Коды Рида - Маллера

Коды Рида - Маллера над GF(2)

- Коды Рида – Маллера (РМ) представляют собой класс линейных кодов над $GF(2)$ с простым описанием и декодированием.
- Для любых целых m и l, $l < m$ существует код РМ длиной 2^m, который называется кодом РМ l–го порядка.

Порождающая матрица

- **Порождающая матрица** кода РМ l-го порядка длиной 2^m определяется как совокупность блоков

$$\mathbf{G} = \begin{bmatrix} G_0 & G_1 & \cdots & G_l \end{bmatrix}^T$$

Порождающая матрица (Булевы функции)

- где $\mathbf{G}_0$ – вектор размерностью $n = 2^m$, состоящий из одних единиц;
- $\mathbf{G}_1$- матрица размером ($m \times 2^m$), содержащая в качестве столбцов все двоичные коды из m бит;
- строки матрицы $\mathbf{G}_l$ получаются как все возможные произведения l строк матрицы $\mathbf{G}_1$

Порождающая матрица

- Для определенности будем считать, что первый столбец в $\mathbf{G}_1$ состоит из одних нулей, последний из одних единиц, а остальные – коды чисел 1,2,…, упорядоченных по возрастанию, считая, что младший бит расположен в нижней строке.

Порождающая матрица

- Поскольку существует всего

$$\binom{m}{j}$$

- способов выбора j строк, входящих в произведение, то матрица $\mathbf{G}_j$ имеет размер

$$\binom{m}{j} \times 2^m$$

Параметры кода РМ- *l*

$$k = 1 + \binom{m}{1} + \ldots + \binom{m}{l},$$

$$n - k = 1 + \binom{m}{1} + \ldots + \binom{m}{m-l-1},$$

Это обеспечивает линейную независимость строк в матрице **G**

Параметры кода РМ- *l*

- Код Рида – Маллера *l*-го порядка длиной $n = 2^m$ представляет собой бинарный код с параметрами

$$(n,k) = (2^m, \sum_{i=0}^{l} C_m^i)$$

Кодовые расстояния

- Код РМ-1 является двойственным расширенному коду Хемминга, для него

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

- Код РМ-2 имеет

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

$$1 \le h \le [m/2]$$

$$\mathbf{RM}(3,1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} 1 \\ x_3 \\ x_2 \\ x_1. \end{matrix}$$

$$\mathbf{RM}(3,2) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} 1 \\ x_3 \\ x_2 \\ x_1 \\ x_2x_3 \\ x_1x_3 \\ x_1x_2 \end{matrix}$$

РМ

- РМ – линейный код
- (n, k)-код содержит $2^{\sum_{i=0}^{k}\binom{n}{i}}$
- имеет $d_{min} = 2^{n-k}$

Формирование через булевы переменные

1

$$\mathbf{X} = \bigotimes_{n} \mathbf{X}_i(1), \quad \mathbf{X}_i(1) = \begin{bmatrix} 1 & x_i \end{bmatrix}, \quad x_i \in \{0, 1\}.$$

$$\mathbf{R}(n) = \bigotimes_{i=0}^{n} \mathbf{R}(1), \quad \mathbf{R}(1) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$$

2 $f : Z_2^n \to Z_q \quad q = 2^h$

$$2^{h\sum_{i=0}^{k}\binom{n}{i}}$$

Кодовых слов

$$\mathbf{RM}_{2^h}(4,1) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{matrix}$$

Обобщенный GRM (n,k)

- Кодовых слов $2^{h\sum_{i=0}^{k}\binom{n}{i}} \cdot 2^{(h-1)\binom{n}{r}}$

h=2

$$\mathbf{RM}_{2^h}(4,2) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 \end{bmatrix} \begin{matrix} 1 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ 2x_1x_2 \\ 2x_1x_3 \\ 2x_1x_4 \\ 2x_2x_3 \\ 2x_2x_4 \\ 2x_3x_4 \end{matrix}$$

Не-бинарный код

- На основе системе счисления по смешанному основанию

$$\mathbf{RM}_4(2,1) = \begin{bmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 3 & 3 & 3 & 3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Система счисления по смешанному основанию

- Пусть рассматривается множество целых чисел
  - $\{0,1,\ldots,N-1\}$.
- Если $N = N_1 N_2 \ldots N_m$
- то любое число **a**
- из этого множества можно представить в виде

$$a = a_m + a_{m-1}N_m + a_{m-2}N_m N_{m-1} + \ldots + a_1 N_m N_{m-1} \ldots N_2$$

$$a_1 \in \{0,1,\ldots,N_1 - 1\} \qquad a_2 \in \{0,1,\ldots,N_2 - 1\} \qquad a_m \in \{0,1,\ldots,N_m - 1\}$$

- Числу a можно поставить в соответствие код («m – ка»

$$a \rightarrow (a_1, a_2, \ldots, a_m)$$

Матрица Паскаля

- РМ – линейный код
- (n, k)-код содержит $2^{\sum_{i=0}^{k}\binom{n}{i}}$
- имеет d_1

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & 0 & \cdots & 0 \\ 1 & 2 & 1 & 0 & \cdots & 0 \\ 1 & 3 & 3 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ C_{p-1}^{0} & C_{p-1}^{1} & C_{p-1}^{2} & C_{p-1}^{3} & \cdots & C_{p-1}^{p-1} \end{bmatrix}$$

На основе матрицы Паскаля

$$\mathbf{L}_{(9\times 9)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 4 & 6 & 4 & 1 & 0 & 0 & 0 \\ 1 & 5 & 10 & 10 & 5 & 1 & 0 & 0 \\ 1 & 6 & 15 & 20 & 15 & 6 & 1 & 0 \\ 1 & 7 & 21 & 35 & 35 & 21 & 7 & 1 \end{bmatrix}$$

Алгоритм мажоритарного декодирование кода РМ

- Рассмотрим метод мажоритарного декодирования кода РМ по большинству голосов на конкретном примере.

$$l = 1$$

$$k = 4$$

$$n = 2^3 = 8$$

$$m = 3$$

Кодирование

- Информационная вектор-строка

$$\mathbf{a} = [a_0, a_1, \ldots, a_{k-1}]$$

- код

$$C = \mathbf{a} \cdot \mathbf{G}_{PM} = a_0 \mathbf{v}_0 + a_1 \mathbf{v}_1 + \ldots + a_{k-1} \mathbf{v}_m$$

Матричная запись

$$\mathbf{G} = \begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \end{bmatrix} \Rightarrow$$

$$C = [a_0 \quad a_1 \quad a_2 \quad a_3] \begin{bmatrix} 11111111 \\ 01010101 \\ 00110011 \\ 00001111 \end{bmatrix} = [c_0, c_1, c_2, \ldots, c_7]$$

Кодер РМ

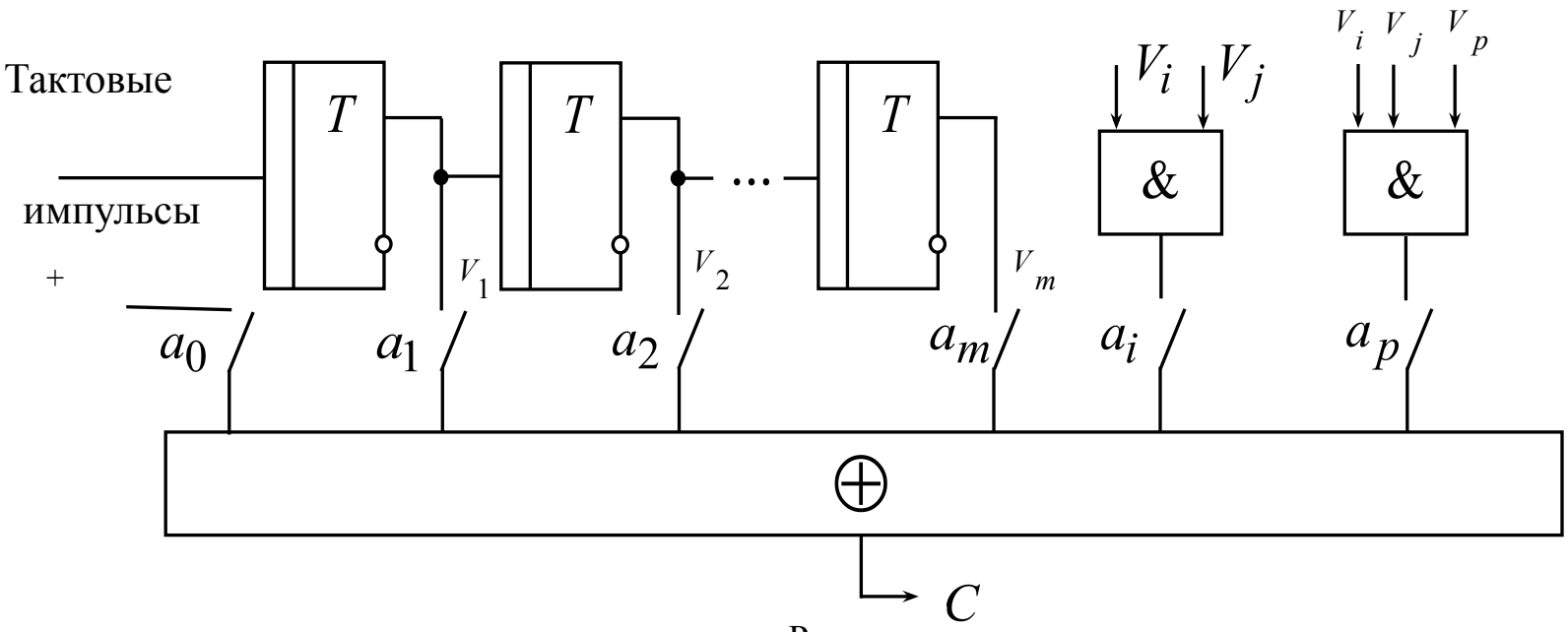

Рис.

Проверочные соотношения

- Можно построить проверочные соотношения, связывающие информационный символ с символами кодового слова.
- Эти соотношения имеют вид:

Проверочные соотношения
Ортогональная система проверок

$$c_0 = a_0$$
$$c_1 = a_0 + a_1$$
$$c_2 = a_0 + a_2$$
$$c_3 = a_0 + a_1 + a_2$$
$$c_4 = a_0 + a_3$$
$$c_5 = a_0 + a_1 + a_3$$
$$c_6 = a_0 + a_2 + a_3$$
$$c_7 = a_0 + a_1 + a_2 + a_3$$

$$a_1 = c_0 + c_1 = l_{11}$$
$$a_1 = c_2 + c_3 = l_{12}$$
$$a_1 = c_4 + c_5 = l_{13}$$
$$a_1 = c_6 + c_7 = l_{14}$$
$$a_2 = c_0 + c_2 = l_{21}$$
$$a_2 = c_1 + c_3 = l_{22}$$
$$a_2 = c_4 + c_6 = l_{23}$$
$$a_2 = c_5 + c_7 = l_{34}$$

$$a_3 = c_0 + c_4 = l_{31}$$
$$a_3 = c_1 + c_5 = l_{32}$$
$$a_3 = c_2 + c_6 = l_{33}$$
$$a_3 = c_3 + c_7 = l_{34}$$

Правило принятия решений

Если $\longrightarrow$ $0 < \sum_{j=1}^{n/2} l_{ij} \le \frac{d_{\min}}{2}$ $\longrightarrow$ $a_i = 0$

Если $\longrightarrow$ $\frac{d_{\min}}{2} < \sum_{j=1}^{n/2} l_{ij} \le d_{\min}$ $\longrightarrow$ $a_i = 1$

Декодер

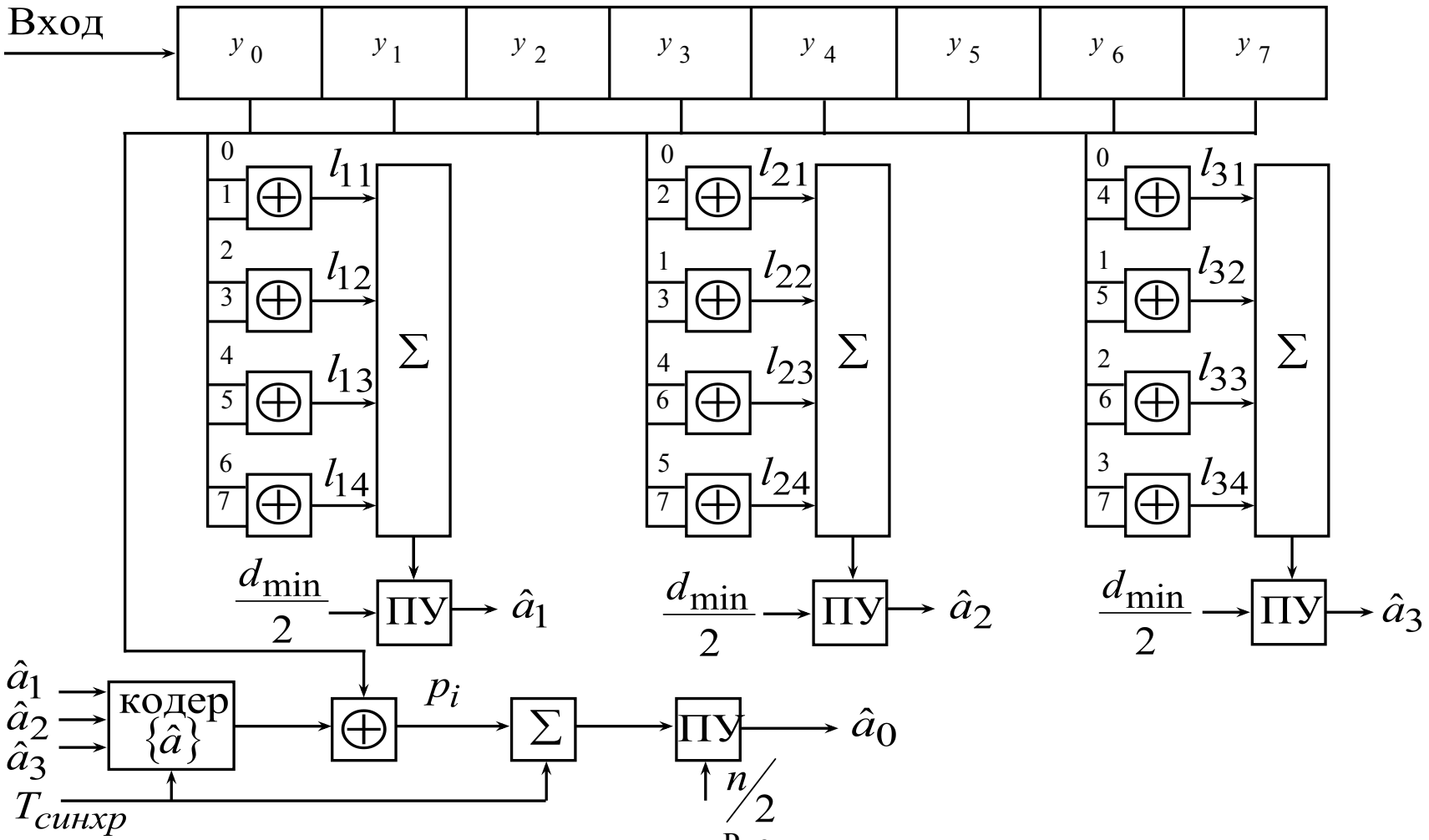
Вход
y 0
y 1
y 2
y 3
y 4
y 5
y 6
y 7
l11
l12
l13
l14
l21
l22
l23
l24
l31
l32
l33
l34
Σ
ПУ
d min / 2
â1
â2
â3
кодер {â}
pi
â0
n/2
Tсинхр

Рис.

Вероятность ошибки на бит

$$P_c(j) = \begin{cases} \sum_{i=(d+1)/2}^{d} C_d^i p^i (1-p)^{d-i} - \text{для ДСК при нечетном } d \\ \frac{1}{2} C_d^{d/2} p^{d/2} (1-p)^{d/2} + \sum_{i=(d/2)+1}^{d} C_d^i p^i (1-p)^{d-i} - \text{для ДСК при четном } d \\ Q\left(\sqrt{2dE_s / N_0}\right) - \text{для канала с АБГШ} \end{cases}$$

Здесь

- d – кодовое расстояние, p – вероятность ошибки на входе декодера, E_s/N_0 – отношение сигнал-шум в канале, $Q(x)$ – функция Маркума.

Вопросы

- ?