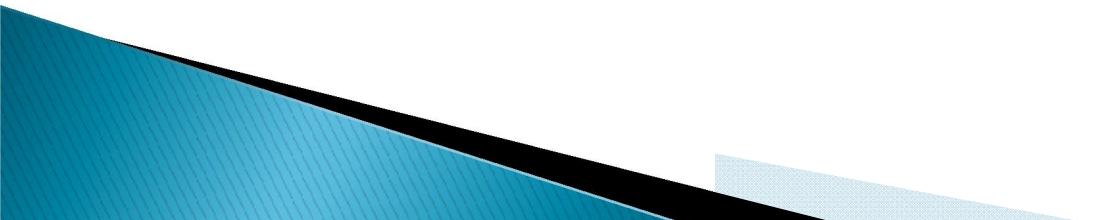
$$c_5 = m_2 + m_3$$

101 - 101110

$$c_6 = m_1 + m_2 + m_3$$

110 - 110010

111 - 111001



# Khả năng khống chế sai của một bộ mã đều nhị phân

---

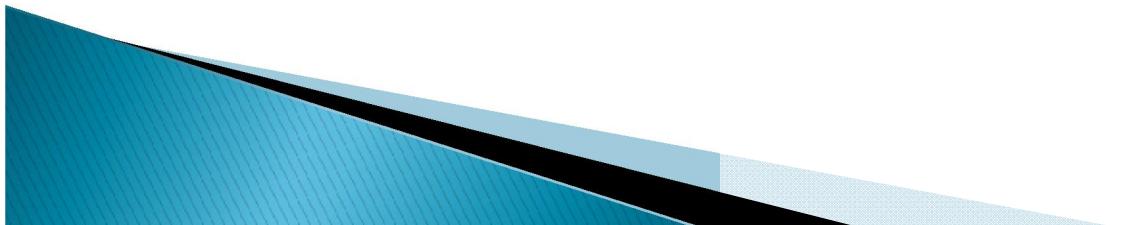
## ▶ **Khả năng phát hiện sai:**

Một bộ mã đều nhị phân có độ thừa ( $D > 0$ ) và có  $d_0 \geq 2$  sẽ có khả năng **phát hiện** được t sai với điều kiện:  $t \leq d_0 - 1$

## ▶ **Khả năng sửa sai:**

Một bộ mã đều nhị phân có độ thừa ( $D > 0$ ) và có  $d_0 \geq 3$  sẽ có khả năng **sửa** được t sai với điều kiện:  $t \leq [(d_0 - 1)/2]$

Ở đây  $[x]$  là phần nguyên của x.



# CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA

## MÃ THỐNG KÊ TỐI ƯU

# MÃ THỐNG KÊ TỐI ƯU

---

- ▶ Độ dài trung bình của từ mã và mã hoá tối ưu
- ▶ Yêu cầu của một phép mã hoá tối ưu
- ▶ Định lý mã hoá thứ nhất của Shannon (đối với mã nhị phân)
- ▶ Nguyên tắc lập mã tiết kiệm
- ▶ Thuật toán Huffman



# Độ dài trung bình của từ mã

- ▶ Xét phép mã hoá sau đối với các tin của nguồn rác A:

$$f : A = \left\{ a_i, p(a_i); i = \overline{1, s} \right\} \rightarrow V = \left\{ \alpha_i^n, p(a_i) \right\}$$

- ▶ **Định nghĩa:** Độ dài trung bình của một từ mã trong bộ mã được xác định như sau:

$$\bar{n} = M[n_i] = \sum_{i=1}^s n_i p(a_i)$$

- ▶ **Định nghĩa:** Một phép mã hoá được gọi là tiết kiệm (hay tối ưu) nếu nó làm cực tiểu giá trị  $\bar{n}$



# Yêu cầu của phép mã hoá tối ưu

---

- ▶  $\bar{n} \rightarrow \min$
- ▶ Có khả năng giải mã tức thì: không một dãy bit nào trong biểu diễn của một tin (ký tự) nào đó lại là phần đầu (prefix) của một dãy bit dài hơn biểu diễn cho một tin (ký tự) khác.



# Định lý mã hoá thứ nhất của Shannon

---

## ► Định lý mã hoá thứ nhất của Shannon:

Luôn luôn có thể xây dựng được một phép mã hoá các tin rác có hiệu quả mà  $\bar{n}$  có thể nhỏ tuỳ ý nhưng không được nhỏ hơn entropy của nguồn A được xác định bởi đặc tính thống kê của nguồn A:  $\bar{n} \geq H(A)$



# Nguyên tắc lập mã tiết kiệm

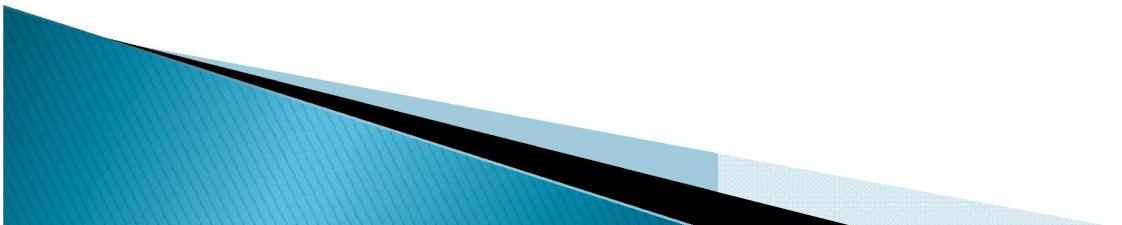
- ▶ Theo định lý ta có:

$$\sum_{i=1}^s p(a_i)n_i \geq -\sum_{i=1}^s p(a_i)\log p(a_i)$$

- ▶ Bất đẳng thức trên sẽ thỏa mãn nếu  $\forall i$  ta có:

$$n_i \geq -\log p(a_i) = \log \frac{1}{p(a_i)}$$

- ▶ **Nguyên tắc:** Các từ mã có độ dài càng nhỏ sẽ được dùng để mã hoá cho các tin có xác suất xuất hiện càng lớn và ngược lại.

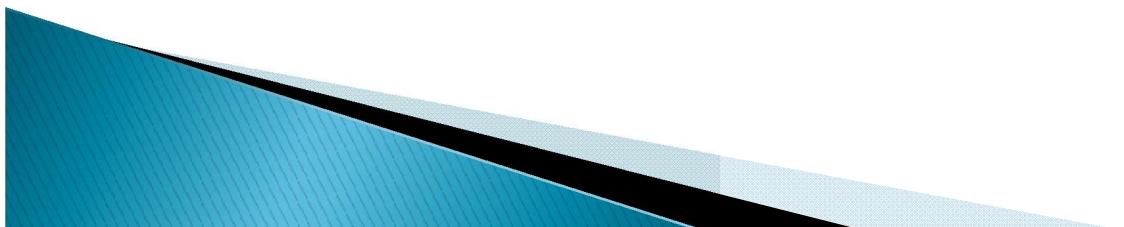


# Thuật toán Huffman

---

- ▶ Thuật toán mã hoá Huffman
  - ▶ Hiệu suất mã hoá
  - ▶ Giải mã Huffman
- 
- ▶ **Ví dụ:** Cho nguồn rời rạc  $A = (a_1, a_2, a_3, a_4, a_5)$  với xác suất lần lượt là: 0,1; 0,1; 0,45; 0,2; 0,15.

Thực hiện mã hóa Huffman cho nguồn A và tính chiều dài trung bình của từ mã.



# Bài tập

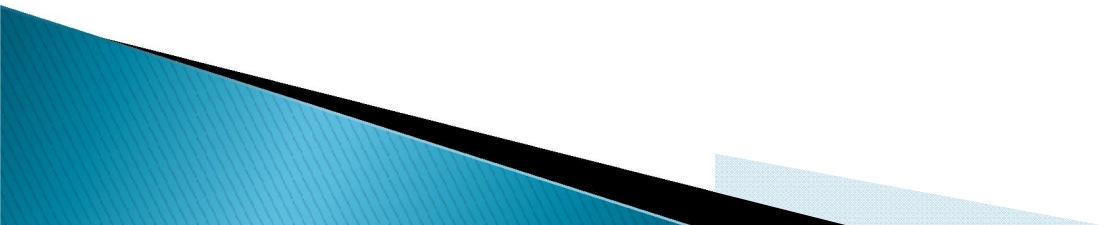
---

1. Cho nguồn rời rạc  $A = (a_1, a_2, a_3, a_4, a_5, a_6)$  với xác suất lần lượt là: 0,05; 0,05; 0,5; 0,2; 0,1; 0,1. Thực hiện mã hóa Huffman cho nguồn A và tính chiều dài trung bình của từ mã.
2. Yêu cầu tương tự bài 1 với

$A = (a_1, a_2, a_3, a_4, a_5, a_6)$  có xác suất lần lượt là:  
(0,12; 0,08; 0,3; 0,15; 0,3; 0,05)

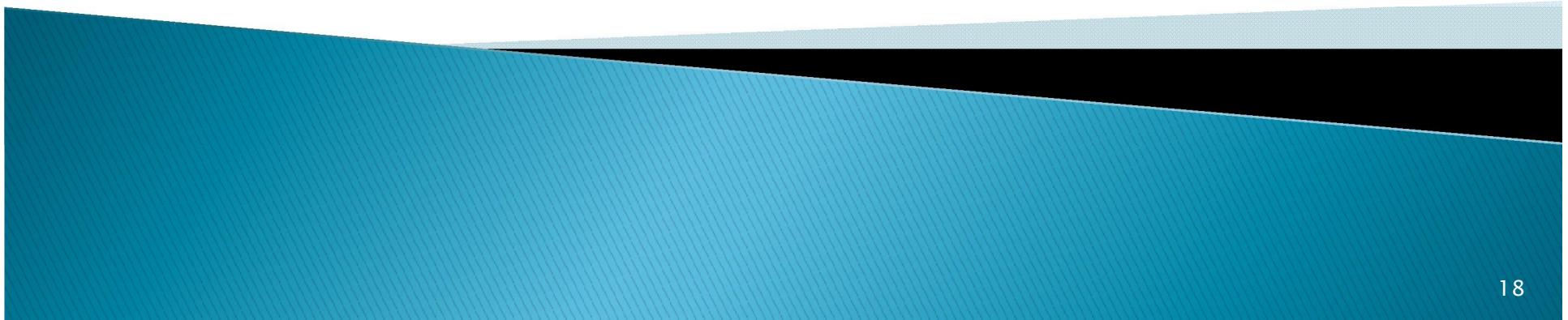
3. Yêu cầu tương tự bài 1 với

$A = (a_1, a_2, a_3, a_4, a_5, a_6, a_7)$  có xác suất lần lượt là:  $(1/32; 1/16; 1/8; 1/32; 1/4; 1/4; 1/4)$ . Giải mã cho chuỗi dữ liệu nhận được 000111001011...



# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

## **MÃ KHỐI TUYỀN TÍNH**



# Nội dung

---

- ▶ Dạng tuyến tính và mã tuyến tính
- ▶ Yêu cầu đối với mã khối tuyến tính
- ▶ Các bài toán tối ưu đối với mã tuyến tính nhị phân
- ▶ Ma trận sinh và ma trận kiểm tra của mã tuyến tính



# Dạng tuyến tính và mã tuyến tính

---

## ▶ Dạng tuyến tính:

Các dạng tuyến tính của k biến độc lập  $x_1, x_2, \dots, x_k$  là các biểu thức có dạng:

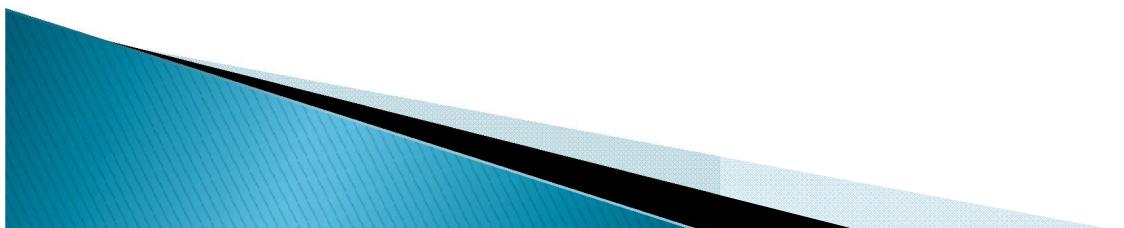
$$f(x_1, x_2, \dots, x_k) = \sum_{i=1}^k a_i x_i \text{ với } a_i \in GF(2)$$

## ▶ Mã tuyến tính:

Mã tuyến tính độ dài n là mã mà các từ mã của nó có các dấu mã là dạng tuyến tính.

## ▶ Mã hệ thống tuyến tính (n,k):

là mã tuyến tính độ dài n trong đó ta có thể chỉ ra được vị trí của k dấu thông tin trong từ mã.



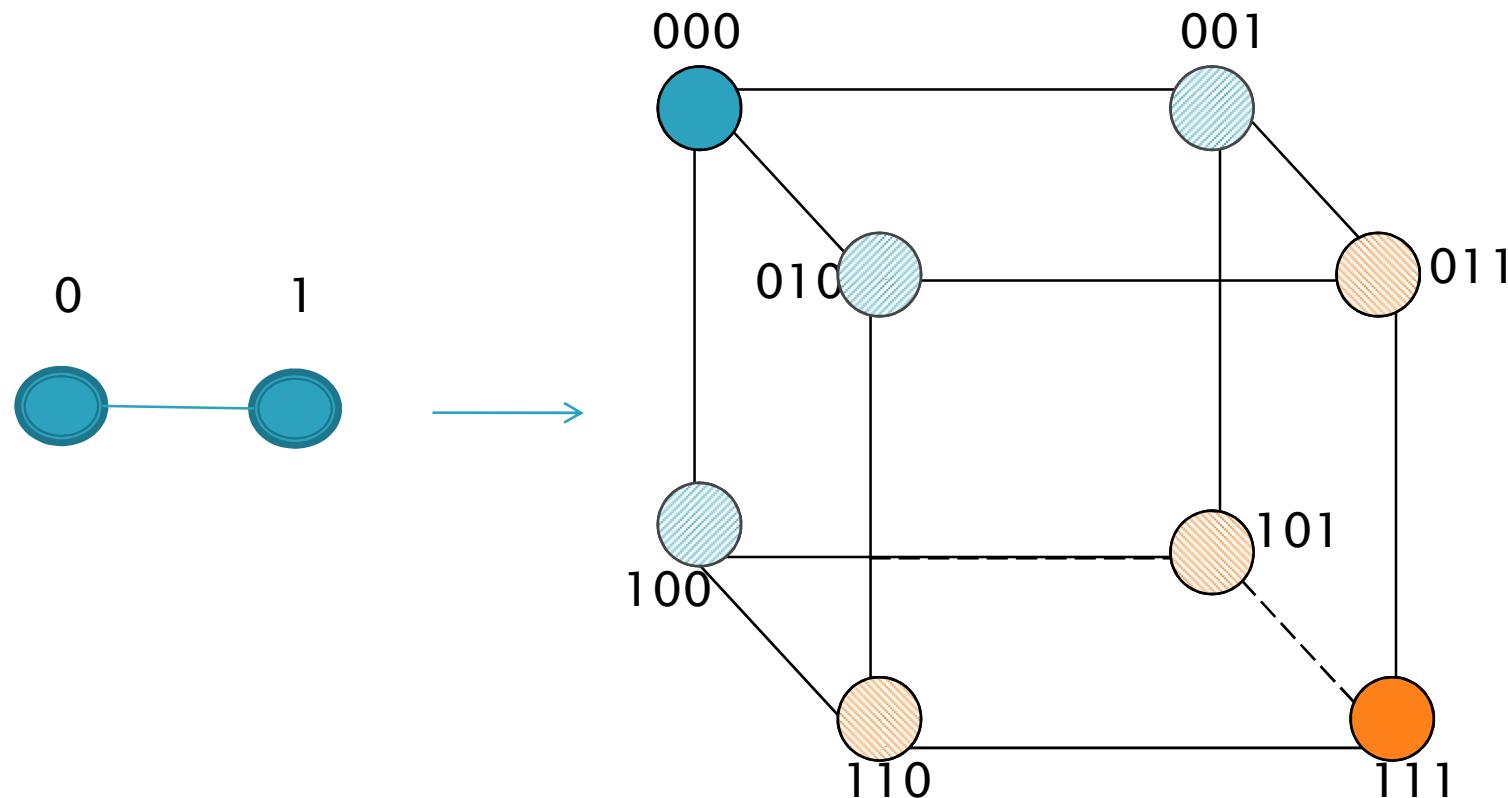
## Yêu cầu đối với mã khối tuyến tính (để kiểm soát lỗi)

- ▶ Xét bộ mã khối tuyến tính  $(n, k, d_0)$ . Người ta luôn mong muốn mã có độ thừa nhỏ nhưng lại có khả năng khống chế sai lớn hay nói cách khác có 2 yêu cầu đối với bộ mã này:
  - Có khả năng phát hiện và sửa nhiều sai hay  $d_0$  lớn.
  - Độ thừa nhỏ hay tỉ lệ mã  $r=k/n$  lớn



# Ví dụ

---



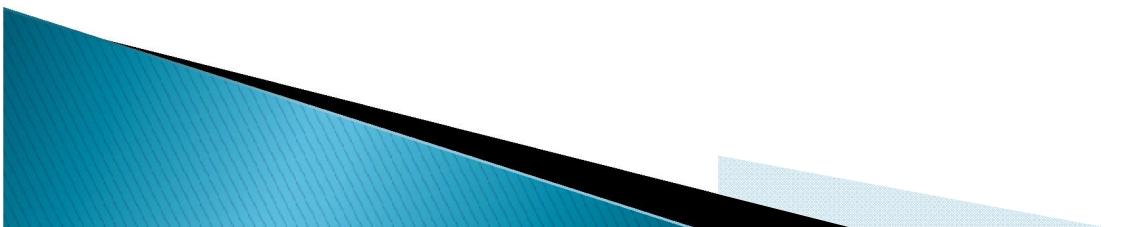
# Các bài toán tối ưu của mã tuyến tính nhị phân (1)

- ▶ **Bài toán 1:** Với  $k$  và  $d_0$  xác định ta phải tìm được mã có độ dài từ mã  $n$  là nhỏ nhất.
- ▶ **Giới hạn Griesmer:**

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d_0}{2^i} \right\rceil$$

- ▶ **Ví dụ:**  $k=4$ ,  $d_0= 3$  khi đó:

$$n \geq \left\lceil \frac{3}{1} \right\rceil + \left\lceil \frac{3}{2} \right\rceil + \left\lceil \frac{3}{4} \right\rceil + \left\lceil \frac{3}{8} \right\rceil = 3 + 2 + 1 + 1 = 7$$



# Các bài toán tối ưu của mã tuyến tính nhị phân (2)

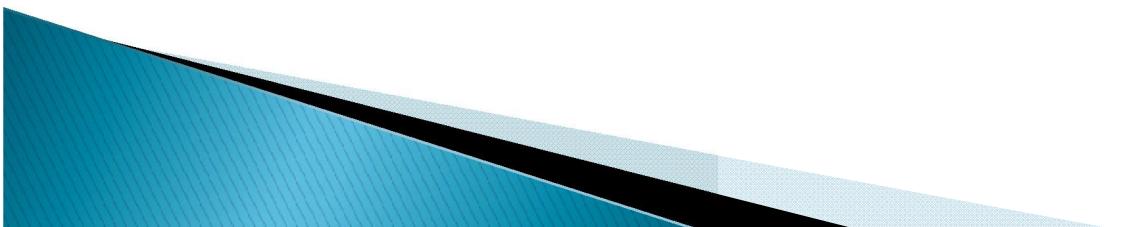
---

- ▶ **Bài toán 2:** Với  $n$  và  $k$  xác định, ta phải tìm được mã có khoảng cách tối thiểu  $d_0$  là lớn nhất.
- ▶ **Giới hạn Plotkin:**

$$d_0 \leq \frac{n \cdot 2^{k-1}}{2^k - 1}$$

- ▶ **Ví dụ:** Cho  $k = 3$ ,  $n = 7$  ta có:

$$d_0 \leq \frac{7 \cdot 2^2}{2^3 - 1} = 4$$



# Các bài toán tối ưu của mã tuyến tính nhị phân (3)

- ▶ **Bài toán 3:** Với  $n$  và số sai có thể sửa  $t$  xác định, ta phải tìm được mã có số dấu thông tin  $k$  là lớn nhất (hay số dấu thừa  $r = n-k$  là nhỏ nhất).
- ▶ **Giới hạn Hamming:**

$$2^r \geq \sum_{i=0}^t C_n^i$$

- ▶ **Ví dụ:**

Cho  $n = 7$  và  $t = 1$  ta có:

$$2^r \geq \sum_{i=0}^1 C_7^i = C_7^0 + C_7^1 = 8 \Rightarrow r \geq 3$$

# Ma trận sinh và ma trận kiểm tra đối với mã khối tuyến tính

► Xét bộ mã khối tuyến tính nhị phân  $(n,k)=(6,3)$

$m_1 \ m_2 \ m_3 \rightarrow c_1 \ c_2 \ c_3 \ c_4 \ c_5 \ c_6$  với

000 - 000000

001 - 001011

$$c_1 = m_1$$

010 - 010111

$$c_2 = m_2$$

011 - 011100

$$c_3 = m_3$$

100 - 100101

$$c_4 = m_1 + m_2$$

101 - 101110

$$c_5 = m_2 + m_3$$

110 - 110010

$$c_6 = m_1 + m_2 + m_3$$

111 - 111001

$$c_{1 \times n} = m_{1 \times k} \cdot G_{k \times n}$$

# Ma trận sinh G

$$(m_1 \ m_2 \ m_3) \begin{pmatrix} g_{11} & g_{12} & g_{13} & g_{14} & g_{15} & g_{16} \\ g_{21} & g_{22} & g_{23} & g_{24} & g_{25} & g_{26} \\ g_{31} & g_{32} & g_{33} & g_{34} & g_{35} & g_{36} \end{pmatrix} = (c_1 \ c_2 \ c_3 \ c_4 \ c_5 \ c_6)$$

$$c_1 = m_1 g_{11} + m_2 g_{21} + m_3 g_{31} = m_1$$

$$c_2 = m_1 g_{12} + m_2 g_{22} + m_3 g_{32} = m_2$$

$$c_3 = m_1 g_{13} + m_2 g_{23} + m_3 g_{33} = m_3$$

$$c_4 = m_1 g_{14} + m_2 g_{24} + m_3 g_{34} = m_1 + m_2$$

.....

$$g_{11} = 1; g_{21} = 0; g_{31} = 0$$

$$g_{12} = 0; g_{22} = 1; g_{32} = 0$$

$$g_{13} = 0; g_{23} = 0; g_{33} = 1$$

$$g_{14} = 1; g_{24} = 1; g_{34} = 0$$

.....



# Ma trận sinh G

---

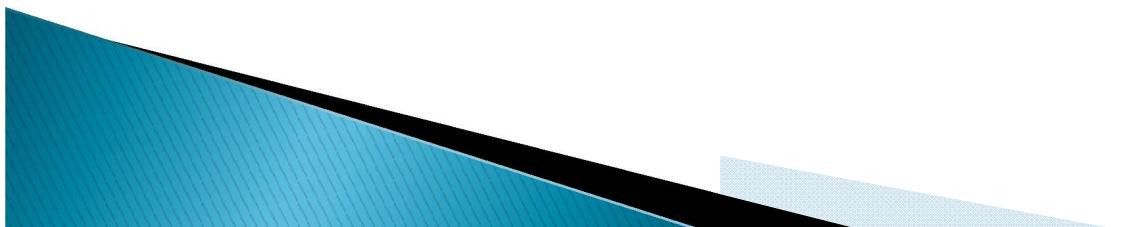
$$G_{3 \times 6} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

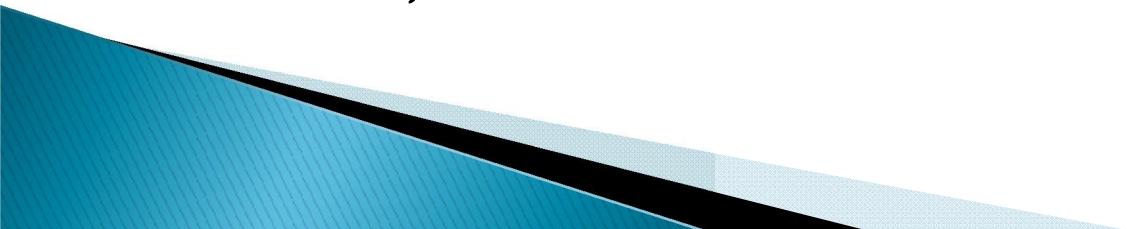
# Ma trận kiểm tra H

- ▶ Với mọi ma trận G có  $\det(G) \neq 0$ , ta luôn tìm được ma trận H thỏa mãn:

$$G \cdot H^T = 0$$

- ▶ Nếu  $G = [P | I_k]$  thì  $H = [I_{n-k} | P^T]$   
(kích thước của H là  $(n-k) \times n$ )



- 
- ▶ Cho mă (7,4):
  - ▶  $m_1 m_2 m_3 m_4 \rightarrow c_1 c_2 c_3 c_4 c_5 c_6 c_7$
  - ▶  $C_1 = m_1$
  - ▶  $C_2 = m_2$
  - ▶  $C_3 = m_3$
  - ▶  $C_4 = m_4$
  - ▶  $C_5 = m_1 + m_2 + m_3$
  - ▶  $C_6 = m_2 + m_3 + m_4$
  - ▶  $C_7 = m_1 + m_2 + m_3 + m_4$
  - ▶ Tim G, H
- 

# Bài tập

---

1. Cho mã (7,3):

$$m_1 m_2 m_3 \rightarrow c_1 c_2 c_3 c_4 c_5 c_6 c_7$$

$$C_1 = m_1; C_2 = m_2; C_3 = m_3; C_4 = m_3 + m_1;$$

$$C_5 = m_1 + m_2 + m_3; C_6 = m_2 + m_3;$$

$$C_7 = m_1 + m_2$$

Tìm ma trận sinh G và ma trận kiểm tra H

2. Cho mã (6,4):

$$m_1 m_2 m_3 m_4 \rightarrow c_1 c_2 c_3 c_4 c_5 c_6$$

$$C_1 = m_1; C_2 = m_2; C_3 = m_3; C_4 = m_4;$$

$$C_5 = m_1 + m_2 + m_3; C_6 = m_2 + m_3 + m_4;$$

Tìm ma trận sinh G và ma trận kiểm tra H



# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

## **VÀNH ĐA THỨC VÀ MÃ CYCLIC**

# Nội dung

---

- ▶ Vành đa thức
  - Phép cộng đa thức
  - Phép nhân đa thức
  - Phép dịch vòng
  - Định nghĩa vành đa thức
- ▶ Ideal của vành đa thức
- ▶ Định nghĩa mã cyclic
- ▶ Ma trận sinh của mã cyclic
- ▶ Ma trận kiểm tra của mã cyclic



# Vành đa thức – Phép cộng đa thức

---

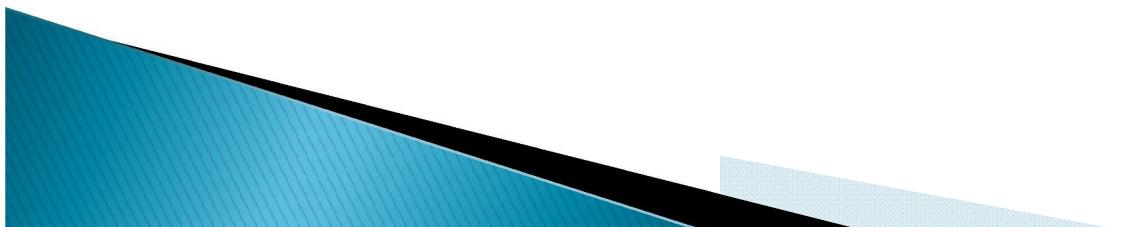
- ▶ Xét tập các đa thức có dạng sau:

$$f(x) = \sum_{i=0}^{n-1} f_i x^i \quad (*) \quad \deg f(x) \leq n - 1; f_i \in GF(2)$$

- ▶ Xét 2 đa thức có dạng giống f(x):

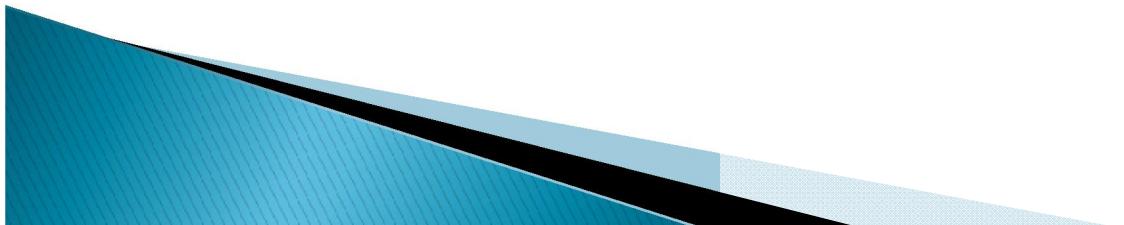
$$a(x) = \sum_{i=0}^{n-1} a_i x^i \text{ và } b(x) = \sum_{i=0}^{n-1} b_i x^i$$

$$a(x) + b(x) = \sum_{i=0}^{n-1} (a_i + b_i) x^i = \sum_{i=0}^{n-1} c_i x^i$$



# Vành đa thức – Phép nhân đa thức

- ▶ Để tích  $a(x)b(x)$  vẫn là đa thức có bậc  $\leq n-1$  thì ta phải thực hiện nhân 2 đa thức theo modul  $x^n + 1$  (hay  $x^n = 1$ )
- ▶  $a(x) \cdot b(x) = (\sum_{i=0}^{n-1} a_i x^i) (\sum_{i=0}^{n-1} b_i x^i) \text{mod}(x^n + 1)$
- ▶ Ví dụ:  $a(x) = 1 + x + x^4$  và  $b(x) = x + x^5$   
 $a(x) + b(x) = 1 + x^4 + x^5$   
 $a(x) \cdot b(x) = (x + x^2 + x^5 + x^5 + x^6 + x^9) \text{mod}(x^7 + 1)$   
 $= x + x^6$



# Vành đa thức – Phép dịch vòng

- ▶ Xét trường hợp đặc biệt của phép nhân:
- ▶  $a(x) = \sum_{i=0}^{n-1} a_i x^i \leftrightarrow a = (a_0, a_1, \dots, a_{n-1})$
- ▶  $b(x) = x.a(x) = x(\sum_{i=0}^{n-1} a_i x^i)$   
 $\leftrightarrow b = (a_{n-1}, a_0, a_1, \dots, a_{n-2})$
- ▶  $c(x) = \frac{a(x)}{x} = \frac{\sum_{i=0}^{n-1} a_i x^i}{x} \leftrightarrow c = (a_1, \dots, a_{n-1}, a_0)$
- ▶ Nhận xét:
  - **vector b** là dịch vòng về **phía phải** một cấp so với vector a.
  - **vector c** là dịch vòng về **phía trái** một cấp so với vector a



## Vành đa thức – Định nghĩa vành đa thức

---

- ▶ Tập các đa thức xác định theo (\*) với hai phép toán cộng đa thức và nhân đa thức theo modul  $x^n + 1$  tạo nên vành đa thức. Trong trường hợp các hệ số của đa thức nằm trong GF(2) ta ký hiệu vành này là  $Z_2[x]/x^n + 1$ .



# Ideal của vành đa thức

- Ideal  $I$  của vành đa thức  $\mathbb{Z}_2[x]/x^n + 1$  gồm tập các đa thức  $a(x)$  là bội của đa thức  $g(x)$  với  $g(x)$  thỏa mãn:

- 1.  $g(x) | x^n + 1$

- 2.  $\deg g(x) = r = n - k = \min \deg a(x)$

với  $\forall a(x) \in I; a(x) \neq 0$

- Ký hiệu Ideal trong vành đa thức  $I = \langle g(x) \rangle$

- Với  $g(x) = \sum_{i=0}^r g_i x^i$  ta có  $g_0 = g_r = 1$

# Định nghĩa mã cyclic

---

- ▶ Mã cyclic  $(n,k)$  là ideal  $I = \langle g(x) \rangle$  của  
vành đa thức  $\mathbb{Z}_2[x]/x^n + 1$ .
- ▶ Vì Ideal  $I$  chứa tất cả các bội số của  $g(x)$  nên nếu  $a(x) \in I$  thì  $a(x) : g(x)$  và  
hiển nhiên  $x.a(x) : g(x)$



# Mã cyclic trên vành đa thức

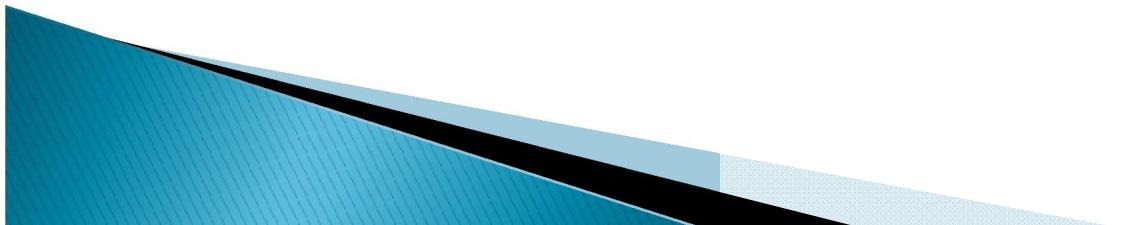
- ▶ **Định nghĩa:** Mã cyclic là một bộ mã tuyến tính có tính chất sau: Nếu  $a(x)$  là một từ mã thì dịch vòng của  $a(x)$  cũng là một từ mã thuộc bộ mã này.
- ▶ **Ví dụ:** Tìm tất cả các mã cyclic trên vành  $Z_2[x]/x^7 + 1$
- ▶ **Giải:**  $x^7 + 1 = (1+x)(1+x+x^3)(1+x^2+x^3)$ 
  - Mỗi mã cyclic là một ideal, vì vậy ta tìm các ideal trên vành này.
  - Mỗi ideal được tạo ra từ đa thức sinh  $g(x)$ .
  - Vậy có thể xây dựng được 7 ideal trên vành này

# Phân tích $x^n + 1$ thành tích các đa thức bất khả quy

---

- ▶ **Định nghĩa:** Đa thức  $a(x)$  được gọi là bất khả quy nếu nó chỉ chia hết cho 1 và cho chính nó.
- ▶ **Định lý:** Với  $n = 2^m - 1$ , đa thức  $x^n + 1$  được phân tích thành tích của tất cả các đa thức bất khả quy có bậc m và ước của m.
- ▶ **Định nghĩa:** Đa thức  $g^*(x)$  được gọi là đa thức đối ngẫu của đa thức  $g(x)$  nếu:

$$g^*(x) = x^{\deg g(x)}.g(x^{-1})$$



# Các mã cyclic trên vành $Z_2[x]/x^7 + 1$

STT	$g(x)$	Mã (n,k)	$d_0$
1	1	(7,7)	1
2	$1+x$	(7,6)	2
3	$1+x+x^3$	(7,4)	3
4	$1+x^2+x^3$	(7,4)	3
5	$(1+x)(1+x+x^3)$	(7,3)	4
6	$(1+x)(1+x^2+x^3)$	(7,3)	4
7	$(1+x^2+x^3) (1+x+x^3)$	(7,1)	7

# Ma trận sinh của mã cyclic

- ▶ Đối với mã khối tuyến tính  $c=m \cdot G$  (1)
- ▶ Đối với mã cyclic:  $c(x)=m(x)g(x)$  (2)
- ▶ Bản tin  $m$  gồm  $k$  bit, do đó  $\deg m(x) \leq k-1$ ;

Từ (2) ta có:

$$\begin{aligned} c(x) &= g(x)(m_0 + m_1x + \dots + m_{k-1}x^{k-1}) \\ &= g(x)m_0 + g(x)m_1x + \dots + g(x)m_{k-1}x^{k-1} \end{aligned}$$

$$c(x) = (m_0 \ m_1 \dots m_{k-1}) \begin{pmatrix} g(x) \\ xg(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix} = mG$$

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix}$$

# Ma trận kiểm tra của mã cyclic

► Đa thức kiểm tra:  $h(x) = \frac{x^n + 1}{g(x)} = \sum_{j=0}^k h_j x^j$

Với  $h_0 = h_k = 1, h_j \in \{0,1\}$

Ma trận kiểm tra:

$$H = \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \dots \\ x^{r-1}h^*(x) \end{pmatrix}$$

$$h^*(x) = x^{\deg h(x)}.h(x^{-1})$$

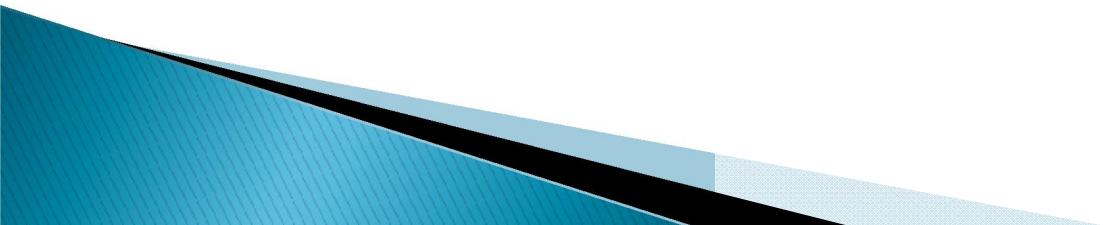
Ví dụ: Tìm ma trận sinh và ma trận kiểm tra cho mã cyclic (7,3) có  $g(x) = 1 + x^2 + x^3 + x^4$

# Bài tập

1. (2.26) Cho  $g(x)=x^8 + x^6 + x^4 + x^2 + 1$  là đa thức trên trường nhị phân.

- a. Tìm mã cyclic có tỷ lệ mã  $r=k/n$  nhỏ nhất với đa thức sinh là  $g(x)$
- b. Tìm khoảng cách Hamming của bộ mã ở câu a.

2. Tìm ma trận sinh và ma trận kiểm tra cho mã cyclic  $(7,4)$  có  $g(x)=1+x^2+x^3$



# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**MÃ HÓA CHO MÃ CYCLIC BẰNG  
PHƯƠNG PHÁP CHIA**

# Nội dung

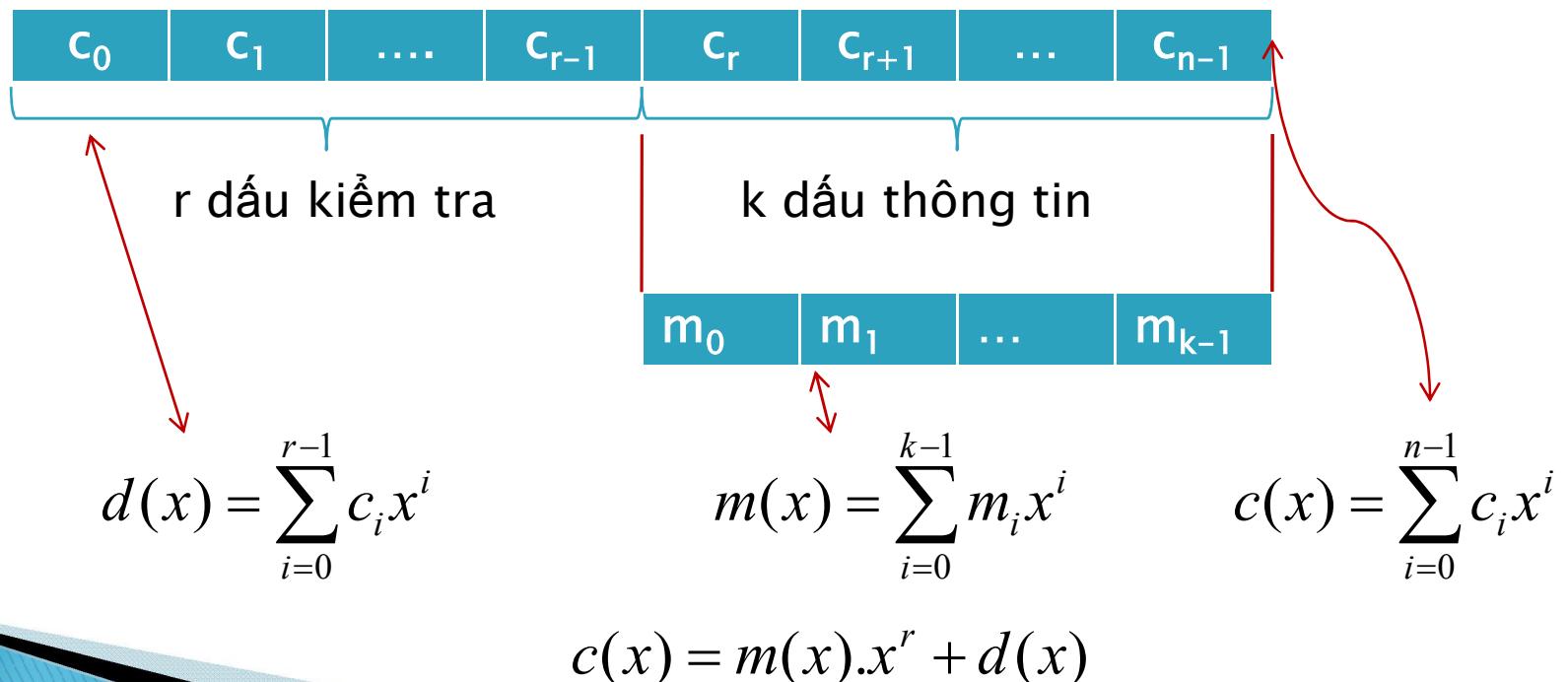
---

- ▶ Mô tả từ mã của mã cyclic hệ thống
- ▶ Thuật toán mã hóa hệ thống
- ▶ Thiết bị mã hóa



# Tùy mã cyclic hệ thống

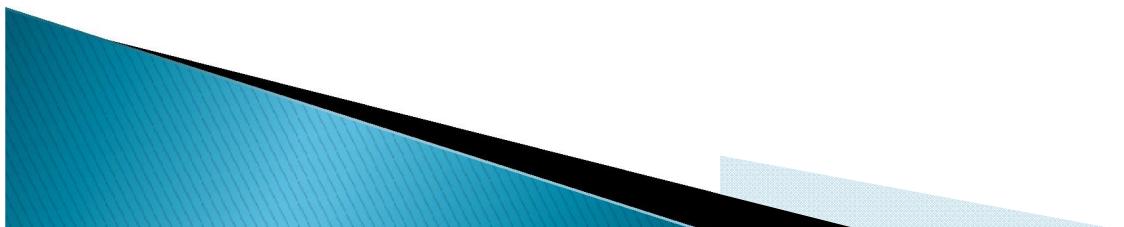
- Định nghĩa: Mã cyclic ( $n, k$ ) được gọi là một tùy mã cyclic hệ thống nếu ta có thể chỉ rõ vị trí của các dấu thông tin và các dấu kiểm tra trong tùy mã.



- 
- ▶ Ta có:  $\deg m(x) \leq k-1$ ;  $\deg g(x) = r$ ;  $\deg d(x) \leq r-1$

$$\frac{c(x)}{g(x)} = \frac{m(x).x^r + d(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)} + \frac{d(x)}{g(x)}$$

- ▶ Do  $c(x) : g(x)$  nêu  $(r(x) + d(x)) : g(x)$   
 $\Rightarrow r(x) + d(x) = 0 \Rightarrow r(x) = d(x)$



# Thuật toán mã hóa hệ thống

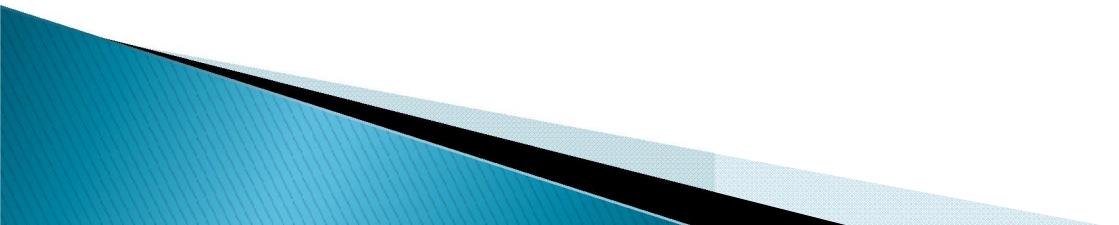
---

- ▶ Bước 1: Mô tả tin  $m_i$  bằng đa thức  $m(x)$ .
- ▶ Bước 2: Nâng bậc  $m(x)$  hay  $x^{n-k} \cdot m(x)$
- ▶ Bước 3: Chia  $x^{n-k} \cdot m(x)$  cho đa thức sinh  $g(x)$  để tìm phần dư  $r(x)$
- ▶ Bước 4: Xây dựng từ mã  $c(x) = m(x) \cdot x^{n-k} + r(x)$

## ▶ Ví dụ:

Cho mã cyclic (7,3) có  $g(x) = 1 + x^2 + x^3 + x^4$

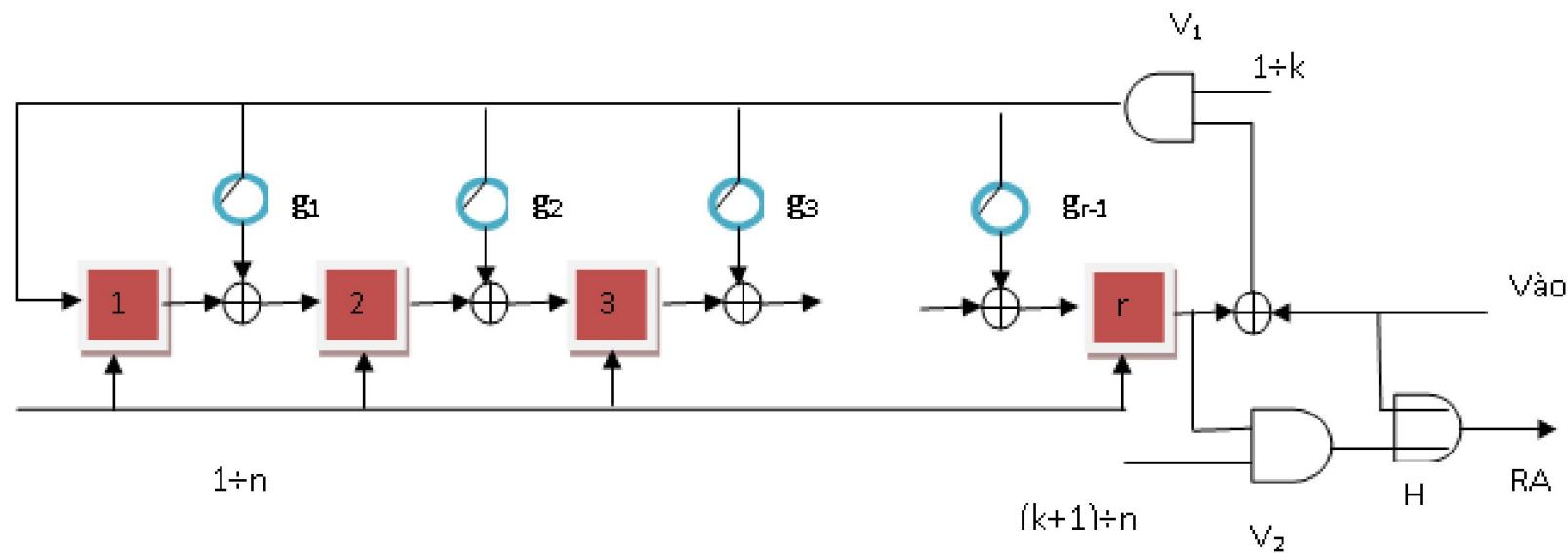
Tìm từ mã đầu ra theo thuật toán 4 bước biết  
bản tin đầu vào  $m=110$



# Hoạt động của thiết bị mã hóa

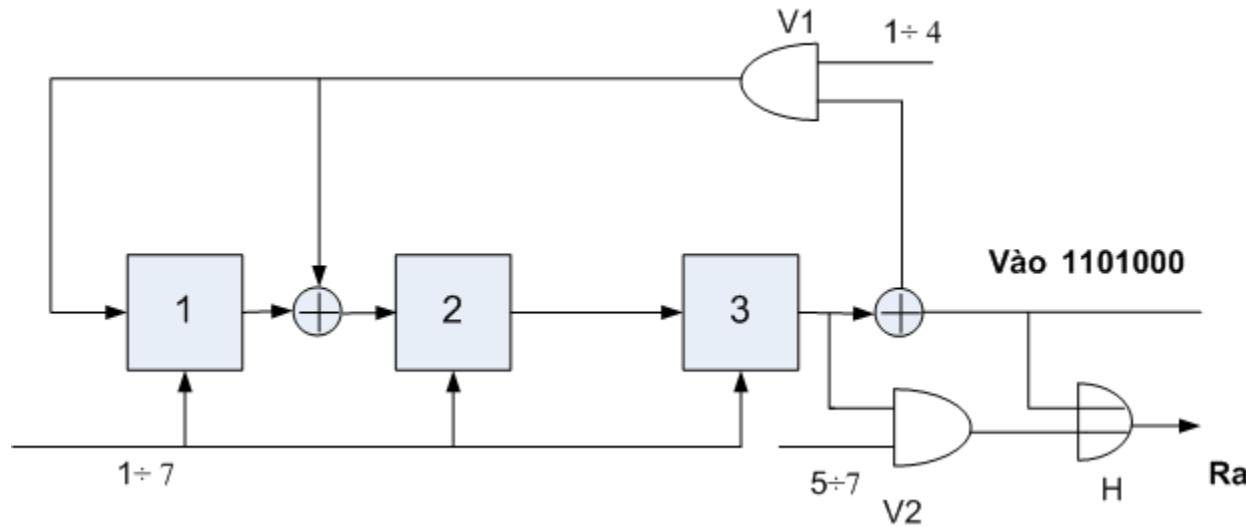
- ▶ **k nhịp đầu:** chia và tính phần dư. Mạch AND V1 mở, V2 đóng, thiết bị hoạt động như một bộ chia để **tính dư**. Kết thúc nhịp thứ k, toàn bộ phần dư nằm trong r ô nhớ. Trong quá trình này, các dấu thông tin  $m(x) \cdot x^{n-k}$  được đưa qua mạch OR H.
- ▶ **r nhịp sau:** đưa ra các dấu kiểm tra (phần dư) tới đầu ra. Mạch AND V1 đóng, thiết bị hoạt động như một thanh ghi dịch nối tiếp. Mạch AND V2 mở, các dấu kiểm tra được lần lượt đưa ra từ bậc cao tới bậc thấp. Kết thúc nhịp thứ n, toàn bộ từ mã được đưa ra đầu ra.

# Sơ đồ thiết bị mã hóa

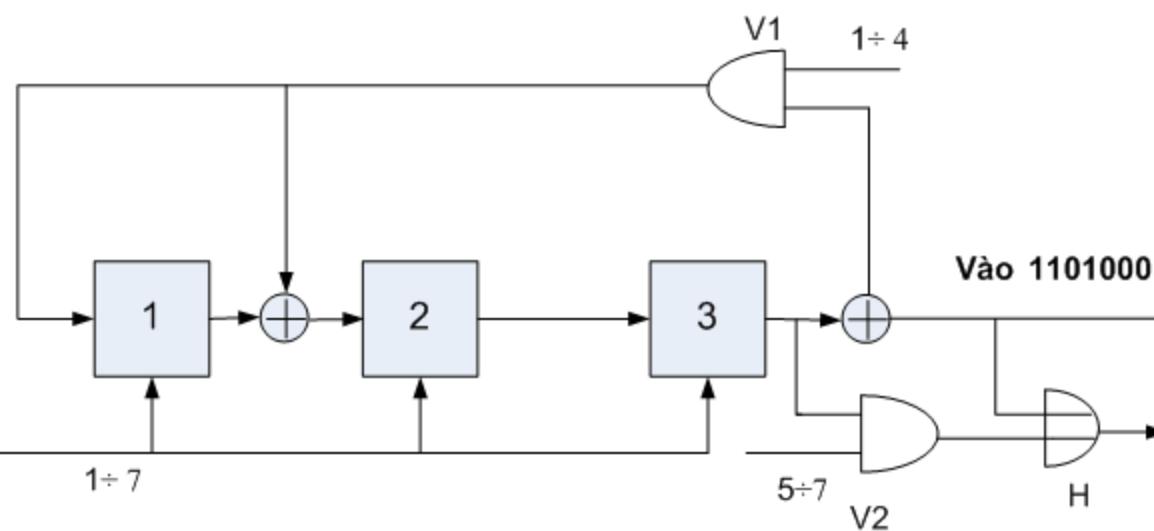


# Ví dụ

- ▶ Cho mã cyclic (7,4) có  $g(x)=1+x+x^3$ 
  - Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia.
  - Tìm từ mã đầu ra tương ứng với đầu vào  $m=1011$
  - Kiểm tra lại kết quả bằng thuật toán mã hóa.



Xung nhịp	Vào	Trạng thái ô nhớ			Ra
		1	2	3	
1	1	1	1	0	1
2	1	1	0	1	1
3	0	1	0	0	0
4	1	1	0	0	1
5			1	0	0
6				1	0
7					1



# Bài tập

1. Cho mã cyclic (7,4) có  $g(x)=1+x^2+x^3$

- Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia (nhân).
- Tìm từ mã đầu ra tương ứng với đầu vào  $m=1011$
- Kiểm tra lại kết quả bằng thuật toán mã hóa.

2. Cho mã cyclic (7,3) có  $g(x)=1+x+x^2+x^4$

- Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia (nhân).
- Tìm từ mã đầu ra tương ứng với đầu vào  $m=011$
- Kiểm tra lại kết quả bằng thuật toán mã hóa.

3. Cho mã cyclic (7,3) có  $g(x)=1+x^2+x^3+x^4$

- Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia (nhân).
- Tìm từ mã đầu ra tương ứng với đầu vào  $m=110$
- Kiểm tra lại kết quả bằng thuật toán mã hóa.

---

Cho mã cyclic (9,3) có  $g(x)=1+x^3+x^6$

- Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia.
  - Tìm từ mã đầu ra tương ứng với đầu vào  $m= 101$
  - Kiểm tra lại kết quả bằng thuật toán mã hóa.
- ▶ Bàn 1:  $m=101 \quad (4)$
  - ▶ Bàn 2:  $m=110 \quad (5)$
  - ▶ Bàn 3:  $m =011 \quad (6)$
  - ▶ Bàn 4:  $m= 001 \quad (6)$

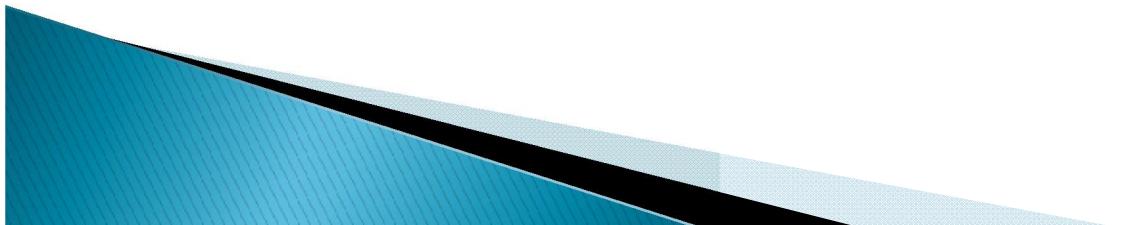
# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**MÃ HÓA CHO MÃ CYCLIC BẰNG  
PHƯƠNG PHÁP NHÂN**

# Nội dung

---

- ▶ Tạo các dấu kiểm tra của mã cyclic
- ▶ Thuật toán thiết lập từ mã hệ thống theo phương pháp nhân
- ▶ Sơ đồ thiết bị mã hóa theo phương pháp nhân



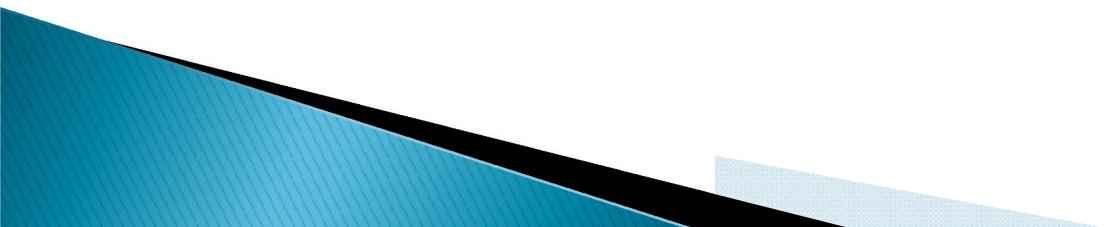
# Tạo các dấu kiểm tra của mã cyclic

- ▶ **Bài toán:** Cho mã cyclic  $(n,k)$  với đa thức sinh  $g(x)$ . Tìm từ mã  $c(x)$  tương ứng với bản tin  $m(x)$
- ▶ Ta có: đa thức kiểm tra

$$h(x) = \frac{x^n + 1}{g(x)}$$

$$c_{n-k-i} = \sum_{j=0}^{k-1} h_j c_{n-i-j}; \quad 1 \leq i \leq n-k \quad (**)$$

- ▶ Phương trình  $(**)$  giúp tính được các dấu kiểm tra  $c_0, c_1, \dots, c_{r-1}$



# Thuật toán thiết lập từ mã hệ thống theo phương pháp nhân

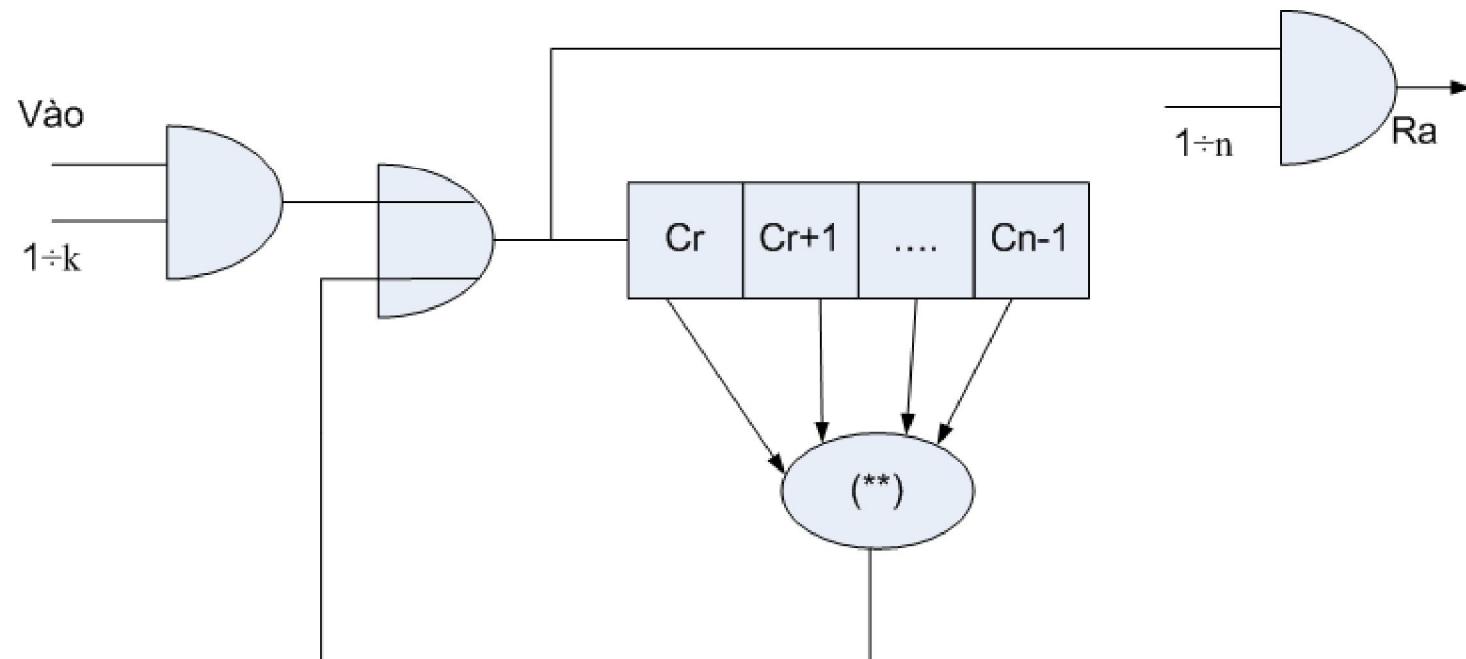
- ▶ Bước 1: Mã hóa tin m bằng đa thức thông tin  $m(x)$ .

$$\begin{aligned}c_{n-1} &= m_{k-1} & c_{n-2} &= m_{k-2} \\c_{n-k} &= c_r = m_0\end{aligned}$$

- ▶ Bước 2: Sử dụng công thức (\*\*) để tìm  $c_0, c_1, \dots, c_{r-1}$
- ▶ Bước 3: Thiết lập từ mã hệ thống:  
 $c = (c_0, c_1, \dots, c_{r-1}, c_r, \dots, c_{n-1})$

# Sơ đồ mã hóa cho mã cyclic bằng phương pháp nhân

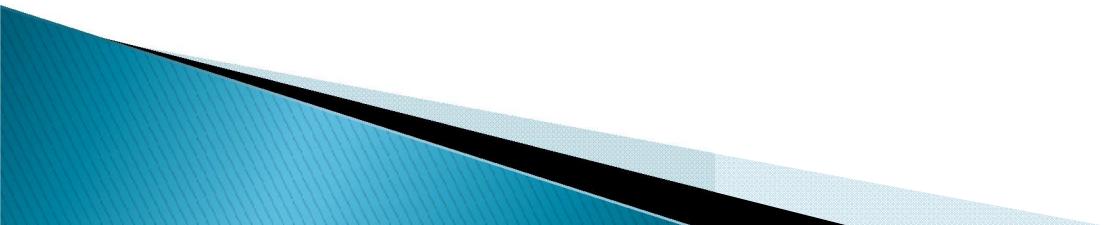
- ▶ k nhịp đầu: Đưa k bit thông tin vào các ô nhớ  $C_r, \dots, C_{n-1}$
- ▶ r nhịp sau: Tính  $C_0, C_1, \dots, C_{r-1}$  theo (\*\*)



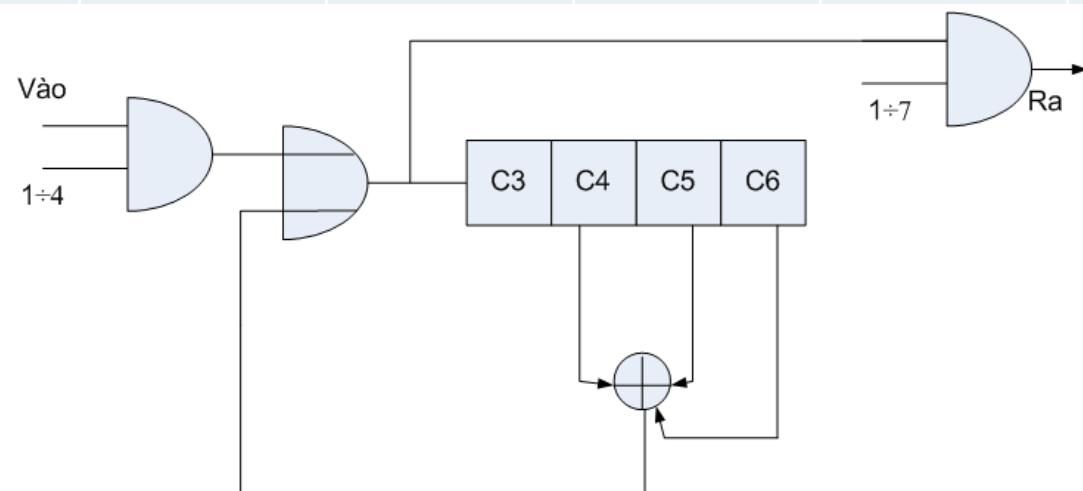
# Ví dụ

---

- ▶ Cho mã cyclic (7,4) có  $g(x)=1+x+x^3$ 
  - Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp nhân.
  - Tìm từ mã đầu ra tương ứng với đầu vào  $m=1001$
  - Kiểm tra lại kết quả bằng thuật toán mã hóa.



Xung nhịp	Vào	Trạng thái ô nhớ				Ra
		c3	c4	c5	c6	
1	1	1	0	0	0	1
2	0	0	1	0	0	0
3	0	0	0	1	0	0
4	1	1	0	0	1	1
5	0	1	1	0	0	1
6	0	1	1	1	0	1
7	0	0	1	1	1	0



# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**GIẢI MÃ CHO MÃ CYCLIC BẰNG  
PHƯƠNG PHÁP TỔNG KIỂM TRA  
TRỰC GIAO**

# Nội dung

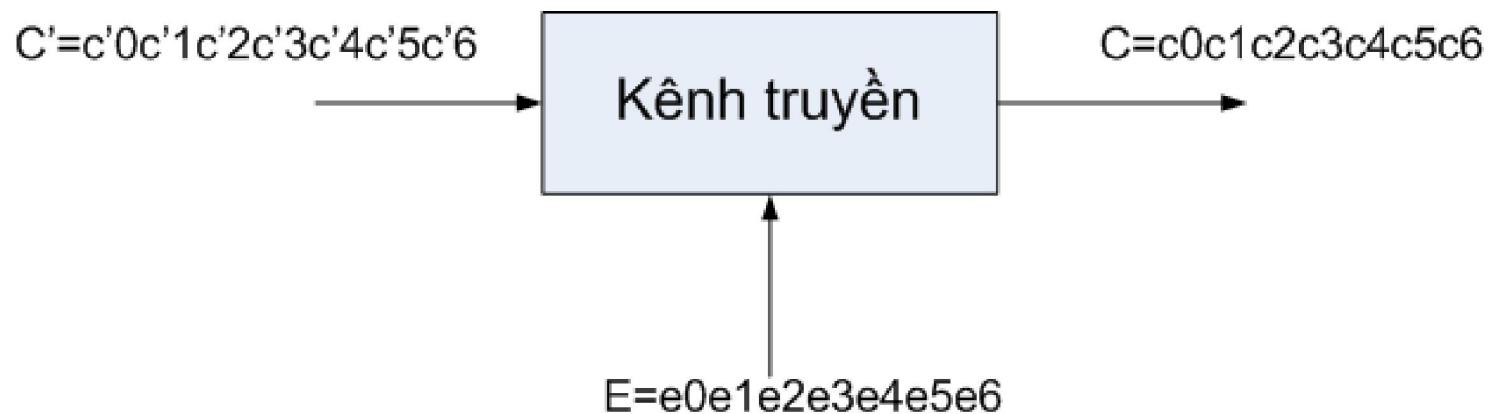
---

- ▶ Giải mã theo Syndrome
- ▶ Tổng kiểm tra trực giao
- ▶ Giải mã theo tổng kiểm tra trực giao
- ▶ Ví dụ



# Giải mã theo Syndrome

- ▶ **Bài toán:** Cho mã cyclic ( $n, k$ ). Giả sử phía thu nhận được từ mã  $n$  bit ( $c_0 c_1 c_2 c_3 c_4 c_5 c_6$ ). Hãy giải mã để tìm từ mã đã phát ở phía phát.
- ▶ Trước hết ta nói đến vecto sai  $e$ :



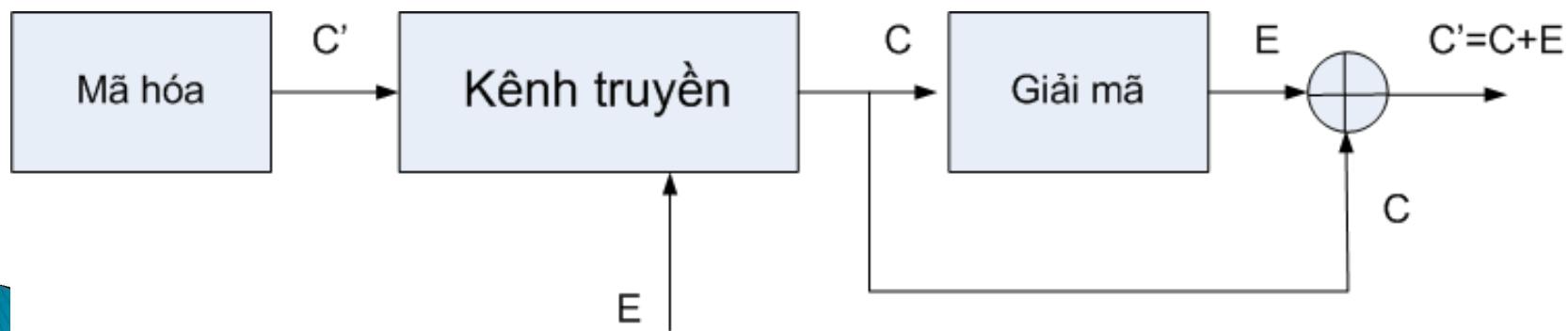
- ▶ Ta có:  $C = C' + E$ ;  $C' = C + E$  và  $E = C + C'$

# Giải mã theo Syndrome

## ▶ Kết luận:

- Tại những vị trí bit mà ở đó  $C'$  khác  $C$  thì bit tương ứng ở  $E$  bằng 1 và ngược lại.
- Ví dụ:  $C' = \textcolor{red}{11}00111$  và  $C = \textcolor{red}{00}00111$  thì  $E = \textcolor{red}{11}00000$
- Để tìm ra từ mã đã phát ở phía phát ta có thể tìm vector sai  $e$  tương ứng và sử dụng công thức:  
 $C' = C + E$

## ▶ Sơ đồ giải mã:



# Giải mã theo Syndrome

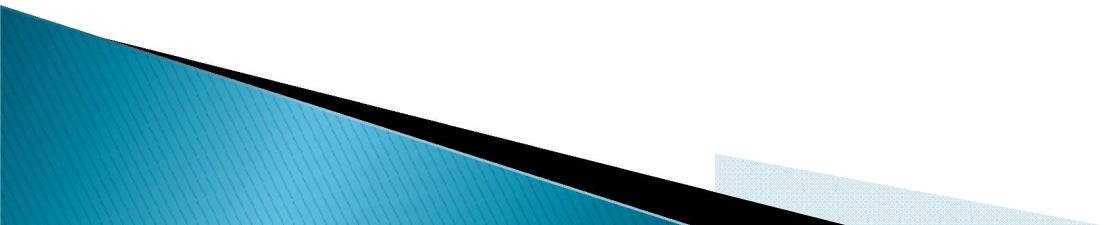
- ▶ Nhắc lại:

$$h(x) = \frac{x^n + 1}{g(x)} \quad h^*(x) = x^{\deg h(x)} \cdot h(x^{-1})$$

- ▶ Ma trận kiểm tra:

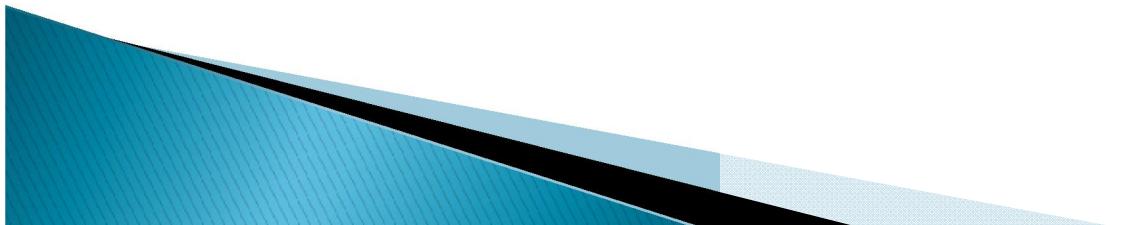
$$H = \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \dots \\ x^{r-1}h^*(x) \end{pmatrix}$$

- ▶ Từ mã:  $c' = m \cdot G$  mà  $G \cdot H^T = 0$  suy ra:  
 $c' \cdot H^T = m \cdot G \cdot H^T = 0$



# Giải mã theo Syndrome

- ▶ Kiểm tra từ mã c nhận được:  $c \cdot H^T = 0$ ?
- ▶ Tổng quát:  $c_{1 \times n} \cdot H_{n \times r}^T = s_{1 \times r}$   
 $\Leftrightarrow (c' + e) \cdot H^T = s$  mà  $c' \cdot H^T = 0$   
**suy ra:**  $e \cdot H^T = s$
- ▶ Dựa vào giá trị của **vector s** ta có thể giải mã ra được **vector sai e** tương ứng.
- ▶ Việc giải mã dựa vào vector s gọi là **giải mã theo syndrome**.



# Hệ tổng kiểm tra trực giao

► **Ví dụ:** Xét mã cyclic (7,3,4) có  $g(x)=1+x+x^2+x^4$   
Giả sử từ mã nhận được  $c(x)=x^2+x^3+x^4+x^5+x^6$   
Giải mã để tìm từ mã đã phát ở phía phát.

**Giải:** Trước hết ta xây dựng **tổng kiểm tra trực giao** cho mã này.

Ta có:

$$h(x) = \frac{x^n + 1}{g(x)} = \frac{x^7 + 1}{x^4 + x^2 + x + 1} = x^3 + x + 1$$

$$h^*(x) = x^3 \left( \frac{1}{x^3} + \frac{1}{x} + 1 \right) = 1 + x^2 + x^3$$

# Hệ tổng kiểm tra trực giao

- ▶ Ma trận kiểm tra:

$$H = \begin{pmatrix} h^*(x) \\ xh^*(x) \\ \dots \\ x^{r-1}h^*(x) \end{pmatrix} = \begin{pmatrix} 1+x^2+x^3 \\ x+x^3+x^4 \\ x^2+x^4+x^5 \\ x^3+x^5+x^6 \end{pmatrix} = \begin{pmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{pmatrix}$$

- ▶ Gia sử từ mã nhận được ở phía thu có dạng:

**C<sub>0</sub>C<sub>1</sub>C<sub>2</sub>C<sub>3</sub>C<sub>4</sub>C<sub>5</sub> C<sub>6</sub>**



# Hệ tổng kiểm tra trực giao

▶ Ta có:  $c \cdot H^T = (c_0 c_1 c_2 c_3 c_4 c_5 c_6)$

$\begin{matrix} 1000 \\ 0100 \\ 1010 \\ 1101 \\ 0110 \\ 0011 \\ 0001 \end{matrix}$

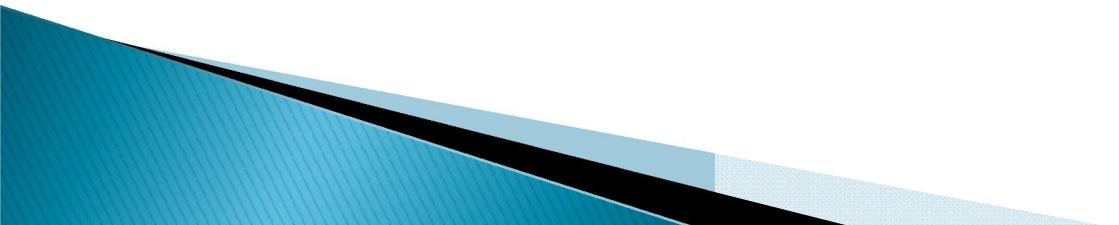
$$s = (c_0 + c_2 + c_3, c_1 + c_3 + c_4, c_2 + c_4 + c_5, c_3 + c_5 + c_6)$$

Chọn hệ tổng kiểm tra trực giao với  $c_3$ :

$$\left\{ \begin{array}{l} s_0 = c_0 + c_2 + c_3 \\ s_1 = c_1 + c_3 + c_4 \\ s_2 = c_3 + c_5 + c_6 \end{array} \right.$$

# Hệ tổng kiểm tra trực giao

- ▶ Đặc điểm của hệ tổng kiểm tra trực giao với  $c_i$  là:
  - Số tổng kiểm tra là  $t=d_0 - 1$
  - $c_i$  nằm trong **tất cả các tổng kiểm tra**.
  - Mọi  $c_j \neq c_i$  chỉ nằm trong **tối đa 1 tổng kiểm tra**
- ▶ Hệ tổng kiểm tra cho thấy:
  - Nếu  $c_i$  bị sai sẽ làm cho **tất cả các  $s_j$  bị sai**
  - Mọi  $c_j \neq c_i$  bị sai chỉ làm ảnh hưởng đến **tối đa 1 tổng kiểm tra** hay nói cách khác chỉ làm tối đa 1  $s_j$  bị sai.

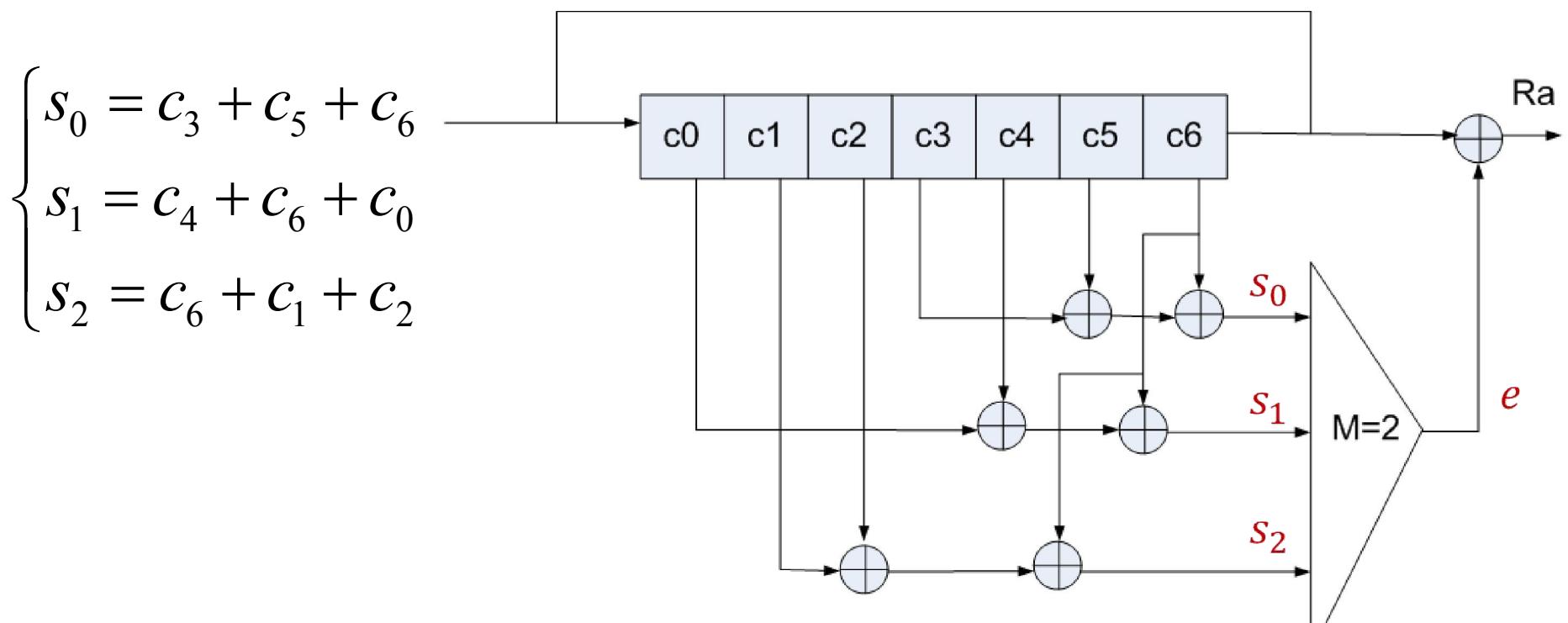


# Hệ tổng kiểm tra trực giao

- ▶ Xét hệ tkt: 
$$\begin{cases} s_0 = c_0 + c_2 + c_3 \\ s_1 = c_1 + c_3 + c_4 \\ s_2 = c_3 + c_5 + c_6 \end{cases}$$
- ▶ Nếu  $c_3$  sai thì tất cả các tkt đều có giá trị là 1 hay  $(s_0s_1s_2) = (111)$
- ▶ Nếu  $c_j \neq c_3$  sai thì chỉ có 1 tkt bằng 1 hay  $(s_0s_1s_2) = (100)(010)(001)$
- ▶ Ngược lại:
  - Nếu  $(s_0s_1s_2) = (111)$  thì  $e_3 = 1$  hay  $c_3$  sai.
  - Nếu  $(s_0s_1s_2) = (100)(010)(001)$  thì  $e_3 = 0$  hay  $c_3$  đúng.

# Sơ đồ giải mã theo tkt trực giao

- Ta có hệ tổng kiểm tra trực giao với  $c_6$ :



→  $c(x) = x^2 + x^3 + x^4 + x^5 + x^6 = 0011111$

# Hoạt động của mạch

Nhip	c <sub>0</sub>	c <sub>1</sub>	c <sub>2</sub>	c <sub>3</sub>	c <sub>4</sub>	c <sub>5</sub>	c <sub>6</sub>	s <sub>0</sub>	s <sub>1</sub>	s <sub>2</sub>	e	Ra
7	0	0	1	1	1	1	1					
8	1	0	0	1	1	1	1	1	0	0	0	1
9	1	1	0	0	1	1	1	1	1	1	1	0
10	1	1	1	0	0	1	1	0	1	0	0	1
11	1	1	1	1	0	0	1	0	0	1	0	1
12	1	1	1	1	1	0	0	0	0	1	0	1
13	0	1	1	1	1	1	0	1	0	0	0	0
14	0	0	1	1	1	1	1	0	1	0	0	0

Vậy từ mã đầu ra: c(x) = 0011101 =  $x^2 + x^3 + x^4 + x^6$

# Bài tập

---

1. Xét mã cyclic (7,3,4) có  $g(x)=1 + x^2 + x^3 + x^4$

Gia sử từ mã nhận được  $c(x)= x^2 + x^5 + x^6$

Giải mã để tìm từ mã đã phát ở phía phát.

2. Xét mã cyclic (7,3,4) có  $g(x)=1 + x^2 + x^3 + x^4$

Gia sử từ mã nhận được  $c(x)= x^2 + x^4 + x^6$

Giải mã để tìm từ mã đã phát ở phía phát.

3. Xét mã cyclic (7,3,4) có  $g(x)=1 + x + x^2 + x^4$

Gia sử từ mã nhận được  $c(x)= x^2 + x^4 + x^6$

Giải mã để tìm từ mã đã phát ở phía phát.



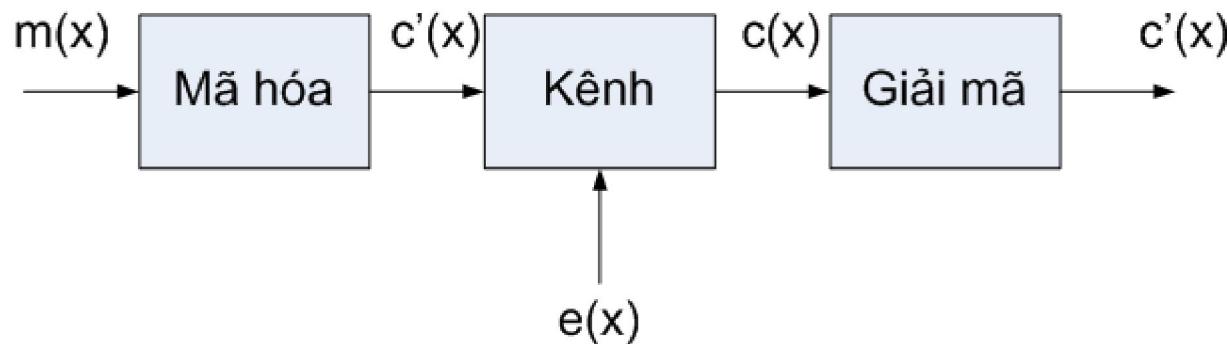
# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**GiẢI MÃ THEO PHƯƠNG PHÁP  
CHIA DỊCH VÒNG**

# Phương pháp chia dịch vòng

▶ Phía thu giải mã  $c(x)$  bằng cách lấy  $c(x)$  chia cho  $g(x)$  để tìm dư.

- Nếu từ mã  $c(x)$  nhận được đúng thì  $e(x)=0$
- Nếu từ mã  $c(x)$  nhận được sai thì  $e(x) \neq 0$



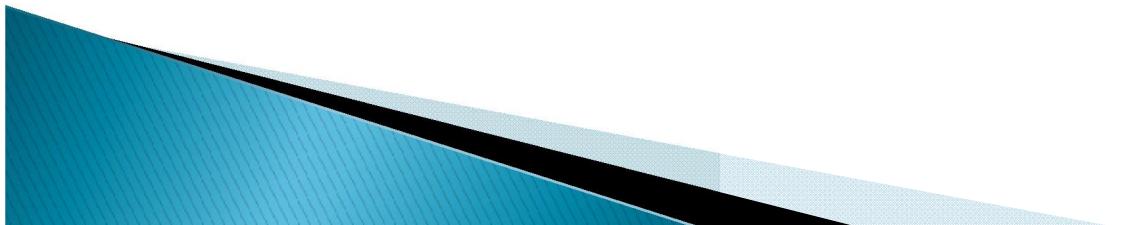
▶ Ta có:  $\frac{c(x)}{g(x)} = \frac{c'(x) + e(x)}{g(x)}$  mà  $c'(x) : g(x)$  nên

phần dư của  $c(x)$  cho  $g(x)$  chính là dư của  $e(x)$  cho  $g(x)$ .

# Phương pháp chia dịch vòng

---

- ▶ Từ mã nhận được:  $c_0c_1 \dots c_{r-1}c_r \dots c_{n-1}$
- ▶ Nếu sai xảy ra ở các vị trí  $c_0c_1 \dots c_{r-1}$  thì vecto sai  $e(x)$  có  $\deg e(x) \leq r-1 < \deg g(x)$ .
- ▶ Khi đó phần dư của  $e(x)$  cho  $g(x)$  chính là  $e(x)$ .
- ▶ Nếu sai không xảy ra ở các vị trí  $c_0c_1 \dots c_{r-1}$  thì sau khi dịch vòng sang trái hoặc sang phải một số lần thì các bit sai sẽ chuyển sang vị trí  $c_0c_1 \dots c_{r-1}$  hay nói cách khác ta **bãy được lỗi về vị trí mà ta muốn.**



# Thuật toán chia dịch vòng

**Vào:** Mã cyclic  $(n, k, d_0)$  với đa thức sinh  $g(x)$ .

Tùy mã nhận được  $c(x)$ .

**Ra:** Tùy mã ước lượng  $c'(x)$ .

**Bước 1:**  $i:=0$  to  $(n-1)$  thực hiện:

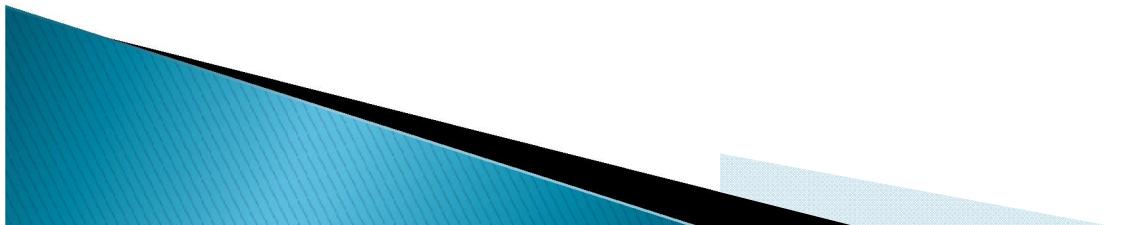
(1) Chia  $c(x) \cdot x^i$  cho  $g(x)$  để tìm dư  $r_i(x)$ .

(2) Tính  $w[r_i(x)]$

- Nếu  $w[r_i(x)] \leq t$  chuyển sang **bước 2**.

- Nếu  $w[r_i(x)] > t$  thì  $i:=i+1$ . Nếu  $i=n$  sang

**bước 3.**



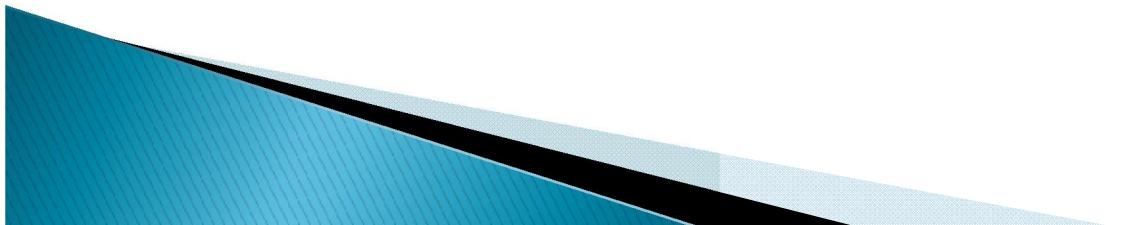
# Thuật toán chia dịch vòng

---

Bước 2: Từ mã ước lượng:

$$c'(x) = \frac{c(x) \cdot x^i + r_i(x)}{x^i}$$

Bước 3: Thông báo không sửa được sai (số sai vượt quá khả năng sửa sai của bộ mã).



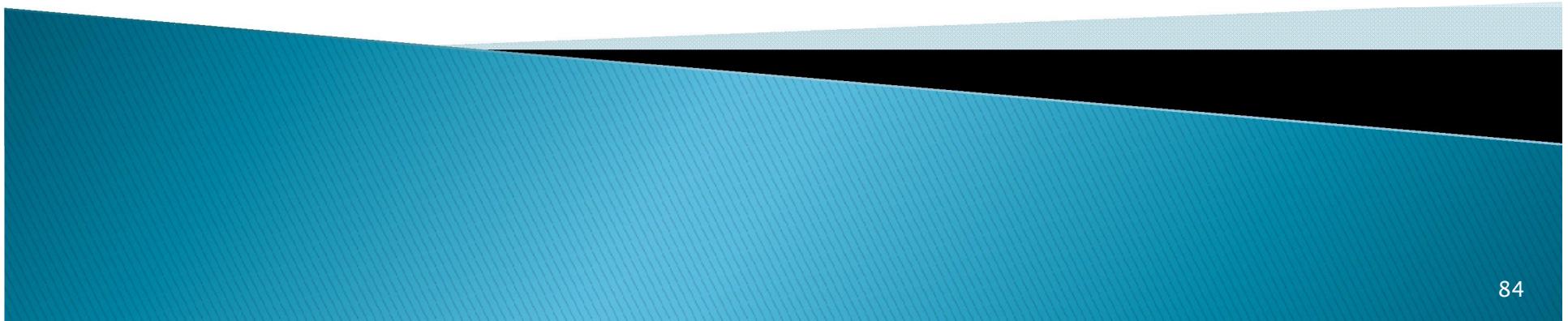
# Bài tập

- 
1. Cho mã cyclic (7,3,4) với đa thức sinh  $g(x)=1 + x^2 + x^3 + x^4$ . Giả sử từ mã nhận được  $c(x)= x^2 + x^4 + x^6$ . Giải mã bằng thuật toán chia dịch vòng để tìm ra từ mã đã phát.
  2. Cho mã cyclic (7,4,3) với đa thức sinh  $g(x)=1 + x^2 + x^3$ . Giả sử từ mã nhận được  $c(x)= x^2 + x^4$ . Giải mã bằng thuật toán chia dịch vòng để tìm ra từ mã đã phát.
  3. Cho mã cyclic (7,4,3) với đa thức sinh  $g(x)=1 + x + x^3$ . Giả sử từ mã nhận được  $c(x)= x^3 + x^4 + x^5 + x^6$ . Giải mã bằng thuật toán chia dịch vòng để tìm ra từ mã đã phát.

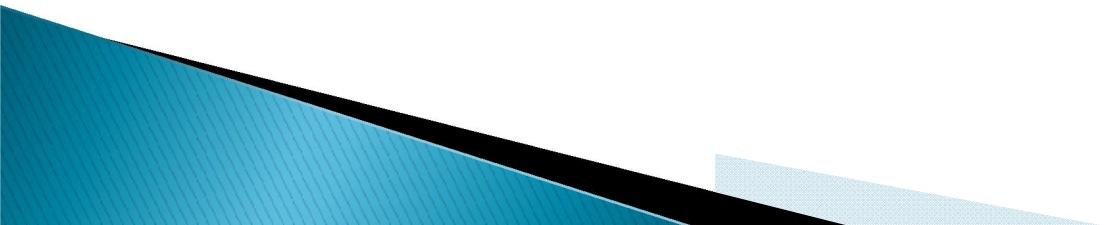


# **CHƯƠNG 4: CƠ SỞ LÝ THUYẾT MÃ HÓA**

**CHUYỂN MA TRẬN G CỦA MÃ CYCLIC  
VỀ DẠNG HỆ THỐNG**



- 
- ▶ Khi xây dựng ma trận sinh G cho mã cyclic từ đa thức sinh  $g(x)$  thì thông thường G không ở dạng hệ thống tức là  $G=[I:P]$ .
  - ▶ Để tạo ra dạng hệ thống ta xây dựng theo cách sau:
    - Hàng thứ  $\ell$  của ma trận G tương ứng với đa thức có dạng  $x^{n-\ell} + R_\ell(x)$  với  $\ell = 1, 2, \dots, k$  ở đó  $R_\ell(x)$  là đa thức bậc nhỏ hơn  $n-k$  và là phần dư của  $x^{n-\ell}$  cho đa thức sinh  $g(x)$



# Ví dụ

▶ Cho mã cyclic (7,4) với đa thức sinh

$g(x)=1 + x + x^3$ . Xây dựng ma trận G dạng hệ thống cho mã cyclic này.

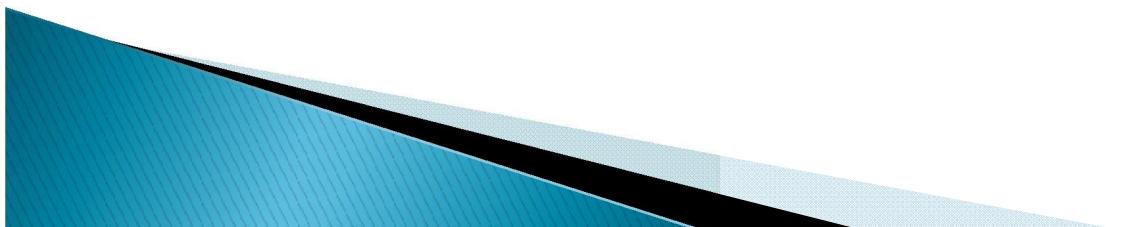
Giải:  $\ell=1,2,3,4$  khi đó  $x^{n-\ell} = x^6, x^5, x^4, x^3$

$$x^6 = (x^3 + x + 1)g(x) + (x^2 + 1)$$

$$x^5 = (x^2 + 1)g(x) + (x^2 + x + 1)$$

$$x^4 = xg(x) + (x^2 + x)$$

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



# Ma trận G dạng hệ thống

► Khi đó G có dạng:

$$G = \begin{pmatrix} x^6 + r_1(x) \\ x^5 + r_2(x) \\ x^4 + r_3(x) \\ x^3 + r_4(x) \end{pmatrix} = \begin{pmatrix} x^6 + x^2 + 1 \\ x^5 + x^2 + x + 1 \\ x^4 + x^2 + x \\ x^3 + x + 1 \end{pmatrix}$$

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