

Faculty of Computer Science and Systems

Код Рид-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

Домашнее задание

Источники

Код Рид-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

12 марта 2022 г.

2022-03-12

Код Рид-Маллера

Рид-Маллер

Высшая Школа Экономики

12 марта 2022 г.

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 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.

Faculty of Computer Science and Systems

Код Рид-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

Домашнее задание

Источники

Введение

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

Обозначается как $RM(r, m)$, где r — ранг, а 2^m — длина кода. Кодировать 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 $u \oplus v = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$.

Faculty of Computer Science and Systems

Код Рид-Маллера

Булевы функции и многочлен Жегалкина

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

Домашнее задание

Источники

Булевы функции и многочлен Жегалкина

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:

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

Faculty of Computer Science and Systems

Код Рид-Маллера

Многочлены Жегалкина

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

Домашнее задание

Источники

Многочлены Жегалкина

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 $m = 2$: $f(x_1, x_2) = c_{12} \cdot x_{11}x_2 + c_{22} \cdot x_2 + c_{11} \cdot x_1 + c_{\emptyset} \cdot 1$

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

Faculty of Computer Science and Systems

Код Рид-Маллера

Функции небольшой степени

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

Домашнее задание

Источники

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

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

В слове «кодирование» буквы «о» и «и» встречаются 1 раз, «е» — 2 раза, «а» — 3 раза, «т» — 4 раза, «р» — 5 раз, «н» — 6 раз, «с» — 7 раз, «л» — 8 раз, «д» — 9 раз, «к» — 10 раз, «м» — 11 раз, «я» — 12 раз, «б» — 13 раз, «г» — 14 раз, «ж» — 15 раз, «з» — 16 раз, «и» — 17 раз, «о» — 18 раз, «п» — 19 раз, «р» — 20 раз, «с» — 21 раз, «т» — 22 раз, «у» — 23 раз, «ф» — 24 раз, «х» — 25 раз, «ц» — 26 раз, «ч» — 27 раз, «ш» — 28 раз, «щ» — 29 раз, «ъ» — 30 раз, «ы» — 31 раз, «э» — 32 раз, «ю» — 33 раз, «я» — 34 раз.

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 не больше, ведь $\deg f \leq r$).

Faculty 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

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

В слове «кодирование» буквы «о» и «и» встречаются 1 раз, «е» — 2 раза, «а» — 3 раза, «т» — 4 раза, «р» — 5 раз, «н» — 6 раз, «с» — 7 раз, «л» — 8 раз, «д» — 9 раз, «к» — 10 раз, «м» — 11 раз, «я» — 12 раз, «б» — 13 раз, «г» — 14 раз, «ж» — 15 раз, «з» — 16 раз, «и» — 17 раз, «о» — 18 раз, «п» — 19 раз, «р» — 20 раз, «с» — 21 раз, «т» — 22 раз, «у» — 23 раз, «ф» — 24 раз, «х» — 25 раз, «ц» — 26 раз, «ч» — 27 раз, «ш» — 28 раз, «щ» — 29 раз, «ъ» — 30 раз, «ы» — 31 раз, «э» — 32 раз, «ю» — 33 раз, «я» — 34 раз.

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 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: 101, тогда $f(x_1, x_2) = x_2 + 0 + 1$.
- Подставим всевозможные комбинации:

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

- Получили код: $\text{Eval}(f) = 1100$.

2022-03-12

Код Риды-Маллера

Кодирование

Пример

Рид-Маллер, 1954, стр. 100-101

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

В слове «кодирование» буквы «о» и «и» встречаются 1 раз, «е» — 2 раза, «а» — 3 раза, «т» — 4 раза, «р» — 5 раз, «н» — 6 раз, «с» — 7 раз, «л» — 8 раз, «д» — 9 раз, «к» — 10 раз, «м» — 11 раз, «я» — 12 раз, «б» — 13 раз, «г» — 14 раз, «ж» — 15 раз, «з» — 16 раз, «и» — 17 раз, «о» — 18 раз, «п» — 19 раз, «р» — 20 раз, «с» — 21 раз, «т» — 22 раз, «у» — 23 раз, «ф» — 24 раз, «х» — 25 раз, «ц» — 26 раз, «ч» — 27 раз, «ш» — 28 раз, «щ» — 29 раз, «ъ» — 30 раз, «ы» — 31 раз, «э» — 32 раз, «ю» — 33 раз, «я» — 34 раз.

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 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.

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

- $c_{\{2\}} = 1, c_{\{1\}} = 0, c_{\emptyset} = 1$, исходное сообщение: 101.

2022-03-12

Код Рида-Маллера

Кодирование

Декодирование когда потеря нет

Мы рассмотрим код

Построение таблиц истинности

Решение задачи

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

Анализ кода Рида-Маллера

Построение таблиц истинности

Решение задачи

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

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

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

Анализ кода Рида-Маллера

Построение таблиц истинности

Решение задачи

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

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

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

1

0

0

\dots

1

0

1

\vdots

\vdots

1

1

\dots

1

0

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

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

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

Анализ кода Рида-Маллера

Построение таблиц истинности

Решение задачи

Задача Рида-Маллера

Свойства кода

Декодирование

Источники

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

Faculty Computer Science

Доказательство линейности

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

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

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.

Faculty Computer Science

Конструкция Плоткина: вывод

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

Докодирование

Система Риды-Маллера

Доказательство

Задача

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. $\deg h \leq r - 1$)

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

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.

Faculty Computer Science

Конструкция Плоткина

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

Докодирование

Система Риды-Маллера

Доказательство

Задача

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

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

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.

Faculty Computer Science

Минимальное расстояние

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

Докодирование

Система Риды-Маллера

Доказательство

Задача

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

- Свойства кода
- Минимальное расстояние
- Минимальное расстояние

Решение задачи минимального расстояния для кода RM(1,1)

$r = 1, m = 1$
Параметры: код $d = 2^{m-r} = 2^0 = 1$ является тривиальным.
Вектор RM(1,1) — это вектор единичности $\vec{1}$ для \mathbb{F}_2^2 .
 $\vec{1} = (1, 1) \in \mathbb{F}_2^2$.
Размерность кода $k = 2^{m-r} = 2^0 = 1$, $n = 2^m = 2$.
Матрица кода $G = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.

1. Случай $RM(0, m)$ 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 $w(00\dots 0)$, 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): $w(x \parallel y) = w(x) + w(y)$. Вес это всего лишь число ненулевых элементов, поэтому нет разницы как мы будем группировать части вектора.
Переход (3): $w(u \oplus v) \geq w(v) - w(u)$. Если у нас в v стоит $w(v)$ бит, то прибавив к нему u , мы сможем изменить (обнулить) не больше $w(u)$ бит. Возможно появится больше единиц, но нас интересует нижняя граница.
Переход (IH): предположение индукции в чистом виде.

2022-03-12

Код Рида-Маллера

- Свойства кода
- Параметры
- Свойства и параметры

Для кода Рида-Маллера $RM(r, m)$

$r \leq m$

- Вектор $\vec{1}$
- Вектор $\vec{1}$ и вектор $\vec{1}$ в \mathbb{F}_2^m
- Вектор $\vec{1}$ и вектор $\vec{1}$ в \mathbb{F}_2^m
- Вектор $\vec{1}$ и вектор $\vec{1}$ в \mathbb{F}_2^m
- Вектор $\vec{1}$ и вектор $\vec{1}$ в \mathbb{F}_2^m
- Вектор $\vec{1}$ и вектор $\vec{1}$ в \mathbb{F}_2^m

1. Теперь можно подвести итоги исследования свойств.
2. , поскольку $t = \lfloor \frac{2^{m-r}-1}{2} \rfloor = \lfloor \frac{2^{m-r}}{2} - \frac{1}{2} \rfloor = \lfloor 2^{m-r-1} - 0.5 \rfloor = 2^{m-r-1} - 1$
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. Однако доказательство можно найти в «Reed-Muller Codes: Theory and Algorithms», раздел Duality.

Faculty of Computer Science

Свойства и параметры

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Параметры

Декодирование

Дополнительно

Домашнее задание

Источники

Для бинарного кода $RM(r, m)$:

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

Faculty of Computer Science

Возможные варианты

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Параметры

Декодирование

Дополнительно

Домашнее задание

Источники

$m \backslash r$	0	1	2	3	4
1	$k=1$ $n=2$ $t=0$	$k=2$ $n=2$ $t=0$	—	—	—
2	$k=1$ $n=4$ $t=1$	$k=3$ $n=4$ $t=0$	$k=4$ $n=4$ $t=0$	—	—
3	$k=1$ $n=8$ $t=3$	$k=4$ $n=8$ $t=1$	$k=7$ $n=8$ $t=0$	$k=8$ $n=8$ $t=0$	—
4	$k=1$ $n=16$ $t=7$	$k=5$ $n=16$ $t=3$	$k=11$ $n=16$ $t=1$	$k=15$ $n=16$ $t=0$	$k=16$ $n=16$ $t=0$

2022-03-12

Код Рида-Маллера

- Свойства кода
- Параметры
- Возможные варианты

Решение задачи минимального расстояния для кода RM(1,1)

$r = 1, m = 1$
Параметры: код $d = 2^{m-r} = 2^0 = 1$ является тривиальным.
Вектор RM(1,1) — это вектор единичности $\vec{1}$ для \mathbb{F}_2^2 .
 $\vec{1} = (1, 1) \in \mathbb{F}_2^2$.
Размерность кода $k = 2^{m-r} = 2^0 = 1$, $n = 2^m = 2$.
Матрица кода $G = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.
Матрица кода $H = (1, 1) \in \mathbb{F}_2^{1 \times 2}$.

1. У красных кодов минимальное расстояние d равно единице — они совершенно бесполезны, там количество кодов равно количеству сообщений; у желтых кодов $d = 2$ — они могут определить наличие ошибки, но не могут её исправить. Для всех остальных кодов $d = 2(t+1)$.
2. Напоминание: k — длина сообщения, n — длина кода, а t — количество ошибок, которое код точно сможет исправить. Заодно о параметрах кода: m — количество переменных у функции (очень влияет на длину кода), а r — максимальная степень многочлена (очень влияет на длину сообщения, и соответственно надёжность кода), причём $r \leq m$. Конечно, таблицу можно продолжать и дальше.
3. И кстати, случай $m = 0, k = 0$ (не влез) будет собой представлять кодирование единственного бита совершенно без изменений.

Faculty of Computer Science

Как линейный код

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Параметры

Декодирование

Дополнительно

Домашнее задание

Источники

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

- Перебор по всему пространству кодовых слов в поисках ближайшего.
- С использованием синдромов: $s = rH^T$.

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.

Faculty Computer Science

Определения

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Классы

Дополнительные доказательства

Алгоритм Рида

Домашнее задание

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...

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

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

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

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

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.

Faculty Computer Science

Смежные классы

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Классы

Дополнительные доказательства

Алгоритм Рида

Домашнее 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).

2022-03-12

Код Рида-Маллера

Декодирование

Алгоритм Рида

Смежные классы

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

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Классы

Дополнительные доказательства

Алгоритм Рида

Домашнее задание

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

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

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

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

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 $RM(r, m)$

Декодирование с использованием BCH-кода (см. BCH-код)

$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$

Важно отметить, что декодирование с использованием BCH-кода требует знания кода Рида-Маллера. В противном случае декодирование невозможно.

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

2. Цель — восстановить все коэффициенты при многочлене вида

$$f(x_1, \dots, x_m) = u_0 + u_1 x_1 + x_2 x_2 + \dots + u_{1,2,\dots,r} x_{1,2,\dots,r},$$

где $\deg f \leq r$. Обратите внимание, что для индексов при u используются подмножества $A \subseteq \{1, \dots, m\}, |A| \leq r$, причём каждый u_A умножается на моном $\prod_{i \in A} x_i$.

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Декодирование сообщения u , если использовался $RM(r, m)$. Для $RM(2, 2)$:

$$f(x_1, x_2) = u_{\{1,2\}} x_1 x_2 + u_{\{2\}} x_2 + u_{\{1\}} x_1 + u_{\emptyset}.$$

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

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

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

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

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

Будем восстанавливать сначала коэффициенты u_A при старших степенях, потом поменьше и так пока не восстановим их все. Начинаем с $t = r$.

2022-03-12

Код Рида-Маллера

└─Декодирование

└─Алгоритм Рида

└─Алгоритм Рида для кода $RM(r, m)$

Декодирование с использованием BCH-кода (см. BCH-код)

$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$

Важно отметить, что декодирование с использованием BCH-кода требует знания кода Рида-Маллера. В противном случае декодирование невозможно.

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

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Декодирование сообщения u , если использовался $RM(r, m)$. Для $RM(2, 2)$:

$$f(x_1, x_2) = u_{\{1,2\}} x_1 x_2 + u_{\{2\}} x_2 + u_{\{1\}} x_1 + u_{\emptyset}.$$

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

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

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

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

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

Хотим восстановить все коэффициенты при мономах степени t . Для этого перебираем все $A, |A| = t$ и для каждого восстанавливаем коэффициент u_A при $x_{A_1} x_{A_2} \dots x_{A_t}$.

2022-03-12

Код Рида-Маллера

└─Декодирование

└─Алгоритм Рида

└─Алгоритм Рида для кода $RM(r, m)$

Декодирование с использованием BCH-кода (см. BCH-код)

$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$
$$f(x) = x^{2^m-1} + \sum_{i=1}^r x^{2^{m-i}-1}$$

Важно отметить, что декодирование с использованием BCH-кода требует знания кода Рида-Маллера. В противном случае декодирование невозможно.

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

Faculty Computer Science

Алгоритм Рида для кода $RM(r, m)$

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Доказательство

Источники

Декодирование сообщения u , если использовался $RM(r, m)$. Для $RM(2, 2)$:

$$f(x_1, x_2) = u_{\{1,2\}} x_1 x_2 + u_{\{2\}} x_2 + u_{\{1\}} x_1 + u_{\emptyset}.$$

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

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

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


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

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

Чтобы восстановить коэффициент, нужно перебрать все смежные классы вида $(V_A + b)$:

$$V_A = \{v \in \mathbb{F}_2^m \mid v_i = 0 \forall i \notin A\}$$
$$b \in \{v \in \mathbb{F}_2^m \mid v_i = 0 \forall i \in A\}$$

[illegible]



Факультет
Компьютерных
Наук

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

Код	Рида-Маллера
Варианты	
Кодирование	
Свойства кода	
Алгоритмы декодирования исправления ошибок с помощью синдромов	
Декриптографические	
Аппаратные реализации	
Практические задания	
Источники	

2022-03-12


└ Код Рида-Маллера

└ Декодирование

└ Алгоритм Рида

└ Алгоритм Рида для кода $\text{RM}(r, m)$

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



Код

Радо Маллера

Введение

Кодирование

Свойства кода

Корректирующие коды

Криптография

Демонстрация

Алгоритм Рида

Демонстрация

Источники

Алгоритм Рида для кода $RM(r, m)$

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 $b \in V_A$

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

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

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

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)

Деконструкция алгоритма с использованием RM(10, 10) — Data RM(10, 10)

$$\{Z_1, Z_2, \dots, Z_{10}\} = \{x^0, x^1, x^2, \dots, x^9\}$$

Вход: $\text{word} = [z_0, z_1, z_2, z_3, z_4, z_5, z_6, z_7, z_8, z_9]$

Выход: $\text{data} = [d_0, d_1, d_2, d_3, d_4, d_5, d_6, d_7, d_8, d_9]$

```

1  Find  $k_1, k_2$ 
2  for  $i = 0$  to 9 do
3     $t_i = \left(\frac{z_{k_1+i}}{z_{k_2+i}}\right)^{\alpha^{2i}}$ 
4  end for
5   $d = -\alpha^{-1} \left[ \sum_{i=0}^9 t_i \cdot \alpha^{2i} \right]$ 
        
```

Замечания: Алгоритм декодирования Рида-Маллера не является эффективным алгоритмом декодирования в общем смысле. Однако, он может использоваться для декодирования кодов Рида-Маллера.

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

Faculty Computer Science Код Рига-Маллера Векторы Кодирование Свойства кода Декодирование Автоматическое декодирование Примеры Заключение Источники	Пример															
	Ранее: 101 кодируется как 1100 при помощи RM(1, 2)															
	$101 \rightsquigarrow (f(x_1, x_2) = x_1 + 1) \rightsquigarrow$															
	<table border="1"> <thead> <tr> <th>x_1</th> <th>x_2</th> <th>f</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>0</td> <td>1</td> </tr> <tr> <td>0</td> <td>1</td> <td>1</td> </tr> <tr> <td>1</td> <td>0</td> <td>0</td> </tr> <tr> <td>1</td> <td>1</td> <td>0</td> </tr> </tbody> </table>	x_1	x_2	f	0	0	1	0	1	1	1	0	0	1	1	0
	x_1	x_2	f													
	0	0	1													
	0	1	1													
	1	0	0													
	1	1	0													
$y_{00} = 1$ $y_{01} = 1 \rightsquigarrow 1100$ $y_{10} = 0$ $y_{11} = 0$																

2022-03-12

Код Рида-Маллера

└─Декодирование

└─└─Алгоритм Рида

└─└─└─Пример

1. Как происходит кодирование, схематически:

Рисунок 10.8: кодирование с помощью RM(1, 2)

	$y_{00} = 1$	$y_{01} = 1$	$y_{10} = 0$	$y_{11} = 0$
$1101 = (y_{00}, y_{01}, y_{10}, y_{11}) = y_0, y_1$	1	1	0	0
	1	1	0	0

Faculty Computer Science

Пример

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Пример

Домашнее задание

Источники

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: $t = 1, A = \{1\}$

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

2022-03-12

Код Рида-Маллера

└─Декодирование

└─└─Алгоритм Рида

└─└─└─Пример

1. Теперь начинаем декодирование.

2. — по одному на каждый вектор из $V_{\bar{A}}$

Рисунок 10.8: кодирование с помощью RM(1, 2)

	$y_{00} = 1$	$y_{01} = 1$	$y_{10} = 0$	$y_{11} = 0$
$1101 = (y_{00}, y_{01}, y_{10}, y_{11}) = y_0, y_1$	1	1	0	0
	1	1	0	0

Faculty Computer Science

Пример

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Пример

Домашнее задание

Источники

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

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

2022-03-12

Код Рида-Маллера

└─Декодирование

└─└─Алгоритм Рида

└─└─└─Пример

1. — по одному на каждый вектор из $V_{\bar{A}}$.

Рисунок 10.8: кодирование с помощью RM(1, 2)

	$y_{00} = 1$	$y_{01} = 1$	$y_{10} = 0$	$y_{11} = 0$
$1101 = (y_{00}, y_{01}, y_{10}, y_{11}) = y_0, y_1$	1	1	0	0
	1	1	0	0

Faculty Computer Science

Пример

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Пример

Домашнее задание

Источники

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. $|A| \leq 1$.

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

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

Вычислим $\text{Eval}(g)$:

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

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

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