

Faculty
Computer
science
for everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Получение
Минимальное
расстояние
Декодирова-
ние
Пара слов и
ошибки
Алгоритм Рида
Домашнее
задание
Источники

Код Рида-Маллера

Илья Коннов
Факультет компьютерных наук
Высшая Школа Экономики
13 февраля 2022 г.

2022-02-13

Код Рида-Маллера

Код Рида-Маллера
Высшая школа экономики
Факультет компьютерных наук
13 февраля 2022 г.

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.

Faculty
Computer
science
for everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Получение
Минимальное
расстояние
Декодирова-
ние
Пара слов и
ошибки
Алгоритм Рида
Домашнее
задание
Источники

Введение

Описан Дэвидом Маллером (автор идеи) и Ирвингом Ридом (автор метода декодирования) в сентябре 1954 года. Обозначаются как $RM(r, m)$, где r — ранг, а 2^m — длина кода. Кодирование сообщений длиной $k = \sum_{i=0}^r C_m^i$ при помощи 2^m бит. Традиционно, считается что коды бинарные и работают над битами, т.е. \mathbb{Z}_2 . Соглашение: сложение векторов $u, v \in \mathbb{Z}_2^n$ будем обозначать как $u \oplus v = (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$.

Faculty
Computer
science
for everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Получение
Минимальное
расстояние
Декодирова-
ние
Пара слов и
ошибки
Алгоритм Рида
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

И при помощи многочлена Жегалкина:

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

Faculty
Computer
science
for everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Получение
Минимальное
расстояние
Декодирова-
ние
Пара слов и
ошибки
Алгоритм Рида
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 $m = 2$:

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

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

Faculty
Computer
science
for everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Получение
Минимальное
расстояние
Декодирова-
ние
Пара слов и
ошибки
Алгоритм Рида
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?

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

2022-02-13

Код Рида-Маллера

Введение

Функции небольшой степени

Рассмотрим функции, степень которых не больше r .
Бинарный код $(f(x_1, x_2, \dots, x_m))$ длины 2^m .
Каждый бит — значение функции.
$$f(x_1, x_2, \dots, x_m) = \sum_{i=0}^r \sum_{|S|=i} a_S \prod_{j \in S} x_j$$

В коде f 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 .

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{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 .

2022-02-13

Код Рида-Маллера

Кодирование

Идея кодирования

Путь кода: бинарный код длины 2^m — кодирование многочлена от m переменных степени не больше r .
Тогда мы можем его представить при помощи 2^m бит, поставив их в качестве коэффициентов многочлена.
Тогда бинарный код — это таблица истинности, из которой можно получить значения многочлена, а также можно получить значения многочлена, а также можно получить значения многочлена, а также можно получить значения многочлена.

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

2022-02-13

Код Рида-Маллера

Кодирование

Пример

Путь кода: бинарный код длины 2^m — кодирование многочлена от m переменных степени не больше r .
Тогда мы можем его представить при помощи 2^m бит, поставив их в качестве коэффициентов многочлена.
Тогда бинарный код — это таблица истинности, из которой можно получить значения многочлена, а также можно получить значения многочлена, а также можно получить значения многочлена.

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

Faculty Computer Science

Идея кодирования

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальные расстояния

Декодирование

Пара слов и синдром

Алгоритм Рида

Домашнее задание

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 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

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

Faculty Computer Science

Пример

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальные расстояния

Декодирование

Пара слов и синдром

Алгоритм Рида

Домашнее задание

Источники

- $r = 1$ (степень многочлена), $m = 2$ (переменных). Это $\text{RM}(1, 2)$.
- Тогда наш многочлен: $f(x, y) = c_1x + c_2y + c_3$.
- 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: $\text{Eval}(f) = 1100$.

Faculty Computer Science

Декодирование когда потерь нет

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальные расстояния

Декодирование

Пара слов и синдром

Алгоритм Рида

Домашнее задание

Источники

- Мы получили код: 1100
- Представим таблицу истинности.

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

- Подстановками в $f(x, y) = c_1x + c_2y + c_3$ получим СЛАУ.

$$\begin{cases} c_1 + c_2 + c_3 = 1 \\ c_1 + c_2 + c_3 = 1 \\ c_1 + c_2 + c_3 = 0 \\ c_1 + c_2 + c_3 = 0 \end{cases}$$

- $c_1 = 1, c_2 = 0, c_3 = 1$, исходное сообщение: 101 .

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

2022-02-13

Код Рида-Маллера

Свойства и параметры кода

Последствия линейности

■ Свойства минимального расстояния d :
 $d = n - k$
 $d = n - k$
 $d = n - k$

■ Минимальное расстояние будет равно минимальному весу ненулевого слова кода.
 $d = \min_{c \in C, c \neq 0} |c|$
 $d = \min_{c \in C, c \neq 0} |c|$

■ Корректирующая способность:
 $t = \lfloor \frac{d-1}{2} \rfloor$

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.

2022-02-13

Код Рида-Маллера

Свойства и параметры кода

Конструкция Плоткина

Конструкция Плоткина: многочлены

■ Как найти минимальное расстояние d :
 $d = n - k$
 $d = n - k$
 $d = n - k$

■ Минимальное расстояние будет равно минимальному весу ненулевого слова кода.
 $d = \min_{c \in C, c \neq 0} |c|$
 $d = \min_{c \in C, c \neq 0} |c|$

■ Корректирующая способность:
 $t = \lfloor \frac{d-1}{2} \rfloor$

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 $m > 1$.

2022-02-13

Код Рида-Маллера

Свойства и параметры кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

■ Как найти минимальное расстояние d :
 $d = n - k$
 $d = n - k$
 $d = n - k$

■ Минимальное расстояние будет равно минимальному весу ненулевого слова кода.
 $d = \min_{c \in C, c \neq 0} |c|$
 $d = \min_{c \in C, c \neq 0} |c|$

■ Корректирующая способность:
 $t = \lfloor \frac{d-1}{2} \rfloor$

1. Теперь рассмотрим те же функции, но со стороны их таблиц истинности. Нам же интересны именно коды, а они как раз очень тесно связаны с этими таблицами.

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

4. Палочка по центру — конкатенация векторов.

Faculty Computer science

Конструкция Плоткина: многочлены

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция Плоткина

Минимальное расстояние

Декодирование

Пара слов о синдроме

Алгоритм Рида

Домашнее задание

Источники

Хотим понять как выглядят кодовые слова.

■ Код — таблица истинности 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 и параметры кода

Конструкция Плоткина

Минимальное расстояние

Декодирование

Пара слов о синдроме

Алгоритм Рида

Домашнее задание

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 $x_1 = 1$.

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

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

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

Faculty Computer science

Конструкция Плоткина: вывод

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция Плоткина

Минимальное расстояние

Декодирование

Пара слов о синдроме

Алгоритм Рида

Домашнее задание

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

Заметим, что $Eval(f)$ — кодовое слово (как и для g, h). Тогда:
 $c = Eval(f) \in RM(r, m)$ (т.к. $\deg f \leq r$)
 $u = Eval(g) \in RM(r, m - 1)$ (т.к. $\deg g \leq r$)
 $v = Eval(h) \in RM(r - 1, m - 1)$ (т.к. $\deg h \leq r - 1$)

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

2022-02-13

Код Рида-Маллера

Декодирование

Как линейный код

Этот код является линейным кодом, к нему применимы все свойства (в информатическом смысле):

■ Проверка на наличие транзитивных парных слов в тексте

■ Декодирование

■ Использование 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.

Faculty Computer science

Синдромы и как их использовать

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальное расстояние

Декодирование

Пара слов с синдромом

Алгоритм Рида

Домашнее задание

Источники

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.

2022-02-13

Код Рида-Маллера

Декодирование

Синдромы и как их использовать

Этот код является линейным кодом, к нему применимы все свойства (в информатическом смысле):

■ Проверка на наличие транзитивных парных слов в тексте

■ Декодирование

■ Использование синдромов $s = rH^T$

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

Faculty Computer science

Пример

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальное расстояние

Декодирование

Пара слов с синдромом

Алгоритм Рида

Домашнее задание

Источники

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

■ $t = 1$

■

■ $t = 0$

■

2022-02-13

Код Рида-Маллера

Декодирование

Алгоритм Рида

Пример

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

■ $t = 1$

■

■ $t = 0$

■

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).

Faculty Computer science

Код Рида-Маллера

Введение

Кодирование

Свойства и параметры кода

Конструкция

Получение

Минимальное расстояние

Декодирование

Пара слов с синдромом

Алгоритм Рида

Домашнее задание

Источники

TODO

Faculty
Computer
Science
for Everyone

Код
Рида-Маллера

Введение
Кодирование
Свойства и
параметры
кода
Конструкция
Голтвинга
Матричные
расширения
Декодирова-
ние
Путь след и
свертывания
Алгоритм Рида
Домашнее
задание
Источники

- 1 <https://arxiv.org/pdf/2002.03317.pdf> — великолепный обзор, очень рекомендую.
- 2 <http://dha.spb.ru/PDF/ReedMullerExamples.pdf> — очень хорошо и подробно, но используется подход через матрицы, а не через полиномы, а это не весело.
- 3 https://en.wikipedia.org/wiki/Reed-Muller_code — кратко, чётко, понятно, но не описано декодирование.
- 4 https://ru.bmstu.wiki/Коды_Рида-Маллера — в целом всё есть, но написано очень непонятно;

2022-02-13

Код Рида-Маллера

Источники

- 1 <https://arxiv.org/pdf/2002.03317.pdf> — великолепный обзор, очень рекомендую.
- 2 <http://dha.spb.ru/PDF/ReedMullerExamples.pdf> — очень хорошо и подробно, но используется подход через матрицы, а не через полиномы, а это не весело.
- 3 https://en.wikipedia.org/wiki/Reed-Muller_code — кратко, чётко, понятно, но не описано декодирование.
- 4 https://ru.bmstu.wiki/Коды_Рида-Маллера — в целом всё есть, но написано очень непонятно;

1. Бонусный раздел, который не включён в основную презентацию, но может быть очень полезен.