Reed-Muller Codes

Hamid Meghdadi

Semnan University

Review: Linear Block Codes

➢ماتریس مولد

$$\boldsymbol{v} = a_0\boldsymbol{g_0} + a_1\boldsymbol{g_1} + \cdots a_{k-1}\boldsymbol{g_{k-1}}$$

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{g_0} \\ \boldsymbol{g_1} \\ \vdots \\ \boldsymbol{g_{k-1}} \end{bmatrix} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,k} \end{bmatrix}$$

$$\boldsymbol{v} = \boldsymbol{u}.\boldsymbol{G}$$

➢ماتریس parity-check

$$\boldsymbol{G}_{k\times n}\boldsymbol{H}^T{}_{n\times n-k} = \boldsymbol{0}_{k\times n-k}$$

$$\boldsymbol{v} \in \mathcal{C} \Leftrightarrow \boldsymbol{v}_{1\times n}\boldsymbol{H}^T{}_{n\times n-k} = \boldsymbol{0}_{1\times n-k}$$

$$\mathbf{G}_{k\times n} = [\mathbf{P}_{k\times n-k} \mid \mathbf{I}_{k\times k}] \qquad \mathbf{H}_{n\times n-k} = [\mathbf{I}_{n-k\times n-k} \mid \mathbf{P}^T{}_{n-k\times k}]$$

➢جدول سندروم

$$\boldsymbol{S} = \boldsymbol{r}\boldsymbol{H}^T = (\boldsymbol{v}+\boldsymbol{e})\boldsymbol{H}^T = \boldsymbol{v}\boldsymbol{H}^T + \boldsymbol{e}\boldsymbol{H}^T = \boldsymbol{e}\boldsymbol{H}^T$$

Introduction

- در ۱۹۵۴ توسط Muller معرفی شدند.
- در ۱۹۵۴ Reed الگوریتم decode کردن آنها را ارائه کرد.
- برای هر دو عدد صحیح m و $0 \le r \le m$ کد باینری RM مرتبهٔ r را با RM(r,m) نشان می‌دهیم:
  - طول کد: $n = 2^m$
  - بعد (طول پیام): $k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$
  - حداقل فاصله: $d_{\min} = 2^{m-r}$
- مثلاً، به ازای $m = 5$ و $r = 2$:
  - RM(2,5)
  - یک کد بلوکی خطی (32,16)
  - حداقل فاصله 8

Algebraic Method

➢ تعریف: بردار باینری $\mathbf{v}_i$ به طول $n = 2^m$ ($1 \le i \le m$):

$$\mathbf{v}_i = [\underbrace{0\ldots0}_{2^{i-1}}, \underbrace{1\ldots1}_{2^{i-1}}, \underbrace{0\ldots0}_{2^{i-1}}, \ldots\ldots, \underbrace{1\ldots1}_{2^{i-1}}]$$

- مثلاً به ازای $m = 4$:

$$\mathbf{v}_1 = [0101\ 0101\ 0101\ 0101]$$
$$\mathbf{v}_2 = [0011\ 0011\ 0011\ 0011]$$
$$\mathbf{v}_3 = [0000\ 1111\ 0000\ 1111]$$
$$\mathbf{v}_4 = [0000\ 0000\ 1111\ 1111]$$

➢ بردار بردار باینری $\mathbf{v}_0$ بردار تمام-یک است:

$$\mathbf{v}_0 = [1111\ 1111\ 1111\ 1111]$$

حاصل‌ضرب مرتبهٔ l
دارای وزن 2^{m-l}

$$\mathbf{G}_{RM}(r,m) = \begin{array}{l} \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m, \\ \mathbf{v}_1\mathbf{v}_2, \mathbf{v}_1\mathbf{v}_3, \cdots, \mathbf{v}_{m-1}\mathbf{v}_m, \\ \vdots, \\ \text{up to products of degree } r\} \end{array}$$

$$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$$

Kronecker Product

➢ تعریف:

$$\mathbf{A}\otimes\mathbf{B}=\begin{bmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B}\end{bmatrix}, \quad \begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix}\otimes\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix}=\begin{bmatrix} 1\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} & 2\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} \\ 3\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix} & 4\begin{bmatrix}0 & 5\\ 6 & 7\end{bmatrix}\end{bmatrix}=\begin{bmatrix}0 & 5 & 0 & 10\\ 6 & 7 & 12 & 14\\ 0 & 15 & 0 & 20\\ 18 & 21 & 24 & 28\end{bmatrix}$$

➢ ماتریس سازنده:

$$\mathbf{G}_{(2,2)}\triangleq\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix} \qquad \mathbf{G}_{(2^m,2^m)}\triangleq\underbrace{\mathbf{G}_{(2,2)}\otimes\mathbf{G}_{(2,2)}\cdots\otimes\mathbf{G}_{(2,2)}}_{m\ \text{times}}$$

➢ ماتریس مولد $\mathbf{G}_{RM}(r,m)$ سطرهایی از $\mathbf{G}_{(2^m,2^m)}$ است که دارای وزن 2^{m-r} یا بیشتر باشد.

u|u+v Construction

- قضیه: به ازای $i = 1,2$، فرض کنید C_i یک کد خطی (n,k_i) با حداقل فاصلهٔ d_i باشد و $d_2 > d_1$.

در این صورت، کد زیر:

$$C = (C_1 | C_1 + C_2) = \{\mathbf{u}|\mathbf{u}+\mathbf{v} : \mathbf{u} \in C_1, \mathbf{v} \in C2\}$$

یک کد خطی $(2n,k_1 + k_2)$ با حداقل فاصلهٔ $d_{min} = \min(2\mathrm{d}_1,\mathrm{d}_2)$ است.

- ساخت کد RM:

$$RM(r,m) = \{\mathbf{u}|\mathbf{u}+\mathbf{v} : \quad \mathbf{u} \in RM(r,m-1), \\ \mathbf{v} \in RM(r-1,m-1)\}$$

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

Structural Properties

- توزیع وزن
  - هر حاصل‌ضرب مرتبهٔ l دقیقاً دارای وزن 2^{m-l} است.
  - دقیقاً $\binom{m}{l}$ کلمهٔ کد با وزن 2^{m-l} داریم
  - حداقل فاصله: $d_{min} = 2^{m-r}$

- زنجیرهٔ شمول:

$$RM(0,m) \subset RM(1,m) \subset \cdots \subset RM(r,m)$$

- کد $RM(m-r-1,m)$ دوگان کد $RM(r,m)$ است.

Special Cases

- RM(0,m)
  - Repetition code
- RM(m-1,m)
  - Single parity check
- RM(m-2,m)
  - Extended Hamming code
- به ازای m فرد: $\mathrm{RM}(\frac{m-1}{2},m)$
  - Self-dual
  - RM(0,1)، RM(1,3)، RM(2,5)، …

$n = 2^m$

$k = 1 + \binom{m}{1} + \binom{m}{2} + \cdots + \binom{m}{r}$

$\mathbf{v}_0 = [1111\ 1111\ 1111\ 1111]$

$\mathbf{v}_1 = [0101\ 0101\ 0101\ 0101]$

$\mathbf{v}_2 = [0011\ 0011\ 0011\ 0011]$

$\mathbf{v}_3 = [0000\ 1111\ 0000\ 1111]$

$\mathbf{v}_4 = [0000\ 0000\ 1111\ 1111]$

$$\mathbf{G}_{RM}(r,m) = \begin{array}{l} \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_m, \\ \mathbf{v}_1\mathbf{v}_2, \mathbf{v}_1\mathbf{v}_3, \cdots, \mathbf{v}_{m-1}\mathbf{v}_m, \\ \vdots, \\ \text{up to products of degree } r\} \end{array}$$

Example (r=1)

RM(1,3) ➤

$$\mathbf{v}_0 = [1111\ 1111]$$
$$\mathbf{v}_1 = [0101\ 0101]$$
$$\mathbf{v}_2 = [0011\ 0011]$$
$$\mathbf{v}_3 = [0000\ 1111]$$

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

$$\mathbf{v} = a_0\mathbf{v}_0 + a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3$$

$$\mathbf{v} = [a_0 , a_0 + a_1 , a_0 + a_2 , a_0 + a_1 + a_2 , a_0 + a_3 , a_0 + a_1 + a_3 , a_0 + a_2 + a_3 , a_0 + a_1 + a_2 + a_3]$$

$$\mathbf{r} = [y_0 \quad y_1 \quad y_2 \quad y_3 \quad y_4 \quad y_5 \quad y_6 \quad y_7]$$

$$a_1 = y_0 + y_1 = y_2 + y_3 = y_4 + y_5 = y_6 + y_7$$

$$a_2 = y_0 + y_2 = y_1 + y_3 = y_4 + y_6 = y_5 + y_7 \qquad \mathbf{r} + a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + a_3\mathbf{v}_3$$

$$a_3 = y_0 + y_4 = y_1 + y_5 = y_2 + y_6 = y_3 + y_7$$

Example (r=2)

RM(4,2)

$\mathbf{v}_0$	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
$\mathbf{v}_4$	0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
$\mathbf{v}_3$	0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
$\mathbf{v}_2$	0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
$\mathbf{v}_1$	0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
$\mathbf{v}_3\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 1
$\mathbf{v}_2\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 0 1 1 0 0 1 1
$\mathbf{v}_1\mathbf{v}_4$	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1
$\mathbf{v}_2\mathbf{v}_3$	0 0 0 0 0 0 1 1 0 0 0 0 0 0 1 1
$\mathbf{v}_1\mathbf{v}_3$	0 0 0 0 0 1 0 1 0 0 0 0 0 1 0 1
$\mathbf{v}_1\mathbf{v}_2$	0 0 0 1 0 0 0 1 0 0 0 1 0 0 0 1

$$\mathbf{v} = a_0\mathbf{v}_0 + a_4\mathbf{v}_4 + a_3\mathbf{v}_3 + a_2\mathbf{v}_2 + a_1\mathbf{v}_1$$
$$+ a_{34}\mathbf{v}_3\mathbf{v}_4 + a_{24}\mathbf{v}_2\mathbf{v}_4 + a_{14}\mathbf{v}_1\mathbf{v}_4 + a_{23}\mathbf{v}_2\mathbf{v}_3 + a_{13}\mathbf{v}_1\mathbf{v}_3 + a_{12}\mathbf{v}_1\mathbf{v}_2$$

$$\mathbf{r}^{(1)} = \mathbf{r}^{(0)} - a_{34}\mathbf{v}_3\mathbf{v}_4 - a_{24}\mathbf{v}_2\mathbf{v}_4 - a_{14}\mathbf{v}_1\mathbf{v}_4 - a_{23}\mathbf{v}_2\mathbf{v}_3 - a_{13}\mathbf{v}_1\mathbf{v}_3 - a_{12}\mathbf{v}_1\mathbf{v}_2$$

$$\mathbf{v}^{(1)} = \mathbf{v}^{(0)} - a_{34}\mathbf{v}_3\mathbf{v}_4 - a_{24}\mathbf{v}_2\mathbf{v}_4 - a_{14}\mathbf{v}_1\mathbf{v}_4 - a_{23}\mathbf{v}_2\mathbf{v}_3 - a_{13}\mathbf{v}_1\mathbf{v}_3 - a_{12}\mathbf{v}_1\mathbf{v}_2$$
$$= a_0\mathbf{v}_0 + a_4\mathbf{v}_4 + a_3\mathbf{v}_3 + a_2\mathbf{v}_2 + a_1\mathbf{v}_1$$

Excercise

- مهلت: دو هفته
- ساده نیست!
- تولید **G** با استفاده از دو روش از سه روش معرفی شده

```
function g=ReedMuller1(m,r)
```

- پیاده‌سازی الگوریتم Majority Logic برای کد RM در حالت کلی با روش معرفی شده در کتاب (ص ۱۱۰ و ۱۱۱)
- پیاده‌سازی الگوریتم Optimal برای کد RM در حالت کلی:
  - ماتریس **H** با استفاده از کد dual، پیاده سازی با استفاده از توابع شخصی لازم است
  - سیستماتیک کردن ماتریس **G** و به دست آوردن **H**، پیاده سازی فقط با استفاده از توابع متلب ممکن است
- مقایسهٔ دو روش بالا از نظر زمان و عملکرد
- یک ارائه
  - فقط برای استاد
  - حدود نیم ساعت
  - روش، الگوریتم، کد، نتایج، تحلیل
  - بهترین ارائه، +۱، ارائه در کلاس