Теория кодирования

Гошин Егор Вячеславович, к.т.н., доцент
кафедры суперкомпьютеров и общей информатики

Расширенный код Голея

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

Код Голея

1. Порождающая матрица кода Голея имеет вид $G = [I, B]$. Длина равна 24, размерность – 12.
2. Проверочная матрица кода Голея имеет вид $H = \begin{bmatrix} I \\ B \end{bmatrix}$.
3. Кодовое расстояние кода Голея равно 8.
4. Код Голея исправляет трёхкратные ошибки.

Декодирование расширенного кода Голея

1. Вычислить синдром $s = wH$.
2. Если $wt(s) \leq 3, u = [s, 0]$.
3. Если $wt(s + b_i) \leq 2$ для какой-либо строки b_i из $B, u = [s + b_i, e_i]$, где e_i – строка с единственной единицей в позиции i.
4. Вычислить второй синдром sB.
5. Если $wt(sB) \leq 3, u = [0, sB]$.
6. Если $wt(sB + b_i) \leq 2$ для какой-либо строки b_i из $B, u = [e_i, sB + b_i]$.
7. Если ошибка не определена, запросить повторную отправку сообщения.

Пример

Пусть принято сообщение $w = [0\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0]$

- 1. $s = wH = [1\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1]$
- 2. $wt(s) = 6 > 3$

Пример

3. $wt(s + b_i)$:

- $wt(s + b_5) = wt([0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0]\ ) = 1 \leq 2$:
- $u = [[0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0], [0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0]]$

Код Рида-Маллера

Код Рида-Маллера порядка r и длины 2^m будет обозначаться $RM(r, m)$, где $0 \le r \le m$.

Рассмотрим рекурсивное задание этого кода:

1. $RM(0, m) = \{00 \dots 0{,}11 \dots 1\}, \; RM(m, m) = K^{2^m}$.
2. $RM(r, m) = \{(x, x + y) \mid x \in RM(r, m-1), y \in RM(r-1, m-1)\}$, $0 < r < m$.

На практике используют рекурсивное задание порождающей матрицы.

Порождающая матрица кода Рида-Маллера

- Для $0 < r < m$:

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

- Для $r = 0$:

$$G(0, m) = [11 \ldots 1]$$

- Для $r = m$:

$$G(m, m) = \begin{bmatrix} G(m-1, m) \\ 0 \ldots 01 \end{bmatrix}$$

Порождающие матрицы для $RM(r, 1)$

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

$$G(1,1) = \begin{bmatrix} G(0,1) \\ 0 \quad 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Порождающие матрицы для $RM(r, 2)$

$$G(0,2) = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G(2,2) = \begin{bmatrix} & G(1,2) & & \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Порождающие матрицы для $RM(r,3)$

$$G(0,3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Код Рида-Маллера

Код Рида-Маллера $RM(r, m)$ с такой рекурсивно-сформированной порождающей матрицей обладает свойствами:

1. Длина $n = 2^m$.
2. Размерность $k = \sum_{i=0}^{r} C_m^i$
3. Кодовое расстояние $d = 2^{m-r}$

Произведение Кронекера

Определим произведение Кронекера как

$$A \times B = [a_{ij}B]$$

Каждый элемент a_{ij} в матрице A заменяется матрицей $a_{ij}B$.

Пример: Пусть $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, тогда

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Матрицы $H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$

Рассмотрим матрицы $H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$ для $i = 1,2,\dots,m$

Пусть $m = 2$, тогда

$$H_2^1 = I_{2^1} \times H \times I_{2^0} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} [1] = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H_2^2 = I_{2^0} \times H \times I_{2^1} = [1] \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Матрицы H_3^i

Для $m = 3$:

$$H_3^1 = I_{2^2} \times H \times I_{2^0} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} [1]$$

$$H_3^2 = I_{2^1} \times H \times I_{2^1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$H_3^3 = I_{2^0} \times H \times I_{2^2} = [1] \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Быстрый алгоритм декодирования для $RM(1, m)$

1. Сформировать $\overline{w}$ из w заменой всех 0 на -1.
2. Вычислить $w_1 = \overline{w} H_m^1$ и $w_i = w_{i-1} H_m^i$ для $i = 2, 3, \dots, m$.
3. Найти позицию j наибольшего по абсолютному значению компонента w_m.

Пусть $v(j) \in K^m$ – двоичное представление j (младшие биты в начале). Тогда если j-й компонент w_m положительный, исходное сообщение равно $\big(1, v(j)\big)$, а если j-й компонент w_m отрицательный, исходное сообщение равно $\big(0, v(j)\big)$.

Пример

Пусть $m = 3$ и $G(1,3)$ порождающая матрица $RM(1,3)$.

Пусть принято сообщение $w = 10101011$.

Преобразуем его в $\overline{w} = [1, -1, 1, -1, 1, -1, 1, 1]$.

Вычислим:

$$w_1 = \overline{w}H_3^1 = (0, 2, 0, 2, 0, 2, 2, 0)$$
$$w_2 = w_1 H_3^2 = (0, 4, 0, 0, 2, 2, -2, 2)$$
$$w_3 = w_2 H_3^3 = (2, 6, -2, 2, -2, 2, 2, -2)$$

Наибольший компонент (6) появляется на позиции 1. Поскольку $v(1) = 100$ и $6 > 0$, исходное сообщение равно (1100)