Булевый код Рида-Маллера

(обобщение кода RS на мн-ны от нескольких переменных)

$\exists (v_1 .. v_m) \in \mathbb{F}_2^m$

$\forall$ ф-ия $f(v) = f(v_1 .. v_m)$, приним. значения в $\mathbb{F}_2$ – булева ф-ия.

степень монома $v_1^{k_1} \dots v_m^{k_m}$ определяется как $k_1 + .. + k_m$

степень мн-на f, $\deg(f)$, – макс. степень его мономов.

f может быть задана, например, таблицей истинности. $\Rightarrow$ вектором длины 2^m:

v_1	0	0	1	1
v_2	0	1	0	1
	$f(00)$	$f(01)$	$f(10)$	$f(11)$

$f = a_0 \vec{1} + a_1 \vec{v}_1 + a_2 \vec{v}_2$

$a_i \in \{0, 1\}$.

Опр-ие Для $0 < r \leq m$, двоичный код Рида-Маллера длины $n = 2^m$ и <u>порядка</u> r:

$$RM(m, r) = \{ f \in \mathbb{F}_2 [x_1 .. x_m] \mid \deg f \leq r \}$$

m – число переменных
r – макс. степень
$n = 2^m$ – длина кода

Пример $m = 2$, $r = 1$ $\Rightarrow n = 4$

$c \in RM(2,1) \Leftrightarrow c = a_0 \vec{1} + a_1 \vec{v}_1 + a_2 \vec{v}_2$

$a_i \in \{0, 1\}$
$v_1 = 0011$
$v_2 = 0101$

a_0, a_1, a_2		c
0 0 0	$\vec{0}$	0000
0 0 1	v_2	0101
0 1 0	v_1	0011
0 1 1	$v_1 + v_2$	0110
1 0 0	$\vec{1}$	1111
1 0 1	$\vec{1} + v_2$	1010

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

110 $\quad 1+v_1 \quad$ 1100

111 $\quad 1+v_1+v_2 \quad$ 1001

РАЗМЕРНОСТЬ кода $RM(m,r)$ = р-р базиса многочленов над $\mathbb{F}_2$ степени $\leq r$, т.е. кол-во мономов степени 0 (=1), степени 1 (таких m: $v_1 .. v_m$), мономов степени 2 ($v_1v_2, v_1v_3 .. v_{m-1}v_m$).

$$\text{Всего } k = \underbrace{\binom{m}{0}}_{=1} + \underbrace{\binom{m}{1}}_{=m} + \binom{m}{2} + .. + \binom{m}{r}$$

(Если $m=r$, $k=2^m$)

в примере: $m=2, r=1$, $k = 1+2 = 3$

ТЕОРЕМА 1 $RM(m+1, r+1) = \{[u|u+v] \mid u \in RM(m, r+1), v \in RM(m,r)\}$

Эквивалентно,

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

$\triangleleft$ $f \in RM(m+1, r+1)$ - мн-н $f(x_1 .. x_{m+1})$, $\deg f \leq r+1$

$$f(x_1 .. x_{m+1}) = \underbrace{g(x_1 .. x_m)}_{\in RM(m, r+1)} + x_{m+1} \underbrace{h(x_1 .. x_m)}_{RM(m,r)}$$

Если $\ast$ g и $h \cdot x_{m+1}$ как мн-ны от $x_1 .. x_{m+1}$, то им соответствуют векторы длины 2^{m+1}

$g \to [g|g]$

$h \to [0|h]$

v_1	0	0	1	1
v_2	0	1	0	1
	g_0	g_1	g_2	g_3
	h_0	h_1	h_2	h_3

v_3	0	0	0	0	1	1	1	1
v_1	0	0	1	1	0	0	1	1
v_2	0	1	0	1	0	1	0	1
	g_0	g_1	g_2	g_3	g_0	g_1	g_2	g_3

$\Rightarrow \quad f = [g|g] + [0|h] = [g|g+h]$ ▶

Теорема 2

Мин. расстояние кода $d(RM(m,r)) = 2^{m-r}$

◁ По индукции по m.

$d=2 \quad a_0 \vec{1} \geq$

$\exists\, m=1 \quad RM(1,0)$ – константный код длины $2^m = 2$ $\{00, 11\}$

$RM(1,1):\ a_0\vec{1} + a_1\vec{v}_1 = \{00, 01, 11, 10\}$

$\vec{v}_1 = 01$, $d=1$

Лемма $\exists\, C_1$ – лин. $[n, k_1, d_1]$-код

C_2 – лин $[n, k_2, d_2]$-код

$C_3 = \{[u|u+v],\ u \in C_1,\ v_2 \in C_2\}$

C_3 – лин. $[2n,\ k_1+k_2,\ d_3 = \min\{2d_1, d_2\}]$-код

◁ $a = [u|u+v]$, $b = [u'|u'+v'] \in C_3$

Если $v = v'$, то $\Delta(a,b) = 2\,dist(u,u') \geq 2d_1$

Иначе, $\exists\, v \neq v'$ используем н-во треугольника

$(\Delta(x,y) \leq \Delta(x,w) + \Delta(w,y))$

$wt(x+y) \leq wt(x+w) + wt(w+y) \Rightarrow$

$wt(x+y) \geq wt(x) - wt(y)$, т.к.

$wt(x+y) + wt(y) \geq wt(x) \Leftrightarrow$

$wt(x) \leq wt(x+y) + wt(y)$

т.е. имеем $wt(x+y) \geq wt(x) - wt(y)$

$\Delta(a,b) = wt(u-u') + wt(\underbrace{u+v-(u'+v')}_{u-u'+v-v'}) \geq \cancel{wt(u-u')} + wt(v-v') - \cancel{wt(u-u')} = wt(v-v') \geq d_2$

Пусть $m = m'$ и для всех $r \le m'$ выполняется $d(RM(m', r)) = 2^{m'-r}$

док-м, для $m = m'+1$ и для всех r: $\underset{r \le m'+1}{RM(m'+1, r)} = RM(m'+1, r'+1)$

$r' := r-1$

$r' \le m'$

Теорема 1 $\{ [u|u+v] \mid u \in RM(m', r'+1), v \in RM(m', r') \}$

$$d(RM(m'+1, r)) \overset{\text{лемма}}{=} \min\{2d(RM(m', r'+1)), d(RM(m', r'))\}$$

$$= \min\{2 \cdot 2^{m'-r'-1}, 2^{m'-r'}\} = 2^{m'-r'} =$$

$$= 2^{m-1-r+1} = 2^{m-r}$$

II Мажоритарное декодирование $RM(m, r)$

Пусть $p \in RM(m, r)$ $p = p(x_1 .. x_m)$, $\deg p \le r$

для $f \in \mathbb{F}_2[x_1 .. x_m]$ $\Delta(f, p) := |\{ a \in \mathbb{F}_2^m : f(a) \ne p(a) \}|$

$S \subseteq \{1 ... m\}$ и для $X \in \mathbb{F}_2^m$, обозначим

$X_S \in \mathbb{F}_2^{|S|}$ – сужение X на S, т.е.

вектор длины $|S|$, состоящий из x_i, $i \in S$

$$P(x) = \sum_{\substack{S \subset \{1..n\} \\ |S| \le r}} c_S \prod_{i \in S} x_i \quad (1) \qquad P(x) = \sum_{\substack{S \subset \{1..n\} \\ |S| \le r}} c_S \cdot R_S(x)$$

$R_S(x) = \prod_{i \in S} x_i$ – моном

Лемма 1 1) $\forall T \subset S \quad \sum_{a \in \mathbb{F}_2^{|S|}} R_T(a) = 0 \qquad R_T(x) = \prod_{i \in T} x_i$

$\triangleleft\ \exists\, i \in S \setminus T : \sum_{a \in \mathbb{F}_2^{|S|}} R_T(a) = \sum_{\substack{a \in \mathbb{F}_2^{|S|} \\ a_i = 0}} R_T(a) + \sum_{\substack{a \in \mathbb{F}_2^{|S|} \\ a_i = 1}} R_T(a) = 2 \sum_{\substack{a \in \mathbb{F}_2^{|S|} \\ a_i = 0/1}} R_T(a) = 0 \ \blacktriangleright$

2) $\forall S \subset \{1..n\} \quad \sum_{a \in \mathbb{F}_2^{|S|}} R_S(a) = 1$

$\triangleleft\ \underset{\prod_{i \in S} x_i}{\overset{\shortparallel}{R_S}}(a) = 0$ для всех зн-ий $a \in \mathbb{F}_2^{|S|}$, кроме одного: $a = \vec{1} \ \blacktriangleright$

S - фиксировано

обозначим за $\overline{S}$ - дополнение S, $\overline{S} = \{1..n\} \setminus S$

Лемма 2 $\forall b \in \mathbb{F}_2^{m-r}$ и мн-ов P как в (1), $\deg P = r$:

$$\sum_{\substack{a \in \mathbb{F}_2^m : \\ a_{\overline{S}} = b}} P(a) = c_S$$

$\triangleleft$ обозначим за P_b - мн-н, полученный подстановкой b в переменные x_i, $i \in \overline{S}$

$$P_b = c_S R_S(x) + \sum_{T \subset S} a_T R_T(x) \quad \text{для какихто } a_T \in \{0, 1\}$$

$$\sum_{\substack{a \in \mathbb{F}_2^m \\ a_{\overline{S}} = b}} P(a) = \sum_{y \in \mathbb{F}_2^r} P_b(y) = c_S \underbrace{\sum_{y \in \mathbb{F}_2^r} R_S(y)}_{\shortparallel\, 1} + \underbrace{\sum_{T \subset S} a_T \sum_{y \in \mathbb{F}_2^r} R_T(y)}_{\overset{\shortparallel \text{ лемма 1.1}}{0}} =$$

$= C_S$ ▶

Лемма 2 даёт алгоритм нахождения коэфф-та C_S мн-на $P(x)$: необходимо просуммировать зн-ие P во всех $Q \in \mathbb{F}_2^n$, т.ч. $Q_{\overline{S}} = b$ для какого-то $b \in \mathbb{F}_2^{m-r}$.

Так как полученный вектор f отличается от P на не более $\left\lfloor \frac{d-1}{2} \right\rfloor \leq 2^{m-r-1} - 1$ символов, то для как минимум $2^{m-r} - (2^{m-r-r} - 1)$ зн-ий b:

$$\sum_{\substack{Q \in \mathbb{F}_2^m \\ Q_{\overline{S}} = b}} f(Q) = \sum_{\substack{Q \in \mathbb{F}_2^m \\ Q_{\overline{S}} = b}} P(Q) = C_S$$

Из всевозможных 2^{m-r} сумм, больше половины должны быть равны C_S $\Rightarrow$ выбираем C_S "мажоритарным голосованием"

Для нахождения коэфф-ов при степени $< r$, положим

$$f' = f - \sum_{|S| = r} C_S R_S(x) \quad ; \deg f' \leq r - 1$$

Повторим процедуру для f'

Алг-м декодирования

Вход: $f \in \mathbb{F}_2^n$ $(n = 2^m)$

Выход: P, $\deg P \le r$, т.ч. $\Delta(f, P) < 2^{m-r-1}$

1. $t \leftarrow r$

   $F \leftarrow f$

   $P \leftarrow 0$

2. Пока $t > 0$:

   для всех $S \subset \{1..m\}$, т.ч. $|S| = t$:

   $$c_S = \underset{b \in \mathbb{F}_2^{m-r}}{\text{Majority}} \sum_{\substack{a \in \mathbb{F}_2^m \\ a_{\bar{S}} = b}} F(a)$$

   $$P = P + c_S \prod_{i \in S} x_i$$

   для всех $x \in \mathbb{F}_2^m$:

   $$F(x) = F(x) - c_S \prod_{i \in S} x_i$$

   $t--$.

3. Вернуть P.

Пример декодирования кода
RM(4, 2)

$n = 2^m = 16$

$$G = \begin{array}{c} \vec{1} \\ \vec{v}_1 \\ \vec{v}_2 \\ \vec{v}_3 \\ v_4 \\ v_1v_2 \\ v_1v_3 \\ v_1v_4 \\ v_2v_3 \\ v_2v_4 \\ v_3v_4 \end{array} \begin{bmatrix} 1111 & 1111 & 1111 & 1111 \\ 0000 & 0000 & 1111 & 1111 \\ 0000 & 1111 & 0000 & 1111 \\ 0011 & 0011 & 0011 & 0011 \\ 0101 & 0101 & 0101 & 0101 \\ 0000 & 0000 & 0000 & 1111 \\ 0000 & 0000 & 0011 & 0011 \\ 0000 & 0000 & 0101 & 0101 \\ 0000 & 0011 & 0000 & 0011 \\ 0000 & 0101 & 0000 & 0101 \\ 0001 & 0001 & 0001 & 0001 \end{bmatrix}$$

(0100) (0101) (0111) (1011) (1110)

$f = [1111\ 0100\ 1100\ 0011]$

(0000) (0001) (0010) (0011) (0110) (1000) (1001) (1010) (1100) (1101) (1111)

I. $r = 2$ Проверяем степени 2.

- $S = \{1, 2\}$ $\bar{S} = \{3, 4\}$, $b \in \{00, 01, 10, 11\}$

1. $b = 00$ $a \in \{0000, 0100, 1000, 1100\}$

$$\sum f(a) = 1 + 0 + 1 + 0 = 0$$

2. $b = 01$: $a \in \{0001, 0101, 1001, 1101\}$

$$\sum_{\substack{a \in \mathbb{F}_2^4 \\ a_{\{3,4\}} = 01}} f(a) = 1 + 1 + 1 + 0 = 1$$

3. $b = 10$ $a \in \{0010, 0110, 1010, 1110\}$

$$\sum_{a \in \mathbb{F}_2^4} f(a) = 1 + 0 + 0 + 1 = 0$$

$a_{\{3,4\}} = 10$

4. $b = 11$, $a \in \{0011, 0111, 1011, 1111\}$

$$\sum f(a) = 1 + 0 + 0 + 1 = 0$$

$$\text{Maj}(\{0, 1, 0, 0\}) = 0 \Rightarrow C_{12} = 0.$$

- $S = \{1, 3\} \Rightarrow \bar{S} = \{2, 4\}$

$$C_{13} = 1 \Rightarrow P = 1 \cdot X_1 X_3$$

$$C_{14} = C_{23} = C_{24} = C_{34} = 0$$

$$f' = f - G_{v_1 v_3} =$$

$$[1111 \ 0100 \ 1100 \ 0011]$$

$$- [0000 \ 0000 \ 0011 \ 0011]$$

$$=$$

$$f' = [1111 \ 0100 \ 1111 \ 0000]$$

II $r = 1$. $\forall S \in \{\{1\}, \{2\}, \{3\}, \{4\}\}$.

например $\forall S = \{2\}$, $\bar{S} = \{1, 3, 4\}$, $b = \{000, 001, 010, 011, 100, 101, 110, 111\}$

$$C_2 = 1, \quad C_1 = C_3 = C_4 = 0$$

$$\Rightarrow P = P + X_2 = X_2 + X_1 \cdot X_3$$

$$f' - G_{v_2} = [1111\ 0100\ 1111\ 0000]$$
$$- [0000\ 1111\ 0000\ 1111$$
$$= [1111\ 1011\ 1111\ 1111]$$

$$\Rightarrow P = P + \vec{1} = 1 + x_2 + x_1 \cdot x_3 \quad u$$

$$e = [0000\ 0100\ 0000\ 0000].$$