

Код Рида-Маллера

Кодировані

Конструкция Плоткина Минимальное

Минимальное расстояние Параметры

ние
Пара слов о синдромах
Алгоритм Рида

Домашнее задание

Источники

Код Рида-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

14 февраля 2022 г.

Код Рида-Маллера

2022-02-14



- 1. Существует три различных варианта этого доклада:
 - 1.1 Краткая презентация, которую несложно рассказать, но может быть сложно понять (ReedMuller-trans.pdf).
 - 1.2 Более длинная презентация с ценными комментариями, дополнительными доказательствами и интересными фактами (ReedMuller-slides.pdf). Вы сейчас читаете именно эту версию.
 - 1.3 Текстовая статья со всем содержимым длинной презентации, комментариями на своих местах, а также бонусным приложением с более подробным описанием алгоритма (ReedMuller-article.pdf).

Их все можно посмотреть здесь: https://sldr.xyz/ReedMuller/

По любым вопросам: r-m@sldr.xyz или t.me/iliago или vk.com/iliago.

Содержание

Код Рида-Маллера

Источники

1 Введение 2 Кодирование 3 Свойства кода ■ Конструкция Плоткина ■ Минимальное расстояние Параметры 4 Декодирование ■ Пара слов о синдромах ■ Алгоритм Рида Пример 5 Домашнее задание

Код Рида-Маллера

2022-02-14 Содержание

Свойства кода Конструкция Плоткина Минимальное расстояние Параметры Декодирование Пара слов о синарома Алгориты Рида • Пример В Домашнее задание 6 Источники

Введение

.....

Рида-Маллера

Свойства к
Конструкция
Плоткина
Минимальное
расстояние

Минимальное расстояние Параметры

Декодирова ние

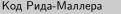
Пара слов о синдромах Алгоритм Рида Пример

Домаш задание

Источни

Код описан 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 бинарные и работают над битами, т.е. \mathbb{Z}_2 . Соглашение: сложение векторов $u,v\in\mathbb{Z}_2^n$ будем обозначать

 $\mathsf{KAK}\ u \oplus v = (u_1 + v_1, u_2 + v_2, ..., u_n + v_n).$



22-02-14

—Введение

Код описан Двеидом Малляром (автор идеи) и Ирвингом Ридои (автор менода декодирования) в свитябре 1954 года Обозваначаются как RM(r, m), гре r — ране, а 2^m — длина кода. Кодирует сообщения длинай $k=\sum_{i=0}^r C_n^i$ при помощи 2^m бит. Традициюнно, считается что коды бинарные и работают

Традиционно, считается что коды бинарные и работают над битами, т.е. Z_2 . Соглашается сложение векторое $u,v\in \mathbb{Z}_2^n$ будем обозначати как $u\oplus v=(u_1+v_1,u_2+v_2,...,u_n+v_n)$.

Булевы функции и многочлен Жегалкина

Код Рида-Маллера

Кодирование тобл

Конструкция Плоткина Минимальное

Минимальное расстояние Параметры

ние Пара слов о синдромах

синдромах Алгоритм Рида Пример

Домашн задание

Источник

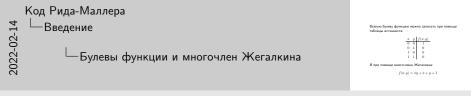
Всякую булеву функцию можно записать при помощи таблицы истинности

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

И при помощи многочлена Жегалкина:

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





Многочлены Жегалкина

Код Рида-Маллера

Кодирование

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

◆□▶◆□▶◆□▶◆□▶ □ 夕久○



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

Hanpuwep, ans m = 2: $f(x_1, x_2) = c_1 \cdot x_1x_2 + c_2 \cdot x_1 + c_3 \cdot x_2 + c_4 \cdot 1$ Boero $n = 2^m$ soaddhuuninton ans onucanes sampoi



Функции небольшой степени

Рида-Маллера

Кодирование

Рассмотрим функции, степень многочленов которых не больше r:

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

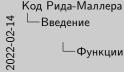
Каждую можно записать следующим образом:

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

В каждом произведении используется не больше rпеременных.

Сколько тогда всего коэффициентов используется?

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



-Функции небольшой степени

Сколько тогда всего коэффициентов используется $k = C_m^0 + C_m^2 + ... + C_m^r = \sum_i C_m^i$

- 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 (поскольку мы работаем в поле \mathbb{Z}_2 , здесь нету x^2, y^2, z^2 , т.к. $a^2 = a$). Тогда легко видеть, почему kименно такое: мы складываем все возможные перестановки сначала для 0 переменных, потом для одной, двух, и так до всех r



Идея кодирования

Код Рида-Маллера

Кодировани

Свойства кода Конструкция Плоткина Минимальное

Декодиров ние

Пара слов о синдромах Алгоритм Рида Пример

Домашне задание

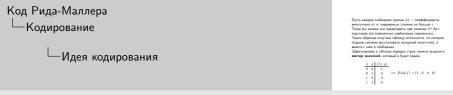
Источні

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.

\boldsymbol{x}	y	f(x,y)				
0	0	1				
0	1	0	$\implies \text{Eval}(f) = (1$	0	0	0)
1	0	0	· ·			
1	1	0				





- 1. Их 2^m , поскольку рассматриваем многочлены только над \mathbb{Z}_2 от m переменных.
- 2. Вектор значений обозначается $\operatorname{Eval}(f)$ столбец таблицы истинности, содержащий значения функции. Имеет смысл только при зафиксированном порядке строк в таблице. У меня он везде самый обычный, как в примере выше.

Код Рида-Маллера

Кодирован

Свойства кода

Плоткина Минимальное

расстояния Параметры

Декодиров ние

Пара слов о синдромах Алгоритм Рида Пример

Домашне залание

Источн

r=1 (степень многочлена), m=2 (переменных). Это $\mathrm{RM}(1,2)$.

■ Тогда наш многочлен: $f(x_1, x_2) = c_3x_2 + c_2x_1 + c_1$.

© Сообщение: 101, тогда $f(x_1, x_2) = x + 0 + 1$.

■ Подставим всевозможные комбинации:

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

■ Получили код: Eval(f) = 1100.





1. Здесь и далее я для краткости и удобства записываю битовые векторы не как $(1 \ 0 \ 0 \ 1)$, а как 1001 при помощи нескучного шрифта.

Декодирование когда потерь нет

Код Рида-Маллера

Свойства кода

Мы получили код: 1100

■ Представим таблицу истинности.

$$egin{array}{c|ccc} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ \end{array}$$

 $x y \mid f(x,y)$

- Подстановками в $f(x,y)=c_1x+c_2y+c_3$ получим СЛАУ. $\begin{cases} c_2 &+ c_3 = 1\\ c_1 &+ c_3 = 0\\ c_1 &+ c_2 &+ c_3 = 0 \end{cases}$ ■ Подстановками в
- $c_1 = 1, c_2 = 0, c_3 = 1,$ исходное сообщение: 101.

Код Рида-Маллера -Кодирование -Декодирование когда потерь нет

1. Теперь покажем, как можно декодировать когда потерь нет. Этот пример продолжение предыдущего.



Коды 0-го порядка

Рида-Маллера

Код

Свойства кода

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

- $f(x_1, x_2, ..., x_m) = 0$
- $q(x_1, x_2, ..., x_m) = 1$

Таблица истинности:

$$2^{m} \begin{cases} x_{1} & x_{2} & \dots & x_{m} & f(x_{1}, \dots, x_{m}) & g(x_{1}, \dots, x_{m}) \\ 0 & 0 & \dots & 0 & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 & 1 \\ & & \ddots & & & & \\ 1 & 1 & \dots & 1 & 0 & 1 \end{cases}$$

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

Вывод: это 2^m -кратное повторение символа

- lacktriangle Сообщение 0 даст код 00...0
- lacktriangle Сообщение 1 даст код 11...1

Код Рида-Маллера Кодирование -Коды 0-го порядка

- 1. Отдельно стоит рассмотреть вариант кода при r=0, он нам в будущем пригодится для доказательств.
- 2. Таких функций существует всего лишь две, поскольку мы можем влиять лишь на свободный член. Все остальные коэффициенты обнуляются из-за требования $\deg f \leq 0$.
- 3. Здесь число строк, как и в любой другой таблице истинности, равно 2^m , а колонки со значениями никак не зависят от аргументов функций. Получается две колонки – одна с нулями, другая с единицами.



Коды m-го порядка

Код Рида-Маллера

Кодировані

Свойства кода Конструкция Плоткина

Минимально расстояние

Декодирова

Пара слов о синдромах Алгоритм Рида

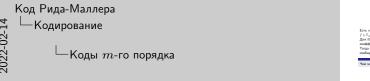
Домашне залание

Источні

Есть m переменных, и мы рассматриваем многочлены $f \in \mathbb{F}_2[x_1,...,x_m]: \deg f \leq m$, т.е. все возможные. Для $\mathrm{RM}(m,m)$ мы используем все доступные коэффициенты многочлена для кодирования сообщения. Тогда нет избыточности: $k = \sum_{i=0}^m C_m^i = 2^m = n$ — длина сообщения равна длине кода.

Чем меньше порядок r, тем больше избыточность.





Ест. m первыенных, n мы рассывтриваем многочлены $f \in F_2(x_1, \dots, x_m)$: $\deg f \leq m$, r. a. a se возможные. Для RM(m, m) мы используем все доступные можфонциямты многочлена для ходирования сообщения ходфонциямты многочлена для ходирования сообщения равна дляне ходы.

Чем меньше порядок r, тем больше избыточность

1. Есть ещё один тривиальный случай, когда m=r.

Доказательство линейности

Рида-Маллера

Декодирова-

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.

сообщений (\mathbb{Z}_2^k) в пространство слов (\mathbb{Z}_2^m). Для этого необходимо немного формализовать всё описанное раньше.

Код Рида-Маллера

Свойства кода

операция сложения побитовая.

1, x, y, z, xy, yz, xz (для трёх переменных, степени не выше 2). Чтобы преобразовать сообщение в многочлен, мы берём каждый бит

2. Пояснение: перебираем все векторы a_i (2^m штук), подставляем каждый в $p_{\scriptscriptstyle T}$ в качестве переменных и таким образом получаем вектор значений (длины 2^m). Именно он и называется кодом. 3. Напомню, что базис пространства многочленов выглядит примерно так:

такое преобразование будет изоморфизмом. Именно поэтому

-Доказательство линейности

1. Хотим показать, что этот код является линейным, т.е. что его кодовые слова образуют линейное пространство, и у нас есть изоморфизм из пространства

Пусть C(x) нодирует сообщение $x \in \mathbb{Z}_+^k$ в код $C(x) \in \mathbb{Z}_+^m$ $C(x) = (p_s(a_i) \mid a_i \in \mathbb{Z}_2^m)$

инейное пространство, то $p_{(\mu m_0)} = p_\mu + p_\mu$ $C(x \oplus y)_i = p_{(x \cap y)}(a_i) = p_x(a_i) + p_y(a_i) = C(x)_i + C(y)_i$ T.e. $\forall x, y \ C(x \oplus y) = C(x) + C(y)$, y, r, a.

сообщения и умножаем его на соответствующий базисный вектор. Очевидно, $p_{(x+y)} = p_x + p_y$. Обратите внимание, что сообщение x это не просто число

 (\mathbb{Z}_{2^k}) и мы рассматриваем его биты, а реально вектор битов (\mathbb{Z}_2^k) . У него 4. Здесь я использую запись $C(x)_i$ для i-го элемента вектора C(x). Поскольку i произвольное, то и весь вектор получился равен. Таким образом, этот код действительно линейный и к нему применимы уже известные теоремы!



Последствия линейности

Код Рида-Маллера

Кодировани

Конструкци: Плоткина Минимальн

Минимально расстояние Параметры

Декодирование

Пара слов о синдромах Алгоритм Рида Пример

Домашне задание

Источниі

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:

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





- 1. Так можно кодировать сообщения x в коды c. Но искать её мы не будем, обойдёмся одними многочленами, это интереснее.
- 2. Вес Хэмминга вектора количество в нём ненулевых элементов.
- 3. Доказательство очень просто: минимальное расстояние вес разности каких-то двух различных кодов, но разность двух кодов тоже будет кодом, т.к. мы в линейном пространстве. Значит достаточно найти минимальный вес, но не учитывая нулевой вектор, т.к. разность равна нулю тогда и только тогда, когда коды равны.
- 4. Однако мы ещё не знаем как выглядят наши коды (как выглядят таблицы истинности функций степени не больше r?). А значит не можем ничего сказать про минимальное расстояние.



Конструкция Плоткина: многочлены

Код Рида-Маллера

Кодировані

Своиства ко Конструкция Плоткина

глинимально расстояние Параметры

Декодирова ние Пара слов о

синдромах **Алгоритм Рида** Пример

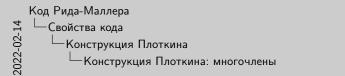
Домашне задание

Источникі

Хотим понять как выглядят кодовые слова.

- Код таблица истинности функции $f(x_1,...,x_m)\in \mathrm{RM}(r,m)$, причём $\deg f\leq r$.
- Разделим функцию по x_1 : $f(x_1,...,x_m) = g(x_2,...,x_m) + x_1h(x_2,...,x_m).$
- $lacksymbol{\blacksquare}$ Заметим, что $\deg f \leq r$, а значит $\deg g \leq r$ и $\deg h \leq r-1.$





- Код таблица истинности функции
- В Разделим функцию по x_1 : $f(x_1,...,x_m) = g(x_2,...,x_m) + x_1h(x_2,...,x_m)$
- В Заметим, что $\deg f \le r$, а значит $\deg g \le r$ и $\deg h \le r 1$.
- 1. Порядок очевидно не больше r, потому что это условие для включения в пространство кодов $\mathrm{RM}(r,m)$.
- 2. Теперь у нас есть две функции от меньшего числа аргументов. Очевидно, так можно сделать всегда, когда ${\sf m}>1$.

Конструкция Плоткина: таблица истинности

Код Рида-Маллера

Кодирование

Конструкция Плоткина Минимально

расстояние
Параметры

Декодиро

ние
Пара слов о синдромах
Алгоритм Рида
Пример

Домашнее задание

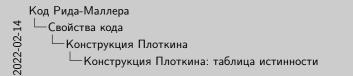
Источни

Panee: $f(x_1,...,x_m) = g(x_2,...,x_m) + x_1h(x_2,...,x_m)$.

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

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

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



Parker: $f(x_1,...,x_m)=g(x_2,...,x_m)+x_1\hbar(x_2,...,x_m)$. \blacksquare Заметим, что таблица истинности f состоит из частей: при $x_1=0$ и при $x_1=1$.

 $\text{Eval}(f) = \frac{1}{(\text{Eval}^{|\theta_1|-1})}$

- Причём $\operatorname{Eval}^{(x_1=0]}(f) = \operatorname{Eval}(g)$, a $\operatorname{Eval}^{(x_1=0)}(f) \oplus \operatorname{Eval}^{(x_1=1)}(f) = \operatorname{Eval}(h)$
- \blacksquare Таким образом, $\operatorname{Eval}(f) = (\operatorname{Eval}(g) \mid \operatorname{Eval}(g) \oplus \operatorname{Eval}(h))$
- 1. Теперь рассмотрим те же функции, но со стороны их таблиц истинности. Нам же интересны именно коды, а они как раз очень тесно связаны с этими таблицами.
- 2. Про обозначения: $\operatorname{Eval}(f)$ таблица для всей функции (вектор значений, если точнее), $\operatorname{Eval}^{[x_1=0]}(f)$ кусок таблицы при $x_1=0$, $\operatorname{Eval}^{[x_1=1]}(f)$ кусок таблицы при $x_1=1$. Они нам после этого доказательства больше не понадобятся.
- 3. Это всё следует из ранее полученного утверждения. Если мы подставим $x_1=0$, то останется только g первое равенство очевидно. Если же мы рассмотрим $\mathrm{Eval}^{[x_1=1]}(f)$, то получим $\mathrm{Eval}(g+h)$, но если туда прибавить ещё раз $\mathrm{Eval}(g)$, то останется только $\mathrm{Eval}(h)$ (поскольку 1+1=0 в \mathbb{Z}_2) получили второе равенство.
- 4. Палочка по центру конкатенация векторов.

Конструкция Плоткина: вывод

Код Рида-Маллера

дировани

Свойства кода Конструкция Плоткина Минимальное

Параметры
Декодирова-

Пара слов о синдромах

Алгоритм Рида
Пример

Домашн задание

Источни

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

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

Также известно, что $\operatorname{Eval}(f) = (\operatorname{Eval}(q) \mid \operatorname{Eval}(q) \oplus \operatorname{Eval}(h)).$

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

$$c = \operatorname{Eval}(f) \in \operatorname{RM}(r,m)$$
 (т.к. $\deg f \leq r$) $u = \operatorname{Eval}(g) \in \operatorname{RM}(r,m-1)$ (т.к. $\deg g \leq r$) $v = \operatorname{Eval}(h) \in \operatorname{RM}(r-1,m-1)$ (т.к. $\deg h \leq r-1$)





- 1. Теперь собираем всё это в одно важное утверждение.
- 2. Причём мы уже знаем, что $\deg g \leq r$ и $\deg h \leq r-1$, если $\deg f \leq r$
- 3. Напомню, что $\mathrm{RM}(r,m)$ включает в себя все функции (их таблицы истинности, если точнее) от m аргументов и степени не выше r. Очевидно, наши годятся.



Конструкция Плоткина

Код Рида-Маллера

Кодировані

Конструкция Плоткина Минимальное

Минимальное расстояние Параметры

Декодирова ние

Пара слов о синдромах Алгоритм Рида Пример

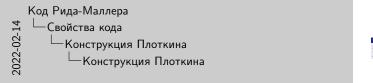
Домашне задание

Лсточники

Теорема

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





Творима Дин всикого кодового слова $c\in \mathrm{RM}(r,m)$ можно найти $u\in \mathrm{RM}(r,m-1)$ и $v\in \mathrm{RM}(r-1,m-1)$, такие что $c=(u\mid u+v)$.

1. Что здесь важно отметить — оба наших новых кодовых слова u,v получились «меньше», чем исходное c. Это позволяет, во-первых, устраивать индукцию по m, чем мы скоро и займёмся. Во-вторых, это позволяет легко строить большие порождающие матрицы, но мы этим не будем заниматься.



Минимальное расстояние

Рида-Маллера

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

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

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

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

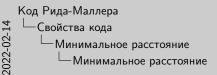
Очевидно,
$$w(\underbrace{\text{11...1}}) = 2^m = 2^{m-0} \geq 2^{m-r}.$$

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

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

$$\begin{split} w(c) &\stackrel{(1)}{=} w((u \mid u \oplus v)) \stackrel{(2)}{=} w(u) + w(u \oplus v) \geq \\ &\stackrel{(3)}{\geq} w(u) + (w(v) - w(u)) = w(v) \stackrel{IH}{\geq} 2^{m-r} \blacksquare \end{split}$$





 $d = \min_{e \in C, e \neq 0} w(e)$ Прадположим, что $d = 2^{mn}$ и докажем по индукции Базас RM(0, m) — единственный бит повторён 2^m р. Оченидно, $w(21,...1) = 2^m = 2^{m-2} \geq 2^{m-r}$.

этела: Если $v \in \text{RM}(r-1, m-1)$, то $w(v) \ge 2^{nv-p}$. $r: \mathsf{Xorum}$ доказать для $c \in \mathsf{RM}(r, m)$. $w(c) \stackrel{(a)}{=} w((u \mid u \oplus v)) \stackrel{(2)}{=} w(u) + w(u \oplus v) \ge \frac{r}{2}$ $\stackrel{(a)}{\geq} w(u) + (w(v) - w(u)) = w(v) \ge 2^{rv-p}$

- 1. Случай $\mathrm{RM}(0,m)$ мы разбирали раньше, но я напомню. Здесь длина сообщения равна $k=\sum_{i=0}^r C_m^i=C_m^0=1$, а длина кода $n=2^m$. Причём мы просто берём один бит (соответствует функции $f(x_1,...,x_m)=0$ или $f(x_1,...,x_m)=1$) и повторяем его 2^m раз (в таблице истинности). Замечу, что не рассматриваю второй случай w(00...0), поскольку он нам не нужен для расчёта минимального расстояния. Вариант с нулевым вектором явно выкидывается, см. определение d выше.
- 2. Теперь немного объяснений. Переход (1): используем конструкцию Плоткина, чтобы разбить c на конкатенацию двух кодовых слов поменьше. Переход (2): $w((x\mid y))=w(x)+w(y)$. Вес это всего лишь число ненулевых элементов, поэтому нет разницы как мы будем группировать части вектора. Переход (3): $w(u\oplus v)\geq w(v)-w(u)$. Если у нас в v стоит w(v) бит, то прибавив к нему u, мы сможем изменить (обнулить) не больше w(u) бит. Возможно появится больше единиц, но нас интересует нижняя граница. Переход (IH): предположение индукции в чистом виде.



Свойства и параметры

Код Рида-Маллера

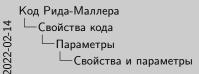
Кодировани

Свойства код Конструкция Плоткина

Декодирова

Для бинарного кода $\mathrm{RM}(r,m)$:

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



Для банарного хода $\mathrm{RM}(r,m)$: $\mathbf{z} r \leq m$ $\mathbf{z} \neq m$ $\mathbf{z$

Коррактирующая способность: t = 2^{m-m} − 1
 Существует порождающая матрица G для кодирован
 Проверочная матрица H совпадает с порождающей для RM(m − r − 1, m)

- 1. Теперь можно подвести итоги исследования свойств.
- 2. , поскольку $t=\left|\frac{d-1}{2}\right|=\left|\frac{2^{m-r}}{2}-\frac{1}{2}\right|=\left|2^{m-r-1}-0.5\right|=2^{m-r-1}-1$
- 3. , она позволяет делать так: C(x) = xG. Но я, как обычно, её избегаю. Рекомендую почитать «Коды Рида-Маллера: Примеры исправления ошибок», если интересно.
- 4. , но это я это доказывать не собираюсь. Но его можно найти в «Reed-Muller Codes: Theory and Algorithms», раздел Duality.



Как линейный код

Код Рида-Маллера

Кодирован

Конструкция Плоткина

Минимальное расстояние Параметры

Декодирова ние

Пара слов о синдромах Алгоритм Рида Пример

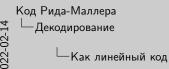
Домашнее задание

1сточники

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: $s = rH^{T}$.





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

ближайшего.

■ С использованием синдромов: $s = rH^T$.

- 1. Этот способ применим ко всем кодам, но никто в здравом уме им не пользуется.
- 2. Здесь s синдром, r полученное сообщение, H проверочная матрица. Этот метод обычен для линейных кодов.
- 3. Эти способы нужно иметь в виду, но о них было рассказано и без меня, так что я их пропущу.



Синдромы и как их использовать

Код Рида-Маллера

Кодировані

Конструкция Плоткина

расстояние Параметры

Декодирова ние

Пара слов о синдромах Алгоритм Рида

Домашнее задание

Источни

Пусть у нас в полученном сообщении r есть ошибка e. Тогда r=v+e, где v — кодовое слово, которое крайне легко можно декодировать. Получается, что $s=rH^T=(v+e)H^T=vH^T+eH^T=eH^T$, поскольку $vH^T=0$ (есть такое свойство). Мы можем перебрать всевозможные ошибки (e), для каждой посчитать синдром и записать всё это в таблицу. Тогда, чтобы восстановить сообщение, нужно посчитать синдром, по таблице найти ошибку и исправить её.



Пусть у нас в палученном сообщения r есть сшибка c. Тогра r=r+c, $r_B v$ — ворхово слово, жогоро врайне писть моном роморовать. Палученски, что $s=rH^2=(r+c)H^2=cH^2+cH^2-cH^2$, свосомых размен восможные ошибке (c), для каждой посчитать сикиров и записать вай от в таблицу. Тогдь, и тобы восстаномых сообщеном, что что в таблицу. Тогдь, и тобы восстаномых сообщения, чунно посчитать сихиров, по таблице, найти сообщения, чунно посчитать сообщения, чунно посчитать с

- 1. Я не стал включать это в презентацию, но вообще-то говоря метод полезный, так что пусть будет здесь.
- 2. Источник: https://ru.wikipedia.org/wiki/Линейный_код

Определения

Код Рида-Маллера

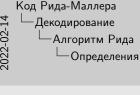
Пусть $A\subseteq\{1,...,m\}$ для $m\in\mathbb{N}$

2 Подпространство $V_A\subseteq \mathbb{F}_2^m$, которое обнуляет все v_i , если $i\notin A\colon V_A=\{v\in \mathbb{F}_2^m: v_i=0\ \forall i\notin A\}$

3 Аналогично для $V_{\bar{A}}$, где $\bar{A}=\{1,...,m\}\setminus A$: $V_{\bar{A}}=\{v\in\mathbb{F}_2^m:v_i=0\ \forall i\in A\}$

Пример:

- Пусть $m = 3, A = \{1, 2\}$, тогда ...
- \blacksquare $\mathbb{F}_2^m = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- $V_A = \{000, 010, 100, 110\} \ (v_3 = 0 \ \forall v)$
- $\bar{A} = \{1, 2, 3\} \setminus A = \{3\}$
- $V_{\bar{A}} = \{000, 001\} \ (v_1 = v_2 = 0 \ \forall v)$



■ Пусть $A \subseteq \{1,...,m\}$ для $m \in \mathbb{N}$ ■ Подпрострамство $V_A \subseteq \mathbb{F}_2^m$, которое обмужеет все v: если $i \notin A$: $V_A = \{v \in \mathbb{F}_2^m : v_i = 0 \ \forall i \notin A\}$ ■ Аналогично для V_A : $r_{AB} : \tilde{A} = \{1,...,m\} \setminus A$:

 \blacksquare Аналогично для $V_{\bar{A}}$, где $\bar{A} = \{1, ..., V_{\bar{A}} = \{v \in \mathbb{F}_2^m : v_i = 0 \ \forall i \in A\}$

- \blacksquare Пусть $m=3, A=\{1,2\}$, тогда ... \blacksquare $\mathbb{F}_2^n=\{000,001,010,011,100,101,110,111\}$ \blacksquare $V_A=\{000,010,100,110\}$ $\{v_3=0\ \forall v\}$
- $\mathbf{E} V_A = \{000, 010, 100, 110\} (v_3 = 0 \ \forall v)$ $\mathbf{E} \tilde{A} = \{1, 2, 3\} \ A = \{3\}$ $\mathbf{E} V_{\tilde{A}} = \{000, 001\} (v_1 = v_2 = 0 \ \forall v)$
- 1. Начать стоит с нескольких определений, без которых алгоритм Рида объяснить не получится.
- 2. все 8 векторов этого пространства
- 3. обнулилась третья позиция, первые две остались
- 4. осталась только третья позиция, остальные обнулились.



Смежные классы

Код Рида-Маллера

Кодировані

Свойства код Конструкция Плоткина

расстояние Параметры

Декодирова ние

Пара слов о синдромах Алгоритм Рида

Домашне задание

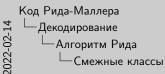
Источни

Если фиксирован $V_A\subseteq \mathbb{F}_2^m$, то для каждого $b\in \mathbb{F}_2^m$ существует смежный класс V_A+b :

$$(V_A + b) = \{v + b \mid v \in V_A\}$$

Утверждается, что если брать $b \in V_{\bar{A}}$, то полученные смежные классы будут все различны (и это будут все смежные классы).





Если фиксирован $V_A\subseteq \mathbb{F}_2^n$, то для каждого $b\in \mathbb{F}_2^n$ существует смежный килас V_A+b : $(V_A+b)=\{v+b\mid v\in V_A\}$ Утворждается, что если брать $b\in V_A$, то полученные смежные классы будут все различны (в это будут все

1. Почему все смежные классы $(V_A + b)$ можно получить именно перебором $b \in V_{\bar{A}}$ можно найти в разделе «Дополнительные доказательства» из пдфки



Код Рида-Маллера

Кодировани

Свойства ко Конструкция Плоткина

Минимальн расстояние Параметры

Декодирование

Пара слов о синдромах Алгоритм Рида

Домашнее задание

Источни

Декодирует сообщение u, если использовался RM(r, m). Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. На вход поступает **Data:** vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$ бинарный вектор yt = rдлины 2^m . Это вектор while t > 0значений функции, foreach $A \subseteq \{1, ..., m\}$ with |A| = tвозможно с ошибками c = 0(но их не больше, чем foreach $b \in V_{\bar{A}}$ $c + = \left(\sum_{z \in (V_A + b)} y_z
ight) mod 2$ $t = 2^{m-r-1} - 1$). $u_A \leftarrow \mathbf{1} [c \ge 2^{m-t-1}]$ $y = \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1, \dots, m\} \ |A| = t}} u_A \prod_{i \in A} x_i\right)$ t -= 1

◆□▶◆□▶◆□▶◆□▶ ■ 釣魚@



- 1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в рdfке.
- 2. Цель восстановить все коэффициенты при многочлене вида $f(x_1,...,x_m) = u_{\varnothing} + u_1x_1 + x_2x_2 + ... + u_{1,2,...,r}x_{1,2,...,r}, \text{ где } \deg f \leq r.$ Обратите внимание, что для индексов при u используются подмножества $A \subseteq \{1,...,m\}, |A| \leq r$, причём каждый u_A умножается на свой $\prod_{i \in A} x_i.$



Код Рида-Маллера

Кодировани

Свойства к Конструкция Плоткина

Минимальное расстояние Параметры

Декодирование

Пара слов о синдромах Алгоритм Рида

Домашнее задание

Источни

Декодирует сообщение u, если использовался RM(r, m). Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. Будем восстанавливать **Data:** vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$ сначала коэффициенты t=r u_A при старших while t > 0степенях, потом foreach $A \subseteq \{1, ..., m\}$ with |A| = tпоменьше и так пока не c = 0foreach $b \in V_{\bar{A}}$ восстановим их все. $\bigg| \quad c \mathrel{+}= \left(\sum_{z \in (V_A + b)} y_z \right) \bmod 2$ Hачинаем с t=r. $u_A \leftarrow \mathbf{1} [c \ge 2^{m-t-1}]$ $y = \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1, \dots, m\} \ |A| = t}} u_A \prod_{i \in A} x_i\right)$ t -= 1

◆□▶◆□▶◆□▶◆□▶ □ 夕久○



1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает — см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в рdfке.

Код Рида-Маллера

Кодировани

Свойства к

Минимальное расстояние

Декодирова ние

Пара слов о синдромах Алгоритм Рида

Домашнее задание

Источни

Декодирует сообщение u, если использовался $\mathrm{RM}(r,m)$. Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. Хотим восстановить все **Data:** vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$ коэффициенты при t = rмономах степени t. Для while t > 0этого перебираем все Aforeach $A \subseteq \{1, ..., m\}$ with |A| = tи для каждого c = 0foreach $b \in V_{\bar{A}}$ восстанавливаем $c += \left(\sum\limits_{z\in (V_A+b)} y_z
ight) mod 2 \qquad$ коэффициент u_A при $x_{A_1}x_{A_2}...x_{A_t}.$ $u_A \leftarrow 1 [c \ge 2^{m-t-1}]$ $y = \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1,\dots,m\} \ |A|=t}} u_A \prod_{i \in A} x_i
ight)$ t -= 1

◆□▶◆□▶◆□▶◆□▶ □ 夕久○



1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает — см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в рdfке.

Рида-Маллера

t -= 1

Декодирует сообщение u, если использовался $\mathrm{RM}(r,m)$. Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. Чтобы восстановить **Data:** vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$ коэффициент, нужно t = rперебрать все смежные while t > 0классы вида $(V_A + b)$: foreach $A \subseteq \{1, ..., m\}$ with |A| = t $V_{\Delta} = \{v \in \mathbb{F}_2^m\}$ c = 0foreach $b \in V_{\bar{A}}$ $: v_i = 0 \ \forall i \notin A$ все остальные $v_i = 0$.

◆□▶◆□▶◆□▶◆□▶ ■ 釣魚@

Код Рида-Маллера –Декодирование —Алгоритм Рида \square Алгоритм Рида для кода $\mathrm{RM}(r,m)$

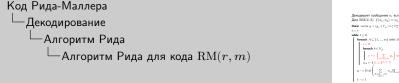


1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает — см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в pdfке.

Рида-Маллера

```
Декодирует сообщение u, если использовался \mathrm{RM}(r,m).
Для RM(2,2): f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4.
                                     Считаем количество (c)
Data: vector y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)
                                           смежных классов, в
t = r
                                           которых
while t > 0
                                           \sum y_z = 1 \pmod{2}.
    foreach A \subseteq \{1, ..., m\} with |A| = t
                                          Пороговое значение
        foreach b \in V_{\bar{A}}
                                          (2^{m-t-1}) здесь —
                                           половина от числа
                                           смежных классов.
       u_A \leftarrow \mathbf{1} \left[ c \geq 2^{m-t-1} \right]
                                           Таким образом, если
                                           большинство сумм
                                          дало 1, то u_A = 1,
                                           иначе u_A = 0.
    t -= 1
```

◆□▶◆□▶◆□▶◆□▶ ■ 釣魚@





- 1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает — см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в pdfке.
- 2. Если это количество больше порогового значения, то считаем, что $u_A = 1$, иначе же $u_A = 0$.



Рида-Маллера

t -= 1

Декодирует сообщение u, если использовался RM(r, m). Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. Затем мы вычитаем из **Data:** vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$ y (вектор значений t = rфункции) всё while t > 0найденное на этой foreach $A \subseteq \{1, ..., m\}$ with |A| = tитерации, после чего c = 0foreach $b \in V_{\bar{A}}$ переходим к мономам $c \mathrel{+}= \left(\sum_{z \in (V_A + b)} y_z
ight) mod 2$ меньшей степени. Повторять до $u_A \leftarrow \mathbf{1} \left[c \geq 2^{m-t-1} \right]$ восстановления всех $y == \operatorname{Eval} \left(\sum_{\substack{A \subseteq \{1,\dots,m\} \\ |A|=t}} u_A \prod_{i \in A} x_i \right)$ коэффициентов.

◆□▶◆□▶◆□▶◆□▶ ■ 釣魚@

Код Рида-Маллера –Декодирование —Алгоритм Рида \square Алгоритм Рида для кода $\mathrm{RM}(r,m)$



1. Теперь, наконец, сам алгоритм Рида с объяснением, что тут происходит. Почему он именно такой и почему это работает — см. раздел (на русском) «Reed's Algorithm: Unique decoding up to half the code distance» [??] в pdfке.

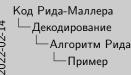
Код Рида-Маллера

Ранее: 101 кодируется как 1100 при помощи ${
m RM}(1,2)$ Положим $y_{00} = 1, y_{01} = 1, y_{10} = 0, y_{11} = 0$ Здесь m=2, значит $A\subseteq \{1,2\}$. Причём r=1, т.е. $|A|\leq 1$.

Шаг 1/3: $t = 1, A = \{1\}$

- \blacksquare Здесь $V_{\Lambda} = \{00, 10\}, V_{\bar{\Lambda}} = \{00, 01\}.$ Нужно рассмотреть два смежных класса.
- $(V_A + 00) = \{00, 10\}, \text{ cymma: } y_{00} + y_{10} = 1 + 0 = 1$
- $(V_A + 01) = \{01, 11\}, \text{ cymma: } y_{01} + y_{11} = 1 + 0 = 1$
- Итого: $u_A = u_{\{1\}} = 1$





этих аргументах.

Положим $y_{00} = 1, y_{01} = 1, y_{10} = 0, y_{11} = 0$ Здесь m=2, аначит $A\subseteq \{1,2\}$. Причём r=1, т.е. $|A|\le 1$

- Здесь $V_A = \{00, 10\}, V_A = \{00, 01\}$
- Нужно рассмотреть два смежных класса
- $(V_A + 00) = \{00, 10\}, \text{ Cymma: } y_{as} + y_{ss} = 1 + 0 = 1$ $\mathbf{H}(V_A + \mathbf{01}) = \{\mathbf{01}, \mathbf{11}\}, \text{ cymma: } y_{\mathbf{01}} + y_{\mathbf{11}} = 1 + 0 = 1$ Итого: и 4 − и 11 − 1
- 1. именно так, поскольку 1100 вектор значений, который мы сейчас распаковываем обратно в таблицу истинности. В индексе при y находится вектор значений переменных, а его (y) значение — значение функции при
- 2. по одному на каждый вектор из $V_{ar{A}}$

Код Рида-Маллера

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

Положим $y_{00} = 1, y_{01} = 1, y_{10} = 0, y_{11} = 0$ Здесь m=2, значит $A\subseteq \{1,2\}$. Причём r=1, т.е. $|A|\leq 1$.

Шаг 2/3: $t = 1, A = \{2\}$

 \blacksquare Здесь $V_{\Lambda} = \{00, 01\}, V_{\bar{\Lambda}} = \{00, 10\}.$ Нужно рассмотреть два смежных класса.

$$ullet$$
 $(V_A + 00) = \{00, 01\}$, cymma: $y_{00} + y_{01} = 1 + 1 = 0$

$$\bullet \ (V_A + \mathbf{10}) = \{\mathbf{10}, \mathbf{11}\}, \ \mathsf{суммa} \colon y_{\mathbf{10}} + y_{\mathbf{11}} = 0 + 0 = 0$$

■ Итого:
$$u_A = u_{\{2\}} = 0$$



◆□▶◆□▶◆□▶◆□▶ □ 夕久○



■ Итого: $u_A = u_{col} = 0$

- 1. именно так, поскольку 1100 вектор значений, который мы сейчас распаковываем обратно в таблицу истинности. В индексе при y находится вектор значений переменных, а его (y) значение — значение функции при этих аргументах.
- 2. по одному на каждый вектор из $V_{ar{A}}$



Код Рида-Маллера

дировани

Конструкция
Плоткина
Минимальное
расстояние

Декодирование
Пара слов о синдромах

Домашнее задание

источн

Ранее: 101 кодируется как 1100 при помощи $\mathrm{RM}(1,2)$ Положим $y_{\mathrm{PR}}=1,y_{\mathrm{PR}}=1,y_{\mathrm{TR}}=0,y_{\mathrm{TR}}=0$

Здесь m=2, значит $A\subseteq\{1,2\}$. Причём r=1, т.е. $|A|\le 1$.

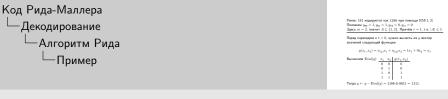
Перед переходом к t=0, нужно вычесть из y вектор значений следующей функции:

$$g(x_1,x_2)=u_{\{1\}}x_1+u_{\{2\}}x_2=1x_1+0x_2=x_1$$

Вычислим
$$\mathrm{Eval}(g)$$
: $\begin{array}{c|ccc} x_1 & x_2 & g(x_1,x_2) \\ \hline 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \\ \end{array}$

Тогда $y \leftarrow y - \text{Eval}(g) = 1100 \oplus 0011 = 1111.$





- 1. именно так, поскольку 1100 вектор значений, который мы сейчас распаковываем обратно в таблицу истинности. В индексе при y находится вектор значений переменных, а его (y) значение значение функции при этих аргументах.
- 2. Здесь мы берём все u, полученные при t=1, домножаем каждую на соответствущие ей x-ы и получаем функцию от m переменных.
- 3. Очень важно, чтобы у вас во всех таблицах истинности (в т.ч. той, которая использовалась при кодировании для получения y) был одинаковый порядок строк. Иначе чуда не выйдет.
- 4. Полезно заметить, что в \mathbb{F}_2 сложение и вычитание одно и то же.

Продолжение примера: t=0

Код Рида-Маллера

$$g_{00} = 1, g_{01} = 1, g_{10} = 1, g_{1$$

Шаг 3/3: $t = 0, A = \emptyset$

Теперь $y_{00} = 1, y_{01} = 1, y_{10} = 1, y_{11} = 1$

$$lacktriangle$$
 Здесь $V_A=\{00\}$, но $V_{ar{A}}=\{00,01,10,11\}.$ Нужно рассмотреть **четыре** смежных класса.

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

$$ullet$$
 $(V_A + 00) = \{00\}$, сумма: $y_{00} = 1$

$$(V_A + 01) = \{01\}$$
, cymma: $y_{01} = 1$

$$(V_A + 10) = \{10\}, \text{ сумма: } y_{10} = 1$$

$$\blacksquare \ (V_A + {\bf 11}) = \{{\bf 11}\} \text{, cymma: } y_{\bf 11} = 1$$

■ Итого:
$$u_A = u_\varnothing = 1$$

```
Код Рида-Маллера
   -Декодирование
     Алгоритм Рида
      \squareПродолжение примера: t=0
```

Теперь $y_{00} = 1, y_{01} = 1, y_{10} = 1, y_{11} = 1$ Шаг 3/3: t = 0, A = ∅

■ Здесь $V_A = \{00\}$, но $V_A = \{00,01,10,11\}$. Нужно рассмотреть четыре смежных класса.

 $(V_A + 00) = \{00\}, \text{ cymma: } y_{an} = 1$ $(V_A + 01) = \{01\}, \text{ cymma: } y_{01} = 1$

 $(V_A + 10) = \{10\}, \text{ cymma: } y_{10} = 1$

 $(V_A + 11) = \{11\}, \text{ cymma: } y_{11} = 1$

Продолжение примера: t=0

Код Рида-Маллера

Теперь
$$y_{00} = 1, y_{01} = 1, y_{10} = 1, y_{11} = 1$$

Кодировани

Конструкция Плоткина

Декодирова

Получили $u_{\{1\}}=1, u_{\{2\}}=0, u_{\varnothing}=1.$

Это значит, что исходный многочлен был таков:

$$f(x_1,x_2) = u_{\{1\}}x_1 + u_{\{2\}}x_2 + u_{\varnothing} = \frac{\mathbf{x_1}+\mathbf{1}}{},$$

а исходное сообщение: 101, как и ожидалось.

Время работы

Утверждается, что время работы алгоритма — $O(n \log^r n)$, где $n = 2^m$ — длина кода.

2022-02-14

Теперь $y_{00} = 1, y_{01} = 1, y_{10} = 1, y_{11} = 1$

Получили $u_{(1)} = 1, u_{(2)} = 0, u_{o} = 1.$ Это аначит, что исходный многочлен был таков: $f(x_1, x_2) = u_{(1)}x_1 + u_{(2)}x_2 + u_{o} = x_1 + 1,$

> а исходное сообщение: 181, как и ожидалось Всемя работы

Время работы

Утверждается, что время работы алгоритма — $O(n \cdot rae \cdot n - 2^m - ann + a \cdot rae \cdot n)$



Код Рида-Маллера

Источники

Домашнее задание

Вариант 1

- Закодировать сообщение: 1001.
- **2** Декодировать код, если ошибок нет: 1010, использовался $\mathrm{RM}(1,2)$.
- **3** Декодировать код, полученный с ошибками: 1101 1010, использовался $\mathrm{RM}(1,3)$

Вариант 2

- 20/08/4908071 0006/400400 0101
- Закодировать сообщение: 0101.

использовался RM(1,3)

- **2** Декодировать код, если ошибок нет: 0110, использовался $\mathrm{RM}(1,2)$.
- З Декодировать код, полученный с ошибками: 1111 0100,

000

71 — Домашнее задание

Код Рида-Маллера

└─Домашнее задание

напишите его и своё имя.

использовался RM(1, 2).

■ Деходировать под, полученный с ошибками использовался RM(1, 3)

Вариант 2

■ Заходировать сообщение: 6101.

■ Деходировать сообщение: 6101.

использовался $\mathrm{RM}(1,2)$.

Деходировать код, полученный с ошибками: 1111 0100 использовался $\mathrm{RM}(1,3)$

1. Замечание: каких-либо требований на методы решения нет, но если используете код — приложите его. Различных способов решить существует больше одного. Номер варианта можете определять как $1+((5n+98) \bmod 2)$, но главное



Код Рида-Маллера

Кодирован

Конструкция Плоткина Минимально

Декодиров

Пара слов о синдромах

Авгоритм Рипа

Домашнее

Источниі

1 https://arxiv.org/pdf/2002.03317.pdf — великолепный обзор, очень рекомендую.

- 2 http://dha.spb.ru/PDF/ReedMullerExamples.pdf очень хорошо и подробно, но используется подход через матрицы, а не через полиномы, а это не весело.
- https://en.wikipedia.org/wiki/Reed-Muller_code кратко, чётко, понятно, но не описано декодирование.
- 4 https://ru.bmstu.wiki/Коды_Рида-Маллера в целом всё есть, но написано очень непонятно;



Код Рида-Маллера —Источники

- http://arxiv.org/pdf/2002.03317.pdf великолепный обхор, очень рекомендую.
 http://dha.upb.ru/F00/ReedMulterExamples.pdf очень рекомендую и предоставления пре
- http://dwa.spb.ru/F09/RecedWulterTxamples.pdf о хорошо и подробно, но используется подход через матрицы, а не через поличномы, а это не восило.
 https://en.wikipedia.org/wiki/Reced-Maller_code —
- кратко, чётко, понятно, но не описано декодирования

 https://ru.bmstu.wiki/Кори_Риде-Маллера в целом
 всё есть, но написано очень непонятно;