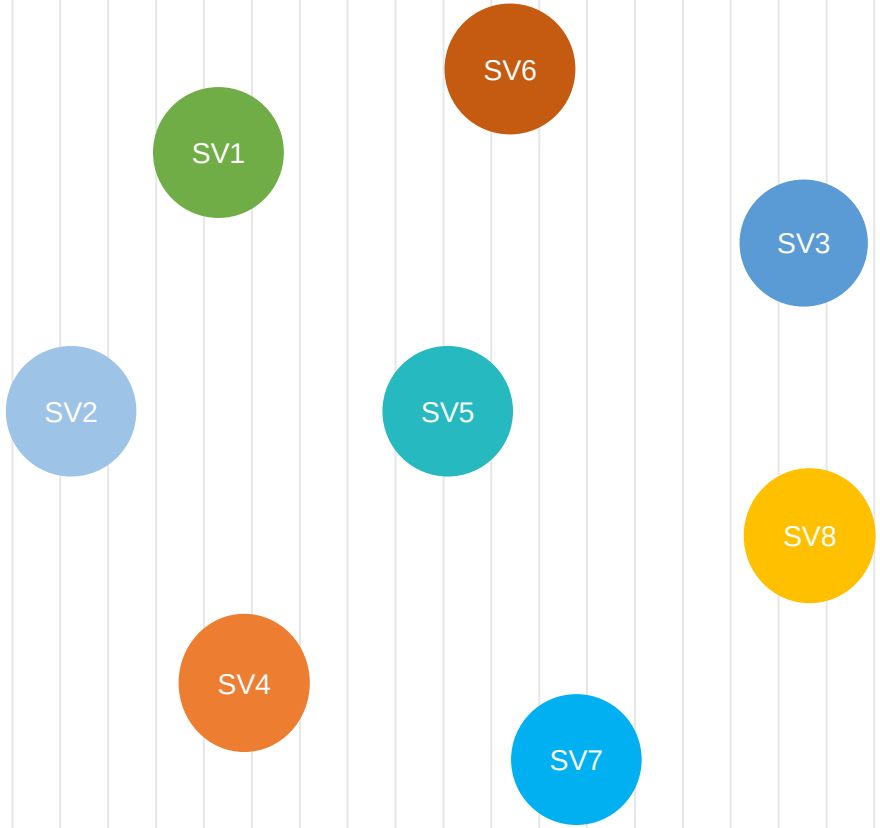
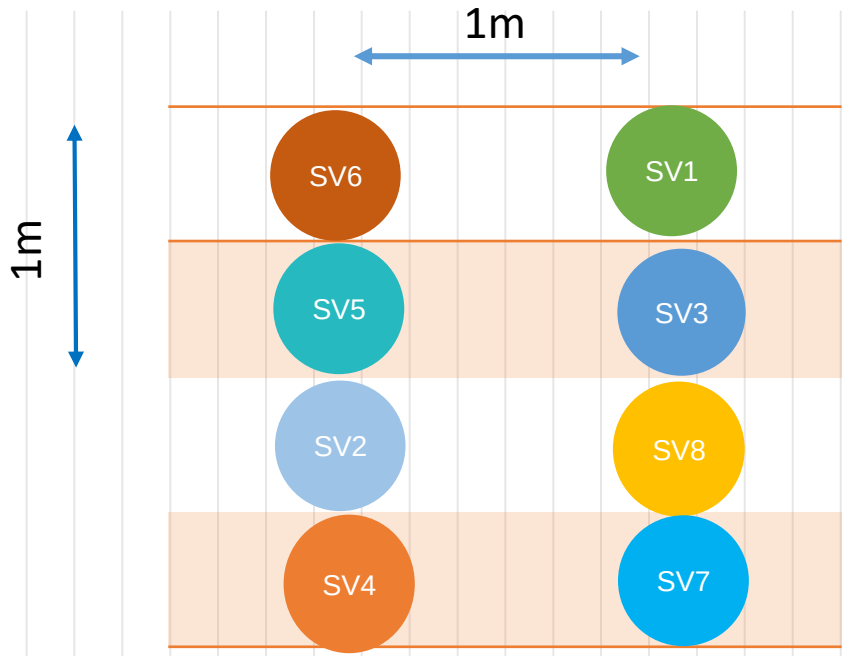
CHƯƠNG 5. MÃ HÓA KÊNH

KHÔNG GIAN BẢN TIN



Có 8 sinh viên

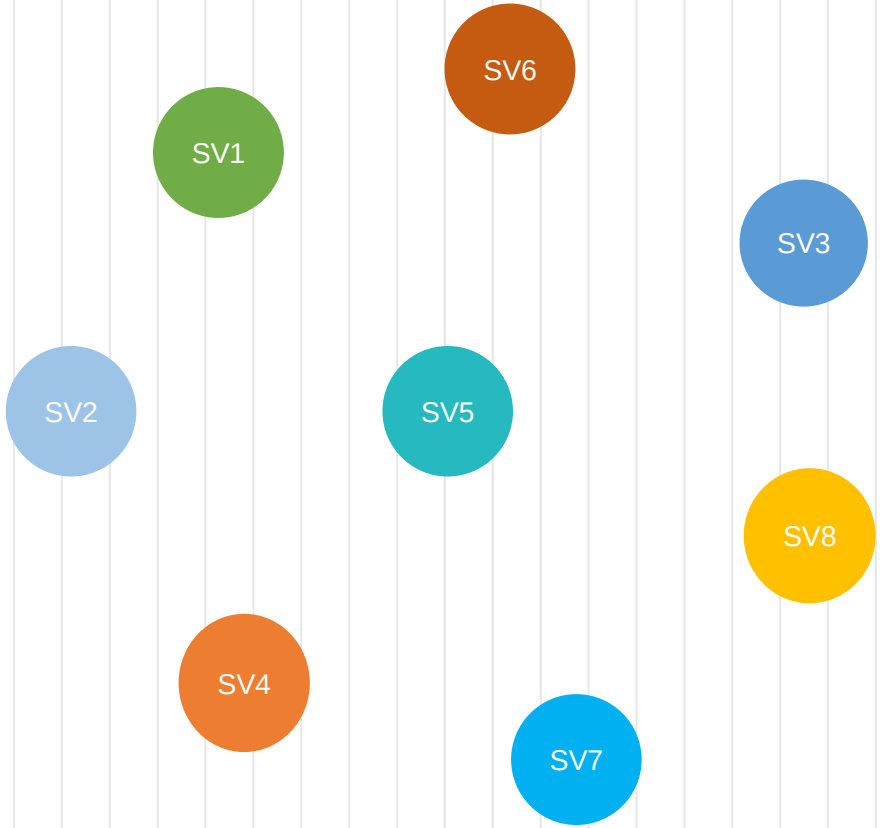
KHÔNG GIAN TỪ MÃ



Trường hợp 1: Chỉ có 8 chỗ ngồi

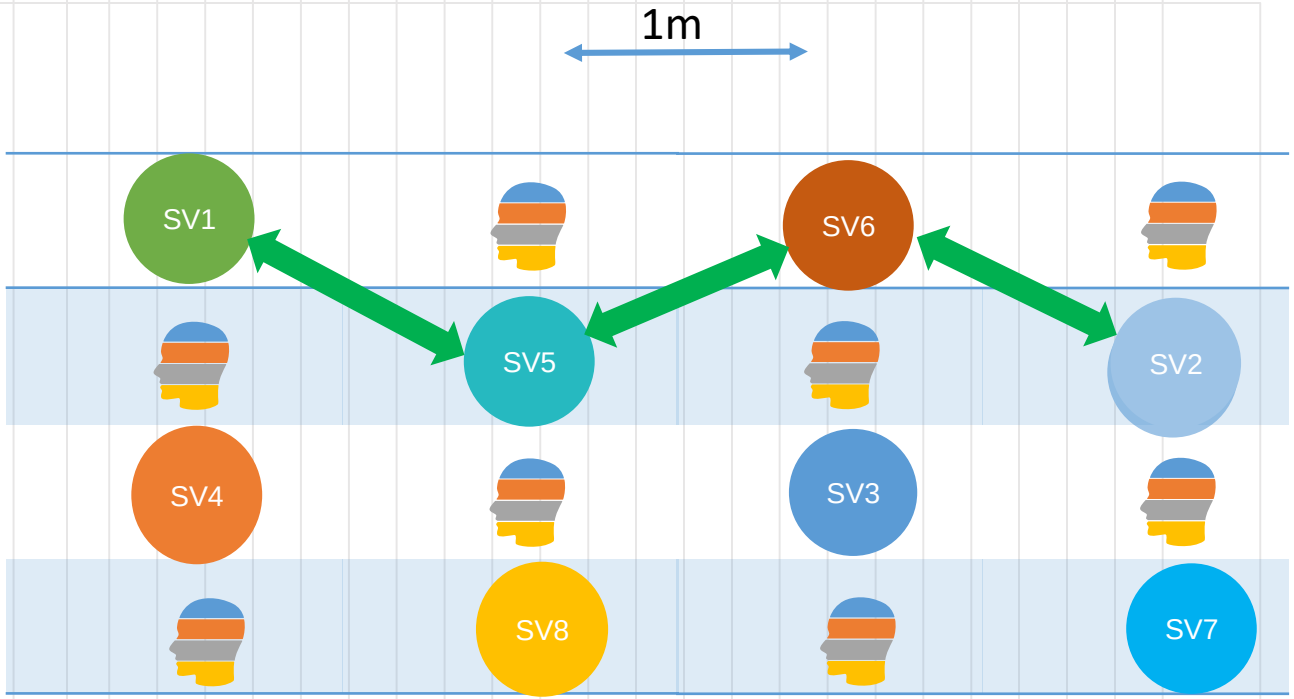
Câu hỏi: Có cách sắp xếp nào để khoảng cách giữa 2 sv lớn hơn 1m?

KHÔNG GIAN BẢN TIN



Có 8 sinh viên

KHÔNG GIAN TỪ MÃ



Trường hợp 2: Có 16 chỗ ngồi

Câu hỏi: Có cách sắp xếp nào để khoảng cách giữa 2 sv lớn hơn 1m?

Giới thiệu

- Mã hóa kênh, hay còn gọi là mã sửa sai được sử dụng để sửa các lỗi khi bản tin được truyền qua một kênh nhiễu. Phương tiện vật lý mà qua đó bản tin được truyền được gọi là kênh (ví dụ, đường dây điện thoại, đường dây vệ tinh, kênh không dây cho thông tin di động…).
- Ý tưởng chính đằng sau mã sửa sai là thêm một lượng dư thừa nào đó vào bản tin trước khi truyền trên kênh nhiễu. Lượng dư thừa này, về cơ bản gồm một số các ký tự thêm vào theo một quy luật đã biết. Bản tin sau mã hóa được truyền qua kênh có thể bị sai do nhiễu trên kênh. Tại phía thu, có thể khôi phục lại bản tin gốc từ phiên bản lỗi nếu số lỗi nằm trong giới hạn mà chiến lược mã hóa đã thiết kế.

Ví dụ 5.1

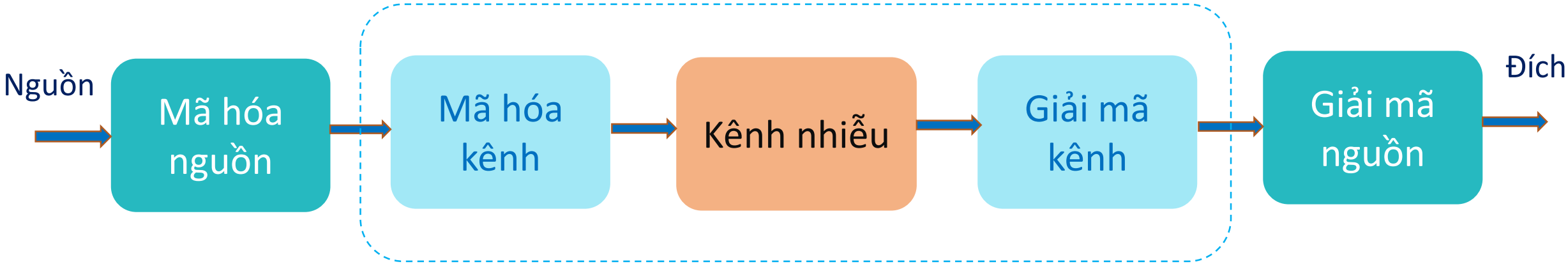
- Hãy xem xét dư thừa có thể chống lại ảnh hưởng của nhiễu như thế nào.
- Ngôn ngữ thông thường mà chúng ta sử dụng (ví dụ, tiếng Anh) có rất nhiều dư thừa trong bản thân nó.
- Xem xét câu sau (câu có thể bị sai do nhiễu):

CODNG THEORY IS AN INTRSTNG SUBJCT

- Do sự tương đồng của ngôn ngữ, chúng ta có thể dự đoán ra đoạn văn bản gốc:
- CODING THEORY IS AN INTERESTING SUBJECT

Chúng ta đã sử dụng chiến lược sửa sai bằng cách tận dụng dư thừa bên trong của bản thân ngôn ngữ để xây dựng lại bản tin gốc từ phiên bản nhiễu.

Sơ đồ khối của một hệ thống truyền tin số



Kênh không nhiễu tương đương

Mục tiêu của một bộ mã sửa sai tốt

(1) Khả năng sửa sai ở khía cạnh số lượng lỗi có thể sửa

(2) Mã hóa bản tin nhanh, nghĩa là chiến lược mã hóa hiệu quả

(3) Giải mã nhanh và hiệu quả cho từ mã nhận được

(4) Truyền thông tin tối đa trên một đơn vị thời gian (nghĩa là càng ít dữ liệu thêm vào)

Giới thiệu về mã khối

- Trong các hệ thống truyền dữ liệu số, thông tin được mã hóa bằng các chữ số nhị phân ‘0’ và ‘1’.
- Chuỗi thông tin nhị phân được chia thành các đoạn nhỏ gọi là các khối bản tin (message) có chiều dài cố định trong mã hóa khối.
- Mỗi khối bản tin gồm k bit thông thông tin, ký hiệu là vecto $\boldsymbol{u}$. Khi đó có tổng cộng 2^k bản tin.
- Khi thực hiện mã hóa kênh, bản tin $\boldsymbol{u}$ này sẽ được chuyển thành từ mã $\boldsymbol{v}$ gồm n bit (n>k).
- 2^k bản tin sẽ tương ứng với 2^k từ mã. Tập 2^k vecto từ mã này gọi là một bộ mã khối.

Ví dụ 5.2

- Bộ mã $C = \{00000, 10100, 11110, 11001\}$ là một bộ mã khối có độ dài khối là 5.
- Mã $(5,2)$ này được sử dụng để mã hóa cho các bản tin có 2 bit như sau:

Bản tin (k bit)	Từ mã (n bit)
00	00000
01	10100
10	11110
11	11001

- Giả sử phải truyền một chuỗi 1 và 0 sử dụng mã trên: 1001010011…
- Mã hóa: Chia chuỗi dữ liệu thành các khối 2 bit 10 01 01 00 11… và mã hóa thành chuỗi: 11110 10100 10100 00000 11001…
- Giả sử chuỗi nhận được: 11100 10100 10100 00100 11001

Một số định nghĩa cơ bản

Định nghĩa 5.1. Một từ mã là một chuỗi các ký tự.

Định nghĩa 5.2. Một bộ mã là một tập các vector gọi là từ mã

Định nghĩa 5.3. Trọng số của một từ mã bằng số lượng các thành phần khác 0 trong từ mã. Trọng số của từ mã c được ký hiệu là $w(c)$.

Định nghĩa 5.4. Khoảng cách Hamming giữa hai từ mã là số các vị trí mà ở đó hai từ mã khác nhau. Ký hiệu khoảng cách Hamming giữa hai từ mã c_1 và c_2 là $d(c_1, c_2)$.

Tính chất: $$d(c_1, c_2) = w(c_1 + c_2)$$

Khoảng cách tối thiểu của bộ mã: $d_0 = \min d(c_i, c_j)$

Định nghĩa 5.5. Một bộ mã khối gồm một tập các từ mã độ dài cố định. Độ dài cố định của các từ mã này được gọi độ dài khối và thường được ký hiệu là n. Vì vậy, một bộ mã độ dài n gồm một tập các từ mã có n thành phần.

Ví dụ 5.3

Xét một bộ mã $C = \{0100, 1111\}$ gồm hai từ mã $c_1 = 0100$ và $c_2 = 1111$.

Trọng số từ mã: $w(0100) = 1; w(1111) = 4$

Khoảng cách giữa hai từ mã:

$$d(0100, 1111) = 3$$

$$(c_1 + c_2) = 1011;$$

$$w(c_1 + c_2) = 3 = d(0100, 1111)$$

1.
MÃ KHỐI TUYẾN TÍNH

Dạng tuyến tính và mã tuyến tính

- Dạng tuyến tính:

Các dạng tuyến tính của k biến độc lập $m_1, m_2, \dots, m_k$ là các biểu thức có dạng:

$f(m_1, m_2, \dots, m_k) = \sum_{i=1}^{k} m_i x_i$ với $x_i \in \{0,1\}$.

- Mã tuyến tính:

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

- Mã hệ thống tuyến tính (n, k): là mã tuyến tính độ dài từ mã n trong đó có k ký tự đầu tiên (hoặc cuối cùng) của từ mã chính là k ký tự thông tin. $(n - k)$ ký tự còn lại gọi là các ký tự kiểm tra chẵn lẻ (dư thừa).

Phần kiểm tra (dư thừa) (n-k) bit	Phần bản tin (k) bit

Tính chất của mã khối tuyến tính

- Tổng của hai từ mã trong bộ mã cũng là một từ mã thuộc bộ mã.
- Từ mã toàn 0 luôn luôn là một từ mã.
- Khoảng cách Hamming tối thiểu giữa hai từ mã của một bộ mã khối tuyến tính bằng trọng số tối thiểu của các từ mã khác 0 trong bộ mã.

Ví dụ 5.4 về mã khối tuyến tính

- Bộ mã $C = \{0000, 1010, 0101, 1111\}$ là mã khối tuyến tính có độ dài 4.
- Quan sát tổng các từ mã:
  - 0000 + 0000 = 0000, 0000 + 1010 = 1010,
  - 0000 + 0101 = 0101, 0000 + 1111 = 1111,
  - 1010 + 1010 = 0000, 1010 + 0101 = 1111,
  - 1010 + 1111 = 0101, 0101 + 0101 = 0000,
  - 0101 + 1111 = 1010 và
  - 1111 + 1111 = 0000

  Tất cả các tổng đều là các từ mã nằm trong bộ mã.
- Khoảng cách Hamming giữa hai từ mã:
  - d(0000, 1010) = 2, d(0000, 0101) = 2, d(0000, 1111) = 4
  - d(1010, 0101) = 4, d(1010, 1111) = 2, d(0101, 1111) = 2

  $d_0 = \min\{d\} = 2$
- Trọng số tối thiểu của từ mã: $\mathbf{min}\left(\boldsymbol{W}(\boldsymbol{c_i})\right) = \mathbf{2} = \boldsymbol{d_0}$
- Hỏi mã trong ví dụ 5.2 có phải là mã khối tuyến tính không? Tại sao?

Ví dụ 5.5

- Xét mã khối nhị phân (6,3):
- $m_1 m_2 m_3 \rightarrow c_1 c_2 c_3 c_4 c_5 c_6$

000	000000
001	001011
010	010111
011	011100
100	100101
101	101110
110	110010
111	111001

c_1=	m_1
c_2=	m_2
c_3=	m_3
c_4=	m_1+m_2
c_5=	m_2+m_3
c_6=	m_1+m_2+m_3

- Mã này có phải là mã khối tuyến tính hay không? Vì sao?

Định lý về khả năng phát hiện sai và sửa sai của một bộ mã khối tuyến tính

Định lý về khả năng phát hiện sai:

Một bộ mã khối tuyến tính (n, k, d_0) có khả năng phát hiện được t sai thỏa mãn: $t \leq d_0 - 1$.

Định lý về khả năng sửa sai:

Một bộ mã khối tuyến tính (n, k, d_0) có khả năng sửa được t sai thỏa mãn: $t \leq \left[\frac{d_0 - 1}{2}\right]$

Ma trận sinh và ma trận kiểm tra

- Một trong những mục tiêu của việc thiết kế một bộ mã tốt là phải có phương pháp mã hóa và giải mã nhanh và hiệu quả.
- Để tạo bộ mã khối tuyến tính một cách hiệu quả, sử dụng ma trận sinh **G**.
- Từ mã được tạo ra bằng cách nhân bản tin với ma trận sinh.
- Ở phía thu, có thể phát hiện ra từ mã hợp lệ sử dụng khái niệm tương đương, đó là sử dụng ma trận kiểm tra **H**.

Ma trận sinh của mã khối tuyến tính

- Trở lại ví dụ 5.5: $m_1 m_2 m_3 \rightarrow c_1 c_2 c_3 c_4 c_5 c_6$ hay $\boldsymbol{m}_{1\times 3} \rightarrow \boldsymbol{c}_{1\times 6}$.
- Tìm ma trận $\boldsymbol{G}$ thỏa mãn: $\boldsymbol{c}_{1\times 6} = \boldsymbol{m}_{1\times 3}.\boldsymbol{G}_{3\times 6}$.

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

$$c_1 = m_1 g_{11} + m_2 g_{21} + m_3 g_{31} = m_1$$
$$c_2 = m_1 g_{12} + m_2 g_{22} + m_3 g_{32} = m_2$$
$$c_3 = m_1 g_{13} + m_2 g_{23} + m_3 g_{33} = m_3$$
$$c_4 = m_1 g_{14} + m_2 g_{24} + m_3 g_{34} = m_1 + m_2$$
$$\ldots\ldots$$

$$g_{11} = 1; g_{21} = 0; g_{31} = 0$$
$$g_{12} = 0; g_{22} = 1; g_{31} = 0$$
$$g_{13} = 0; g_{23} = 0; g_{33} = 1$$
$$g_{14} = 1; g_{24} = 1; g_{31} = 0$$
$$\ldots\ldots$$

Ma trận sinh G

- $\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$
- Mã này có phải là mã khối tuyến tính dạng hệ thống?
- $\boldsymbol{G} = (I|P)$ hoặc $(P|I)$ (dạng hệ thống)
- Khi G ở dạng hệ thống thì mã được tạo ra là mã hệ thống.

Ví dụ 5.6 về ma trận sinh

- Xét ma trận sinh: $\boldsymbol{G} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$

$$\boldsymbol{c}_1 = [0\ 0]\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = [0\ 0\ 0], \qquad \boldsymbol{c}_2 = [0\ 1]\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = [0\ 1\ 0]$$

$$\boldsymbol{c}_3 = [1\ 0]\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = [1\ 0\ 1], \qquad \boldsymbol{c}_4 = [1\ 1]\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} = [1\ 1\ 1]$$

- Ma trận sinh tạo ra bộ mã $C = \{000, 010, 101, 111\}$.
- Đây là mã $(3,2)$ với kích thước ma trận sinh là 2×3.
- Tỷ lệ mã: $r = \frac{k}{n} = \frac{2}{3}$
- Mã này là mã dạng hệ thống vì G ở dạng hệ thống.

Ví dụ 5.7

Ma trận sinh của mã khối tuyến tính (5,3) được cho bởi:

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

Tìm các từ mã của bộ mã dạng hệ thống và không hệ thống.

Giải: Vì G không ở dạng hệ thống, có thể tạo ra dạng hệ thống cho G bằng một số phép hoán vị các hàng với nhau.

Hoán đổi vị trí của hàng 2 và hàng 3 ta được: $\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$

Cộng hàng 1 và hàng 2 ta được: $\boldsymbol{G} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = (\boldsymbol{P}|\boldsymbol{I})$

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

Từ mã dạng không hệ thống		Từ mã dạng hệ thống	
Bản tin	Từ mã	Bản tin	Từ mã
(0 0 0)	(0 0 0 0 0)	(0 0 0)	(0 0 0 0 0)
(1 0 0)	(1 0 1 0 0)	(1 0 0)	(1 0 1 0 0)
(0 1 0)	(0 1 0 0 1)	(0 1 0)	(1 1 0 1 0)
(1 1 0)	(1 1 1 0 1)	(1 1 0)	(0 1 1 1 0)
(0 0 1)	(0 1 1 1 0)	(0 0 1)	(0 1 0 0 1)
(1 0 1)	(1 1 0 1 0)	(1 0 1)	(1 1 1 0 1)
(0 1 1)	(0 0 1 1 1)	(0 1 1)	(1 0 0 1 1)
(1 1 1)	(1 0 0 1 1)	(1 1 1)	(0 0 1 1 1)

Ma trận kiểm tra H của mã khối tuyến tính

- Đối với bất kỳ ma trận $\boldsymbol{G}_{k\times n}$, luôn tồn tại ma trận $\boldsymbol{H}_{(n-k)\times n}$ sao cho:

$$\boldsymbol{G}.\boldsymbol{H}^{T} = \mathbf{0}$$

- Ma trận H này gọi là ma trận kiểm tra chẵn lẻ của mã.
- Nếu c là một từ mã hợp lệ của bộ mã thì: $\boldsymbol{c} = \boldsymbol{m}.\boldsymbol{G}$
- Do đó:

$$\boldsymbol{c}.\boldsymbol{H}^{\boldsymbol{T}} = \boldsymbol{m}.\boldsymbol{G}.\boldsymbol{H}^{\boldsymbol{T}} = \mathbf{0}$$

- Nếu $\boldsymbol{G}$ ở dạng hệ thống, ma trận $\boldsymbol{H}$ sẽ có dạng:

$\boldsymbol{G} = (\boldsymbol{I}\|\boldsymbol{P})$	$\mathbf{H} = (\boldsymbol{P}^{\boldsymbol{T}}\|\mathbf{I}')$
$\boldsymbol{G} = (\mathbf{P}\|\mathbf{I})$	$\mathbf{H} = (\mathbf{I}'\|\boldsymbol{P}^{\boldsymbol{T}})$

Ví dụ 5.8

- Tìm ma trận kiểm tra của mã (7,4) với ma trận sinh:

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

- Giải: Ma trận $\boldsymbol{G} = (\mathbf{P}|\mathbf{I})$ nên $\mathbf{H} = (\mathbf{I}'|\boldsymbol{P^T})$ với $\mathbf{P} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$
- Chuyển vị của ma trận P là:

$$\mathbf{P}^T = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

- Do đó ma trận kiểm tra **H** là:

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

Bài tập

1. a. Tìm ma trận kiểm tra $\boldsymbol{H}$ của mã khối tuyến tính (5,3) biết: $\mathbf{G} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$

   b. Tính $\boldsymbol{G}.\boldsymbol{H}^T$ và c. $\boldsymbol{H}^T$ với $c = (11010)$

2. Xét một mã hệ thống (8, 4) với các bit kiểm tra (dư thừa) được tạo ra như sau:

$$c_0 = m_0 + m_1 + m_2$$
$$c_1 = m_1 + m_2 + m_3$$
$$c_2 = m_0 + m_1 + m_3$$
$$c_3 = m_0 + m_2 + m_3$$

ở đó m_0, m_1, m_2, m_3 là các bit bản tin và c_0, c_1, c_2, c_3 là các bit kiểm tra

(a) Tìm ma trận sinh và ma trận kiểm tra của mã.

(b) Tìm trọng số tối thiểu của bộ mã.

(c) Mã này có khả năng phát hiện và sửa bao nhiêu sai.

(d) Cho một ví dụ mã có thể phát hiện được 3 sai trong một từ mã.

2.

MÃ CYCLIC (MÃ VÒNG)

Giới thiệu

- Mã cyclic là một lớp mã con của mã khối tuyến tính.
- Dịch vòng của một từ mã cyclic là một từ mã hợp lệ khác.
- Đặc điểm này của mã cyclic giúp việc mã hóa và giải mã dễ dàng nhờ sử dụng các thanh ghi dịch và kết nối phản hồi.

Vành đa thức

- Phép cộng đa thức
- Phép nhân đa thức
- Phép dịch vòng
- Định nghĩa vành đa thức

Phép cộng đa thức

- Xét tập các đa thức có dạng sau:

  $f(x) = \sum_{i=0}^{n-1} f_i x^i \quad (*)$ với $degf(x) \leq n-1; \quad f_i \in \{0,1\}$

- Xét 2 đa thức có dạng giống $f(x)$:

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

Ta có:

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

Phép cộng đa thức là một phép toán trong hai ngôi.

Phép nhân đa thức

- Để tích $a(x).b(x)$ cũng là một phép toán trong hai ngôi (nghĩa là bậc đa thức tối đa là $n-1$) thì phải thực hiện nhân hai đa thức theo modulo x^n+1 (hay $x^n=1$).

$$\mathrm{a}(x).b(x) = \left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) mod(x^n+1)$$

- Ví dụ: $n=6; a(x)=1+x+x^3; b(x)=x+x^4$
- $\mathrm{a}(x)+b(x)=1+x^3+x^4$
- $\mathrm{a}(x).b(x)=(1+x+x^3)(x+x^4)mod(x^6+1)=x^5+x^2$

Phép dịch vòng

- Ví dụ: $n = 6; a(x) = 1 + x + x^3; b(x) = x + x^4$
- $a(x) \leftrightarrow 1\ 1\ 0\ 1\ 0\ 0$
- $b(x) \leftrightarrow 0\ 1\ 0\ 0\ 1\ 0$
- $x.a(x) = x + x^2 + x^4 \leftrightarrow 0\ 1\ 1\ 0\ 1\ 0$
- $x^5.a(x) = x^5 + x^6 + x^8 = x^5 + 1 + x^2$ ($x^6 = 1$)
- 0 1 1 0 1 0 chính là dịch vòng phải của 1 1 0 1 0 0

- Tổng quát: Dịch vòng của $(c_0, c_1, \dots, c_{n-1})$ là $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$

- $F(x)=f0+f1.x+f2.x^2+f3.x^3+f4.x^4+f5.x^5$

Định nghĩa vành đa thức

- Tập các đa thức có dạng $f(x) = \sum_{i=0}^{n-1} f_i x^i$ với hai phép toán cộng đa thức và phép 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 này là $Z_2[x]/x^n + 1$.
- Ví dụ: Các phần tử trong vành $Z_2[x]/x^7 + 1$ là các đa thức có dạng $f(x) = \sum_{i=0}^{6} f_i x^i$ với $f_i \in \{0,1\}$

Ideal của vành đa thức

- Ideal I của vành đa thức $Z_2[x]/\ x^n+1$ gồm các đa thức $a(x)$ với $a(x)$ là bội của đa thức $g(x)$ với $g(x)$ thỏa mãn:

  (1) $g(x)$ là ước của x^n+1

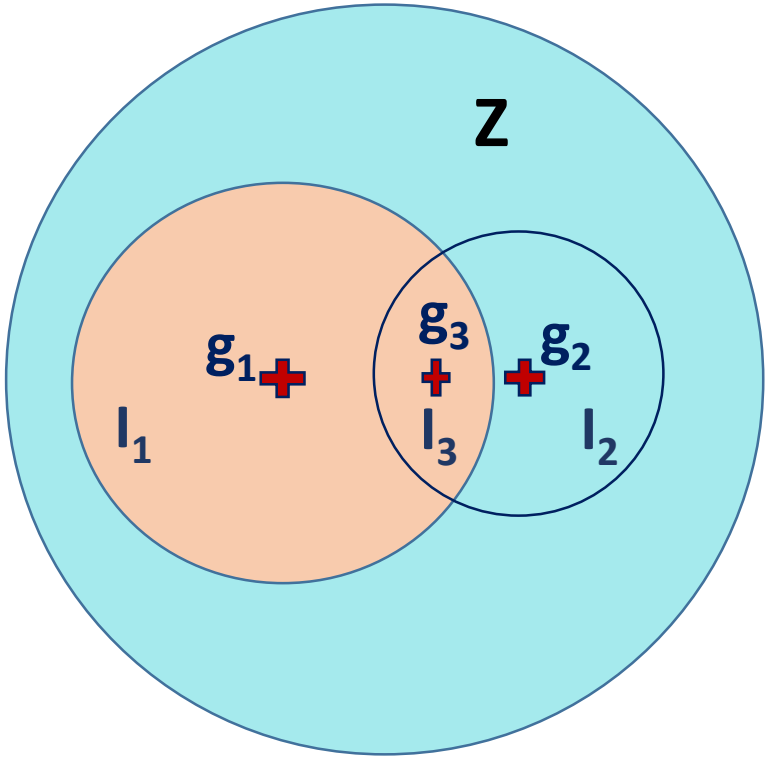
  (2) $\deg g(x) = r = n - k = \min(\deg a(x))$

  Ký hiệu $I =< g(x) >$

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

Ví dụ 5.9

- Xét vành số $Z = \{0,1,2 \ \ldots, 17\}$
- Ideal của vành Z là tập hợp các số a là bội số của g với g là ước của 18.
- $g \in \{1, 2, 3, 6, 9\}$
- $g_1 = 2$, khi đó $I_1 = \{2, 4, 6, 8, 10, 12, 14, 16\}$
- $g_2 = 3$, khi đó $I_2 = \{3, 6, 9, 12, 15\}$ …
- $g_3 = 6$, khi đó $I_3 = \{6, 12\}$ …



Ví dụ 5.10

- Tìm các Ideal trên vành $Z_2[x]\ /x^7+1$.
- $x^7+1=(x+1)(x^3+x+1)(x^3+x^2+1)$

$\boldsymbol{g_1(x)}$	$\boldsymbol{x+1}$
$\boldsymbol{g_2(x)}$	$\boldsymbol{x^3+x+1}$
$\boldsymbol{g_3(x)}$	$\boldsymbol{x^3+x^2+1}$
$\boldsymbol{g_4(x)}$	$\boldsymbol{(x+1)(x^3+x+1)}$
$\boldsymbol{g_5(x)}$	$\boldsymbol{(x+1)(x^3+x^2+1)}$
$\boldsymbol{g_6(x)}$	$\boldsymbol{(x^3+x+1)(x^3+x^2+1)}$

Ví dụ 5.11

- Cho $g(x) = x^4 + x^2 + x + 1$. Xây dựng các phần tử của Ideal $I = < g(x) >$
- Giải:
- Gọi $a(x)$ là phần tử của Ideal I. $a(x) = g(x).m(x)$
- $\deg a(x) \leq 6$ ➔ $\deg m(x) \leq 2$. Vậy $m(x) = m_0 + m_1 x + m_2 x^2$

$m_0 m_1 m_2$	$m(x)$		$a(x)$	$a_0 a_1 a_2 a_3 a_4 a_5 a_6$
000	0	$\times g(x)$ $1 + x + x^2 + x^4$	0	0000000
100	1		$1 + x + x^2 + x^4$	1110100
010	x		$x + x^2 + x^3 + x^5$	0111010
001	x^2		$x^2 + x^3 + x^4 + x^6$	0011101
110	$1 + x$		$1 + x^3 + x^4 + x^5$	1001110
101	$1 + x^2$		$1 + x + x^3 + x^6$	1101001
011	$x + x^2$		$x + x^4 + x^5 + x^6$	0100111
111	$1 + x + x^2$		$1 + x^2 + x^5 + x^6$	1010011

Mã cyclic

- Một mã cyclic C(n,k) là một ideal trên vành $Z_2[x]/\ x^n+1$ với đa thức sinh g(x) có $\deg g(x) = n - k = r$

- Định nghĩa: Một mã khối tuyến tính $C(n, k)$ được gọi là mã cyclic nếu dịch vòng của một vector từ mã trong C là một vector từ mã khác trong C. Điều này có nghĩa là nếu từ mã $(c_0, c_1, \dots, c_{n-1})$ nằm trong C thì $(c_{n-1}, c_0, c_1, \dots, c_{n-2})$ cũng là một từ mã nằm trong C.

Ma trận sinh của mã cyclic

- Đối với mã khối tuyến tính: $c = m.G$ (1)
- Đối với mã cyclic: $c(x) = m(x)g(x)$ (2)
- Bản tin m gồm k bit nên $m(x) = m_0 + m_1x^1 + \cdots + m_{k-1}x^{k-1}$
- Từ (2): $c(x) = g(x)(m_0 + m_1x^1 + \cdots + m_{k-1}x^{k-1})$
- $= g(x)m_0 + g(x)m_1x^1 + \cdots + g(x)m_{k-1}x^{k-1}$
- $= (m_0 \;\; m_1 \;\; \ldots m_{k-1}) \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix} = m.G$
- Do đó: $G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$

Ma trận kiểm tra của mã cyclic

- Ma trận kiểm tra: H= $\begin{pmatrix} h^*(x) \\ x.h^*(x) \\ \vdots \\ x^{r-1}h^*(x) \end{pmatrix}$
- Với $h^*(x) = x^{\deg h(x)} h(x^{-1})$
- $h(x)$ là đa thức kiểm tra của mã cyclic: $h(x) = \frac{x^n+1}{g(x)}$
- $\deg h(x) = k;\ h_0 = h_k = 1$

- Ví dụ:
- Tìm ma trận sinh và ma trận kiểm tra của mã cyclic C(7,3) với $g(x) = 1 + x^2 + x^3 + x^4$.

Bài tập

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

a. Tìm mã cyclic có tỉ lệ mã k/n nhỏ nhất với đa thức sinh là $g(x)$.

b. Tìm khoảng cách Hamming của bộ mã ở câu a.

2. Tìm mã cyclic (8,5) trên vành đa thức $Z_2[x]/\ x^8+1$. Tìm khoảng cách Hamming của mã đó.

3. a. Xây dựng một mã cyclic (6,2) trên trường $Z_2[x]/\ x^6+1$.

b. Tìm ma trận G dạng hệ thống của mã này và tìm tất cả các từ mã của bộ mã.

c. Mã này có thể sửa bao nhiêu lỗi?

Một số biến đổi

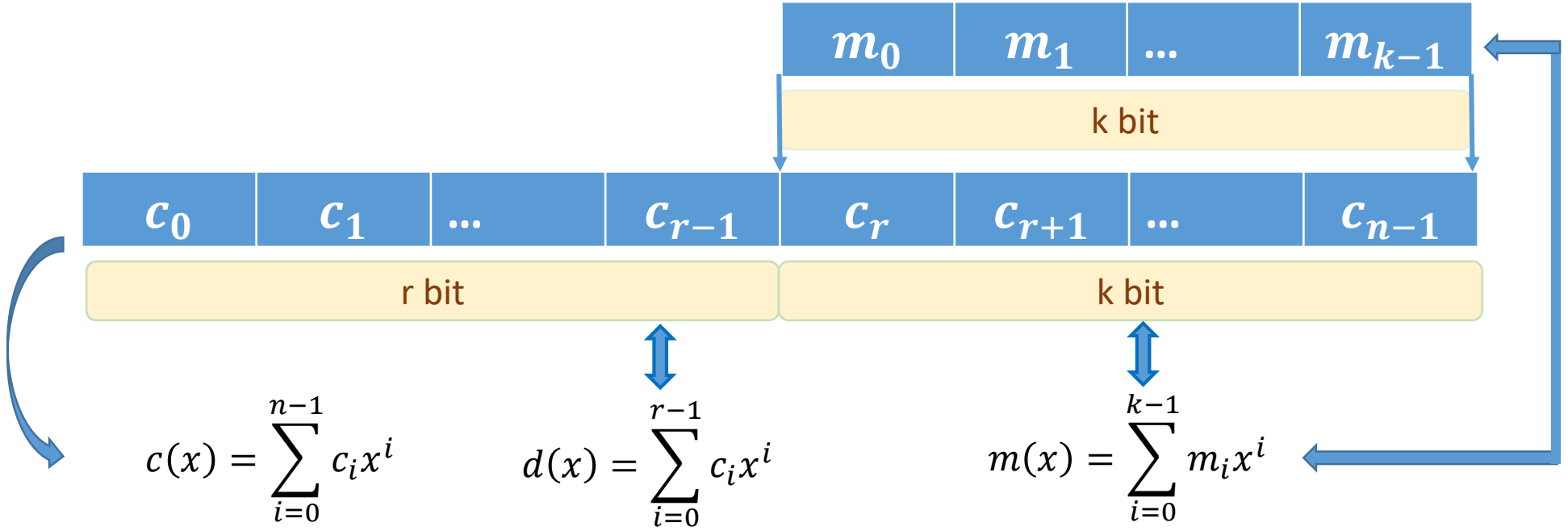
- $(x^n + 1)^2 = x^{2n} + 1$
- $x^n + 1 = (x + 1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$

3.

MÃ HÓA CHO MÃ CYCLIC BẰNG PHƯƠNG PHÁP CHIA

Tạo từ mã cyclic hệ thống

- Cho mã cyclic hệ thống (n,k) với đa thức sinh g(x). Với bản tin đầu vào m(x), hãy xác định từ mã cyclic hệ thống tương ứng c(x).



$$c(x) = m(x).x^r + d(x)$$

Tạo từ mã cyclic hệ thống

- Vì c(x) là từ mã cyclic nên $c(x) \vdots g(x)$.
- $\deg m(x) \leq k-1; \deg g(x) = r; \deg d(x) \leq r-1$

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

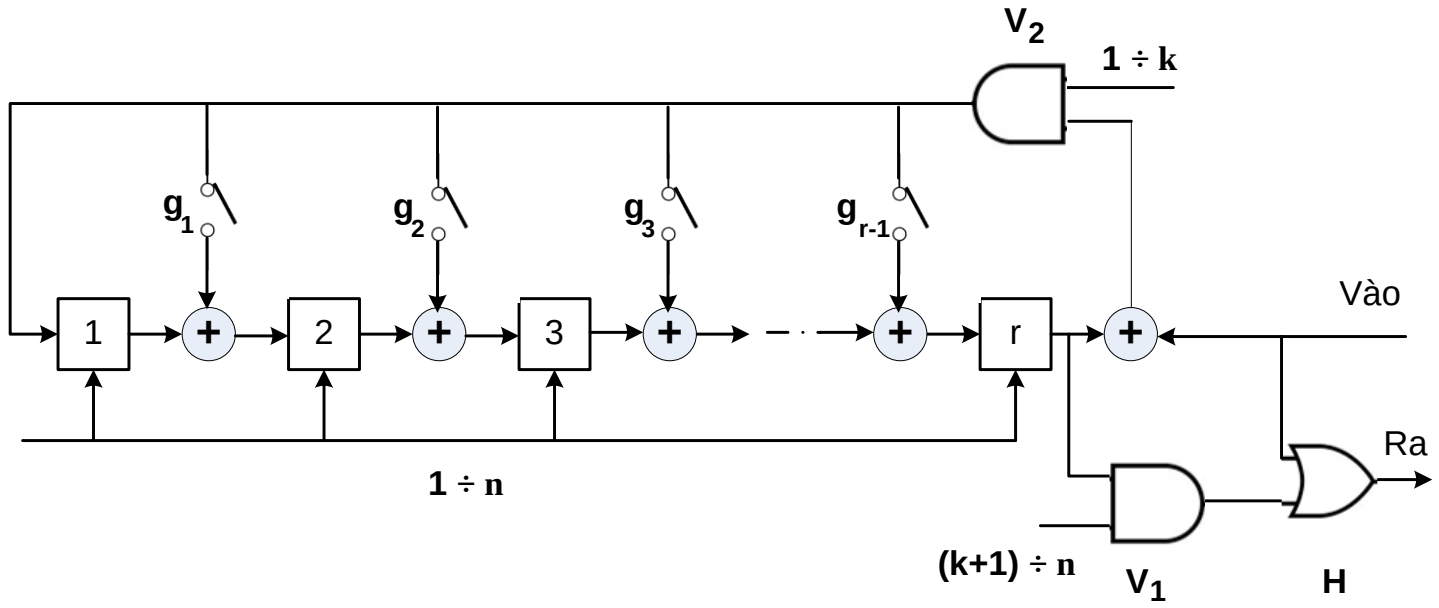
- Do $c(x) \vdots g(x)$ nên $(r(x) + d(x)) \vdots g(x)$.
- Suy ra: $r(x) + d(x) = 0$ hay $r(x) = d(x)$

Thuật toán mã hóa hệ thống

- Bước 1: Mô tả bản tin m dưới dạng đa thức $m(x)$.
- Bước 2: Nâng bậc $m(x)$ hay $m(x).x^{n-k}$
- Bước 3: Tính $r(x) = m(x).x^{n-k} mod\ g(x)$
- Bước 4: Xây dựng từ mã $c(x) = m(x).x^{n-k} + r(x)$

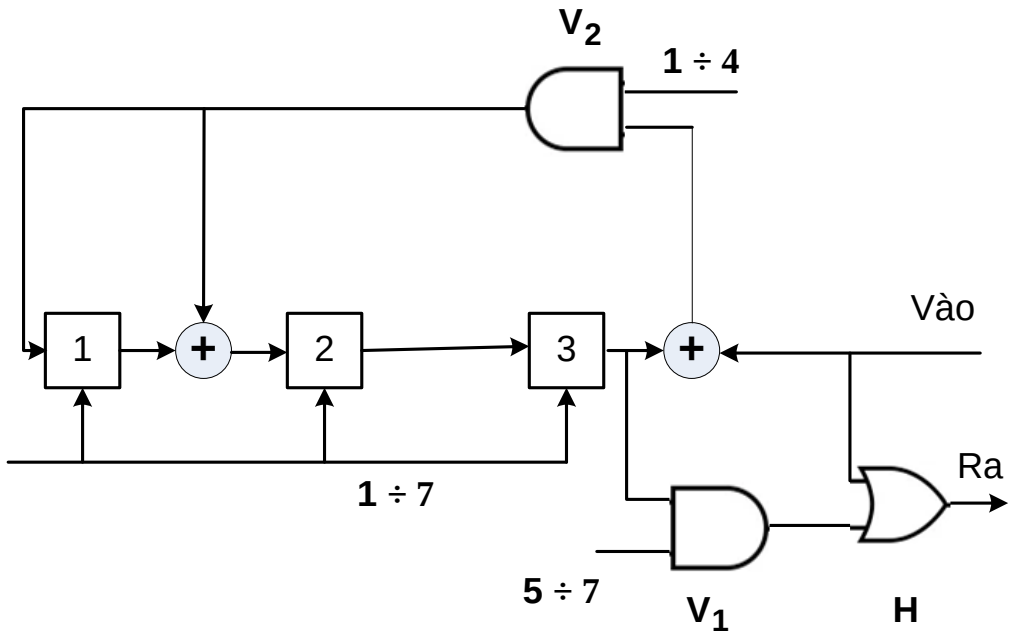
- Ví dụ 5.12:
- Cho mã cyclic (7,4) có $g(x) = 1 + x + x^3$.
- Tìm từ mã tương ứng với bản tin đầu vào $m = 1011$

Sơ đồ thiết bị mã hóa



Ví dụ 5.13

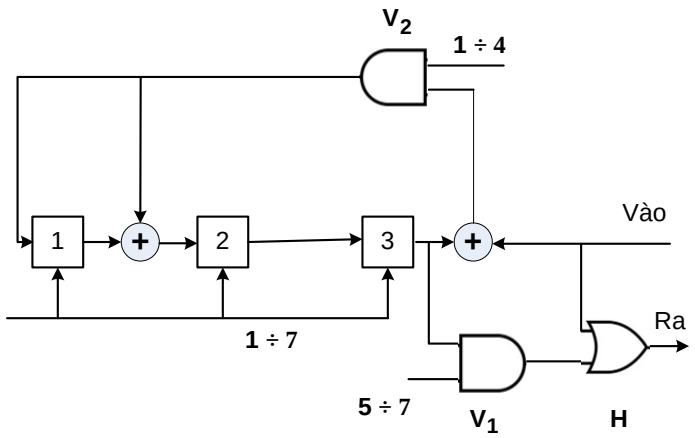
- Cho mã cyclic (7,4) có $g(x) = 1 + x + x^3$.
- (a) Vẽ sơ đồ mã hóa cho mã cyclic này theo phương pháp chia.
- (b) Dựa vào sơ đồ, tìm từ mã tương ứng với bản tin đầu vào $m = 1011$
- (c) Kiểm tra lại kết quả bằng thuật toán mã hóa.



Ví dụ 5.13

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

$$m(x) = 1 + x^2 + x^3$$



$$c(x) = 1 + x^3 + x^5 + x^6$$

- Cho mã cyclic (7,3) có đa thức sinh $g(x) = 1 + x + x^2 + x^4$. Hãy mô tả sơ đồ chức năng của thiết bị mã hoá hệ thống cho bộ mã này theo phương pháp chia (nhân). Giả sử đa thức thông tin $m(x) = x + x^2$. Hãy tìm từ mã ở đầu ra của thiết bị và kiểm tra lại bằng thuật toán tạo từ mã hệ thống theo phương pháp chia (nhân).