Chương 7. Mã tuyến tính

Mã tuyến tính

ĐN: Cho F là một trường hữu hạn. ***Mã tuyến tính*** là một không gian con của không gian F^n các từ độ dài n. Nói cách khác, một KG con k-chiều của F^n là một mã (n,k) trên bộ ký tự F.

Lưu ý:

- Một mã tuyến tính (n,k) có k bit mang thông tin và n – k bit kiểm tra.
- Nếu F có r ký tự, thì bộ mã có r^k từ mã.

Ma trận sinh

ĐN: Cho K là một mã tuyến tính và B = $\{e_1, e_2, \ldots, e_k\}$ là một cơ sở của K. Một ***ma trận sinh (generator matrix)*** G ứng với cơ sở B của K là ma trận

$$G = \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_k \end{pmatrix}$$

VD: Một ma trận sinh của mã Hamming (7,4)

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

Ví dụ

- Mã kiểm chẵn kẻ độ dài 4 có một ma trận sinh

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

- Mỗi ma trận G' thu được từ các phép biến đổi dòng sơ cấp của ma trận G cũng là ma trận sinh của cùng một mã.

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

Mã tuyến tính hệ thống

- **ĐN**: Một mã tuyến tính được gọi là ***hệ thống (systematic)*** nếu ma trận sinh G = [I | B], trong đó I là ma trận đơn vị.
- Hai mã K và K' được gọi là ***tương đương (equivalent)*** nếu chúng chỉ khác nhau ở thứ tự của các ký tự trong từ mã. Tức là, tồn tại một hoán vị (p_1, p_2, …, p_n) của (1, 2, …, n) sao cho $v_1v_2…v_n$ là từ mã của K$\Leftrightarrow$ $v_{p1}v_{p2}…v_{pn}$ là từ mã của K'.

Ví dụ

- Mã Hamming (7,4) có ma trận sinh G sau là hệ thống

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right].$$

- **<u>Mệnh đề:</u>** *Mọi mã tuyến tính đều tương đương với một mã hệ thống.*

Ma trận kiểm chẵn lẻ

ĐN: Cho K là một mã tuyến tính độ dài n trên trường F.
Một ma trận H có n cột trên F được gọi là ***ma trận kiểm chẵn lẻ (parity check matrix)*** của K nếu
v là từ mã của K $\Leftrightarrow$ Hv = **0**.

Ma trận kiểm chẵn lẻ H thoả : $GH^T = 0$.

Mệnh đề: *Một mã hệ thống với ma trận sinh* $G = [I \mid B]$
thì có ma trận kiểm chẵn lẻ $H = [-B^T \mid I]$.

Ngược lại, nếu $H = [A \mid I]$ *thì* $G = [I \mid -A^T]$.

Syndrome

ĐN: Cho K là một mã tuyến tính có ma trận kiểm chẵn lẻ H kích thước m x n. Syndrome của từ w là s = Hw.

Giải mã: Khi nhận từ w, tính syndrome s = Hw. Chọn từ có trọng Hamming nhỏ nhất có syndrome như thế.

Phát hiện và sửa lỗi

Mệnh đề: *Trọng nhỏ nhất d của mã tuyến tính (n,k) thoả* $d \leq n - k + 1$.

Nhắc lại: *Một mã K phát hiện được t lỗi nếu khoảng cách nhỏ nhất của K lớn hơn t.*

Ta mong muốn:

1. Khoảng cách nhỏ nhất (d) lớn.
2. Số bit mang thông tin (k) lớn.

Lưu ý: *Hai mã tương đương nhau K và K' thì có cùng các thông số n, k, d.*

Giải mã bằng syndrome

- Mã tuyến tính K (n,k) có ma trận kiểm chẵn lẻ H.
- Khi truyền v, ta nhận được w = e + v. Trong đó e được gọi là ***error pattern***.
- Các từ cùng một lớp ghép (coset) có cùng syndrome.

1. Khi nhận w, tính s = Hw.
2. Tìm coset leader e tương ứng với s.
3. Suy ra v = w – e.

Ví dụ

- Giả sử mã K độ dài 5 định nghĩa bởi

$$x_4 = x_1 + x_2,$$
$$x_5 = x_1 + x_2 + x_3 + x_4.$$

00000 | 10010 01010 00101 11000 10111 01111 11101

- Có ma trận $\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$.

Syndrome	Coset Leader
00	00000
11	10000
01	00001
10	10001

Syndrome	Coset Leader
00	00000
11	10000
01	00001
10	10001

- Giả sử nhận w = 11111.
- Tính s:

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

- Suy ra: e = 10000
- Suy ra: v = w – e = 01111.

Xác định bảng sau như thế nào?

Syndrome	Coset Leader
00	00000
11	10000
01	00001
10	10001

- Syndrome gồm tất cả các từ s độ dài n – k.
- Coset leader là các nghiệm e có trọng Hamming nhỏ nhất của pt He = s.
- **VD**:

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \Leftrightarrow \begin{cases} e_1 + e_2 + e_4 = 0 \\ e_3 + e_5 = 0 \end{cases}$$

Phát hiện và sửa lỗi ngay

- Mã Hamming (7,4) có d = 3, có thể phát hiện 2 lỗi nhưng chỉ sửa được 1 lỗi (không sửa được 2 lỗi).
- **VD**: truyền 0000000 nhưng nhận 1010000. Theo cách giải mã bằng syndrome:
  - syndrome là 010.
  - Bit số 2 bị lỗi
  - Giải mã là 1110000. (không phải 0000000)

Phát hiện và sửa lỗi ngay

ĐN: Mã K được gọi là ***phát hiện được s lỗi và sửa được t lỗi ngay*** nếu với mọi từ mã v ta có: từ w có $d(w,v) \leq s$ thì có $d(w,v') > t$ với các từ mã v' khác v.

Hoạt động của mã K theo ĐN trên như sau:

- Khi nhận từ w
- Tìm từ mã v có khoảng cách Hamming với w là nhỏ nhất
- Nếu $d(w,v) \leq t$ thì sửa được trở lại thành v.
- Nếu $d(w,v) > t$ thì thông báo rằng có ít nhất s lỗi xảy ra.

Phát hiện và sửa lỗi ngay

Mệnh đề: *Một mã có thể phát hiện được s lỗi và sửa được t lỗi ngay nếu và chỉ nếu*

$$d \geq t + s + 1.$$

Cho G không hệ thống, tính H?

- **VD**: trên $\mathbf{Z}_3$, cho ma trận sinh của một mã như sau

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

- Ta chuyển thành ma trận sinh của mã hệ thống tương đương bằng một phép hoán vị p=(1,4,6,2,5,3) các cột về dạng [I | B].

$$\mathbf{G^*} = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{array}\right].$$

- Ta tính được H* tương ứng với G* là

$$\mathbf{H^*} = \left[\begin{array}{ccc|ccc} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 & 0 & 1 \end{array}\right] = \begin{bmatrix} 2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

- Tính H bằng hoán vị ngược p^{-1}.
- Thử lại: $GH^T = 0$.

$$\mathbf{H} = \begin{bmatrix} 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 2 & 0 & 0 \end{bmatrix}$$

Tóm tắt

- Mã tuyến tính
- Ma trận sinh
- Mã tuyến tính hệ thống
- Parity check matrix
- Syndrome
- Phát hiện và sửa lỗi ngay

Homework

- Đọc và làm chương 8 [1]

Bài tập

1. Cho ma trận sinh của một mã tuyến tính trên $\mathbf{Z}_5$ bên. Tìm ma trận kiểm chẵn lẻ H.

$$\mathbf{G} = \begin{bmatrix} 1 & 2 & 3 & 1 & 2 \\ 2 & 2 & 4 & 1 & 0 \\ 1 & 1 & 2 & 2 & 1 \end{bmatrix}.$$

2. Tính toán lại bài 1 trên $\mathbf{Z}_7$.
3. Cho ma trận sinh của một mã tuyến tính nhị phân K bên. Hỏi K có hệ thống không? Nếu không, tìm mã hthống tương đương K'.

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

4. Lập bảng mã ứng với hai mã K và K' trong bài 3.