Код Рида-Маллера

Илья Коннов

9 февраля 2022 г.

Если вы смотрите презентацию, то на сером фоне справа 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. 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.

Содержание

1 Введение

Введение

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

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

Традиционно, считается что коды работают над битами, т.е. $\mathbb{Z}_2$.

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:

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

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.

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.

Замечу, что при $S = \varnothing$, мы считаем, что $\prod_{i \in S} x_i = 1$, таким образом всегда появляется свободный член.

Сколько тогда всего коэффициентов используется?

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

Если говорить несколько проще, то для составления многочленов мы сложим сначала одночлены $(x + y + z)$, затем произведения одночленов $(xy + yz + xz)$ и т.д. вплоть до r множителей. 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

2 Кодирование

Идея кодирования

Пусть каждое сообщение (длины k) — коэффициенты некоторого многочлена от m переменных степени не больше r.

Тогда мы можем его представить при помощи 2^n бит, подставив все возможные комбинации переменных (ведь рассматриваем многочлены над $\mathbb{Z}_2$).

Таким образом получим таблицу истинности, из которой позднее сможем восстановить исходный многочлен, а вместе с ним и сообщение.

Пример

- $r = 1$ (степень многочлена), $m = 2$ (переменных).Это 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: `1100`.

3 Свойства кода

Линейность

> Линейный (блоковый) код — такой код, что множество его кодовых слов образует k-мерное линейное подпространство в n-мерном линейном пространстве, изоморфное пространству k-битных векторов.

Слова —

4 Декодирование

Потерь нет