Расширенный код Голея. Коды Рида-Маллера

Гошин Егор Вячеславович

Самарский университет

25 сентября 2020 г.

Расширенный код Голея

Рассмотрим матрицу

$$B = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

Свойства расширенного кода Голея

Определим матрицу расширенного кода Голея $G = \begin{bmatrix} I & B \end{bmatrix}$, где I – единичная матрица 12×12.
Код Голея обладает следующими свойствами:
(1) Длина C_{24} равна 24, размерность – 12 и он содержит $2^{12} = 4096$ кодовых слов.
(2) Проверочная матрица $H = \begin{bmatrix} I \\ B \end{bmatrix}$.
(3) Кодовое расстояние расширенного кода Голея равно 8. Соответственно, этот код позволяет исправлять трёхкратные ошибки.

Алгоритм декодирования

Код Голея интересен тем, что имеет довольно простой и эффективный алгоритм декодирования.

(1) Вычислить синдром $s = wH$

(2) Если $wt(s) \leq 3$, то $u = [s, 0]$.

(3) Если $wt(s + b_i) \leq 2$ для какой-либо строки b_i из B, тогда $u = [s + b_i, e_i]$.

(4) Вычислить второй синдром sB.

(5) Если $wt(sB) \leq 3$, тогда $u = [0, sB]$.

(6) Если $wt(sB + b_i) \leq 2$ для какой-либо строки b_i из B, тогда $u = [e_i, s + b_i]$

(7) Если u до этого момента не определена, то ошибка не подлежит исправлению, запросить повторную передачу.

Пример

Декодировать $w = 101.111.101.111\ 010.010.010.010$
Вычислим синдром
$s = wH = 101.111.101.111 + 001.111.101.110 = 100.000.000.001.$
Вес синдрома 2, поэтому ошибка
$u = 100.000.000.001\ 000.000.000.000$
И переданное сообщение $v = 001.111.101.110\ 010.010.010.010$

Пример

Декодировать $w = 001.001.001.101\ 101.000.101.000$.
Вычислим синдром
$s = wH = 001.001.001.101 + 111.000.000.100 = 110.001.001.001$.
Вес синдрома равен 5, поэтому переходим к следующему шагу алгоритма.
$s + b_1 = 000.110.001.100$
$s + b_2 = 011.111.000.010$
$s + b_3 = 101.101.011.110$
$s + b_4 = 001.001.100.100$
$s + b_5 = 000.000.010.010$
Поскольку $wt(s + b_5) = 2$, ошибка
$u = 000.000.010.010\ 000.010.000.000$
И переданное сообщение $v = 001.001.011.111\ 101.010.101.000$.

Коды Рида-Маллера

В этой лекции рассмотрим ещё один важный класс кодов (включающий в себя расширенные коды Хэмминга). Код Рида-Маллера длины 2^m будем обозначать $RM(r,m)$, где r и m – целые числа, удовлетворяющие условию $0 \leq r \leq m$.

Рассмотрим рекурсивное определение этих кодов:

(1) $RM(0,m) = 00...0, 11...1$,

$RM(m,m) = K^{2^m}$ (где $K = \{0,1\}$).

(2) $RM(r,m) = \{(x, x+y) | x \in RM(r, m-1), y \in RM(r-1, m-1)\}$, $0 < r < m$.

Пример

Таким образом:
$RM(0,0) = \{0,1\}$
$RM(0,1) = \{00,11\}, RM(1,1) = K^2 = \{00,01,10,11\},$
$RM(0,2) = \{0000,1111\}, RM(2,2) = K^4 = \{0000,0001,...,1111\},$
$RM(1,2) = \{(x,x+y)\}|x \in RM(1,1), y \in RM(0,1) =$
$\{0000,0011,0101,0110,1010,1001,1111,1100\}.$

Правило формирования порождающей матрицы

Вместо того, чтобы использовать такое определение кода в явном виде, мы зададим рекурсивное правило формирования порождающей матрицы кода $RM(r,m)$, которую мы будем обозначать $G(r,m)$. Для $0 < r < m$ матрица $G(r,m)$ определяется как

$$G(r,m) = \begin{bmatrix} G(r,m-1) & G(r,m-1) \\ 0 & G(r-1,m-1) \end{bmatrix}$$

Для $r = 0$ определим

$$G(0,m) = [11...1],$$

а для $r = m$

$$G(m,m) = \begin{bmatrix} G(m-1,m) \\ 0....01 \end{bmatrix}$$

Пример

Порождающие матрицы для $RM(0,1)$ и $RM(1,1)$ равны

$$G(0,1) = \begin{bmatrix} 1 & 1 \end{bmatrix}$$

$$G(1,1) = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Пример

Пусть $m = 2$, тогда длина равна $2^2 = 4$ и для $r = 1, 2$ получаем

$$G(1,2) = \begin{bmatrix} G(1,1) & G(1,1) \\ 0 & G(0,1) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G(2,2) = \begin{bmatrix} G(1,2) \\ 0001 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Пример

$$G(0,3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Пример

$$G(2,3) = \begin{bmatrix} G(2,2) & G(2,2) \\ 0 & G(1,2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$G(3,3) = \begin{bmatrix} G(2,3) \\ 00000001 \end{bmatrix}$$

Базовые свойства кода Рида-Маллера

(1) Длина кода Рида-Маллера равна $n = 2^m$
(2) Кодовое расстояние $d = 2^{m-r}$
(3) Размерность кода $k = \sum\limits_{i=0}^{r} C_m^i$.
(4) $RM(r-1, m)$ полностью содержится в $RM(r, m)$, $r > 0$.

Порождающая матрица

Рассмотрим код Рида-Маллера первого порядка $RM(1,m)$. Заметим, что код $RM(1,m)$ – это довольно короткий код с большим кодовым расстоянием, поэтому хорошим декодирующим алгоритмом является одновременно и самый простой: для каждого полученного кодового слова w найти кодовое слово из $RM(1,m)$, наиболее близкое к нему. Это можно сделать очень эффективно.

Пример

Пусть $m = 3$. Рассмотрим код $RM(1,3)$ длины 8 с 16 кодовыми словами. Минимальное кодовое расстояние равно 4.

$$G(1,3) = \begin{bmatrix} G(1,2) & G(1,2) \\ 0 & G(0,2) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Заметим, что если получено слово w и $d(w,c) < 2$, мы можем декодировать w в c. Более того, если $d(w,c) > 6$, то $d(w, 1+c) < 2$ и можно декодировать w в $1+c$. К примеру, получено слово $w = 1000111$. Для него $c = 00001111$ – ближайшее. Если получено слово $w = 10101011$ и мы нашли $c = 01010101$, то ближайшее кодовое слово – $c + 1 = 10101010$. Таким образом, нам необходимо будет рассмотреть не больше половины кодовых слов в $RM(1,m)$.

Быстрое декодирование для $RM(1, m)$

Кратко и без доказательства рассмотрим очень эффективный алгоритм декодирования для $RM(1, m)$. Он использует быстрое преобразование Адамара для поиска ближайшего кодового слова. Определим произведение Кронекера как $A \times B = [a_{ij}B]$. При этом каждый элемент a_{ij} в матрице A заменяется матрицей $a_{ij}B$.

Пример

Пусть $H = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ и $I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

тогда

$$I_2 \times H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

$$H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Декодирующие матрицы

Рассмотрим набор матриц, определённых как

$$H_m^i = I_{2^{m-i}} \times H \times I_{2^{i-1}}$$

для $i = 1, 2, ..., m$, где H – как в предыдущем примере.

Пример

Пусть $m = 2$, тогда

$$H_2^1 = I_2 \times H \times I_1 = I_2 \times H$$

$$H_2^2 = I_1 \times H \times I_2 = H \times I_2$$

Пример

Пусть $m = 3$

$$H_3^1 = I_4 \times H \times I_1 = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{bmatrix}$$

Пример

$$H_3^2 = I_2 \times H \times I_2 = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

Пример

$$H_3^3 = I_1 \times H \times I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{bmatrix}$$

Алгоритм декодирования

Рекурсивный характер формирования кода $RM(1,m)$ позволяет предположить, что существует и рекурсивный подход к декодированию.

Алгоритм. Предположим, что получено сообщение w и $G(1,m)$ – порождающая матрица кода $RM(1,m)$.

(1) заменим 0 на -1 в w, сформировав $\hat{w}$

(2) вычислим $w_1 = \hat{w}H_m^1$ и $w_i = w_{i-1}H_m^i$ для $i = 2,3\ldots,m$.

(3) Найдём положение j наибольшего компонента по абсолютному значению в w_m.

Пусть $v(j) \in K^m$ – двоичное представление j с младшими разрядами слева. Тогда если j-я компонента w_m положительна, тогда исходное сообщение – $(1, v(j))$, иначе – $(0, v(j))$.

Пример

Пусть $m = 3$ и $G(1,3)$ порождающая матрица $RM(1,3)$. Пусть было получено сообщение $w = 10101011$.
(1) Преобразуем его в $\hat{w} = [1, -1, 1, -1, 1, -1, 1, 1]$.
(2) Вычислим:
$w_1 = \hat{w}H_3^1 = [0, 2, 0, 2, 0, 2, 2, 0]$
$w_2 = w_1H_3^2 = [0, 4, 0, 0, 2, 2, -2, 2]$
$w_3 = w_2H_3^3 = [2, 6, -2, 2, -2, 2, 2, -2]$

Пример

Было получено сообщение $w = 10101011$.
$w_3 = w_2 H_3^3 = [2, 6, -2, 2, -2, 2, 2, -2]$.
$j = 1, v(1) = 100, j > 0$, следовательно, исходное сообщение –
$m = (1100)$

Пример

Пусть было получено сообщение $w = 10001111$.
(1) Преобразуем его в $\hat{w} = [1, -1, -1, -1, 1, 1, 1, 1]$.
(2) Вычислим:
$w_1 = \hat{w}H_3^1 = [0, 2, -2, 0, 2, 0, 2, 0]$
$w_2 = w_1H_3^2 = [-2, 2, 2, 2, 4, 0, 0, 0]$
$w_3 = w_2H_3^3 = [2, 2, 2, 2, -6, 2, 2, 2]$

Пример

Было получено сообщение $w = 10001111$.
$w_3 = w_2 H_3^3 = [2, 2, 2, 2, -6, 2, 2, 2]$.
$j = 4$, $v(1) = 001$, $j > 0$, следовательно, исходное сообщение – $m = (0001)$