Коды Рида-Маллера

Гошин Егор Вячеславович

Самарский университет

25 сентября 2020 г.

Коды Рида-Маллера

Для линейных кодов Рида-Маллера $RM(r, m)$:

$$n = 2^m,$$

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

и

$$d = 2^{m-r}.$$

Рассмотрим альтернативный способ построения кодов Рида-Маллера, более подходящий для декодирования.

Обозначим координатные позиции в словах длины $n = 2^m$ векторами K^m ($K = \{0, 1\}$). Каждой позиции i поставим в соответствие двоичное представление целого числа i с использованием m разрядов с цифрами, **расположенными в обратном порядке** (как для циклических кодов).

Например:
$\{0, 1, 2, 3, 4, 5, 6, 7\} \leftrightarrow \{000, 100, 010, 110, 001, 101, 011, 111\}$

Любая функция, преобразующая K^m в $\{0,1\}$ может быть единственным образом представлена в векторной форме $v = (f(u_0), f(u_1), ..., f(u_{2^m-1})) \in K^n$, где $u_i \in K^m$, $n = 2^m$ и u_i – двоичные представления векторов из K^m.
Рассмотрим конкретный класс базисных функций. Пусть задано подмножество $I \subseteq \{0,1,...,m-1\}$. Определим функцию

$$f_I(x_0, x_1, ..., x_2) = \begin{cases} \prod_{i \in I} (x_i + 1), & I \neq 0, \\ 1, & I = 0. \end{cases}$$

f_I – это функция, отображающая K^m на $\{0,1\}$. Определим v_I как соответствующую векторную форму f_I.

Пусть $m = 3$, тогда $n = 2^3 = 8$
Если $I = \{1, 2\}$, тогда $f_I(x_0, x_1, x_2) = (x_1 + 1)(x_2 + 1)$. Векторная форма $f_{\{1,2\}}(x_0, x_1, x_2)$ формируется посредством выбора всех возможных комбинаций элементов $x_0x_1x_2 \in K^3$ (с использованием ранее введённого бинарного представления) и вычисления для них $f_{\{1,2\}}(x_0x_1x_2)$. Таким образом:
$f_{\{1,2\}}(0, 0, 0) = 1,$
$f_{\{1,2\}}(1, 0, 0) = 1,$
$f_{\{1,2\}}(0, 1, 0) = 0,$
$f_{\{1,2\}}(1, 1, 0) = 0,$
$f_{\{1,2\}}(0, 0, 1) = 0,$
$f_{\{1,2\}}(1, 0, 1) = 0,$
$f_{\{1,2\}}(0, 1, 1) = 0,$
$f_{\{1,2\}}(1, 1, 1) = 0.$
Таким образом, $v_{\{1,2\}} = 11000000.$

Если $I = \{0\}$, тогда $f_{\{0\}}(x_0, x_1, x_2) = (x_0 + 1)$. И $v_{\{0\}} = 10101010$.
Если $I = \emptyset$, тогда $f_{\emptyset}(x_0, x_1, x_2) = 1$. И $v_{\emptyset} = 11111111$.

Два важных свойства f_I, которые мы дальше будем использовать.
(1) $f_I(x_0, x_1, ..., x_{m-1}) = 1$ тогда и только тогда, когда $x_i = 0$ для всех $i \in I$.
Так, в примере для $I = \{1, 2\}$. $f_{\{1,2\}} = 1$ только в случае $f(x_0, 0, 0)$, где $x_0 \in \{0, 1\}$.

(2) Для каждого $u_i \in K^m$: $f_I(u_i)f_J(u_i) = f_{I \cup J}(u_i)$ и, следовательно:

$$v_I v_J = \sum_{i=0}^{2^m-1} f_I(u_i)f_J(u_i) = \sum_{i=0}^{2^m-1} f_{I \cup J}(u_i) = wt(v_{I \cup J})(mod\ 2).$$

Будем обозначать множество целых чисел $\{0, 1, 2, ..., m-1\}$ как Z_m.

Код Рида-Маллера $RM(r,m)$ может быть определён как линейный код $(\{v_I | I \subseteq Z_m, |I| \leq r\})$.
Можно показать, что $S = \{v_I | I \subseteq Z_m, |I| \leq r\}$ – линейно независимое множество и, следовательно, может быть базисом $RM(r,m)$.
Простой подсчёт слов v_I для $I \subseteq Z_m$ и $|I| \leq r$ даёт нам

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

и, очевидно,

$$n = 2^m.$$

Кодовые слова v_I могут быть расположены в любом порядке для формирования порождающей матрицы $RM(r,m)$. Определим каноническую форму матрицы $G_{r,m}$ следующим образом. Строки этой матрицы упорядочены так, что v_I идёт раньше v_J если:

(1) $|I| < |J|$

либо

(2) $|I| = |J|, \quad f_I(u_j) < f_J(u_j)$ и $f_I(u_i) = f_J(u_i)$ при $i > j$.

Порождающая матрица для $RM(4,4)$ в канонической форме – это $G_{4,4}$

Пример

$$G_{4,4} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} v_{\emptyset} \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_{2,3} \\ v_{1,3} \\ v_{0,3} \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \\ v_{1,2,3} \\ v_{0,2,3} \\ v_{0,1,3} \\ v_{0,1,2} \\ v_{0,1,2,3} \end{matrix}$$

Кодирование, как и для любого линейного кода производится посредством умножения ссобщения на $G_{r,m}$.
В этом случае любое кодовое слово может быть записано в виде

$$c = \sum_{J \subseteq Z_m, |I| \leq r} m_I v_I,$$

где разряды сообщения обозначены m_I, чтобы соответствовать строкам v_I матрицы $G_{r,m}$.

Пример. Закодировать следующие сообщения m с использованием матрицы $G_{2,4}$.

(a) Если входное сообщение равно $m = 10000001000$ (то есть, $m_\emptyset = 1$ и $m_{\{0,3\}} = 1$), тогда

$c = v_\emptyset + v_{0,3} = 0101010111111111$

$$G_{2,4} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{bmatrix} \begin{matrix} v_\emptyset \\ v_3 \\ v_2 \\ v_1 \\ v_0 \\ v_{2,3} \\ v_{1,3} \\ v_{0,3} \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \end{matrix}$$

$$c_2 = m_\emptyset + m_3 + m_2 + m_0 + m_{2,3} + m_{0,3} + m_{0,2},$$
$$c_3 = m_\emptyset + m_3 + m_2 + m_{2,3},$$
$$c_6 = m_\emptyset + m_3 + m_0 + m_{0,3},$$
$$c_7 = m_\emptyset + m_3$$
$$c_2 + c_3 + c_6 + c_7 = m_{0,2}$$

$$m_{0,2} = c_0 + c_1 + c_4 + c_5$$
$$m_{0,2} = c_2 + c_3 + c_6 + c_7$$
$$m_{0,2} = c_8 + c_9 + c_{12} + c_{13}$$
$$m_{0,2} = c_{10} + c_{11} + c_{14} + c_{15}$$

Декодирование Рида-Маллера

Декодирование Рида-Маллера производится посредством процесса известного как мажоритарное декодирование.
Для любого $I \subseteq Z_m$ определим комплементарное множество $I^c = Z_m \backslash I$
Пусть $H_I = \{u \in K^m | f_I(u) = 1\}$. Как мы заметили ранее, $f_I(x_0, ..., x_{m-1}) = 1$ тогда и только тогда, когда $x_i = 0$ для всех $i \in I$. Очевидно, если $x, y \in H_I$, тогда $x_i = y_i = 0 = x_i + y_i$ для всех $i \in I$, поэтому $x + y \in H_I$. Следовательно, H_I – подпространство K^m.

Для любого $u = (x_0, x_1, x_{m-1}) \in K^m$ и любого
$t = (t_0, t_1, t_{m-1}) \in K^m$ определим функцию
$f_{I,t}(x_0, x_1, x_{m-1}) = f_I(x_0 + t_0, x_1 + t_1, x_{m-1} + t_{m-1}) = f_I(x + t)$ и
соответствующую ей векторную форму $v_{I,t}$.

Попробуем определить значение $v_{I,s} \cdot v_{J^c,t}$. Для этого подсчитаем число слов $u \in K^m$, для которых $f_{I,s}(u) f_{J^c,t}(u) = 1$.
По определению H_I: $f_{I,t}(u) = f_I(u+t) = 1$ тогда и только тогда, когда $u + t = u' \in H_I$ или, что эквивалентно, $u = u' + t \in H_I + t$, где $H_I + t$ – класс смежности H_I по t.

При этом значение
$f_{I,s}(u)f_{J^c,t}(u) = \prod_{i\in I}(x_i + s_i + 1)\prod_{j\in J^c}(x_j + t_j + 1)$ остаётся постоянным для всех возможных $x_k \in \{0, 1\}, k \in Z_m \setminus (I \cup J^c)$. Поскольку существует $2^{m-|I\cup J^c|}$ таких возможных u (потому что u принимает значения из K^m), то число случаев, когда

$$f_{I,s}(u)f_{J^c,t}(u) = 1$$

делится на $2^{m-|I\cup J^c|}$ и, следовательно, чётно, кроме случая, когда $|I \cup J^c| = m$ или, что то же самое, $I \cup J^c = Z_m$.

Однако, если предположить, что $|I| \leq |J|$, то $|J^c| \leq |I^c|$.
Тогда $|I \cup J^c| = |I| + |J^c| - |I \cap J^c| < m$ кроме случая, когда $I = J$.
Если $I = J$, тогда существует единственный $u \in K^m$, для которого $f_{I,s}(u)f_{J^c,t}(u) = 1$, а именно u, для которого $x_i = s_i$ для всех $i \in I$ и $x_i = t_i$ для всех $i \in I^c$.

Ещё раз обратим внимание, что число позиций, для которых $f_{I,s}(u)f_{J^c,t}(u) = 1$, даёт $v_{I,s} \cdot v_{J^c,t}$. В результате получаем следующее утверждение.

Лемма 1

Пусть I и J подмножества Z_m с $|I| \leq |J|$. Для любого $s \in H_{I^c}$ и для любого $t \in H_J$:

$$v_{I,s} \cdot v_{J^c,t} = 1$$

тогда и только тогда, когда $I = J$.

Теперь получим следующее утверждение, которое послужит основой для алгоритма декодирования.

Следствие 2

Если c – кодовое слово в $RM(r,m)$ и если $|J| = r$, тогда $m_J = c \cdot v_{J^c,t}$ для любого $t \in H_J$.

Доказательство:

Если $|J| = r$ тогда для любого $t \in H_J$:

$$c \cdot v_{J^c,t} = \sum_{I \subseteq Z_m, |I| \leq r} m_I v_I \cdot v_{J^c,t} = m_J v_J \cdot v_{J^c,t} = m_J$$

поскольку по Лемме 1 единственное скалярное произведение в сумме не равное нулю – то, для которого $I = J$.

Лемма 3. Пусть $J \subseteq Z_m$. Для любого слова e (длины 2^m) $e \cdot v_{J^c,t} = 1$ не больше, чем для $wt(e)$ значений $t \in H_J$.

И, наконец, перейдём к алгоритму декодирования.
Пусть $w = c + e$ – полученное слово, где c – кодовое слово из $RM(r, m)$, то есть $c = \sum_{I \subseteq Z_m} m_I v_I)$, где $|I| \leq r$. Тогда по лемме 3 $e \cdot v_{J^c,t} = 0$ по меньшей мере для $|H_j| - wt(e)$ значений t из H_J. Для таких значений имеем:

$$w \cdot v_{J^c,t} = c \cdot v_{J^c,t} + e \cdot v_{J^c,t} = c \cdot v_{J^c,t} = m_J$$

Таким образом, если $2wt(e) < |H_J|$, то при присвоении t различных значений из H_J, больше половины значений $w \cdot v_{J^c,t}$ будут равны m_J.

Как только мы вычислим таким образом m_J для всех $J \subseteq Z_m$ с $|J| = r$ определим $w(r-1) = w + \sum_{|J|=r} m_J v_J$. Теперь декодируем $w(r-1)$ как будто это слово, принятое кодом $RM(r-1, m)$. Этот процесс может быть продолжен, пока не будут найдены m_J для всех $J \subseteq Z_m$ при $|J| \leq r$.

Прежде чем привести алгоритм в итогой форме, заметим, что этот алгоритм исправляет все шаблоны ошибок веса меньше, чем $|H_J|/2$, где $|J| \leq r$. Однако, можно показать, что $|H_J| = wt(v_J) = 2^{m-|J|}$. Поэтому все шаблоны ошибок кратности меньше, чем 2^{m-r-1} исправляются этим кодом и, следовательно, минимальное кодовое расстояние кода Рида-Маллера $RM(r,m)$ равно по меньшей мере 2^{m-r}. Однако, если $I \subseteq Z_m$ и $|I| = r$, тогда v_I – кодовое слово в $RM(r,m)$ и имеет вес Хэмминга 2^{m-r}, что значит:

Лемма 4. Минимальное кодовое расстояние кода Хэмминга равно 2^{m-r}

Алгоритм мажоритарного декодирования

Пусть получено сообщение w.
1. Пусть $i = r$ и пусть $w(r) = w$.
2. Для каждого $J \subseteq Z_m$ с $|J| = i$ вычислим $w(i) \cdot v_{J^c,t}$ для каждого $t \in H_J$, пока либо 0, либо 1 не появится больше, чем 2^{m-i-1} раз. В этом случае назначим m_J значение 0 или 1, соответственно.
Если 0 и 1 оба появились $e = 2^{m-r-1}$ раз – запросить повторную отправку сообщения.
3. Если $i > 0$, тогда $w(i-1) = w(i) + \sum_{J \subseteq Z_m} m_J v_J$, где $|J| = i$.
Если $w(i-1)$ имеет вес не больше $e = 2^{m-r-1} - 1$, тогда $m_J = 0$ для всех $J \subseteq Z_M$ с $|J| \leq r$ и остановить алгоритм.
Иначе, заменить i на $i-1$ и перейти к шагу 2. (Если $i = 0$, тогда m_J было вычислено для всех $J \subseteq Z_m$ с $|J| \leq r$ и наиболее вероятное сообщение было найдено).

Пример

Пусть получено слово $w = 0101.0111.1010.0000$, закодированное с помощью $G_{2,4}$.
Начнём с $i = r = 2$ и $w(2) = w$.
Получим $m_{2,3} = 0$, $m_{1,3} = 0$, $m_{0,3} = 0$, $m_{1,2} = 0$, $m_{0,2} = 1$ и $m_{1,2} = 0$.
Тогда $w(1) = w(2) + v_{0,2} = 1111.0111.0000.0000$ и $i = 1$.
После очередного шага вычислений получим $m_3 = 1$, $m_2 = 0$, $m_1 = 0$ и $m_0 = 0$.
Пусть $w(0) = w(1) - v_3 = 0000.1000.0000.0000$ и пусть $i = 0$.
Поскольку $w(0)$ имеет вес не выше $e = 1$, обозначим $m_\emptyset = 0$ и остановимся.
Таким образом, наиболее вероятное отправленное сообщение равно

$$0.1000.000010.$$

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{0,1}	0000	1111 0000 0000 0000	0	
	0010	0000 1111 0000 0000	1	0
	0001	0000 0000 1111 0000	0	
	0011	0000 0000 0000 1111	0	
{0,2}	0000	1100 1100 0000 0000	0	
	0100	0011 0011 0000 0000	1	1
	0001	0000 0000 1100 1100	1	
	0101	0000 0000 0011 0011	1	
{1,2}	0000	1010 1010 0000 0000	1	
	1000	0101 0101 0000 0000	0	0
	0001	0000 0000 1010 1010	0	
	1001	0000 0000 0101 0101	0	

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{0,3}	0000	1100 0000 1100 0000	0	
	0100	0011 0000 0011 0000	0	0
	0010	0000 1100 0000 1100	1	
	0110	0000 0011 0000 0011	0	
{1,3}	0000	1010 0000 1010 0000	0	
	1000	0101 0000 0101 0000	0	0
	0010	0000 1010 0000 1010	1	
	1010	0000 0000 0101 0101	0	
{2,3}	0000	1000 1000 1000 1000	1	
	1000	0100 0100 0100 0100	0	0
	0100	0010 0010 0010 0010	0	
	1100	0001 0001 0001 0001	0	

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{0}	0000	1100 0000 0000 0000	0	
	0100	0011 0000 0000 0000	0	
	0010	0000 1100 0000 0000	1	0
	0110	0000 0011 0000 0000	0	
	0001	0000 0000 1100 0000	0	
	0101	0000 0000 0011 0000	0	
	0011	0000 0000 0000 1100		
	0111	0000 0000 0000 0011		
{1}	0000	1010 0000 0000 0000	0	
	1000	0101 0000 0000 0000	0	
	0010	0000 1010 0000 0000	1	0
	1010	0000 0101 0000 0000	0	
	0001	0000 0000 1010 0000	0	
	1001	0000 0000 0101 0000	0	
	0011	0000 0000 0000 1010		
	1011	0000 0000 0000 0101		

J	t	$v_{J^c,t}$	$w \cdot v_{J^c,t}$	m_J
{2}	0000	1000 1000 0000 0000	1	
	1000	0100 0100 0000 0000	0	
	0100	0010 0010 0000 0000	0	0
	1100	0001 0001 0000 0000	0	
	0001	0000 0000 1000 1000	0	
	1001	0000 0000 0100 0100	0	
	0101	0000 0000 0010 0010		
	1101	0000 0000 0001 0001		
{3}	0000	1000 0000 1000 0000	1	
	1000	0100 0000 0100 0000	1	
	0100	0010 0000 0010 0000	1	1
	1100	0001 0000 0001 0000	1	
	0010	0000 1000 0000 1000	0	
	1010	0000 0100 0000 0100	1	
	0110	0000 0010 0000 0010		
	1110	0000 0001 0000 0001		