

Код Рида-Маллера

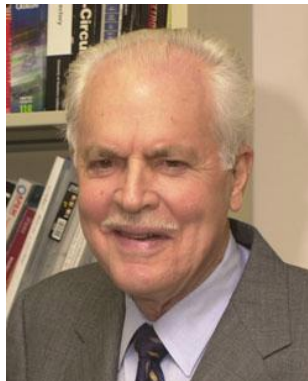
Илья Коннов

Факультет компьютерных наук

Высшая Школа Экономики

15 марта 2022 г.

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



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

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

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

Булевы функции и многочлен Жегалкина

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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:

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

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 $m = 2$: $f(x_1, x_2) = c_{\{1,2\}} \cdot x_1 x_2 + c_{\{2\}} \cdot x_2 + c_{\{1\}} \cdot x_1 + c_{\emptyset} \cdot 1$
Всего $n = 2^m$ коэффициентов для описания каждой функции.

Функции небольшой степени

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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?

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

Идея кодирования

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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

Пример

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

- $r = 1$ (степень многочлена), $m = 2$ (переменных).
Это $RM(1, 2)$.
- 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: $\text{Eval}(f) = 1100$.

Декодирование когда потерь нет

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

- Мы получили код: 1100
- Представим таблицу истинности.

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

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

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

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

Коды 0-го порядка

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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	$f(x_1, \dots, x_m)$	$g(x_1, \dots, x_m)$
2^m	0	0	\dots	0	0	1
	0	0	\dots	1	0	1
			\ddots		\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 $\underbrace{11\dots1}_{2^m}$

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 $\text{RM}(m, m)$ 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.

Доказательство линейности

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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

- 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:

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

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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

Минимальное расстояние

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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,

$$w(\underbrace{11\dots 1}_{2^m}) = 2^m = 2^{m-0} \geq 2^{m-r}.$$

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

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

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

Код с весом 2^{m-r}

Код

Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

Дано: $\text{RM}(r, m)$, $0 \leq r \leq m$

Хотим: такой $c \in \text{RM}(r, m)$, что $w(c) = 2^{m-r}$

Рассмотрим функцию:

$$f(x_1, x_2, \dots, x_m) = \prod_{i=1}^r x_i = x_1 x_2 \dots x_r$$

В её таблице истинности ровно 2^{m-r} строк, когда $f(\dots) = 1$:

r				$m-r$			f
x_1	x_2	\dots	x_r	x_{r+1}	\dots	x_m	
1	1	\dots	1	*	\dots	*	1
\vdots	\vdots	\ddots	\vdots	\vdots	\ddots	\vdots	\vdots
1	1	\dots	1	*	\dots	*	1

Для бинарного кода $RM(r, m)$:

- $0 \leq r \leq m$
- 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 $RM(m - r - 1, m)$

Возможные варианты

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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

Как линейный код

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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: $s = rH^T$.

- 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...
- $\mathbb{F}_2^m = \{000, 001, 010, 011, 100, 101, 110, 111\}$
- $V_A = \{000, 010, 100, 110\} \ (v_3 = 0 \ \forall v)$
- $\bar{A} = \{1, 2, 3\} \setminus A = \{3\}$
- $V_{\bar{A}} = \{000, 001\} \ (v_1 = v_2 = 0 \ \forall v)$

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).

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

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

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

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

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

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

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

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

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

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

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

Считаем количество (c) смежных классов, в которых

$$\sum_{z \in (V_A + b)} y_z = 1 \pmod{2}.$$

Пороговое значение (2^{m-t-1})

здесь — половина от числа

смежных классов. Таким

образом, если большинство

сумм дало 1, то $u_A = 1$, иначе

$u_A = 0$.

Алгоритм Рида для кода $RM(r, m)$

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритм Рида

Пример

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

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

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

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

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.

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

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

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: $u_A = u_{\{1\}} = 1$

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: $u_A = u_{\{2\}} = 0$

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 $\text{Eval}(g)$:

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

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

Продолжение примера: $t = 0$

Код
Рида-Маллера

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

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

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: $u_A = u_{\emptyset} = 1$

Продолжение примера: $t = 0$

Код
Рида-Маллера

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.

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

Код
Рида-Маллера

Введение

Кодирование

Свойства кода

Минимальное
расстояние

Параметры

Декодирование

Алгоритмы Рида

Пример

Спасибо за внимание