

[illegible]

Код Риды-Маллера

2022-03-12

Код: Error Message

Blank Document

Word count: 100 words / 100
View all documents >
10 pages / 1000 x

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).

1.3 Текстовая статья со всем содержимым длиной 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/jiliago или vk.com/jiliago.



Факультет

Computer Science

и Математики

Код

Рида-Маллера

Введение

Введение

Кодирование

Свойства кода

Декодирование

Задачи Рида-Маллера

Дополнение

Источники


Введение

Код описан Дэвидом Маллером (автор идеи) и Ирвингом Ридом (автор метода декодирования) в сентябре 1954 года.

Обозначается как $\text{RM}(r, m)$, где r — ранг, а 2^m — длина кода. Кодировует сообщения длиной $k = \sum_{i=0}^r C_m^i$ при помощи 2^m бит.

Традиционно, считается что коды двоичные и работают над битами, т.е. \mathbb{F}_2 .

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



Факультет

Компьютерной

наук

Код

Рада-Маллера

Введение

Кодирование

Свойства кода

Алгоритмы

Универсальное кодирование

Декодирование

Алгоритм Рада-Маллера

Демонстрация кодирования

Источники


Булевы функции и многочлен Жегалкина

Всюкую 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:

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



Faculty of
Computer
Science

Многочлены Жегалкина

Код

Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Линейные

Коды

Систематические

Не систематические

Декодирование

Алгоритм Рид-Солемана

Дополнительная литература


Источники

В общем случае, многочлены будут иметь следующий вид:

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

Например, для $m = 2$: $f(x_1, x_2) = c_{12} \cdot x_{\{1\}} x_2 + c_{\{2\}} \cdot x_2 + c_{\{1\}} \cdot x_1 + c_{\emptyset} \cdot 1$

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



Faculty of Computer Science

Физико-математический факультет

Код

Рига-Маллера

Введение

Кодирование

Свойства кода

Алгоритмы

Задачи

Динамика

Введение

История

Функции небольшой степени

Рассмотрим функции, степень многочленов которых не больше r :

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

Каждую можно записать следующим образом:

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

В каждом произведении используется не больше r переменных.

Сколько тогда всего коэффициентов используется?

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

2022-03-12

Код Риды-Маллера

Введение

Функции небольшой степени

Рид-Маллер, 1954, стр. 100-101

$$f(x,y,z) = x^2y + xy^2 + xz + yz$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

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 $(x + y + z + \dots)$, затем произведения одночленов $(xy + yz + xz + \dots)$ 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 k именно такое: мы складываем все возможные перестановки сначала для 0 переменных, потом для одной, двух, и так вплоть до r (не больше, ведь $\deg f \leq r$).

Faculty of Computer Science

Идея кодирования

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Задачи

Источники

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.

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

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

2022-03-12

Код Риды-Маллера

Кодирование

Идея кодирования

Рид-Маллер, 1954, стр. 100-101

$$f(x,y,z) = x^2y + xy^2 + xz + yz$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

1. Их 2^m , поскольку рассматриваем многочлены только над \mathbb{F}_2 от m переменных.

2. Вектор значений — обозначается $\text{Eval}(f)$ — 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.

Faculty of Computer Science

Пример

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Задачи

Источники

- $r = 1$ (степень многочлена), $m = 2$ (переменных). Это $\text{RM}(1, 2)$.
- Тогда наш многочлен: $f(x_1, x_2) = c_{\{2\}}x_2 + c_{\{1\}}x_1 + c_{\emptyset}$.
- Сообщение: 011, тогда $f(x_1, x_2) = 0 + x_1 + 1$.
- 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: $\text{Eval}(f) = 1100$.

2022-03-12

Код Риды-Маллера

Кодирование

Пример

Рид-Маллер, 1954, стр. 100-101

$$f(x,y,z) = x^2y + xy^2 + xz + yz$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

Вспомогательные функции: $f_1(x,y,z) = x^2y + xy^2$, $f_2(x,y,z) = xz + yz$

$$f(x,y,z) = f_1(x,y,z) + f_2(x,y,z)$$

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

2. Для кодирования очень важно понимать, как именно биты сообщения ставятся в соответствие коэффициентам многочлена. Поэтому давайте введём **соглашение**: если упорядочить элементы множества u каждого коэффициента по возрастанию, то коэффициенты сортируются в лексикографическом порядке: $c_{1,2}$ раньше $c_{1,3}$, поскольку $2 < 3$ и $c_{2,3}$ раньше $c_{3,4}$, поскольку $2 < 3$.

Пример для $m = 4$:

$$f(x_1, x_2, x_3, x_4) = c_{\{1,2,3,4\}}x_1x_2x_3x_4 + c_{\{1,2,3\}}x_1x_2x_3 + c_{\{1,2,4\}}x_1x_2x_4 + c_{\{1,3,4\}}x_1x_3x_4 + c_{\{2,3,4\}}x_2x_3x_4 + c_{\{1,2\}}x_1x_2 + c_{\{1,3\}}x_1x_3 + c_{\{1,4\}}x_1x_4 + c_{\{2,3\}}x_2x_3 + c_{\{2,4\}}x_2x_4 + c_{\{3,4\}}x_3x_4 + c_{\{1\}}x_1 + c_{\{2\}}x_2 + c_{\{3\}}x_3 + c_{\{4\}}x_4 + c_{\emptyset}$$

Также можно кодировать множества при помощи битов, используя отношение $x \in A \Leftrightarrow v_x = 1$ (нумерация битов слева направо, начиная с единицы), где свойство ортогональности сохраняется и хорошо видно (но только в пределах группы мономов одной степени):

$$f(x_1, x_2, x_3, x_4) = c_{1111}x_1x_2x_3x_4 + c_{1110}x_1x_2x_3 + c_{1101}x_1x_2x_4 + c_{1011}x_1x_3x_4 + c_{0111}x_2x_3x_4 + c_{1100}x_1x_2 + c_{1010}x_1x_3 + c_{1001}x_1x_4 + c_{0110}x_2x_3 + c_{0101}x_2x_4 + c_{0011}x_3x_4 + c_{1000}x_1 + c_{0100}x_2 + c_{0010}x_3 + c_{0001}x_4 + c_{0000}$$

Faculty of Computer Science

Декодирование когда потерь нет

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Задачи

Источники

- Мы получили код: 1100
- Представим таблицу истинности.

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

- Подстановками в $f(x_1, x_2) = c_2x_2 + c_1x_1 + c_0$ получим СЛАУ.

$$\begin{cases} c_0 = 1 \\ c_2 + c_0 = 1 \\ c_1 + c_0 = 0 \\ c_1 + c_2 + c_0 = 0 \end{cases}$$

- $c_{\{1\}} = 1, c_{\{2\}} = 0, c_{\emptyset} = 1$, исходное сообщение: 011.

2022-03-12

Код Рида-Маллера

Кодирование

Декодирование когда потеря нет

Мы рассмотрим код

Построение таблиц истинности

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

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

2022-03-12

Код Рида-Маллера

Кодирование

Коды 0-го порядка

Мы рассмотрим код

Построение таблиц истинности

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

1. Отдельно стоит рассмотреть вариант кода при $r = 0$, он нам в будущем пригодится для доказательства.

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.

Faculty Computer Science

Коды 0-го порядка

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Домашнее задание

Источники

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

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

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

Таблица истинности:

2^m

x_1

x_2

\dots

x_m

$f(x_1, \dots, x_m)$

$g(x_1, \dots, x_m)$

0

0

\dots

0

0

0

\dots

1

\vdots

\vdots

\vdots

1

0

0

\dots

1

1

1

\dots

1

Вывод: это 2^m -кратное повторение символа

Сообщение 0 даст код $\underbrace{00\dots0}_{2^m}$

Сообщение 1 даст код $\underbrace{11\dots1}_{2^m}$

Faculty Computer Science

Коды m -го порядка

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Домашнее задание

Источники

Есть m переменных, и мы рассматриваем многочлены $f \in \mathbb{F}_2[x_1, \dots, x_m] : \deg f \leq m$, т.е. все возможные.

Для $RM(m, m)$ 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.

2022-03-12

Код Рида-Маллера

Кодирование

Коды m -го порядка

Мы рассмотрим код

Построение таблиц истинности

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

Решение задачи

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

Faculty Computer Science

Доказательство линейности

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Домашнее задание

Источники

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 . 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.

2022-03-12

Код Рида-Маллера

Свойства кода

Доказательство линейности

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

1. Хотим показать, что этот код является линейным, т.е. что его кодовые слова образуют линейное пространство, и у нас есть изоморфизм из пространства сообщений (\mathbb{F}_2^m) в пространство слов (\mathbb{F}_2^n) .
Для этого необходимо немного формализовать всё описанное раньше.

2. Пояснение: перебираем все векторы a_i (2^m штук), подставляем каждый в p_x в качестве переменных и таким образом получаем вектор значений (длины 2^m). Именно он и называется кодом.

3. Напомним, что базис пространства многочленов выглядит примерно так: $1, x, y, z, xy, yz, xz$ (для трёх переменных, степени не выше 2).
Чтобы преобразовать сообщение в многочлен, мы берём каждый бит сообщения и умножаем его на соответствующий базисный вектор. Очевидно, такое преобразование будет изоморфизмом. Именно поэтому $p(x \oplus y) = p_x + p_y$. 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 операция сложения побитовая.

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!

2022-03-12

Код Рида-Маллера

Свойства кода

Последствия линейности

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

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.

2022-03-12

Код Рида-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: многочлены

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Рида-Маллера

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

1. Порядок очевидно не больше r , потому что это условие для включения в пространство кодов $RM(r, m)$.

2. Теперь у нас есть две функции от меньшего числа аргументов. Очевидно, так можно сделать всегда, когда $m > 1$.

Faculty Computer Science

Последствия линейности

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

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:

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

Faculty Computer Science

Конструкция Плоткина: многочлены

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Хотим понять как выглядят кодовые слова.

■ Код — вектор значений функции $f(x_1, \dots, x_m) \in RM(r, m)$, причём $\deg f \leq r$.

■ Разделим функцию по x_1 : $f(x_1, \dots, x_m) = g(x_2, \dots, x_m) + x_1 h(x_2, \dots, x_m)$.

■ Заметим, что $\deg f \leq r$, а значит $\deg g \leq r$ и $\deg h \leq r-1$.

Faculty Computer Science

Конструкция Плоткина: таблица истинности

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

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

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

$$\text{Eval}(f) = \begin{pmatrix} \text{Eval}^{[x_1=0]}(f) \\ \text{Eval}^{[x_1=1]}(f) \end{pmatrix}$$

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

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

2022-03-12

Код Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

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: $\text{Eval}(f)$ — таблица для всей функции (вектор значений, если точнее). $\text{Eval}^{[x_1=0]}(f)$ — кусок таблицы при $x_1 = 0$, $\text{Eval}^{[x_1=1]}(f)$ — 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 $\text{Eval}^{[x_1=1]}(f)$, то получим $\text{Eval}(g + h)$, но если туда прибавить ещё раз $\text{Eval}(g)$, то останется только $\text{Eval}(h)$ (поскольку $1 + 1 = 0$ в \mathbb{F}_2) — получили второе равенство.

4. Палочка по центру — конкатенация векторов.

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

2022-03-12

Код Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

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 $\text{RM}(r, m)$ включает в себя **все** функции (их таблицы истинности, если точнее) от m аргументов и степени не выше r . Очевидно, наши годятся.

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

2022-03-12

Код Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина

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.

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина

Риды-Маллера

Свойства кода

Конструкция Плоткина

Конструкция Плоткина

Faculty Computer Science

Конструкция Плоткина: вывод

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

Доказательство

Задача

Доказательство

Источники

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

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

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

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

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

Faculty Computer Science

Конструкция Плоткина

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

Доказательство

Задача

Доказательство

Источники

Теорема

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

Faculty Computer Science

Минимальное расстояние

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

Доказательство

Задача

Доказательство

Источники

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

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

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

База: $\text{RM}(0, m)$ — единственный бит повторён 2^m раз. Очевидно, $w(\mathbf{11\dots1}) = 2^m = 2^{m-0} \geq 2^{m-r}$.

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

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

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

2022-03-12

Код Рида-Маллера

Декодирование

Как линейный код

1. Этот способ применим ко всем кодам, но никто в здравом уме им не пользуется.

2. Здесь s — синдром, t — полученное сообщение, H — проверочная матрица. Этот метод привычен для линейных кодов.

3. Эти способы нужно иметь в виду, но о них было рассказано и без меня, так что я их пропущу.

Вот как выглядит линейный код, и если правильно им обстоит (я не уверен, что так)

Решить на этом примере можно с помощью линейного кода

А в общем случае можно с помощью

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Определения

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.

Вот как выглядит линейный код, и если правильно им обстоит (я не уверен, что так)

Решить на этом примере можно с помощью линейного кода

А в общем случае можно с помощью

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Смежные классы

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

Вот как выглядит линейный код, и если правильно им обстоит (я не уверен, что так)

Решить на этом примере можно с помощью линейного кода

А в общем случае можно с помощью

Faculty Computer Science

Определения

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

Источники

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

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

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

Пример:

Пусть $m = 3, A = \{1, 2\}$, тогда...

$\mathbb{F}_2^m = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$V_A = \{000, 010, 100, 110\}$ ($v_3 = 0 \ \forall v$)

$\bar{A} = \{1, 2, 3\} \setminus A = \{3\}$

$V_{\bar{A}} = \{000, 001\}$ ($v_1 = v_2 = 0 \ \forall v$)

Faculty Computer Science

Смежные классы

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

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 $b \in V_A$, то полученные смежные классы будут все различны (и это будут все смежные классы).

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

Источники

Декодировать сообщение u , если использовался $RM(r, m)$. Для $RM(2, 2)$:
 $f(x_1, x_2) = u_{\{1,2\}}x_1x_2 + u_{\{2\}}x_2 + u_{\{1\}}x_1 + u_{\emptyset}$.

Data: vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$

for $t \leftarrow r$ to 0

foreach $A \subseteq \{1, \dots, m\}$ with $|A| = t$

c = 0

foreach $b \in V_A$

c += $\left(\sum_{z \in (V_A + b)} y_z \right) \bmod 2$

$u_A \leftarrow 1 \mid c \geq 2^{m-t-1}$

$y \leftarrow \text{Eval} \left(\sum_{\substack{A \subseteq \{1, \dots, m\} \\ |A|=t}} u_A \prod_{i \in A} x_i \right)$

На вход поступает бинарный вектор y длины 2^m . Это вектор значений функции, возможно с ошибками (но их не больше, чем $t = 2^{m-r-1} - 1$).

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования кода Рида-Маллера $RM(r, m)$ (см. RM(2, 2)).

Вход: вектор $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$.

Выход: вектор $x = (x_1, \dots, x_m) \in \mathbb{F}_2^m$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

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 пдфке.

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Декодирует сообщение u , если использовался $RM(r, m)$. Для $RM(2, 2)$:
 $f(x_1, x_2) = u_{\{1,2\}}x_1x_2 + u_{\{2\}}x_2 + u_{\{1\}}x_1 + u_{\emptyset}$.

Data: vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$

for $t \leftarrow r$ **to** 0

foreach $A \subseteq \{1, \dots, m\}$ with $|A| = t$

$c = 0$

foreach $b \in V_{\bar{A}}$

$c += \left(\sum_{z \in (V_A + b)} y_z \right) \bmod 2$

$u_A \leftarrow 1 \mid [c \geq 2^{m-t-1}]$

$y \leftarrow \text{Eval} \left(\sum_{A \subseteq \{1, \dots, m\}} u_A \prod_{i \in A} x_i \right)$

Считаем количество (c) смежных классов, в которых $\sum_{z \in (V_A + b)} y_z = 1 \pmod{2}$. Пороговое значение (2^{m-t-1}) здесь — половина от числа смежных классов. Таким образом, если большинство сумм дало 1, то $u_A = 1$, иначе $u_A = 0$.

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования кода Рида-Маллера $RM(r, m)$ (см. RM(2, 2)).

Вход: вектор $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$.

Выход: вектор $x = (x_1, \dots, x_m) \in \mathbb{F}_2^m$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

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 пдфке.

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

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Декодирует сообщение u , если использовался $RM(r, m)$. Для $RM(2, 2)$:
 $f(x_1, x_2) = u_{\{1,2\}}x_1x_2 + u_{\{2\}}x_2 + u_{\{1\}}x_1 + u_{\emptyset}$.

Data: vector $y = (y_z \in \mathbb{F}_2 \mid z \in \mathbb{F}_2^m)$

for $t \leftarrow r$ **to** 0

foreach $A \subseteq \{1, \dots, m\}$ with $|A| = t$

$c = 0$

foreach $b \in V_{\bar{A}}$

$c += \left(\sum_{z \in (V_A + b)} y_z \right) \bmod 2$

$u_A \leftarrow 1 \mid [c \geq 2^{m-t-1}]$

$y \leftarrow \text{Eval} \left(\sum_{A \subseteq \{1, \dots, m\}} u_A \prod_{i \in A} x_i \right)$

Затем мы вычитаем из y (вектор значений функции) всё найденное на этой итерации, после чего переходим к мономам меньшей степени. Повторять до восстановления всех коэффициентов.

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования кода Рида-Маллера $RM(r, m)$ (см. RM(2, 2)).

Вход: вектор $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$.

Выход: вектор $x = (x_1, \dots, x_m) \in \mathbb{F}_2^m$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

Если $y = (y_1, \dots, y_m) \in \mathbb{F}_2^m$ — вектор кода, то $y = (y_1, \dots, y_m) = (x_1, \dots, x_m)$.

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 пдфке.

Faculty Computer Science

Пример

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Ранее: 011 кодируется как 1100 при помощи $RM(1, 2)$

$101 \rightsquigarrow (f(x_1, x_2) = x_1 + 1) \rightsquigarrow$

x_1	x_2	f	
0	0	1	$y_{00} = 1$
0	1	1	$y_{01} = 1$
1	0	0	$y_{10} = 0$
1	1	0	$y_{11} = 0$

$\rightsquigarrow 1100$

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

