Trại hè toán và khoa học MaSSP 2021

Báo cáo khoa học

môn toán

Mã tuyến tính tự sửa sai

Tác giả

Tạ Đức Minh (Trường THPT Chuyên Hà Nội - Amsterdam - Hà Nội)
Lê Trần Duy Anh (Trường THPT Chuyên KHTN - Hà Nội)
Nguyễn Hòa Phan (Trường THPT Chuyên Quốc Học - Huế)
Tạ Đình Tiến (Trường THPT Chuyên Quốc Học - Huế)
Hoàng Việt Bách (Trường THPT Chuyên KHTN - Hà Nội)

Headmentor

Nguyễn Mạnh Linh

Giáo Viên Giảng Dạy

Đào Vũ Quang
Nguyễn Hùng Quang

Tóm tắt nội dung

Trong quá trình mã hóa và truyền thông tin, một số bit có thể bị thay đổi do nhiễu của kênh. Ý tưởng của mã tự sửa sai là thêm vào một số ký tự dư cho phép phát hiện và chỉnh sửa một lượng lỗi sai nhất định do nhiễu gây ra (như vậy, trái với việc nén thông tin, mã hóa tự sửa sai sẽ làm tăng chiều dài của thông điệp, làm giảm tỉ lệ thông tin thực sự). Các mã này thường có một cấu trúc tuyến tính để có thể áp dụng các kỹ thuật của đại số. Việc mã hóa là tương đối đơn giản, trong khi việc giải mã nói chung là phức tạp và yêu cầu các thuật toán đặc trưng cho từng loại mã. Mục tiêu của lý thuyết mã tuyến tính tự sửa sai là xây dựng các loại mã với tỉ lệ thông tin cao và thuật toán giải mã dễ cài đặt.

Ngày 25/07/2021

Mục lục

Lời cảm ơn

1 Mã tuyến tính

1.1 Ma trận

1.1.1 Định nghĩa về ma trận

Định nghĩa 1.1. Mỗi bảng A với m hàng, n cột có dạng

$$A = \begin{bmatrix} a_{11} & a_{12} & ... & a1n \\ a_{21} & a_{22} & ... & a_{2n} \\ ... & ... & ... & ... \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix}$$

trong đó $a_{ij} \in R$ được gọi là một ma trận cỡ $m \times n$. Ta kí hiệu ngắn gọn là $A = [a_{ij}]_{m\times n}$.

- Nếu $m = 1$, ta gọi A là một véc-tơ hàng. Nếu $n = 1$, ta gọi A là một véc-tơ cột. Nếu $m = n$, ta gọi A là một ma trận vuông cỡ n.
- Với mỗi $i = 1, 2, ..., m$, véc-tơ hàng $(a_{i1}, a_{i2}, ..., a_{in}) := [a_{i1}, a_{i2}, ..., a_{in}]$ được gọi là hàng thứ i của A. Với mỗi $j = 1, 2, ..., n$, véc-tơ cột $\begin{bmatrix} a_{1j} \\ . \\ . \\ a_{mj} \end{bmatrix}$ được gọi là cột thứ j của A. Giá trị a_{ij} được gọi là phần tử thứ (i, j) của A.

1.1.2 Các phép toán cơ bản trên ma trận

Cho $A = \begin{bmatrix} a_{11} & ... & a_{1n} \\ ... & ... & ... \\ a_{m1} & ... & a_{mn} \end{bmatrix} = [a_{ij}]_{m\times n}$ và $B = \begin{bmatrix} b_{11} & ... & b_{1n} \\ ... & ... & ... \\ b_{m1} & ... & b_{mn} \end{bmatrix} = [b_{ij}]_{m\times n}$ là hai ma trận cùng cỡ. Ta định nghĩa các phép toán với ma trận sau đây

- Ma trận chuyển vị của A là ma trận cỡ $n \times m$

$$A^T = \begin{bmatrix} a_{11} & a_{21} & ... & am1 \\ a_{21} & a_{22} & ... & a_{m2} \\ ... & ... & ... & ... \\ a_{1n} & a_{2n} & ... & a_{mn} \end{bmatrix}$$

  Nói cách khác, ta đổi vai trò của các hàng và các cột của A. Hay ta có thể viết mỗi véc-tơ cột $\begin{bmatrix} a_1 \\ . \\ . \\ a_n \end{bmatrix}$ thành các véc-tơ hàng $(a_1, ..., a_n)^T$.

- Tổng của hai ma trận A và B là ma trận

$$A + B = \begin{bmatrix} a_{11} + b_{11} & ... & a_{1n} + b_{1n} \\ ... & ... & ... \\ a_{m1} + b_{m1} & ... & a_{mn} + b_{mn} \end{bmatrix} = [a_{ij} + b_{ij}]_{m\times n}$$

  Nói cách khác, ta cộng từng phần tử của A và B theo từng tọa độ.

- Với mỗi vô hướng $\lambda \in \mathbb{R}$, ta có thể nhân λ với A.

$$\lambda A = \begin{bmatrix} \lambda a_{11} & ... & \lambda a_{1n} \\ ... & ... & ... \\ \lambda a_{m1} & ... & \lambda a_{mn} \end{bmatrix} = [\lambda a_{ij}]_{m\times n}$$

  Nói cách khác, ta nhân λ với từng phần tử của A.

Cho hai ma trận $A = [a_{ij}]_{m\times n}$, $B = [b_{ij}]_{n\times p}$. Tích AB của hai ma trận trên là ma trận $m \times p$ $AB = [c_{ij}]_{m\times p}$ với $c_{ij} = \sum_{s=1}^{n} a_{is}b_{sj}$

. Ví dụ: $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} x & t \\ y & u \\ z & v \end{bmatrix} = \begin{bmatrix} ax+by+cz & at+bu+cv \\ dx+ey+fz & dt+eu+fv \\ gx+hy+iz & gt+hu+iv \end{bmatrix}$

Phép nhân ma trận thỏa mãn các tính chất sau:

- Kết hợp: Với mọi $A \in M_{m\times n}(R)$, $B \in M_{n\times p}(R)$ và $C \in M_{p\times q}(R)$, ta có
$$(AB)C = A(BC)$$
- Phân phối hai phía với phép cộng: với mọi $A, A_1, A_2 \in M_{m\times n}(R)$ và $B, B_1, B_2 \in M_{n\times p}(R)$
$$A(B_1 + B_2) = AB_1 + AB_2$$
$$(A_1 + A_2)B = A_1B + A_2B$$
- Tương thích với phép nhân vô hướng: với mọi $A \in M_{m\times n}(R)$, $B \in M_{n\times p}(R)$ và $\lambda \in R$
$$\lambda(AB) = (\lambda A)B = A(\lambda B)$$

1.2 Mã tuyến tính

1.2.1 Trường và không gian véc-tơ

Định nghĩa 1.2. Trường $\mathbb{F}$ là một tập hợp được trang bị 2 phép toán + và . thỏa mãn các tính chất sau

- $(\mathbb{F}, +)$ là nhóm abel với phần tử trung hòa 0.
- $(\mathbb{F}, .)$ là nhóm abel với phần tử trung hòa 1.
- Phép cộng và phép nhân có tính phân phối.

Ví dụ:

- Tập $\mathbb{F}_p$ gồm các phần tử $0, 1, ..., p-1$ với p nguyên tố. Phép cộng và phép nhân tính theo modulo p.
$$(a+b)c = ab + bc \mod p$$
- Tập số thực $\mathbb{R}$ và tập số phức $\mathbb{C}$ là trường với phép nhân và phép cộng thông thường.

Định nghĩa 1.3. Một không gian véc-tơ V trên trường F là một tập hợp cùng với hai phép cộng véc tơ và phép nhân vô hướng thỏa mãn

- $(V, +)$ là nhóm abel
- Tính phân phối: Với mọi $x, y \in V$ và $\lambda, \mu \in \mathbb{F}$, ta có
$$\lambda(x+y) = \lambda x + \lambda y, (\lambda + \mu)x = \lambda x + \mu x$$
- $1x = x$ với 1 là phần tử đơn vị của $\mathbb{F}$

Ví dụ 1.4.
- Mọi trường đều là không gian véc-tơ trên chính nó
- Vành đa thức $\mathbb{F}[X]$ là không gian véc-tơ với phép cộng đa thức và phép nhân đa thức với vô hướng
- Cho V, W là hai không gian véc-tơ. Tích Descartes $V \times W$ của V và W là không gian véc-tơ với phép toán
$$(x, x') + (y, y') = (x + x', y + y')$$
$$\lambda(x, x') = (\lambda x, \lambda x')$$

- $\mathbb{F}^n$ là không gian véc-tơ đạt được bằng cách lấy tích trực tiếp của n không gian véc-tơ $\mathbb{F}$. Các phần tử của $\mathbb{F}^n$ có thể xem như một mảng n phần tử

Cho trường $\mathbb{F}$. Kí hiệu $\mathbb{F}_n$ là tập các véc-tơ gồm n phần tử thuộc $\mathbb{F}$, với phép toán cộng véc-tơ và nhân vô hướng.

Định nghĩa 1.5. Cho tập k véc-tơ độc lập tuyến tính thuộc $\mathbb{F}_n$, không gian véc-tơ con của $\mathbb{F}_n$ là tập các véc-tơ có thể viết thành tổ hợp tuyến tính của k véc-tơ trên.

- Số k được gọi là số chiều của không gian véc-tơ con.
- Tập k véc-tơ trên được gọi là cơ sở của không gian véc-tơ con.

1.2.2 Mã tuyến tính

Định nghĩa 1.6. Cho $\mathbb{F}_p$ là một trường hữu hạn. Một mã (n, k) tuyến tính C là một không gian véc-tơ con k chiều của $\mathbb{F}^n$. Các véc-tơ thuộc C được gọi là từ mã.

Ví dụ 1.7.
- Khi $C =^n$, tất cả véc-tơ n chiều đều là từ mã của C.
- Tập các véc-tơ có độ dài n và tất cả các phần tử đều bằng nhau tạo thành một mã $(n, 1)$ tuyến tính. Mã này được gọi là mã lặp lại.

Định nghĩa 1.8. Một ma trận sinh của mã (n, k) tuyến tính C là một ma trận $k \times n$ G sao cho các hàng của G tạo thành một cơ sở của C.

Ví dụ 1.9. Ma trận dưới đây là ma trận sinh của một mã $(5, 3)$ tuyến tính.

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

Định nghĩa 1.10. Cho mã (n, k) tuyến tính C. Một ma trận điều kiện của C là một ma trận $(n - k) \times n$ H thỏa mãn:

$$H \cdot m^T = 0 \ \forall \ m \in C.$$

Ví dụ 1.11. Cho mã $(5, 3)$ tuyến tính với ma trận sinh

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

Một ma trận điều kiện của mã trên là

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

Định nghĩa 1.12. Cho một mã (n, k) tuyến tính C. Ta định nghĩa mã đối ngẫu $C^\perp$ của C như sau

$$C^\perp = \{c \in F^n \mid c.m^T = 0 \ \forall \ m \in C\}$$

Ta dễ dàng thấy ma trận sinh của C là ma trận điều kiện của $C^\perp$ và ngược lại.

Ví dụ 1.13. Mã đối ngẫu của mã $(5, 3)$ tuyến tính trong ví dụ trên là mã $(5, 2)$ tuyến tính với ma trận sinh và ma trận điều kiện như sau

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

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

2 Mã Hamming

2.1 Định nghĩa và tính chất

2.1.1 Trọng số

Định nghĩa 2.1. Cho mã (n, k) tuyến tính C. Với $m \in C$ ta định nghĩa trọng số của m là số kí tự khác 0 của m, kí hiệu là $wt(m)$. Trọng số của C là số nhỏ nhất khác 0 trong các trọng số của $m \in C$.

Ví dụ 2.2.
- Véc-tơ $x = [0, 1, 0, 1, 1, 0, 0]$ có trọng số $wt(x)$ là 3.
- Cho mã tuyến tính gồm 4 từ mã $\{(0, 1, 0), (0, 0, 1), (0, 1, 1), (0, 0, 0)\}$. Trọng số của mã này là 1.

2.1.2 Khoảng cách Hamming

Định nghĩa 2.3. Cho $m, m' \in \mathbb{F}^n$. Khi đó, khoảng cách Hamming giữa m và m' là

$$d(m, m') = wt(m - m').$$

Tính chất 1. Cho mã (n, k) tuyến tính C. Khi đó:

$$wt(C) = \min_{m,m' \in C, m \neq m'} d(m, m') = \min_{m \in C} wt(m).$$

Khoảng cách Hamming thoả mãn bất đẳng thức tam giác

$$d(m, m') + d(m', m'') \geq d(m, m'').$$

Ta có cách phát hiện lỗi và sửa lỗi với C như sau: cho $x \in \mathbb{F}^n$,

- Ta phát hiện x có lỗi nếu $0 < d(x, m) < d \ \forall m \in C$.
- Ta sửa được lỗi đối với x nếu như tồn tại $m_0 \in C$ sao cho $d(x, m_0) < \frac{d}{2}$.

2.1.3 Định nghĩa mã Hamming

Định nghĩa 2.4. Cho $m \geqslant 2$ và $n = 2^m - 1$. Ta xây dựng ma trận $m \times n$ $H_{m,2}$ có các cột khác 0 và đôi một khác nhau. Mã tuyến tính nhị phân có ma trận điều kiện $H_{m,2}$ gọi là mã Hamming, kí hiệu là $Ham(2^m - 1, 2^m - m - 1)$. Các cột của H là biểu diễn nhị phân của các số nguyên từ 1 đến $2^m - 1$.

Ví dụ 2.5. Mã $Ham(7, 4)$ có ma trận điều kiện

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

2.1.4 Trọng cực tiểu của mã Hamming

Gọi d_i là các từ mã có độ dài $n = 2^m - 1$ có vị trí khác 0 duy nhất là i, d_{ij} là các từ mã có độ dài n khác 0 tại i và j.

- Nếu $Ham(2^m - 1, 2^m - m - 1)$ có trọng cực tiểu bằng 1, tồn tại d_i sao cho $Hd_i^T = 0$. Điều này tương đương với H có cột bằng 0.
- Nếu $Ham(2^m - 1, 2^m - m - 1)$ có trọng cực tiểu bằng 2, tồn tại d_{ij} sao cho $Hd_{ij}^T = 0$. Điều này tương đương với H có 2 cột bằng nhau.

Vậy $Ham(2^m - 1, 2^m - m - 1)$ có trọng cực tiểu lớn hơn 2.
Xét 3 số tự nhiên a, b, c nhỏ hơn n sao cho $a + b = c$. Các véc-tơ là biểu diễn nhị phân của a, b, c là cột của H, giả sử là cột thứ p, q, r. Từ mã có vị trí p, q, r khác 0 thuộc $Ham(2^m - 1, 2^m - m - 1)$, do đó $Ham(2^m - 1, 2^m - m - 1)$ có trọng bằng 3.

Hệ quả 2.6. Mã Hamming (nhị phân) là một mã $(2^m - 1, 2^m - m - 1, 3)$. Như vậy, mã Hamming có thể phát hiện tối đa 2 lỗi và sửa tối đa 1 lỗi.

2.2 Giải mã

2.2.1 Mã hóa

Định nghĩa 2.7. Xét mã (n, k, d) có ma trận sinh G và ma trận điều kiện H. Ta mã hoá một thông điệp $x \in \mathbb{F}^k$ bởi ánh xạ $x \to c = xG$.

Ví dụ 2.8. Xét mã có ma trận sinh

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

- Mọi thông điệp $x = x_1x_2x_3x_4x_5$ được mã hóa thành

$$c = x_1x_2x_3x_4x_5(x_2 + x_3 + x_4 + x_5)(x_2 + x_3 + x_4).$$

Xét mã có hệ thống với ma trận sinh $G = [I|A]$, nhận thông điệp x và mã hóa thành $c = xG$. Ta có thể thấy k phần tử đầu tiên của c chính là x. Do đó ta chỉ cần tính $n - k$ phần tử còn lại thay vì nhân ma trận xG.

2.2.2 Giải mã hợp lý cực đại

Định nghĩa 2.9. Khi nhận được véc-tơ $y = x + e$, ta tìm trong q^n véc-tơ z thuộc mã C có khoảng cách Hamming với y nhỏ nhất

$$x = \arg\min_{z \in C} d(z, y).$$

- Nếu có không quá $t = \lfloor \frac{d-1}{2} \rfloor$ lỗi trong quá trình truyền tin, cách giải mã trên trả về duy nhất véc-tơ x.
  Chứng minh: Kí hiệu $S_t(c)$ là tập các véc-tơ (không nhất thiết thuộc C) có khoảng cách tới c không quá t. Cho $c_1, c_2 \in C$, ta có $S_t(c_1)$ và $S_t(c_2)$ không giao nhau. Véc-tơ nhận được thuộc $S_t(x)$, do đó không tồn tại véc-tơ khác x có khoảng cách với y nhỏ hơn t.
- Nếu có không quá $d - 1$ lỗi, ta có thể phát hiện có lỗi nhưng chưa chắc giải mã được.

2.2.3 Giải mã syndrome

Giải mã hợp lí cực đại thực hiện bằng cách tính khoảng cách của q^n véc-tơ trong C, sẽ gặp khó khăn khi $|C|$ lớn. Phương pháp giải mã syndrome giúp tìm véc-tơ lỗi hiệu quả hơn.

Nhận xét 1. Nếu ta nhận được véc-tơ $y = x + e$ với $x \in C$ thì

$$Hy^T = Hx^T + He^T = He^T.$$

- Lớp kề của $y \in \mathbb{F}^n$ là tập $y + C = \{y + c \mid c \in C\}$. Véc-tơ có trọng nhỏ nhất trong lớp kề gọi là phần tử dẫn của lớp kề, đặt là e.
- Gọi syndrome của y là véc-tơ $syn(y) = Hy^T \in \mathbb{F}^{n-k}$. Các phần tử cùng thuộc lớp kề có cùng syndrome.
- Nếu $\mathbb{F}$ có q phần tử, khi đó ta sẽ có q^{n-k} lớp kề tương ứng với q^{n-k} syndrome.
- Giải mã syndrome: với mỗi lớp kề của C, ta tính trước phần tử dẫn và syndrome ứng với lớp đó. Khi nhận được y, ta tính $syn(y)$ và so sánh với syndrome đã được tính trước.

Ví dụ 2.10. Xét mã nhị phân C có

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

- Syndrome 1 ứng với phần tử dẫn $[1, 0, 0]$, $[0, 1, 0]$, $[0, 0, 1]$, syndrome 0 ứng với $[0, 0, 0]$.

Ví dụ 2.11. Cho mã Hamming $(7, 4)$ với ma trận điều kiện H và ma trận sinh G như sau

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

- Cho thông điệp ban đầu $x = [0, 1, 1, 0]$. Véc-tơ c sau khi mã hóa là: $c = xG = [0, 1, 1, 0, 0, 1, 1]$.
- Tính chất: Đối với mã Hamming, phần tử dẫn của nó sẽ là các véc-tơ có duy nhất 1 phần tử bằng 1. Tính syndrome tương ứng bằng cách lấy H nhân với chuyển vị của mỗi phần tử dẫn.
- Giả sử trong quá trình truyền tin kí tự tại vị trí thứ 3 bị thay đổi. $\rightarrow c' = [0, 1, 0, 0, 0, 1, 1]$. Kí tự tại vị trí thứ 3 bị thay đổi $syn(c') = [0, 1, 1]$ tương ứng với phần tử dẫn là $[0, 0, 1, 0, 0, 0, 0]$. Đó chính là véc-tơ e nhiễu trong quá trình chuyển.

3 Mã Reed-Muller

3.1 Định nghĩa mã Reed-Muller theo đa thức Bool

3.1.1 Hàm Bool

Định nghĩa 3.1. Hàm Bool là 1 ánh xạ từ $\mathbb{F}_2^m \rightarrow \mathbb{F}_2$:

$$(x_0, x_1, ..., x_{m-1}) \rightarrow x$$

- Ví dụ: Bảng chân trị biểu diễn hàm Bool $f : \mathbb{F}_2^2 \rightarrow \mathbb{F}_2$

x_0	0	1	0	1
x_1	0	0	1	1
f	0	1	1	0

- Biến x_i có thể xem như một hàm Bool với véc-tơ biểu diễn là hàng ứng với biến x_i trong bảng chân trị

Định nghĩa 3.2. Tổng logic $f + g$ và tích logic fg của 2 hàm Bool f, g là 1 ánh xạ $\mathbb{F}_2^m \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$ lần lượt là phép cộng và nhân từng phần tử tương ứng của f và g trên trường $\mathbb{F}_2$

- Ví dụ: $011010 + 101010 = 110000$; $011010.101010 = 001010$

Tính chất 2.

- Phép toán tổng logic là phép toán xor, phép toán tích logic là phép toán and.
- Phép phủ định: $\overline{f} = f + 1$, phép or: f or $g = f + g + fg$
- Tính chất quan trọng: $ff = f$

3.1.2 Đa thức Bool

Định nghĩa 3.3. Đơn thức Bool là tích của 1 số lượng x_i nhất định có dạng: $\prod_{i \in I} x_i$ với $I \subseteq \{0, 1, ..., m-1\}$

- $|I|$ là bậc của đơn thức

Định nghĩa 3.4. Đa thức Bool là tổng Logic của các đơn thức Bool.

- Bậc của đa thức Bool được tính bằng bậc cao nhất của đơn thức Bool.

Tính chất 3. Với hàm Bool f bất kì,

$$f(x_0, ..., x_t) = f(x_0, x_1, \cdots, x_{t-1}, 0) + (f(x_0, x_1, \cdots, x_{t-1}, 0) + f(x_0, x_1, \cdots, x_{t-1}, 1))x_t$$

Chứng minh. Ta có x_t chỉ có thể nhận được giá trị 1 hoặc 0. Nếu $x_t = 0$, ta có $VT = f(x_0, x_1, \cdots, x_{t-1}, 0) = VP$.

Còn nếu $x_t = 1$ thì $VT = f(x_0, x_1, \cdots, x_{t-1}, 1) = 2f(x_0, x_1, \cdots, x_{t-1}, 0) + f(x_0, x_1, \cdots, x_{t-1}, 1) = f(x_0, x_1, \cdots, x_{t-1}, 0) + (f(x_0, x_1, \cdots, x_{t-1}, 0) + f(x_0, x_1, \cdots, x_{t-1}, 1)) = VP$

Kết luận lại, ta thu được

$$f(x_0, ..., x_t) = f(x_0, x_1, \cdots, x_{t-1}, 0) + (f(x_0, x_1, \cdots, x_{t-1}, 0) + f(x_0, x_1, \cdots, x_{t-1}, 1))x_t$$

□

Tính chất 4. Mọi hàm Bool là một đa thức Bool

Chứng minh. Ta chứng minh theo nguyên lý quy nạp. Với $t = 0$, Theo tính chất 2 thì $f(x_0) = f(0) + (f(0) + f(1))x_0$ là một đa thức Bool

Giả sử khẳng định đúng đến $t = k$ hay $f(x_0, x_1, \cdots, x_k)$ là một đa thức Bool. Ta chứng minh $f(x_0, x_1, \cdots, x_{k+1})$ cũng là đa thức Bool

Theo tính chất 2

$$f(x_0, ..., x_{k+1}) = f(x_0, x_1, \cdots, x_k, 0) + (f(x_0, x_1, \cdots, x_k, 0) + f(x_0, x_1, \cdots, x_k, 1))x_{k+1}$$

Ta có $f(x_0, x_1, \cdots, x_k, 0) = g(x_0, x_1, \cdots, x_k)$ là một hàm Bool hay nó là một đa thức Bool, $f(x_0, x_1, \cdots, x_k, 0) + f(x_0, x_1, \cdots, x_k, 1) = h(x_0, x_1, \cdots, x_k)$ là một hàm Bool hay nó là một đa thức Bool.

Vậy $f(x_0, ..., x_{k+1})$ cũng là một đa thức Bool □

Ta có thể xem từ mã là một đa thức được tạo từ các đơn thức trong ma trận sinh với hệ số của thông điệp

Định nghĩa 3.5. Mã Reed-Muller $R(r, m)$ là tập hợp tất cả các từ mã độ dài 2^m có biểu diễn dưới dạng đa thức Bool bậc $\leq$ r.

3.2 Định nghĩa mã Reed-Muller đệ quy và mã hóa

Định nghĩa 3.6. Mã Reed-Muller $R(r, m)$ có độ dài 2^m được định nghĩa đệ quy qua $R(r, m-1)$ và $R(r-1, m-1)$ như sau:

$$\{(u|u+v) \text{ với } u \in R(r, m-1) \text{ và } v \in R(r-1, m-1)\}$$

Định nghĩa 3.7. Mã hóa sẽ được thực hiện bằng cách nhân ma trận sinh. Ma trận sinh của $R(r, m)$ cũng được tính từ ma trận sinh của 2 mã $R(r, m-1)$ và $R(r-1, m-1)$ như sau:

$$G(r, m) = \begin{bmatrix} G(r, m-1) & G(r, m-1) \\ 0 & G(r-1, m-1) \end{bmatrix}$$

Ví dụ 3.8. Ví dụ, mã R(1,2) có ma trận sinh là:

$$G = \begin{bmatrix} 1 \\ x_0 \\ x_1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Ở đây, thông điệp $s = 011$ được mã hóa thành $x_0 + x_1$

3.3 Tính chất của mã Reed-Muller

- Số chiều k của mã Reed-Muller $R(r,m)$ là $\sum_{i=0}^{r}\binom{n}{i}$

Chứng minh. Do mã Reed-Muller là tập hợp các hàm Bool có bậc nhỏ hơn hoặc bằng r, khi ta áp dụng tính chất $ff = f$ của đa thức Bool, ta thấy 1 từ mã Reed-Muller sẽ có dạng tổng của nhỏ hơn hoặc bằng r đơn thức Bool (hiển nhiên độc lập tuyến tính với nhau). Mà có $\binom{n}{i}$ đơn thức Bool bậc i, nên có số chiều của từ mã là $\sum_{i=0}^{r}\binom{n}{i}$ □

- Trọng số của $R(r,m)$ là 2^{m-r} và vì vậy $R(r,m)$ sửa được $2^{m-r-1}-1$

Chứng minh. Quy nạp qua tính chất

$$wt(R(r,m)) = \min\{2wt(R(r,m-1)), wt(R(r-1,m-1))\}.$$

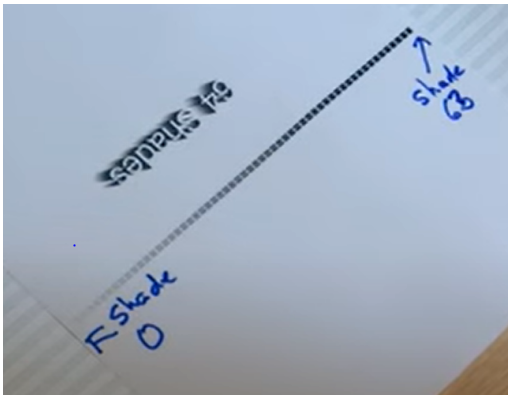
□

- Tỉ lệ thông tin: $R = \dfrac{k}{2^m}$ ($\approx 2^{-m(1-H_2(\frac{r}{m}))}$ khi $r << m$)

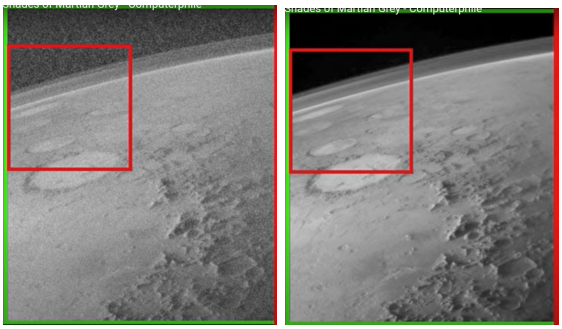
Khoảng cách tương đối: $\delta = \dfrac{d}{n} = \dfrac{2^{m-r}}{2^m} = 2^{-r}$

Ví dụ 3.9. Từ các tính chất trên, ta có một số mã Reed-Muller thường gặp:

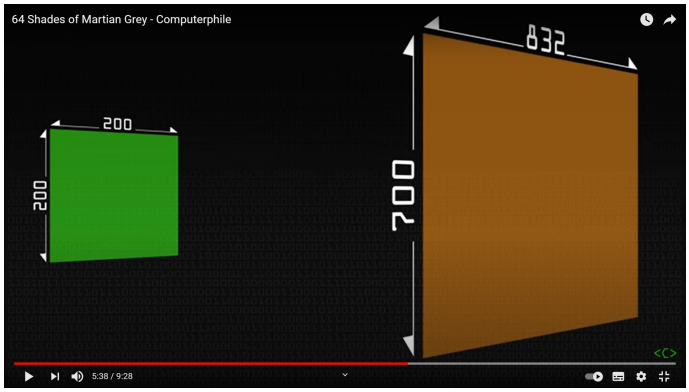
- Mã $R(0,m)$ là các mã lặp độ dài 2^m
- Mã $R(1,m)$ là mã $(2^m, m+1)$-tuyến tính
- Mã $R(1,4)$ là mã $(16,5,3)$-tuyến tính và mã $R(1,5)$ là mã $(32,6,7)$-tuyến tính (được NASA sử dụng trong truyền các pixel trong không gian từ 1969 đến 1977)
  Mỗi Pixel ảnh sẽ được quy ước bằng mã nhị phân độ dài 6 nên sẽ có 2^6 trạng thái màu sắc từ shade 0 đến shade 63



Khi chưa sử dụng mã Reed-Muller, với xấp xỉ 24 % bị lỗi, hình ảnh gửi về từ sao hỏa của tàu Mariner 3 truyền về Trái Đất "chỉ"mất 8 tiếng năm 1964 trước và sau khi qua lọc nhiễu:



Thử thách được đặt ra khi cần chụp tấm ảnh to gấp 3 năm 1964 với độ hiệu quả hơn, mã tự sửa sai RM(1,5) đã được NASA sử dụng khi có thể tự sửa 7 lỗi/32 kí tự, tiệm cận được phần trăm trung bình bị sai khi truyền từ sao hỏa về Trái Đất



- Mã $R(m-2,m)$ chính là mã mở rộng của mã Hamming độ dài 2^m

Ma trận điều kiện của $R(m-2,m)$:

$$H = \begin{bmatrix} 1 \\ x_1 \\ x_2 \\ ... \\ x_m \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & ... & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & ... & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & ... & 0 & 0 & 1 & 1 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & 0 & ... & 1 & 1 & 1 & 1 \end{bmatrix}$$

Cộng hàng 1 vào tất cả các hàng dưới rồi chuyển xuống vị trí hàng cuối cùng ta có ma trận điều kiện của mã Hamminng ở phần tư bên trên của bên trái.

$$H = \left[\begin{array}{cccccccc|c} 1 & 0 & 1 & 0 & ... & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & ... & 1 & 1 & 0 & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... \\ 1 & 1 & 1 & 1 & ... & 0 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & ... & 1 & 1 & 1 & 1 \end{array}\right]$$

3.4 Tính chất hình học và mối liên hệ với mã Reed-Muller

Định nghĩa 3.10. Cho 1 trường K bất kì, 1 r-phẳng là 1 tập con của K^n với $(n > r)$ có dạng $a + V$ với $a \in K^n$ và $V \subset K^n$

Nhận xét 2. Khi $K = \mathbb{F}_2 = \{0, 1\}$, mỗi r-phẳng đều có 2^r điểm

Ví dụ 3.11. Ví dụ, với $\{0, 1\}^3$, ta có:

- Có 2^3 là 8 0-phẳng (các điểm) tương ứng với $p_0 = 000, p_1 = 001, ..., p_6 = 110, p_7 = 111$.
- Do mỗi đường được tạo từ 2 điểm bất kì, có $\binom{8}{2}$ 1-phẳng (đường) tương ứng với $p_0 + tp_1, p_2 + tp_5, ...$
- 2-phẳng sẽ được hình thành bằng cách thêm 1 vector p_2 vào cơ sở của 1-phẳng, chẳng hạn như $p_0 + tp_1$ sẽ trở thành $p_0 + t_1p_1 + t_2p_2$, gồm 4 phần tử là $\{p_0, p_1, p_{0+2}, p_{1+2}\}$.

Định nghĩa 3.12. Với mọi $x \in \mathbb{F}_2^n$, Hàm chỉ thị của 1 r-phẳng là

$$f_L(x) = \begin{cases} 1 \text{ nếu } x \in L, \\ 0 \text{ nếu } x \notin L \end{cases}$$

Nói một cách dễ hiểu hơn, $f_L = f_{r-1}...f_0$ mà ở đó:

$$f_i = \begin{cases} 1 \text{ nếu } p_i \in L, \\ 0 \text{ nếu } p_i \notin L \end{cases}$$

Khi đó, chỉ khi tất cả các vị trí đều trùng với các vị trí 1 véc tơ x nào đó thuộc L thì f_L mới là 1.

Mặt khác, ta lại có các định nghĩa r-phẳng dựa trên ma trận điều kiện.

Định nghĩa 3.13. Xét không gian con V,

$$V = \{x | H.x^T = 0\}$$

Khi đó, r-phẳng $L = a + V$ được định nghĩa bởi $c^T = H.a^T$ và H:

$$\{x | H.x^T = c^T\}$$

Từ định nghĩa này, ta dễ dàng suy ra được bổ đề sau:

Bổ đề 3.14. Hàm chỉ thị của 1 r-phẳng bất kì là 1 đa thức Bool với bậc $m - r$

Chứng minh. Xét dòng H_i nhân với x^T, với c_i là hàng thứ i của c, ta có:

$$h_{i1}x_1 + ... + h_{im}x_m = c_i$$

Từ đó dễ thấy, hàng chỉ thị của vị trí thứ i có dạng:

$$f_i = h_{i1}x_1 + ... + h_{im}x_m + c_i + 1$$

Và theo định nghĩa, ta chỉ ra được

$$f_L(x) = \prod_{i=1}^{m-r} (h_{i1}x_1 + ... + h_{im}x_m + c_i + 1)$$

là hàm chỉ thị của L với bậc là $m - r$ (do c có $m - r$ hàng) □

Từ tính chất trên, ta liên hệ tới mã Reed-Muller qua 2 tính chất:

Tính chất 5. Các phần tử trong $R(r, m)$ là tổ hợp tuyến tính của hàm chỉ thị các s-phẳng với $s \geq m - r$

Chứng minh. Ta sẽ chỉ ra rằng các hàm chỉ thị của các s-phẳng với $s \geq m - r$ có chứa 1 cơ sở của $R(r, m)$, hay nói các khác là chứa các đơn thức Bool
Mặt khác, các đơn thức Bool có dạng $f(x) = x_{i_1}xi_2...x_{i_n}$ lại tương đương với các (m-k)-phẳng $\{x | x_{i_1} = x_{i_2} = ... = x_{i_n} = 1\}$. Mà khi ta nhân 2 đơn thức Bool f_L và $f_{L'}$ là hàm chỉ thị của 2 phẳng L và L' bất kì thì ta sẽ nhận được hàm chỉ thị của $L \cap L'$ là 1 s-phẳng nào đó. Vì vậy, ta có điều phải chứng minh. □

Tính chất 6. Mọi $(r + 1)$-phẳng đều thuộc mã đối ngẫu của $R(r, m)$

Chứng minh. Cho L là 1 không gian con của $\mathbb{F}^n$. Mã đối ngẫu của L là tập hợp tất cả các vector vuông góc với mỗi vector thuộc L, được kí hiệu là $L^\perp$, tức là:

$$\{a.b = 0 \text{ với mọi } b \in L\}$$

Xét ma trận sinh của L là G, với $c \in L$, ta có $c = xG$. Do $0 = cm^t = xGm^t$ nên $Gm^t = 0$, nên ma trận điều kiện của mã đối ngẫu của L là ma trận sinh của L. Do đó $L^\perp$ là mã $R(m - r - 1, m)$ (Bổ đề 3.14), ta có điều phải chứng minh. □

Ví dụ 3.15. Xét mã $R(1,3)$, có:

2-phẳng	Hàm chỉ thị	Đa thức Bool
$\{p_1,p_3,p_5,p_7\}$	10101010	x_0
$\{p_2,p_3,p_6,p_7\}$	11001100	x_1
$\{p_4,p_5,p_6,p_7\}$	11110000	x_2
$\{p_0,p_2,p_4,p_6\}$	01010101	$1+x_0$
$\{p_0,p_l,p_4,p_5\}$	00110011	$1+x_1$
$\{p_0,p_l,p_2,p_3\}$	00001111	$1+x_2$
$\{p_l,p_2,p_5,p_6\}$	01100110	x_0+x_1
$\{p_l,p_3,p_4,p_6\}$	01011010	x_0+x_2
$\{p_2,p_3,p_4,p_5\}$	00111100	x_1+x_2
$\{p_1,p_2,p_4,p_7\}$	10010110	$x_0+x_1+x_2$
$\{p_0,p_3,p_4,p_7\}$	10011001	$1+x_0+x_1$
$\{p_0,p_2,p_5,p_7\}$	10100101	$1+x_1+x_2$
$\{p_0,p_l,p_6,p_7\}$	11000011	$1+x_1+x_2$
$\{p_0,p_3,p_5,p_6\}$	01101001	$1+x_0+x_1+x_2$

3.5 Giải mã Reed-Muller

3.5.1 Các tính chất hình học sử dụng trong giải mã

Tính chất 7. Mỗi s-phẳng L được chứa trong đúng $2^{m-s}-1$ (s+1)-phẳng

Chứng minh. Xét $L=a+V$ với $a\in\mathbb{F}_2^m, dim(V)=s$. Khi đó, nếu $L'=b+V'$ là 1 (r+1)-phẳng chứa L, ta có: $a\in L'=b+V'$ nên $a+v'=b$ với v' nào đó thuộc V'. Khi đó, $L'=a+v'+V'=a+V'$ do $v'inV'$. Do đó, $a=b$ trong mọi trường hợp.

Cho L', L'' là 2 (s+1)-phẳng chứa L với: $\begin{cases} L'=a+(V+<v_0'>) \\ L''=a+(V+<v_0''>) \end{cases}$ Vì vậy, L' = L" sẽ tương đướng với việc $v_0'-v_0''\in V$.

Suy ra, các (s+1)-phẳng chứa L sẽ tương ứng với các lớp kề khác 0 của $\mathbb{F}_2^m$/V So số lớp kề là 2^{m-s} nên có tổng cộng $2^{m-s}-1$ (s+1)-phẳng chứa L □

Tính chất 8. Mỗi điểm $x\notin L$ thì được chứa trong đúng 1 (s+1)-phẳng chứa L

Chứng minh. Giả sử $\begin{cases} x\in a+(V+<u_0>) \\ x\in a+(V+<u_1>) \end{cases}$ nên x có dạng $a+v_0+u_0$ và $a+v_1+u_1$ với $v_0,v_1\in V$. Từ đó, ta có $u_0-u_1=v_0-v_1\in V$ nên u_0,u_1 thuộc cùng lớp kề, nên 2 (s+1)-phẳng $(V+<u_0>)$ và $(V+<u_1>)$ là 1. □

Tính chất 9. Nếu số lỗi nhỏ hơn số lỗi tối đa có thể sửa được thì tính chẵn lẻ của 1 s-phẳng bằng phần đông tính chẵn lẻ của các (s+1)-phẳng chứa nó $(s\le r-1)$

Do số lỗi trong (s+1)-phẳng tối đa là 2^{m-r} nhỏ hơn một nửa của số (s+1)-phẳng chứa L là $2^{m-s}-1$, mà theo định lí 2 ta có các lỗi không thuộc L sẽ nằm ở duy nhất 1 (s+1)-phẳng chứa L, nên số (s+1)-phẳng không chứa lỗi sẽ lớn hơn số (s+1) phẳng chứa lỗi. Vì vậy, tính chẵn lẻ của s-phẳng sẽ bằng phần đông (chẵn hoặc lẻ) của (s+1)-phẳng.

3.5.2 Mô hình giải mã

- *Bước 1:* Khi nhận được w, xác định tính chẵn/lẻ của (r+1)-phẳng L.
  Ta có các vị trí của L có chẵn lỗi khi và chỉ khi $w.f_L=0$ và có lẻ lỗi khi và chỉ khi $w.f_L=1$
- *Bước 2:* Với $s=r,r-1,...,0$, ta xác định tính chẵn/lẻ của s-phẳng L từ phần đông (s+1)-phẳng chứa L
- *Bước 3:* Sửa bit thứ i của w khi và chỉ khi 0-phẳng của vị trí i là lẻ.

Ví dụ 3.16. Cho mã $R(1,3)$ với từ mã nhận được là 11101010.
Bước 1: Xét tính chẵn/lẻ của các 2-phẳng

2-phẳng	Hàm chỉ thị	Tính chẵn/lẻ
$\{p_1, p_3, p_5, p_7\}$	10101010	chẵn
$\{p_2, p_3, p_6, p_7\}$	11001100	lẻ
$\{p_4, \boldsymbol{p_5}, \boldsymbol{p_6}, p_7\}$	11110000	lẻ
$\{p_0, p_2, p_4, p_6\}$	01010101	lẻ
$\{p_0, p_l, p_4, p_5\}$	00110011	chẵn
$\{p_0, p_l, p_2, p_3\}$	00001111	chẵn
$\{p_l, p_2, \boldsymbol{p_5}, \boldsymbol{p_6}\}$	01100110	lẻ
$\{p_l, p_3, p_4, p_6\}$	01011010	lẻ
$\{p_2, p_3, p_4, p_5\}$	00111100	chẵn
$\{p_1, p_2, p_4, p_7\}$	10010110	chẵn
$\{p_0, p_3, p_4, p_7\}$	10011001	chẵn
$\{p_0, p_2, p_5, p_7\}$	10100101	lẻ
$\{p_0, p_l, p_6, p_7\}$	11000011	chẵn
$\{p_0, p_3, \boldsymbol{p_5}, \boldsymbol{p_6}\}$	01101001	lẻ

Bước 2: Xác định tính chẵn lẻ của các 1-phẳng bằng cách lấy phần đông

2-phẳng	Tính chẵn/lẻ	2-phẳng	Tính chẵn/lẻ
$\{p_0, p_1\}$	chẵn	$\{p_2, p_4\}$	chẵn
$\{p_0, p_2\}$	chẵn	$\{p_2, p_5\}$	chẵn
$\{p_0, p_3\}$	chẵn	$\{p_2, \boldsymbol{p}_6\}$	lẻ
$\{p_0, p_4\}$	chẵn	$\{p_2, p_7\}$	chẵn
$\{p_0, p_5\}$	chẵn	$\{p_3, p_4\}$	chẵn
$\{p_0, \boldsymbol{p_6}\}$	lẻ	$\{p_3, p_5\}$	chẵn
$\{p_0, p_7\}$	chẵn	$\{p_3, \boldsymbol{p_6}\}$	lẻ
$\{p_1, p_2\}$	chẵn	$\{p_3, p_7\}$	chẵn
$\{p_1, p_3\}$	chẵn	$\{p_4, p_5\}$	chẵn
$\{p_1, p_4\}$	chẵn	$\{p_4, \boldsymbol{p_6}\}$	lẻ
$\{p_1, p_5\}$	chẵn	$\{p_4, p_7\}$	chẵn
$\{p_1, \boldsymbol{p_6}\}$	chẵn	$\{p_5, \boldsymbol{p_6}\}$	lẻ
$\{p_1, p_7\}$	chẵn	$\{p_5, p_7\}$	chẵn
$\{p_2, p_3\}$	chẵn	$\{\boldsymbol{p_6}, p_7\}$	lẻ

Bước 3: Xác định tính chẵn/lẻ của các 0-phẳng hay các vị trí p_i:

0-phẳng	Tính chẵn lẻ
p_0	chẵn
p_1	chẵn
p_2	chẵn
p_3	chẵn
p_4	chẵn
p_5	chẵn
$\boldsymbol{p_6}$	lẻ
p_7	chẵn

Vậy, từ mã sai ở vị trí p_6, từ mã đúng là 10101010 ứng với biểu diễn đa thức Bool là $1 + x_1$

4 Mã vòng

4.1 Mã vòng và tính chất

4.1.1 Định nghĩa

Định nghĩa 4.1. Cho véc-tơ $w = a_0 a_1 \dots a_{n-1} \in \mathbb{F}_q^n$. Ta xét phép tịnh tiến vòng tròn như sau

$$\sigma : \mathbb{F}_q^n \to \mathbb{F}_q^n, \sigma(w) = a_{n-1} a_0 \dots a_{n-2}.$$

Ví dụ 4.2.

$$\sigma(1001) = 1100$$

$$\sigma(111001) = 111100$$

Định nghĩa 4.3. Mã tuyến tính C được gọi là mã vòng nếu với mọi $w \in C$, ta có $\sigma(w) \in C$.

4.1.2 Tính chất

Mỗi từ mã $w = a_0a_1 \dots a_{n-1}$ được gán với một đa thức

$$w(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}.$$

Tính chất 10. Cho từ mã g, đa thức $q(x)$ sao cho $\deg(qg) < n$, thì $q(x)g(x)$ là từ mã.

Chứng minh. Phép tịnh tiến vòng tròn tương đương với việc nhân x với $w(x)$ rồi trừ đi $a_{n-1}(x^n - 1)$:

$$x(a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) - a_{n-1}(x^n - 1) = a_{n-1} + a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1},$$

Do $\deg(qg) < n$ nên khi ta nhân $g(x)$ với từng số hạng trong $q(x)$ thì ta sẽ có đa thức $q(x)g(x)$ ứng với tổng các từ mã do đó $q(x)g(x)$ là một từ mã. □

Tính chất 11. Cho từ mã g, với mọi đa thức $q(x)$ và $q(x)g(x) = p(x)(x^n - 1) + r(x), \deg(r) < n$ ta có $r(x)$ là từ mã.

Chứng minh.

$$\sigma(w)(x) = a_{n-1} + a_0x + \cdots + a_{n-2}x^{n-1} = xw(x) - a_{n-1}(x^n - 1).$$

Khi ta nhân $g(x)$ với từng số hạng trong $q(x)$, với $\deg(qg) < n$ thì tính chất đúng như chứng minh ở trên.
Với $\deg(qg) > n$ thì đa thức dư của $g(x)q(x)$ khi chia cho $x^n - 1$ ứng với tổng của đa thức dư của mỗi tích $g(x)$ với mỗi số hạng trong $q(x)$ khi chia cho $x^n - 1$ (mỗi đa thức dư ở đây là các mã vòng nhờ tính chất vòng)
Do đó $r(x)$ là từ mã. □

4.1.3 Ma trận sinh

G là ma trận sinh của mã vòng (n, k) tuyến tính C. Phép khử Gauss trên hàng đưa G về dạng:

$$G = \begin{pmatrix} c_0 & \dots & & & \\ 0 & c_1 & \dots & & \\ \dots & & & & \\ 0 & \dots & 0 & c_{k-1} & \dots \end{pmatrix}$$

Hàng cuối cùng có $k - 1$ số 0 đầu tiên tương ứng với đa thức:

$$a_{k-1}x^{k-1} + \cdots + a_{n-1}x^{n-1} = x_{k-1}(a^{k-1} + \cdots + a_{n-1}x^{n-k}) = x^{k-1}g(x)$$

- Ta có $g, xg, x^2g, \dots, x^{k-1}g$ là một hệ độc lập tuyến tính (Mã vòng), có k phần tử, do đó tạo thành một cơ sở.
- Nếu $deg(g) < n - k$, ta thêm x^kg vào tập trên vẫn tạo thành một hệ độc lập tuyến tính. Vậy $deg(g) = n - k$
- Ta có thể tạo một ma trận sinh từ g như sau:

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \dots \\ x^{k-1}g(x) \end{pmatrix} = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-k} & 0 & \dots & 0 \\ 0 & a_0 & \dots & a_{n-k} & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \dots & \\ 0 & 0 & \dots & 0 & a_0 & \dots & a_{n-k} \end{pmatrix}$$

Trong đó $g(x) = a_0 + \cdots + a_{n-k}x^{n-k}$ được gọi là đa thức sinh của C.

Tính chất 12. Mọi từ mã thuộc C có thể viết dưới dạng $q(x)g(x)$.

Ví dụ 4.4. Mã $Ham(7,4)$ là mã vòng, với đa thức sinh $g(x) = 1 + x + x^3$ có ma trận sinh:

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

Ví dụ 4.5. Mã chẵn lẻ là mã vòng, với đa thức sinh $g(x) = 1 + x$ và ma trận sinh sau:

$$G = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & 1 \end{pmatrix}.$$

Tính chất 13. Đa thức sinh là ước của x^{n-1}, và mọi ước của x^{n-1} sinh ra một mã vòng độ dài n.

Chứng minh. Giả sử $g(x)$ là đa thức sinh. Ta có:

$$x^{n-1} = q(x)g(x) + r(x), deg(r) < deg(g)$$

Lấy đồng dư mod x^{n-1} cả hai vế, ta có:

$$0 = q'(x) + r(x)$$

Vì $q'(x)$ là từ mã, nên $r(x)$ cũng là từ mã, suy ra $r(x) = g(x)t(x)$. Mà $deg(r) < deg(g)$, vậy $r(x) = 0$.
Ngược lại nếu $g(x)$ là ước của x^{n-1}, ta sinh ra một mã tuyến tính gồm các từ mã $q(x)g(x)$ với $deg(q) < ndeg(g)$. □

4.1.4 Mã hóa

- Mã hóa thông thường: Cho thông điệp $u \to$ từ mã:

  $$x = uG = (u_0 + u_1x^1 + \cdots + u_{k-1}x^{k-1})g(x) = u(x)g(x).$$

  Ví dụ: Mã $Ham(7,4)$ mã hóa 1001 thành 1100101 ứng với đa thức $1 + x + x^4 + x^6$.

- Mã hóa hệ thống: Ta viết thông điệp u thành đa thức sau:

  $$u(x) = u_{k-1}x^{n-1} + u_{k-2}x^{n-2} + \cdots + u_0x^{n-k}$$

  Ta tính được $r(x)$ là đa thức dư của $u(x)$ khi chia cho $g(x)$. Khi đó thông điệp u $\to$ từ mã:

  $$x = u(x) - r(x)$$

  Ví dụ: Mã $Ham(7,4)$ với đa thức sinh $g(x) = 1 + x + x^3$, mã hóa thông điệp 1001 thành 0111001 ứng với đa thức $x + x^2 + x^3 + x^6$.

4.1.5 Ma trận điều kiện

Tính chất 14. Nếu $g(x)$ là đa thức sinh của mã vòng C độ dài n, ta gọi đa thức sau là đa thức điều kiện của mã

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + \cdots + h_kx^k.$$

Chứng minh. Đặt H_i là hàng thứ i của H, $G_i$là hàng thứ i của G. Ta có:

$$H_1.G_1^t = \sum_{i=0}^{n-1} h_i g_{n-i-1}$$

Đây là hệ số bậc $n-1$ của hg, do đó bằng 0. Lập luận tương tự cho các hàng khác, ta có $H_i.G_j^T = 0$.
Ma trận H có $n-k$ hàng độc lập tuyến tính, do đó nó là ma trận điều kiện của C. □

Tính chất 15. Mã đối ngẫu của mã vòng C là một mã vòng với đa thức sinh $x^k h(x^{-1})$.

Mệnh đề 4.6. Ma trận điều kiện của C có dạng

$$H = \begin{pmatrix} x^{n-1}h(x^{-1}) \\ x^{n-2}h(x^{-1}) \\ \cdots \\ x^k h(x^{-1}) \end{pmatrix} = \begin{pmatrix} 0 & \dots & 0 & h_k & \dots & h_0 \\ 0 & \dots & h_k & \dots & h_0 & 0 \\ \vdots & & & & & \vdots \\ h_k & \dots & h_0 & 0 & \dots & 0 \end{pmatrix}.$$

4.2 Mã sữa cụm lỗi

Định nghĩa 4.7. Cụm lỗi độ dài l là véc-tơ có các kí tự khác 0 nằm trong l vị trí liên tiếp theo vòng tròn.

Ví dụ 4.8. Véc-tơ 0011010 là cụm lỗi độ dài 4.

Ví dụ 4.9. Véc-tơ 1100001 là cụm lỗi độ dài 3.

Tính chất 16. Một mã (n, k) tuyến tính có thể phát hiện cụm lỗi độ dài l nếu không có từ mã nào là cụm lỗi có độ dài l.

Tính chất 17. Nếu mã (n, k) tuyến tính C có thể phát hiện cụm lỗi độ dài l, ta có $n - k \geq l$.

Chứng minh. Số các cụm lỗi độ dài l với các vị trí khác 0 nằm trong l vị trí đầu tiên là r^l, và tổng của hai cụm lỗi nãy cũng là một cụm lỗi độ dài l. Các cụm lỗi này thuộc các lớp kề khác nhau, do đó số phần từ nhỏ hơn số syndrome là r^{n-k}. □

Tính chất 18. Mọi mã vòng (n, k) đều có thể phát hiện cụm lỗi độ dài $n - k$.

Chứng minh. Nếu có một cụm lỗi $e(x)$ độ dài $n - k$ là từ mã, khi tịnh tiến vòng tròn e vẫn được một từ mã.
Tịnh tiến đến khi được véc-tơ $[e_0, e_1, \dots, e_{n-k-1}, 0, \dots, 0]$, đây là đa thức có bậc nhỏ hơn nk, tức là nhỏ hơn bậc của đa thức sinh, suy ra mâu thuẫn. □

Tính chất 19. Mã (n, k) tuyến tính có thể sửa cụm lỗi có độ dài l nếu hai cụm lỗi độ dài l khác nhau thuộc hai lớp kề khác nhau.

Tính chất 20. Nếu mã (n, k) tuyến tính sửa được cụm lỗi độ dài l, ta có $n - k \geq 2l$.

Chứng minh. Một cụm lỗi độ dài $2l$ có thể phân tích thành hiệu của hai cụm l lỗi. Do hai cụm lỗi thuộc hai lớp kề khác nhau nên hiệu của chúng không phải là từ mã.
Hiệu của 2 cụm lỗi độ dài $2l$ với các kí tự khác 0 nằm trong $2l$ kí tự đầu tiên là một cụm lỗi độ dài $2l$, nên không phải từ mã, do đó 2 cụm lỗi độ dài này thuộc hai lớp kề khác nhau. Số các cụm lỗi như vậy là r^{2l}, do đó $r^{2l} \leq r^{n-k}$ hay $2l \leq n - k$. □

Ví dụ 4.10. Mã Hamming bỏ bớt $(7, 3)$ có thể sửa được cụm lỗi độ dài 2.
Đây là mã vòng với đa thức sinh $g(x) = 1 + x^2 + x^3 + x^4$. Ta có thể kiểm tra tính chất sửa lỗi theo định nghĩa bằng cách kiểm tra các véc-tơ

$$1100000 - 0011000 = 1111000$$
$$1100000 - 0001100 = 1101100$$
$$1100000 - 0000110 = 1100110$$
$$1100000 - 0000011 = 1100011$$

Không véc-tơ nào bên trên là từ mã. Do đó mã này sửa được cụm lỗi độ dài 2.

Tính chất 21. Một mã có thể sửa cụm lỗi có thể tạo ra bằng phương pháp xen kẽ.

Mệnh đề 4.11. Giả sử mã (n, k) tuyến tính có thể sửa cụm l lỗi. Ta tạo mã (nj, kj) bằng cách lấy j từ mã bất kì và sắp xếp lại các kí tự xen kẽ nhau.

$$\begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & & & \vdots \\ p_{j1} & p_{j2} & \dots & p_{jn} \end{pmatrix}$$

Hệ quả 4.12. Xen kẽ một mã vòng sẽ được một mã vòng mới.

Chứng minh. Giả sử mã (n, k) tuyến tính có thể sửa cụm l lỗi. Ta tạo mã (nj, kj) bằng cách lấy j từ mã bất kì và sắp xếp lại các kí tự xen kẽ nhau.
$\rightarrow$ Từ các từ mã ban đầu: $p_i = (p_{i1}, \ldots, p_{in})$ ta sắp xếp xen kẽ j từ mã bất kỳ $\rightarrow p(x) = (p_{11}, p_{21}, \ldots, p_{j1}, \ldots, p_{1n}, p_{2n}, \ldots, p_{jn})$
Dạng đa thức:

$$\begin{aligned} p(x) &= (p_{11} + p_{12}x^j + \cdots + p_{1n}x^{j(n-1)}) + \cdots + x^{j-1}(p_{j1} + \cdots + (p_{jn}x^{j(n-1)}) \\ &= \sum_{i=1}^{j} x^{i-1} p_i(x^j) \end{aligned}$$

Vì các $p_i(x^j)$ chia hết cho $g(x^j)$ nên $p(x)$ chia hết cho $g(x^j) \rightarrow$ mã xen kẽ là mã vòng với đa thức sinh là $g(x^j)$. □

Ví dụ 4.13. Xét mã Hamming bỏ bớt $(7, 3)$ với đa thức sinh $g(x) = 1 + x + x^2 + x^3$
Giả sử ta cần truyền 2 từ mã 1110010 và 0010111. Nếu ta truyền theo dạng 1110010|0010111, cách làm này chỉ sửa được cụm 2 lỗi.
Phương pháp xen kẽ truyền 2 từ mã này theo dạng sau: 10|10|11|00|01|11|01.Cách làm này sửa được cụm 4 lỗi. Từ mã này thuộc mã vòng $(14, 6)$.

4.3 Giải mã vòng

4.3.1 Giải mã syndrome

- Với mỗi đa thức $p(x)$, phần dư của $p(x)$ khi chia cho $g(x)$ được gọi là đa thức syndrome.
  Hai đa thức $p(x)$ và $p(x)$ có cùng syndrome $\iff p(x) - q(x) = t(x)g(x)$.
- Giải mã syndrome: Véc-tơ lỗi sẽ ứng với đa thức có cùng đa thức syndrome với $p(x)$ và có trọng số nhỏ nhất.

Ví dụ 4.14. Mã $Ham(7, 4)$ với đa thức sinh là $g(x) = 1 + x + x^3$. Véc-tơ 1011001 có syndrome là $x + 1$.
Ta liệt kê các phần tử dẫn cùng syndrome tương ứng, đa thức x^3 là đa thức duy nhất có syndrome là $x + 1$.
Vậy bit vị trí thứ 4 bị lỗi $\rightarrow$ 1010001

4.3.2 Giải mã Meggit

- Cách giải mã trên cần liệt kê tất cả các đa thức và tính syndrome. Ta có thể giải mã hiệu quả hơn.
- Vì đa thức syndrome sau khi tịnh tiến vòng tròn có thể đạt được bằng cách tịnh tiến vòng tròn rồi tính syndrome, ta chỉ cần quan tâm đến các đa thức có cùng một bậc.

Mệnh đề 4.15. Thuật toán:

- Bước 1:Liệt kê các đa thức bậc $n - 1$ cùng syndrome của chúng.
- Bước 2: Với mỗi bước, nếu syndrome của véc-tơ có trong danh sách trên, đa thức đó là véc-tơ lỗi sau đó ta tịnh tiến ngược trở lại. Nếu không đến Bước 3.
- Bước 3: Tịnh tiến vòng tròn véc-tơ, về lại Bước 2.

Ví dụ 4.16. Ta cũng xét ví dụ ở trên: Cho mã $Ham(7, 4)$ với đa thức sinh $1+x+x^3$, tìm bit bị lỗi của véc-tơ 1011001
Vì đây là mã hamming nên ta sẽ chỉ xét đa thức bậc 6 là x^6 và có syndrome là $x^2 + 1$.
Ta tính véc-tơ 1011001 có syndrome là x+1, khi đó ta tịnh tiến vòng tròn vec-tơ này đến lúc thu được syndrome là $x^2 + 1 \rightarrow 3$ lần
Vậy véc-tơ lỗi là $x^3 \rightarrow$ lỗi tại bit thứ 4 $\rightarrow$ 1010001

4.3.3 Giải mã bằng bẫy lỗi

Giải mã Meggit: chúng ta phải liệt kê hết các đa thức bậc $n-1$ và tính các syndrome của chúng. Sau đây giải mã bằng bẫy lỗi sẽ giúp ta tối ưu hơn.

- Giả sử mã C sửa được t lỗi và có không quá t vị trí bị sai. Nếu syndrome của véc-tơ có trọng không quá t, nó là đa thức ứng với véc-tơ lỗi.
- Nếu lỗi e là cụm độ dài $n-k$, có một phép tịnh tiến vòng tròn khiến syndrome có trọng không quá t.

Mệnh đề 4.17. Thuật toán:

- Bước 1: tính syndrome của véc-tơ. Nếu syndrome có trọng không quá t thì đây chính là véc-tơ lỗi, còn nếu không đi tới bước 2.
- Bước 2: tịnh tiến vòng tròn véc-tơ. Quay lại bước 1.

Ví dụ 4.18. Ta tiếp tục xét ví dụ như 2 cách giải mã trên: Mã $Ham(7,4)$ với đa thức sinh là $g(x) = 1 + x + x^3$. Véc-tơ 1011001 có syndrome là $x + 1$.
Ta tịnh tiến vòng tròn đến khi thu được véc-tơ 1001101 có syndrome là 1 hay đây chính là véc-tơ lỗi nên 1001101 $\rightarrow$ 0001101 do đó tính tiến ngược lại ta thu được 1010001

5 Trường hữu hạn

5.1 Trường hữu hạn

Định nghĩa 5.1. Trường hữu hạn là trường có hữu hạn phần tử

Ví dụ 5.2. Cho số nguyên tố p, trường $_p$ là trường gồm p phần từ $\{0, 1, \ldots, p-1\}$, với phép cộng và phép nhân lấy đồng dư mô đun p.

Ta sẽ chứng minh mọi trường hữu hạn đều có p^k phần tử với p nguyên tố, và chỉ có duy nhất một trường có p^k phần tử, kí hiệu là $\mathbb{F}_{p^k}$.

5.2 Thuật toán Euclid mở rộng

Cho hai đa thức f, g $\in \mathbb{K}$. Suy ra,

1. Tìm được $gcd(f, g)$
2. Tồn tại hai đa thức u, v $\in \mathbb{K}$ thỏa mãn
$$f * u + g * v = gcd(f, g)$$

Chứng minh. Không mất tính tổng quát, deg f $\geq$ deg g. Xét hai dãy đa thức (a_n) thỏa mãn a_0 =f và $a_1 = g$ và a_n là đa thức dư của phép chia a_{n-2} cho a_{n-1} (với n geq 2)

1. Xét phương trình trên, có thể thấy deg $a_n <$ deg a_{n-1} , vậy tồn tại N thỏa mãn deg a_N =0. Khi đó, nếu a_N =0, suy ra $gcd(f, g) = a_{N-1}$. Ngược lại, nếu a_N khác 0 thì $gcd(f, g) = 1$.
2. Ta xét dãy (q_n) thỏa mãn q_i là số thương của phép chia a_{i-1} cho a_i Xét hai dãy đa thức (u_n) và (v_n) thỏa mãn
$$\begin{cases} u_0 = 1, v_0 = 1 \\ u_1 = 0, v_1 = 1 \\ u_{n+1} = u_{n-1} - u_n * q_n \text{nếu } n \geq 1 \\ v_{n+1} = v_{n-1} - v_n * q_n \text{nếu } n \geq 1 \end{cases}$$
Xét đẳng thức
$$u_i * f + v_i * g = a_i \tag{5.1}$$

Nhận thấy với $u_0 * f + v_0 * g = f = a_0$ và $u_1 * f + v_1 * g = g = a_1$. Ta có thể giả sử quy nạp rằng với số $k \geq 1$ thỏa mãn (1) đúng với i từ 1 đến k. Ta sẽ chứng minh (1) đúng với $i = k + 1$. Thật vậy,

$$\begin{aligned} u_{k+1} * f + v_{k+1} * g &= (u_{k-1} - q_k * u_k) * f + (v_{k-1} - q_k * v_k) * g \\ &= (u_{k-1} * f + v_{k-1} * g) - q_n * (u_k * f + v_k * g) \\ &= a_{k-1} - q_k.a_k \\ &= a_{k+1} \end{aligned}$$

Vậy khi $i = k + 1$, (1) vẫn đúng. Từ đó theo giả thiết quy nạp, ta có điều thỏa mãn. Chọn $u = n_N$ và $v = v_N$, ta sẽ có hai đa thức thỏa mãn

□

5.3 Xây dựng trường hữu hạn

Xét một trường $\mathbb{K}$ và đa thức $f(x) \in \mathbb{K}[x]$. Ta xét một vành thương $\mathbb{K}[x]/f(x)$ được định nghĩa như sau

1. phần tử là các đa thức có cùng nhóm kề trên $f(x)$. Nói cách khác, với hai đa thức $m(x)$ và $n(x)$ chung một vành thương thì $a(x) - b(x)$ chia hết cho f(x)
2. Phép cộng và phép nhân được thực hiện trên $f(x)$

Hệ quả 5.3. Các vành thương có phần tử dẫn là các đa thức có bậc nhỏ hơn deg f

Ta sẽ xây dựng trường hữu hạn thông qua vành thương. Trước hết ta có định nghĩa sau

Định nghĩa 5.4. Đa thức bất khả quy trên trường $\mathbb{K}[x]$ là đa thức không thể tách thành tích của hai đa thức bậc khác hằng (deg ≥ 1)

Ví dụ 5.5. Các đa thức sau là bất khả quy trên trường $\mathbb{F}_2$ là $x^2 + x + 1$, $x^3 + x + 1$, $x^3 + x^2 + 1$, ….

Định lý 5.6. Nếu đa thức $f(x)$ là một đa thức bất khả quy thì vành thương $\mathbb{K}[x]/f(x)$ là một trường.

Chứng minh. Ta cần chứng minh vành thương này có phần tử nghich đảo.
Xét đa thức $a(x) \in K[x]$ và $f(x) \nmid a(x)$. Do f(x) là đa thức bất khả quy, ta có gcd(f,a)=1
Sử dụng thuật toán Euclid mở rộng, tồn tại hai đa thức u(x), v(x) thỏa mãn

$$u * f + v * a = 1$$

Suy ra mọi da thức $a(x) \in K[x]$ tồn tại một phần tử nghịch đảo theo mod $f(x)$ □

Định lý trên chỉ ra mọi trường hữu hạn đều có p^k phần tử, tương ứng với số đa thức có hệ số thuộc $_p$ và có bậc nhỏ hơn k. Hơn nữa, ta có định lý sau.

Định lý 5.7. Với số nguyên tố p và số nguyên dương k, tồn tại duy nhất một trường có p^k phần tử.

5.4 Cấp và phần tử sinh

Xét q = p^m, với p là một số nguyên tố
Xét a $\in \mathbb{F}_q^\times$
Ta gọi *cấp* của a là số k nhỏ nhất thỏa mãn a^k=1
Ta gọi một *phần tử sinh* trong $\mathbb{F}_q^\times$ là phần tử có cấp là $q - 1$

Định lý 5.8. Mọi trường hữu hạn $\mathbb{F}_r$ đều có phần tử sinh

Chứng minh. Xét a là phần tử trong $\mathbb{F}_r$ có cấp lớn nhất. Không mất tính tổng quát, giả sử cấp của a là n
Dễ thấy $n \leq r - 1$. Ta cần chứng minh $n \geq r - 1$ thì ta có điều phải chứng minh.

Bổ đề 5.9. Cấp của mọi phần tử khác trong trường đều là cấp của n

Chứng minh. Xét s là cấp của phần tử b bất kỳ. Xét phân tích nguyên tố của s

$$s = p_1^{i_1} * p_2^{i_2} \dots$$

Xét phân tích của n như sau

$$n = p_1^t * n'$$

với $p_1 \nmid n'$.
Đặt $s' = s/p_1^{i_1}$. Ta xét một phần tử c có dạng

$$c = a^{p_1^t} * b^{s'}$$

Ta sẽ chứng minh c có cấp là $m = p_1^{i_1} * n'$. Để chứng minh điều này, ta cần chứng minh 2 điều

1. c^m=1
   Ta có
   $$c^m = a^{p_1^t m} * b^{s'm} = a^{p_1^{i_1} p_1^t n'} * b^{s' p_1^{i_1} n'} = a^{n p_1^{i_1}} * b^{s n'} = 1^{p_1^{i_1}} * 1^{n'} = 1$$

2. Nếu $c^{m'}$=1 thì $m' \geq m$

   $$1 = (c^{m'})^{n'} = a^{p_1^t m' n'} * b^{s' m' n'} = (a^n)^{m'} * b^{s' m' n'} = b^{s' m' n'}$$

   Suy ra $m'n' \vdots p_1^{i_1}$, vậy $m' \vdots p_1^{i_1}$ $gcd(n', p)$=1,
   Mặt khác,
   $$1 = (c^{m'})^{p_1^{i_1}} = a^{p_1^t p_1^{i_1} m'} * b^{p_1^{i_1} s' m'} = a^{p_1^t p_1^{i_1} m'} * b^{s m'} = a^{p_1^t p_1^{i_1} m'}$$

   Suy ra $p_1^t p_1^{i_1} m' \vdots n$, vậy $m \vdots n'$ (do $gcd(p, n')$=1) Từ hai điều trên, ta nhận thấy $m' \vdots p_1^{i_1} * n'$, tức $m' \vdots m$, suy ra $m' \geq m$

Do n là cấp lớn nhất => $n \geq m$ => $p_1^t * n' \geq p_1^{i_1} * n'$ => $t \geq i_1$ => $n \vdots p_1^{i_1}$ => $n \vdots s$ □

Quay trở lại bài toán, ta xét phương trình $x^n - 1$=0.Qua bổ đề, nhận thấy mọi b $\in \mathbb{F}_r$ là nghiệm , suy ra $n \geq r - 1$. □

5.5 Đa thức tối thiểu

Xét một phần tử đại số a của mở rộng trường $\mathbb{L}$ của $\mathbb{K}$, tồn tại một đa thức f có bậc nhỏ nhất thỏa mãn $f(a) = 0$. Đây còn gọi là *đa thức cực tiểu* của a. f là một đa thức bất khả quy

Chứng minh. Giả sử đa thức f không bất khả quy, suy ra tồn tại hai đa thức g và h thuộc $\mathbb{K}_{[x]}$ thỏa mãn

$$f = g * h$$

Do f(a)= 0, nên thay x= a suy ra hoặc g(a)=0 hoặc h(a)=0. Mặt khác, deg g, deg h < deg f nên luôn tồn tại một đa thức lấy a làm nghiệm có bậc nhỏ hơn f (Điều này là vô lý do khái niệm của đa thức cực tiểu của a) □

6 Mã BCH sửa hai lỗi

6.1 Mã BCH sửa hai lỗi: Mở đầu

6.1.1 Định Nghĩa

Xét a là một phần tử cấp n của mở rông trường F_2, ta có mã BCH sửa hai lỗi là một mã vòng gồm các từ mã w thỏa mãn

$$w(a) = w(a^3) = 0$$

6.1.2 Tính chất

1. Đa thức sịnh
   Xét $M(x)$ và $N(x)$ là hai đa thức cực tiểu cho hai phần tử a và a^3. Khi đó, đa thức sinh của mã vòng này là $lcm(M(x), N(x))$

2. Ma trận điểu kiện
   Ma trận điểu kiện H của mã này sẽ có dạng như sau:

$$H = \begin{bmatrix} G \\ T \end{bmatrix} = \begin{bmatrix} 1 & a & a^2 \dots a^{(n-1)} \\ 1 & a^3 & a^6 \dots a^{3(n-1)} \end{bmatrix}$$

   Với G là ma trận có các vector cột là các hệ số của các phần tử thuộc $F_2[x]$/M(x) còn T ma trận có các vector cột là hệ số của các phần tử thuộc $F_2[x]$/N[x]

6.1.3 Ví dụ

Ví dụ : Xét phần tử sinh β trên mở rộng trường $\mathbb{F}_{16}$ có đa thức cực tiểu là G(x)= $1+x+x^4$.Như vậy đa thức cực tiểu cho β^3 là T(x)= $1+ x+x^2+x^3+x^4$.Suy ra ta có thể có ma trận điều kiện sau :

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

6.2 Mã BCH sửa hai lỗi: Giải mã

Giả sử ta nhận được một mã w= w_1 w_2..... w_n có vị trí i và j bị lỗi.

6.2.1 Các cách tìm đa thức Syndrome

Xét phần tử a và ma trận tổng quát như định nghĩa , ta có hai biểu diễn của syndrome:

1. Cách 1: Xét theo vị trí của lỗi
   Xét vị trí i và j bị lỗi, đa thức syndrome là

$$e(x) = x^i + x^j$$

2. Cách 2 : Xét theo ma trận điểu kiện
   Xét ma trận điểu kiện H nhân với mã w

$$\begin{bmatrix} 1 & a & a^2 \dots a^{(n-1)} \\ 1 & a^3 & a^6 \dots a^{3(n-1)} \end{bmatrix} * \begin{bmatrix} w_1 \\ w_2 \\ \cdots \\ w_n \end{bmatrix} = \begin{bmatrix} s_1 \\ s_3 \end{bmatrix}$$

   Vậy

$$s_1 = w_1 + w_2 * a + \cdots + w_n * a^{(n-1)}$$
$$s_3 = w_1 + w_2 * a^3 + \cdots + w_n * a^{3(n-1)}$$

6.2.2 Giải mã

Sau khi ta có hai cách biểu diễn đa thức syndrome, ta có thể giải ra theo một hệ phương trình hai ẩn để tìm ra đề bài.

$$e(a) = s_1$$

$$e_(a^3) = s_3$$

Qua đó, ta có

$$s_1^3 = a^{3i} + a^{2i+j} + a^{i+2i} + a^{3j} = s_3 + a^i a^j s_1$$

Suy ra

$$a^i a^j = (s_1^3 - s_3)s_1^{-1}$$

Như vậy, a^i và a^j là nghiệm của phương trình sau

$$x^2 + s_1 x + s_1^2 + s_3 s_1^{-1} = 0 \tag{6.1}$$

6.3 Mã BCH sửa hai lỗi: Thuật toán

Sau khi tính được a^i và a^j, ta có những khả năng sau

- nếu $s_1 = a^i$ và $s_3 = a^{3i}$, sửa bước i và kết thúc thuật toán
- nếu phương trình (1) có 2 nghiệm a^i và a^j, sửa hai vị trí i và j
- nếu phương trình (1) vô nghiệm, có nhiều hơn hai lỗi

7 Mã BCH tổng quát

7.1 Định nghĩa mã BCH tổng quát

Định nghĩa 7.1. Cho một trường $\mathbb{F}_q$ và số nguyên dương n thỏa mãn $gcd(n, q) = 1$.
Mã **BCH (Bose–Chaudhuri–Hocquenghem)** sửa t lỗi với độ dài n là các mã $w \in \mathbb{F}_q$ thỏa mãn

$$w(\beta) = w(\beta^2) = \cdots = w(\beta^{2t-1}) = w(\beta^{2t}) = 0,$$

với β là một phần tử bậc n trong một mở rộng trường nào đó của $\mathbb{F}_q$.

Ví dụ 7.2. Khi xét trên trường $\mathbb{F}_2$ với $n = 15,\ t = 2$. khi đó nếu xét β là một phần tử sinh của $\mathbb{F}_{16}^{\times}$. Ta thu được một mã $(15, 7)$ BCH sửa được 2 lỗi với ma trận điều kiện

$$H = \begin{pmatrix} 1 & \beta & \cdots & \beta^{14} \\ 1 & \beta^3 & \cdots & \beta^{42} \end{pmatrix}$$

cỡ 8×15 hay ma trận sinh G có kích cỡ 7×15
Ta lại thấy được $w(\beta) = w(\beta^2) = w(\beta^3) = w(\beta^4) = 0$ nên $w(\beta) = w(\beta^3) = 0$

Ví dụ 7.3. Xét một mã nhị phân BCH sửa 3 lỗi thu bởi phần tử sinh β thỏa mãn

$$w(\beta) = w(\beta^3) = w(\beta^5)$$

Khi đó, nếu $M_i(x)$ là đa thức tối tiểu của β^i thì

$$M_1(x) = x^4 + x + 1$$
$$M_3(x) = x^4 + x^3 + x^2 + x + 1$$
$$M_5(x) = x^2 + x + 1$$

Ta sẽ thu được mã vòng C có đa thức sinh $g(x) = M_1(x)M_3(x)M_5(x)$ có bậc 10 nên C là mã vòng $(15, 5)$

Ta có một định nghĩa của mã BCH nguyên thủy

Định nghĩa 7.4. Một mã BCH được gọi là **nguyên thủy** nếu $n = q^m - 1$ với m nào đó. Thường mã này được tạo từ phần tử β là 1 phần tử nguyên thủy của một mở rộng trường nào đó

Ví dụ 7.5. Xét các mã có độ dài $n = 2^m - 1$ như các ví dụ bên trên. Khi đó mã $(15, 7)$ BCH là một mã BCH nguyên thủy

7.2 Tính chất

Ta có một số tính chất của mã BCH như sau:

Tính chất 22. Xét một mã BCH C sửa t lỗi với $\beta \in \mathbb{F}_q^m$, có bậc n. Với mỗi $i = 1, \ldots, 2t$, xét $M_i(x)$ là đa thức cực tiểu của β^i. Khi đó, C là một mã vòng với đa thức sinh

$$g(x) = lcm(M_1(x), M_2(x), \cdots, M_{2t}(x))$$

Chứng minh. Ta xét một mã $w \in C$. Khi đó, $w(\beta^i) = 0 \ \forall \ i = 1, \cdots, 2t$. Ta thu được $M_i(x) \mid w(x) \ \forall \ i = 1, \cdots, 2t$.

Do $g(x) = lcm(M_1(x), M_2(x), \cdots, M_{2t}(x))$ nên $g(x) \mid w(x)$ hay mã $C \subseteq$ mã vòng sinh bởi $g(x)$.

Với mỗi mã được sinh bởi đa thức $g(x)$, ta viết dưới dạng $w(x) = g(x)h(x)$. Khi đó $w(\beta^i) = 1 \ \forall \ i = 1, \cdots, 2t$.

Ta thu được $w \in C$ hay C chính là mã vòng với đa thức sinh $g(x)$ □

Tính chất 23. Ma trận điều kiện của mã C là

$$H = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \cdots & \beta^{n-1} \\ 1 & \beta^2 & (\beta^2)^2 & (\beta^2)^3 & \cdots & (\beta^2)^{n-1} \\ 1 & \beta^3 & (\beta^3)^2 & (\beta^3)^3 & \cdots & (\beta^3)^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{2t} & (\beta^{2t})^2 & (\beta^{2t})^3 & \cdots & (\beta^{2t})^{n-1} \end{pmatrix}.$$

Chứng minh. Xét một mã $w = (w_0 w_1 \cdots w_{n-1})$. Khi đó

$$H.w^T = \begin{pmatrix} w_0 + w_1\beta + \cdots + w_{n-1}\beta^{n-1} \\ w_0 + w_1\beta^2 + \cdots + w_{n-1}(\beta^2)^{n-1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ w_0 + w_1\beta^{2t} + \cdots + w_{n-1}(\beta^{2t})^{n-1} \end{pmatrix} = \begin{pmatrix} w(\beta) \\ w(\beta^2) \\ \cdots \\ w(\beta^{2t}) \end{pmatrix}$$

Nên H là ma trận điều kiện của mã C vì $w \in C$ khi và chỉ khi $H.w^T = 0$ □

Ta thu được nhận xét sau đấy

Nhận xét 3. Nếu $\beta \in \mathbb{F}_q^m$ thì H là ma trận $2tm \times n$ và ta thu được mã (n, k) với $k = n - 2tm$ nếu các hàng của H độc lập tuyến tính

Tính chất 24. Cho một mã C là mã BCH sửa t lỗi. Khi đó $wt(C) \ \geq 2t + 1$.

Chứng minh. Ta nhắc lại về định thức Vandermonde

Bổ đề 7.6. Định thức Vandermonde: Cho một ma trận vuông có kích thước $n \times n$

$$A = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ 1 & \alpha_3 & \alpha_3^2 & \cdots & \alpha_3^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{pmatrix}$$

Khi đó, định thức của A được tính theo công thức

$$det(A) = \prod_{1 \leq i < j \leq n} (\alpha_j - \alpha_i)$$

Trở lại bài toán, ta giả sử tồn tại một mã $w \in C$ có trọng $\leq 2t$. Gọi $w_{i_1}, w_{i_2}, \cdots, w_{i_{2t}}$ là các vị trí của mã w thỏa mãn $w_i = 0 \ \forall \ i \neq i_1, i_2, \cdots, i_{2t}$. Khi đó ta sẽ chứng minh $H.w^T = 0$ chỉ có nghiệm 0 duy nhất

Khi ta xét 1 hàng của H là H_j khi nhân với w^T, ta thấy rằng kết quả chỉ phụ thuộc vào các entries thứ $i_1, i_2, \cdots, i_{2t}$ của hàng H_j. Điều này có nghĩa là nếu xét H' là ma trận H khi chỉ còn các cột $i_1, i_2, \cdots, i_{2t}$ và $w' = (w_{i_1} w_{i_2} \cdots w_{i_{2t}})$ thì

$$H.w^T = 0 \iff H'.(w')^T = 0$$

Ta có $H' = \begin{pmatrix} \beta^{i_1} & \beta^{i_2} & \cdots & \beta^{i_{2t}} \\ (\beta^2)^{i_1} & (\beta^2)^{i_2} & \cdots & (\beta^2)^{i_{2t}} \\ \cdots & \cdots & \cdots & \cdots \\ (\beta^{2t})^{i_1} & (\beta^{2t})^{i_2} & \cdots & (\beta^{2t})^{i_{2t}} \end{pmatrix}$ là ma trận $2t \times 2t$ và $det(H') = det((H')^T)$ nên nếu ta chứng minh được rằng $det((H')^T) \neq 0$ thì ta thu được nghiệm duy nhất của $H'.(w')^T = 0$ là vecto 0 hay suy ra $w = 0$ nên vô lý.

Ta có $(H')^T = \begin{pmatrix} \beta^{i_1} & (\beta^2)^{i_1} & \cdots & (\beta^{2t})^{i_1} \\ \beta^{i_2} & (\beta^2)^{i_2} & \cdots & (\beta^{2t})^{i_2} \\ \cdots & \cdots & \cdots & \cdots \\ \beta^{i_{2t}} & (\beta^2)^{i_{2t}} & \cdots & (\beta^{2t})^{i_{2t}} \end{pmatrix}$ thì

$$det((H')^T) = \beta^{i_1} \beta^{i_2} \cdots \beta^{i_{2t}} det(A)$$

với $A = \begin{pmatrix} 1 & \beta^{i_1} & \cdots & (\beta^{i_1})^{2t-1} \\ 1 & \beta^{i_2} & \cdots & (\beta^{i_2})^{2t-1} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & \beta^{i_{2t}} & \cdots & (\beta^{i_{2t}})^{2t-1} \end{pmatrix}$. Theo định thức Vandermonde thì $det(A) = \prod_{1 \leq m < n \leq 2t} (\beta^{i_n} - \beta^{i_m})$

Mà $\beta^{i_m} \neq \beta^{i_n} \ \forall \ m \neq n$ và $\beta^{i_m} \neq 0 \ \forall \ 1 \leq m \leq 2t$ nên $det((H')^T) \neq 0$ hay nghiệm duy nhất của $H'.(w')^T = 0$ chính là vecto 0 nên ta thu được mã w là vecto 0 (vô lý) □

Tính chất 25. Với n, t bất kì, ta có thể xây dựng được một mã BCH sửa t lỗi có độ dài n trong một trường hữu hạn có số phần tử nguyên tố cùng nhau với n

Chứng minh. Ta có bổ đề về cấp như sau:

Bổ đề 7.7. Cho trường $\mathbb{F}_q$ và số nguyên dương n thỏa mãn $gcd(q, n) = 1$. Khi đó, tồn tại một trường mở rộng $\mathbb{F}_q^m$ sao cho $\exists \ \beta \ \in \mathbb{F}_q^m$ sao cho cấp của β bằng n (Cấp của β là n khi và chỉ khi $\beta^n = 1$ và $\beta^k \neq 1$ với $k < n$)

Từ đây ta có thể suy ra được cách xây dựng mã BCH đó □

Định nghĩa 7.8. Hai mã A, B gọi là **tương đương nhau** nếu có cùng 1 độ dài n và $\sigma(n)$ là 1 hoán vị của tập $(1, 2, \cdots, n)$ thì

$$w = (w_1 w_2 \cdots w_n) \in A \iff (w_{\sigma(1)} w_{\sigma(2)} \cdots w_{\sigma(n)}) \in B$$

Tính chất 26. Việc chọn $\beta \in \mathbb{F}_q$ với cấp bằng n sẽ không ảnh hưởng đến việc tạo mã BCH (Điều này có nghĩa là nếu ta lấy β_1 và $\beta_2 \in \mathbb{F}_q$ với cấp bằng n thì mã tạo bởi β_1 và β_2 là tương đương nhau)

Chứng minh. Ta xét 2 phần tử β, β' đều có cấp là n với $\beta \in \mathbb{F}[x]/p(x), \beta' \in \mathbb{F}[x]/p'(x)$. Gọi bậc của $p(x), p'(x)$ lần lượt là an và $a'n$.

Ta xét một đa thức bất khả quy $q(x)$ có bậc là $an + a'n$. Khi đó $\beta, \beta' \in \mathbb{F}[x]/q(x)$. Tồn tại phần tử $\alpha \in \mathbb{F}[x]/q(x)$ sao cho một phần tử có cấp là n khi và chỉ khi viết được dưới dạng α^j sao cho $\gcd(j, n) = 1$. Do đó, ta có thể viết $\beta' = \beta^i$ với i nào đó. Ta thu được $gcd(i, n) = 1$

Ta sẽ xét một ánh xạ $\pi : k \to ik \mod n$. Ta có được π là một song ánh do $gcd(i, n) = 1$ nên $\pi(k)$ quét được hết từ $0, 1, \cdots, n-1$

Ta xét mã BCH C_1 sinh bởi β và mã $w = (w_0 w_1 \cdots w_{n-1})$ là một mã $\in C_1$. Khi đó $w(\beta) = w(\beta^2) = \cdots = w(\beta^{2t})$

Xét một số z thỏa mãn $w(\beta^z) = 0$. Khi đó $\sum_{i=0}^{n-1} w_i \beta^{iz} = 0$. Do $\pi(k)$ là một hoán vị của $0, 1, \cdots, n-1$ nên ta có thể viết lại thành $\sum_{i=0}^{n-1} w_{\pi(i)} \beta^{\pi(i)z} = 0$.

Mà $\beta^{\pi(k)z} = \beta^{ikz} = (\beta')^{kz}$ nên $0 = \sum_{i=0}^{n-1} w_{\pi(i)} \beta^{\pi(i)z} = \sum_{i=0}^{n-1} w_{\pi(i)} (\beta')^{iz}$ hay $w'((\beta')^z) = 0$ với $w' = (w_{\pi(0)} w_{\pi(1)} \cdots w_{\pi(n-1)})$

Vậy w' là một mã thuộc mã BCH sinh bởi β' hay 2 mã BCH sinh bởi β, β' là tường đương nhau □

7.3 Mã Reed-Solomon

Định nghĩa 7.9. Mã Reed-Solomon là một mã BCH trên $\mathbb{F}_q$ có độ dài $n = q - 1$ và sửa được t lỗi. Ta có thể lấy phần tử sinh của $\mathbb{F}_q^\times$ làm β thì sẽ thỏa mãn tính chất

$$w(\beta) = w(\beta^2) = \cdots = w(\beta^{2t})$$

Ví dụ 7.10. Do 3 là một phần tử nguyên thủy của $\mathbb{Z}_7$, ta có thể tạo được một mã Reed-Solomon sửa được 2 lỗi với độ dài 6 bởi đa thức sinh

$$g(x) = (x-3)(x-3^2)(x-3^3)(x-3^4) = (x-3)(x-2)(x-6)(x-4)$$

Tính chất 27. Đa thức sinh của mã Reed-Solomon là $g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{2t}) = 0$ với β là phần tử sinh

Chứng minh. Do β là phần tử sinh của $\mathbb{F}_q^\times$ nên trong $\mathbb{F}_q$, ta có được $x^n - 1 = (x-\beta)(x-\beta^2)\cdots(x-\beta^{n-1})$.

Đồng thời đa thức cực tiểu của β^i là $x - \beta^i$ nên ta thu được $g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{2t})$ □

Tính chất 28. Mã Reed-Solomon sửa t lỗi sẽ có trọng $d = 2t + 1$

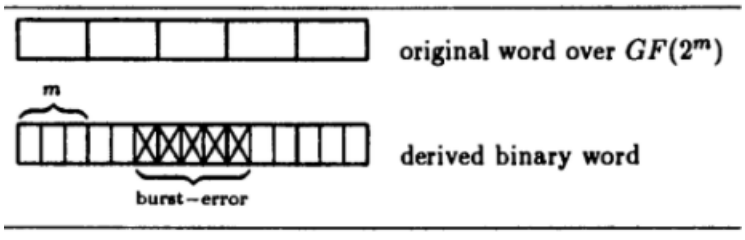
Chứng minh. Từ tính chất trên, ta thu được trọng của $g(x) \leq 2t+1$. Mà theo Tính chất 3, ta lại thu được $wt(C) \geq 2t+1$. Kết hợp lại, ta thu được trọng của mã Reed-Solomon là $2t + 1$ □

Tính chất 29. Mã Reed-Solomon là mã xảy ra dấu bằng của ràng buộc Singleton ($k + d \leq n + 1$)

Chứng minh. Ta có $k = n - 2t$, $d = 2t + 1$ hay $k + d = n + 1$ □

Ta sẽ nói về việc chuyển mã Reed-Solomon thành mã nhị phân sửa cụm lỗi

Cho một mã Reed-Solomon K sửa được t lỗi trên trường $\mathbb{F}_{2^m}$. Ta có thể biến các phần tử $f(a) = f_0 + f_1 a + \cdots + f_{m-1} a^{m-1}$ trong trường $\mathbb{F}_{2^m}$ thành 1 nhóm nhị phân $f_0 f_1 \cdots f_{m-1}$. Khi đó từ 1 mã dài $n = 2^m - 1$, ta thu được một mã dài mn như ở Hình 1.



Hình 1: Chuyển mã Reed-Solomon sang dạng nhị phân

Ví dụ 7.11. Xét mã có độ dài 7 trên trường $\mathbb{F}_8$, ta được đa thức sinh $\alpha^3 + \alpha x + x^2 + \alpha^3 x^3 + x^4$ hay ta thu được mã $\alpha^3\alpha 1\alpha^3 100$.
Mà $\alpha^3 = \alpha + 1$ ứng với 110, α ứng với 010 nên ta thu được mã nhị phân 21 kí tự 110|010|100|110|100|000|000
$\rightarrow$ Ta thu được mã $(21, 6)$ nhị phân từ mã Reed-Solomon $(7, 2)$

Ta thu được một nhận xét

Nhận xét 4. Một mã Reed-Solomon sửa t lỗi trên $\mathbb{F}_{2^m}$ thì khi chuyển sang mã nhị phân sẽ thu được 1 mã sửa tối đa $(t-1)m+1$ lỗi liên tiếp

Chứng minh. Giả sử rằng ta thu được mã sửa tối thiểu $(t-1)m+2$ lỗi liên tiếp. Khi đó nếu ta xét lỗi ở $(t-1)m$ lỗi liên tiếp ở giữa và 2 lỗi 2 bên thì ta thu được mã BCH sửa $t+1$ lỗi (Vô lý)

Vậy mã chỉ sửa tối đa $(t-1)m+1$ lỗi liên tiếp □

7.4 Giải mã mã BCH tổng quát

7.4.1 Vị trí lỗi và đánh giá lỗi

Cho một mã BCH có độ dài n trên $\mathbb{F}_q$ sửa được t lỗi. Giả sử ta nhận được vecto w có $\leq t$ lỗi. Ta tách thành được

$$w = c + e$$

với e là vecto lỗi có $wt(e) \leq t$, c là mã thuộc BCH

Ta giả sử $wt(e) = p$ và $e_{i_1}, e_{i_2}, \cdots, e_{i_p}$ là các vị trí $\neq 0$ của e. Mục tiêu của chúng ta là cần tìm $e_{i_1}, e_{i_2}, \cdots, e_{i_p}$ đó

Định nghĩa 7.12. Với mỗi k chạy từ 1 đến p, ta đặt

$$a_k = \beta^{i_k},\ b_k = e_{i_k}$$

Ở đây a_k được gọi là **vị trí lỗi** và b_k được gọi là **đánh giá lỗi**

Ta sẽ tìm $e_{i_1}, \cdots, e_{i_p}$ từ $a_1, a_2, \cdots, a_p, b_1, b_2, \cdots, b_p$ bằng cách

$$e_k = \begin{cases} 0 & \text{nếu } \beta^k \neq a_j\ \forall\ j \\ b_j & \text{nếu } \exists\ j:\ \beta^k = a_j \end{cases}$$

7.4.2 Đa thức vị trí lỗi, đa thức đánh giá lỗi, và đa thức syndrome

Định nghĩa 7.13. Từ $a_1, a_2, \cdots, a_p, b_1, b_2, \cdots, b_p,\ s_i = w(\beta^i)\ \forall i = 0, 1, \cdots, 2t-1$, ta xét 3 đa thức:

$$\sigma(x) = \prod_{i=1}^{p}(1 - a_i x)\ ,\ \omega(x) = \sum_{i=1}^{p} b_i \prod_{j \neq i}(1 - a_j x)\ ,\ s(x) = s_0 + s_1 x + \cdots + s_{2t-1}x^{2t-1}$$

Đa thức $\sigma(x)$ được gọi là **đa thức vị trí lỗi** do ta có thể tìm được các vị trí lỗi a_i với $\dfrac{1}{a_i}$ là nghiệm của $\sigma(x)$, còn $\omega(x)$ được gọi là **đa thức đánh giá lỗi** vì ta có thể tính được đánh giá lỗi b_i

Tính chất 30. Đánh giá lỗi b_i được tính nhờ công thức

$$b_i = -a_i \frac{\omega\left(\dfrac{1}{a_i}\right)}{\sigma'\left(\dfrac{1}{a_i}\right)}\ \forall 1 \leq i \leq p$$

Với $\sigma'(x)$ là đạo hàm của đa thức $\sigma(x)$

Chứng minh. Xét tại một vị trí i bất kì. Ta gọi $A_i(x) = \prod_{t=1,\ t\neq i}^{p} (1 - a_i x)$. Khi đó $\sigma(x) = A_i(x)(1 - a_i x)$

Ta thu được $\sigma(x)' = A_i(x)'(1 - a_i x) + A_i(x)(-a_i)$ hay $\sigma'\left(\frac{1}{a_i}\right) = -a_i A_i\left(\frac{1}{a_i}\right)$

Mà $\omega\left(\frac{1}{a_i}\right) = b_i A_i\left(\frac{1}{a_i}\right)$ nên ta suy ra được $b_i = -a_i \frac{\omega\left(\frac{1}{a_i}\right)}{\sigma'\left(\frac{1}{a_i}\right)}$ □

Tính chất 31. $\omega(x) \equiv \sigma(x)s(x) \ \ (mod\ x^{2t})$

Chứng minh. Ta có syndrome của w và e là như nhau nên ta có

$$s_i = e(\beta^i) = e_{i_1}(\beta^{i_1})^i + e_{i_2}(\beta^{i_2})^i + \cdots + e_{i_p}(\beta^{i_p})^i$$

Do $e_{i_1}, e_{i_2}, \cdots, e_{i_p}$ là các vị trí khác 0 của e, $e_{i_j} = b_j,\ \beta^{i_j} = a_j\ \forall j = 1, 2, \cdots, p$ nên ta thu được

$$s_i = \sum_{j=1}^{p} b_j a_j^i$$

Ta lại có $\omega(x) = \sum_{i=1}^{p} b_i \frac{\sigma(x)}{1 - a_i x},\ \ \frac{1}{1 - a_i x} = \sum_{j=0}^{\infty} (a_i x)^j$ nên ta thu được

$$\begin{aligned}
\omega(x) &= \sigma(x) \sum_{i=1}^{p} \left(b_i \sum_{j=0}^{\infty} (a_i x)^j \right) \\
&= \sigma(x) \sum_{j=0}^{\infty} \sum_{i=1}^{p} b_i a_i^j x^j \\
&= \sigma(x) \sum_{j=0}^{\infty} s_j x^j \\
&\equiv \sigma(x) \sum_{j=0}^{2t-1} s_j x^j \ \ (mod\ x^{2t}) \\
&\equiv \sigma(x) s(x) \ \ (mod\ x^{2t})
\end{aligned}$$

□

Tính chất 32. $deg(\omega(x)) \ < \ t, deg(\sigma(x)) \ \leq \ t$

Chứng minh. Ta có $deg(\omega(x)) = p - 1 < t$, $deg(\sigma(x)) = p \leq t$ □

Tính chất 33. $s(x) \ \not\equiv 0 \ \ (mod\ x^t)$

Chứng minh. Giả sử phản chứng, $s(x) \ \equiv 0 \ \ (mod\ x^t)$ hay $s_0 = s_1 = \cdots = s_{t-1} = 0$. Do $p \leq t, s_i = \sum_{j=1}^{p} b_j a_j^i$ nên ta thu được

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_p \\ a_1^2 & a_2^2 & \cdots & a_p^2 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{p-1} & a_2^{p-1} & \cdots & a_p^{p-1} \end{pmatrix} . \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_p \end{pmatrix} = \begin{pmatrix} s_1 \\ s_2 \\ s_3 \\ \cdots \\ s_p \end{pmatrix} = 0 \ (*)$$

Ta có được $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_p \end{pmatrix} \neq 0$. Ta lại có theo định thức Vandermonde, $det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_p \\ a_1^2 & a_2^2 & \cdots & a_p^2 \\ \cdots & \cdots & \cdots & \cdots \\ a_1^{p-1} & a_2^{p-1} & \cdots & a_p^{p-1} \end{pmatrix} = \prod_{m<n} (a_n - a_m) \neq 0$

nên nếu phương trình $(*)$ có nghiệm thì $\begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ \cdots \\ b_p \end{pmatrix} = 0$ và ta thu được điều mâu thuẫn □

7.4.3 Xây dựng các đa thức lỗi

Ý tưởng ở đây là sử dụng thuật toán chia Euclid để tìm $\sigma(x)$ và $\omega(x)$

Bổ đề 7.14. (Thuật toán chia Euclid cho đa thức) Ta xét $a_0(x) = f(x),\ a_1(x) = g(x)$, đồng thời $a_{i-1}(x) = a_i(x)q_i(x) + a_{i+1}(x)$ hay $q_i(x)$ là thương của phép chia $a_{i-1}(x)$ cho $a_i(x)$ nên $deg(q_i(x)) = deg(a_{i-1}(x)) - deg(a_i(x))$. Ta có $deg(a_0(x)) > deg(a_1(x)) > \cdots$ và sẽ đến lúc $a_{k+1}(x) = 0$ hay $gcd(a_0(x), a_1(x)) = a_k(x)$

Ta xét 2 dãy đa thức $\{u_n(x)\},\ \{v_n(x)\}$ thỏa mãn

$$u_0(x) = 0, u_1(x) = 1,\ u_{k+1}(x) = q_k(x)u_k(x) + u_{k-1}(x)$$
$$v_0(x) = 1, v_1(x) = 0,\ v_{k+1}(x) = q_k(x)v_k(x) + v_{k-1}(x)$$

Tính chất 34. $f(x)v_i(x) - g(x)u_i(x) = (-1)^i a_i(x)\ \forall i$

Chứng minh. Ta chứng minh bằng nguyên lý quy nạp

Với $i = 0$, ta có $v_0(x) = 1,\ u_0(x) = 0,\ a_0(x) = f(x)$. Vậy $f(x)v_0(x) - g(x)u_0(x) = a_0(x)$ hay tính chất đúng với $i = 0$

Với $i = 1$, ta có $v_1(x) = 0,\ u_1(x) = 1,\ a_1(x) = g(x)$. Vậy $f(x)v_1(x) - g(x)u_1(x) = -a_1(x)$ hay tính chất đúng với $i = 1$

Giả sử khẳng định đúng đến $i = m$, hay $f(x)v_j(x) - g(x)u_j(x) = (-1)^j a_j(x)\ \forall j = 0, 1, \cdots, m$. Ta chứng minh

$$f(x)v_{m+1}(x) - g(x)u_{m+1}(x) = (-1)^{m+1} a_{m+1}(x)$$

Ta có

$$\begin{aligned} f(x)v_{m+1}(x) - g(x)u_{m+1}(x) &= f(x)(q_m(x)v_m(x) + v_{m-1}(x)) - g(x)(q_m(x)u_m(x) + u_{m-1}(x)) \\ &= q_m(x)(f(x)v_m(x) - g(x)u_m(x)) + f(x)v_{m-1}(x) - g(x)u_{m-1}(x) \\ &= q_m(x)((-1)^m a_m(x)) + (-1)^{m-1} a_{m-1}(x) \\ &= (-1)^{m-1}(a_{m-1}(x) - q_m(x)a_m(x)) \\ &= (-1)^{m+1}(a_{m-1}(x) - q_m(x)a_m(x)) \end{aligned}$$

Theo bổ đề 7.14, $a_{m+1}(x) = a_{m-1}(x) - a_m(x)q_m(x)$ nên $(-1)^{m+1}(a_{m-1}(x) - q_m(x)a_m(x)) = (-1)^{m+1}a_{m+1}(x)$

Vậy $f(x)v_{m+1}(x) - g(x)u_{m+1}(x) = (-1)^{m+1}a_{m+1}(x)$ hay khẳng định đúng với $i = m + 1$. Theo nguyên lý quy nạp, ta thu được $f(x)v_i(x) - g(x)u_i(x) = (-1)^i a_i(x)\ \forall i$ □

Ta sẽ sử dụng thuật toán chia Euclid với $f(x) = x^{2t}$ và $g(x) = s(x)$. Ta xét tại vị trí thứ l nhỏ nhất thỏa mãn $deg(a_l(x)) < t$ hay $deg(a_0(x)),\ deg(a_1(x)), \cdots,\ deg(a_{l-1}(x)) \geq t$

Tính chất 35. $deg(u_k(x)) = deg(a_0(x)) - deg(a_{k-1}(x))$

Chứng minh. Ta chứng minh bằng nguyên lý quy nạp

Với $k = 1$, ta có $deg(u_1(x)) = 0 = deg(a_0(x)) - deg(a_0(x))$ hay khẳng định đúng với $k = 1$

Với $k = 2$, ta có $deg(u_2(x)) = deg(q_1(x)) + deg(u_1(x)) = deg(q_1(x)) = deg(a_0(x)) - deg(a_1(x))$ hay khẳng định đúng với $k = 2$

Giả sử khẳng định đúng đến $k = n$ hay $deg(u_i(x)) = deg(a_0(x)) - deg(a_{i-1}(x))\ \forall i = 1, 2, \cdots, n$

Ta chứng minh khẳng định đúng với $k = n + 1$

Ta có $deg(u_{n+1}(x)) = deg(q_n(x)u_n(x) + u_{n-1}(x))$.

Mà $deg(u_{n-1}(x)) = deg(a_0(x)) - deg(a_{n-2}(x))$

$deg(q_n(x)u_n(x)) = deg(q_n(x)) + deg(u_n(x)) = deg(a_{n-1}(x)) - deg(a_n(x)) + deg(a_0(x)) - deg(a_{n-1}(x)) = deg(a_0(x)) - deg(a_n(x))$, đồng thời $deg(a_{n-2}(x)) > deg(a_n(x))$ nên $deg(u_{n-1}(x)) < deg(u_n(x)q_n(x))$

Vậy $deg(q_n(x)u_n(x) + u_{n-1}(x)) = deg(q_n(x)u_n(x)) = deg(a_0(x)) - deg(a_n(x))$ nên $deg(u_{n+1}(x)) = deg(a_0(x)) - deg(a_n(x))$ hay khẳng định đúng với $k = n + 1$ □

Tính chất 36. $\sigma(x) = \dfrac{u_l(x)}{u_l(0)},\ \omega(x) = \dfrac{(-1)^{l+1}a_l(x)}{u_l(0)}$

Chứng minh. Ta gọi $gcd(x^{2t}, s(x)) = x^a$. Ta thu được $a < t$ do $s(x) \not\equiv 0\ (mod\ x^t)$

Do $x^{2t}v_l(x) - s(x)u_l(x) = (-1)^l a_l(x)$ nên $s(x)u_l(x) \equiv (-1)^{l+1}a_l(x)\ (mod\ x^{2t})$

Đặt $\overline{\sigma}(x) = u_l(x),\ \overline{\omega}(x) = (-1)^{l+1}a_l(x)$. Khi đó $s(x)\overline{\sigma}(x) \equiv \overline{\omega}(x)\ (mod\ x^{2t}),\ deg(\overline{\omega}(x)) < t$. Theo tính chất 14, $deg(\overline{\sigma}(x)) = deg(u_l(x)) = deg(a_0(x)) - deg(a_{l-1}(x)) = 2t - deg(a_{l-1}(x))$. Do $deg(a_{l-1}(x)) \geq t$ nên $deg(\overline{\sigma}(x)) \leq t$

Ta có $\begin{cases} s(x)\overline{\sigma}(x) \equiv \overline{\omega}(x)\ (mod\ x^{2t}) \\ s(x)\sigma(x) \equiv \omega(x)\ (mod\ x^{2t}) \end{cases}$ nên $\begin{cases} s(x)\overline{\sigma}(x)\omega(x) \equiv \overline{\omega}(x)\omega(x)\ (mod\ x^{2t}) \\ s(x)\sigma(x)\overline{\omega}(x) \equiv \omega(x)\overline{\omega}(x)\ (mod\ x^{2t}) \end{cases}$ hay $\overline{\sigma}(x)\omega(x) \equiv \sigma(x)\overline{\omega}(x)\ (mod\, x^{2t})$
(Do $s(x)\ \not\equiv 0\ (mod\ x^{2t})$

Do $deg(\sigma(x)), deg(\overline{\sigma}(x)) \leq t$ và $deg(\omega(x)), deg(\overline{\omega}(x)) < t$ nên $deg(\sigma(x)\overline{\omega}(x)), deg(\overline{\sigma}(x)\omega(x)) < 2t$

Mà $\overline{\sigma}(x)\omega(x) \equiv \sigma(x)\overline{\omega}(x)\ (mod\ x^{2t})$ nên $\overline{\sigma}(x)\omega(x) = \sigma(x)\overline{\omega}(x)$

Ta có $gcd(\sigma(x), \omega(x)) = 1$ (Do $\sigma(x), \omega(x)$ không có nghiệm chung) nên $\sigma(x) \mid \overline{\sigma}(x)$. Mà $deg(\sigma(x)) = t \geq deg(\overline{\sigma}(x))$ nên $\exists\ d \in \mathbb{F}_q^\times$ sao cho $\sigma(x) = d\overline{\sigma}(x)$

Thay $x = 0$, ta có $1 = d\overline{\sigma}(0)$ nên $d = \dfrac{1}{\overline{\sigma}(0)} = \dfrac{1}{u_l(0)}$. Vậy $\sigma(x) = \dfrac{\overline{\sigma}(x)}{u_l(0)} = \dfrac{u_l(x)}{u_l(0)}$ và $\omega(x) = d\overline{\omega}(x) = \dfrac{(-1)^{l+1}a_l(x)}{u_l(0)}$ □

7.4.4 Phương pháp tổng quát

Cách giải mã sử dụng thuật toán chia Euclid bao gồm 5 bước

- Bước 1: Tìm đa thức syndrome $s(x)$
- Bước 2: Dùng thuật toán Euclid mở rộng để tìm $a_k(x), u_k(x)$
- Bước 3: Tìm $\omega(x)$ và $\sigma(x)$ theo công thức

$$\sigma(x) = \frac{u_k(x)}{u_k(0)},\ \omega(x) = \frac{(-1)^{k+1}a_k(x)}{u_k(0)}$$

- Bước 4: Ta tìm $a_1, a_2, \cdots, a_p$ với $\frac{1}{a_i}$ là nghiệm của đa thức $\sigma(x)$ và $b_1, b_2, \cdots, b_p$ từ công thức $b_i = -a_i \frac{\omega\left(\frac{1}{a_i}\right)}{\sigma'\left(\frac{1}{a_i}\right)}$ $\forall 1 \leq i \leq p$
- Bước 5: Tìm các vecto lỗi $e = e_1 \cdots e_n$ và tìm từ mã $c = w - e$

Chú ý 1. Đôi khi việc tìm nghiệm của $\sigma(x)$ khá lâu nên ta có thể sử dụng ngôn ngữ Sage 9.3 trên CoCalc để có thể làm việc nhanh và hiệu quả hơn.

Ví dụ 7.15. Giải mã 001000100000000 với mã BCH sửa 2 lỗi với độ dài 15

Bước 1: Ta có $w(x) = x^2 + x^6$. Xét đa thức syndrome $s(x) = s_0 + s_1 x + s_2 x^2 + s_3 x^3$ với $s_i = \alpha^{2i} + \alpha^{6i}$ (α là phân tử sinh của $\mathbb{F}_{16}$)

$$
\begin{aligned}
&s_0 = 0\\
&s_1 = \alpha^2 + \alpha^6 = \alpha^2(\alpha^4 + 1) = \alpha^2(\alpha) = \alpha^3\\
&s_2 = \alpha^4 + \alpha^{12} = \alpha^4(\alpha^8 + 1) = \alpha^4(\alpha^2) = \alpha^6\\
&s_3 = \alpha^6 + \alpha^{18} = \alpha^6(1 + \alpha^{12}) = \alpha^6(\alpha + \alpha^2 + \alpha^3) = \alpha^7(\alpha^{10}) = \alpha^{17} = \alpha^2\\
&\rightarrow\ s(x) = \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3
\end{aligned}
$$

Bước 2: Ta thực hiện thuật toán chia Euclid mở rộng với $a_0(x) = x^4$ và $a_1(x) = s(x) = \alpha^3 x + \alpha^6 x^2 + \alpha^2 x^3$

- Chia $a_0(x)$ cho $a_1(x)$, ta thu được $q_1(x) = \alpha^{13} x + \alpha^2$ và $a_2(x) = \alpha^{10} x^2 + \alpha^5 x$. Ta có $deg(a_2(x)) \leq 2$ nên tiếp tục thuật toán
- Chia $a_1(x)$ cho $a_2(x)$ ta thu được $q_2(x) = \alpha^7 x + \alpha^9$ và $a_3(x) = x$. Do $deg(a_3(x)) < 2$ nên ta dừng lại. Khi đó ta cần tìm $u_3(x)$
- Ta có $u_0(x) = 0,\ u_1(x) = 1,\ u_2(x) = q_1(x),\ u_3(x) = u_2(x)q_2(x) + u_1(x) = \alpha^5 x^2 + x + \alpha^{12}$

Bước 3: Ta thu được

$$\sigma(x) = \frac{u_3(x)}{u_3(0)} = \alpha^8 x^2 + \alpha^3 x + 1$$

và

$$\omega(x) = \frac{a_3(x)}{u_3(0)} = \alpha^3 x$$

Bước 4: Ta tìm nghiệm của $\sigma(x) = (x\alpha^2 - 1)(x\alpha^6 - 1)$ là $a_0 = \alpha^2, a_1 = \alpha^6$

Bước 5: Ta thu được mã gốc là 000000000000000

7.5 Ứng dụng của mã BCH trong cuộc sống

Mã BCH $(63, 56)$ được sử dụng trong chíp Field-programmable gate array (FPGA) của Ủy ban Tư vấn về Hệ thống Dữ liệu Không gian (CCSDS) để liên lạc trong không gian

Mã BCH $(15, 7)$ được dùng trong mã QR. Điều này có nghĩa là nếu ta input một mã QR code như bên trái thì khi truyền tin, nó sẽ bị mã hóa thành hình bên phải. Ta sẽ sử dụng mã BCH $(15, 7)$ đó để tìm ra được mã QR code ban đầu

Tài liệu

"Introduction to the Theory of Error-Correcting Codes". **in**: John Wiley Sons, Ltd, 1998. ISBN: 9781118032749. DOI: https://doi.org/10.1002/9781118032749. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118032749. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118032749.

"Foundations of Coding". **in**: John Wiley Sons, Ltd, 1991. ISBN: 9781118033265. DOI: https://doi.org/10.1002/9781118033265. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/9781118033265. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/9781118033265.

Posner, E.C. *Combinatorial Structures in Planetary Reconnaissance*. 1968.

Arunkumar, S. **and** T. Kalaivani. "FPGA implementation of CCSDS BCH (63, 56) for satellite communication". **in**: *2012 IEEE International Conference on Electronics Design, Systems and Applications (ICEDSA)*. 2012, **pages** 248–253. DOI: 10.1109/ICEDSA.2012.6507808.

Davide Boscaini, Simone Parisotto. *QR CODE An industrial application of Code Theory*. 2012. URL: http://simoneparisotto.com/math/misc/qrcode/qrcode.pdf.