

Faculty of Computer Science

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

История Риды-Маллера

Домашнее задание

Источники

Код Риды-Маллера

Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

14 марта 2022 г.

Код Риды-Маллера

2022-03-14

Риды-Маллер

Код Риды-Маллера

18 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

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

История Риды-Маллера

Домашнее задание

Источники

Авторы

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



Faculty of Computer Science

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

История Риды-Маллера

Домашнее задание

Источники

Введение

Обозначается как $RM(r, m)$, 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 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

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

История Риды-Маллера

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

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Краткая презентация

Декодирование

История Риды-Маллера

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

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

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?

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

2022-03-14

Код Рида-Маллера

Введение

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?

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

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 of Computer Science

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

История

Идея кодирования

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

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

2022-03-14

Код Рида-Маллера

Кодирование

Идея кодирования

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

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

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

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

История

Пример

- $r = 1$ (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: $\text{Eval}(f) = 1100$.

2022-03-14

Код Рида-Маллера

Кодирование

Пример

1. Здесь и далее я для краткости и удобства записываю битовые векторы не как $(1 \ 0 \ 0 \ 1)$, а как 1001 при помощи несмешанного 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 $m = 4$:

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

Также можно кодировать множества при помощи битов, используя отношение $x \in A \iff v_x = 1$ (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 at SPbU

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Декодирование когда потерь нет

- 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.
$$\begin{cases} c_0 = 1 \\ c_1 + c_0 = 1 \\ c_1 + c_2 + c_0 = 0 \end{cases}$$
- $c_{\{1\}} = 1, c_{\{2\}} = 0, c_{\emptyset} = 1$, исходное сообщение: 011.

2022-03-14

Код Рида-Маллера

Кодирование

Декодирование когда потерь нет

Мы получили код: 1100

Представим таблицу истинности

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

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

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

Faculty Computer science at SPbU

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Коды 0-го порядка

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:

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	\ddots	\vdots	\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 $\underbrace{11\dots1}_{2^m}$

2022-03-14

Код Рида-Маллера

Кодирование

Коды 0-го порядка

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

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

2. Таких функций существует всего лишь две, поскольку мы можем влиять лишь на свободный член. Все остальные коэффициенты обнуляются из-за требования $\deg f \leq 0$.

3. Здесь число строк, как и в любой другой таблице истинности, равно 2^m , а колонки со значениями никак не зависят от аргументов функций. Получается две колонки — одна с нулями, другая с единицами.

Faculty Computer science at SPbU

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Доказательство

Источники

Коды m -го порядка

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.

2022-03-14

Код Рида-Маллера

Кодирование

Коды m -го порядка

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

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

Faculty Computer science

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция

Плоткина

Декларация

Источники

Конструкция Плоткина: таблица истинности

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

Код Риды-Маллера

2022-03-14

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: таблица истинности

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

- 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.
- 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.
- 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.
- Палочка по центру — конкатенация векторов.

Faculty Computer science

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция

Плоткина

Декларация

Источники

Конструкция Плоткина: вывод

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

Код Риды-Маллера

2022-03-14

Свойства кода

Конструкция Плоткина

Конструкция Плоткина: вывод

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

- Теперь собираем всё это в одно важное утверждение.
- Причём мы уже знаем, что $\deg g \leq r$ и $\deg h \leq r - 1$, если $\deg f \leq r$
- Напомним, 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

Код Риды-Маллера

Введение

Кодирование

Свойства кода

Конструкция

Плоткина

Декларация

Источники

Конструкция Плоткина

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

Код Риды-Маллера

2022-03-14

Свойства кода

Конструкция Плоткина

Конструкция Плоткина

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

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

1. Теперь можно подвести итоги исследования свойств.
2. , поскольку $t = \left\lfloor \frac{d+1}{2} \right\rfloor = \left\lfloor \frac{2^{m-r}-1}{2} \right\rfloor = 2^{m-r-1} - 0,5 = 2^{m-r-1} - 1$
3. , она позволяет делить 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 Computer Science

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Алгоритм Рида

Домашнее задание

Источники

Возможные варианты

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

2022-03-14

Код Рида-Маллера

Свойства кода

Параметры

Возможные варианты

r	k	n	t	k	n	t
0	1	2	0	1	2	0
1	2	4	1	3	4	0
2	4	8	3	7	8	1
3	8	16	7	15	16	3
4	16	32	15	31	32	7

- 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 $d = 2(t + 1)$.
- 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.
- И кстати, случай $m = 0, k = 0$ (не влез) будет собой представлять колирование единственного бита совершенно без изменений.

Faculty Computer Science

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Алгоритм Рида

Домашнее задание

Источники

Как линейный код

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: $s = rH^T$.

2022-03-14

Код Рида-Маллера

Декодирование

Как линейный код

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

Здесь s — синдром, r — полученное сообщение, H — проверочная матрица. Этот метод обычен для линейных кодов.

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

Faculty Computer Science

Код Рида-Маллера

Введение

Кодирование

Свойства кода

Декодирование

Алгоритм Рида

Домашнее задание

Источники

Определения

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...
- $V_2^m = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- $V_A = \{000, 010, 100, 110\}$ ($v_3 = 0 \ \forall v$)
- $\bar{A} = \{1, 2, 3\} \setminus A = \{3\}$
- $V_{\bar{A}} = \{000, 001\}$ ($v_1 = v_2 = 0 \ \forall v$)

2022-03-14

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

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

Домашнее задание

Источники

Смежные классы

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).

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Смежные классы

Код Рида-Маллера $V_A \subseteq \mathbb{F}_2^m$, 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).

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

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

Домашнее задание

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

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

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

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

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

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

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

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

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

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

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

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

2. Цель — восстановить все коэффициенты при многочлене вида $f(x_1, \dots, x_m) = u_{\emptyset} + u_1x_1 + x_2x_2 + \dots + u_{1,2,\dots,r}x_1x_2\dots x_r$, 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

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Дополнительные доказательства

Домашнее задание

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

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

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

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

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

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

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

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

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

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

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

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

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Домашнее задание

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

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

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

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

Faculty Computer Science

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Домашнее задание

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

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

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

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

Faculty Computer Science

Код Рида-Маллера

Введение

Декодирование

Свойства кода

Алгоритм Рида

Домашнее задание

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

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

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

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

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования, если использован $RM(r, m)$ (см. RM(2, 2))

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

Выход: вектор $u = (u_A \in \mathbb{F}_2 \mid A \subseteq \{1, \dots, m\})$

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

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 пдфке.

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования, если использован $RM(r, m)$ (см. RM(2, 2))

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

Выход: вектор $u = (u_A \in \mathbb{F}_2 \mid A \subseteq \{1, \dots, m\})$

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

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 пдфке.

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования, если использован $RM(r, m)$ (см. RM(2, 2))

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

Выход: вектор $u = (u_A \in \mathbb{F}_2 \mid A \subseteq \{1, \dots, m\})$

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

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 пдфке.

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

Faculty
Computer
science
MSU

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Алгоритм Рида

Домашнее задание

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 $|A| = t$

$c \leftarrow 0$

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

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

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

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

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.

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Алгоритм Рида для кода $RM(r, m)$

Алгоритм декодирования, 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 $|A| = t$

$c \leftarrow 0$

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

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

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

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

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.

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
MSU

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Алгоритм Рида

Домашнее задание

Источники

Пример

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

$$101 \rightsquigarrow (f(x_1, x_2) = x_1 + 1) \rightsquigarrow \begin{array}{c|c|c} x_1 & x_2 & f \\ \hline 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{array} \rightsquigarrow \begin{array}{l} y_{00} = 1 \\ y_{01} = 1 \\ y_{10} = 0 \\ y_{11} = 0 \end{array} \rightsquigarrow 1100$$

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Пример

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

00	01	10	11
1	1	0	0

000 → 010, 010 → 100, 100 → 110, 110 → 000

1. Как происходит кодирование, схематически:

Faculty
Computer
science
MSU

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Алгоритм Рида

Домашнее задание

Источники

Пример

Ранее: 011 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: $u_A = u_{\{1\}} = 1$

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Пример

Ранее: 011 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: $u_A = u_{\{1\}} = 1$

1. Теперь начинаем декодирование.

2. (меняется только первый бит)

3. (первый бит обнулится)

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

Faculty of Computer Science
of Moscow

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Пример

Домашнее задание

Источники

Пример

Ранее: 011 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
- $(V_A + 00) = \{00, 01\}$, сумма: $y_{00} + y_{01} = 1 + 1 = 0$
- $(V_A + 10) = \{10, 11\}$, сумма: $y_{10} + y_{11} = 0 + 0 = 0$
- Итого: $u_A = u_{\{2\}} = 0$

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Пример

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

Ранее: 011 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.
• $(V_A + 00) = \{00, 01\}$, сумма по y_{00}, y_{01} равна 0.
• $(V_A + 10) = \{10, 11\}$, сумма по y_{10}, y_{11} равна 0.
Итого: $u_A = u_{\{2\}} = 0$.

Faculty of Computer Science
of Moscow

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Пример

Домашнее задание

Источники

Пример

Ранее: 011 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 $Eval(g)$:

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

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

2022-03-14

Код Рида-Маллера

Декодирование

Алгоритм Рида

Пример

1. Здесь мы берём все u , полученные при $t = 1$, домножаем каждую на соответствующие ей x -ы и получаем функцию от m переменных.

2. Очень важно, чтобы у нас во всех таблицах истинности (в т.ч. той, которая использовалась при кодировании для получения y) был одинаковый порядок строк. Иначе чуда не выйдет.

3. Полезно заметить, что в \mathbb{F}_2 сложение и вычитание — одно и то же.

Ранее: 011 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 $Eval(g)$:

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

Faculty of Computer Science
of Moscow

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Пример

Домашнее задание

Источники

Продолжение примера: $t = 0$

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

Шаг 3/3: $t = 0, A = \emptyset$

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

Faculty of Computer Science
of Moscow

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Классификация

Декодирование

Пример

Домашнее задание

Источники

Продолжение примера: $t = 0$

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

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

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

а исходное сообщение: 011, как и ожидалось.

Время работы

Утверждается, что время работы алгоритма — $O(n \log^r n)$, где $n = 2^m$ — длина кода.

