

Код Рида-Маллера

Введени

Свойства к

Плоткина Минимально пасстояние

Леколированы

Пара слов о синдромах

Пример

Источники

Код Рида-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

15 февраля 2022 г.

Код Рида-Маллера

2022-02-15



- 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). Слайды с особенным фоном — не вошедшие в маленькую презентацию. 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

1 Введение

2 Кодирование

3 Свойства кода

■ Конструкция Плоткина

■ Минимальное расстояние

Параметры

4 Декодирование

■ Пара слов о синдромах

■ Алгоритм Рида

Пример

5 Домашнее задание

Источники

Код Рида-Маллера

2022-02-15

Содержание

Минимальное расстояние Декодирование
 Вара стое о синдрома Алгориты Рида • Пример В Домашнее задание 6 Источники

Свойства кода Конструкция Плоткина

Параметры

<ロ>
(日)
(日)

Введение

оведение

Рида-Маллера

ведени

войства ко

Конструкция

Плоткина Минимально расстояние

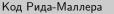
Декодирован
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

Источни

Код описан Дэвидом Маллером (автор идеи) и Ирвингом Ридом (автор метода декодирования) в сентябре 1954 года. Обозначается 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{F}_2 . Соглашение: сложение векторов $u,v\in\mathbb{F}_2^n$ будем обозначать как $u\oplus v=(u_1+v_1,u_2+v_2,...,u_n+v_n)$.

◆ロト 4 個ト 4 国 ト 4 国 ト 日 ・ 9 Q P | 1 日 ・ 1 日



22-02-15

-Введение

Код описан Двеидом Маллером (автор идеи) и Ирвингом Ридом (автор метода двеодирования) в свитября 1954 года Обозвачается жк RMIr, глу, граг г — рава, а 2^m — длина кода. Кодируют сообщения длиной $k = \sum_{i=0}^r C_{in}^2$ при повеоци 2^m бит. Традиционом, считается что коды бинарные и работают жад

традиционно, счатается что жоры овизарные и разотают нау битами, $v_n \in \mathbb{F}_2^n$ 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

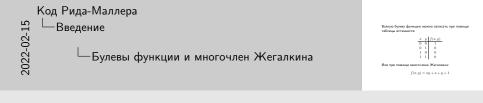
Введение

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

Или при помощи многочлена Жегалкина:

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



Многочлены Жегалкина

Например, для m=2:

функции.

В общем случае, многочлены будут иметь следующий вид:

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

 $f(x_1, x_2) = c_3 \cdot x_1 x_2 + c_2 \cdot x_2 + c_1 \cdot x_1 + c_0 \cdot 1$

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

Код Рида-Маллера

Введение

2

Свойства код Конструкция

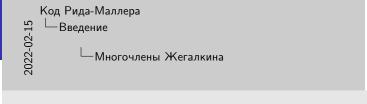
Плоткина Минимальное расстояние

Декодировани Пара слов о синдромах Алгоритм Рида Пример

Домашнее задание

1сточники

4 ロ ト 4 何 ト 4 喜 ト 4 喜 ト 喜 - 夕 Q (^



В общем случае, многочлены будут иметь следующий вг $f(x_1,x_2,...,x_m) = \sum_{S\subseteq \{1,..m\}} c_S \prod_{i\in S} x_i$

Например, $a_n s m = 2$: $f(x_1, x_2) = c_3 \cdot x_1 x_2 + c_2 \cdot x_2 + c_1 \cdot x_1 + c_0 \cdot 1$ Воего $n = 2^m$ козффициентов для описания каждой функции.



Функции небольшой степени

Код Рида-Маллера

Введение

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?

$$k = C_m^0 + C_m^1 + C_m^2 + \ldots + C_m^r = \sum_{i=0}^r C_m^i$$

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

Код Рида-Маллера

-Функции небольшой степени

 $k = C_m^0 + C_m^1 + C_m^2 + ... + C_m^r = \sum_i C_m^i$

- 1. Замечу, что при $S=\varnothing$, 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{F}_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 вплоть до r (не не больше, ведь $\deg f \leq r$).



Идея кодирования

Код Рида-Маллера

...

Кодирование

Свойства код

Плоткина Минимально расстояние

Цекодирова
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

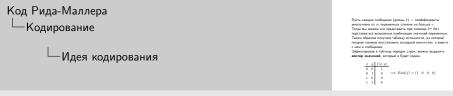
Источник

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 значений 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.

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





- 1. Их 2^m , поскольку рассматриваем многочлены только над \mathbb{F}_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.



Пример

Код Рида-Маллера

..

Кодирование

Свойства к

Конструкция Плоткина

Минимально расстояние Параметры

Декодирован
Пара слов о
синдромах
Алгоритм Рида
Пример

Домашнее задание

Источникі

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

■ Тогда наш многочлен: $f(x_1, x_2) = c_2x_2 + c_1x_1 + c_0$.

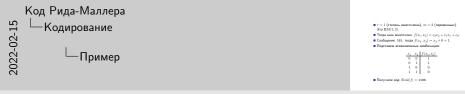
 \blacksquare Сообщение: 101, тогда $f(x_1, x_2) = x_2 + 0 + 1$.

■ Подставим всевозможные комбинации:

x_1	x_2	$\ \left \ f(x_1,x_2)\right $
0	0	1
0	1	1
1	0	0
1	1	0

■ Получили код: $\mathrm{Eval}(f) = 1100$.





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

Кодирование

. . .

Конструкция

Плоткина Минимальное расстояние

Декодирован

Пара слов о синдромах Алгоритм Рида Пример

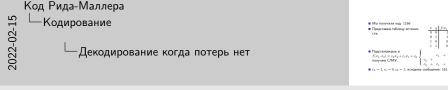
Домашнее задание

1сточник

- Мы получили код: 1100
- Представим таблицу истинности.

$$\begin{array}{c|cccc} x & y & f(x_1, y_2) \\ \hline 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ \end{array}$$

- Подстановками в $f(x_1,x_2)=c_2x_2+c_1x_1+c_0 \ \begin{cases} &c_0=1\\ &c_1+c_0=1\\ c_2+&c_0=0\\ c_2+c_1+c_0=0 \end{cases}$
- $\mathbf{c}_2 = 1, c_1 = 0, c_0 = 1$, исходное сообщение: 101.



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

Коды 0-го порядка

Код

Рида-Маллера

Кодирование

Свойства ко

Конструкция Плоткина Минимальное

Минимальное расстояние Параметры

Декодирован Пара слов о синдромах Алгоритм Рида Пример

Домашнее задание

Источні

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

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

Таблица истинности:

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

Вывод: это 2^m -кратное повторение символа

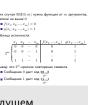
- Сообщение 0 даст код $\underbrace{00...0}_{2^m}$
- Сообщение 1 даст код $\underbrace{11...1}^{2^m}$

— Кодирование

Коды 0-го порядка

Отдельно стоит рассмотреть вариант кода при

Код Рида-Маллера



- 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.



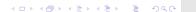
Коды m-го порядка

Рида-Маллера

Кодирование

Есть m переменных, и мы рассматриваем многочлены $f \in \mathbb{F}_2[x_1, ..., x_m] : \deg f \le m$, 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 кода r, тем больше избыточность.





м меньше порядок кода т, тем больше избыточности

Есть ещё один тривиальный случай, когда m=r.

Рида-Маллера

Свойства кода

Доказательство линейности

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

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

где $p_x(a_i)$ — соответствующий сообщению x многочлен. Причём p_x берёт в качестве своих коэффициентов биты из x.

Для этого необходимо немного формализовать всё описанное раньше.

Код Рида-Маллера

Свойства кода

1, x, y, z, xy, yz, xz (для трёх переменных, степени не выше 2).

3. Напомню, что базис пространства многочленов выглядит примерно так:

в качестве переменных и таким образом получаем вектор значений (длины 2^m). Именно он и называется кодом.

2. Пояснение: перебираем все векторы a_i (2^m штук), подставляем каждый в p_x

-Доказательство линейности

образуют линейное пространство, и у нас есть изоморфизм из пространства сообщений (\mathbb{F}_2^k) в пространство слов (\mathbb{F}_2^m).

i произвольное, то и весь вектор получился равен. Таким образом, этот код

действительно линейный и к нему применимы уже известные теоремы!

1. Хотим показать, что этот код является линейным, т.е. что его кодовые слова

Пусть C(x) нодирует сообщение $x \in \mathbb{F}_2^k$ в нод $C(x) \in \mathbb{F}_2^m$ $C(x) = (p_x(a_i) \mid a_i \in \mathbb{F}_2^m)$

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

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.

◆ロト→同ト→三ト ● りへ○

4. Здесь я использую запись $C(x)_i$ для i-го элемента вектора C(x). Поскольку

 $p_{(x \oplus y)} = p_x + p_y$. 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

такое преобразование будет изоморфизмом. Именно поэтому

сообщения и умножаем его на соответствующий базисный вектор. Очевидно,

операция сложения побитовая.

Чтобы преобразовать сообщение в многочлен, мы берём каждый бит



Последствия линейности

Код Рида-Маллера

Введение

...

Свойства кода

Плоткина Минимальное расстояние

Декодировани
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

Источники

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

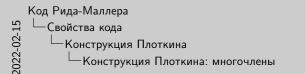
Введени

Хотим понять как выглядят кодовые слова.

- Код вектор значений 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 $\deg h \leq r-1.$







 \mathbf{z} Код — вектор значений функции $f(x_1,...,x_m) \in \mathrm{RM}(r,m)$, причём $\deg f \leq 1$

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

Рида-Маллера

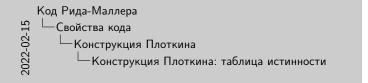
Panee: $f(x_1,...,x_m) = g(x_2,...,x_m) + x_1h(x_2,...,x_m)$.

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





- Passes: $f(x_1, ..., x_m) = g(x_2, ..., x_m) + x_1h(x_2, ..., x_m)$.
 - $val(f) = (Eval(g) \mid Eval(g) \oplus Eval(h)).$
- \blacksquare Причём $\operatorname{Eval}^{[\omega_1=0]}(f) = \operatorname{Eval}(g)$, а $\operatorname{Eval}^{[\omega_1=0]}(f) \oplus \operatorname{Eval}^{[\omega_1=1]}(f) = \operatorname{Eval}(h)$.
- 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: Eval(f) таблица для всей функции (вектор значений, если точнее), $\mathrm{Eval}^{[x_1=0]}(f)$ — кусок таблицы при $x_1=0$, $\mathrm{Eval}^{[x_1=1]}(f)$ 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 $\mathrm{Eval}(q)$, то останется только $\mathrm{Eval}(h)$ (поскольку 1+1=0 в \mathbb{F}_2) получили второе равенство.
- 4. Палочка по центру конкатенация векторов.



Конструкция Плоткина: вывод

Код Рида-Маллера

... ...

одировани

Конструкция Плоткина

Декодирован
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

Источн

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

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

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

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

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

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





- 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

Введени

...

Своиства код

Плоткина Минимальное

Декодирован

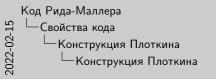
Пара слов о синдромах Алгоритм Рида

Домашне залание

Асточники

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 $c=(u\mid u+v).$





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



Минимальное расстояние

Код 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.

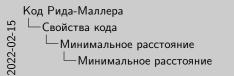
Очевидно,
$$w(\underbrace{11...1}_{2m}) = 2^m = 2^{m-0} \ge 2^{m-r}$$
.

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

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

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





 $d = \min_{v \in C, v \neq 0} s(c)$. Прадположим, что $d = 2^{m-v}$ и досмамем по видущим. Базах: RAI(0, m) — адмистичным бит повторім 2^m ра Очевидно, $s(11, 1) = 2^m = 2^{m-0} \ge 2^{m-v}$. Гипотекаж Если $v \in RM(r-1, m-1)$, то $s(v) \ge 2^{m-v}$. Наят: Хотим доказать, для $c \in RM(r, m)$.

 $w(c) \stackrel{(1)}{=} w((u \mid u \oplus v)) \stackrel{(2)}{=} w(u) + w(u \oplus v) \ge$ $\ge w(u) + (w(v) - w(u)) = w(v) \stackrel{IH}{\ge} 2^{pu-r} \blacksquare$

- 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 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.

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

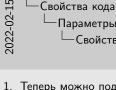
Рида-Маллера

Параметры

Для бинарного кода 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 RM(m-r-1,m)

◆□▶◆□▶◆□▶◆□▶ □ 夕久○



Код Рида-Маллера

Свойства кода

Для бинарного кода RM(r, m): B + < 100

ш Длина сообщения: $k = \sum_{i=1}^{r} C_{ii}^{i}$

1. Теперь можно подвести итоги исследования свойств.

-Свойства и параметры

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. Однако доказательство можно найти в «Reed-Muller Codes: Theory and Algorithms», раздел Duality.



Как линейный код

Код Рида-Маллера

Бведение

Свойства ко

Конструкция

Плоткина Минимально расстояние

Декодирование

Пара слов о синдромах Алгоритм Рида Пример

Домашнее залание

Асточники

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

- Перебор по всему пространству кодовых слов в поисках ближайшего.
- \blacksquare 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

Введение

Свойства ко

Плоткина Минимальное расстояние

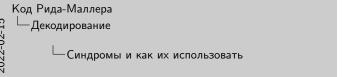
Декодирование
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

Лсточники

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 міс в получанном собіщения г єсть симба в . Тох = v + c, c + v сиде v ходором сидео, отпров країнь летох можно денодировать. Получайтех, что $x = rH^2 (v + L)H^2 = H^2 RH^2 HH^2 ROSAMY VIII = HI ROSAMY VIII = 0 (стът такое скоїство). Мы можны префарта записть ней это и табопку. Тоху, чтобы восстановить и в лично предостановать ней это и табопку. Тоху, чтобы восстановить и становать <math>v$ v -
- 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

Алгоритм Рида

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

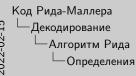
2 Подпространство $V_A\subseteq \mathbb{F}_2^m$, которое обнуляет все v_i , если $i\notin A\colon V_A=\{v\in \mathbb{F}_2^m: v_i=0\ \forall i\notin A\}$

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 $m \in \mathbb{N}$ ■ Подпространство $V_A \subseteq \mathbb{F}_n^2$, которое обкульяет все vсель $i \notin A : V_A = \{v \in \mathbb{F}_n^2 : v_i = 0 \ \forall i \notin A\}$ ■ Аналогично для $V_A : \operatorname{FR}_A = \{1,...,m\} \setminus A$: $V_A = \{v \in \mathbb{F}_n^2 : v_i = 0 \ \forall i \in A\}$ Поммес

- $$\begin{split} & \text{III } \text{ Pyct. } \text{III } = 3, A = \{1, 2\}, \text{ Torgla}... \\ & \text{III } \tilde{y} = \{900, 001, 911, 100, 101, 110, 111\} \\ & \text{III } V_A = \{900, 010, 100, 110\} \left(v_2 = 0 \,\forall v\right) \\ & \text{III } \tilde{A} = \{1, 2, 3\} \, \backslash A = \{3\} \\ & \text{III } V_2 = \{900, 001\} \left(v_1 = v_2 = 0 \,\forall v\right) \end{split}$$
- 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

Введени

Свойства ко

Конструкция Плоткина Минимальное расстояние

Минимальное расстояние Параметры

Декодировані
Пара слов о
синдромах

Алгоритм Рида

Домашне задание

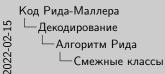
Источники

Если фиксировано $V_A\subseteq \mathbb{F}_2^m$, 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 фиксировано $V_A \subseteq \mathbb{F}_2^n$, то для каждого $b \in \mathbb{F}_2^n$ существует смежний класс $V_A + b$: $(V_A + b) = \{v + b \mid v \in V_A\}$ Утворждается, что если брать, $b \in V_A$

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

Введение

Свойства ко

Конструкция Плоткина Минимальное расстояние

Декодировани
Пара слов о
синдромах

Алгоритм Рида

_{Пример} Домашнее

Источники

Декодирует сообщение u, если использовался $\mathrm{RM}(r,m)$. Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. 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 $\text{for each } b \in V_{\bar{A}}$ $c + = \left(\sum_{z \in (V_A + b)} y_z
ight) mod 2$ (по их не больш $t = 2^{m-r-1} - 1$). (но их не больше, чем $u_A \leftarrow \mathbf{1} [c \ge 2^{m-t-1}]$ $y == \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1,\dots,m\}\\ |A|=t}} u_A \prod_{i \in A} x_i\right)$ 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 пдфке.
- 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 моном $\prod_{i \in A} x_i.$



Рида-Маллера

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. $c \mathrel{+}= \left(\sum_{z \in (V_A + b)} y_z
ight) mod 2$ Hачинаем с t=r. $u_A \leftarrow \mathbf{1} \left[c \ge 2^{m-t-1} \right]$ $y = \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1,\dots,m\} \ |A|=t}} u_A \prod_{i \in A} x_i
ight)$ 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 пдфке.

 \square Алгоритм Рида для кода $\mathrm{RM}(r,m)$

Код Рида-Маллера

–Декодирование —Алгоритм Рида



Код Рида-Маллера

Введение

Колирова

Свойства код

Конструкция Плоткина Минимальное расстояние

Декодировани
Пара слов о
синдромах

Домашнее задание

Лсточники

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 foreach $A \subseteq \{1, ..., m\}$ with |A| = tA, |A| = t и для c = 0foreach $b \in V_{\bar{A}}$ каждого $c += \left(\sum\limits_{z \in (V_A + b)} y_z
ight) mod 2$ восстанавливаем коэффициент u_A при $u_A \leftarrow 1 [c \ge 2^{m-t-1}]$ $x_{A_1} x_{A_2} ... x_{A_t}$ $y == \operatorname{Eval} \left(\sum_{\substack{A \subseteq \{1,\dots,m\} \\ |A|=t}} u_A \prod_{i \in A} x_i \right)$ t -= 1





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 пдфке.



Код Рида-Маллера

Введение

Свойства кол

Конструкция Плоткина Минимальное расстояние

Декодировани
Пара слов о
синдромах

Домашнее задание

Источники

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 $V_{\Lambda} = \{v \in \mathbb{F}_2^m \mid v \in \mathbb{F}_2^m \mid v \in \mathbb{F}_2^m \mid v \in \mathbb{F}_2^m \}$ c = 0foreach $b \in V_{\bar{A}}$ $: v_i = 0 \ \forall i \notin A$ $c \mathrel{+}= \left(\sum_{z \in (V_A + b)} y_z\right) \bmod 2 \qquad \qquad b \in \{v \in \mathbb{F}_2^m \\ : v_i = 0 \ \forall i \in A\}$ $u_A \leftarrow \mathbf{1} \left[c \ge 2^{m-t-1} \right]$ $y = \operatorname{Eval}\left(\sum_{\substack{A \subseteq \{1, ..., m\} \ |A| = t}} u_A \prod_{i \in A} x_i
ight)$ 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 пдфке.

Код Рида-Маллера

Код Рида-Маллера

...

Свойства код

Конструкция Плоткина Минимальное расстояние

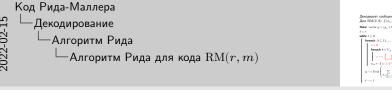
Декодировани
Пара слов о
синдромах
Алгоритм Рида

Домашнее задание

1сточники

```
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.
Data: vector y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m) Считаем количество (c)
                                                       смежных классов, в
t = r
while t > 0
                                                       которых
                                                       \sum y_z = 1 \pmod{2}.
     foreach A \subseteq \{1, ..., m\} with |A| = t
                                                      Пороговое значение
          foreach b \in V_{\bar{A}}
          c + = \left(\sum_{z \in (V_A + b)} y_z
ight) mod 2 половина от числа
         u_A \leftarrow 1 \left[c \geq 2^{m-t-1}\right]
    u_A\leftarrow 1 c\geq 2^{m-i-1} Таким образом, если y-=\mathrm{Eval}\left(\sum\limits_{\substack{A\subseteq\{1,\dots,m\}\|A|=t}}u_A\prod_{i\in A}x_i
ight) Таким образом, если большинство сумм x 1, то x 1, то x 1, иначе
                                                       Таким образом, если
                                                   большинство сумм дало
     t -= 1
```

◆ロ → ← 荷 → ← 三 → → ○ へ ○ ○



- 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 пдфке.
- 2. Если это количество больше порогового значения, то считаем, что $u_A=1$, иначе же $u_A=0$.



Код Рида-Маллера

Введение

Содирование

Конструкция Плоткина Минимальное расстояние

Декодировани
Пара слов о
синдромах

Алгоритм Рида Пример

Домашнее задание

t -= 1

Декодирует сообщение u, если использовался $\mathrm{RM}(r,m)$. Для RM(2,2): $f(x_1,x_2)=u_{1,2}x_1x_2+u_1x_1+u_2x_2+u_4$. 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 найденное while t > 0на этой итерации, после foreach $A \subseteq \{1, ..., m\}$ with |A| = tчего переходим к c = 0мономам меньшей foreach $b \in V_{\bar{A}}$ $c \mathrel{+}= \left(\sum\limits_{z\in (V_A+b)} y_z
ight) mod 2$ 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@

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 пдфке.

Пример

Код Рида-Маллера

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

Введени

Кодировані

Свойства код

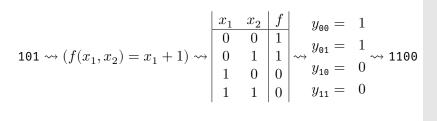
Конструкция Плоткина Минимальное

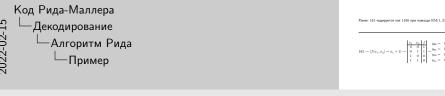
Декодировани

Пара слов о синдромах Алгоритм Рида Пример

Домашнее задание

Асточники



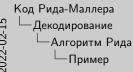


Как происходит кодирование, схематически:

Ранее: 101 кодируется как 1100 при помощи 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
$$1/3$$
: $t = 1, A = \{1\}$

- lacktriangle Здесь $V_A = \{00, 10\}$, $V_{\bar{A}} = \{00, 01\}$. 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: $u_A = u_{\{1\}} = 1$



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

Шаг 1/3: t = 1. $A = {1}$ ■ Здесь $V_A = \{00, 10\}, V_{\bar{A}} = \{00, 01\}.$

- Нужно рассмотреть два смежных класса
- $(V_A + 00) = \{00, 10\}, \text{ Cymma: } y_{aa} + y_{aa} = 1 + 0 = 1$ $\mathbf{H}(V_A + \mathbf{01}) = \{\mathbf{01}, \mathbf{11}\}, \text{ cymma: } y_{\mathbf{01}} + y_{\mathbf{11}} = 1 + 0 = 1$ Итого: и 4 − и 11 − 1

- 1. Теперь начинаем декодирование.
- 2. по одному на каждый вектор из $V_{ar{A}}$

Пример

Код Рида-Маллера

введение

Кодирован

Свойства ко

Конструкция
Плоткина
Минимальное
расстояние

Декодирован
Пара слов о
синдромах
Алгоритм Рида
Пример

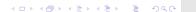
Домашнее задание

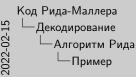
Лсточники

Ранее: 101 кодируется как 1100 при помощи $\mathrm{RM}(1,2)$ 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. $|A|\le 1$.

Шаг
$$2/3$$
: $t = 1, A = \{2\}$

- lacktriangle Здесь $V_A=\{{\tt 00,01}\},\ V_{ar A}=\{{\tt 00,10}\}.$ Нужно рассмотреть два смежных класса
- $(V_A + 00) = \{00, 01\}, \text{ cymma: } y_{00} + y_{01} = 1 + 1 = 0$
- $(V_A + 10) = \{10, 11\}, \text{ сумма: } y_{10} + y_{11} = 0 + 0 = 0$
- Итого: $u_A = u_{\{2\}} = 0$





Ранее: 101 кодируется как 1100 при повлощи $\mathrm{RM}(1,2)$ Положим $y_{\mathrm{lin}}=1, y_{\mathrm{lin}}=1, y_{\mathrm{lin}}=0, y_{\mathrm{lin}}=0$ Здесь m=2, заячит $A\subseteq\{1,2\}$. Причём r=1, τ .e. $|A|\le 1$

Har 2/3: $t = 1, A = \{2\}$

- **в** Здесь $V_A = \{00,01\}, V_{\bar{A}} = \{00,10\}.$ Нужно рассмотреть два смежных класса
- \mathbf{H} $(V_A + 00) = \{00, 01\}$, cymma: $y_{00} + y_{01} = 1 + 1 = 0$ \mathbf{H} $(V_A + 10) = \{10, 11\}$, cymma: $y_{10} + y_{11} = 0 + 0 = 0$ \mathbf{H} foro: $u_A = u_{20} = 0$

1. — по одному на каждый вектор из $V_{ar{arLeta}}.$



Пример

Код Рида-Маллера

ORMBORSE

одирован

Конструкция
Плоткина
Минимальное

Декодирова Пара слов о синдромах Алгоритм Рида Пример

Домашнее задание

Источ

Ранее: 101 кодируется как 1100 при помощи $\mathrm{RM}(1,2)$ 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. $|A|\le 1$.

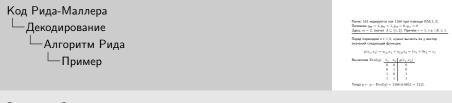
Перед переходом к t=0, нужно вычесть из y вектор значений следующей функции:

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

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

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

4□ > 4♠ > 4 = > 4 = > 9 < 0</p>



- 1. Здесь мы берём все u, полученные при t=1, домножаем каждую на соответствущие ей x-ы и получаем функцию от m переменных.
- 2. 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.
- 3. Полезно заметить, что в \mathbb{F}_2 сложение и вычитание одно и то же.

Продолжение примера: t=0

Код Рида-Маллера

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

Шаг 3/3: $t = 0, A = \emptyset$

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

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

$$V_A + 00 = \{00\}, \text{ сумма: } y_{00} = 1$$

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

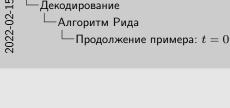
$$(V_A + 10) = \{10\}, \text{ сумма: } y_{10} = 1$$

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

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

■ Итого:
$$u_A = u_\varnothing = 1$$

Пример



Код Рида-Маллера

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

Рида-Маллера

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

Пример

Получили $u_{\{1\}} = 1, u_{\{2\}} = 0, u_{\emptyset} = 1.$ Это значит, что исходный многочлен был таков:

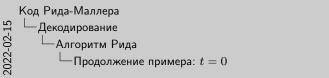
$$f(x_1, x_2) = u_{\{1\}}x_1 + u_{\{2\}}x_2 + u_{\varnothing} = \frac{\mathbf{x}_1 + \mathbf{1}}{\mathbf{1}},$$

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.

◆□▶◆□▶◆□▶◆□▶ □ 夕久○



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

Получили $u_{(1)} = 1$, $u_{(2)} = 0$, $u_{m} = 1$. Это значит, что исходный многочлен был такое $f(x_1,x_2)=u_{\{1\}}x_1+u_{\{2\}}x_2+u_{o}={\color{red}x_1+1},$

а исходное сообщение: 101, как и ожидалось

где п - 244 - длина кода,



Код Рида-Маллера

Домашнее задание

Домашнее задание

Вариант 1

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

Вариант 2

- Закодировать сообщение: 0101. 2 Декодировать код, если ошибок нет: 0110,
- использовался RM(1,2). 3 Декодировать код, полученный с ошибками: 1111 0100,

использовался RM(1,3)◆□▶◆□▶◆□▶◆□▶ □ 夕久○

Домашнее задание cnon-sceance RM(1, 3) Домашнее задание Закодировать сообщение: 0101 Поколиповать кол ости опибок нат- 8118 Декодировать код, полученный с ошибками: 1111 0100 1. Замечание: каких-либо требований на методы решения нет, но если

Вариант 2

Код Рида-Маллера

используете код — приложите его. Различных способов решить существует больше одного. Номер варианта можете определять как $1 + ((5n + 98) \mod 2)$, но главное напишите его и своё имя.



Источники

Код Рида-Маллера

вание

. Войства к

Конструкция

Минимально расстояние

Пара слов о синдромах

Домашнее задание

Источники

- 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.
- 3 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;





обзор, очень рекомендую.

■ http://dha.spb.ru/PDF/ReedMullerExamples.pdf — очень хорошо и подробно, но используются подход через

■ https://arxiv.org/pdf/2002.03317.pdf — великолепный

- mttp://ena.spb.ru/vos/keedmulcerixamples.pdr охорошо и подробно, но используется подход через матрицы, а не через полиномы, а это не весело. http://en.wikisedia.org/wiki/Rerd-Muller code —
- кратио, чётко, поняжню, но не описано декодирование

 https://ru.bmswiki/Kopw_Рида-Маллера в целом
 вой есть, но написано очень непонятно;