Math-Net.Ru

Общероссийский математический портал

В. И. Круглов, В. Г. Михайлов, О ранге случайной матрицы над простым полем, состоящей из независимых строк с заданными числами ненулевых элементов, *Матем. вопр. криптогр.*, 2020, том 11, выпуск 3, 41–52

DOI: <https://doi.org/10.4213/mvk331>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 52.87.193.239

26 апреля 2023 г., 11:52:50

**О ранге случайной матрицы над простым полем,
состоящей из независимых строк
с заданными числами ненулевых элементов**

В. И. Круглов, В. Г. Михайлов

*Математический институт им В. А. Стеклова
Российской академии наук, Москва*

Получено 15.V.2020

Аннотация. Недавно полученная явная оценка для распределения ранга матрицы, состоящей из независимых случайных строк, имеющих заданные веса, распространяется на более широкий класс двоичных матриц с независимыми строками, а также на матрицы над простым полем $GF(p)$ из строк, которые выбираются независимо из множеств векторов с заданным числом ненулевых элементов.

Ключевые слова: случайная матрица над полем $GF(p)$, распределение ранга матрицы, явная оценка

On the rank of random matrix over prime field consisting of independent rows with given numbers of nonzero elements

V. I. Kruglov, V. G. Mikhailov

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

Abstract. In a recent paper we had proposed explicit bound for the distribution function of the rank of matrix with independent rows having fixed weights. Here this bound is generalized for a wider class of binary matrices with independent rows and also to matrices over prime field $GF(p)$ that consist of independent rows, which are chosen from sets of vectors with given numbers of non-zero elements.

Keywords: random matrix over $GF(p)$, distribution of rank of a random matrix, explicit bound

1. Введение

Матрицы над конечными полями давно используются в задачах теории кодирования, криптографии и в других направлениях дискретной математики (см., например, [4, 5, 7, 8]). В ряде случаев интерес представляют свойства ранга матрицы при независимом случайном выборе ее строк из заданных множеств вариантов (см., например, [11]).

В [6] рассматривался класс матриц, состоящих из n независимых случайных строк, которые выбираются равновероятно из множеств всех m -мерных ($m > n$) двоичных векторов заданных весов s_i , $i = 1, \dots, n$, соответственно. Основной результат работы [6] следующий.

Теорема 1. Пусть B — двоичная матрица размера $n \times m$, $n < m$, строки $b_1, \dots, b_n$ которой выбраны независимо и равновероятно из множеств всех m -мерных двоичных векторов заданных весов $s_1, \dots, s_n$ соответственно. Тогда при любом $l \in \{1, \dots, n-1\}$

$$\mathbf{P}\{\text{rank}(B) \leq n-l\} \leq \frac{1}{l^{2^m}} \sum_{t=0}^m C_m^t \left[\prod_{i=1}^n \left(1 + \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right) - \sum_{i=1}^n \frac{K_{s_i}^m(t)}{C_m^{s_i}} - 1 \right]. \quad (1)$$

Здесь и далее $K_s^m(t) = \sum_{\substack{j \geq 0, \\ j \leq s, j \leq t}} (-1)^j C_t^j C_{m-t}^{s-j}$ (многочлены

Кравчука). О свойствах многочленов Кравчука см., например, в [3, 10].

В данной работе эта теорема обобщается на матрицы над простым полем $GF(p)$ из строк, которые выбираются независимо из множеств векторов с заданным числом ненулевых элементов.

Теорема 2. Пусть $B = \|b_{i,j}\|$ — матрица над $GF(p)$ из n случайных строк, которые выбираются независимо и равновероятно из множеств всех m -мерных ($m > n$) векторов с заданным числом ненулевых элементов s_i соответственно, $i = 1, \dots, n$. Тогда при любом $l \in \{1, \dots, n-1\}$

$$l \mathbf{P}\{\text{rank}(B) \leq n-l\} \leq \sum_{r=2}^n \left(1 - \frac{1}{p} \right)^r \times \sum_{1 \leq i_1 < \dots < i_r \leq n} \sum_{u_1=0}^{p-1} \dots \sum_{u_m=0}^{p-1} \prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(\omega^{u_{k_j}}) \right), \quad (2)$$

где

$$L(z) = \frac{1}{p-1} \sum_{r=1}^{p-1} z^r, \quad \omega = e^{2\pi i/p}. \quad (3)$$

Замечание 1. При $p = 2$ выражение в правой части (2) приводится к виду (1).

Вернемся к работе [6]. Другая ее теорема имеет следующий вид (приводим ее с небольшим огрублением).

Теорема 3. Пусть выполнены условия теоремы 1 и числа $s_1, \dots, s_n$ таковы, что найдется натуральное число t_0 , для которого

$$\min \left\{ t \in \{1, \dots, m\} : C_m^t \geq 2^m \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}} \right)^2 \right\} \leq t_0 \leq \frac{m}{2}. \quad (4)$$

Тогда при любом $l \in \{1, \dots, n-1\}$

$$l \mathbf{P}\{\text{rank}(B) \leq n-l\} \leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e \cdot m \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}} \right)^2. \quad (5)$$

Замечание 2. В [6] в последнем члене оценки (5) вместо множителя m стояла несколько меньшая величина $m - 2t_0 + 1$.

Следующее утверждение распространяет этот результат на более широкий класс двоичных матриц, состоящих из независимых строк, количества единиц в которых случайны и независимы.

Пусть

$$\begin{aligned} U_s &= \{k \in \{1, \dots, s\} : C_m^k \geq C_m^s\} \\ &= \left\{ k \in \{1, \dots, s\} : \left| k - \frac{m}{2} \right| \leq \left| s - \frac{m}{2} \right| \right\}, \end{aligned} \quad (6)$$

$$V_s = \{v \in \{0, 1\}^m : \text{wt}(v) \in U_s\}. \quad (7)$$

Здесь $s \in \{1, \dots, m-1\}$, а $\text{wt}(v)$ — вес вектора v .

Обозначим через $\mathcal{P}_s$ множество всех инвариантных относительно перестановок координат вероятностных распределений на V_s .

Теорема 4. Пусть заданы некоторые распределения $P_t \in \mathcal{P}_{s_t}$, $t = 1, \dots, n$, где числа $s_1, \dots, s_n \in \{1, \dots, m-1\}$ таковы, что найдется натуральное число t_0 , удовлетворяющее неравенствам (4).

Пусть B — двоичная матрица размера $n \times m$, $n < m$, строки $b_1, \dots, b_n$ которой выбраны случайно и независимо в соответствии с распределениями P_t , $t = 1, \dots, n$.

Тогда при любом $l \in \{1, \dots, n-1\}$ выполнено неравенство (5).

В настоящей работе будет показано, что оценку (5) ценой некоторого загробления можно значительно упростить.

Следствие. Пусть выполнены условия теоремы 4. Тогда

$$\mathbf{P}\{\text{rank}(B) \leq n-l\} \leq \frac{C_m^{t_0}}{l}(m+2)(2^n + e)2^{-m} \quad \forall l \in \{1, \dots, n-1\}. \quad (8)$$

Определенную трудность при использовании теоремы 4 и следствия представляет проверка условия (4) при больших m и n . В некоторой степени этот вопрос решает следующее утверждение, которое дает оценку скорости убывания вероятностей $\mathbf{P}\{\text{rank}(B) \leq n-l\}$, обоснованную только при достаточно больших m и n . Положим

$$h(x) = -x \ln x - (1-x) \ln(1-x), \quad 0 < x < 1.$$

При $0 < x < 1/2$ функция $h(x)$ монотонно возрастает от 0 до $\ln 2$. При $1/2 < x < 1$ она монотонно убывает, $h(x) = h(1-x)$.

Рассмотрим равенство

$$h(x) + h(y) = \ln 2, \quad 0 < x, y < 1.$$

При $0 < x, y < 1/2$ это равенство устанавливает взаимно однозначную связь между x и y . Функцию, выражающую эту связь, обозначим $y = g(x)$; здесь $g : (0, 1/2) \Rightarrow (0, 1/2)$ — непрерывная функция, убывающая от $1/2$ до 0 при возрастании x от 0 до $1/2$.

Теорема 5. Пусть выполнены условия теоремы 4, числа s' и $\varepsilon > 0$ удовлетворяют условиям

$$s' \in \left\{1, 2, \dots, \left\lceil \frac{m}{2} \right\rceil\right\} : C_m^{s'} = \min \{C_m^{s_1}, \dots, C_m^{s_n}\},$$

$$0 < \varepsilon < \frac{1}{2} - g\left(\frac{s'}{m}\right),$$

а

$$t_0 = \left\lceil m \left(g\left(\frac{s'}{m}\right) + \varepsilon \right) \right\rceil. \quad (9)$$

Тогда найдется такое число $t_0(\varepsilon)$, что при $m \geq t_0(\varepsilon)$ выполнена оценка следствия.

Замечание 3. Для использования теоремы 5 полезной будет следующая таблица значений функции $g(x)$ (значения округлены вверх).

x	$g(x)$	x	$g(x)$	x	$g(x)$	x	$g(x)$	x	$g(x)$
0.02	0.2823	0.12	0.1006	0.22	0.0395	0.32	0.0123	0.42	0.0018
0.04	0.2187	0.14	0.0839	0.24	0.0322	0.34	0.0092	0.44	0.0010
0.06	0.1766	0.16	0.0700	0.26	0.0259	0.36	0.0067	0.46	0.0004
0.08	0.1453	0.18	0.0582	0.28	0.0206	0.38	0.0046	0.48	0.0001
0.10	0.1206	0.20	0.481	0.30	0.0161	0.40	0.0030	0.50	0.0001

Например, при условии $s_1, \dots, s_n \in (0.16m, 0.34m)$ имеем $s' > 0.16m$, и согласно таблице можно взять $t_0 = [0.071m]$.

Интересно также, что в диапазоне $0.097 < x < 0.124$ функция $g(x)$ оценивается сверху линейной функцией: $g(x) < 0.221 - x$. Поэтому при s'/m из указанного диапазона можно взять $t_0 = [m(0.222 - s'/m)]$.

2. Доказательство теоремы 2

Доказательство ведется по схеме, предложенной в [6]. Пусть $\Delta = n - \text{rank}(B)$ — дефект ранга матрицы B , а ζ — число нулевых линейных комбинаций строк матрицы B :

$$\zeta = \sum_{r=1}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} \sum_{a_1, \dots, a_r \in \{1, \dots, p-1\}} I\{a_1 b_{i_1} \oplus \dots \oplus a_r b_{i_r} = 0\}. \quad (10)$$

Здесь и далее $I\{E\}$ — индикатор события E , а $\oplus$ — операция сложения в поле $GF(p)$.

Ясно, что $\Delta \leq \zeta$. Поэтому

$$\mathbf{P}\{\text{rank}(B) \leq n - l\} = \mathbf{P}\{\Delta \geq l\} \leq \mathbf{P}\{\zeta \geq l\}. \quad (11)$$

Случайная величина ζ принимает только неотрицательные целочисленные значения. Поэтому

$$\mathbf{P}\{\zeta \geq l\} \leq \frac{1}{l} \mathbf{E}\zeta. \quad (12)$$

Из (11) и (12) следует неравенство

$$\mathbf{P}\{\text{rank}(B) \leq n - l\} \leq \frac{1}{l} \mathbf{E}\zeta. \quad (13)$$

Теперь надо вычислить величину $\mathbf{E}\zeta$.

Как было показано в [1], производящая функция распределения случайного вектора $X = (x_1, \dots, x_m)$, имеющего равномерное распределение на множестве $\{x \in \{0, 1\}^m : \text{wt}(x) = s\}$ двоичных векторов веса s , равна

$$g(s; z_1, \dots, z_m) = \mathbf{E} z_1^{x_1} \dots z_m^{x_m} = \frac{1}{C_m^s} \sum_{1 \leq k_1 < \dots < k_s \leq m} z_{k_1} \dots z_{k_s}.$$

В нашем случае производящая функция распределения строки $b_i = (b_{i,1}, \dots, b_{i,m})$ матрицы $B = \|b_{i,j}\|$ имеет более сложный вид:

$$g_{b_i}(s_i; z_1, \dots, z_m) = \frac{1}{C_m^{s_i}} \sum_{1 \leq k_1 < \dots < k_{s_i} \leq m} \prod_{j=1}^{s_i} L(z_{k_j}).$$

Ясно, что при всех $a \in \{1, \dots, p-1\}$

$$g_{ab_i}(s; z_1, \dots, z_m) = g_{b_i}(s; z_1, \dots, z_m).$$

В свою очередь, производящая функция вектора-суммы r независимых строк $a_1 b_{i_1}, \dots, a_r b_{i_r}$ при всех $a_1, \dots, a_r \in \{1, \dots, p-1\}$ равна

$$\prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(z_{k_j}) \right). \quad (14)$$

Далее доказывается аналог леммы 2 из [1], согласно которому если r — натуральное число, случайные величины $\xi_1, \dots, \xi_r$ принимают целочисленные значения, $\mathbf{P}\{(\xi_1, \dots, \xi_r) = (k_1, \dots, k_r)\} = p_{k_1, \dots, k_r}$ и

$$f(z_1, \dots, z_r) = \mathbf{E} z_1^{\xi_1} \dots z_r^{\xi_r} = \sum_{k_1, \dots, k_r \in \mathbb{Z}} p_{k_1, \dots, k_r} z_1^{k_1} \dots z_r^{k_r}$$

— производящая функция их совместного распределения, то

$$\mathbf{P}\{\xi_1 = 0, \dots, \xi_r = 0\} = \frac{1}{p^r} \sum_{u_1=0}^{p-1} \sum_{u_m=0}^{p-1} f(\omega^{u_1}, \dots, \omega^{u_m}). \quad (15)$$

Из (14) и (15) следует, что при всех $a_1, \dots, a_r \in \{1, \dots, p-1\}$

$$\begin{aligned} & \mathbf{P}\{a_1 b_{i_1} \oplus \dots \oplus a_r b_{i_r} \equiv (0, \dots, 0) \pmod{p}\} \\ &= \mathbf{P}\{a_1 b_{i_{1,j}} \oplus \dots \oplus a_r b_{i_{r,j}} \equiv 0 \pmod{p}, j = 1, \dots, m\} \end{aligned}$$

$$= \frac{1}{p^r} \sum_{u_1=0}^{p-1} \cdots \sum_{u_m=0}^{p-1} \prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(\omega^{u_{k_j}}) \right), \quad (16)$$

а

$$\begin{aligned} & \sum_{a_1, \dots, a_r \in \{1, \dots, p-1\}} \mathbf{P}\{a_1 b_{i_1} \oplus \dots \oplus a_r b_{i_r} \equiv 0 \pmod{p}\} \\ &= \frac{(p-1)^r}{p^r} \sum_{u_1=0}^{p-1} \cdots \sum_{u_m=0}^{p-1} \prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(\omega^{u_{k_j}}) \right). \end{aligned} \quad (17)$$

Заметим, что

$$\mathbf{E}\zeta = \sum_{r=1}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} \sum_{\substack{a_1, \dots, a_r \\ \in \{1, \dots, p-1\}}} \mathbf{P}\{a_1 b_{i_1} \oplus \dots \oplus a_r b_{i_r} \equiv 0 \pmod{p}\}, \quad (18)$$

а $\mathbf{P}\{b_i = (0, \dots, 0)\} = 0$ при всех $i = 1, \dots, n$. Из (17) и (18) следует равенство

$$\begin{aligned} \mathbf{E}\zeta &= \sum_{r=2}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} \frac{(p-1)^r}{p^r} \\ &\quad \times \sum_{u_1=0}^{p-1} \cdots \sum_{u_m=0}^{p-1} \prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(\omega^{u_{k_j}}) \right). \end{aligned}$$

Таким образом, приходим к неравенству (2):

$$\begin{aligned} l \mathbf{P}\{\text{rank}(B) \leq n-l\} &\leq \sum_{r=2}^n \left(1 - \frac{1}{p}\right)^r \\ &\quad \times \sum_{1 \leq i_1 < \dots < i_r \leq n} \sum_{u_1=0}^{p-1} \cdots \sum_{u_m=0}^{p-1} \prod_{h=1}^r \left(\frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} \prod_{j=1}^{s_{i_h}} L(\omega^{u_{k_j}}) \right), \end{aligned}$$

выполненному для любого $1 \leq l \leq n-1$. Теорема 2 доказана.

3. Доказательство теоремы 4 и следствия

Следующее утверждение вытекает из определений и формулы полной вероятности.

Лемма 1. Пусть случайный вектор b имеет распределение $P \in \mathcal{P}_s$. Тогда его распределение представимо в виде смеси

$$P(v) = \sum_{k \in U_s} \pi_k P_k(v),$$

где $P(v) = \mathbf{P}\{b = v\}$, $\pi_k = \mathbf{P}\{\text{wt}(b) = k\}$, а $P_k(v) = \mathbf{P}\{b = v | \text{wt}(b) = k\}$.

Перейдем к доказательству теоремы 4. Из леммы 1 и независимости строк матрицы B следует, что

$$\mathbf{P}\{\text{rank}(B) \leq n - l\} \quad (19)$$

$$= \sum_{k_1 \in U_{s_1}, \dots, k_n \in U_{s_n}} \left(\prod_{t=1}^n \pi_{k_t} \right) \mathbf{P}\{\text{rank}(B) \leq n - l | \text{wt}(b_1) = k_1, \dots, \text{wt}(b_n) = k_n\}.$$

Согласно предположениям теоремы 4 строки $v_1, \dots, v_n$ матрицы B независимы, причем v_t при условии $\text{wt}(b_t) = k_t$ имеет равномерное распределение на множестве строк с k_t единицами, $t = 1, \dots, n$. При этом

$$C_m^{k_t} \geq C_m^{s_t}, \quad t = 1, \dots, n.$$

Из условия $k_1 \in U_{s_1}, \dots, k_n \in U_{s_n}$ вытекает, что при t_0 , указанном в условиях теоремы,

$$\min \left\{ t \in \{1, \dots, m\} : C_m^t \geq 2^m \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{k_i}}} \right)^2 \right\} \leq t_0 \leq \frac{m}{2}. \quad (20)$$

Следовательно, условное распределение матрицы B при $\{\text{wt}(b_1) = k_1, \dots, \text{wt}(b_n) = k_n\}$ удовлетворяет требованиям теоремы 3 (где надо взять $s_t = k_t$). Из этой теоремы следует, что

$$\begin{aligned} & l \mathbf{P}\{\text{rank}(B) \leq n - l | \text{wt}(b_1) = k_1, \dots, \text{wt}(b_n) = k_n\} \\ & \leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e \cdot m \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}} \right)^2 \end{aligned} \quad (21)$$

при всех $k_1 \in U_{s_1}, \dots, k_n \in U_{s_n}$.

Так как $\sum_{k_t \in U_{s_t}} \pi_{k_t} = 1$ при всех $t = 1, \dots, n$, то из (19) вытекает (5). Теорема 4 доказана.

Далее понадобится следующее утверждение.

Лемма 2. Пусть m и t — натуральные числа, причем $1 \leq t \leq m/2$. Тогда

$$\sum_{k=0}^t C_m^k < C_m^t \left(1 - \frac{t}{m-t+1}\right)^{-1} \leq \frac{m+2}{2} C_m^t.$$

Доказательство леммы 2. Воспользуемся тем, что

$$\sum_{k=0}^t C_m^k = C_m^t \sum_{k=0}^t \frac{C_m^k}{C_m^t},$$

а при $k \leq t < m/2$ величина

$$\frac{C_m^{k-1}}{C_m^k} = \frac{k}{m-k+1} \leq \frac{t}{m-t+1} < 1$$

и монотонно возрастает с ростом k . Следовательно,

$$\frac{C_m^1}{C_m^2} \leq \frac{C_m^2}{C_m^3} \leq \dots \leq \frac{C_m^{t-2}}{C_m^{t-1}} \leq \frac{C_m^{t-1}}{C_m^t}.$$

Поэтому

$$\begin{aligned} \sum_{k=0}^t C_m^k &= C_m^t \sum_{k=0}^t \frac{C_m^k}{C_m^t} = C_m^t \left(1 + \sum_{k=0}^{t-1} \frac{C_m^k}{C_m^{k+1}} \frac{C_m^{k+1}}{C_m^{k+2}} \cdot \dots \cdot \frac{C_m^{t-1}}{C_m^t}\right) \\ &\leq C_m^t \left(1 + \sum_{k=0}^{t-1} \left(\frac{C_m^{t-1}}{C_m^t}\right)^{t-k}\right) = C_m^t \sum_{k=0}^t \left(\frac{C_m^{t-1}}{C_m^t}\right)^k \\ &< C_m^t \sum_{k=0}^{\infty} \left(\frac{t}{m-t+1}\right)^k = C_m^t \frac{1}{1 - \frac{t}{m-t+1}} \leq \frac{m+2}{2} C_m^t. \end{aligned}$$

Лемма 2 доказана. □

Доказательство следствия. Согласно предположениям выполнено неравенство

$$C_m^{t_0} 2^{-m} \geq \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}} \right)^2.$$

Подставив его вместе с оценкой леммы 2 в (5), получаем, что при каждом $l \in \{1, \dots, n-1\}$

$$\begin{aligned} \mathbf{P}\{\text{rank}(B) \leq n - l\} &\leq \frac{C_m^{t_0}}{l} \left(\frac{m+2}{2} 2^{n+1} + em \right) 2^{-m} \\ &= \frac{C_m^{t_0}}{l} ((m+2)2^n + em) 2^{-m} < \frac{C_m^{t_0}}{l} (m+2)(2^n + e) 2^{-m}. \end{aligned}$$

Следствие доказано. $\square$

4. Доказательство теоремы 5

Напомним, что

$$h(x) = -x \ln x - (1-x) \ln (1-x), \quad 0 < x < 1.$$

Лемма 3. Пусть m и t — натуральные числа, причем $1 \leq t \leq m-1$. Тогда

$$\ln C_m^t = mh \left(\frac{t}{m} \right) + \beta(m, t), \quad (22)$$

где $\beta(m, t) = O(\ln m)$ при $m, t, m-t \rightarrow \infty$.

Этот факт, вероятно, хорошо известен. Для доказательства леммы 2 надо воспользоваться неравенством (9.14) из [9] (обобщенная формула Стирлинга), из которого следует, что

$$C_m^t = \frac{1}{\sqrt{2\pi m}} \left(\frac{t}{m} \left(1 - \frac{t}{m} \right) \right)^{-1/2} \exp \left\{ mh \left(\frac{t}{m} \right) \right\} (1 + \theta(m, t)), \quad (23)$$

где $\theta(m, t) = O(m^{-1} + t^{-1} + (m-t)^{-1})$, если $m, t, m-t \rightarrow \infty$. Из (23) вытекает равенство (22). Лемма доказана.

Перейдем к доказательству теоремы. Неравенство

$$C_m^t \geq 2^m \left(\sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}} \right)^2,$$

фигурирующее в условии (4), будет выполнено, если

$$C_m^t \geq 2^m \frac{n^2}{C_m^{s'}}, \quad (24)$$

что эквивалентно неравенству

$$\ln C_m^t + \ln C_m^{s'} \geq m \ln 2 + 2 \ln n.$$

Здесь $s' = s'(s_1, \dots, s_n)$ равно тому s_i , при котором $C_m^{s_i}$ минимально. С учетом (22) это неравенство принимает вид

$$h\left(\frac{t}{m}\right) + h\left(\frac{s'}{m}\right) \geq \ln 2 + \frac{2 \ln n - \beta(m, t) - \beta(m, s')}{m}.$$

Найдем теперь, при каких значениях t выполняется условие (24). Используем равенство

$$h\left(g\left(\frac{s'}{m}\right)\right) + h\left(\frac{s'}{m}\right) = \ln 2,$$

вытекающее из определения функции $g(x)$ и свойства монотонности функций $h(x)$ и $g(x)$: функция $h(x)$ возрастает на $(0, 1/2)$, а функция $g(x)$ на $(0, 1/2)$ убывает. Получаем, что при любом

$$\gamma \in \left(g\left(\frac{s'}{m}\right), \frac{1}{2}\right)$$

найдется такая величина $a(\gamma) > 0$, что

$$h(\gamma) + h\left(\frac{s'}{m}\right) \geq \ln 2 + a(\gamma). \quad (25)$$

Из (25) следует, что для выполнения (24) достаточно, чтобы выполнялось неравенство

$$a(\gamma) \geq \frac{2 \ln n - \beta(m, t) - \beta(m, s')}{m},$$

которое в условиях теоремы выполнено при любом достаточно большом m .

Резюмируя сказанное, заключаем, что для выполнения указанной в формулировке следствия оценки достаточно выполнения условия

$$t_0 \geq m\gamma, \quad \text{где} \quad \gamma \in \left(g\left(\frac{s'}{m}\right), \frac{1}{2}\right).$$

Другими словами,

$$m\left(g\left(\frac{s'}{m}\right) + \varepsilon\right) \leq t_0 < \frac{m}{2}, \quad \text{где} \quad 0 < \varepsilon < \frac{1}{2} - g\left(\frac{s'}{m}\right).$$

Таким образом, можно взять

$$t_0 = \left\lceil m\left(g\left(\frac{s'}{m}\right) + \varepsilon\right) \right\rceil.$$

Теорема 5 доказана.

Замечание 4. Настоящая работа написана в продолжение исследований работ [1, 2] и [12] о свойствах случайных линейных кодов над простыми конечными полями.

Авторы признательны А. М. Зубкову и В. А. Копытцеву за полезные замечания.

Список литературы

- [1] Зубков А. М., Круглов В. И., “Моментные характеристики весов векторов в случайных двоичных линейных кодах”, *Математические вопросы криптографии*, **3:4** (2012), 55–70.
- [2] Зубков А. М., Круглов В. И., “Статистические характеристики весовых спектров случайных линейных кодов над $\text{GF}(p)$ ”, *Математические вопросы криптографии*, **5:1** (2014), 27–38.
- [3] Ивченко Г. И., Медведев Ю. И., Миронова В. А., “Многочлены Кравчука и их применения в задачах криптографии и теории кодирования”, *Математические вопросы криптографии*, **6:1** (2015), 33–56.
- [4] Коблиц Н., *Курс теории чисел и криптографии*, М.: Научное изд-во ТВП, 2001.
- [5] Коваленко И. Н., Левитская А. А., Савчук М. Н., *Избранные задачи вероятностной комбинаторики*, Киев: Наукова думка, 1986.
- [6] Круглов В. И., Михайлов В. Г., “О ранге случайной двоичной матрицы с заданными весами независимых строк”, *Математические вопросы криптографии*, **10:4** (2019), 67–76.
- [7] Лидл Р., Нидеррайтер Г., *Конечные поля*, **2**, М.: Мир, 1988.
- [8] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*, М.: Связь, 1979.
- [9] Феллер В., *Введение в теорию вероятностей и ее приложения*, **1**, М.: Мир, 1984.
- [10] Krasikov I., “Nonnegative quadratic forms and bounds on orthogonal polynomials”, *J. Approx. Theory*, **111:1** (2001), 31–49.
- [11] Salmond D., Grant A., Grivell I., Chan T., “On the rank of random matrices over finite fields”, 2016, arXiv: <https://arxiv.org/pdf/1404.3250v2>.
- [12] Zubkov A. M., Kruglov V. I., “On quantiles of minimal codeword weights of random linear codes over F_p ”, *Математические вопросы криптографии*, **9:2** (2018), 99–102.