C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2: Mã vòng tuyến tính)

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

ver 22a

Notes

Mục tiêu của bài học

- Tiếp tục trang bị một số khái niệm cơ bản về mã hóa kênh
- Mã vòng (mã cyclic, mã xyclic) tuyến tính

Notes

Các câu hỏi cần trả lời

- Vành đa thức đồng dư?
- Đa thức sinh, đa thức kiểm tra của mã vòng tuyến tính?
- Mã vòng tuyến tính hệ thống? Thuật toán lập mã cho mã vòng tuyến tính hệ thống?
- Các phương pháp giải mã cơ bản cho mã vòng tuyến tính?

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

Đa thức mã và các phép biến đổi

Đa thức mã

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

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{l-1} x^{l-1}$$

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.
  - $c \in \mathfrak{C}(l,k) \Leftrightarrow c(x) \in GF(q)[x]/(x^l - 1)$

Notes

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

$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{l-1} x^{l-1}$
$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{l-1} x^{l-1}$
$\Rightarrow f(x) + g(x) = (f_0 + g_0) + (f_1 + g_1)x + \cdots + (f_{l-1} + g_{l-1})x^{l-1}$

Phép nhân đa thức

$f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_{l-1} x^{l-1} = \sum_{i=0}^{l-1} f_i x^i$
$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{l-1} x^{l-1} = \sum_{j=0}^{l-1} g_j x^j$
$\Rightarrow f(x) \times g(x) = (\sum_{i=0}^{l-1} f_i x^i)(\sum_{j=0}^{l-1} g_j x^j)$ modulo $(x^l - 1)$

Notes

Đa thức mã và các phép biến đổi

Phép dịch vòng

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

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

- b thu được bằng cách dịch vòng về phía phải của 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 $g(x) = \frac{f(x)}{x} \longleftrightarrow \mathrm{b} = (f_1, f_2, f_3, \ldots, f_{l-1}, f_0)$ (chú ý: mod $x^l - 1$)

- b thu được bằng cách dịch vòng về phía trái của 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.

Notes

Đa thức mã và các phép biến đổi

Đa thức đối ngẫu

Định nghĩa

Cho đa thức $f(x)$ bậc k: $f(x) = f_0 + f_1 x + f_2 x^2 + \cdots + f_k x^k$.
Đa thức đối ngẫu của $f(x)$, kí hiệu là $f^*(x)$ được định nghĩa là:

$$f^*(x) = x^k \times f(x^{-1}) = f_k + f_{k-1} x + f_{k-2} x^2 + \cdots + f_1 x^{k-1} + f_0 x^k$$

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

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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 tuyến tính nếu với mọi từ mã $c = (c_0, c_1, \ldots, c_{l-1}) \in \mathfrak{C}$ thì kết quả của mỗi dịch vòng từ mã 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 $c(x)$

$\Rightarrow a(x)c(x) \in \mathfrak{C}\ \forall a(x) \in GF(q)[x]/(x^l - 1)$, $c(x) \in \mathfrak{C}$

Notes

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Một số tính chất, Đa thức sinh

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 $\mathfrak{C}(l,k)$.

Notes

Mã vòng tuyến tính

Một số định nghĩa và khái niệm: Đa thức kiểm tra, Mã vòng đối ngẫu

Định nghĩa

Một bộ mã vòng tuyến tính $\mathfrak{C}(l,k)$ có đa thức sinh $g(x)$. Một đa thức $h(x) \neq 0$ được gọi là đa thức kiểm tra của $\mathfrak{C}(l,k)$ nếu $g(x) \times h(x) = x^l - 1 \equiv 0$ (mod $x^l - 1$)

- $deg(h(x)) = k$
- $h(x) = \frac{x^l-1}{g(x)}$

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 $h(x) = \frac{(x^l-1)}{g(x)}$.

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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:

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

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

Notes

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:

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

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

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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 $c = [p \mid a]$

Bài toán

Nhập vào: $\mathfrak{C}(l, k)$, $g(x)$, khối tin cần mã hóa $a = (a_0, a_1, \ldots, a_{k-1})$.
In ra: Từ mã dạng hệ thống tương ứng c

Thuật toán

1. Mô tả khối tin bằng biểu diễn đa thức tương ứng $a(x)$.
2. Tính $a^{(l-k)}(x) = x^{l-k}a(x)$.
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 $c(x)$.

Notes

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: $c_{l-k} = a_0$, $c_{l-k+1} = a_1$, ..., $c_{l-1} = a_{k-1}$.
2. Tính toán c_0, c_1, ..., 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 $c = (c_0, c_1, c_2, \ldots, c_{l-k-1}, a_0, \ldots, a_{k-1})$.

Notes

Mã vòng tuyến tính dạng hệ thống

Ma trận sinh, ma trận kiểm tra dạng hệ thống

$$G \xrightarrow{\text{phương pháp khử Gausse}} G_{\text{dạng hệ thống}}$$

- Nếu $G = \begin{bmatrix} P & | & I_k \end{bmatrix} \Rightarrow H = \begin{bmatrix} I_{l-k} & | & P^T \end{bmatrix}$
- Nếu $G = \begin{bmatrix} I_k & | & P \end{bmatrix} \Rightarrow H = \begin{bmatrix} P^T & | & I_{l-k} \end{bmatrix}$

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Da thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

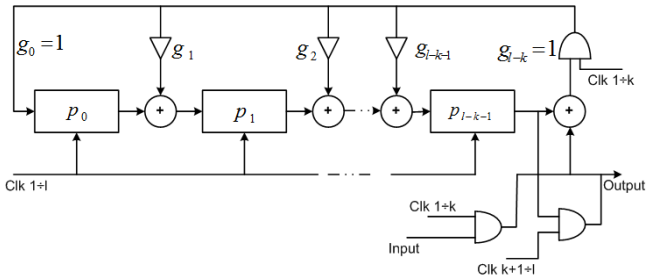
Nội dung chính

1. Da thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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

Notes

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 (a) được dịch trực tiếp ra đầu ra và đồng thời được dịch vào mạch để tính các bít kiểm tra. 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.

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

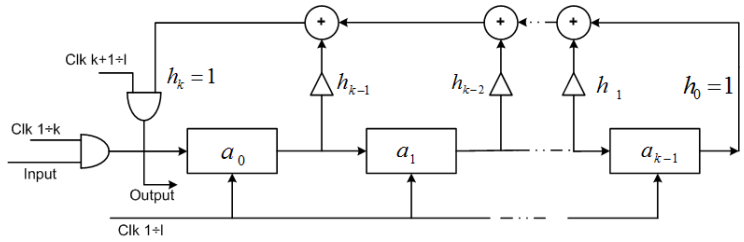
Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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

Notes

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, các c_{l-k-i} $(i=\overline{1,l-k})$ 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.

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

Các phương pháp giải mã vòng

Phương pháp giải mã ngưỡng: Hệ tổng kiểm tra

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

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 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.*

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

Notes

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 $t = \lfloor (d_0 - 1)/2 \rfloor$.

Notes

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

1. *Mọi vị trí bít lỗi e_{i_j} của E đều được kiểm tra bởi mọi tổng kiểm tra 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.*

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

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 $i = l$ 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.

Notes

C4: Mã hóa kênh - Truyền dẫn dữ liệu (Part 2)

Nội dung chính

1. Đa thức mã và các phép biến đổi
2. Mã vòng tuyến tính
   - Một số định nghĩa và khái niệm
   - Ma trận sinh và ma trận kiểm tra của mã vòng
   - Mã vòng tuyến tính dạng hệ thống
3. Mạch nguyên lý mã hóa mã vòng
   - Xây dựng từ đa thức sinh
   - Xây dựng từ đa thức kiểm tra
4. Các phương pháp giải mã vòng
   - Phương pháp giải mã ngưỡng
   - Phương pháp bẫy lỗi - Thuật toán chia dịch vòng
5. Kết thúc

Notes

Kết thúc phần mã vòng

Notes