Помехоустойчивое кодирование

Коды Рида-Маллера

Отождествление булевых функций с их таблицами (столбцами)

x_1	x_2	$f(x_1, x_2)$
0	0	0
0	1	1
1	0	0
1	1	1

$$f(x_1, x_2) \quad \Rightarrow \quad \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Покомпонентное произведение кодовых слов

$$\alpha = (a_0, a_1, \ldots, a_{n-1})^T \quad u \quad \beta = (b_0, b_1, \ldots, b_{n-1})^T$$

$$\alpha * \beta = (a_0 b_0, a_1 b_1, \ldots, a_{n-1} b_{n-1})^T$$

Степень булевой функции

$$\textit{степень} \quad \textit{коньюнкции}$$

$$\deg x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_k} = k$$

$$\textit{степень} \quad \textit{функции}$$

$$\deg f(x_1, x_2, \ldots \cdot x_n) \quad \Rightarrow$$

$$\textit{наибольшая из степеней конъюнкций,}$$

$$\textit{входящих в полином Жегалкина}$$

$$(\textit{полином Рида} - \textit{Маллера})$$

Пример

степень коньюнкции

$$\deg x_1 \cdot x_3 \cdot x_4 = 3$$

степень функции

$$f(x_1, x_2, \ldots \cdot x_n) = x_1 \oplus x_1 x_2 \oplus x_2 x_3$$

равна 2

Определение

- *Код Рида-Маллера порядка r (РМ-r – код)* – это множество булевых функций степени не выше *r*.

Порождающая матрица РМ-1 - кода

Пример.

$$G = \begin{array}{c} \begin{array}{cccc} \mathbf{1} & \mathbf{x_1} & \mathbf{x_2} & \mathbf{x_3} \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix} \end{array} = \begin{pmatrix} G_0 & G_1 \end{pmatrix}$$

Порождающая матрица РМ-2 - кода

Пример.

$$
\begin{array}{c}
\begin{array}{ccccccc} \mathbf{1} & \mathbf{x}_1 & \mathbf{x}_2 & \mathbf{x}_3 & \mathbf{x}_1\mathbf{x}_2 & \mathbf{x}_1\mathbf{x}_3 & \mathbf{x}_2\mathbf{x}_3 \end{array} \\
G = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix} = \begin{pmatrix} G_0 & G_1 & G_2 \end{pmatrix}
\end{array}
$$

Параметры РМ-r - кода

Длина кода $n = 2^m$

Число информационных разрядов

$$k = 1 + m + C_m^2 + ... + C_m^r$$

Минимальное расстояние $d_{\min} = 2^{m-r}$

Пример параметров РМ-2 - кода

Длина кода $n = 2^4 = 16,$ $m = 4$

Число информационных разрядов

$$k = 1 + 4 + C_4^2 = 1 + 4 + 6 = 11$$

Минимальное расстояние $d_{\min} = 2^{m-r} = 4$

Пример параметров РМ-3 - кода

Длина кода $n = 2^4 = 16, \qquad m = 4$

Число информационных разрядов

$$k = 1 + 4 + C_4^2 + C_4^3 = 1 + 4 + 6 + 4 = 15$$

Минимальное расстояние $d_{\min} = 2^{4-3} = 2$

Кодирование – блоки информационного и кодового слова

$$G \cdot \alpha = \begin{pmatrix} G_0 & G_1 & \dots & G_r \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \dots \\ \alpha_r \end{pmatrix} =$$

$$G_0 \alpha_0 \oplus G_1 \alpha_1 \oplus \dots \oplus G_r \alpha_r$$

Пример

.G_0 G_1 G_2

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

Построение проверок - на примере РМ-1 кода длины 16

$$\gamma = \begin{bmatrix} 1&0&0&0&0\\ 1&0&0&0&1\\ 1&0&0&1&0\\ 1&0&0&1&1\\ 1&0&1&0&0\\ 1&0&1&0&1\\ 1&0&1&1&0\\ 1&0&1&1&1\\ 1&1&0&0&0\\ 1&1&0&0&1\\ 1&1&0&1&0\\ 1&1&0&1&1\\ 1&1&1&0&0\\ 1&1&1&0&1\\ 1&1&1&1&0\\ 1&1&1&1&1 \end{bmatrix} \cdot \begin{bmatrix} a_0\\ a_1\\ a_2\\ a_3\\ a_4 \end{bmatrix} \Rightarrow$$

$$\left.\begin{aligned} c_0 &= a_0\\ c_1 &= a_0 \oplus a_4\\ c_2 &= a_0 \oplus a_3\\ c_3 &= a_0 \oplus a_3 \oplus a_4 \end{aligned}\right\} \Rightarrow c_0 \oplus c_1 \oplus c_2 \oplus c_3 = 0$$

$$\left.\begin{aligned} c_4 &= a_0 \oplus a_2\\ c_5 &= a_0 \oplus a_2 \oplus a_4\\ c_6 &= a_0 \oplus a_2 \oplus a_3\\ c_7 &= a_0 \oplus a_2 \oplus a_3 \oplus a_4 \end{aligned}\right\} \Rightarrow \begin{aligned} c_4 \oplus c_5 \oplus c_6 \oplus c_7 &= 0\\ c_0 \oplus c_1 \oplus c_4 \oplus c_5 &= 0\\ c_0 \oplus c_2 \oplus c_4 \oplus c_6 &= 0 \end{aligned}$$

$$\left.\begin{aligned} c_8 &= a_0 \oplus a_1\\ c_9 &= a_0 \oplus a_1 \oplus a_4\\ c_{10} &= a_0 \oplus a_1 \oplus a_3\\ c_{11} &= a_0 \oplus a_1 \oplus a_3 \oplus a_4 \end{aligned}\right\} \Rightarrow c_8 \oplus c_9 \oplus c_{10} \oplus c_{11} = 0$$

$$\left.\begin{aligned} c_{12} &= a_0 \oplus a_2\\ c_{13} &= a_0 \oplus a_2 \oplus a_4\\ c_{14} &= a_0 \oplus a_2 \oplus a_3\\ c_{15} &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \end{aligned}\right\} \Rightarrow \begin{aligned} c_{12} \oplus c_{13} \oplus c_{14} \oplus c_{15} &= 0\\ c_8 \oplus c_9 \oplus c_{12} \oplus c_{13} &= 0\\ c_8 \oplus c_{10} \oplus c_{12} \oplus c_{14} &= 0 \end{aligned}$$

Построение проверок - на примере РМ-1 кода длины 16 – шаг 1

$$a_4 = c_0 \oplus c_1 = c_2 \oplus c_3 = c_4 \oplus c_5 = c_6 \oplus c_7 =$$

$$c_8 \oplus c_9 = c_{10} \oplus c_{11} = c_{12} \oplus c_{13} = c_{14} \oplus c_{15}$$

$$a_3 = c_0 \oplus c_2 = c_1 \oplus c_3 = c_4 \oplus c_6 = c_5 \oplus c_7 =$$

$$c_8 \oplus c_{10} = c_9 \oplus c_{11} = c_{12} \oplus c_{14} = c_{13} \oplus c_{15}$$

$$a_2 = c_0 \oplus c_4 = c_1 \oplus c_5 = c_2 \oplus c_6 = c_3 \oplus c_7 =$$

$$c_8 \oplus c_{12} = c_9 \oplus c_{13} = c_{10} \oplus c_{14} = c_{11} \oplus c_{15}$$

$$a_1 = c_0 \oplus c_8 = c_1 \oplus c_9 = c_2 \oplus c_{10} = c_3 \oplus c_{11} =$$

$$c_4 \oplus c_{12} = c_5 \oplus c_{13} = c_6 \oplus c_{14} = c_7 \oplus c_{15}$$

Построение проверок - на примере РМ-1 кода длины 16 – шаг 2

$$a_0 = c_0 = c_1 = c_2 = c_3 = c_4 = c_5 = c_6 = c_7 =$$

$$c_8 = c_9 = c_{10} = c_{11} = c_{12} = c_{13} = c_{14} = c_{15}$$

Мажоритарное декодирование РМ - кодов

- *Строятся проверки для*
  $\alpha_r \quad - \quad \text{всего } 2^{m-r} \text{ проверок}$
- *Затем – для* $\alpha_{r-1} \quad - \quad \text{всего } 2^{m-r+1} \text{ проверок}$ *и т.д.*

- *На последнем шаге исправляется*

$$\alpha_0 = a_0 \quad - \quad \text{всего } 2^m \text{ проверок}$$

Циклический код Рида-Маллера

- Рассмотрим разложение числа *j* по степеням двойки:

$$j = j_0 + j_1 \cdot 2 + j_2 \cdot 4 + \ldots + j_{m-1} 2^{m-1}$$

- ***Весом целого числа j в двоичном разложении*** назовем сумму

$$w_2(j) = j_0 + j_1 + \ldots + j_{m-1}$$

- *Пример. 7=1+2+4, m=3, (111),* $w_2(7) = 3$
- *12=4+8, m=4 (0011),* $w_2(12) = 2$

Циклический код Рида-Маллера

- Циклическим кодом Рида Маллера порядка *r* и длины $n = 2^m - 1$ над полем *GF(2)* называется циклический код, порождающий многочлен *g(x)* которого имеет корни α^j такие, что

$$0 < w_2(j) \le m - r - 1, \quad j = 1,\ldots,n$$

Циклический код Рида-Маллера

- Заметим, что если α^{j} является корнем *g(x),* то и α^{2j} является корнем.

Параметры циклического РМ-кода

- Длина: $$n = 2^m - 1$$

- Число информационных разрядов:

$$k = \sum_{i=0}^{r} C_m^i$$

- Минимальное расстояние:

$$d_{\min} = 2^{m-r} - 1$$

Циклический РМ – код порядка *m*-2

$$0 < w_2(j) \le m - (m-2) - 1,$$

$$j = 1, \ldots, n \quad \Rightarrow \quad w_2(j) = 1 \quad \Rightarrow$$

$$\textit{корнями} \quad \textit{являются}$$

$$\alpha, \alpha^2, \alpha^4, \ldots$$

- Это циклический код Хэмминга

m=5, циклический РМ – код порядка *r*=2

$$0 < w_2(j) \le 5 - 2 - 1 = 2,$$

$$j = 1, \ldots, n \quad \Rightarrow \quad w_2(j) = 1,2 \quad \Rightarrow$$

$$\textit{корнями} \quad \textit{являются} \quad \alpha, \alpha^3, \alpha^5:$$

$$00001, \quad 00011, \quad 00101$$

$$\textit{и} \quad \textit{их} \quad \textit{циклические} \quad \textit{сдвига}$$

- Это (31,16) – код БЧХ, исправляющий 3 ошибки

Связь между обычными и циклическими РМ - кодами

- *Обычный РМ код получается из циклического добавлением одного проверочного разряда – разряда проверки на четность.*

Преимущества циклического РМ кода

- Декодирование – мажоритарное, циклический сдвиг кодового слова соответствует циклическому сдвигу проверок.

Код, дуальный к циклическому РМ- коду порядка *r=m-2*

- Длина: $n = 2^m - 1$
- Число информационных разрядов:

$$k = 2^m - 1 - (1 + m + \ldots C_m^{m-2}) =$$

$$2^m - 1 - (2^m - C_m^{m-1} + C_m^m) = m$$

- Минимальное расстояние:

$$d_{\min} = 2^{m-1}$$

Код, дуальный к циклическому РМ- коду порядка *r*=*m*-2

- Пример. $m=4$, $n=15$.
- Порождающий многочлен $g(x)=\dfrac{1\oplus x^{15}}{1\oplus x\oplus x^{4}}=$

$$1\oplus x\oplus x^{2}\oplus x^{3}\oplus x^{5}\oplus x^{7}\oplus x^{8}\oplus x^{11}$$

- Некоторые кодовые слова:
  111101011001000
  011110101100100
  100011110101100
  101100100011110

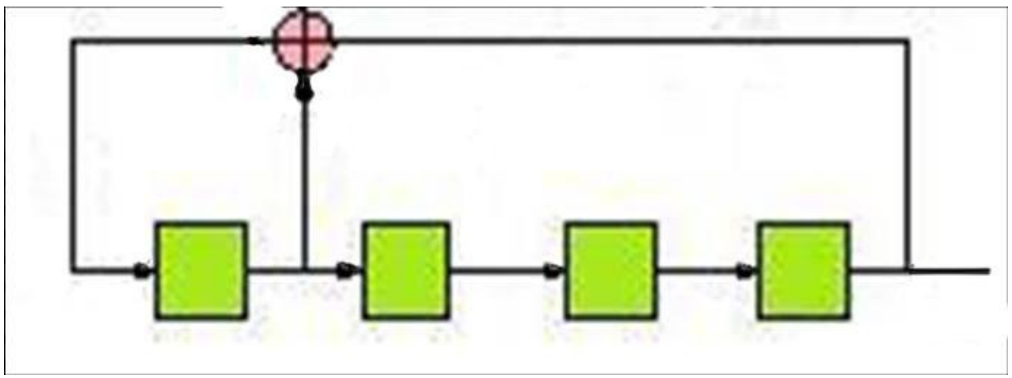
Код, дуальный к циклическому РМ- коду порядка $r=m-2$

- Рассмотрим подробнее слово: 111101011001000 | 11…

- Число нулей и единиц – ½ длины слова
- Число биграмм 00,01,10,11 – ¼ длины слова
- Число триграмм – 1/8 длины слова
- Автокорреляция
  111101011001000
  011110101100100

Генератор кода - генератор псевдослучайных чисел

- LFSR, начальное состояние – любое ненулевое



- g(x) – многочлен обратных связей – примитивный многочлен

состояние	выход
1111	1
0111	1
1011	1
0101	1
1010	0
1101	1
0110	0
0011	1
1001	1
0100	0
0010	0
0001	1
1000	0
1100	0
1110	0

Периодические последовательности на LFSR

- Примитивный многочлен степени *m* – *последовательности максимальной длины* (период равен $2^m - 1$ - порядок многочлена)
- В других случаях период последовательности – порядок многочлена ОС
- Примеры.

многочлен	период
$1 \oplus x^4$	4
$1 \oplus x \oplus x^4$	15
$1 \oplus x^2 \oplus x^4$	6
$1 \oplus x^3 \oplus x^4$	15
$1 \oplus x \oplus + x^2 + x^4$	7
$1 \oplus x \oplus + x^3 + x^4$	6
$1 \oplus x^2 \oplus x^3 \oplus x^4$	7
$1 \oplus \oplus x \oplus x^2 \oplus x^3 \oplus x^4$	5

Некоторые часто используемые примитивные трехчлены

$$x^3 \oplus x \oplus 1, \quad x^4 \oplus x \oplus 1, \quad x^5 \oplus x^2 \oplus 1,$$

$$x^{31} \oplus x^3 \oplus 1, \quad x^{31} \oplus x^6 \oplus 1, \quad x^{31} \oplus x^7 \oplus 1,$$

$$x^{39} \oplus x^4 \oplus 1, \quad x^{60} \oplus x \oplus 1, \quad x^{63} \oplus x \oplus 1,$$

$$x^{71} \oplus x^6 \oplus 1, \quad x^{93} \oplus x^2 \oplus 1, \quad x^{137} \oplus x^{21} \oplus 1,$$

$$x^{145} \oplus x^{52} \oplus 1, \quad x^{161} \oplus x^{18} \oplus 1, \quad x^{521} \oplus x^{32} \oplus 1$$