Lý thuyết thông tin

ptit.edu.vn

Phần 4
Cyclic coding

- Cơ sở toán học
- Mã hóa
- Giải mã

dinhnq@ptit.edu.vn

Vành đa thức $Z_2[x]/x^n+1$

Tập các đa thức $f(x)=\sum_{i=0}^{n-1} f_i x^i \qquad f_i \in GF(2)$

với hai phép toán: cộng và nhân đa thức theo modulo X^n+1

tạo nên một vành đa thức, ký hiệu vành này là $Z_2[x]/x^n+1$

Cộng và nhân đa thức theo modulo X^n+1 như thế nào?

Xét hai đa thức thuộc vành: $a(x)=\sum_{i=0}^{n-1} a_i x^i \quad b(x)=\sum_{i=0}^{n-1} b_i x^i$

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

with a_i+b_i is add in GF(2)

Nếu ta coi mỗi đa thức f(x) là một véctơ trong không gian tuyến tính V_n

$$f(x)=f_0+f_1x+....+f_{n-1}x^{n-1} \leftrightarrow f=(f_0\,f_1.....f_{n-1})$$

thì phép cộng đa thức hoàn toàn tương tự như phép cộng véctơ.

Vành đa thức $Z_2[x]/x^n+1$ (tt)

Phép nhân đa thức

Phép nhân 2 đa thức được thực hiện theo mod X^n+1 (tức là coi $X^n=1 (=x^0)$).

(Để đảm bảo c(X) vẫn là một đa thức có bậc $\leq n-1$ thuộc R)

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

Chú ý: Tích của hai đa thức được thực hiện trên cơ sở tích của hai đơn thức $a_i x^i$ và $b_j x^j$ theo nguyên tắc:

- $x^i.x^j = x^{(i+j) \bmod n}$
- $a_i\, b_j$ là phép nhân mod trên trường F

Phép dịch vòng trên vành đa thức $Z_2[x]/x^n+1$

Xét đa thức thuộc vành: $a(X)=\sum_{i=0}^{n-1} a_i x^i \leftrightarrow a=(a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1})$

Khi đó: $b(X)=x.a(X)=x.\left(\sum_{i=0}^{n-1} a_i x^i\right) \leftrightarrow b=(a_{n-1},\ a_0,\ a_1,\ \ldots,\ a_{n-2})$

Tổng quát: $c(X)=x^j.a(X)=x^j.\left(\sum_{i=0}^{n-1} a_i x^i\right) \leftrightarrow c=(a_{n-j},\ a_{n-j+1},\ \ldots,\ a_{n-j-1})$

Hệ quả: $d(X)=\frac{a(X)}{x}=x^{-1}a(X)=\frac{x^n a(X)}{x}=x^{n-1}a(X)$

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. Như vậy đa thức này không thể phân tích thành tích các đa thức có bậc nhỏ hơn.

Chú ý 1: Một số đa thức bất khả quy

Bậc 1: $1+x$

Bậc 2: $1+x+x^2$

Bậc 3: $1+x+x^3$; $1+x^2+x^3$

Bậc 4: $1+x+x^4$; $1+x^3+x^4$; $1+x+x^2+x^3+x^4$;

Chú ý 2:

- Trọng số của đa thức = trọng số của vector biểu diễn đa thức đó.
- Đa thức bất khả quy (ngoại trừ 1+x) là đa thức có trọng số lẻ và có số hạng tự do bằng 1, (tức nó chứa một số lẻ các đơn thức).

Phân tích của nhị thức x^n+1

Định lý: Nếu $2^m-1=n$, thì 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.

Xét x^7+1: m = 3, n = 7: Trong số 8 đa thức bậc 3 chỉ có 2 đa thức sau là các đa thức bất khả quy, đó là x^3+x+1 và x^3+x^2+1. Như vậy:

$$X^7+1=(1+x)(1+x+x^3)(1+x^2+x^3)$$

Câu hỏi:

Chứng minh rằng: $(x^n+1)\vdots(x+1) \quad \forall n\geq 1$

Ideal của Vành đa thức $Z_2[x]/x^n+1$

Định nghĩa: Ideal I của vành đa thức $Z_2[x]/X^n+1$ gồm tập các đa thức là bội của một đa thức $g(X)=\sum_{i=0}^{r} g_i x^i$ thỏa mãn:

- $g(X) \mid X^n+1$ (tức $g(X)$ là ước của X^n+1)
- Với $\forall a(X) \in I, a(X) \neq 0$ ta có: $\deg g(X) = r = \min \deg a(X)$

Ký hiệu Ideal của vành đa thức là $I=\langle g(X) \rangle$

Mã Cyclic

Một mã cyclic (n,k) sinh bởi $g(x) = g_0 + g_1 x + \ ... \ + g_r x^r$

chính là một ideal I=<g(x)> của $Z_2[x] / x^n + 1$

g(x): generator polynomial, order r=n-k

Câu hỏi:

Điều kiện để g(x) là đa thức sinh của mã cyclic (n,k)?

- Ở dạng general, đa thức mã của một bộ mã Cyclic(n,k) là tích của đa thức sinh g(x) với đa thức thông tin a(x)

Số mã cyclic trên vành đa thức $Z_2[x]/x^n+1$

- Để tìm được tất cả các mã trong vành $Z_2[x]/X^n+1$

  ta phải thực hiện phân tích nhị thức X^n+1

  thành tích của các đa thức bất khả quy

  Gọi số các đa thức bất khả quy trong phân tích của X^n+1 là a, khi đó số các Ideal (tức số bộ mã) trong vành được xác định theo biểu thức: $|I| = 2^a - 1$.

Ví dụ: Xét vành $Z_2[x]/X^7+1$:

	g(x)	C(n, k)	d_0	Note
1	1	(7, 7)	1	no parity code
2	1 + x	(7, 6)	2	Single parity-check code
3	$1+x+x^3$	(7, 4)	3	Hamming code
4	$1+x^2+x^3$	(7, 4)	3	Hamming code
5	$1+x+x^2+x^4$	(7, 3)	4	
6	$1+x^2+x^3+x^4$	(7, 3)	4	
7	$1+x+x^2+x^3+x^4+x^5+x^6$	(7, 1)	7	repetition code

Generator matrix / parity-check matrix

- Ở dạng general, mã cyclic (n,k) sinh bởi g(x) có:

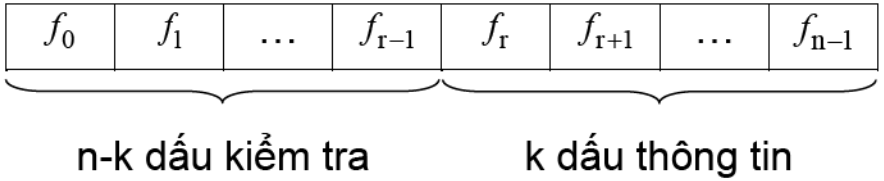
$$G = \begin{pmatrix} g(x) \\ x.g(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix} \qquad H = \begin{pmatrix} h^*(X) \\ x.h^*(X) \\ \dots \\ x^{r-1}.h^*(X) \end{pmatrix}$$

Trong đó đa thức kiểm tra: $h(x) = \dfrac{x^n + 1}{g(x)}$

Đa thức đối ngẫu (reciprocal) của h(x): $h^*(x) = x^{\deg h(x)} h(x^{-1})$

Linear Systematic (n,k) code :

- Từ mã dạng hệ thống



- Mã dạng hệ thống sử dụng G và H dạng hệ thống:
  - $G_{sys} = [\, P_{k.r} : I_{k.k} \,]$
  - $H_{sys} = [\, I_{r.r} : P_{r.k}^{T} \,]$

Mã hóa cyclic hệ thống theo phương pháp chia

Thuật toán tạo từ mã hệ thống

VÀO: C(n,k), g(x)

Message $a = (a_0, a_1, ..., a_{k-1})$ $\quad a \in A$

RA: Codeword dạng hệ thống

BƯỚC 1: Mô tả message a thành đa thức thông tin

$$a(x) = a_0 + a_1 x + ... + a_{k-1} x^{k-1} \qquad \deg a(x) \le k-1$$

BƯỚC 2: Nâng bậc a(x) để dịch chuyển lên vùng bit cao

$$[x^{n-k} a(x)] = a_0 x^{n-k} + a_1 x^{n-k+1} + ... + a_{k-1} x^{n-1}$$

BƯỚC 3: Tính $\quad r(x) = [x^{n-k} a(x)] \bmod g(x) = r_0 + r_1 x + ... + r_{n-k-1} x^{n-k-1}$

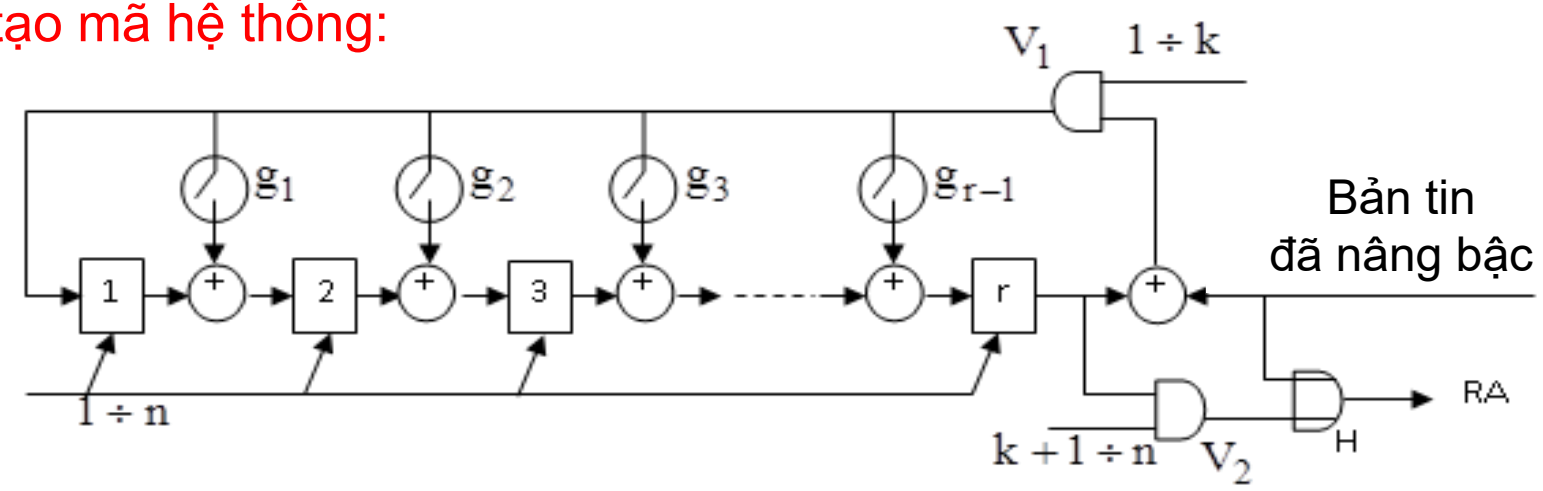
BƯỚC 4: Xác lập đa thức mã ra $\quad f(x) = r(x) + x^{n-k} a(x)$

$$= \underbrace{r_0 + r_1 x + ... + r_{n-k-1} x^{n-k-1}}_{r(x)} + \underbrace{a_0 x^{n-k} + a_1 x^{n-k+1} + ... + a_{k-1} x^{n-1}}_{x^{n-k} a(x)}$$

tương ứng với codeword $\quad f = (\underbrace{f_0, f_1, ..., f_{n-k-1}}, \underbrace{f_{n-k}, ..., f_{n-1}})$

Mã hóa cyclic hệ thống theo phương pháp chia (tt)

-Bộ tạo mã hệ thống:



Mã hóa cyclic hệ thống theo phương pháp nhân

Thuật toán tạo từ mã hệ thống

VÀO: C(n,k), g(x)

Message $a \in A$ (có 2^k message), $a = (a_0, a_1, ..., a_{k-1})$

RA: Codeword dạng hệ thống $f = (\underbrace{f_0, f_1, ..., f_{n-k-1}}, \underbrace{f_{n-k}, ..., f_{n-1}})$

BƯỚC 1: Tính $$h(x) = \frac{x^n + 1}{g(x)} = \sum_{j=0}^{k} h_j x^j$$

BƯỚC 2: Lập công thức các dấu mã vùng bit cao

$$f_{n-k} = a_0 \ , f_{n-k+1} = a_1 \ , \quad ..... \ , \ f_{n-1} = a_{k-1}$$

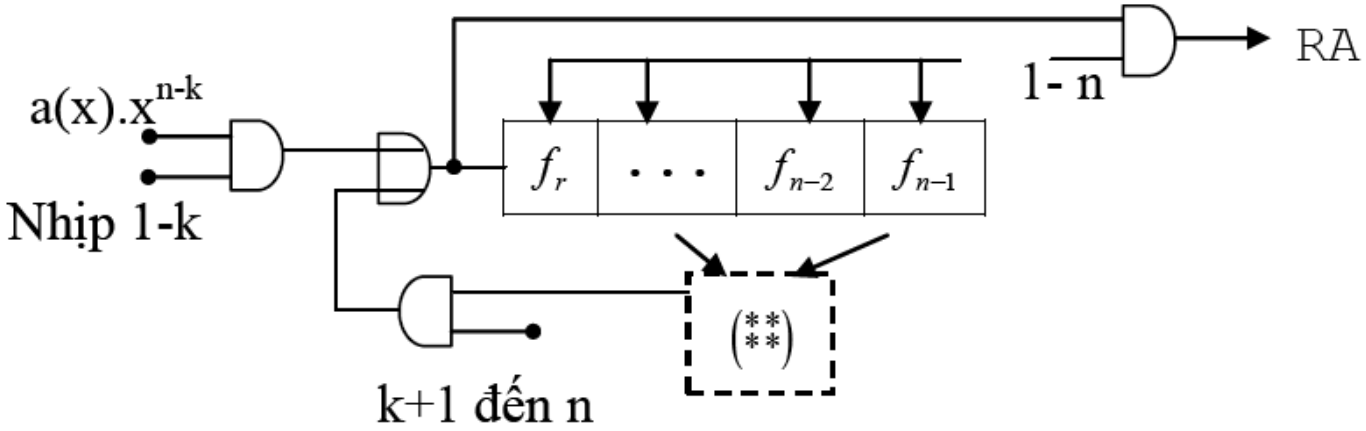
BƯỚC 3: Lập công thức các dấu mã vùng bit thấp

$$f_{n-k-i} = \sum_{j=0}^{k-1} h_j f_{n-i-j} \qquad 1 \le \mathrm{i} \le \mathrm{n} - \mathrm{k}$$

BƯỚC 4: Xác lập giá trị codeword theo bản tin vào

Mã hóa cyclic hệ thống theo phương pháp nhân (…)

-Bộ tạo mã hệ thống:



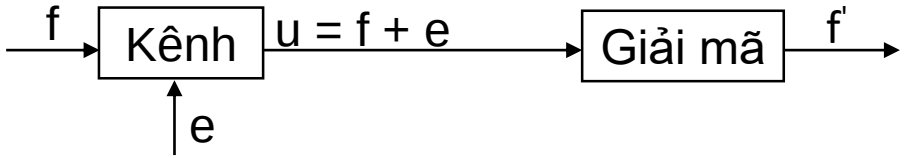
$$f_{n-k-i} = \sum_{j=0}^{k-1} h_j f_{n-i-j}$$

Giải mã ngưỡng

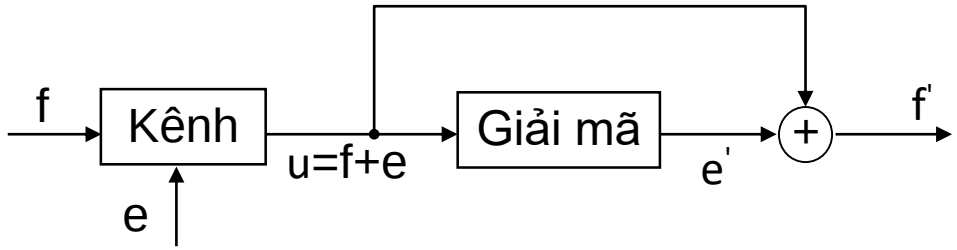
a. Thủ tục giải mã

Mọi phương pháp giải mã đều có thể tiến hành theo một trong hai thủ tục giải mã sau:

-Thủ tục 1: Dẫn ra từ mã gốc f từ vector u.



-Thủ tục 2: Dẫn ra véctơ sai e từ u.



$$u + e' = [f + e] + e' = f + [e + e']$$

$$\text{if } \; e = e' \; \text{ then } \; e + e' = 0, \Rightarrow f' = f$$

Giải mã ngưỡng (…)

b. Syndrom của vector mã nhận được

Gọi vector tới đầu vào máy thu là: $u = (u_0 u_1 ... u_{n-1})$

Syndrom của u: $S(u) = u.H^T$

Khai triển: $S(u) = (f + e)H^T = eH^T = S(e)$

Vậy S(u) đặc trưng cho cấu trúc lỗi trong vector u

-Quá trình giải mã dựa trên việc phân tích trạng thái của $S(u)$ được gọi là giải mã theo syndrom (hội chứng).

- Hiển nhiên là khi không có sai $(e \equiv 0)$ ta có: $S(u) = S(e) = 0$
- Khi có sai: $S(u) = S(e) \neq 0$

Giải mã ngưỡng (…)

Các tổng kiểm tra trong S(u)

$$S(u) = u.H^T = (s_0 \quad s_1 \quad .... \quad s_{n-k-1})$$

-Mỗi thành phần của S(u) sẽ mô tả một mối quan hệ nào đó giữa các dấu mã, và được gọi là một tổng kiểm tra.

Tập r tổng kiểm tra trong $S(u)$ tạo nên hệ tổng kiểm tra. Mỗi tổng kiểm tra trong hệ sẽ chứa một thông tin nhất định về dấu cần giải mã u_i, thông tin đó có thể nhiều, ít hoặc bằng không. Ngoài ra mỗi tổng kiểm tra này còn chứa thông tin về các dấu mã u_j khác.

Giải mã ngưỡng (…)

c. Hệ tổng kiểm tra trực giao

Để dễ giải cho u_i hiển nhiên rằng ta cần xây dựng một hệ tổng kiểm tra chứa nhiều thông tin nhất về u_i. Trên cơ sở đó ta đưa ra khái niệm hệ tổng kiểm tra trực giao sau:

Định nghĩa: Hệ J tổng kiểm tra được gọi là trực giao với dấu mã u_i nếu:

- Mỗi tổng kiểm tra trong hệ đều chứa u_i.
- Dấu mã $u_j\ (j \neq i)$ chỉ nằm tối đa trong một tổng kiểm tra

Giải mã ngưỡng (…)

d. Thủ tục giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao

B1: Tính H

B2: Tính syndrom theo công thức $S(u)=u.H^T$

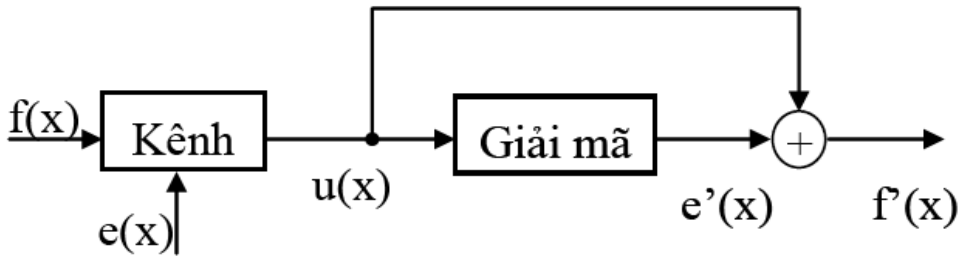
B3: Lập hệ J tổng kiểm tra trực giao với dấu mã u_i , kiểm tra $J=d_0-1$

B4: Lập sơ đồ bộ giải mã theo đa số

B5: Lập bảng hoạt động giải mã vector u thành từ mã f

B6: Kiểm tra f có phải là từ mã hợp lệ ?

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



$$h(X) = \frac{x^7 + 1}{g(X)} = x^3 + x + 1, \qquad h^*(X) = 1 + x^2 + x^3$$

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

Từ mã nhận được: $u=(u_0u_1u_2u_3u_4u_5u_6)$

Tính syndrom: $uH^T = S(u) = (s_0 s_1 s_2 s_3)$

$$= (u_0 u_1 \ldots . u_6) \begin{pmatrix} 1000 \\ 0100 \\ 1010 \\ 1101 \\ 0110 \\ 0011 \\ 0001 \end{pmatrix}$$

Hệ 4 tổng kiểm tra:

$s_0 = u0 + u2 + u3$

$s_1 = u1 + u3 + u4$

$s_2 = u2 + u4 + u5$

$s_3 = u3 + u5 + u6$

Hệ tổng kiểm tra trực giao với dấu mã u_3

$s_0 = u0 + u2 + u3$

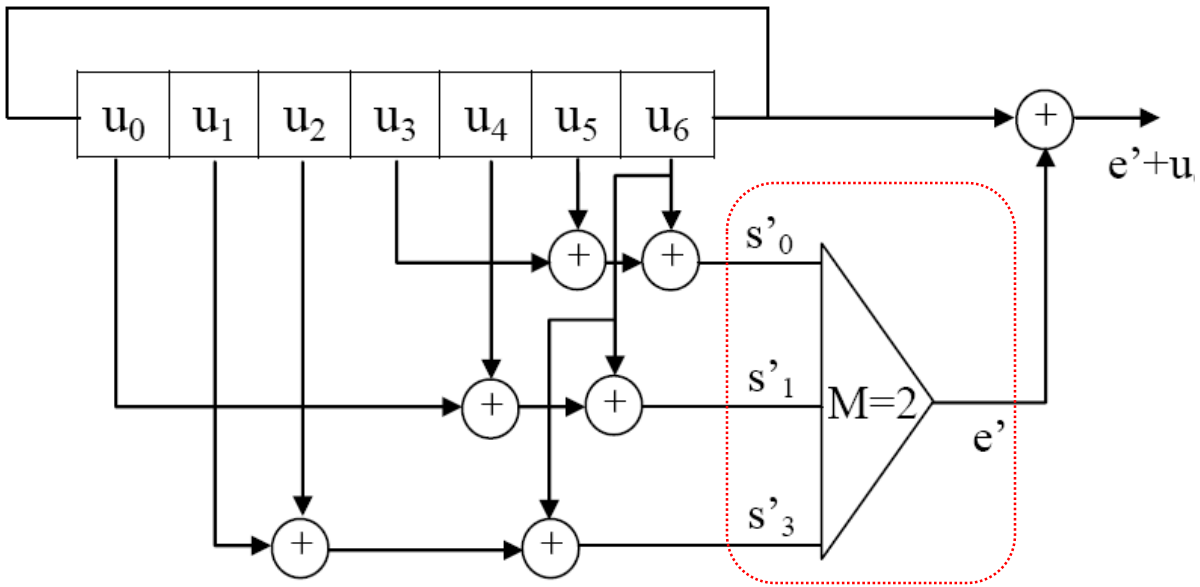
$s_1 = u1 + u3 + u4$

$s_3 = u3 + u5 + u6$

Do $J = d_0 - 1$, nên ta có thể sửa được sai bởi phương pháp giải mã đa số.

Do tính chất dịch vòng, nên để thuận tiện cho dãy bít ra theo trật tự, ta có thể dịch vòng hệ tổng kiểm tra trên đi 3 vị trí sang phải). Hệ tổng kiểm tra trực giao với dấu mã u_6

$$\begin{aligned} s_0 &= u0 + u2 + u3 \\ s_1 &= u1 + u3 + u4 \\ s_3 &= u3 + u5 + u6 \end{aligned} \quad \Rightarrow \quad \begin{cases} s'_0 = u6 + u3 + u5 \\ s'_1 = u6 + u0 + u4 \\ s'_3 = u6 + u1 + u2 \end{cases}$$



Quá trình giải mã từ mã u nhận được có dạng: 0 0 1 1 1 1 1

(Hay $u(x) = x^6 + x^5 + x^4 + x^3 + x^2$)

Nhịp	Trạng thái các ô nhớ							s'_0	s'_1	s'_2	e'	Ra	Dấu mã ra
	u_0	u_1	u_2	u_3	u_4	u_5	u_6						
7	0	0	1	1	1	1	1						
8	1	0	0	1	1	1	1	1	0	0	0	1	f'6
9	1	1	0	0	1	1	1	1	1	1	1	0	f'5
10	1	1	1	0	0	1	1	0	1	0	0	1	f'4
11	1	1	1	1	0	0	1	0	0	1	0	1	f'3
12	1	1	1	1	1	0	0	0	0	1	0	1	f'2
13	0	1	1	1	1	1	0	1	0	0	0	0	f'1
14	0	0	1	1	1	1	1	0	1	0	0	0	f'0

u =0 0 1 1 1 1 1

e'=0 0 0 0 0 1 0

0 0 1 1 1 0 1

Sai ở vị trí x^5 đã được sửa

Từ mã đã giải mã $\hat{f}(x) = x^6 + x^4 + x^3 + x^2$

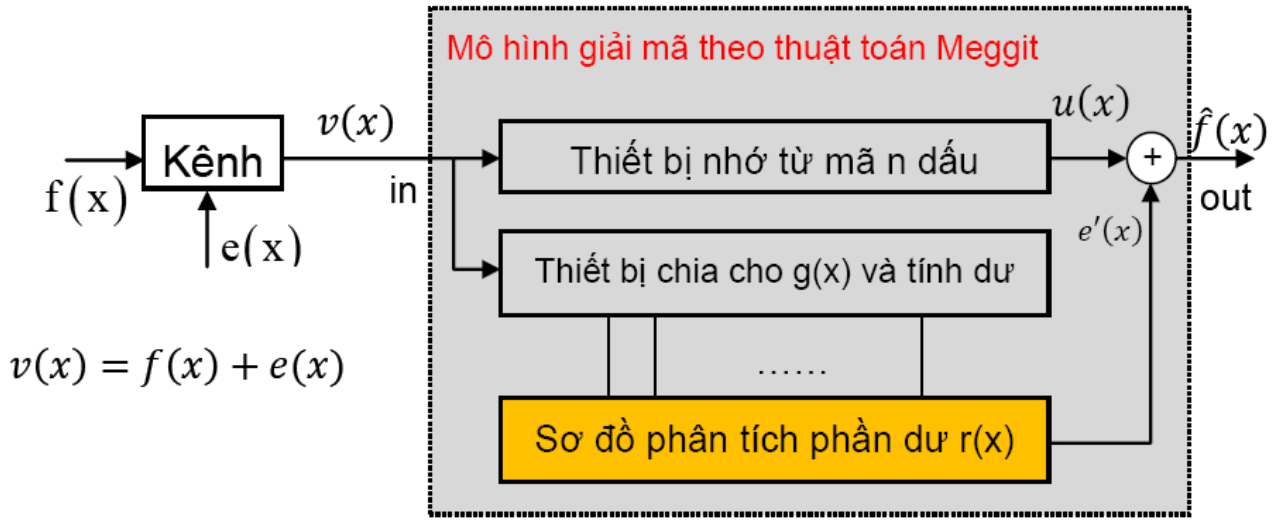
-Kiểm tra lại:

$$\begin{array}{l|l} x^6 + x^4 + x^3 + x^2 & x^4 + x^2 + x + 1 \\ \underline{x^6 + x^4 + x^3 + x^2} & x^2 \\ 0 & \end{array}$$

Lưu ý rằng d_0=4, nên chỉ sửa được một lỗi.

Giải mã theo thuật toán Meggitt

Giả sử $f(x)$ là một từ mã của một bộ mã xyclic $V_{-}(n,k)$ có đa thức sinh g(x)



Do $f(x) \vdots g(X)$. khi đó phép chia: $\frac{v(x)}{g(x)} = \frac{f(x)}{g(x)} + \frac{e(x)}{g(x)}$ → Phần dư r(x)

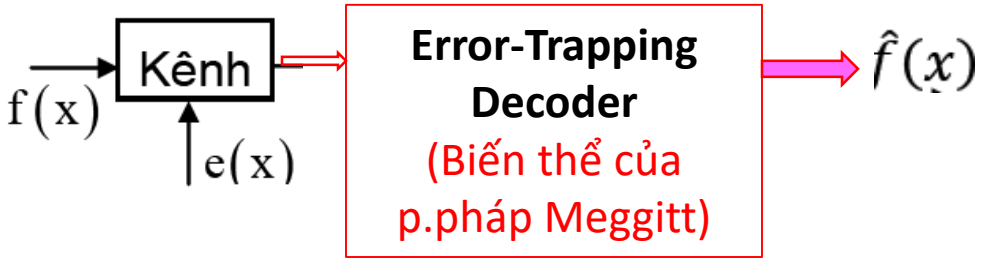
Chú ý: do g(x) có bậc r, nên r(x) có bậc ≤r-1

Phần dư r(x) đặc trưng cho e(x)

Bằng cách phân tích r(x) ta có thể tìm được $e(x)$. Sơ đồ phân tích r(x) là một sơ đồ logic tổng hợp, đây là một thành phần quan trọng trong sơ đồ giải mã theo thuật toán Meggit.

Error trapping decoding

- Phương pháp Meggitt thực tế có mạch giải mã khá phức tạp. Nếu giới hạn lại một số điều kiện thì có thể cho ra một biến thể giải mã đơn giản.



Nếu có thể dịch vòng (bẫy) lỗi về chỉ nằm trong vùng n-k dấu mã đầu tiên, khi đó có thể xác định e(x).

- **Dấu hiệu lỗi bị bẫy thành công:** là ngay khi $w\big(r(x)\big) \leq t$.

Thuật toán chia dịch vòng (Error trapping decoding)

Thuật toán (dịch phải)

VÀO: - Từ mã nhận được v(x)

- Mã $V_{-}(n,k)$ có g(x), có d_0.

RA: - Từ mã $\hat{f}(X)$

For $i := 0$ to $(n-1)$ do

(1) Chia $v(x).x^i$ cho g(x) để tìm phần dư $r_i(x)$.

(2) Tính $w(r_i(x))$.

- Nếu $w(r_i(x)) \le t = \left[\frac{d_0 - 1}{2}\right]$ thì $\hat{f}(x) = \frac{v(x).x^i + r_i(x)}{x^i}$ và stop.

- Nếu $w(r_i(x)) > t \Rightarrow i := i+1$. Nếu $i+1 = n$ thì thông báo "không sửa được sai (Số sai vượt quá khả năng sửa sai của bộ mã)" và stop.

Note: Có thể giải theo cách dịch trái (chia v(x) cho x^i).

Giải mã theo thuật toán chia dịch vòng (…)

Thí dụ: mã xyclic (7, 3, 4) với đa thức sinh $g(x) = 1 + x + x^2 + x^4$

Giả sử từ mã nhận được $v(x) = x + x^2 + x^3 + x^5 + x^6 \leftrightarrow 0111011$

Ta sử dụng thuật toán chia dịch vòng để tìm lại từ mã đã phát:

i = 0

(1) Chia $v(x).x^0$ cho $g(x)$ để tìm phần dư $r_0(x)$.

$$
\begin{array}{l|l}
x^6 + x^5 + x^3 + x^2 + x & \underline{x^4 + x^2 + x + 1} \\
\underline{x^6 + x^4 + x^3 + x^2} & x^2 + x + 1 \\
x^5 + x^4 + x & \\
\underline{x^5 + x^3 + x^2 + x} & \\
x^4 + x^3 + x^2 & \\
\underline{x^4 + x^2 + x + 1} & \\
r_0(x) = x^3 + x + 1 &
\end{array}
$$

(2) $w(r_0(x)) = 3 > \left[\frac{4-1}{2}\right] = 1$ Không thỏa mãn điều kiện

i = 1:

(1) Chia $x.v(x)$ cho $g(x)$ để tìm phần dư $r_1(x)$.

$$\begin{array}{l|l} x^6+x^4+x^3+x^2+1 & \underline{x^4+x^2+x+1} \\ \underline{x^6+x^4+x^3+x^2} & x^2 \\ r_1(x)=1 & \end{array}$$

(2) $w(r_1(x))=1=t$

Từ mã ra: $\hat{f}(X)=\dfrac{x.v(x)+r_1(x)}{x}=x^5+x^3+x^2+x$

Vậy sai ở vị trí x^6 đã được sửa $v=0111011\rightarrow f=0111010$

Giải theo cách dịch trái cũng sẽ cho cùng kết quả.

Tài liệu tham khảo

- ✓ John Proakis & Masoud Salehi, **Digital Communication,** 2007
- ✓ Shu Lin, **Error Control Coding-Fundamentals and Aplications**, Prentice Hall, 2004
- ✓ Simon Haykin, **Communication Systems**, 4rd edition, John Wiley & Sons, 2001.

dinhnq@ptit.edu.vn