

#### Код Рида-Маллера

Илья Кон

Введени

Кодировани

Декодирова ние

#### Код Рида-Маллера

#### Илья Коннов

Факультет компьютерных наук Высшая Школа Экономики

9 февраля 2022 г.



Код Рида-Маллера

2022-02-09



1. Если вы смотрите презентацию, то на сером фоне справа видны некоторые ценные комментарии, для которых поля слайда оказались слишком узки. Если вы читаете pdf-ку, то эти комментарии уже находятся в самом подходящем для них месте в тексте. Если вы смотрите мой доклад и видите этот текст, то что-то пошло серьёзно не так. Да, у этого одного файла есть три разные версии.



# Введение

 $\mathbb{Z}_2$ .

Код Рида-Маллера

Илья Кс

Введение

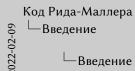
Кодировані

....

Декодирова<sup>.</sup> ние Описаны Дэвидом Маллером (автор идеи) и Ирвингом Ридом (автор метода декодирования) в сентябре 1954 года. Обозначаются как  $\mathrm{RM}(r,m)$ , 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 работают над битами, т.е.

◆ロ → 4回 → 4 三 → 4 三 → 9 Q (\*)



Описаны Дивидом Маллером (автор иден) и Ирвингом Ридом (автор метора декодирования) в сентябре 1954 года. Обозначаются как  $8M(r_n)$  (де r - раня  $r_n 2^{m-r}$  дивиз кода. Кодирует сообщения длиной  $k = \sum_{i=0}^{r} C_m^i$  при помощи  $2^m$  бат. Традициюнно, считается что коды работают над битами, т.е.

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

#### Булевы функции и многочлен Жегалкина

Код Рида-Маллера

Илья Конно

Введение

Колиповани

кодировани

Декодирова

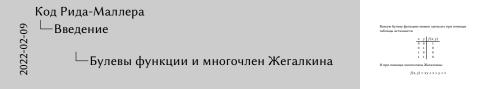
Всякую булеву функцию можно записать при помощи таблицы истинности

$$\begin{array}{c|cccc} x & y & f(x, y) \\ \hline 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ \end{array}$$

И при помощи многочлена Жегалкина:

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





## Многочлены Жегалкина

Код Рида-Маллера

1лья Ко

Введение

Кодировані

Декодирова

В общем случае, многочлены будут иметь следующий вид:

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

Например, для m=2:  $f(x_1,x_2)=c_1\cdot x_1x_2+c_2\cdot x_1+c_3\cdot x_2+c_4\cdot 1$ Всего  $n=2^m$  коэффициентов для описания каждой функции.

4□ > 4₱ > 4 ₺ > 4 ₺ > ₺

Код Рида-Маллера



## Функции небольшой степени

Код Рида-Маллера

Илья Конн

Введение

Своиства код

Декодирова ние Рассмотрим функции, степень многочленов которых не больше r:

$$\{f(x_1, x_2, ..., x_m) \mid \deg f \le r\}$$

Каждую можно записать следующим образом:

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

В каждом произведении используется не больше r переменных.

Сколько тогда всего коэффициентов используется?

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



Код Рида-Маллера —Введение

2022-02-09

Функции небольшой степени

- 1. Замечу, что при  $S=\emptyset$ , мы считаем, что  $\prod_{i\in S} x_i=1$ , таким образом всегда появляется свободный член.
- 2. Если говорить несколько проще, то для составления многочленов мы сложим сначала одночлены (x+y+z), затем произведения одночленов (xy+yz+xz) и т.д. вплоть до r множителей. Тогда легко видеть, почему k именно такое: мы складываем все возможные перестановки сначала для 0 переменных, потом для одной, двух, и так до всех r

### Идея кодирования

Код Рида-Маллера

4лья Коі

ведение

Кодирование

Свойства ко

Декодирова-

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

Тогда мы можем его представить при помощи  $2^n$  бит, подставив все возможные комбинации переменных (ведь рассматриваем многочлены над  $\mathbb{Z}_2$ ). Таким образом получим таблицу истинности, из которой позднее сможем восстановить исходный многочлен, а вместе с ним и сообщение.

4 D > 4 P > 4 E > 4 E > 9 Q P

### Код Рида-Маллера —Кодирование

∟Идея кодирования

Пусть каждое сообщение (длины k) — коэффициенты некоторого многочлена от лг переменных степени не больш

Тогда мы можем его представить при помощи 2<sup>6</sup> бит, подставия ясе возможные комбинации переменных (вать, рассматришаем миного-сеньи мая Z<sub>2</sub>). Таком образом получим таблику истинности, их которой подние соложем восставиять истодный миногочлем, а вместе с ним и сообщение.

# Пример

#### Рида-Маллера

Илья Конн

Введение

Кодирование

....

Декодирова

r = 1 (степень многочлена), m = 2 (переменных). Это RM(1, 2).

■ Тогда наш многочлен:  $f(x, y) = c_1 x + c_2 y + c_3$ .

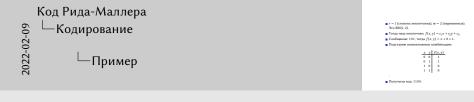
■ Сообщение: 101, тогда f(x, y) = x + 0 + 1.

■ Подставим всевозможные комбинации:

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

■ Получили код: 1100.







#### Линейность

Рида-Маллера

илья ко

ведение

Кодировани

Свойства кода ЛеколироваЛинейный (блоковый) код — такой код, что множество его кодовых слов образует k-мерное линейное подпространство в n-мерном линейном пространстве, изоморфное пространству k-битных векторов.

Слова —

4日 → 4周 → 4 差 → 4 差 → 2 9 9 0 0 0

#### Код Рида-Маллера 6-Свойства кода 70-77 — Линейность

Пинеймый (блоковый) код — гакой код, что множество его кодовых слов образует Е-мермое линеймое подпространство в п-мермом линеймом пространстве, изоморфное пространству k-битиых векторов. Слова —



# Потерь нет

Рида-Маллера



Код Рида-Маллера

2022-02-09

**–**Декодирование

□Потерь нет