Mã hóa kênh - Truyền dẫn dữ liệu (Part 1)

Lý thuyết thông tin

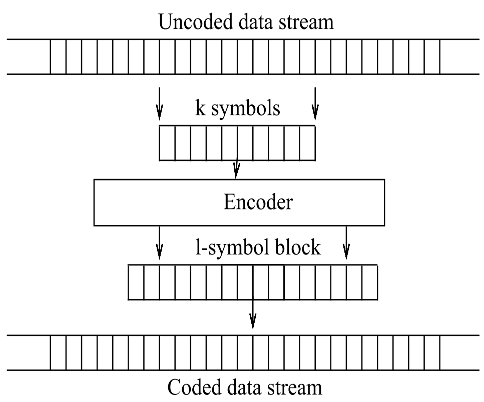
Biên soạn: Phạm Văn Sự

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

10/09/2011

Một số định nghĩa và khái niệm cơ bản

Mã hóa khối



Hình: Quá trình mã hóa khối

Một số định nghĩa và khái niệm cơ bản

Véc-tơ mã

Định nghĩa (Véc-tơ mã)

Một bộ mã $\mathfrak{C} = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{M-1}\}$ *chứa các từ mã có độ dài* l, *mỗi từ mã* $\mathbf{c}_k = (c_{k,0}, c_{k,1}, \ldots, c_{k,l-1})$ *với các dấu mã* $c_{k,i} \in GF(q)$ $(i = \overline{0, l-1})$. *Các từ mã* $\mathbf{c}_k$ *được gọi là các véc-tơ mã.*

- $\mathfrak{C}$: *bộ mã cơ số* q
- *Các từ mã* $\mathbf{c}_k$ *được gọi là từ mã, véc-tơ mã*
- M *là số từ mã của bộ mã* $\mathfrak{C}$.

Khối thông tin đầu vào là tập $\{\mathbf{m}_i\}$, trong đó $\mathbf{m}_i = (m_{i,0}, m_{i,1}, \ldots, m_{i,k-1})$ với $m_{i,j} \in GF(q)$. Tập $\{\mathbf{m}_i\}$ tạo thành một không gian véc-tơ trên $GF(q)$.

- Nếu các khối thông tin có cùng độ dài k thì số từ mã của bộ mã $\mathfrak{C}$ phải thỏa mãn $M = q^k$.
- Nếu các khối tin có độ dài thay đổi thì M không có dạng trên.
  - Các bộ mã hóa loại này khó thực thi hơn.

Một số định nghĩa và khái niệm cơ bản

Độ dư thừa mã, Tỷ số mã, Trọng số mã

Định nghĩa (Độ dư thừa của bộ mã)

Độ dư thừa của bộ mã $\mathfrak{C}$ *được định nghĩa là* $r = l - \log_q(M)$.

- *Nếu* $M = 2^k$ *thì* $r = l - k$.

Định nghĩa (Tỷ số mã hóa)

Tỷ số mã hóa R *được định nghĩa:* $R = \frac{\log_q(M)}{l}$

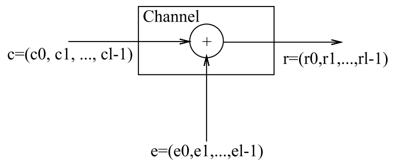
Định nghĩa (Trọng số của từ mã/cấu trúc lỗi)

Trọng số của một từ mã $\mathbf{c}$ *hoặc của một cấu trúc lỗi* $\mathbf{e}$ *là số vị trí khác 0 trong* $\mathbf{c}$ *hoặc* $\mathbf{e}$. *Kí hiệu là* $w(\mathbf{c})/w(\mathbf{e})$

- $0 \leq w(\mathbf{c}) \leq l$

Một số định nghĩa và khái niệm cơ bản

Mô hình mã truyền dẫn trong kênh có nhiễu



Hình: Mô hình kênh nhiễu cộng

- $\mathbf{c}$: từ mã phát, $\mathbf{e}$: cấu trúc lỗi, $\mathbf{r} = \mathbf{c} + \mathbf{e}$: véc-tơ thu.
  - Nếu không có lỗi thì véc-tơ thu là một từ mã hợp lệ.
- Định dạng điều chế, mức công suất phát, và mức nhiễu trên kênh quyết định xảy ra một cấu trúc lỗi trong q^l cấu trúc lỗi có thể.
- Máy thu thực hiện việc xem xét véc-tơ thu có phải là từ mã hợp lệ hay không: quá trình phát hiện lỗi.
- Khi máy thu phát hiện lỗi:
  1. Yêu cầu phát lại: thông qua ARQ
  2. HOẶC Đánh dấu từ mã lỗi: với các ứng dụng real-time (voice, video,...)
  3. HOẶC Sửa lỗi: FEC.

Một số định nghĩa và khái niệm cơ bản

Khoảng cách mã Hamming

Định nghĩa (Khoảng cách mã Hamming)

Khoảng cách Hamming giữa hai từ mã $\mathbf{c}_1$ và $\mathbf{c}_2$ là tổng số vị trí tương ứng trong hai từ mã mà chúng khác nhau.

$$d_{Hamming}(\mathbf{c}_1, \mathbf{c}_2) = d(\mathbf{c}_1, \mathbf{c}_2) = |\{i | c_{1,i} \neq c_{2,i}, i = 0, 1, ..., l-1\}|$$

- $d(\mathbf{c}_1, \mathbf{c}_2) = d(\mathbf{c}_2, \mathbf{c}_1)$.
- $0 \leq d(\mathbf{c}_1, \mathbf{c}_2) \leq l$.
- $d(\mathbf{c}_1, \mathbf{c}_2) + d(\mathbf{c}_2, \mathbf{c}_3) \geq d(\mathbf{c}_1, \mathbf{c}_3)$ (Bất đẳng thức tam giác).

Định nghĩa (Khoảng cách Hamming tối thiểu)

Khoảng cách mã tối thiểu, hay khoảng cách Hamming tối thiểu của một bộ mã khối $\mathfrak{C}$ là khoảng cách Hamming tối thiểu giữa tất cả các cặp từ mã phân biệt trong bộ mã.

$$d_{min} = d_0 = \min_{\forall \mathbf{c}_1, \mathbf{c}_2 \in \mathfrak{C}, \mathbf{c}_1 \neq \mathbf{c}_2} d(\mathbf{c}_1, \mathbf{c}_2)$$

Một số định nghĩa và khái niệm cơ bản

Các luật quyết định giải mã MAP và ML

Giả sử: $\{\mathbf{c}_i\} \sim p_c(\mathbf{c}_i)$, $\{\mathbf{r}_i\} \sim p_r(\mathbf{r}_i)$.

Định nghĩa (MAP)

Phương pháp giải mã cực đại xác suất hậu nghiệm (MAP-Maximum a Posteriori) sẽ quyết định từ mã đã phát là $\mathbf{c}_i$ nếu nó làm $p(\mathbf{c} = \mathbf{c}_i | \mathbf{r})$ đạt giá trị cực đại.

Định nghĩa (ML)

Phương pháp giải mã cực đại sự tương đồng (ML-Maximum Likelihood) sẽ quyết định từ mã đã phát là $\mathbf{c}_i$ nếu nó làm $p(\mathbf{r} | \mathbf{c} = \mathbf{c}_i)$ đạt giá trị cực đại.

- ML $\equiv$ MAP khi giả thiết các xác suất tiên nghiệm bằng nhau.
- Khi xác suất phát các từ mã không bằng nhau, xác suất giải mã sai của ML không đạt giá trị tối thiểu.
- ML tìm từ mã có khoảng cách mã với véc-tơ thu nhỏ nhất.

Một số định nghĩa và khái niệm cơ bản

Khả năng phát hiện và sửa lỗi của mã

Định lý (Khả năng phát hiện lỗi của bộ mã)

Một bộ mã có khoảng cách mã tối thiểu d_{min} có khả năng phát hiện tất cả các cấu trúc lỗi có trọng nhỏ hơn hoặc bằng $(d_{min} - 1)$.

- **Chú ý**: Một số bộ mã có thể phát hiện được các cấu trúc lỗi có trọng $\geq d_{min}$

Định lý (Khả năng sửa lỗi của bộ mã)

Một bộ mã có khoảng cách mã tối thiểu d_{min} có khả năng sửa được tất cả các cấu trúc lỗi có trọng nhỏ hơn hoặc bằng $\lfloor \frac{d_{min}-1}{2} \rfloor$ [a].

[a] $\lfloor x \rfloor$ là phần nguyên lớn nhất nhỏ hơn x

- **Chú ý**: Một số bộ mã có thể sửa được các cấu trúc lỗi có trọng $\lfloor \frac{d_{min}-1}{2} \rfloor + 1$ hoặc lớn hơn.

Một số định nghĩa và khái niệm cơ bản

Giới hạn Hamming, Giới hạn Gilbert

Định lý (Giới hạn Hamming)

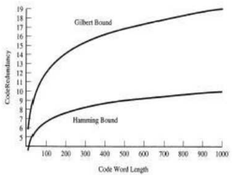
Một bộ mã khối cơ số q có độ dài từ mã l có khả năng sửa t lỗi thì độ dư thừa của bộ mã phải thỏa mãn:

$$r \geq \log_2(V_2(l,t))$$

Định lý (Giới hạn Gilbert)

Tồn tại một bộ mã cơ số q có độ dài từ mã l có khả năng sửa t lỗi với độ dư thừa thỏa mãn:

$$r \leq \log_q(V_q(l,2t))$$



Định nghĩa (Mã hoàn hảo)

Một bộ mã khối được cho là hoàn hảo nếu nó thỏa mãn giới hạn Hamming với dấu đẳng thức.

Một số định nghĩa và khái niệm cơ bản

Bộ giải mã hoàn chỉnh

Định nghĩa (Bộ giải mã hoàn chỉnh)

Một bộ giải mã sửa lỗi hoàn chỉnh (complete error correcting decoder) là bộ giải mã mà với một véc-tơ thu **r** *cho trước, nó sẽ chọn ra được từ mã* **c** *sao cho* $d(\mathbf{r},\mathbf{c})$ *đạt giá trị tối thiểu.*

- Bộ giải mã sửa lỗi hoàn chỉnh của hầu hết các kênh truyền là ML.
- Khi tồn tại nhiều hơn một từ mã **c** cùng làm cho $d(\mathbf{r},\mathbf{c})$ đạt cực tiểu thì bộ giải mã chọn ngẫu nhiên một trong các từ mã đó.
- Với một số mã, bộ giải mã sửa lỗi hoàn chỉnh hiệu quả vẫn chưa được tìm ra.

Định nghĩa

Với một véc-tơ thu **r** *cho trước, bộ giải mã có khả năng sửa t lỗi với khoảng cách giới hạn (t-error correcting bounded-distance decoder) sẽ chọn ra từ mã* **c** *để cho* $d(\mathbf{r},\mathbf{c})$ *đạt giá trị cực tiểu nếu và chỉ nếu tồn tại từ mã* **c** *sao cho* $d(\mathbf{r},\mathbf{c}) \leq t$*. Nếu không tồn tại từ mã* **c** *như vậy thì bộ mã sẽ thông báo việc giải mã bị thất bại.*

Một số định nghĩa và khái niệm cơ bản

Mã hoàn hảo

Định lý

Số từ mã của một bộ mã hoàn chỉnh cơ số q phải có dạng $M = q^k$*, với k là một hằng số dương nào đó.*

- Một bộ mã hoàn hảo cơ số q có khả năng sửa t lỗi có q^k từ mã với độ dài từ mã bằng l, bộ tham số $\{q,l,k,t\}$ thỏa mãn phương trình:

$$\sum_{j=0}^{t} \binom{l}{j}(q-1)^j = q^{l-k}$$

Định lý

Bất cứ bộ mã hoàn hảo nào cũng phải có cùng độ dài từ mã l, cùng bộ dấu mã $GF(q)$*, và cùng số lượng từ mã* $M = q^k$ *như các mã Hamming, Golay, hoặc mã lặp.*

Một số định nghĩa và khái niệm cơ bản

Cầu Hamming

Định nghĩa

Một cầu Hamming bán kính t chứa tất cả các véc-tơ thu có khoảng cách Hamming $\leq t$ *so với từ mã đã phát. Trên* $GF(q)$*, dung tích cầu* $V_2(l,t)$*:*
$V_q(l,t) = \sum_{j=1}^{t} \binom{l}{j}(q-1)^j$

- $V_q(l,t)$: số véc-tơ trong cầu bán kính t trong không gian l-chiều trên $GF(q)$.
- Nếu **r** thuộc cầu Hamming của từ mã **c**, thì bộ giải mã sẽ quyết định từ mã đã phát là **c**.
- Nếu **r** thuộc vùng biên ngoài giữa các cầu Hamming của các từ mã $\mathbf{c}_i$, thì bộ giải mã sẽ thông báo giải mã thất bại (đối với bộ giải mã độ dài giới hạn), hoặc quyết định từ mã đã phát là $\mathbf{c}_j$ nào đó gần **r** nhất (đối với bộ giải mã hoàn chỉnh).

Mã khối tuyến tính

Ma trận kiểm tra tính chẵn lẻ

Với $\mathfrak{C}$, tồn tại $\mathfrak{C}^{\perp}$ là không gian véc-tơ đối ngẫu $(l-k)$ chiều.

Gọi $\{\mathbf{h}_0, \mathbf{h}_1, \ldots, \mathbf{h}_{l-k-1}\}$ là cơ sở của $\mathfrak{C}^{\perp}$. $\Rightarrow$ Ma trận sinh $\mathbf{H}(l-k \times l)$ của $\mathfrak{C}^{\perp}$:

$$\mathbf{H} = \begin{pmatrix} \mathbf{h}_0 \\ \mathbf{h}_1 \\ \cdots \\ \mathbf{h}_{l-k-1} \end{pmatrix} = \begin{pmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,l-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{l-k-1,0} & h_{l-k-1,1} & \cdots & h_{l-k-1,l-1} \end{pmatrix}$$

- $\mathbf{H}$ là ma trận kiểm tra chẵn lẻ của mã $\mathfrak{C}$
- $\mathbf{G}\mathbf{H}^T = \mathbf{0}$.

Định lý

Một véc-tơ $\mathbf{c}$ là một từ mã thuộc $\mathfrak{C}$ nếu và chỉ nếu $\mathbf{c}\mathbf{H}^T = \mathbf{0}$

- $\mathbf{c}\mathbf{H}^T = \mathbf{0}$ gọi là biểu thức kiểm tra chẵn lẻ.

Mã khối tuyến tính

Định nghĩa

Định nghĩa (Mã khối tuyến tính)

Xét một bộ mã khối $\mathfrak{C}$ gồm các từ mã độ dài l $\{(c_{k,0}, c_{k,1}, \ldots, c_{k,l-1})\}$ với các dấu mã thuộc $GF(q)$. Bộ mã khối $\mathfrak{C}$ là một bộ mã khối tuyến tính cơ số q nếu và chỉ nếu $\mathfrak{C}$ tạo thành một không gian véc-tơ con trên $GF(2)$.

Định nghĩa (Chiều của một bộ mã khối)

Chiều của một bộ mã khối là chiều của không gian véc-tơ tương ứng.

- Ký hiệu: $\mathfrak{C}(l,k)$ hoặc $\mathfrak{C}(l,k,d_0)$.

1. Tổ hợp tuyến tính của một tập các từ mã bất kỳ là một từ mã $\Rightarrow$ $\mathfrak{C}$ luôn chứa từ mã toàn 0
2. Khoảng cách mã tối thiểu của bộ mã khối tuyến tính bằng trọng số của một từ mã có trọng số nhỏ nhất khác từ mã toàn không.
3. Các cấu trúc lỗi không thể phát hiện được của bộ mã độc lập với từ mã phát và luôn chứa tập tất cả các từ mã không toàn 0.

Mã khối tuyến tính

Ma trận kiểm tra tính chẵn lẻ và khoảng cách mã

Định lý

Giả sử bộ mã $\mathfrak{C}$ có ma trận kiểm tra tính chẵn lẻ $\mathbf{H}$. Khoảng cách mã tối thiểu của bộ mã $\mathfrak{C}$ bằng số cột tối thiểu khác 0 của $\mathbf{H}$ mà tổ hợp tuyến tính không tầm thường của chúng bằng 0.

Định lý (Giới hạn Singleton)

Với bộ mã khối tuyến tính $\mathfrak{C}(l,k)$, khoảng cách mã tối thiểu thỏa mãn bất đẳng thức:

$$d_{min} \le l - k + 1$$

Mã khối tuyến tính

Ma trận sinh của mã khối tuyến tính

Gọi $\{\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{k-1}\}$ là cơ sở của các từ mã trong bộ mã $\mathfrak{C}(l,k)$.

Ma trận sinh $\mathbf{G}(k \times l)$của bộ mã được thành lập như sau:

$$\mathbf{G} = \begin{pmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \cdots \\ \mathbf{g}_{k-1} \end{pmatrix} = \begin{pmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,l-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,l-1} \end{pmatrix}$$

Gọi $\mathbf{a} = (a_0, a_1, \ldots, a_{k-1})$ là khối dữ liệu đầu vào (bản tin) cần mã hóa.

Từ mã thu được từ phép mã hóa:

$$\begin{aligned} \mathbf{c} &= \mathbf{aG} = [a_0, a_1, \ldots, a_{k-1}]\mathbf{G} \\ &= a_0\mathbf{g}_0 + a_1\mathbf{g}_1 + \cdots + a_{k-1}\mathbf{g}_{k-1} \end{aligned}$$

Mã khối tuyến tính

Một số phương pháp giải mã: Phương pháp sử dụng bảng chuẩn - Giải mã

$$
\begin{array}{cccccc}
\mathbf{c}_0 & \mathbf{c}_1 & \dots & \mathbf{c}_k & \dots & \mathbf{c}_{M-1} \\
\vdots & \vdots & \dots & \dots & \dots & \vdots \\
\mathbf{e}_k & \dots & \dots & \mathbf{r} & \dots & \dots \\
\vdots & \vdots & \dots & \dots & \dots & \vdots
\end{array}
$$

Giải mã:

- Tra trong bảng chuẩn, tìm véc-tơ nào bằng véc-tơ thu $\mathbf{r}$, khi đó đầu cột là từ mã cần tìm, đầu hàng là cấu trúc lỗi.

Nhận xét:

- Mỗi véc-tơ trong hàng có cùng mẫu lỗi ở cột đầu tiên cùng hàng .
- Một số cấu trúc lỗi có thể là thành phần trong bảng (không ở cột đầu).
- Tốn bộ nhớ để lưu bảng nếu làm việc với bộ mã có độ dài từ mã lớn.

Mã khối tuyến tính

Mã khối tuyến tính hệ thống

Định nghĩa (Mã khối tuyến tính hệ thống)

Mã khối tuyến tính hệ thống $\mathfrak{C}(l,k)$ thực hiện việc ánh xạ bản tin (khối dữ liệu) độ dài k thành một véc-tơ/từ mã độ dài l sao cho trong số l bít có thể chỉ ra k bít bản tin và số còn lại $l-k$ bít kiểm tra tính chẵn lẻ.

Giả sử từ mã xây dựng mã có dạng $\mathbf{c} = [\mathbf{p}_1 \mid \mathbf{a}]$

- $\mathbf{a}$: khối thông tin (bản tin) độ dài k; $\mathbf{p}_1$: khối bít kiểm tra độ dài $l-k$

$\mathbf{G} \xrightarrow{\text{phương pháp khử Gausse}} \mathbf{G} = [\mathbf{P} \mid \mathbf{I}_k]$

- $\mathbf{P}_{(k\times l-k)}$: ma trận tạo dấu kiểm tra
- $\mathbf{I}_{(k\times k)}$: ma trận đơn vị.

$\Rightarrow \mathbf{H} = [\mathbf{I}_{l-k} \mid -\mathbf{P}^T]$

- $\Rightarrow \mathbf{G}\mathbf{H}^T = \mathbf{0}$

Chú ý: Nếu xét $\mathbf{c} = [\mathbf{a} \mid \mathbf{p}_1]$

- $\mathbf{G} = [\mathbf{I}_k \mid \mathbf{P}]$
- $\Rightarrow \mathbf{H} = [-\mathbf{P}^T \mid \mathbf{I}_{l-k}]$

Mã khối tuyến tính

Một số phương pháp giải mã: Phương pháp sử bảng Syndrome

Định nghĩa

Véc-tơ Syndrome $\mathbf{s}$ của một véc-tơ thu $\mathbf{r}$ được xác định: $\mathbf{s} = \mathbf{r}\mathbf{H}^T$

$\mathbf{s} = \mathbf{e}\mathbf{H}^T$

- $\mathbf{s}$ là một hàm của cấu trúc lỗi $\mathbf{e}$ và độc lập với từ mã đã phát $\mathbf{c}$.
- Tất cả các véc-tơ của cùng một hàng trong bảng chuẩn có cùng véc-tơ $\mathbf{s}$.
- $\Rightarrow$ Chỉ cần lưu các phần tử đầu hàng của bảng chuẩn và các véc-tơ $\mathbf{s}$ tương ứng. Bảng này gọi là bảng Syndrome.

$$
\begin{array}{cc}
\mathbf{e}_0 & \mathbf{e}_0\mathbf{H}^T \\
\vdots & \vdots
\end{array}
$$

- Với véc-tơ $\mathbf{s}$, tra cấu trúc lỗi tương ứng, $\Rightarrow$ vị trí sai.

Mã khối tuyến tính

Một số phương pháp giải mã: Phương pháp sử dụng bảng chuẩn - Lập bảng chuẩn

1. Rút từ V_2^l (tập tất cả các véc-tơ độ dài l trên $GF(2)$) ra các từ mã $\mathbf{c}_i$ của bộ mã $\mathbf{C}$. Viết các từ mã này trên đầu các cột, bắt đầu từ từ mã toàn 0.
2. Từ phần còn lại của V_2^l, rút một véc-tơ có $\mathbf{e}_i$ trọng nhỏ nhất và viết nó vào cột đầu ngay dưới từ mã toàn 0. Trên hàng của $\mathbf{e}_i$, lấy $\mathbf{e}_i$ kết với đầu các cột được $\mathbf{r}_i$ và ghi vào vị trí cùng hàng của cột tương ứng. Xóa các véc-tơ $\mathbf{r}_i$ trong phần còn lại của V_2^l.
3. Lặp lại bước 2 cho đến hết.

$$
\begin{array}{cccc}
\mathbf{c}_0 & \mathbf{c}_1 & \dots & \mathbf{c}_{M-1} \\
\mathbf{e}_1 & \mathbf{c}_1+\mathbf{e}_1 & \dots & \mathbf{c}_{M-1}+\mathbf{e}_1 \\
\vdots & \vdots & \dots & \vdots
\end{array}
$$

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Ví dụ

Ví dụ

Xét bộ mã nhị phân đều chiều dài l (ví dụ bộ mã nhị phân đều chiều dài 2: $\mathfrak{C} = (00), (01), (11), (10)$). Giả sử kết quả mã hóa được truyền qua kênh nhị phân rời rạc đối xứng không nhớ (BSC) có xác suất truyền sai p_0, các bít được phát đi độc lập nhau, và xác suất phát đi bít 0 và bít 1 tương đương nhau.

1. *Tính xác suất thu được một từ mã đúng.*
2. *Giả sử xác suất sai cho phép đối với việc thu các từ mã là p_a, tìm điều kiện đối với p_0 để có thể sử dụng được bộ mã cho việc thông tin qua kênh.*

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Xác suất sai qua kênh AWGN

Thực hiện việc truyền tín hiệu nhị phân qua kênh AWGN với nhiễu có PSD là $\frac{N_0}{2}$.

- Bít 1: $s_1(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t)$
- Bít 0: $s_2(t) = \sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t + \pi) = -\sqrt{\frac{2E_b}{T_b}}\cos(2\pi f_c t)$

trong đó $0 \le t < T_b$, E_b là năng lượng được phát đi cho mỗi bít, $f_c = n_c/T_b$ với $n_c \in Z^+$.

- $\Rightarrow$ cơ sở không gian tín hiệu $\Phi(t) = \sqrt{\frac{2}{T_b}}cos(2\pi f_c t)$, $0 \le t < T_b$
  - $\Rightarrow s_1(t) = \sqrt{E_b}\Phi(t)$ $s_2(t) = -\sqrt{E_b}\Phi(t)$

$p = p_e = Q(\sqrt{\frac{2E_b}{N_0}})$

Một cách tổng quát: $p = p_e = Q(\frac{d_{min}}{\sqrt{2N_0}})$

Mã khối tuyến tính

Phân bố trọng số của bộ mã

Định nghĩa (Phân bố trọng số của bộ mã)

Phân bố trọng số của một bộ mã khối $\mathfrak{C}(l, k)$ là dãy các hệ số $A_0, A_1, A_2, \ldots, A_l$. Trong đó A_i là số từ mã có trọng là i.

- Phân bố trọng số của bộ mã thường được biểu diễn dưới dạng đa thức, gọi là đa thức liệt kê trọng:

$$A(x) = A_0 + A_1x + A_2x^2 + \cdots + A_lx^l$$

- Phân bố trọng của nhiều bộ mã hiện vẫn chưa biết.

Định lý

Gọi $A(x)$ và $B(x)$ là các đa thức liệt kê trọng tương ứng của các bộ mã $\mathfrak{C}(l, k)$ và bộ mã đối ngẫu tương ứng $\mathfrak{C}^\perp$. Khi đó, $A(x)$ và $B(x)$ thỏa mãn biểu thức:

$$B(x) = 2^{-k}(1+x)^l A\left[\frac{(1-x)}{(1+x)}\right]$$

Mã khối tuyến tính

Mã Hamming nhị phân

- Mã Hamming nhị phân $\mathfrak{C}(l = 2^m - 1, k = 2^m - m - 1, t = 1)$, $m \ge 2$
  - $\Rightarrow r = m$
- Ma trận kiểm tra của mã Hamming nhị phân xây dựng đơn giản.
  - Các cột của $\mathbf{H}$ là các véc-tơ khác không có độ dài m

Thuật toán giải mã Hamming nhị phân

1. Tính véc-tơ Syndrome $\mathbf{s}$. Nếu $\mathbf{s} = \mathbf{0}$ nhảy đến bước 4.
2. Xác định vị trí cột j nào đó của $\mathbf{H}$ mà cột đó bằng $\mathbf{s}^T$.
3. Lấy phần bù của vị trí thứ j (vừa tìm được) trong từ mã thu được.
4. In ra từ mã và kết thúc.

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Đánh giá khả năng phát hiện lỗi

Cho $\mathfrak{C}(l, k, d_{min})$ truyền qua kênh BSC có xác suất chuyển sai p.

- $P_u(E)$: xác suất véct-tơ thu có lỗi mà không phát hiện được.
- $P_e(E)$: xác suất véc-tơ thu có lỗi.
- $P_d(E)$: xác suất véc-tơ thu có lỗi được phát hiện.

$$\begin{aligned}
P_u(E) &\leq \sum_{j=d_{min}}^{l} \binom{l}{j} p^j (1-p)^{l-j} = 1 - \sum_{j=0}^{d_{min}-1} \binom{l}{j} p^j (1-p)^{l-j} \\
P_u(E) &= \sum_{j=d_{min}}^{l} A_j p^j (1-p)^{l-j} \\
P_e(E) &= \sum_{j=1}^{l} \binom{l}{j} p^j (1-p)^{l-j} = 1 - (1-p)^l \\
P_d(E) &= P_e(E) - P_u(E) = 1 - (1-p)^l - P_u(E)
\end{aligned}$$

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Đánh giá khả năng phát hiện lỗi (cont.)

- P_{u_b}: tỷ lệ bít lỗi không được phát hiện
  - $\triangleq$ xác suất bít thông tin nhận được bị lỗi trong một từ mã bị tác động bởi cấu trúc lỗi không phát hiện được
  - $P_u(E) \geq P_{u_b}(E) \geq \frac{1}{k} P_u(E)$
- P_{d_b}: tỷ lệ bít lỗi được phát hiện
  - $\triangleq$ xác suất bít thông tin nhận được bị lỗi trong một từ mã bị tác động bởi cấu trúc lỗi có thể phát hiện được.
  - $P_d(E) \geq P_{d_b}(E) \geq \frac{1}{k} P_d(E)$
- Nếu biết phân bố trọng của bộ mã, P_{u_b} có thể tính một cách chính xác:

$$P_{u_b} = \sum_{j=d_{min}}^{l} \frac{B_j}{k} p^j (1-p)^{l-j}$$

trong đó B_j là tổng trọng của các khối tin tương ứng với tất cả các từ mã có trọng là i.

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Đánh giá khả năng sửa lỗi

Cho $\mathfrak{C}(l, k, d_{min})$ truyền qua kênh BSC có xác suất chuyển sai p.

Xét bộ giải mã có độ dài giới hạn.

- $P(E)$: xác suất giải mã sai

$$P(E) \leq \sum_{j=\lfloor \frac{d_{min}-1}{2} \rfloor + 1}^{l} \binom{l}{j} p^j (1-p)^{l-j} = 1 - \sum_{j=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} \binom{l}{j} p^j (1-p)^{l-j}$$

Đẳng thức xảy ra chỉ khi mã là hoàn hảo.

- $P(F)$: xác suất giải mã thất bại

$$P(F) \leq 1 - \sum_{j=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} \binom{l}{j} p^j (1-p)^{l-j}$$

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC

Đánh giá khả năng sửa lỗi (cont')

Xét $\mathfrak{C}(l, k, d_{min})$ với phân bố trọng số đã biết $\{A_i\}$

$P_k^j \triangleq$ xác suất một véc-tơ thu có khoảng cách Hamming chính xác là k so với một từ mã có trọng là j.

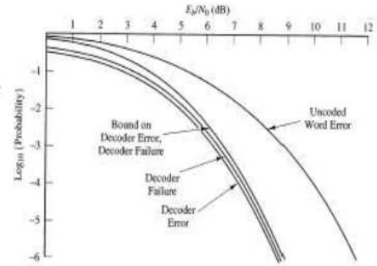
$$P_k^j = \sum_{r=0}^{k} \binom{j}{k-r} \binom{l-j}{r} p^{j-k+2r} (1-p)^{l-j+k-2r}$$

$$\begin{aligned}
P(E) &= \sum_{j=d_{min}}^{l} A_j \sum_{k=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} P_k^j \\
P(F) &= 1 - \sum_{j=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} \binom{l}{j} p^j (1-p)^{l-j} - P(E)
\end{aligned}$$

Đánh giá mã khối nhị phân tuyến tính trên kênh BSC
Đánh giá khả năng sửa lỗi (cont')

- Nếu biết được mối quan hệ giữa trọng số của các khối tin và trọng số các từ mã tương ứng
  - $\Rightarrow B_j$
- $\Rightarrow$

$$BER = P_b(E) = \frac{1}{k}\sum_{j=d_{min}}^{l} B_j \sum_{k=0}^{\lfloor \frac{d_{min}-1}{2} \rfloor} P_k^j$$



Chú ý: Thường, thông tin $\{B_j\}$ không khả thi.

- $\Rightarrow$ Chủ yếu dựa vào các đánh giá biên

$$P(E) \geq P_b(E) \geq \frac{1}{k}P(E)$$

Các vấn đề khi thiết kế mã khối tuyến tính
Thiết kế mã khối tuyến tính tối ưu

Khi thiết kế, ta mong muốn có được bộ mã có độ dư thừa nhỏ nhất có thể, nhưng lại có khả năng phát hiện và sửa lỗi lớn nhất có thể.

Trường hợp 1

Với k và d_{min} cho trước, xây dựng bộ mã có độ dư thừa tối thiểu: $\min\{l\}$.
Độ dài từ mã của bộ mã thỏa mãn giới hạn Griesmer:

$$l \geq \sum_{i=0}^{k-1} \lceil \frac{d_{min}}{2^i} \rceil$$

$\lceil x \rceil$: phần nguyên nhỏ nhất lớn hơn hoặc bằng x.

Các vấn đề khi thiết kế mã khối tuyến tính
Thiết kế mã khối tuyến tính tối ưu (cont')

Trường hợp 2

Với l và k cho trước, xây dựng bộ mã có khả năng phát hiện và sửa sai lớn nhất: $\max\{d_{min}\}$.
Khoảng cách Hamming tối thiểu của bộ mã thỏa mãn giới hạn Plotkin:

$$d_{min} \leq \frac{l \times 2^{k-1}}{2^k - 1}$$

Trường hợp 3

Với l và khả năng sửa sai t cho trước, xây dựng bộ mã có độ dư thừa nhỏ nhất: $\max\{k\}$.
Mối liên hệ giữa l, k và t thỏa mãn giới hạn Hamming:

$$2^{l-k} \geq \sum_{i=0}^{t} \binom{l}{i}$$

Kết thúc phần mã khối tuyến tính