ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 59 **2023** **Вып. 1**

УДК 621.391 : 519.725

© 2023 г. **С.Г. Колесников, В.М. Леонтьев**

СЕРИИ ФОРМУЛ ДЛЯ ПАРАМЕТРОВ БХАТТАЧАРЬИ В ТЕОРИИ ПОЛЯРНЫХ КОДОВ[1]

В теории полярных кодов для определения позиций замороженных и информационных бит используются параметры Бхаттачарьи. Они характеризуют скорость поляризации каналов $W_N^{(i)}$, $1 \leqslant i \leqslant N$, специальным образом построенных из исходного канала W, где $N = 2^n$ – длина кода, $n = 1, 2, \ldots$ В случае, когда W – двоичный симметричный канал без памяти, приведены две серии формул для параметров $Z\big(W_N^{(i)}\big)$: при $i = N - 2^k + 1$, $0 \leqslant k \leqslant n$, и при $i = N/2 - 2^k + 1$, $1 \leqslant k \leqslant n-2$. Формулы требуют порядка $\binom{2^{n-k} + 2^k - 1}{2^k} 2^{2^k}$ операций сложения для первой серии и порядка $\binom{2^{n-k-1} + 2^k - 1}{2^k} 2^{2^k}$ для второй. Для случаев $i = 1, N/4 + 1, N/2 + 1, N$ найденные выражения для параметров удалось упростить, вычислив входящие в них суммы. Указаны возможные обобщения для значений i из интервала $(N/4, N)$. Также исследуются комбинаторные свойства поляризационной матрицы G_N полярного кода с ядром Арикана. В частности, установлены простые рекуррентные соотношения между строками матриц G_N и $G_{N/2}$.

Ключевые слова: полярный код, параметр Бхаттачарьи, поляризационная матрица.

DOI: 10.31857/S0555292323010011, **EDN:** JDDBTP

§ 1. Введение и основные результаты

Пусть W – двоичный симметричный канал без памяти с входным алфавитом $X = \{0, 1\}$, выходным алфавитом $Y = \{0, 1\}$ и переходными вероятностями

$$W(y \,|\, x) = \begin{cases} p, & \text{если } x \neq y, \\ 1 - p & \text{в противном случае.} \end{cases}$$

Через W^N, $N = 2^n$, $n = 1, 2, \ldots$, обозначим N-ю декартову степень канала W. Для каждого натурального числа i, $1 \leqslant i \leqslant N$, определим канал $W_N^{(i)} \colon X \to Y^N \times X^{i-1}$ с переходными вероятностями

$$W_N^{(i)}(y, u' \,|\, u_i) = \frac{1}{2^{N-1}} \sum_{u'' \in X^{N-i}} W^N(y \,|\, uG_N),$$

где $y \in Y^N$, $u' \in X^{i-1}$, $u_i \in X$, $u = u'u_iu''$ – конкатенация векторов u', (u_i) и u'', а G_N – поляризационная матрица полярного кода с ядром Арикана $F = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

[1] Работа поддержана Красноярским математическим центром, финансируемым Министерством образования и науки Российской Федерации (номер соглашения 075-02-2022-876).

Тогда [1] значение параметра Бхаттачарьи $Z\big(W_N^{(i)}\big)$ определяется равенством

$$Z\big(W_N^{(i)}\big) = \sum_{y\in Y^N}\sum_{u'\in X^{i-1}} \sqrt{W_N^{(i)}(y,u'\,|\,0)\; W_N^{(i)}(y,u'\,|\,1)}. \tag{1}$$

В той же работе [1] формула (1) была упрощена до следующей:

$$Z\big(W_N^{(i)}\big) = 2^{N-1}\sum_{y\in L} \sqrt{W_N^{(i)}(y,(0,\ldots,0)\,|\,0)\; W_N^{(i)}(y,(0,\ldots,0)\,|\,1)},$$

где L – подмножество в Y^N мощности 2^i, и было показано, что числа $Z\big(W_N^{(i)}\big)$ удовлетворяют рекуррентной системе равенств и неравенств

$$\begin{cases} Z\big(W_{2N}^{(2i-1)}\big) \leqslant 2Z\big(W_N^{(i)}\big) - \big[Z\big(W_N^{(i)}\big)\big]^2, \\ Z\big(W_{2N}^{(2i)}\big) = \big[Z\big(W_N^{(i)}\big)\big]^2. \end{cases} \tag{2}$$

В [2] предложены два метода аппроксимации (“сверху” и “снизу”) вероятности ошибки в поляризованных битовых каналах. Там же [2, теорема 1] показывается, что для достаточно больших N сложность алгоритма аппроксимаций для всех каналов одновременно имеет порядок $O(N\mu^2\log\mu)$, где $\mu > \mu_0$, причем константа μ_0 зависит от пропускной способности канала $I(W)$, скорости и вероятности блоковой ошибки кода, но не зависит от N.

В настоящей статье авторы ставили перед собой задачу получения точных формул для параметров Бхаттачарьи, которые в перспективе можно использовать для расчетов. Приведем основные результаты.

Т е о р е м а 1. *Справедливы равенства*

$$Z\big(W_N^{(1)}\big) = \sqrt{1-(1-2p)^{2N}}, \quad Z\big(W_N^{(N)}\big) = 2^N p^{N/2}(1-p)^{N/2}.$$

Для формулировки следующего результата нам потребуется ввести ряд обозначений. Пусть $m \in \mathbb{N}$ – произвольное натуральное число. Через $\mathbb{Z}_2^m$ обозначим m-ю декартову степень поля вычетов $\mathbb{Z}_2$ с операцией сложения $\oplus$. Подмножества в $\mathbb{Z}_2^m$, состоящие из векторов с четной и нечетной суммой координат, обозначим, соответственно, через $\mathbb{Z}_{2,\mathrm{e}}^m$ и $\mathbb{Z}_{2,\mathrm{o}}^m$. Для произвольного $(0,1)$-вектора $z = (z_1,\ldots,z_m)$ и произвольного целочисленного вектора $t = (t_1,\ldots,t_m)$ положим

$$r(t,z) = w(z)\frac{N}{m} + \sum_{j=1}^{m}(\bar z_j - z_j)t_j,$$

где, как обычно, $w(z) = z_1 + \ldots + z_m$ – вес Хэмминга вектора z, $\bar 0 = 1$, $\bar 1 = 0$. Пусть также

$$H(t,z) = p^{r(t,z)}(1-p)^{N-r(t,z)}.$$

Наконец, определим на векторах t функцию $\theta(t)$, полагая

$$\theta(t) = \frac{m!}{k_1!\ldots k_\ell!},$$

где $k_1,\ldots,k_\ell$ – мощности всех подмножеств, состоящих из одинаковых элементов набора $t_1,\ldots,t_m$.

Теорема 2. *Пусть* $n, k \in \mathbb{N}$, *причем* $1 \leqslant k < n$, *и пусть* $N = 2^n$, $m = 2^k$, $s = 2^{n-k} - 1$. *Тогда*

$$Z\big(W_N^{(N-m+1)}\big) = \\ = 2 \sum_{t_1=0}^{s} \dots \sum_{t_m=t_{m-1}}^{s} \binom{s}{t_1} \dots \binom{s}{t_m} \theta(t) \sqrt{\left[\sum_{z \in \mathbb{Z}_{2,\mathrm{e}}^m} H(t,z)\right]\left[\sum_{z \in \mathbb{Z}_{2,\mathrm{o}}^m} H(t,z)\right]}.$$

Замечание 1. Несложно видеть, что число слагаемых во внешних суммах в совокупности равно числу сочетаний с повторениями из $s+1$ по m, т.е. $\binom{s+m}{m}$, а суммы под корнем содержат по 2^{m-1} слагаемых каждая.

Замечание 2. Пусть $N = 2^n$ и $m = 2^k + \ell$, где $1 \leqslant k < n$ и $0 < \ell < 2^k$. Для $j = 1, 2, \dots, 2^{k+1}$ обозначим через z_j вектор, у которого на позициях с номерами $(j-1)2^{n-k-1} + 1, \dots, j2^{n-k-1}$ стоят единицы, а остальные координаты равны нулю. Допустим, что существует эффективно вычислимая функция $\varkappa_m$, принимающая значение 1, если вектор $\alpha_1 z_1 + \dots + \alpha_{2^{k+1}} z_{2^{k+1}}$, $\alpha_j \in \{0,1\}$, принадлежит подпространству, порожденному последними m строками матрицы G_N, и равная нулю в противном случае. Тогда справедлив следующий аналог формулы из теоремы 2:

$$Z\big(W_N^{(N-m+1)}\big) = 2 \sum_{t_1=0}^{s'} \dots \sum_{t_{m'}=t_{m'-1}}^{s'} \binom{s'}{t_1} \dots \binom{s'}{t_{m'}} \theta(t) \sqrt{\left[\sum_{z} H(t,z)\right]\left[\sum_{z} H(t,z)\right]},$$

где $m' = 2^{k+1}$, $s' = 2^{n-k-1} - 1$, $t = (t_1, \dots, t_{m'})$, а векторы z пробегают множество $\mathbb{Z}_2^{m'}$ и удовлетворяют условию $\varkappa_{m-1}(z) = 1$ для первой суммы и условиям $\varkappa_m(z) = 1$ и $\varkappa_{m-1}(z) = 0$ для второй.

Далее, положим

$$tz = \sum_{j=1}^{m} (-1)^{z_j} t_j$$

и

$$F(t,z) = 2^{(s+1)w(z)+tz} p^{Nw(z)/2m+tz} (1-p)^{N-Nw(z)/2m-2(s+1)(m-w(z))+tz} \times \\ \times \left(p^2 + (1-p)^2\right)^{(s+1)(m-w(z))-tz}.$$

Теорема 3. *Пусть* $n, k \in \mathbb{N}$, *причем* $1 \leqslant k < n-1$, *и пусть* $N = 2^n$, $m = 2^k$, $s = 2^{n-k-1} - 1$. *Тогда*

$$Z\big(W_N^{N/2-m+1}\big) = \\ = 2 \sum_{t_1=0}^{s} \dots \sum_{t_m=t_{m-1}}^{s} \binom{s}{t_1} \dots \binom{s}{t_m} \theta(t) \sqrt{\left[\sum_{z \in \mathbb{Z}_{2,\mathrm{e}}^m} F(t,z)\right]\left[\sum_{z \in \mathbb{Z}_{2,\mathrm{o}}^m} F(t,z)\right]}.$$

Легко видеть, что для вычислений по формуле из теоремы 3 потребуется порядка $\binom{2^{n-k-1}+2^k-1}{2^k} 2^{2^k}$ операций сложения. Также отметим, что все сказанное в замечании 2 можно с незначительными изменениями переформулировать для значений i из множества $\{N/4+1, \dots, N/2-1\}$.

Для $i = N/2+1$ и $i = N/4+1$ формулы из теорем 2 и 3 удалось упростить.

Следствие 1. *Положим* $L_1 = p^2 + (1-p)^2$ *и* $L_2 = 2p(1-p)$. *Справедливы равенства*

$$Z\big(W_N^{(N/2+1)}\big) = 1 - \big(p^2+(1-p)^2\big)^{N/2} + \sqrt{\big(p^2+(1-p)^2\big)^N - \big(p^2-(1-p)^2\big)^N},$$
$$Z\big(W_N^{(N/4+1)}\big) = 1 - \big(L_1^2+L_2^2\big)^{N/4} + \sqrt{\big(L_1^2+L_2^2\big)^{N/2} - \big(L_1^2-L_2^2\big)^{N/2}}.$$

Таким образом, для фиксированного $N = 2^n$ теоремы 1–3 вместе с формулой (2) дают точные выражения для параметров Бхаттачарьи для n^2+1 каналов. Конечно, приведенные формулы являются не альтернативой, а дополнением к методу из [2] в тех случаях, когда расчеты по ним возможны. Также авторы выражают надежду на то, что дальнейшие исследования свойств поляризационной матрицы откроют возможности для построения новых серий, а изучение симметрий в найденных формулах позволит значительно упростить последние, в идеале – до такого вида, как в теореме 1 или следствии 1, в крайнем случае – до формул с полиномиальным числом слагаемых под корнем.

§ 2. Свойства поляризационной матрицы

Напомним, что поляризационная матрица G_{2^n} является произведением перестановочной матрицы B_N на n-ю кронекерову степень ядра Арикана $F^{\otimes n}$. В свою очередь, матрица B_N раскладывается в произведение

$$B_N = R_N(E_2 \otimes R_{N/2}) \dots (E_{N/2} \otimes R_2),$$

где R_{2^i}, $i = 1, \dots, n$, – такая перестановочная матрица, что

$$(x_1, \dots, x_{2^i})R_{2^i} = (x_1, x_3, \dots, x_{2^i-1}, x_2, x_4, \dots, x_{2^i}),$$

E_{2^i} – единичная матрица порядка 2^i.

Обозначим через $f_{2^n}(i,j)$ и $g_{2^n}(i,j)$ элементы матриц $F^{\otimes n}$ и G_{2^n} соответственно, стоящие на позициях (i,j). В [3] для $i,j \in \{1,\dots,2^n\}$ доказано, что

$$f_{2^n}(i,j) = \begin{cases} 1, & \text{если } i-1 \succeq j-1, \\ 0 & \text{в противном случае,} \end{cases}$$

где условие $i-1 \succeq j-1$ выполняется, когда в n-разрядных двоичных записях чисел $i-1$ и $j-1$ каждый разряд числа $i-1$ больше соответствующего разряда числа $j-1$ или равен ему. Чтобы напомнить известную связь между элементами матриц $F^{\otimes n}$ и G_{2^n} и установить ряд новых фактов, определим две функции, областью определения и областью значений которых является множество $\{0,\dots,2^n-1\}$. Положим

$$\mathrm{rev}_n(d_{n-1}\dots d_0) = d_0 \dots d_{n-1}$$

и

$$\mathrm{inv}_n(d_{n-1}\dots d_0) = \bar{d}_{n-1}\dots\bar{d}_0,$$

где $d_{n-1}\dots d_0$ – двоичная n-разрядная запись числа k, дополненная нулями, если для записи k достаточно меньшего числа разрядов.

В [1, с. 3064] установлено равенство

$$g_{2^n}(i,j) = f_{2^n}(\mathrm{rev}_n(i-1)+1, j)$$

для любых $i,j \in \{1,\dots,2^n\}$. Имеют место также следующие утверждения.

Теорема 4. *Для любого $n \in \mathbb{N}$ матрица G_{2^n} является персимметричной, т.е. симметричной относительно побочной диагонали*:

$$g_{2^n}(i,j) = g_{2^n}(2^n - j + 1, 2^n - i + 1)$$

для любых $i, j \in \{1, \ldots, 2^n\}$.

Доказательство. Имеем

$$g_{2^n}(i,j) = f_{2^n}(\mathrm{rev}_n(i-1) + 1, j),$$
$$g_{2^n}(2^n - j + 1, 2^n - i + 1) = f_{2^n}(\mathrm{rev}_n(2^n - j) + 1, 2^n - i + 1).$$

Используя соотношение $\mathrm{inv}_n(k) = 2^n - 1 - k$, справедливое для любого k из множества $\{0, \ldots, 2^n - 1\}$, перепишем второе равенство в виде

$$g_{2^n}(2^n - j + 1, 2^n - i + 1) = f_{2^n}(\mathrm{rev}_n(\mathrm{inv}_n(j-1)) + 1, \mathrm{inv}_n(i-1) + 1).$$

Убедимся, что $\mathrm{rev}_n(i-1) \succeq j - 1$ тогда и только тогда, когда

$$\mathrm{rev}_n(\mathrm{inv}_n(j-1)) \succeq \mathrm{inv}_n(i-1).$$

Для двоичных n-разрядных записей $i - 1 = x_{n-1} \ldots x_0$ и $j - 1 = y_{n-1} \ldots y_0$ неравенства $x_0 \ldots x_{n-1} \succeq y_{n-1} \ldots y_0$ и $\bar{y}_0 \ldots \bar{y}_{n-1} \succeq \bar{x}_{n-1} \ldots \bar{x}_0$ эквивалентны. ▲

Следствие 2. *Для любых $n \in \mathbb{N}$ и $i, j \in \{1, \ldots, 2^n\}$ в i-й строке матрицы G_{2^n} правее последней единицы расположено $\mathrm{rev}_n(\mathrm{inv}_n(i-1))$ нулей, а в j-м столбце матрицы G_{2^n} выше первой единицы расположено $\mathrm{rev}_n(j-1)$ нулей.*

Доказательство. Так как $F^{\oplus n}$ является нижнетреугольной матрицей с единицами по главной диагонали, то ее i-я строка содержит $2^n - i$ нулей правее последней единицы. Из равенства $g_{2^n}(i,j) = f_{2^n}(\mathrm{rev}_n(i-1) + 1, j)$ заключаем, что в i-й строке матрицы G_{2^n} правее последней единицы расположено

$$2^n - 1 - \mathrm{rev}_n(i-1) = \mathrm{inv}_n(\mathrm{rev}_n(i-1)) = \mathrm{rev}_n(\mathrm{inv}_n(i-1))$$

нулей.

Из персимметричности матрицы G_{2^n} следует, что в ее j-м столбце выше первой сверху единицы расположено $\mathrm{rev}_n(\mathrm{inv}_n(2^n - j)) = \mathrm{rev}_n(j-1)$ нулей. ▲

Теорема 5. *Для любых $n \in \mathbb{N}$ и $i \in \{1, \ldots, 2^{n-1}\}$ строка с номером $2i$ матрицы G_{2^n} представляет собой повторенную два раза строку с номером i матрицы $G_{2^{n-1}}$, а строка с номером $2i - 1$ матрицы G_{2^n} – строку с номером i матрицы $G_{2^{n-1}}$, дополненную справа 2^{n-1} нулями.*

Доказательство. Ввиду соотношений

$$F^{\oplus n} = \begin{pmatrix} F^{\oplus(n-1)} & 0 \\ F^{\oplus(n-1)} & F^{\oplus(n-1)} \end{pmatrix}$$

и

$$g_{2^n}(k,j) = f_{2^n}(\mathrm{rev}_n(k-1) + 1, j), \quad k, j = 1, \ldots, 2^n,$$

достаточно для любого $i \in \{1, \ldots, 2^{n-1}\}$ доказать равенства

$$\mathrm{rev}_n(2i-1) - 2^{n-1} = \mathrm{rev}_{n-1}(i-1), \quad \mathrm{rev}_n(2i-2) = \mathrm{rev}_{n-1}(i-1).$$

Рассмотрим двоичную запись $i - 1 = d_{n-2} \ldots d_0$. Имеем

$$\mathrm{rev}_n(2i-2) = \mathrm{rev}_n(2(i-1)) = \mathrm{rev}_n(d_{n-2} \ldots d_0 0) = d_0 \ldots d_{n-2} = \mathrm{rev}_{n-1}(i-1),$$
$$\mathrm{rev}_n(2(i-1)+1) - 2^{n-1} = \mathrm{rev}_n(d_{n-2} \ldots d_0 1) - 2^{n-1} = d_0 \ldots d_{n-2} =$$
$$= \mathrm{rev}_{n-1}(i-1). \quad ▲$$

§ 3. Доказательство теорем 1–3

Зафиксируем еще несколько обозначений. Всюду далее V – линейное пространство размерности $N = 2^n$ над полем $\mathbb{Z}_2$. Операцию сложения в V будем обозначать так же, как и операцию сложения в поле, а именно $\oplus$. Для любых натуральных чисел i, j, удовлетворяющих условиям $1 \leqslant i \leqslant j \leqslant N$, через U_i^j обозначим подпространство в V, образованное векторами, у которых равны нулю первые $i-1$ и последние $j+1$ координат. Также по определению положим $U_1^0 = U_{N+1}^N = \{0\}$. Далее, для $i, j, k \in \mathbb{N}$, таких что $1 \leqslant i \leqslant k \leqslant j \leqslant N$, через $u_i^j(k, \varepsilon)$ обозначим вектор из U_i^j, у которого k-я координата равна ε. Наконец, для произвольного числа $i \in \mathbb{N}$, $1 \leqslant i \leqslant N$, произвольных векторов $y \in V$, $u \in U_1^{i-1}$ и числа $\varepsilon \in \{0, 1\}$ положим

$$A(y, u, i, \varepsilon) = \sum_{u' \in U_{i+1}^N} W^N\big(y \,|\, (u \oplus u_i^i(i, \varepsilon) \oplus u')G_N\big)$$

и будем полагать $A(y, i, \varepsilon) = A(y, u, i, \varepsilon)$, если вектор u нулевой.

Лемма 1. *Пусть $i \in \mathbb{N}$ и $1 \leqslant i \leqslant N$. Тогда*

$$Z\big(W_N^{(i)}\big) = 2 \sum_{y \in U_1^{i-1}} \sqrt{A(yG_N, i, 0)\, A(yG_N, i, 1)}.$$

Доказательство. Заметим, что $V = \{yG_N \,|\, y \in V\}$, поскольку матрица G_N обратима; далее, $V = \{y \oplus u \,|\, y \in V\}$ для любого фиксированного вектора $u \in V$; наконец, для любых векторов $y, x, u \in V$ справедливо равенство $W^N(y \oplus u \,|\, x \oplus u) = W^N(y \,|\, x)$. Поэтому

$$\begin{aligned}
Z\big(W_N^{(i)}\big) &= \frac{1}{2^{N-1}} \sum_{y \in V} \sum_{u \in U_1^{i-1}} \sqrt{A(y, u, i, 0)\, A(y, u, i, 1)} = \\
&= \frac{1}{2^{N-1}} \sum_{y \in V} \sum_{u \in U_1^{i-1}} \sqrt{A(yG_N, u, i, 0)\, A(yG_N, u, i, 1)} = \\
&= \frac{1}{2^{N-1}} \sum_{u \in U_1^{i-1}} \left[\sum_{y \in V} \sqrt{A((y \oplus u)G_N, u \oplus u, i, 0)\, A((y \oplus u)G_N, u \oplus u, i, 1)} \right] = \\
&= \frac{2^{i-1}}{2^{N-1}} \sum_{y \in V} \sqrt{A(yG_N, i, 0)\, A(yG_N, i, 1)}.
\end{aligned}$$

Для завершения доказательства остается заметить, что для любого вектора $u \in U_{i+1}^N$ имеем

$$A\big((y \oplus u)G_N, i, \varepsilon\big) = A(yG_N, i, \varepsilon),$$

и значит, суммирование по V в последней сумме можно заменить, предварительно домножив ее на 2^{N-i}, на суммирование по представителям фактор-пространства V/U_{i+1}^N, т.е. по U_1^i. Наконец, с учетом равенства $A((y \oplus 1_i^i)G_N, i, \varepsilon) = A(yG_N, i, \bar{\varepsilon})$ подпространство суммирования можно сократить до U_1^{i-1}, удвоив при этом сумму. ▲

Доказательство теоремы 1. Первая строка матрицы G_N имеет вид $(1, 0, \ldots, 0)$, а остальные строки содержат четное число единиц. Поэтому множества $\{(0, u_2, \ldots, u_N)G_N\}$ и $\{(1, u_2, \ldots, u_N)G_N\}$ состоят из всех N-мерных векторов

с четным и нечетным числом единиц соответственно. Значит,

$$A(0,1,0) = \sum_{j=0}^{N/2} \binom{N}{2j} p^{2j}(1-p)^{N-2j},$$

$$A(0,1,1) = \sum_{j=1}^{N/2} \binom{N}{2j-1} p^{2j-1}(1-p)^{N-2j+1}.$$

Первая и вторая суммы являются, соответственно, суммами всех положительных и отрицательных слагаемых в разложении выражения $(-p+(1-p))^N$ в бином Ньютона, а обе вместе дают $(p+(1-p))^N$. Следовательно,

$$Z\big(W_N^{(1)}\big) = 2\sqrt{A(0,1,0)A(0,1,1)} =$$
$$= 2\sqrt{\big((1+(1-2p)^N\big)/2\big)\big((1-(1-2p)^N\big)/2\big)} = \sqrt{1-(1-2p)^{2N}}.$$

Докажем второе равенство теоремы 1. Имеем

$$A(yG_N, N, 0) = W^N(yG_N \,|\, (0,\ldots,0)) = p^{w(yG_N)}(1-p)^{N-w(yG_N)},$$
$$A(yG_N, N, 1) = W^N(yG_N \,|\, (1,\ldots,1)) = p^{N-w(yG_N)}(1-p)^{w(yG_N)}.$$

Отсюда

$$Z\big(W_N^{(N)}\big) = 2 \sum_{y \in U_1^{N-1}} \sqrt{A(yG_N, N, 0)\cdot A(yG_N, N, 1)} =$$
$$= 2\cdot 2^{N-1}\sqrt{p^N(1-p)^N} = 2^N p^{N/2}(1-p)^{N/2},$$

что завершает доказательство теоремы 1. ▲

В нижеследующих леммах 2–4 полагаем $N = 2^n$, где $n > 1$, и $m = 2^k$, где $0 \leqslant k < n$. Также полагаем $s = N/m - 1$.

Лемма 2. *Первые $N-m$ строк матрицы G_N порождают подпространство*

$$L_{N,m} = \Big\{(\underbrace{x_1,\ldots,x_{N/m-1},0}_{N/m},\ldots,\underbrace{x_{N-N/m+1},\ldots,x_{N-1},0}_{N/m}) \mid x_i \in \mathbb{Z}_2\Big\}.$$

Доказательство. Поскольку матрица G_N невырождена, ее первые $N-m$ строк линейно независимы и порождают подпространство размерности $N-m$. Мы докажем лемму, если установим, что в столбцах с номерами $N/m, 2N/m, \ldots, mN/m$ первые сверху $N-m$ элементов равны нулю. Согласно следствию 2 для этого достаточно доказать неравенство

$$\mathrm{rev}_n(tN/m-1) \geqslant N-m = 2^n - 2^k \quad \text{для} \quad t = 1,2,\ldots,m.$$

Зафиксируем целое число t, $1 \leqslant t \leqslant m$, и пусть $t-1 = d_{k-1}\ldots d_0$ – двоичная запись числа $t-1$. Из тождества

$$2^{n-k}(t-1) + 2^{n-k} - 1 = t2^{n-k} - 1$$

следует, что $t2^{n-k} - 1 = d_{k-1}\ldots d_0 1\ldots 1$, здесь справа от d_0 расположено $n-k$ единиц. Отсюда

$$\mathrm{rev}_n(tN/m-1) = 1\ldots 1 d_0\ldots d_{k-1} = (2^{n-k}-1)2^k + C = 2^n - 2^k + C,$$

где $C = d_0\ldots d_{k-1} \geqslant 0$. ▲

Лемма 3. *Последние m строк матрицы G_N порождают подпространство*

$$R_{N,m} = \{(z_1, \dots, z_1, \dots, z_m, \dots, z_m) \mid z_1, \dots, z_m \in \mathbb{Z}_2\},$$

здесь каждая переменная z_i повторяется N/m раз. Последние $m-1$ строк матрицы G_N порождают в $R_{N,m}$ подпространство $R^{\mathrm{e}}_{N,m}$ с четной суммой $z_1 + \ldots + z_m$. Линейные комбинации строки $N-m+1$ со строками с бóльшими номерами образуют в $R_{N,m}$ подмножество $R^{\mathrm{o}}_{N,m}$ с нечетной суммой $z_1 + \ldots + z_m$, или, иначе говоря,

$$R^{\mathrm{o}}_{N,m} = (\underbrace{1, \dots, 1}_{N/m}, 0, \dots, 0) \oplus R^{\mathrm{e}}_{N,m}.$$

Доказательство. Когда $m = 1$ или $n = 1$, утверждение очевидно. Далее воспользуемся индукцией по n. Рассмотрим матрицу G_N, $N = 2^n > 2$, и пусть $m > 1$. По предположению индукции последние $m/2$ строк матрицы $G_{N/2}$ порождают подпространство $R_{N/2,m/2}$, векторы которого имеют вид $(z_1, \dots, z_1, \dots, z_{m/2}, \dots, z_{m/2})$, где каждая переменная z_i повторяется $(N/2)/(m/2) = N/m$ раз. Применяя теорему 5, получаем, что каждая из последних m строк матрицы G_N содержится в $R_{N,m}$. Учитывая, что размерность пространства $R_{N,m}$ равна m, а последние m строк матрицы G_N линейно независимы, получаем, что они порождают $R_{N,m}$. По тем же соображениям последние $m-1$ строк матрицы G_N порождают подпространство $R^{\mathrm{e}}_{N,m-1}$. Кратное применение теоремы 5 показывает, что строка с номером $N-m+1$ имеет вид $(1, \dots, 1, 0 \dots, 0)$, где единица повторяется N/m раз. ▲

Зафиксируем произвольный вектор $y \in U_1^{N-m}$, и пусть $x = yG_N$. По лемме 2 имеем $x \in L_{N,m}$, и следовательно, $x = (x_1, \dots, x_s, 0, \dots, x_{N-s}, \dots, x_{N-1}, 0)$. Обозначим через t_i, $1 \leqslant i \leqslant m$, число единиц среди координат $x_{(i-1)N/m+1}, \dots, x_{(i-1)N/m+s}$ вектора x.

Лемма 4. *Имеют место равенства*

$$A(yG_N, N-m+1, 0) = \sum_{z \in \mathbb{Z}^m_{2,\mathrm{e}}} H(t,z), \quad A(yG_N, N-m+1, 1) = \sum_{z \in \mathbb{Z}^m_{2,\mathrm{o}}} H(t,z).$$

Доказательство. Пусть $i = N-m+1$. Зафиксируем вектор $u \in U^N_{i+1}$, и пусть $v = u^i_i(i,\varepsilon) \oplus u$, где $\varepsilon \in \{0,1\}$. По лемме 3 имеем $vG_N = (z_1, \dots, z_1, \dots, z_m, \dots, z_m)$, где $z_1, \dots, z_m \in \mathbb{Z}_2$ и каждая переменная повторяется N/m раз. Для фиксированного j, $1 \leqslant j \leqslant m$, количество отличных от z_j чисел среди $x_{(j-1)N/m+1}, \dots, x_{(j-1)N/m+s}, 0$ равно $z_j N/m + (\bar{z}_j - z_j)t_j$. Отсюда следует, что количество различных координат у векторов yG_N и vG_N выражается числом $r(t,z)$, где $t = (t_1, \dots, t_m)$, $z = (z_1, \dots, z_m)$, а количество одинаковых равно $N - r(t,z)$. Значит, $W^N(yG_N \,|\, vG_N) = H(t,z)$. Для завершения доказательства остается заметить, что согласно лемме 3, когда u пробегает подпространство U^N_{i+1} и $\varepsilon = 0$, вектор vG_N пробегает подпространство $R^{\mathrm{e}}_{N,m}$, а соответствующий ему вектор z пробегает множество $\mathbb{Z}^m_{2,\mathrm{e}}$. Если $\varepsilon = 1$, то vG_N пробегает множество $R^{\mathrm{o}}_{N,m}$, а соответствующий ему вектор z – множество $\mathbb{Z}^m_{2,\mathrm{o}}$. ▲

Доказательство теоремы 2. Очевидно, что каждое из чисел $t_1, \dots, t_m$ может изменяться от 0 до s. Далее, для фиксированных $t_1, \dots, t_m$ в $L_{N,m}$ существует $\binom{s}{t_1} \dots \binom{s}{t_m}$ векторов с t_j единицами среди координат $x_{(j-1)N/m+1}, \dots, x_{(j-1)N/m+s}$. Поэтому из лемм 1 и 4 следует равенство

$$Z\big(W_N^{(N-m+1)}\big) = 2 \sum_{t_1=0}^{s} \dots \sum_{t_m=0}^{s} \binom{s}{t_1} \dots \binom{s}{t_m} \sqrt{\left[\sum_{z \in \mathbb{Z}^m_{2,\mathrm{e}}} H(t,z)\right]\left[\sum_{z \in \mathbb{Z}^m_{2,\mathrm{o}}} H(t,z)\right]}.$$

Упростим полученную формулу до вида, указанного в теореме 2. Заметим, что при перестановке чисел $t_1, \ldots, t_m$ не меняется произведение $\binom{s}{t_1} \ldots \binom{s}{t_m}$ и не меняются суммы, стоящие под корнем. Количество различных перестановок, которые можно получить из чисел $t_1, \ldots, t_m$, очевидно, равно $\theta(t_1, \ldots, t_m)$. В связи с этим определим на декартовой степени $\{0, 1, \ldots, s\}^m$ отношение эквивалентности $\sim$, считая $(t_1, \ldots, t_m) \sim (t'_1, \ldots, t'_m)$, если один набор можно путем перестановки компонент привести ко второму. Ввиду биективности отображения

$$\{(t_1, \ldots, t_m) \mid 0 \leqslant t_1 \leqslant \ldots \leqslant t_m \leqslant s\} \to \{0, \ldots, s\}^m / \sim$$

нижний предел в j-й сумме можно заменить на t_{j-1} для $j = 2, \ldots, m$, что завершает доказательство теоремы 2. ▲

Прежде чем приступить к доказательству теоремы 3, отметим следующий факт, вытекающий из теоремы 5. Для любого натурального числа i, $1 \leqslant i \leqslant N/2$, строка с номером $i + N/2$ матрицы G_N получается добавлением по одной единице справа к каждой группе отдельно стоящих единиц ее i-й строки. Следующие три леммы непосредственно следуют из этого замечания и лемм 2–4. До конца этого параграфа полагаем $N = 2^n$ и $n > 2$; $m = 2^k$ и $1 \leqslant k \leqslant n - 2$; $s = 2^{n-k-1} - 1$.

Лемма 5. *Первые $N/2 - m$ строк матрицы G_N порождают подпространство*

$$L'_{N,m} = \big\{x = (\ldots, x_1^\ell, 0, x_2^\ell, 0, \ldots, x_{s-1}^\ell, 0, x_s^\ell, 0, 0, 0, \ldots) \mid \ell = 1, \ldots, m,\ x_j^\ell \in \mathbb{Z}_2\big\}.$$

Лемма 6. *Строки матрицы G_N с номерами $N/2 - m + 1, \ldots, N/2$ порождают подпространство*

$$\widetilde{R}_{N,m} = \big\{\widetilde{z} = (\ldots, z_\ell, 0, z_\ell, 0, \ldots, z_\ell, 0, \ldots) \mid \ell = 1, \ldots, m,\ z_\ell \in \mathbb{Z}_2\big\}.$$

Строки с номерами $N/2 - m + 2, \ldots, N/2$ порождают в $\widetilde{R}_{N,m}$ подпространство $\widetilde{R}^{\mathrm{e}}_{N,m}$ с четной суммой $z_1 + \ldots + z_m$. Линейные комбинации строки $N/2 - m + 1$ с элементами из $\widetilde{R}^{\mathrm{e}}_{N,m}$ образуют в $\widetilde{R}_{N,m}$ подмножество $\widetilde{R}^{\mathrm{o}}_{N,m}$ с нечетной суммой $z_1 + \ldots + z_m$.

Лемма 7. *Строки матрицы G_N с номерами $N/2 + 1, \ldots, N$ порождают подпространство*

$$L_{N,2} = \big\{u = \big(\ldots, u_1^\ell, u_1^\ell, u_2^\ell, u_2^\ell, \ldots, u_{s+1}^\ell, u_{s+1}^\ell, \ldots\big) \mid \ell = 1, \ldots, m,\ u_j^\ell \in \mathbb{Z}_2\big\}.$$

Обозначим через x^ℓ и u^ℓ ℓ-й блок координат векторов x и u соответственно, а каждому вектору $\widetilde{z} = (\ldots, z_\ell, 0, z_\ell, 0, \ldots, z_\ell, 0, \ldots) \in \widetilde{R}_{N,m}$ поставим в соответствие вектор $z = (z_1, \ldots, z_m) \in \mathbb{Z}_2^m$. Несложно проверить, что число несовпадений координат у векторов $(x', 0)$ и $(z' \oplus u', u')$ выражается суммой $z' + u' + (-1)^{z'} u' + (-1)^{u'+z'} x'$. Отсюда вытекает следующая

Лемма 8. *Число несовпадений координат у векторов x и $\widetilde{z} \oplus u$ выражается суммой*

$$\gamma(x, z, u) = w(z)\frac{N}{2m} + w(u) + \sum_{\ell=1}^{m} (-1)^{z_\ell} w(u^\ell) + \sum_{\ell=1}^{m} \sum_{j=1}^{s} (-1)^{u_j^\ell + z_\ell} x_j^\ell. \tag{3}$$

Доказательство теоремы 3. Из лемм 1 и 5–8 следует равенство

$$Z\big(W_N^{(N/2-m+1)}\big) = 2 \sum_{x \in L'_{N,m}} \sqrt{\left[\sum_{z \in \mathbb{Z}^m_{2,\mathrm{e}}} \widetilde{H}(x, z)\right]\left[\sum_{z \in \mathbb{Z}^m_{2,\mathrm{o}}} \widetilde{H}(x, z)\right]}, \tag{4}$$

где

$$\widetilde{H}(x,z)=\sum_{u\in R_{N,2}} p^{\gamma(x,z,u)}(1-p)^{N-\gamma(x,z,u)}. \tag{5}$$

Глядя на формулы (3)–(5), видим, что суммы под корнем в (4) зависят только от количества t_ℓ ненулевых координат вектора x внутри блока x^ℓ, но не зависят от их расположения. Поэтому формула (4) упрощается до следующей:

$$Z\bigl(W_N^{(N/2-m+1)}\bigr)=$$
$$=2\sum_{t_1=0}^{s}\dots\sum_{t_m=t_{m-1}}^{s}\binom{s}{t_1}\dots\binom{s}{t_m}\theta(t)\sqrt{\left[\sum_{z\in\mathbb{Z}_{2,\mathrm{e}}^m}\widetilde{H}(t,z)\right]\left[\sum_{z\in\mathbb{Z}_{2,\mathrm{o}}^m}\widetilde{H}(t,z)\right]}, \tag{6}$$

где $t=(t_1,\dots,t_m)$.

Упростим $\widetilde{H}(t,z)$. Обозначим через a_ℓ и b_ℓ уменьшенное в два раза число единиц в блоке u^ℓ вектора u, расположенных от первой координаты до координаты $2t_\ell$ и от $2t_\ell+1$ до $2s+2$ соответственно. Пусть $a=(a_1,\dots,a_m)$ и $b=(b_1,\dots,b_m)$. Тогда

$$\gamma(x,z,u)=\gamma(t,z,a,b)=w(z)\frac{N}{2m}+w(a)+w(b)+\sum_{j=1}^{m}(-1)^{z_j}(t_j-a_j+b_j)$$

и

$$\widetilde{H}(t,z)=\sum_{a_1=0}^{t_1}\dots\sum_{a_m=0}^{t_m}\sum_{b_1=0}^{s+1-t_1}\dots\sum_{b_m=0}^{s+1-t_m}\binom{t_1}{a_1}\dots\binom{t_m}{a_m}\times$$
$$\times\binom{s+1-t_1}{b_1}\dots\binom{s+1-t_m}{b_m}p^{\gamma(t,z,a,b)}(1-p)^{N-\gamma(t,z,a,b)}.$$

Зафиксируем вектор z, и пусть $z_{\alpha_1}=\dots=z_{\alpha_q}=0$, а $z_{\alpha_{q+1}}=\dots=z_{\alpha_m}=1$. Здесь $\alpha_1,\dots,\alpha_m$ – некоторая перестановка чисел $1,\dots,m$. Тогда

$$\gamma(t,z,a,b)=w(z)\frac{N}{2m}+2h+tz,$$

где $h=a_{\alpha_{q+1}}+\dots+a_{\alpha_m}+b_{\alpha_1}+\dots+b_{\alpha_q}$. Величина $\gamma(t,z,a,b)$ не зависит от групп переменных $a_{\alpha_1},\dots,a_{\alpha_q}$ и $b_{\alpha_{q+1}},\dots,b_{\alpha_m}$. Поэтому $\widetilde{H}(t,z)$ раскладывается в произведение числа $p^{w(z)N/2m+tz}(1-p)^{N-w(z)N/2m-tz}$, сумм

$$\sum_{a_{\alpha_1}=0}^{t_{\alpha_1}}\binom{t_{\alpha_1}}{a_{\alpha_1}},\ \dots,\ \sum_{a_{\alpha_q}=0}^{t_{\alpha_q}}\binom{t_{\alpha_q}}{a_{\alpha_q}},\ \sum_{b_{\alpha_{q+1}}=0}^{s+1-t_{\alpha_{q+1}}}\binom{s+1-t_{\alpha_{q+1}}}{b_{\alpha_{q+1}}},\ \dots,$$
$$\dots,\ \sum_{b_{\alpha_m}=0}^{s+1-t_{\alpha_m}}\binom{s+1-t_{\alpha_m}}{b_{\alpha_m}},$$

произведение которых равно $2^{(s+1)(m-q)+tz}$, и суммы

$$S=\sum_{a_{\alpha_{q+1}}=0}^{t_{\alpha_{q+1}}}\dots\sum_{a_{\alpha_m}=0}^{t_{\alpha_m}}\sum_{b_{\alpha_1}=0}^{s+1-t_{\alpha_1}}\dots\sum_{b_{\alpha_q}=0}^{s+1-t_{\alpha_q}}\binom{t_{\alpha_{q+1}}}{a_{\alpha_{q+1}}}\dots\binom{t_{\alpha_m}}{a_{\alpha_m}}\times$$
$$\times\binom{s+1-t_{\alpha_1}}{b_{\alpha_1}}\dots\binom{s+1-t_{\alpha_q}}{b_{\alpha_q}}p^{2h}(1-p)^{-2h}.$$

Вычислим сумму S. Показатели степеней p и $1-p$ зависят от величины h, которая принимает все целые значения от 0 до $(s+1)q-tz$. Используя обобщенную свертку Вандермонда и формулу бинома Ньютона, находим

$$S = \sum_{h=0}^{(s+1)q-tz} p^{2h}(1-p)^{-2h} \times$$
$$\times \sum_{a_{\alpha_{q+1}}+\ldots+a_{\alpha_m}+b_{\alpha_1}+\ldots+b_{\alpha_q}=h} \binom{t_{\alpha_{q+1}}}{a_{\alpha_{q+1}}} \ldots \binom{t_{\alpha_m}}{a_{\alpha_m}} \binom{s+1-t_{\alpha_1}}{b_{\alpha_1}} \ldots \binom{s+1-t_{\alpha_q}}{b_{\alpha_q}} =$$
$$= (1-p)^{-2(s+1)q+2tz} \sum_{h=0}^{(s+1)q-tz} \binom{(s+1)q-tz}{h} (p^2)^h \big((1-p)^2\big)^{(s+1)q-tz-h} =$$
$$= (1-p)^{-2(s+1)q+2tz} \big(p^2+(1-p)^2\big)^{(s+1)q-tz}.$$

Таким образом,

$$\widetilde{H}(t,z) = 2^{(s+1)(m-q)+tz} p^{w(z)N/2m+tz} (1-p)^{N-w(z)N/2m-2(s+1)q+tz} \times$$
$$\times \big(p^2+(1-p)^2\big)^{(s+1)q-tz} = 2^{(s+1)w(z)+tz} p^{w(z)N/2m+tz} \times$$
$$\times (1-p)^{N-w(z)N/2m-2(s+1)(m-w(z))+tz} \big(p^2+(1-p)^2\big)^{(s+1)w(z)-tz} = H(t,z),$$

что завершает доказательство теоремы 3. ▲

§ 4. Доказательство следствия 1

Сперва докажем первую формулу. Имеем $k=n-1$, $m=N/2$, $s=1$, $i=N/2+1$. Из вида функции $r(t,z)$ следует, что величины

$$H_{\mathrm{e}}(t_1,\ldots,t_m) = \sum_{z\in\mathbb{Z}^m_{2,\mathrm{e}}} H(t,z), \quad H_{\mathrm{o}}(t_1,\ldots,t_m) = \sum_{z\in\mathbb{Z}^m_{2,\mathrm{o}}} H(t,z)$$

зависят только от количества единиц среди чисел $t_1,\ldots,t_m$, но не от их расположения, поэтому

$$Z\big(W_N^{(N/2+1)}\big) = \sum_{j=0}^{N/2} \binom{N/2}{j} \sqrt{H_{\mathrm{e}}(e_j) H_{\mathrm{o}}(e_j)},$$

где e_j – $N/2$-мерный $(0,1)$-вектор с j единицами в начале. Вычислим $H_{\mathrm{e}}(e_j)$, когда $j>0$. Имеем

$$r(e_j,z) = 2w(z) + (\bar{z}_1 - z_1) + \ldots + (\bar{z}_j - z_j) = j + 2(z_{j+1}+\ldots+z_{N/2}).$$

Величина $j+2(z_{j+1}+\ldots+z_{N/2})$ принимает значения $j+0$, $j+2$, …, $j+2(N/2-j) = N-j$, причем значение $j+2\ell$, $0 \leqslant \ell \leqslant N/2-j$, принимается на следующем количестве векторов z при четном и нечетном ℓ соответственно:

$$\binom{N/2-j}{\ell}\left[\binom{j}{0}+\binom{j}{2}+\ldots\right] = \binom{N/2-j}{\ell}\left[\binom{j}{1}+\binom{j}{3}+\ldots\right] =$$
$$= 2^{j-1}\binom{N/2-j}{\ell}.$$

Следовательно,

$$H_{\mathrm{e}}(e_j) = \sum_{\ell=0}^{N/2-j} 2^{j-1}\binom{N/2-j}{\ell} p^{j+2\ell}(1-p)^{N-j-2\ell}.$$

Аналогичные рассуждения приводят к равенству $H_{\mathrm{o}}(e_j) = H_{\mathrm{e}}(e_j)$. Наконец, легко видеть, что

$$H_{\mathrm{e}}(e_0) = \sum_{\ell=0}^{N/4} \binom{N/2}{2\ell} p^{4\ell}(1-p)^{N-4\ell}, \quad H_{\mathrm{e}}(e_0) = \sum_{\ell=0}^{N/4-1} \binom{N/2}{2\ell+1} p^{4\ell+2}(1-p)^{N-4\ell-2},$$

откуда

$$H_{\mathrm{e}}(e_0) = \frac{Q_1^{N/2} + Q_2^{N/2}}{2}, \quad H_{\mathrm{o}}(e_0) = \frac{Q_1^{N/2} - Q_2^{N/2}}{2},$$

где $Q_1 = p^2 + (1-p)^2$ и $Q_2 = p^2 - (1-p)^2$. Поэтому

$$Z\big(W_N^{(N/2+1)}\big) = \sqrt{Q_1^N - Q_2^N} + \sum_{j=1}^{N/2} \sum_{\ell=0}^{N/2-j} 2^j \binom{N/2}{j}\binom{N/2-j}{\ell} p^{j+2\ell}(1-p)^{N-j-2\ell}.$$

Величина $j + 2\ell$ изменяется при указанных ограничениях на изменение индексов j и ℓ от 1 до $N-1$. Положим $j' = j + 2\ell$. Коэффициент при $p^{j'}(1-p)^{N-j'}$ равен

$$\sum_{\ell=0}^{[(j'-1)/2]} 2^{j'-2\ell}\binom{N/2}{j'-2\ell}\binom{N/2-j'+2\ell}{\ell},$$

где $[\,\cdot\,]$ – целая часть числа. Используя метод коэффициентов [4] (авторы благодарят Г.П. Егорычева за проведенные вычисления), находим

$$\sum_{\ell=0}^{[(j'-1)/2]} 2^{j-2\ell}\binom{N/2}{j'-2\ell}\binom{N/2-j'+2\ell}{\ell} = \begin{cases} \binom{N}{j'}, & \text{если } j'-1 \text{ четно,} \\ \binom{N}{j'} - \binom{N/2}{j'/2} & \text{в противном случае.} \end{cases}$$

Поэтому

$$\begin{aligned} &Z\big(W_N^{(N/2+1)}\big) = \\ &= \sqrt{Q_1^N - Q_2^N} + \sum_{j'=1}^{N-1}\binom{N}{j'}p^{j'}(1-p)^{N-j'} - \sum_{j'=1}^{N/2-1}\binom{N/2}{j'}p^{2j'}(1-p)^{N-2j'} = \\ &= \sqrt{Q_1^N - Q_2^N} + (p+1-p)^N - (1-p)^N - p^N - \big(p^2+(1-p)^2\big)^{N/2} + p^N + \\ &+ (1-p)^N = 1 - \big(p^2+(1-p)^2\big)^{N/2} + \sqrt{\big(p^2+(1-p)^2\big)^N - \big(p^2-(1-p)^2\big)^N}. \end{aligned}$$

Теперь докажем вторую формулу следствия. Пусть $N = 2^n > 4$, $m = N/4$, $s = 1$. Так как числа t_j в рассматриваемом случае равны 0 или 1, то суммы

$$\sum_{z\in\mathbb{Z}_{2,\mathrm{e}}^m} F(t,z) \quad \text{и} \quad \sum_{z\in\mathbb{Z}_{2,\mathrm{o}}^m} F(t,z) \tag{7}$$

зависят от количества чисел t_j, равных 1, но не от их расположения. Обозначим через t_0 число единиц в векторе $t = (t_1, \ldots, t_m)$ и будем считать, что они расположены в начале. Тогда

$$tz = \sum_{j=1}^{m} (-1)^{z_j} t_j = \sum_{j=1}^{t_0} (-1)^{z_j},$$

где при $t_0 = 0$ сумму считаем равной нулю. Далее, заметим, что $F(t,z) = F(t,z')$, если в первых t_0 координатах векторов z и z' расположено одинаковое число единиц и в последних $m - t_0$ координатах тоже расположено одинаковое число единиц. Обозначим количества этих единиц через k_1 и k_2 соответственно. Тогда $w(z) = k_1 + k_2$ и $tz = (-1)^0(t_0 - k_1) + (-1)^{-1}k_1 = t_0 - 2k_1$. Отсюда $(s+1)w(z) + tz = t_0 + 2k_2$, $w(z)N/2m + tz = t_0 + 2k_2$ и

$$N - w(z)N/2m - 2(s+1)(m - w(z)) + tz = t_0 + 2k_2,$$
$$(s+1)(m - w(z)) - tz = N/2 - t_0 - 2k_2.$$

Следовательно, $F(t,z) = Q_1^{N/2} Q_2^{t_0 + 2k_2}$, где $Q_1 = p^2 + (1-p)^2$ и $Q_2 = 2p(1-p)/Q_1$.

Рассмотрим выражение

$$Q_1^{N/2} Q_2^{t_0} \sum_{k_1=0}^{t_0} \sum_{k_2=0}^{m-t_0} \binom{t_0}{k_1} \binom{m-t_0}{k_2} Q_2^{2k_2}. \tag{8}$$

Если суммирование в (8) вести только по таким k_1 и k_2, что сумма $k_1 + k_2$ четна, то мы получим первую из сумм (7), а если нечетна, то вторую.

Пусть $t_0 = 0$. Тогда

$$\sum_{z \in \mathbb{Z}_{2,\mathrm{e}}^m} F(t,z) = Q_1^{\frac{N}{2}} \sum_{k_1=0}^{0} \binom{0}{2k_1} \sum_{k_2=0}^{N/8} \binom{N/4}{2k_2} Q_2^{4k_2} = \frac{\left(1+Q_2^2\right)^{\frac{N}{4}} + \left(1-Q_2^2\right)^{\frac{N}{4}}}{2} Q_1^{\frac{N}{2}},$$

$$\sum_{z \in \mathbb{Z}_{2,\mathrm{o}}^m} F(t,z) = Q_1^{\frac{N}{2}} \sum_{k_1=0}^{0} \binom{0}{2k_1} \sum_{k_2=0}^{N/8-1} \binom{N/4}{2k_2+1} Q_2^{4k_2+2} =$$

$$= \frac{\left(1+Q_2^2\right)^{\frac{N}{4}} - \left(1-Q_2^2\right)^{\frac{N}{4}}}{2} Q_1^{\frac{N}{2}}.$$

При $0 < t_0 < N/4$ имеем

$$\sum_{z \in \mathbb{Z}_{2,\mathrm{e}}^m} F(t,z) = Q_1^{\frac{N}{2}} Q_2^{t_0} \times$$

$$\times \left[\sum_{k_1=0}^{\left[\frac{t_0}{2}\right]} \binom{t_0}{2k_1} \sum_{k_2=0}^{\left[\frac{m-t_0}{2}\right]} \binom{m-t_0}{2k_2} Q_2^{4k_2} + \sum_{k_1=0}^{\left[\frac{t_0}{2}\right]} \binom{t_0}{2k_1+1} \sum_{k_2=0}^{\left[\frac{m-t_0}{2}\right]} \binom{m-t_0}{2k_2+1} Q_2^{4k_2+2} \right] =$$

$$= Q_1^{\frac{N}{2}} Q_2^{t_0} 2^{t_0-1} \sum_{k_2=0}^{\frac{N}{4}-t_0} \binom{N/4-t_0}{k_2} Q_2^{2k_2} = Q_1^{\frac{N}{2}} Q_2^{t_0} 2^{t_0-1} \left(1+Q_2^2\right)^{\frac{N}{4}-t_0}$$

и аналогично

$$\sum_{z \in \mathbb{Z}_{2,\mathrm{o}}^m} F(t,z) = Q_1^{\frac{N}{2}} Q_2^{t_0} 2^{t_0-1} \left(1+Q_2^2\right)^{\frac{N}{4}-t_0}.$$

Наконец, если $t_0 = N/4$, то

$$\sum_{z\in\mathbb{Z}^m_{2,\mathrm{e}}} F(t,z) = \sum_{z\in\mathbb{Z}^m_{2,\mathrm{o}}} F(t,z) = Q_1^{\frac{N}{2}} Q_2^{\frac{n}{4}} 2^{\frac{N}{4}-1}.$$

Отсюда

$$\begin{aligned}
&Z\big(W_N^{(N/4+1)}\big) = Q_1^{N/2}\sqrt{\big(1+Q_2^2\big)^{N/2} - \big(1-Q_2^2\big)^{N/2}} + \\
&+ Q_1^{N/2} \sum_{t_0=1}^{N/4-1} \binom{N/4}{t_0} (2Q_2)^{t_0} \big(1+Q_2^2\big)^{N/4-t_0} + Q_1^{N/2} Q_2^{N/4} 2^{N/4} = \\
&= Q_1^{\frac{N}{2}} \left[\sqrt{\big(1+Q_2^2\big)^{\frac{N}{2}} - \big(1-Q_2^2\big)^{\frac{N}{2}}} + (1+Q_2)^{\frac{N}{2}} - \big(1+Q_2^2\big)^{\frac{N}{4}} - (2Q_2)^{\frac{N}{4}} + \right. \\
&\left. + (2Q_2)^{\frac{N}{4}}\right] = Q_1^{\frac{N}{2}} \left[\sqrt{\big(1+Q_2^2\big)^{\frac{N}{2}} - \big(1-Q_2^2\big)^{\frac{N}{2}}} + (1+Q_2)^{\frac{N}{2}} - \big(1+Q_2^2\big)^{\frac{N}{4}}\right].
\end{aligned}$$

Внося в скобки $Q_1^{N/2}$ и замечая, что $Q_1 + Q_1Q_2 = 1$, $Q_1 = L_1$ и $Q_1Q_2 = L_2$, получаем требуемую формулу. ▲

В заключение авторы выражают благодарность рецензенту за полезные ссылки и замечания, позволившие значительно упростить доказательства утверждений из § 2 и улучшить текст статьи в целом.

СПИСОК ЛИТЕРАТУРЫ

1. *Arıkan E.* Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels // IEEE Trans. Inform. Theory. 2009. V. 55. № 7. P. 3051–3073. https://doi.org/10.1109/TIT.2009.2021379
2. *Tal I., Vardy A.* How to Construct Polar Codes // IEEE Trans. Inform. Theory. 2013. V. 59. № 10. P. 6542–6582. https://doi.org/10.1109/TIT.2013.2272694
3. *Sarkis G., Tal I., Giard P., Vardy A., Thibeault C., Gross W.J.* Flexible and Low-Complexity Encoding and Decoding of Systematic Polar Codes // IEEE Trans. Commun. 2016. V. 64. № 7. P. 2732–2745. https://doi.org/10.1109/TCOMM.2016.2574996
4. *Егорычев Г.П.* Интегральное представление и вычисление комбинаторных сумм. Новосибирск: Наука, 1977.

Колесников Сергей Геннадьевич
Леонтьев Владимир Маркович
Институт математики и фундаментальной информатики
Сибирского федерального университета, Красноярск,
кафедра алгебры и математической логики
sklsnkv@mail.ru
v.m.leontiev@outlook.com

Поступила в редакцию
23.08.2022
После доработки
01.02.2023
Принята к публикации
08.02.2023