

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ

DOI 10.17223/20710410/23/7

УДК 519.7

О ВЕСОВЫХ СПЕКТРАХ ОДНОГО КЛАССА ЛИНЕЙНЫХ КОДОВ

А. В. Покровский

Институт проблем информационной безопасности Московского государственного университета им. М. В. Ломоносова, г. Москва, Россия

E-mail: AlexPokrovskiy@yandex.ru

Рассматривается класс линейных кодов, являющихся подкодами кода Рида — Маллера. Для данного класса кодов рассчитываются их весовые спектры.

Ключевые слова: код Рида — Маллера, весовой спектр, булевы функции, вес булевой функции.

Введение

Проблема описания весового спектра кода Рида — Маллера тесным образом связана с задачей классификации булевых функций относительно группы аффинных или линейных преобразований, действующих на её аргументах. Для квадратичных булевых функций она была решена с помощью аппарата симплектических форм и теоремы Диксона [1, 2], что позволило описать весовой спектр кода Рида — Маллера второго порядка. Иначе обстоит дело с классификацией булевых функций более высоких степеней. Начиная уже с кубических форм, нет их полной классификации, хотя исследования в этом направлении проводятся довольно давно. В этой связи следует отметить работу [3], в которой получено существенное продвижение в данном вопросе. Аналогичная ситуация складывается и при описании весового спектра кодов Рида — Маллера более высоких порядков. Существенными результатами в области описания этой характеристики кодов являются формула Касами — Токуры [2] для числа кодовых слов, вес которых лежит в определённом диапазоне, и теорема, описывающая весовой спектр произвольного кода с максимальным расстоянием [4]. В настоящей работе рассматривается один из подкодов кода Рида — Маллера произвольного порядка и описывается его весовой спектр.

1. Основные обозначения и определения

Символом $\mathcal{F}_n$, $n \in \mathbb{N}$, будем обозначать множество булевых функций от n переменных, $\mathbb{F}_q$ — поле из q элементов. Для веса булевой функции и степени её полинома Жегалкина используем запись $\text{wt}(f)$ и $\deg(f)$ соответственно.

Определение 1. *Линейным кодом над $\mathbb{F}_q$ называется подпространство $\mathcal{C}$ векторного пространства $\mathbb{F}_q^n$. Размерность $\mathcal{C}$ называется *размерностью кода*. Если она равна k , то такой код называется (n, k) -кодом. *Кодовым расстоянием $\mathcal{C}$* называется минимальный вес Хемминга ненулевого элемента $c \in \mathcal{C}$. Если кодовое расстояние $\mathcal{C}$ равно d , то такой код называется (n, k, d) -кодом.*

Для любого линейного (n, k, d) -кода справедлива оценка Синглтона [1, 2, 4]

$$d \leq n - k + 1.$$

Определение 2. Любой код с кодовым расстоянием, удовлетворяющим равенству $d = n - k + 1$, называется *кодом с максимальным расстоянием*.

Определение 3. *Весовым спектром* (n, k) -кода $\mathcal{C}$ называется совокупность чисел $A_0, A_1, \dots, A_n$, где $A_i = |\{c \in \mathcal{C} : \text{wt}(c) = i\}|$, $i = 0, 1, \dots, n$.

Весовой спектр кодов с максимальным расстоянием описывает следующая теорема.

Теорема 1 [4]. Распределение весов (n, k, d) -кода над $\mathbb{F}_q$ с максимальным расстоянием определяется формулами $A_0 = 1$, $A_l = 0$ при $l = 1, \dots, d - 1$ и

$$A_l = \binom{n}{l} (q - 1) \sum_{j=0}^{l-d} (-1)^j \binom{l-1}{j} q^{l-d-j} \quad \text{при } l \geq d.$$

Практически важным классом линейных кодов является код Риды — Маллера, который определяется через булевы функции заданной степени. Обозначим Ω_f вектор значений функции $f \in \mathcal{F}_n$:

$$\Omega_f = (f(u_0), f(u_1), \dots, f(u_{2^n-1})), \quad u_i \in \mathbb{F}_2^n, \quad i = 0, \dots, 2^n - 1.$$

Определение 4. Для произвольных $n, r \in \mathbb{N}$, $0 \leq r \leq n$, *кодом Риды — Маллера* $\text{RM}(r, n)$ порядка r и длины 2^n называется множество всех строк Ω_f булевых функций $f \in \mathcal{F}_n$, удовлетворяющих условию $\deg(f) \leq r$.

На данный момент полностью описан весовой спектр кода $\text{RM}(2, n)$. Эту задачу удалось решить, используя полученную классификацию квадратичных форм. Обозначим AGL группу аффинных преобразований на $\mathbb{F}_2^n$.

Определение 5. Функции $f_1, f_2 \in \mathcal{F}_n$ называются *аффинно эквивалентными*, если существует пара $(A, \gamma) \in \text{AGL}$, такая, что $f_1(xA \oplus \gamma) = f_2(x)$ для любого $x \in \mathbb{F}_2^n$, где A — невырожденная матрица размера $n \times n$ над $\mathbb{F}_2$; γ — вектор из $\mathbb{F}_2^n$.

В дальнейшем обозначать аффинную эквивалентность функций будем символом $f_1 \sim_{\text{AGL}} f_2$. Как известно [1, 2], любая квадратичная форма аффинной заменой переменных может быть приведена к одному и только одному каноническому виду:

$$\begin{aligned} q_1^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k}; \\ q_2^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k} \oplus 1; \\ q_3^k(x_1, \dots, x_n) &= x_1 x_2 \oplus \dots \oplus x_{2k-1} x_{2k} \oplus x_{2k+1}. \end{aligned}$$

Число k называется *рангом квадратичной формы* и может изменяться в интервале от 1 до $\lfloor n/2 \rfloor$. Канонические формы q_1^k , q_2^k , q_3^k имеют вес $2^{n-t-1} - 2^{n-t-k-1}$, $2^{n-t-1} + 2^{n-t-k-1}$, 2^{n-t-1} соответственно и лежат на разных орбитах.

Обозначим $O_{q_i}(k)$, $i = 1, 2, 3$, мощность орбиты, на которой лежит i -я каноническая форма ранга k . Аффинные функции в этом смысле могут трактоваться как квадратичные формы ранга 0. Тогда всё множество аффинных функций от n переменных разбивается на три орбиты:

$$\begin{aligned} O_{q_1}(0) &= |\{0\}| = 1, \\ O_{q_2}(0) &= |\{1\}| = 1, \\ O_{q_3}(0) &= |\{a_1 x_1 \oplus \dots \oplus a_n x_n \oplus \varepsilon, \quad a_i, \varepsilon \in \mathbb{F}_2, \quad i = 1, \dots, n, \quad (a_1, \dots, a_n) \neq \bar{0}\}| = 2^{n+1} - 2. \end{aligned}$$

Совершенно иначе обстоит дело с описанием весового спектра кода $\text{RM}(r, n)$ при $r \geq 3$. Уже при $r = 3$ его весовой спектр не известен для произвольного n . На данный

момент наиболее исчерпывающий ответ на этот вопрос даёт формула Касами — Токуры, которая позволяет подсчитать количество слов, вес которых лежит в диапазоне $2^{n-r} \leq \text{wt}(f) < 2^{n-r+1}$, $\Omega_f \in \text{RM}(r, n)$. Позже эта формула была обобщена на случай $2^{n-r} \leq \text{wt}(f) \leq 2,5 \cdot 2^{n-r}$.

2. Весовой спектр одного подкода кода Рида — Маллера

Рассмотрим множество $\mathcal{C}_t \subset \mathcal{F}_n$, $t = 1, \dots, n-1$, определяемое следующим образом:

$$\mathcal{C}_t = \left\{ g(x_{n-t+1}, \dots, x_n) \oplus \bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus \bigoplus_{k=n-t+1}^n x_k l_k(x_1, \dots, x_{n-t}) \oplus \right. \\ \left. \oplus l(x_1, \dots, x_{n-t}) \oplus \varepsilon, \text{ где } g \in \mathcal{F}_t, a_{ij}, \varepsilon \in \{0, 1\}, \right. \\ \left. l(x_1, \dots, x_{n-t}), l_k(x_1, \dots, x_{n-t}) \text{ — линейные функции} \right\}.$$

Очевидно следующее утверждение.

Утверждение 1. Множество векторов значений Ω_f , $f \in \mathcal{C}_t$, является подкодом кода $\text{RM}(\max\{t, 2\}, n)$ размерности $2^t + \binom{n-t}{2} + (n-t)(t+1)$.

Наиболее интересен этот код при $t \geq 3$, так как при этих значениях параметра получаем подкод кода Рида — Маллера третьего или более высокого порядка. В случае $t = 3$ это подкод кода $\text{RM}(3, n)$, включающий в себя функции третьей степени нелинейности, содержащие лишь один кубический моном. Весовой спектр этого кода рассчитан в [5]. В данной работе предлагается обобщение этого результата для произвольного значения t из указанного интервала.

Имеет место следующая теорема.

Теорема 2. Весовой спектр кода $\mathcal{C}_t$ в случае нечётного $(n-t)$ представлен в табл. 1, где $i = 0, \dots, 2^{t-r}$; $r = 0, \dots, \min\{t, n-t-2k\}$; $k = 0, \dots, [(n-t)/2]$; в случае чётного $(n-t)$ — в табл. 2, где $i = 0, \dots, 2^{t-r}$; $j = 0, \dots, 2^t$; $r = 0, \dots, \min\{t, n-t-2k\}$; $k = 0, \dots, (n-t)/2 - 1$;

$$N(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\}, \\ 1, & \text{если } r = 0, \\ (2^{n-t-2k})(2^t - 1), & \text{если } r = 1, \\ N(t-1, n-t-2k, r-1) \times \\ \quad \times (2^{n-t-2k} - 2^{r-1}) + \\ \quad + N(t-1, n-t-2k, r)2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}; \end{cases}$$

$$M(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\} \text{ или } r = 0, \\ 2^t - 1, & \text{если } r = 1, \\ N(t, n-t-2k, r) - \\ \quad - N(t, n-t-2k-1, r)2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Т а б л и ц а 1

Весовой спектр кода $\mathcal{C}_t$ в случае нечётного $(n - t)$

Количество функций	Вес
$O_{q_3}(k)2^{2^t+2kt}\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right)$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k)M(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_2^k) + (2^{t-r} - i) \text{ wt}(q_1^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$

Т а б л и ц а 2

Весовой спектр кода $\mathcal{C}_t$ в случае чётного $(n - t)$

Количество функций	Вес
$O_{q_3}(k)2^{2^t+2kt}\left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r)\right)$	2^{n-1}
$\binom{2^{t-r}}{i} O_{q_3}(k)M(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_1}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_1^k) + (2^{t-r} - i) \text{ wt}(q_2^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$\binom{2^{t-r}}{i} O_{q_2}(k)N(t, n-t-2k, r)2^{2^t-2^{t-r}+2kt}$	$i \text{ wt}(q_2^k) + (2^{t-r} - i) \text{ wt}(q_1^k) +$ $+(2^t - 2^{t-r}) \text{ wt}(q_3^k)$
$O_{q_1}\left(\frac{n-t}{2}\right)\binom{2^t}{j}2^{t(n-t)}$	$j \text{ wt}\left(q_1^{(n-t)/2}\right) + (2^t - j) \text{ wt}\left(q_2^{(n-t)/2}\right)$
$O_{q_2}\left(\frac{n-t}{2}\right)\binom{2^t}{j}2^{t(n-t)}$	$j \text{ wt}\left(q_2^{(n-t)/2}\right) + (2^t - j) \text{ wt}\left(q_1^{(n-t)/2}\right)$

Доказательство. Для фиксированной функции из $\mathcal{C}_t$ возможен лишь один из трёх случаев:

$$\begin{aligned}
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t}); \\
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t}); \\
& \bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_3^k(x_1, \dots, x_{n-t}).
\end{aligned}$$

Пусть $(A, \gamma) \in \text{AGL}$ — преобразование, приводящее квадратичную форму

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij}x_i x_j \oplus l(x_1, \dots, x_{n-t})$$

к одному из канонических видов. Применим это преобразование к произвольной функции $f \in \mathcal{C}_t$ и будем рассматривать вес функции $f(xA \oplus \gamma) = \hat{f}(x)$. Функция $\hat{f}$ может

быть лишь одного из трёх видов:

$$\begin{aligned} &g(x_{n-t+1}, \dots, x_n) \oplus q_1^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'; \\ &g(x_{n-t+1}, \dots, x_n) \oplus q_2^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'; \\ &g(x_{n-t+1}, \dots, x_n) \oplus q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}) \oplus \varepsilon'. \end{aligned}$$

Вес функции $\widehat{f}$ равен $\text{wt}(\widehat{f}) = \sum_{(i_{n-t+1}, \dots, i_n) \in \mathbb{F}^t} \text{wt}(\widehat{f}_{n-t+1, \dots, n}^{i_{n-t+1}, \dots, i_n})$, где $\widehat{f}_{n-t+1, \dots, n}^{i_{n-t+1}, \dots, i_n}$ — подфункция функции $\widehat{f}$, полученная фиксацией переменных с номерами $n-t+1, \dots, n$ константами $i_{n-t+1}, \dots, i_n$ соответственно.

Рассмотрим $t \times (n-t)$ -матрицу $\mathcal{L}$, состоящую из коэффициентов линейных функций $l^{(i)}(x_1, \dots, x_{n-t})$, $i = n-t+1, \dots, n$:

$$\mathcal{L} = \begin{pmatrix} l_1^{(1)} & \dots & l_{n-t}^{(1)} \\ l_1^{(2)} & \dots & l_{n-t}^{(2)} \\ & \ddots & \\ l_1^{(t)} & \dots & l_{n-t}^{(t)} \end{pmatrix}.$$

Разобьём матрицу $\mathcal{L}$ на две подматрицы

$$\mathcal{L} = (\mathcal{L}'_{t \times 2k} | \mathcal{L}''_{t \times (n-t-2k)}),$$

и пусть $\text{rang}(\mathcal{L}'') = r$, $r = 0, \dots, \min\{t, n-t-2k\}$. Для сокращения записи обозначим число $t \times (n-t-2k)$ -матриц ранга r через $N(t, n-t-2k, r)$:

$$N(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\}, \\ 1, & \text{если } r = 0, \\ (2^{n-t-2k} - 1)(2^t - 1), & \text{если } r = 1, \\ N(t-1, n-t-2k, r-1) \times \\ \quad \times (2^{n-t-2k} - 2^{r-1}) + \\ + N(t-1, n-t-2k, r) 2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Пусть

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t})$$

и $\text{rang}(\mathcal{L}'') = r$. Тогда система

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = 0 \tag{1}$$

имеет 2^{t-r} решений. Если $(x_{n-t+1}, \dots, x_n) \in \mathbb{F}^t$ является решением системы, то $\text{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n})$ равен $\text{wt}(q_1^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 0$, и равен $\text{wt}(q_2^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 1$. Поскольку $g(x_{n-t+1}, \dots, x_n)$, а следовательно и $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$, пробегает всё множество $\mathcal{F}_t$, то при любой фиксации переменных $x_{n-t+1}, \dots, x_n$ значение функции $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ может быть произвольным.

В противном случае (когда $(x_{n-t+1}, \dots, x_n)$ не является решением системы (1)) выполняется равенство $\text{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \text{wt}(q_3^k)$.

Далее рассмотрим два случая:

- 1) $(n - t)$ нечётно и $0 \leq k \leq [(n - t)/2]$ или $(n - t)$ чётно и $0 \leq k \leq (n - t)/2 - 1$;
- 2) $(n - t)$ чётно и $k = (n - t)/2$.

Из сказанного выше следует, что в первом случае ровно

$$\binom{2^{t-r}}{i} N(t, n - t - 2k, r) O_{q_1}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_1^k) + (2^{t-r} - i) \operatorname{wt}(q_2^k) + (2^t - 2^{t-r}) \operatorname{wt}(q_3^k),$$

где $r = 0, \dots, \min\{n - t - 2k, t\}$, $i = 0, \dots, 2^{t-r}$.

Для случая

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t})$$

рассуждения проводятся аналогичным образом, заменяя q_1^k на q_2^k и наоборот. Получим, что

$$\binom{2^{t-r}}{i} N(t, n - t - 2k, r) O_{q_2}(k) 2^{2^t - 2^{t-r} + 2kt}$$

функций имеют вес

$$i \operatorname{wt}(q_2^k) + (2^{t-r} - i) \operatorname{wt}(q_1^k) + (2^t - 2^{t-r}) \operatorname{wt}(q_3^k),$$

где $r = 0, \dots, \min\{n - t - 2k, t\}$; $i = 0, \dots, 2^{t-r}$.

Теперь рассмотрим случай, когда $(n - t)$ чётно и $k = (n - t)/2$ при условии, что

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_1^k(x_1, \dots, x_{n-t}).$$

В этом случае $\mathcal{L} = \mathcal{L}'$, и при любой фиксации $x_{n-t+1}, \dots, x_n$ прибавление к q_1^k линейной комбинации $\bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_t)$ либо оставляет её на орбите, содержащей q_1^k , либо переводит на орбиту, содержащую q_2^k . В конечном итоге вес $\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}$ будет определяться лишь значением функции $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$, которое может быть произвольным.

Зафиксируем в $\mathbb{F}^t$ j векторов, на которых функция $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ принимает такие значения, что выполняется условие $\operatorname{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \operatorname{wt}(q_1^k)$, а на оставшихся $(2^t - j)$ векторах $\operatorname{wt}(\widehat{f}_{n-t+1, \dots, n}^{x_{n-t+1}, \dots, x_n}) = \operatorname{wt}(q_2^k)$. Тогда вес функции $\operatorname{wt}(\widehat{f})$ равен

$$j \operatorname{wt}\left(q_1^{(n-t)/2}\right) + (2^t - j) \operatorname{wt}\left(q_2^{(n-t)/2}\right).$$

Поскольку при указанных условиях $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon'$ однозначно определяется, то функций указанного веса будет ровно

$$O_{q_1}\left(\frac{n-t}{2}\right) \binom{2^t}{j} 2^{t(n-t)}, \quad j = 0, \dots, 2^t.$$

Случай, когда $(n - t)$ чётно и $k = (n - t)/2$ при условии, что

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t}) \underset{\text{AGL}}{\sim} q_2^k(x_1, \dots, x_{n-t}),$$

рассматривается аналогично предыдущему.

Опишем теперь последний из возможных случаев, когда

$$\bigoplus_{1 \leq i < j \leq n-t} a_{ij} x_i x_j \oplus l(x_1, \dots, x_{n-t})_{\text{AGL}} q_3^k(x_1, \dots, x_{n-t}).$$

Рассмотрим систему

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = (1, 0, \dots, 0). \quad (2)$$

Если вектор $(x_{n-t+1}, \dots, x_n) \in \mathbb{F}^t$ является её решением, то $\text{wt}(q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=n-t+1}^n x_i l^{(i)}(x_1, \dots, x_{n-t}))$ равен $\text{wt}(q_1^k)$, если $g(x_{n-t+1}, \dots, x_n) \oplus \varepsilon' = 0$, и $\text{wt}(q_2^k)$ в противном случае.

Для всех остальных векторов α , для которых система

$$(x_{n-t+1}, \dots, x_n) \mathcal{L}'' = \alpha$$

совместна и вектор $(x_{n-t+1}, \dots, x_n)$ лежит в множестве её решений, выполняется равенство

$$\text{wt} \left(q_3^k(x_1, \dots, x_{n-t}) \oplus \bigoplus_{i=1}^{n-t} x_i l^{(i)}(x_1, \dots, x_{n-t}) \right) = 2^{n-t-1}.$$

Число $t \times (n-t-2k)$ -матриц ранга r , для которых система (2) совместна, обозначим $M(t, n-t-2k, r)$. Поскольку система совместна тогда и только тогда, когда $\text{rang}(\mathcal{L}'')^T = \text{rang}((\mathcal{L}'')^T | \beta^T)$, где $\beta = (1, 0, \dots, 0)$, то имеет место рекуррентная формула

$$M(t, n-t-2k, r) = \begin{cases} 0, & \text{если } r > \min\{t, n-t-2k\} \text{ или } r = 0, \\ 2^t - 1, & \text{если } r = 1, \\ N(t, n-t-2k, r) - \\ - N(t, n-t-2k-1, r) 2^r, & \text{если } 2 \leq r \leq \min\{t, n-t-2k\}. \end{cases}$$

Из этого следует, что $t \times (n-t-2k)$ -матриц ранга r , для которых система (2) несовместна, ровно

$$2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r).$$

Поэтому в исследуемом коде содержится

$$O_{q_3}(k) \left(2^{t(n-t-2k)} - \sum_{r=1}^{\min\{t, n-t-2k\}} M(t, n-t-2k, r) \right) 2^{2^t+2kt}$$

функций веса

$$\text{wt}(q_3^k) 2^t = 2^t 2^{n-t-1} = 2^{n-1}$$

и

$$\binom{2^{t-r}}{i} O_{q_3}(k) M(t, n-t-2k, r) 2^{2^t-2^{t-r}+2kt}$$

функций веса

$$i \text{wt}(q_1^k) + (2^{t-r} - i) \text{wt}(q_2^k) + 2^{2^t-2^{t-r}} \text{wt}(q_3^k),$$

где $i = 0, \dots, 2^{t-r}$, $r = 1, \dots, \min\{t, n-t-2k\}$, $k = 1, \dots, [(n-t)/2]$. ■

ЛИТЕРАТУРА

1. *Логачев О. А., Сальников А. А., Яценко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 469 с.
2. *Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.* Теория кодов, исправляющих ошибки. М.: Связь, 1979. 744 с.
3. *Черемушкин А. В.* Методы аффинной и линейной классификации булевых функций // Труды по дискретной математике. 2001. Т. 4. С. 273–314.
4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М.: Мир, 1986. 576 с.
5. *Покровский А. В., Никифоров М. С.* Весовой спектр одного подкода кода $RM(3, n)$ // XIV Междунар. конф. «Проблемы теоретической кибернетики». Пенза: ПГУ, 2006. Ч. 2. С. 68–70.