ТЕОРИЯ КОДИРОВАНИЯ

http://sites.google.com/site/musinbsuirby/

Мусин Сергей Борисович,
магистр техн. наук,
ассистент кафедры ПОИТ БГУИР

ДУАЛЬНЫЕ КОДЫ

Тема

Мусин С. Б.,
БГУИР

Дуальные коды

- Векторы u, v являются ортогональными, если скалярное произведение

$$u \cdot v = 0$$

- Код C_1 дуален коду C_2, если все слова C_1 ортогональны каждому слову C_2.

- Дуальный код обозначается как $C^{\perp}$

Мусин С. Б.,
БГУИР

Дуальные коды

- Из определения следует, что скалярное произведение каждой строки матрицы **G** на каждую строку матрицы **H** равно 0, т.е.

$$H \cdot G^T = 0 \text{ и } G \cdot H^T = 0$$

- Следовательно, можно *«поменять ролями»* эти две матрицы и использовать **H** как порождающую матрицу, а **G** как проверочную матрицу дуального кода.

Мусин С. Б.,
БГУИР

Примеры дуальных кодов

- Легко проверить, что если $C = \begin{cases} 0000 \\ 1100 \\ 0011 \\ 1111 \end{cases}$, то $C^{\perp} = C$
-
- Если $C = \begin{cases} 000 \\ 110 \\ 011 \\ 101 \end{cases}$, то $C^{\perp} = \begin{cases} 000 \\ 111 \end{cases}$

Мусин С. Б.,
БГУИР

Примеры дуальных кодов

- Код с повторением и код с проверкой на четность являются дуальными кодами.
- Порождающая матрица расширенного -кода Хэмминга (8,4)
- $$G^{\perp} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

совпадает с проверочной матрицей этого кода. Таким образом, этот код является дуальным самому себе.

Мусин С. Б.,
БГУИР

КОДЫ РИДА-МАЛЛЕРА

Тема

Мусин С. Б.,
БГУИР

Код Рида-Маллера

- Код, дуальный для расширенного (8, 4, 4)-кода Хемминга:

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

- является порождающей матрицей (G) кода Рида-Маллера первого порядка.
- Код задаётся параметрами r и m, где r – порядок кода Рида-Маллера, а длина кода зависит от m:

$$n = 2^m$$

Мусин С. Б.,
БГУИР

Код Рида-Маллера

- Каждая строка порождающей матрицы кода Рида-Маллера первого порядка имеет один и тот же вес 4, т.е. код Рида-Маллера первого порядка ортогональный.

- Для получения матрицы второго порядка надо взять сочетание по 2 строк матрицы первого порядка и перемножить (операция И) их между собой.

Мусин С. Б.,
БГУИР

- Получение кода Рида-Маллера второго порядка:
- $H = \begin{matrix} 1 \\ v_3 \\ v_2 \\ \\ v_1 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \rightarrow$
- $H = \begin{matrix} 1 \\ v_3 \\ v_2 \\ \\ v_1 \\ v_1v_2 \\ \\ v_1v_3 \\ v_2v_3 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$

Коды Рида-Маллера

Мусин С. Б.,
БГУИР

- Получение кода Рида-Маллера третьего порядка:

$$H = \begin{matrix} 1 \\ v_3 \\ v_2 \\ v_1 \\ v_1v_2 \\ v_1v_3 \\ v_2v_3 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \rightarrow H = \begin{matrix} 1 \\ v_3 \\ v_2 \\ v_1 \\ v_1v_2 \\ v_1v_3 \\ v_2v_3 \\ v_1v_2v_3 \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Коды Рида-Маллера

Мусин С. Б.,
БГУИР

- Построение порождающей матрицы кода Рида–Маллера может быть проведено рекурсивно следующим образом:
- $G_{R(r,m)} = \begin{bmatrix} G_0 \\ G_1 \\ \vdots \\ G_r \end{bmatrix}$, где $G_0 = g_0 = [\underbrace{1\,1\,\ldots 1}_{2^m}]$
- $G_1 = \begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_m \end{bmatrix} = \begin{bmatrix} & \underbrace{1\,1\,\ldots 1}_{2^{m-1}}\,\underbrace{0\,0\,\ldots 0}_{2^{m-1}} & \\ \underbrace{1\,1\,\ldots 1}_{2^{m-2}}\,\underbrace{0\,0\,\ldots 0}_{2^{m-2}}\,\underbrace{1\,1\,\ldots 1}_{2^{m-2}}\,\underbrace{0\,0\,\ldots 0}_{2^{m-2}} & \\ \vdots & \\ \underbrace{1\,0\,1\,0\,\ldots 1\,0}_{2^m} & \end{bmatrix}$ и $G_r = \begin{bmatrix} g_1 g_2 \\ g_1 g_3 \\ \vdots \\ g_{m-1} g_m \\ g_1 g_2 g_3 \\ \vdots \\ g_{m-r} g_{m-r+1} \ldots g_m \end{bmatrix}$

Коды Рида-Маллера

Мусин С. Б.,
БГУИР

Коды Рида-Маллера

- Коды Рида-Маллера корректируют больше, чем одну ошибку, но являются избыточными.
- Характеристики:
  - $n = 2^m$
  - $k = 1 + C_m^1 + C_m^2 + \cdots + C_m^r$
  - $d^* = 2^{m-r}$
- Если код Рида-Маллера порядка r, то код, дуальный данному порядка $(m - r - 1)$
- Кодирование: $m \cdot G =$ кодовое слово

Мусин С. Б.,
БГУИР

Матрица Адамара

- Матрица H_m размером $m \times m$, состоящая из элементов множества 1, -1, называется матрицей Адамара, если выполняется
- следующее условие:

$$\boldsymbol{H_m}^T \boldsymbol{H_m} = m\boldsymbol{E}$$

Мусин С. Б.,
БГУИР

Матрица Адамара

- Матрица Адамара имеет порядок:

$$H_1 = [1]$$

$$H_2 = H_1 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \text{ где } \otimes - \begin{matrix} \text{кронекерово} \\ \text{произведение} \end{matrix}$$

- $$H_{2m} = \begin{bmatrix} H_m & H_m \\ H_m & -H_m \end{bmatrix}$$

в общем случае: $H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$

Мусин С. Б.,
БГУИР

Построение кода Рида-Маллера с помощью матрицы Адамара

- Способ построения порождающей матрицы двоичных кодов Рида–Маллера с помощью матриц Адамара: заменим в матрице Адамара, элемент -1 на 0, затем последовательно будем находить кронекерово произведение $H_2 \otimes H_m$
- $$H_2 \otimes H_2 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Мусин С. Б.,
БГУИР

$$H_2 \otimes H_4 = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

- получили порождающую матрицу кода R(3,3)

Построение кода Рида-Маллера с помощью матрицы Адамара

Мусин С. Б.,
БГУИР

МЕТОД МАЖОРИТАРНОГО ДЕКОДИРОВАНИЯ

Тема

Мусин С. Б.,
БГУИР

- Допустим, при кодировании получили слово

$$c' = (i_1 i_2 i_3 i_4) \cdot G = (1\,1\,1\,0\,0\,1\,1\,0)$$

- где:

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

Метод мажоритарного декодирования

Мусин С. Б.,
БГУИР

- Выразим символы полученного слова:

$$G = \begin{array}{c} \\ i_1 \\ i_2 \\ i_3 \\ i_4 \end{array} \begin{array}{c} \begin{array}{cccccccc} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

- $c_1 = i_1$
  $c_2 = i_1 + i_4$
  $c_3 = i_1 + i_3$
  $c_4 = i_1 + i_3 + i_4$
  $c_5 = i_1 + i_2$
  $c_6 = i_1 + i_2 + i_4$
  $c_7 = i_1 + i_2 + i_3$
  $c_8 = i_1 + i_2 + i_3 + i_4$

Метод мажоритарного декодирования

Мусин С. Б.,
БГУИР

- Выразим i_4 во всех уравнениях, где оно участвует, начиная с последнего: $\begin{cases} i_4 = c_8 + c_7 \\ i_4 = c_6 + c_5 \\ i_4 = c_4 + c_3 \\ i_4 = c_2 + c_1 \end{cases}$
- Имея кодовое слово $c' = (\overset{c_1}{1}\ \overset{c_2}{1}\ \overset{c_3}{1}\ \overset{c_4}{0}\ \overset{c_5}{0}\ \overset{c_6}{1}\ \overset{c_7}{1}\ \overset{c_8}{0})$ получаем:

$$\begin{cases} i_4 = 1 \\ i_4 = 1 \\ i_4 = 1 \\ i_4 = 0 \end{cases} \Rightarrow i_4 = 1 \left(\begin{matrix}\text{Определяем} \\ \text{по большинству}\end{matrix}\right)$$

Метод мажоритарного декодирования

Мусин С. Б.,
БГУИР

- Если большинства нет (50/50), то ошибку выявили, но не обнаружили.
- Таким образом определяем i_4, i_3, i_2
- Для определения i_1 строим вектор:

$$x = (i_4 \quad i_3 \quad i_2) \cdot G'$$

где G' - матрица G без верхней строки.

Метод мажоритарного декодирования

Мусин С. Б.,
БГУИР

- Далее выполняем $x + c'$:

$$\begin{array}{r} c' = (1\,1\,1\,0\,0\,1\,1\,0) \\ + \\ x = (0\,1\,0\,1\,1\,0\,1\,0) \\ \hline e = (1\,0\,1\,1\,1\,1\,0\,0) \end{array}$$

  отсюда i_1 равно 1 (по большинству в e)

- Таким образом закодированное сообщение

$$(i_1 i_2 i_3 i_4) = (?\ ?\ 1\ 1)$$

  символ i_2 содержит ошибку и определён быть не может, т.к. большинства при его вычислении не было. Поэтому не может быть определён и i_1. В примере был использован произвольный вектор x с предположением, что i_2, i_3, i_4 удалось определить лишь для демонстрации нахождения i_1.

Метод мажоритарного декодирования

Мусин С. Б.,
БГУИР