Теория кодирования

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

Код Рида-Маллера

Коды Рида-Маллера – это линейные коды (n, k, d), где

$$n = 2^m,$$

$$k = \sum_{i=0}^{r} C_n^i,$$

$$d = 2^{m-r}.$$

Рассмотрим альтернативный способ формирования этих кодов, более подходящий для декодирования.

Стандартный порядок

Обозначим позиции в слове длины $n = 2^m$ векторами из K^m.

Будем обозначать позицию i вектором $u_i \in K^m$, где u_i является двоичным представлением i с обратным порядком разрядов (младшие биты впереди).

Так стандартным порядком для $m = 2$ будет $(00, 10, 01, 11)$.

Для $m = 2 - (000, 100, 010, 110, 001, 101, 011, 111)$.

Векторная форма

Любая функция $f\colon K^m \to \{0,1\}$ может быть представлена в векторной форме

$$v = \left(f(u_0), f(u_1), \dots, f(u_{2^m-1})\right) \in K^n,$$

где $u_i \in K^m$, $n = 2^m$ и $u_0, u_1, \dots, u_{2^m-1}$ – стандартный порядок векторов.

Класс базисных функций

Пусть задано подмножество $I \subseteq \{0, 1, \dots, m-1\}$. Определим функцию

$$f_I(x_0, x_1, \dots, x_{m-1}) = \begin{cases} \prod_{i \in I} (x_i + 1), & \text{если } I \neq \emptyset, \\ 1, & \text{если } I = \emptyset. \end{cases}$$

Определим v_I как соответствующую векторную форму для f_I.

Пример

Пусть $m = 3$, тогда $n = 2^3$.

Если $I = \{1,2\}$, тогда $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$.

Векторная форма $f_{\{1,2\}}(x_0, x_1, x_2)$ получается подстановкой элементов $x_0x_1x_2 \in K^3$ в стандартном порядке и вычислением $f_{\{1,2\}}(x_0, x_1, x_2)$. Таким образом

$f_{\{1,2\}}(0,0,0) = 1$, $f_{\{1,2\}}(1,0,0) = 1$, $f_{\{1,2\}}(0,1,0) = 0$, $f_{\{1,2\}}(1,1,0) = 0$,

$f_{\{1,2\}}(0,0,0) = 0$, $f_{\{1,2\}}(1,0,0) = 0$, $f_{\{1,2\}}(0,1,0) = 0$, $f_{\{1,2\}}(1,1,1) = 0$.

$$v_I = \{11000000\}$$

Свойства функции f_I

Есть два важных свойства функции f_I, которые понадобятся в дальнейшем.

1. $f_I(x_0, x_1, \dots, x_{m-1}) = 1$ тогда и только тогда, когда $x_i = 0$ для всех $i \in I$.
2. Для каждого $u_i \in K^m$ $f_I(u_i) f_J(u_i) = f_{I \cup J}(u_i)$ и, следовательно:

$$v_I \cdot v_J = \sum_{i=0}^{2^m-1} f_I(u_i) f_J(u_i) = \sum_{i=0}^{2^m-1} f_{I \cup J}(u_i) = wt\left(v_{I \cup J}\right)(mod 2)$$

Далее для обозначения всего набора $\{0, 1, 2, \dots, m-1\}$ будет использоваться обозначение Z_m.

Код Рида-Маллера

Код Рида-Маллера $RM(r, m)$ можно определить как линейный код $(\{v_I \mid I \subseteq Z_m, |I| \leq r\})$. Можно показать, что

$$S = \{v_I \mid I \subseteq Z_m, |I| \leq r\}$$

линейно независимое множество, и поэтому может являться базисом линейного кода $RM(r, m)$.

Порождающая матрица кода Рида-Маллера

Слова v_I можно расположить в любом порядке для формирования порождающей матрицы $G_{r,m}$. Определим канонический вид матрицы $G_{r,m}$, в котором строки расположены так, что v_I встречается раньше (выше), чем v_J, если:

1. $|I| < |J|$

или

2. если $|I| = |J|$, $f_I(u_j) < f_J(u_j)$ и $f_I(u_i) = f_J(u_i)$ для $i > j$.

Порождающая матрица для $RM(3,4)$

$$G_{4,4} = \begin{matrix}
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\begin{matrix}
v_{\emptyset} \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_{2,3} \\ v_{1,3} \\ v_{0,3} \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \\ v_{1,2,3} \\ v_{0,2,3} \\ v_{0,1,3} \\ v_{0,1,2}
\end{matrix} \\
\begin{matrix}
0000 & 1000 & 0100 & 1100 & 0010 & 1010 & 0110 & 1110 & 0001 & 1001 & 0101 & 1101 & 0011 & 1011 & 0111 & 1111
\end{matrix}
\end{matrix}$$

Порождающая матрица для $RM(3,4)$

$$G_{4,4} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & v_{\emptyset} \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_3 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & v_2 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & v_1 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & v_0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{2,3} \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,3} \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,3} \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,2} \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & v_{0,2} \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & v_{0,1} \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{1,2,3} \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,2,3} \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,1,3} \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & v_{0,1,2} \\
0000 & 1000 & 0100 & 1100 & 0010 & 1010 & 0110 & 1110 & 0001 & 1001 & 0101 & 1101 & 0011 & 1011 & 0111 & 1111 &
\end{bmatrix}$$

Порождающая матрица для $RM(3,4)$

$$G_{4,4} = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\begin{matrix}
v_{\emptyset} \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_{2,3} \\ v_{1,3} \\ v_{0,3} \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \\ v_{1,2,3} \\ v_{0,2,3} \\ v_{0,1,3} \\ v_{0,1,2}
\end{matrix}$$

0000 1000 0100 1100 0010 1010 0110 1110 0001 1001 0101 1101 0011 1011 0111 1111

Мажоритарное декодирование

Будем называть $I^c \subseteq Z_m$ комплементарным множеством к множеству $I \subseteq Z_m$, если $I^c = Z_m \backslash I$.

Пусть $H_I = \{u \in K^m \mid f_I(u) = 1\}$. Напомним, что $f_I(x_0, \dots, x_{m-1}) = 1$ тогда и только тогда, когда $x_i = 0$ для всех $i \in I$. H_I – подпространство K^m.

Для любого $u = (x_0, x_1, \dots, x_{m-1}) \in K^m$ и для любого $t = (t_0, \dots, t_{m-1}) \in K^m$ определим функцию $f_{I,t} = f_I(x_0 + t_0, \dots, x_{m-1} + t_{m-1}) = f_I(x + t)$. Соответственно, $v_{I,t}$ векторная форма это функции.

Алгоритм мажоритарного декодирования

Пусть w – принятое слово.

1. Пусть $i = r$ и пусть $w(r) = w$.
2. Для каждого $J \subseteq Z_m$, удовлетворяющего условию $|J| = i$, вычисляем $w(i) \cdot v_{J^c,t}$ для каждого $t \in H_J$ до тех пор, пока 0 или 1 не встретятся более чем 2^{m-i-1} раз, в этом случае m_j принимаем равным 0 или 1, соответственно. Если и 0, и 1 встретились более, чем $2^{m-r-1} - 1$ раз, запрашиваем повторную отправку сообщения.
3. Если $i > 0$, $w(i-1) = w(i) + \sum_{J \subseteq Z_m} m_J v_J$, где $|J| = i$. Если $w(i-1)$ имеет вес не более $2^{m-r-1} - 1$, принимаем $m_J = 0$ и для всех $J \subseteq Z_m$, где $|J| \leq r$ и останавливаем выполнение алгоритма. Иначе, заменяем i на $i - 1$ и возвращаемся к шагу 2. (Если $i = 0$, тогда m_J было вычислено для всех $J \subseteq Z_m$, где $|J| \leq r$ и наиболее вероятное отправленное сообщение было вычислено)

Пример

Используем рассмотренный ранее алгоритм для декодирования слова $w = 0101011110100000$, закодированного с использованием $G_{2,4}$.

Начинаем с $i = r = 2$ и $w(2) = w$.

Пусть $J = \{0,1\}$. Тогда $J^c = \{2,3\}$ и $H_J = \{0000, 0010, 0001, 0011\}$.

$v_{J^c,t}$:

$$v_{\{2,3\},\{0000\}} = \{1111\ 0000\ 0000\ 0000\}$$
$$v_{\{2,3\},\{0010\}} = \{0000\ 1111\ 0000\ 0000\}$$
$$v_{\{2,3\},\{0001\}} = \{0000\ 0000\ 1111\ 0000\}$$
$$v_{\{2,3\},\{0011\}} = \{0000\ 0000\ 0000\ 1111\}$$

$v_{\{2,3\},\{0000\}}$ и $v_{\{2,3\},\{0010\}}$

$v_{\{2,3\},\{0000\}} = \{1111\ 0000\ 0000\ 0000\}$

единицы только в тех строках, в номерах которых в позициях 2 и 3 нули, то есть вида $(** 00)$*!*

$f_{\{2,3\},\{0000\}}(0000) = 1,$
$f_{\{2,3\},\{0000\}}(0100) = 1,$
$f_{\{2,3\},\{0000\}}(0010) = 0,$
$f_{\{2,3\},\{0000\}}(0110) = 0,$
$f_{\{2,3\},\{0000\}}(0001) = 0,$
$f_{\{2,3\},\{0000\}}(0101) = 0,$
$f_{\{2,3\},\{0000\}}(0011) = 0,$
$f_{\{2,3\},\{0000\}}(0111) = 0,$

$f_{\{2,3\},\{0000\}}(1000) = 1,$
$f_{\{2,3\},\{0000\}}(1100) = 1,$
$f_{\{2,3\},\{0000\}}(1010) = 0,$
$f_{\{2,3\},\{0000\}}(1110) = 0,$
$f_{\{2,3\},\{0000\}}(1001) = 0,$
$f_{\{2,3\},\{0000\}}(1101) = 0,$
$f_{\{2,3\},\{0000\}}(1011) = 0,$
$f_{\{2,3\},\{0000\}}(1111) = 0,$

$v_{\{2,3\},\{0010\}} = \{0000\ 1111\ 0000\ 0000\}$

$t = 0010$

это означает, что бит на 2 позиции инвертируется, поэтому единицы только в тех строках, в номерах которых в позиции 2 – единица, а в позиции 3 – ноль, то есть вида $(** 10)$

$f_{\{2,3\},\{0010\}}(0000) = 0,$
$f_{\{2,3\},\{0010\}}(0100) = 0,$
$f_{\{2,3\},\{0010\}}(0010) = 1,$
$f_{\{2,3\},\{0010\}}(0110) = 1,$
$f_{\{2,3\},\{0010\}}(0001) = 0,$
$f_{\{2,3\},\{0010\}}(0101) = 0,$
$f_{\{2,3\},\{0010\}}(0011) = 0,$
$f_{\{2,3\},\{0010\}}(0111) = 0,$

$f_{\{2,3\},\{0010\}}(1000) = 0,$
$f_{\{2,3\},\{0010\}}(1100) = 0,$
$f_{\{2,3\},\{0010\}}(1010) = 1,$
$f_{\{2,3\},\{0010\}}(1110) = 1,$
$f_{\{2,3\},\{0010\}}(1001) = 0,$
$f_{\{2,3\},\{0010\}}(1101) = 0,$
$f_{\{2,3\},\{0010\}}(1011) = 0,$
$f_{\{2,3\},\{0010\}}(1111) = 0,$

Пример

$$w(2) = (0101\ 0111\ 1010\ 0000)$$

$$J = \{0,1\}, \qquad v_{\{2,3\},t}:$$

$$v_{\{2,3\},\{0000\}} = \{1111\ 0000\ 0000\ 0000\}$$

$$v_{\{2,3\},\{0010\}} = \{0000\ 1111\ 0000\ 0000\}$$

$$v_{\{2,3\},\{0001\}} = \{0000\ 0000\ 1111\ 0000\}$$

$$v_{\{2,3\},\{0011\}} = \{0000\ 0000\ 0000\ 1111\}$$

$$w \cdot v_{\{2,3\},\{0000\}} = 0$$

$$w \cdot v_{\{2,3\},\{0010\}} = 1$$

$$w \cdot v_{\{2,3\},\{0001\}} = 0$$

$$w \cdot v_{\{2,3\},\{0011\}} = 0$$

$$m_{\{0,1\}} = 0$$

Пример

$$w(2) = (0101\ 0111\ 1010\ 0000)$$

$$J = \{0,2\}, \qquad v_{\{1,3\},t}:$$

$$v_{\{1,3\},\{0000\}} = \{1100\ 1100\ 0000\ 0000\}$$

$$v_{\{1,3\},\{0100\}} = \{0011\ 0011\ 0000\ 0000\}$$

$$v_{\{1,3\},\{0001\}} = \{0000\ 0000\ 1100\ 1100\}$$

$$v_{\{1,3\},\{0101\}} = \{0000\ 0000\ 0011\ 0011\}$$

$$w \cdot v_{\{1,3\},\{0000\}} = 0$$

$$w \cdot v_{\{1,3\},\{0100\}} = 1$$

$$w \cdot v_{\{1,3\},\{0001\}} = 1$$

$$w \cdot v_{\{1,3\},\{0101\}} = 1$$

$$m_{\{0,2\}} = 1$$

Пример

$w = 0101011110100000.$

$w(2) = (0101\ 0111\ 1010\ 0000).$

Таким образом, для $i = 2$ и $w(2)$.

$m_{0,1} = 0,\ m_{0,2} = 1,\ m_{0,3} = 0,\ m_{1,2} = 0,\ m_{1,3} = 0,\ m_{2,3} = 0.$

Тогда

$$w(1) = w(2) + v_{0,2} = 1111\ 0111\ 0000\ 0000$$
$$i = 1$$

Пример

$$w(1) = (1111\ 0111\ 0000\ 0000)$$

$$J = \{0\}, \qquad v_{\{1,2,3\},t}:$$

$$v_{\{1,2,3\},\{0000\}} = \{1100\ 0000\ 0000\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0000\}} = 0$$
$$v_{\{1,2,3\},\{0100\}} = \{0011\ 0000\ 0000\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0100\}} = 0$$
$$v_{\{1,2,3\},\{0010\}} = \{0000\ 1100\ 0000\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0010\}} = 1$$
$$v_{\{1,2,3\},\{0110\}} = \{0000\ 0011\ 0000\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0110\}} = 0$$
$$v_{\{1,2,3\},\{0001\}} = \{0000\ 0000\ 1100\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0001\}} = 0$$
$$v_{\{1,2,3\},\{0101\}} = \{0000\ 0000\ 0011\ 0000\} \qquad w \cdot v_{\{1,2,3\},\{0101\}} = 0$$
$$v_{\{1,2,3\},\{0011\}} = \{0000\ 0000\ 0000\ 1100\} \qquad w \cdot v_{\{1,2,3\},\{0011\}} = -$$
$$v_{\{1,2,3\},\{0111\}} = \{0000\ 0000\ 0000\ 0011\} \qquad w \cdot v_{\{1,2,3\},\{0111\}} = -$$

$$m_{\{0\}} = 0$$

Пример

$w = 0101\ 0111\ 1010\ 0000.$

$m_{0,1} = 0,\ m_{0,2} = 1,\ m_{0,3} = 0,\ m_{1,2} = 0,\ m_{1,3} = 0,\ m_{2,3} = 0.$

$m_0 = 0,\ m_1 = 0,\ m_2 = 0,\ m_3 = 1.$

$m_\emptyset = 0.$

Отправленное сообщение равно:

$$u = 0\ 1000\ 000010$$

При умножении на порождающую матрицу $G_{2,4}$ даёт:

$$v = (0101\ 1111\ 1010\ 0000)$$