Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Lý thuyết thông tin

Biên soạn: Phạm Văn Sự

Bộ môn Xử lý tín hiệu và Truyền thông
Khoa Kỹ thuật Điện tử I
Học viện Công nghệ Bưu chính Viễn thông

10/09/2011

Đa thức mã và các phép biến đổi

Phép cộng đa thức, Phép nhân đa thức

- Xét các đa thức $f(x)$, $g(x)$ trên $GF(q)[x]/(x^l-1)$

Phép cộng đa thức

$f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_{l-1}x^{l-1}$
$g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{l-1}x^{l-1}$
$\Rightarrow f(x) + g(x) = (f_0 + g_0) + (f_1 + g_1)x + \cdots + (f_{l-1} + g_{l-1})x^{l-1}$

Phép nhân đa thức

$f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_{l-1}x^{l-1} = \sum_{i=0}^{l-1} f_ix^i$
$g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{l-1}x^{l-1} = \sum_{j=0}^{l-1} g_jx^j$
$\Rightarrow f(x) \times g(x) = (\sum_{i=0}^{l-1} f_ix^i)(\sum_{j=0}^{l-1} g_jx^j)$ modulo (x^l-1)

Đa thức mã và các phép biến đổi

Đa thức mã

Véc-tơ mã $\mathbf{c} = (c_0, c_1, \ldots, c_{l-1})$ có thể biểu diễn ở dạng đa thức:

$$c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{l-1}x^{l-1}$$

Nhận xét:

- Mỗi véc-tơ mã/từ mã có chiều dài l tương ứng với một đa thức bậc nhỏ hơn hoặc bằng $l-1$.
- Mối quan hệ giữa véc-tơ mã với biểu diễn đa thức đảm bảo $1-1$.
- $c(x)$ gọi là đa thức mã. Khái niệm từ mã/véc-tơ mã và đa thức mã có thể được dùng thay thế nhau.
  - $\mathbf{c} \in \mathfrak{C}(l,k) \Leftrightarrow c(x) \in GF(q)[x]/(x^l-1)$

Đa thức mã và các phép biến đổi

Phép dịch vòng

Trên $GF(q)[x]/(x^l-1)$, cho $f(x) = \sum_{i=0}^{l-1} f_ix^i \longleftrightarrow \mathbf{a} = (f_0, f_1, \ldots, f_{l-1})$

Xét $g(x) = x.f(x) \longleftrightarrow \mathbf{b} = (f_{l-1}, f_0, f_1, \ldots, f_{l-2})$ (chú ý: mod x^l-1)

- $\mathbf{b}$ thu được bằng cách dịch vòng về phía phải của $\mathbf{a}$ một cấp/nhịp/vòng.
- Kí hiệu $g(x) = f^{(1)}(x)$.
- $\Rightarrow$ Nhân x^i với $f(x)$ thu được một véc-tơ là kết quả dịch vòng phải của véc-tơ ban đầu đi i nhịp/cấp: $f^{(i)}(x)$.

Xét $g(x) = \frac{f(x)}{x} \longleftrightarrow \mathbf{b} = (f_1, f_2, f_3, \ldots, f_{l-1}, f_0)$ (chú ý: mod x^l-1)

- $\mathbf{b}$ thu được bằng cách dịch vòng về phía trái của $\mathbf{a}$ một cấp/vòng.
- $\Rightarrow$ Chia $f(x)$ cho x^i thu được một véc-tơ là kết quả dịch vòng trái của véc-tơ ban đầu đi i nhịp/cấp.

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Một số tính chất

Định lý

Bộ mã $\mathfrak{C}$ là một bộ mã vòng tuyến tính cơ số q có chiều dài từ mã l nếu và chỉ nếu các đa thức mã của $\mathfrak{C}$ tạo thành một ideal trên $GF(q)[x]/(x^l-1)$.

- Trong tập tất cả các đa thức mã của $\mathfrak{C}$, có một đa thức monic duy nhất $g(x)$ với bậc tối thiểu $r = l-k < l$. $g(x)$ được gọi là đa thức sinh của bộ mã $\mathfrak{C}$.
- Mọi đa thức mã $c(x) \in \mathfrak{C}$ tồn tại duy nhất một biểu diễn $c(x) = a(x)g(x)$, trong đó $g(x)$ là đa thức sinh, $a(x)$ là đa thức bậc $\leq l-r = k$ trên $GF(q)[x]$.
- Đa thức sinh $g(x)$ của bộ mã $\mathfrak{C}$ là một thừa số của x^l-1 trên $GF(q)[x]$.

Định lý

Nếu $g(x)$ có bậc $r = l-k$ và là một thừa số của x^l-1 thì $g(x)$ là một đa thức sinh của mã vòng tuyến tính $\mathfrak{C}(l,k)$.

Đa thức mã và các phép biến đổi

Đa thức đối ngẫu

Định nghĩa

Cho đa thức $f(x)$ bậc k: $f(x) = f_0 + f_1x + f_2x^2 + \cdots + f_kx^k$.
Đa thức đối ngẫu của $f(x)$, kí hiệu là $f^*(x)$ được định nghĩa là:

$$f^*(x) = x^k \times f(x^{-1}) = f_k + f_{k-1}x + f_{k-2}x^2 + \cdots + f_1x^{k-1} + f_0x^k$$

- Nếu $f^*(x) = f(x)$ thì $f(x)$ là đa thức tự đối ngẫu.

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Ma trận sinh của mã vòng

Một bộ mã vòng tuyến tính $\mathfrak{C}(l,k)$ với đa thức sinh $g(x) = g_0 + g_1x + g_2x^2 + \cdots + g_{l-k}x^{l-k}$ có ma trận sinh xác định bởi:

$$\mathbf{G} = \begin{bmatrix} g(x) \\ xg(x) \\ x^2g(x) \\ \vdots \\ x^{l-k}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{l-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{l-k-1} & g_{l-k} & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{l-k-2} & g_{l-k-1} & g_{l-k} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & g_{l-k} \end{bmatrix}$$

- $\mathbf{G}$ có kích thước $k \times l$
- $\mathbf{G}$ không có dạng hệ thống

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Định nghĩa

Định nghĩa

Một mã khối tuyến tính $\mathfrak{C}(l,k)$ được gọi là mã vòng nếu với mọi từ mã $\mathbf{c} = (c_0, c_1, \ldots, c_{l-1}) \in \mathfrak{C}$ thì kết quả của mỗi dịch vòng từ mã $\mathbf{c}$ cũng sẽ thu được một véc-tơ cũng là một từ mã thuộc $\mathfrak{C}$.

Cho $a(x) \in GF(q)[x]/(x^l-1)$, $c(x) \in \mathfrak{C}$
$\Rightarrow a(x)c(x)$ là tổ hợp tuyến tính của các dịch vòng của $c(x)$
$\Rightarrow a(x)c(x) \in \mathfrak{C}\ \forall a(x) \in GF(q)[x]/(x^l-1)$, $c(x) \in \mathfrak{C}$

Định nghĩa

Mã vòng $\mathfrak{C}(l,k)$ là một ideal của vành $GF(q)[x]/(x^l-1)$

Mã vòng tuyến tính dạng hệ thống

Thuật toán chia = Thuật toán bốn bước = Thuật toán tạo từ mã dạng hệ thống từ đa thức sinh

Từ mã dạng hệ thống $\mathbf{c} = [\mathbf{p} \mid \mathbf{a}]$

Bài toán

Nhập vào: Các dấu của khối tin cần mã hóa $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1})$.
In ra: Từ mã dạng hệ thống tương ứng $\mathbf{c}$

Thuật toán

1. Mô tả khối tin bằng biểu diễn đa thức tương ứng $a(x)$.
2. Tính $x^{l-k}a(x)$.
3. Chia $x^{l-k}a(x)$ cho đa thức sinh $g(x)$ của bộ mã, thu được phần dư $p(x)$.
4. Thành lập đa thức mã $c(x) = p(x) + x^{l-k}a(x)$. In ra từ mã tương ứng với đa thức mã $c(x)$.

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Ma trận kiểm tra của mã vòng

Trên $GF(q)$, xét bộ mã vòng tuyến tính $\mathfrak{C}(l, k)$ với đa thức sinh $g(x)$. Tồn tại một đa thức $h(x)$ bậc $k = l - r$ thỏa mãn $g(x)h(x) = x^l - 1$, hay $h(x)g(x) \equiv 0 \bmod x^l - 1$. $h(x)$ được gọi là đa thức kiểm tra của mã $\mathfrak{C}(l, k)$.

Xét một bộ mã vòng tuyến tính $\mathfrak{C}(l, k)$ với đa thức kiểm tra $h(x) = h_0 + h_1x + h_2x^2 + \cdots + h_kx^k$, ma trận kiểm tra của nó được xác định bởi:

$$\mathbf{H} = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & \ldots & h_1 & h_0 & 0 & \ldots & 0 \\ 0 & 0 & h_k & \ldots & h_2 & h_1 & h_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & \ldots & h_0 \end{bmatrix}$$

- $\mathbf{H}$ có kích thước $l - k \times l$
- $\mathbf{GH}^T = 0$

Mã vòng tuyến tính dạng hệ thống

Thuật toán nhân = Thuật toán tạo từ mã dạng hệ thống từ đa thức kiểm tra

- Hoàn toàn có thể xây dựng được mã vòng tuyến tính dạng hệ thống từ đa thức (ma trận) kiểm tra.

Xây dựng mã hệ thống từ đa thức kiểm tra

1. Từ khối tin vào (tương ứng đa thức tin) ta có: $c_{l-k} = a_0$, $c_{l-k+1} = a_1$, $\ldots$, $c_{l-1} = a_{k-1}$.
2. Tính toán c_0, c_1, $\ldots$, c_{l-k-1} từ công thức:

$$c_{l-k-i} = \sum_{j=0}^{k-1} h_j c_{l-j-i} \quad (1 \le i \le l-k)$$

3. Từ mã tương ứng dạng hệ thống $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{l-1})$.

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Ma trận kiểm tra của mã vòng (cont')

Định lý

$\mathfrak{C}(l, k)$ là một mã vòng tuyến tính với đa thức sinh $g(x)$. Khi đó, mã đối ngẫu $\mathfrak{C}^\perp$ cũng là một mã vòng tuyến tính $(l, l-k)$ và được sinh ra từ đa thức sinh $h^*(x) = x^k h(x^{-1})$ với $h(x) = \frac{(x^l+1)}{g(x)}$.

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Nguyên lý hoạt động

1. Đầu tiên, nội dung các thanh ghi được xóa về 0.
2. k nhịp đầu tiên, véc-tơ tin được dịch vào thanh ghi đồng thời dịch ra đầu ra. Sau k nhịp, nội dung các thanh ghi là các bít kiểm tra.
3. $l-k$ nhịp tiếp theo, mạch thực hiện dịch nội dung các bít kiểm tra trong thanh ghi ra đầu ra.
4. Quá trình mã hóa kết thúc khi toàn bộ khối bít kiểm tra được dịch ra ngoài.

Mã vòng tuyến tính dạng hệ thống

Ma trận sinh, ma trận kiểm tra dạng hệ thống

Xây dựng ma trận sinh dạng hệ thống từ đa thức sinh

1. Thực hiện chia x^{l-k+j} $(j = 0, 1, \ldots, k-1)$ cho $g(x)$ thu được $p_j(x)$.
2. Lập đa thức $\tilde{g}(x) = p_j(x) + x^{l-k+j}$. $\tilde{g}(x)$ tương ứng với hàng thứ j của $\mathbf{G}$ có tính hệ thống.

- Nếu $\mathbf{G} = \begin{bmatrix} \mathbf{P} & | & \mathbf{I}_k \end{bmatrix} \Rightarrow \mathbf{H} = \begin{bmatrix} \mathbf{I}_{l-k} & | & \mathbf{P}^T \end{bmatrix}$
- Nếu $\mathbf{G} = \begin{bmatrix} \mathbf{I}_k & | & \mathbf{P} \end{bmatrix} \Rightarrow \mathbf{H} = \begin{bmatrix} \mathbf{P}^T & | & \mathbf{I}_{l-k} \end{bmatrix}$

Mã vòng tuyến tính dạng hệ thống

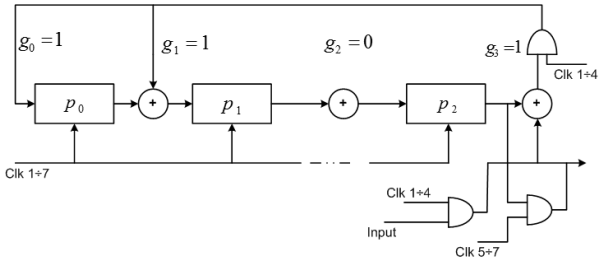
Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Minh họa (1)

Ví dụ

Xét mã vòng tuyến tính $\mathfrak{C}(7,4)$ có ma trận sinh $g(x) = 1 + x + x^3$.

- *Xây dựng mạch mã hóa tạo mã dạng hệ thống.*
- *Giả sử khối thông tin đầu vào là 0101, mô tả hoạt động của mạch và tìm kết quả từ mã thu được.*
- *Kiểm tra kết quả bằng thuật toán chia (thuật toán bốn bước)*

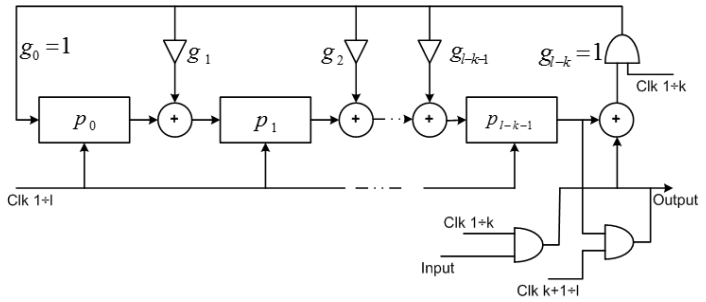
Ta có $g_0 = g_1 = g_3 = 1$, $g_2 = 0$. $\Rightarrow$ ta cần $l - k = 3$ thanh ghi dịch.



Hình: Mạch thực hiện mã hóa cho mã vòng $\mathfrak{C}(7,4)$ dạng hệ thống dựa trên đa thức sinh

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Sơ đồ mạch nguyên lý



Hình: Mạch thực hiện mã hóa mã vòng dạng tuyến tính dựa trên đa thức sinh

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Nguyên lý hoạt động

1. Đầu tiên, nội dung các thanh ghi thông tin được xóa về 0.
2. k nhịp đầu tiên, khối thông tin được dịch vào các thanh ghi đồng thời dịch ra đầu ra. Sau k nhịp, nội dung các thanh ghi là nội dung của khối tin.
3. $l-k$ nhịp tiếp theo, c_{l-k-i} $(i=1, l-k)$ được tính và được chuyển vào thanh ghi đồng thời chuyển ra đầu ra.
4. Quá trình mã hóa kết thúc sau khi $l-k$ bít kiểm tra được lập xong.

Mã vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức sinh - Minh họa (2)

Nhịp	Bít vào	Các thanh ghi			Bít ra
		p_0	p_1	p_2	
0	–	0	0	0	-
1	1	1	1	0	1
2	0	0	1	1	0
3	1	0	0	1	1
4	0	1	1	0	0
5	–	–	1	1	0
6	–	–	–	1	1
7	–	–	–	–	1

Bảng: Bảng mô tả hoạt động mạch mã hóa với khối tin vào 0101

$\Rightarrow$ Từ mã thu được là 1100101

Mạch vòng tuyến tính dạng hệ thống

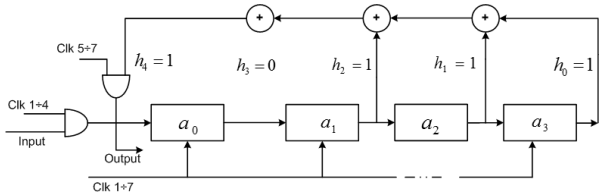
Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Minh họa (1)

Ví dụ

Xét mã vòng tuyến tính nhị phân $\mathfrak{C}(7,4)$ có ma trận sinh $g(x)=1+x+x^3$.

- *Tìm đa thức kiểm tra.*
- *Xây dựng mạch mã hóa tạo mã dạng hệ thống dựa trên đa thức kiểm tra.*
- *Giả sử khối thông tin đầu vào là 1001, mô tả hoạt động của mạch và tìm kết quả từ mã thu được.*
- *Kiểm tra kết quả bằng thuật toán nhân.*

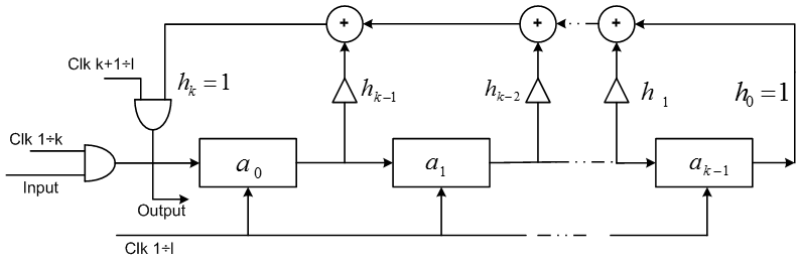
$h(x)=\frac{(x^7+1)}{g(x)}=1+x+x^2+x^4. \Rightarrow h_0=h_1=h_2=h_4=1,\ h_3=0.$



Hình: Mạch thực hiện mã hóa cho mã vòng $\mathfrak{C}(7,4)$ dạng hệ thống dựa trên đa thức kiểm

Mã vòng tuyến tính dạng hệ thống

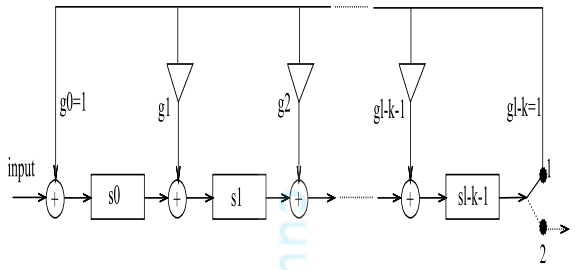
Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Mạch nguyên lý



Hình: Sơ đồ mạch mã hóa mã vòng dạng hệ thống dựa trên đa thức kiểm tra

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Mạch tính Syndrome



Hình: Sơ đồ mạch tính Syndrome cho mã vòng tuyến tính

Mạch vòng tuyến tính dạng hệ thống

Mạch nguyên lý mã hóa mã vòng: Xây dựng từ đa thức kiểm tra - Minh họa (2)

Nhịp	Bít vào	Các thanh ghi				Bít ra
		a_0	a_1	a_2	a_3	
0	–	0	0	0	0	–
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	–	1	1	0	0	1
6	–	1	1	1	0	1
7	–	0	1	1	1	0

Bảng: Bảng mô tả hoạt động mạch mã hóa với khối tin vào 1001

- $\Rightarrow \mathbf{c} = 011\mathbf{1001}$

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Nguyên lý mạch tính Syndrome

1. Chuyển mạch ở vị trí 1, nội dung các thanh ghi bằng 0.
2. l nhịp dịch toàn bộ nội dung véc-tơ thu vào $l-k$ thanh ghi Syndrome. Sau l nhịp, nội dung trong các thanh ghi Syndrome là véc-tơ Syndrome tương ứng với véc-tơ thu.
3. Chuyển mạch chuyển sang vị trí 2. Dòng dữ liệu vào tạm thời ngắt.
4. Mạch thực hiện $l-k$ nhịp tiếp để đọc nội dung các thanh ghi Syndrome ra ngoài.

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Tính toán Syndrome

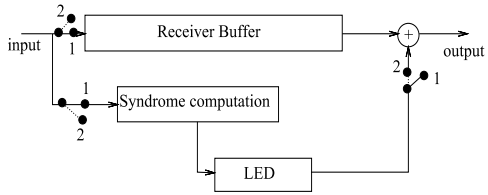
Gọi $s(x)$ là đa thức tương ứng với véc-tơ Syndrome của mã vòng tuyến tính $\mathfrak{C}(l,k)$

- $s(x) \equiv r(x) \bmod g(x)$
- $deg(s(x)) \leq l-k-1$.
- $\mathbf{s} = \mathbf{r}\mathbf{H}^T$.
- $s(x) = r(x)h(x) \bmod (x^l - 1)$

Nếu véc-tơ thu $r(x)$ không có lỗi, khi và chỉ khi $s(x) = 0$

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Mạch nguyên lý



Hình: Sơ đồ mạch thực hiện giải mã vòng tuyến tính theo Syndrome

- Thanh ghi đệm thu chứa véc-tơ thu.
- Mạch tính Syndrome thực hiện tính Syndrome dựa trên đa thức sinh $g(x)$.
- LED: khối lô-gíc phát hiện lỗi từ véc-tơ Syndrome tương ứng.

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Bảng Syndrome

Từ $\frac{r(x)}{g(x)} = a(x) + \frac{e(x)}{g(x)}$

- $\Rightarrow$ Giả sử có $e(x)$, $s(x)$ là phần dư của phép chia $e(x)$ cho $g(x)$.

Ví dụ

Trên $GF(2)$, mã vòng tuyến tính $\mathfrak{C}(7,4)$ với đa thức sinh $g(x) = 1 + x + x^3$, $d_{min} = 3$. Bảng Syndrome tương ứng với lỗi đơn:

Véc-tơ lỗi		*Véc-tơ Syndrome*	
$e_6(x) = x^6$	(0000001)	$s_6(x) = 1 + x^2$	(101)
$e_5(x) = x^5$	(0000010)	$s_5(x) = 1 + x + x^2$	(111)
$e_4(x) = x^4$	(0000100)	$s_4(x) = x + x^2$	(011)
$e_3(x) = x^3$	(0001000)	$s_3(x) = 1 + x$	(110)
$e_2(x) = x^2$	(0010000)	$s_2(x) = x^2$	(001)
$e_1(x) = x$	(0100000)	$s_1(x) = x$	(010)
$e_0(x) = 1$	(1000000)	$s_0(x) = 1$	(100)

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Nguyên lý mạch

1. Các chuyển mạch ở vị trí 1, nội dung các thanh ghi bằng 0.
2. l nhịp đầu tiên, nội dung véc-tơ thu được dịch vào thanh ghi đệm thu và đồng thời vào mạch tính Syndrome. Sau l nhịp, nội dung các thanh ghi Syndrome chứa véc-tơ Syndrome, thanh ghi đệm thu chứa véc-tơ thu.
3. Chuyển mạch chuyển sang vị trí 2.
4. Mạch dịch đồng bộ các thanh ghi đệm và thanh ghi Syndrome, đồng thời sửa sai nếu có.

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Bảng Syndrome

Định lý

$s(x)$ là đa thức Syndrome tương ứng với véc-tơ thu $r(x)$. Gọi phần dư thư được từ phép chia $xs(x)$ cho đa thức sinh $g(x)$ là $s^{(1)}(x)$, thì $s^{(1)}(x)$ là véc-tơ Syndrome tương ứng với véc-tơ thu $r^{(1)}(x)$.

- Ta có thể thu nhỏ bảng Syndrome cho mã vòng tuyến tính.

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Minh họa mạch (cont')

Nhịp	Thanh ghi đệm thông tin	Thanh ghi Syndrome	E	Ra
8	– 0 1 1 1 0 0	1 0 0	1	$0+1=1$
9	– – 0 1 1 1 0	0 1 0	0	$0+0=0$
10	– – – 0 1 1 1	0 0 1	0	$0+0=0$
11	– – – – 0 1 1	1 1 0	0	$1+0=1$
12	– – – – – 0 1	0 1 1	0	$1+0=1$
13	– – – – – – 0	1 1 0	0	$1+0=1$
14	– – – – – – –	0 1 1	0	$0+0=0$

Bảng: Mô tả quá trình sửa lỗi

- $\Rightarrow \hat{\mathbf{r}} = 0111001$

Các phương pháp giải mã vòng

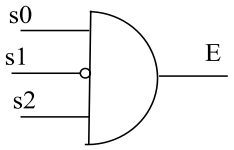
Phương pháp giải mã theo Syndrome: Minh họa mạch

Ví dụ

Xây dựng mạch giải mã theo Syndrome của mã vòng tuyến tính nhị phân $(7,4)$ có đa thức sinh $g(x) = 1 + x + x^3$. Giả sử rằng mạch có khả năng sửa lỗi đơn. Mô tả hoạt động của mạch cho véc-tơ thu 0111000.

Giải:

Không làm mất tính tổng quát ta xây dựng mạch lô-gíc phát hiện lỗi ở vị trí bít bậc cao nhất (x^6) tương ứng với véc-tơ Syndrome $\mathbf{s} = 101$. Ta nhận thấy, $\mathbf{s}$ có thể dễ dạng nhận dạng được bằng các dùng cổng lô-gíc AND 3 đầu vào.



s_0	s_1	s_2	E
...	...	...	0
1	0	1	1

Bảng: Bảng lô-gic của mạch

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Hệ tổng kiểm tra

$\mathbf{c} \in \mathfrak{C}$, $\mathbf{w} \in \mathfrak{C}^{\perp}$ $A \triangleq \mathbf{wr} = \mathbf{we}$

A: một tổng kiểm tra.

$A = w_0 e_0 + w_1 e_1 + \cdots + w_{l-1} e_{l-1}$

- bít lỗi e_k được kiểm tra bằng tổng kiểm tra $\mathbf{A}$ nếu $w_k = 1$.

Định nghĩa (Hệ tổng kiểm tra trực giao)

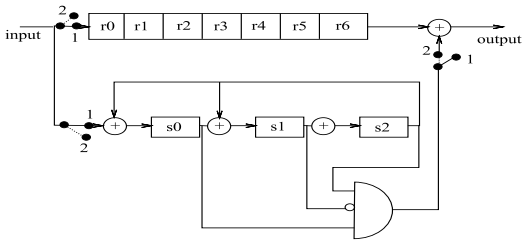
Một hệ gồm J tổng kiểm tra được gọi là hệ tổng kiểm tra trực giao với vị trí bít lỗi e_{l-1} nếu:

1. *Tất cả các hệ số của e_{l-1} trong hệ J tổng kiểm tra bằng* 1.
2. *Với $k \neq l-1$ chỉ có nhiều nhất một véc-tơ trong hệ tổng kiểm tra mà hệ số của e_k bằng 1.*

$\Rightarrow A_k = e_{l-1} + \sum_{i \neq l-1} w_i e_i$

Các phương pháp giải mã vòng

Phương pháp giải mã theo Syndrome: Minh họa mạch (cont')



Hình: Sơ đồ mạch giải mã theo Syndrome của mã vòng (7,4)

- Sau 7 nhịp, ta có nội dung các thanh ghi Syndrome là 101.
- Sau 7 nhịp, ta có nội dung thanh ghi đệm thu là 0111000.

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 1

Ví dụ

Trên GF(2), xét mã vòng tuyến tính $\mathfrak{C}(7,3)$ *có đa thức sinh* $g(x) = 1 + x + x^2 + x^4$.

1. *Xây dựng mạch nguyên lý giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao.*
2. *Mô tả hoạt động của mạch khi véc-tơ thu là* $\mathbf{r} = 0011111$

$\mathfrak{C}(7,3,4)$: mã vòng có khả năng trực giao đầy đủ. $\Rightarrow J = 3$.

$\mathbf{w}_1 = \mathbf{h}_1 + \mathbf{h}_3 + \mathbf{h}_4$, $\mathbf{w}_2 = \mathbf{h}_2 + \mathbf{h}_3 + \mathbf{h}_4$, và $\mathbf{w}_3 = \mathbf{h}_4$

Hệ 3 tổng kiểm tra trực giao với e_6 là:

$$\mathbf{A}_1 = e_0 + e_4 + e_6 \equiv r_0 + r_4 + r_6$$

$$\mathbf{A}_2 = e_1 + e_2 + e_6 \equiv r_1 + r_2 + r_6$$

$$\mathbf{A}_3 = e_3 + e_5 + e_6 \equiv r_3 + r_5 + r_6$$

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Thuật toán một bước

Giải mã ngưỡng dựa trên hệ tổng kiểm tra trực giao

Bít lỗi e_{l-1} được quyết định là 1 nếu có phần lớn các véc-tơ trong tổng kiểm tra trực giao bằng 1. Ngược lại thì bít lỗi e_{l-1} được quyết định là 0.

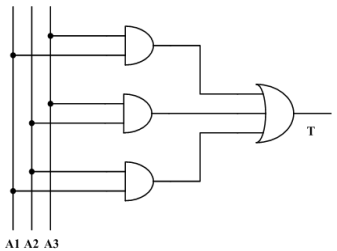
- Bộ giải mã hoạt động đúng khi véc-tơ lỗi có trọng $\leq \lfloor J/2 \rfloor$.
- Nếu có thể tạo hệ J tổng kiểm tra trực giao cho e_{l-1} thì cũng có thể tạo hệ J tổng kiểm tra trực giao cho các vị trí bít lỗi e_k $(k \neq l-1)$ nào đó.
- Nếu J là số tổng kiểm tra trực giao cực đại có thể lập được cho e_{l-1} (hoặc bất kỳ e_k nào đó), phương pháp giải mã nêu trên có thể sửa được các cấu trúc lỗi có trọng $\leq \lfloor J/2 \rfloor$. $t_{ML} = \lfloor J/2 \rfloor$: khả năng sửa lỗi của bộ giải mã ngưỡng.
- Phép giải mã này được gọi là hiệu quả với bộ mã $\mathfrak{C}(l,k,d_0)$ chỉ nếu $t_{ML} = \lfloor J/2 \rfloor$ bằng hoặc xấp xỉ bằng $t = \lfloor (d_0 - 1)/2 \rfloor$.

Các phương pháp giải mã vòng

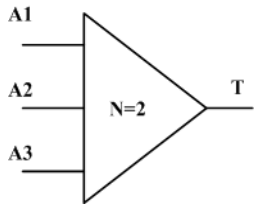
Phương pháp giải mã ngưỡng: Minh họa 1 (cont')

$J = 3 \Rightarrow$ Mức ngưỡng đa số $N = 2$.

Hàm xác định mức ngưỡng: $T = \mathbf{A}_1\mathbf{A}_2 + \mathbf{A}_1\mathbf{A}_3 + \mathbf{A}_2\mathbf{A}_3$



Hình: Mạch nguyên lý mạch hàm ngưỡng



Hình: Ký hiệu tương đương

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Hệ tổng kiểm tra có khả năng trực giao

Định nghĩa (Bộ mã vòng có khả năng trực giao đầy đủ)

Một bộ mã vòng $\mathfrak{C}(l,k,d_0)$ *gọi là khó khả năng trực giao đầy đủ một bước nếu và chỉ nếu nó có thể tạo được hệ* $J = d_0 - 1$ *tổng kiểm tra trực giao với một vị trí bít lỗi nào đó.*

- $J < l - k$.
- Không phải mọi mã vòng $\mathfrak{C}(l,k,d_0)$ đều là có khả năng trực giao đầy đủ.

Định nghĩa (Hệ tổng kiểm tra có khả năng trực giao)

Một tập gồm J *tổng kiểm tra* $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_J$ *là hệ tổng kiểm tra trực giao với tập* M *vị trí bít lỗi* $\mathbf{E} = \{e_{i_1}, e_{i_2}, \ldots, e_{i_M}\}$ $(0 \leq i_1 < i_2 < \cdots < i_M < l)$ *nếu:*

1. *Mọi vị trí bít lỗi* e_{i_j} *của* $\mathbf{E}$ *đều được kiểm tra bởi mọi tổng kiểm tra* $\mathbf{A}_j$ $(1 \leq j \leq J)$, *và*
2. *Không có bất cứ vị trí lỗi nào khác được kiểm tra ở nhiều hơn 1 tổng kiểm tra.*

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 2

Ví dụ

Trên GF(2), xét mã vòng tuyến tính $\mathfrak{C}(7,4)$ có đa thức sinh $g(x) = 1 + x + x^3$.

1. *Xây dựng mạch nguyên lý giải mã ngưỡng dựa trên hệ tổng kiểm tra có thể trực giao.*
2. *Mô tả hoạt động của mạch khi véc-tơ thu là 0001111.*

$\mathfrak{C}(7,4,3)$: không thể xây dựng được hệ tổng kiểm tra trực giao

$\mathbf{w}_1 = \mathbf{h}_1 + \mathbf{h}_3$, $\mathbf{w}_2 = \mathbf{h}_3 \Rightarrow$ hệ tổng kiểm tra trực giao với $e_5 + e_6$:

$$\mathbf{A}_1 = e_0 + e_3 + e_5 + e_6 \equiv r_0 + r_3 + r_5 + r_6$$

$$\mathbf{A}_2 = e_2 + e_4 + e_5 + e_6 \equiv r_2 + r_4 + r_5 + r_6$$

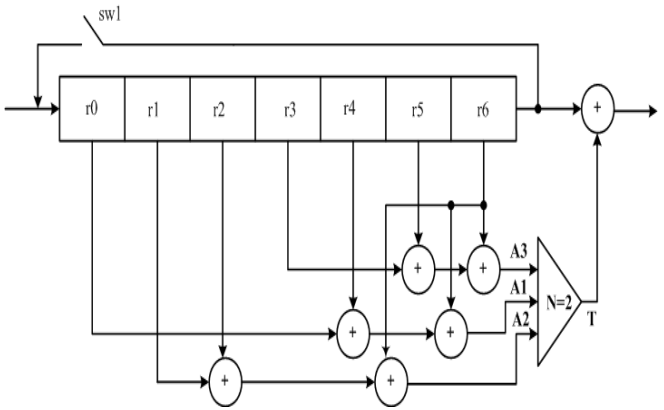
$\mathbf{w}_1 = \mathbf{h}_1 + \mathbf{h}_2 + \mathbf{h}_3$, $\mathbf{w}_2 = \mathbf{h}_3 \Rightarrow$ hệ tổng kiểm tra trực giao với $e_4 + e_6$:

$$\mathbf{B}_1 = e_0 + e_1 + e_4 + e_6 \equiv r_0 + r_1 + r_4 + r_6$$

$$\mathbf{B}_2 = e_2 + e_5 + e_4 + e_6 \equiv r_2 + r_5 + r_4 + r_6$$

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 1 (cont')



Hình: Nguyên lý mạch giải mã ngưỡng dựa và hệ thống kiểm tra trực giao cho mã $\mathfrak{C}(7,3,4)$

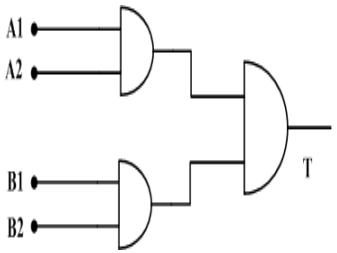
Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 2 (cont')

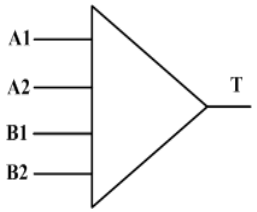
$S(E_1^1) = e_5 + e_6$ ước lượng được từ $\mathbf{A}_1$ và $\mathbf{A}_2$

$S(E_2^1) = e_4 + e_6$ ước lượng được từ $\mathbf{B}_1$ và $\mathbf{B}_2$

$\Rightarrow S(E_1^1)$ và $S(E_2^1)$ trực giao với $e_6 \Rightarrow e_6$ ước lượng từ $S(E_1^1)$ và $S(E_2^1)$.



Hình: Mạch nguyên lý mạch hàm ngưỡng



Hình: Ký hiệu tương đương

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 1 (cont')

Nhịp	r_0	r_1	r_2	r_3	r_4	r_5	r_6	A_3	A_1	A_2	T	Ra
0	0	0	1	1	1	1	1	–	–	–	–	–
1	1	0	0	1	1	1	1	1	0	0	0	$1+0=1$
2	1	1	0	0	1	1	1	1	1	1	1	$1+1=0$
3	1	1	1	0	0	1	1	0	1	0	0	$1+0=1$
4	1	1	1	1	0	0	1	0	0	1	0	$1+0=1$
5	1	1	1	1	1	0	0	0	0	1	0	$1+0=1$
6	0	1	1	1	1	1	0	1	0	0	0	$0+0=0$
7	0	0	1	1	1	1	1	0	1	0	0	$0+0=0$

Bảng: Bảng mô tả hoạt động của mạch giải mã ngưỡng

- $\Rightarrow$ Từ mã giải được là 00111$\bar{0}$1

Các phương pháp giải mã vòng

Phương pháp bẫy lỗi - Thuật toán chia dịch vòng: Thuật toán

Nhập vào: Véc-tơ thu $r(x)$ và thông số bộ mã $\mathfrak{C}(l,k)$ như đa thức sinh $g(x)$ và d_{min}, kí hiệu $\mathfrak{C}(l,k,d_{min})$.
In ra Từ mã đã được sửa sai.

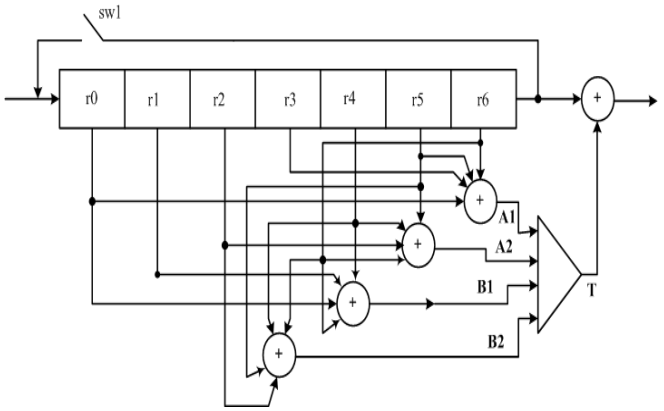
Bước 1: Với $i = 0, ..., l-1$

1. Tính $s_i(x)$ là phần dư của phép chia $x^i r(x)$ [hoặc$\frac{r(x)}{x^i}$] cho $g(x)$.
2. Tính trọng của $s_i(x)$: $w(s_i(x))$.
3. Nếu $w(s_i(x)) \leq t = \lfloor \frac{d_{min}-1}{2} \rfloor$ chuyển đến **Bước 2**.
4. Nếu $w(s_i(x)) > t$ tăng i lên 1 đơn vị.
5. Nếu $i = n$ chuyển đến **Bước 3**.

Bước 2 Đa thức mã được sửa bởi: $\hat{r}(x) = \frac{x^i r(x) + s_i(x)}{x^i}$ [hoặc $\hat{r}(x) = x^i\{\frac{r(x)}{x^i} + s_i(x)\}$]. In ra từ mã đã được sửa lỗi tương ứng. Kết thúc.
Bước 3 Thông báo không sửa được lỗi (số lỗi vượt quá khả năng sửa lỗi). Kết thúc.

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 2 (cont')



Hình: Nguyên lý mạch giải mã ngưỡng dựa và hệ thống kiểm tra trực giao cho mã $\mathfrak{C}(7,4,3)$

Các phương pháp giải mã vòng

Phương pháp bẫy lỗi - Thuật toán chia dịch vòng: Minh họa

Ví dụ

Trên $GF(2)$ xét bộ mã vòng tuyến tính $\mathfrak{C}(7,4)$ với đa thức sinh $g(x) = 1 + x + x^2 + x^4$ có $d_{min} = 4$. Giả sử nhận được véc-tơ $\mathbf{r} = 0111011$. Hãy sử dụng thuật toán chia dịch vòng tìm từ mã đúng tương ứng với véc-tơ thu.

$\Rightarrow r(x) = x + x^2 + x^3 + x^5 + x^6$

Bước 1:

$i = 0$:

- $s_0(x) \equiv r(x) \bmod g(x)$
- $\Rightarrow s_0(x) = 1 + x + x^3$
- $\Rightarrow w(s_0(x)) = 3 \geq t = 1$
- $\Rightarrow i = i + 1 = 1$

$i = 1$:

- $s_1(x) \equiv xr(x) \bmod g(x)$
- $\Rightarrow s_1(x) = 1$
- $\Rightarrow w(s_1(x)) = 1 = t$
- Chuyển đến **Bước 2**

Bước 2:

$$\begin{aligned}\hat{r}(x) &= \frac{x^i r(x) + s_i(x)}{x^i}|_{i=1} \\ &= x + x^2 + x^3 + x^5\end{aligned}$$

$\Rightarrow \hat{\mathbf{r}} = 0111010\bar{\mathbf{0}}$

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Minh họa 2 (cont')

Nhịp	r_0	r_1	r_2	r_3	r_4	r_5	r_6	A_1	A_2	B_1	B_2	T	Ra
0	0	0	0	1	1	1	1	–	–	–	–	–	–
1	1	0	0	0	1	1	1	1	1	0	1	0	$1+0=1$
2	1	1	0	0	0	1	1	1	1	1	1	1	$1+1=0$
3	1	1	1	0	0	0	1	1	0	1	0	0	$1+0=1$
4	1	1	1	1	0	0	0	0	0	1	0	0	$1+0=1$
5	0	1	1	1	1	0	0	0	1	0	1	0	$0+0=0$
6	0	0	1	1	1	1	0	1	0	0	0	0	$0+0=0$
7	0	0	0	1	1	1	1	0	1	1	1	0	$0+0=0$

Bảng: Bảng mô tả hoạt động của mạch giải mã ngưỡng

- $\Rightarrow$ Từ mã giải được là $00011\bar{\mathbf{0}}1$

Kết thúc phần mã vòng