

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина  
Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

# Код Рида-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

13 февраля 2022 г.

Описан Дэвидом Маллером (автор идеи) и Ирвингом Ридом (автор метода декодирования) в сентябре 1954 года. Обозначаются как  $RM(r, m)$ , где  $r$  — ранг, а  $2^m$  — длина кода. Кодирует сообщения длиной  $k = \sum_{i=0}^r C_m^i$  при помощи  $2^m$  бит.

Традиционно, считается что коды бинарные и работают над битами, т.е.  $\mathbb{Z}_2$ .

Соглашение: сложение векторов  $u, v \in \mathbb{Z}_2^n$  будем обозначать как  $u \oplus v = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$ .

# Булевы функции и многочлен Жегалкина

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина  
Минимальное  
расстояние

Декодирование

Алгоритмы Рида

Домашнее  
задание

Всякую булеву функцию можно записать при помощи таблицы истинности

$x$	$y$	$f(x, y)$
0	0	1
0	1	0
1	0	0
1	1	0

И при помощи многочлена Жегалкина:

$$f(x, y) = xy + x + y + 1$$

В общем случае, многочлены будут иметь следующий вид:

$$f(x_1, x_2, \dots, x_m) = \sum_{S \subseteq \{1, \dots, m\}} c_S \prod_{i \in S} x_i$$

Например, для  $m = 2$ :

$$f(x_1, x_2) = c_1 \cdot x_1 x_2 + c_2 \cdot x_1 + c_3 \cdot x_2 + c_4 \cdot 1$$

Всего  $n = 2^m$  коэффициентов для описания каждой функции.

# Функции небольшой степени

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Рассмотрим функции, степень многочленов которых не больше  $r$ :

$$\{f(x_1, x_2, \dots, x_m) \mid \deg f \leq r\}$$

Каждую можно записать следующим образом:

$$f(x_1, x_2, \dots, x_m) = \sum_{\substack{S \subseteq \{1, \dots, m\} \\ |S| \leq r}} c_S \prod_{i \in S} x_i$$

В каждом произведении используется не больше  $r$  переменных.

Сколько тогда всего коэффициентов используется?

$$k = C_m^0 + C_m^2 + \dots + C_m^r = \sum_{i=0}^r C_m^i$$

# Идея кодирования

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Пусть каждое сообщение (длины  $k$ ) — коэффициенты многочлена от  $m$  переменных степени не больше  $r$ .

Тогда мы можем его представить при помощи  $2^m$  бит, подставив все возможные комбинации переменных.

Таким образом получим таблицу истинности, из которой позднее сможем восстановить исходный многочлен, а вместе с ним и сообщение.

Зафиксировав в таблице порядок строк, можно выделить **вектор значений**, который и будет кодом.

$x$	$y$	$f(x, y)$	
0	0	1	$\Rightarrow \text{Eval}(f) = (1 \ 0 \ 0 \ 0)$
0	1	0	
1	0	0	
1	1	0	

# Пример

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина  
Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

- $r = 1$  (степень многочлена),  $m = 2$  (переменных).  
Это  $RM(1, 2)$ .
- Тогда наш многочлен:  $f(x, y) = c_1x + c_2y + c_3$ .
- Сообщение: 101, тогда  $f(x, y) = x + 0 + 1$ .
- Подставим всевозможные комбинации:

$x$	$y$	$f(x, y)$
0	0	1
0	1	1
1	0	0
1	1	0

- Получили код:  $\text{Eval}(f) = 1100$ .

# Декодирование когда потерь нет

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

- Мы получили код: 1100

- Представим таблицу истинности.

$x$	$y$	$f(x, y)$
0	0	1
0	1	1
1	0	0
1	1	0

- Подстановками в  $f(x, y) = c_1x + c_2y + c_3$  получим СЛАУ.

$$\begin{cases} c_3 = 1 \\ c_2 + c_3 = 1 \\ c_1 + c_3 = 0 \\ c_1 + c_2 + c_3 = 0 \end{cases}$$

- $c_1 = 1, c_2 = 0, c_3 = 1$ , исходное сообщение: 101.



# Коды 0-го порядка

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

Для случая  $RM(0, m)$  нужна функция от  $m$  аргументов, степени не выше 0.

- $f(x_1, x_2, \dots, x_m) = 0$
- $g(x_1, x_2, \dots, x_m) = 1$

Таблица истинности:

	$x_1$	$x_2$	$\dots$	$x_m$	$f(x_1, \dots, x_m)$	$g(x_1, \dots, x_m)$
$2^m$	0	0	$\dots$	0	0	1
	0	0	$\dots$	1	0	1
			$\ddots$			
	1	1	$\dots$	1	0	1

Вывод: это  $2^m$ -кратное повторение символа

- Сообщение 0 даст код  $\underbrace{00\dots0}_{2^m}$
- Сообщение 1 даст код  $\underbrace{11\dots1}_{2^m}$

# Доказательство линейности

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина  
Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Пусть  $C(x)$  кодирует сообщение  $x \in \mathbb{Z}_2^k$  в код  $C(x) \in \mathbb{Z}_2^m$ .

$$C(x) = (p_x(a_i) \mid a_i \in \mathbb{Z}_2^m)$$

где  $p_x(a_i)$  — соответствующий сообщению  $x$  многочлен.

Причём  $p_x$  берёт в качестве своих коэффициентов биты из  $x$ . Поскольку многочлены степени не выше  $r$  образуют линейное пространство, то  $p_{(x \oplus y)} = p_x + p_y$ .

Тогда:

$$C(x \oplus y)_i = p_{(x \oplus y)}(a_i) = p_x(a_i) + p_y(a_i) = C(x)_i + C(y)_i$$

т.е.  $\forall x, y \quad C(x \oplus y) = C(x) + C(y)$ , ч.т.д.

# Последствия линейности

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

- 1 Существует порождающая матрица  $G$ .

$$C(x) = x_{1 \times k} G_{k \times n} = c_{1 \times n}$$

- 2 Минимальное расстояние будет равно минимальному весу Хемминга среди всех кодов.

$$d = \min_{\substack{c \in C \\ c \neq 0}} w(c)$$

- 3 Корректирующая способность:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$

# Конструкция Плоткина: многочлены

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирование

Алгоритм Рида

Домашнее  
задание

Хотим понять как выглядят кодовые слова.

- Код — таблица истинности функции  $f(x_1, \dots, x_m) \in \text{RM}(r, m)$ , причём  $\deg f \leq r$ .
- Разделим функцию по  $x_1$ :  
$$f(x_1, \dots, x_m) = g(x_2, \dots, x_m) + x_1 h(x_2, \dots, x_m).$$
- Заметим, что  $\deg f \leq r$ , а значит  $\deg g \leq r$  и  $\deg h \leq r - 1$ .

# Конструкция Плоткина: таблица истинности

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирование

Алгоритм Рида

Домашнее  
задание

Ранее:  $f(x_1, \dots, x_m) = g(x_2, \dots, x_m) + x_1 h(x_2, \dots, x_m)$ .

- Заметим, что таблица истинности  $f$  состоит из двух частей: при  $x_1 = 0$  и при  $x_1 = 1$ .

$$\text{Eval}(f) = \left( \frac{\text{Eval}^{[x_1=0]}(f)}{\text{Eval}^{[x_1=1]}(f)} \right)$$

- Причём  $\text{Eval}^{[x_1=0]}(f) = \text{Eval}(g)$ , а  $\text{Eval}^{[x_1=0]}(f) \oplus \text{Eval}^{[x_1=1]}(f) = \text{Eval}(h)$ .
- Таким образом,  
 $\text{Eval}(f) = (\text{Eval}(g) \mid \text{Eval}(g) \oplus \text{Eval}(h))$ .

# Конструкция Плоткина: вывод

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

Если дана  $f(x_1, \dots, x_m)$ , причём  $\deg f \leq r$ , то можно её разделить:

$$f(x_1, \dots, x_m) = g(x_2, \dots, x_m) + x_1 h(x_2, \dots, x_m)$$

Также известно, что

$$\text{Eval}(f) = (\text{Eval}(g) \mid \text{Eval}(g) \oplus \text{Eval}(h)).$$

Заметим, что  $\text{Eval}(f)$  – кодовое слово (как и для  $g, h$ ).

Тогда:

$$c = \text{Eval}(f) \in \text{RM}(r, m) \quad (\text{т.к. } \deg f \leq r)$$

$$u = \text{Eval}(g) \in \text{RM}(r, m-1) \quad (\text{т.к. } \deg g \leq r)$$

$$v = \text{Eval}(h) \in \text{RM}(r-1, m-1) \quad (\text{т.к. } \deg h \leq r-1)$$

**Утверждение:** Для всякого кодового слова  $c \in \text{RM}(r, m)$  можно найти  $u \in \text{RM}(r, m-1)$  и  $v \in \text{RM}(r-1, m-1)$ , такие что  $c = (u \mid u + v)$ .

# Минимальное расстояние

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Хотим найти минимальное расстояние для кода  $\text{RM}(r, m)$

$$d = \min_{c \in C, c \neq 0} w(c)$$

Предположим, что  $d = 2^{m-r}$  и докажем по индукции.

**База:**  $\text{RM}(0, m)$  — единственный бит повторён  $2^m$  раз.

Очевидно,  $w(\underbrace{11\dots 1}_{2^m}) = 2^m = 2^{m-0} \geq 2^{m-r}$ .

**Гипотеза:** Если  $v \in \text{RM}(r-1, m-1)$ , то  $w(v) \geq 2^{m-r}$ .

**Шаг:** Хотим доказать для  $c \in \text{RM}(r, m)$ .

$$\begin{aligned} w(c) &= w((u \mid u \oplus v)) \stackrel{(1)}{=} w(u) + w(u \oplus v) \geq \\ &\stackrel{(2)}{\geq} w(u) + (w(v) - w(u)) = w(v) \stackrel{IH}{\geq} 2^{m-r} \blacksquare \end{aligned}$$

# Свойства и параметры

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирование

Алгоритмы Рида

Домашнее  
задание

Для бинарного кода  $RM(r, m)$ :

- $r \leq m$
- Длина кода:  $2^m$
- Длина сообщения:  $k = \sum_{i=0}^r C_m^i$
- Минимальное расстояние:  $d = 2^{m-r}$
- Корректирующая способность:  $t = 2^{m-r-1} - 1$
- Существует порождающая матрица  $G$  для кодирования
- Проверочная матрица  $H$  совпадает с порождающей для  $RM(m - r - 1, m)$



# Как линейный код

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина  
Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Этот код является линейным кодом, к нему применимы все обычные (и неэффективные методы):

- Перебор по всему пространству кодовых слов в поисках ближайшего.
- С использованием синдромов:  $s = rH^T$ .

Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритм Рида

Домашнее  
задание

Ранее: 101 кодируется как 1100 при помощи  $RM(1, 2)$

- $t = 1$



- $t = 0$



Код  
Рида-Маллера

Введение

Кодирование

Свойства и  
параметры  
кода

Конструкция  
Плоткина

Минимальное  
расстояние

Декодирова-  
ние

Алгоритмы Рида

Домашнее  
задание

TODO