

Код Рида-Маллера

Введение

Свойства

параметрі кода

Плоткина Минимально расстояние

Декодиров ние

Пара слов о синдромах Алгоритм Рида

задание

1сточники

Код Рида-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

13 февраля 2022 г.



Код Рида-Маллера

2022-02-13



1. Если вы смотрите презентацию, то на сером фоне справа иногда 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 (а в внешних полях видны заголовки слайдов). 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.

По любым вопросам: ReedMuller@sldr.xyz или t.me/iliago или vk.com/iliago.

Введение

помощи 2^m бит.

над битами, т.е. \mathbb{Z}_2 .

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

Традиционно, считается что коды бинарные и работают

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

Соглашение: сложение векторов $u,v\in\mathbb{Z}_2^n$ будем обозначать

Код Рида-Маллера

Введение

Свойства і параметрь

кода Конструкция Плоткина

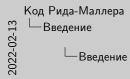
Плоткина Минимальное расстояние

ние
Пара слов о
синдромах
Алгоритм Рида

Домашне задание

Источник





Описан Двиядом Маллером (автор идеи) и Ирвингом Ридом (автор вытора двиодирования) в сентябре 1954 года Обсывачалого как RMI(r, m), rge r — ране, a 2^m — дянна хода. Кодирует сообщения динной $k=\sum_{i=0}^r C_{in}^i$ при повесци 2^m бит.

Традиционно, считается что ходы бинарные и работают над битами, т.е. \mathbb{Z}_2 . Сомание векторов $u,v\in\mathbb{Z}_2^n$ 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

Введение

Свойства і параметрь

кода Конструкция Плоткина Минимальное

. Декодирование

Пара слов о синдромах Алгоритм Рида

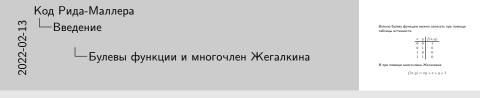
домашнеє задание Всякую булеву функцию можно записать при помощи таблицы истинности

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

И при помощи многочлена Жегалкина:

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





Многочлены Жегалкина

Например, для m=2:

функции.

В общем случае, многочлены будут иметь следующий вид:

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

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

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

Код Рида-Маллера

Введение

Кодиров

войства араметрі ола

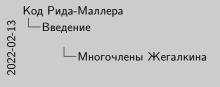
ода Конструкция Плоткина Минимальное

Декодирование Пара слов о синдромах

Алгоритм Ри **Домашне**

адание Істочники





В общем случае, много-члены будут иметь следующий ви, $f(x_1,x_2,...,x_m) = \sum_{S\subseteq \{1,...m\}} c_S \prod_{i\in S} x_i$ Напомиес. для m=2:

Напривер, для m=2: $f(x_1,x_2)=c_1\cdot x_1z_2+c_2\cdot x_1+c_3\cdot x_2+c_4\cdot 1$ Всего $n=2^{ns}$ коэффициентов 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 r переменных.

Сколько тогда всего коэффициентов используется?

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

)-Z0Z 1. Код Рида-Маллера
—Введение
—Функции небольшой степени

Paccustypas dynaujus, citatina, sacro-cisacia acropais fostinas $\tau: \{f(x_1,x_2,\dots x_n) \mid \deg f \leq \tau\}$ Karagyos sacrosa samentas. Calagyosus displacas. $f(x_1,x_2,\dots x_n) = \sum_{G_i \in G_i} \log \frac{1}{|G_i|} E_G$ B assigned proparagianeas architecture of social arrappearagianeas architecture of social arrappearagianeas architecture architecture of social arrappearagianeas. Contacts torqui accross consideration architecture of the social arrappearagianeas architecture architecture of the social architecture of the

- 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{Z}_2 , здесь нету x^2,y^2,z^2 , т.к. $a^2=a$). 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

...

Кодирование

Свойства і іараметрь кола

Конструкция Плоткина Минимальное

екодиров: ие

Пара слов о синдромах Алгоритм Рида

домашн задание

Істочники

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.





- абото очимо и то подпечатать при посещи зг бит, тогу из за зоним ието придставить при посещи зг бит, подставия его возможным сооблюдии переменных. Тими образом опоучем забаму истичести, из которой подцен сакомых восстановить которынай многочлен, а макете с чим и сообщение. Забичисировая в таблици порядок строк, ченное выделеты выетом замений, котором битам маком.
- 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.

Пример

Код Рида-Маллера

.,

Кодирование

Свойства параметр кола

> Конструкция Плоткина Минимальное расстояние

Декодирова ние Пара слов о

. Домашне

1сточники

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

- 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: $\mathrm{Eval}(f) = 1100$.





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

Мы получили код: 1100

■ Представим таблицу

Код Рида-Маллера

Кодирование

истинности.

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

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

- 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.

-Декодирование когда потерь нет продолжение предыдущего.

Код Рида-Маллера

-Кодирование



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



Код

Рида-Маллера

Коды 0-го порядка

Кодирование

зойства и граметры

кода Конструкция Плоткина

Плоткина Минимальное расстояние

Пара слов о синдромах Алгоритм Рида

Домашн задание

задание Источники

сточники

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 <u>0</u>0...0
- Сообщение 1 даст код $\underbrace{11...1}_{2^m}$

Код Рида-Маллера

Кодирование

Кодирование

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 с значениями никак не зависят от аргументов функций. Получается две колонки одна с нулями, другая с единицами.

Доказательство линейности

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

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

x. Поскольку многочлены степени не выше r образуют

линейное пространство, то $p_{(x \oplus y)} = p_x + p_y$.

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

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

Причём p_{x} берёт в качестве своих коэффициентов биты из

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

◆□▶◆□▶◆□▶◆□▶ □ 夕久○

Код Рида-Маллера

Свойства и параметры кода

-Доказательство линейности

сообщений (\mathbb{Z}_2^k) в пространство слов (\mathbb{Z}_2^m).

(длины 2^m). Именно он и называется кодом.

операция сложения побитовая.

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

Для этого необходимо немного формализовать всё описанное раньше.

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

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

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!

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

такое преобразование будет изоморфизмом. Именно поэтому

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

пинейное 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.

Рида-Маллера

кода

Свойства и

параметры

Тогда:



Последствия линейности

Код Рида-Маллера

Введение

Свойства и

параметры кода Конструкция

Конструкция Плоткина Минимальное расстояние

ние

синдромах Алгоритм Рида _

задание

1 Существует порождающая матрица G.

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

2 Минимальное растояние 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

Введение

Свойства параметр

> Конструкция Плоткина Минимально

Декодирова ние

Пара слов о синдромах Алгоритм Рида

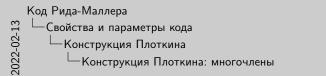
----задание

Істочники

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 $\deg h \leq r-1.$





- \mathbf{E} Код таблица истинности фун $f(x_1,...,x_m) \in \text{RM}(r,m)$, причёк
- В Разделим функцию по x_1 : $f(x_1,...,x_m) = q(x_2,...,x_m) + x_1h(x_2,...,x_m)$
- **B** 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

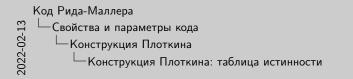
Код Рида-Маллера

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 $x_1=1$.

 $\text{Eval}(f) = \frac{1}{(\text{Eval}^{|\sigma_1|})}$

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

Рида-Маллера

разделить:

Конструкция

 $f(x_1,...,x_m) = g(x_2,...,x_m) + x_1h(x_2,...,x_m)$ Также известно, что $\text{Eval}(f) = (\text{Eval}(q) \mid \text{Eval}(q) \oplus \text{Eval}(h)).$ Заметим, что $\operatorname{Eval}(f)$ – кодовое слово (как и для q, h). Тогда: $c = \text{Eval}(f) \in \text{RM}(r, m)$ (T.K. $\deg f \le r$)

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

 $u = \text{Eval}(q) \in \text{RM}(r, m - 1)$ (т.к. $\deg q \le r$) $v = \text{Eval}(h) \in \text{RM}(r-1, m-1)$ (T.K. $\deg h < r-1$) **Утверждение:** Для всякого кодового слова $c \in \mathrm{RM}(r,m)$ можно найти $u \in RM(r, m-1)$ и $v \in RM(r-1, m-1)$, такие что $c = (u \mid u + v)$. ◆□▶◆□▶◆□▶◆□▶ □ 夕久○ Код Рида-Маллера Свойства и параметры кода

Конструкция Плоткина

—Конструкция Плоткина: вывод

 $\text{Eval}(f) = (\text{Eval}(g) \mid \text{Eval}(g) \oplus \text{Eval}(h)).$ Утверждение: Для всякого корового слова $c \in RM(r, m)$

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

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

- 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 $\deg f \leq r$

матрицы, но мы этим не будем заниматься.

3. Напомню, что RM(r,m) включает в себя все функции (их таблицы истинности, если точнее) от m аргументов и степени не выше r. Очевидно, наши годятся. 4. Что здесь важно отметить — оба наших новых кодовых слова u,vполучились «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



Рида-Маллера

Минимальное расстояние

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 потворён 2^m раз.

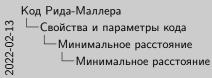
Очевидно,
$$w(\underbrace{11...1}_{2m}) = 2^m = 2^{m-0} \ge 2^{m-r}$$
.

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

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

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





 $d = \min_{c \in C, c \neq 0} w(c)$ Предположим, что $d = 2^{m \cdot v}$ и докажем по индукции База: $\mathrm{RM}(0, m) = a_0 m \cdot c_0 m \cdot c_0$

Байа: Клі $(u, m) = a_0$ инственный бит потворён 2^m ді Очавидно, $w(\underbrace{1, \dots, 1}_{2^m}) = 2^m = 2^{m-2} \ge 2^{m-r}$. Гипотеал: Если $v \in \text{RM}(r-1, m-1)$, то $w(v) \ge 2^{m-r}$ Шаг: Хотим доказать для $c \in \text{RM}(r, m)$. $w(c) = w((u \mid u \oplus v)) \stackrel{(i)}{=} w(u) + w(u \oplus v) >$

 $u(v) - u((u \mid u \uplus v)) - u(u) + u(u \uplus v) \ge$ $\ge w(u) + (w(v) - w(u)) = w(v) \ge 2^{m-r} \blacksquare$

- 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 (соответсвует 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): $w((x\mid y))=w(x)+w(y)$. Вес это всего лишь число ненулевых элементов, поэтому нет разницы как мы будем группировать части вектора. Переход (2): $w(u\oplus v)\geq w(v)-w(u)$. 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

...

Кодирован

Свойства і параметрь кода

Конструкция Плоткина Минимальное расстояние

> lекодироваие

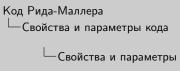
синдромах Алгоритм Рида

домашне задание

1сточники

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 $\mathrm{RM}(m-r-1,m)$





- 1. Теперь можно подвести итоги исследования свойств.
- 2. , поскольку $t=\left\lfloor\frac{d-1}{2}\right\rfloor=\left\lfloor\frac{2^{m-r}}{2}-\frac{1}{2}\right\rfloor=\left\lfloor2^{m-r-1}-0.5\right\rfloor=2^{m-r-1}-1$
- 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

Свойства

параметры кода

Плоткина
Минимальное расстояние

Декодирова-

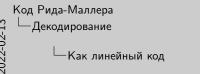
ние
Пара слов о
синдромах
Алгоритм Рид

домашне задание

сточники

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: $s=rH^T$.



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

ближайшего.

в 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 ввиду, но о них было рассказано и без меня, так что я их пропущу.



Синдромы и как их использовать

Код Рида-Маллера

Бведение

Свойства параметры кода

Конструкция Плоткина Минимально расстояние

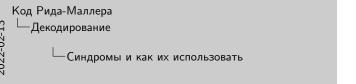
Декодирование
Пара слов о синдромах

Домашнее задание

Істочникі

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 мас в полученном сообщения τ есть ошибка x. τ $t_{\rm TR} v = -$ водовое сповь, которов реадин лега михом денедировать. Получентся, τ $t_{\rm TR} v = H^2$ — t_{\rm

- 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

Пример

Код Рида-Маллера

Введение

Свойства и

кода Конструкция Плоткина Минимальное

Минимальное расстояние Цекодиров

Пара слов о синдромах Алгоритм Рида

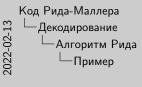
Домашнее задание

Источник

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

$$t = 1$$

$$t = 0$$





- 1. Теперь начинаем нормальный алгоритм декодирования, придуманный Ридом (тем самым). Именно из-за алгоритма декодирования Рида включили в соавторы кода Рида-Маллера.
- 2. (см. самый первый пример).



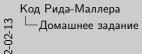
Код Рида-Маллера

TODO

Домашнее



2022-02-13









Код Рида-Маллера

Бведение

Кодирова

Свойства

Конструкция Плоткина Минимально

Декодиров: ние

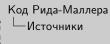
синдромах Алгоритм Ри

Домашне задание

Источники

- I 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;





- Inttps://arxiv.org/pdf/2002.03317.pdf великолепный обзор, очень рекомендую.
 Inttp://dba.spb.ru/700/ReedBultertxamples.pdf очень хорошо и подробно, но используется подход черка матюмы. а не чевой полиномы. В это не всесяло.
- https://en.wikipedia.org/wiki/Reed-Multer_code кратио, чётио, понятио, но не описано декодировании
 https://ru.bmstw.wiki/Кори_Рида-Малиера — в целом вой есть, но написано очень непонятно:
- . Бонусный раздел, который не включён в основную презентацию, но может быть очень полезен.