Math-Net.Ru

Общероссийский математический портал

В. И. Круглов, В. Г. Михайлов, О ранге случайной двоичной матрицы с заданными весами независимых строк,
Матем. вопр. криптогр., 2019, том 10, выпуск 4, 67–76

DOI: <https://doi.org/10.4213/mvk308>

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: 54.162.127.20

26 апреля 2023 г., 17:51:33

О ранге случайной двоичной матрицы с заданными весами независимых строк

В. И. Круглов, В. Г. Михайлов

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

Получено 29.IV.2019

Аннотация. Изучаются асимптотические свойства ранга матрицы из n независимых случайных строк, каждая из которых равновероятно и независимо от остальных строк выбирается из множества всех m -мерных ($m > n$) двоичных векторов заданных весов s_i , $i = 1, \dots, n$.

Основным результатом работы является явная оценка сверху для функции распределения ранга матрицы.

Ключевые слова: случайная матрица над полем $GF(2)$, распределение ранга матрицы, явная оценка

On the rank of random binary matrix with fixed weights of independent rows

V. I. Kruglov, V. G. Mikhailov

Steklov Mathematical Institute of Russian Academy of Sciences, Moscow

Abstract. We consider random matrix consisting of n independent rows such that each row is equiprobably chosen from the set of all m -dimensional ($m > n$) binary vectors with given weights s_i , $i = 1, \dots, n$, and study asymptotic properties of the rank of such matrix.

We propose explicit upper bound for the distribution function of the rank of matrixes.

Keywords: random matrix over $GF(2)$, distribution of the rank of random matrix, upper bound

1. Введение

Матрицы над конечными полями активно используются в задачах теории кодирования, криптографии и в других направлениях дискретной математики (см., например, [6, 10, 11, 13, 19]). Во многих из этих задач интерес представляют свойства ранга матрицы со случайными элементами.

Естественно, что в первую очередь внимание привлекает задача о ранге матрицы, элементы которой выбраны независимо и равновероятно из множества элементов рассматриваемого поля. Формулы для распределения ранга матрицы в этих случаях и литературные ссылки можно найти, например, в [8, 9].

Изучение предельного поведения распределения ранга таких матриц дало следующий интересный результат.

Пусть число строк n и число столбцов m матрицы A , элементы которой независимы в совокупности и имеют равновероятное распределение на множестве элементов поля $GF(q)$, связаны соотношением $m - n = k$, где k — фиксированное целое число. Тогда (см. [8, 9]) при любом неотрицательном целом l , для которого $l + k \geq 0$,

$$\lim_{n \rightarrow \infty} \mathbf{P}\{\text{rank}(A) = n - l\} = q^{-l(k+l)} \prod_{i=l+1}^{\infty} \left(1 - \frac{1}{q^i}\right) \prod_{j=1}^{k+l} \left(1 - \frac{1}{q^j}\right)^{-1}.$$

Оказалось, что это утверждение выполнено и в случаях, когда распределения элементов матрицы A отличаются (в довольно широких пределах) от равновероятного. Для матрицы $A = \|a_{i,j}\|$ над полем $GF(2)$ достаточным для этого является условие (см. [8, 9])

$$\frac{\ln n + x_n}{n} \leq \mathbf{P}\{a_{i,j} = 1\} \leq 1 - \frac{\ln n + x_n}{n},$$

где $x_n \rightarrow \infty$ сколь угодно медленно. Эти границы точны в том смысле, что существует пример (см. [9]), в котором величина x_n постоянна и ранг матрицы A имеет другое предельное распределение.

Уточнениям и обобщениям результатов для равновероятного случая были посвящены работы [16, 18]: в [16] была получена оценка скорости сходимости распределения случайной величины $n - \text{rank}(A)$ к предельному в терминах расстояния по вариации, а в [18] был исследован случай, когда некоторые элементы матрицы A заменены нулями.

Отметим, что в ряде работ (см., например [1, 2, 7]) изучались свойства так называемого *линейного ранга* случайной матрицы, равного

размеру максимального минора без нулевых строк и столбцов. Здесь эта характеристика рассматриваться не будет.

Ясно, что для случая, когда элементы случайной матрицы зависимы между собой, получить достаточно подробное описание предельного поведения ранга в сколь-либо общей постановке задачи невозможно. Поэтому интерес представляет изучение частных постановок, например матриц из независимых случайных строк (или столбцов). Наибольший интерес вызывал случай *разреженных* матриц, когда число единиц в каждой из строк невелико по сравнению с длиной строк (см., например, [14, 15] и ссылки в этих работах). Так, в [14] исследовано асимптотическое поведение ранга двоичной матрицы $A_{n,m,k}$ размера $n \times m$, столбцы которой выбираются независимо и равновероятно из множества всех C_n^k столбцов с k единицами, а $n, m \rightarrow \infty$ таким образом, что n существенно меньше m . Показано наличие своего рода порогового эффекта в поведении ранга матрицы при $n, m \rightarrow \infty$ и фиксированном k в зависимости от соотношения между параметрами m, n, k . В частности, в случае $k \geq 3$ доказано, что если $m = n(\log n + c_n)/k$, то для вероятности $P_{n,m,k}$ того, что матрица $A_{n,m,k}$ имеет максимальный возможный ранг $n - I\{k \text{ четное}\}$ (здесь и далее $I\{E\}$ — индикатор события E), справедливы соотношения

$$\lim_{n \rightarrow \infty} P_{n,m,k} = \begin{cases} 0, & \text{если } c_n \rightarrow -\infty, \\ \exp\{-e^{-c}\}, & \text{если } c_n \rightarrow c, \\ 1, & \text{если } c_n \rightarrow \infty. \end{cases}$$

Кроме этого, показано, что для любого $a > 0$ существует такое $\gamma = \gamma(a)$, что для $m \geq \gamma n \log n$

$$1 - P_{n,m,k} = o(n^{-a}), \quad n \rightarrow \infty.$$

Так как параметр k в этих утверждениях фиксирован, то речь в них идет о разреженных матрицах. Интерес к таким матрицам связан, в частности, с их использованием при построении эффективных вычислительных алгоритмов.

Отметим, что «классическая» постановка задачи о ранге случайной разреженной матрицы над полем из двух элементов и результаты для нее были приведены в [9].

В настоящей работе рассматривается класс матриц, состоящих из n независимых случайных строк, которые выбираются равновероятно из множества всех m -мерных ($m > n$) двоичных векторов заданных

весов s_i , $i = 1, \dots, n$, соответственно. Для них строятся явные оценки сверху в форме неравенств для функций распределения ранга таких случайных матриц (теоремы 1 и 2). Эти оценки применимы и к матрицам, в которых число ненулевых элементов в каждой из строк сравнимо с длиной строк (см. пример к теореме 2).

2. Теоремы о распределении рангов матриц

При выводе оценок для распределения ранга исследуемых матриц естественным образом возникают многочлены Кравчука $K_s^m(t) = \sum_{j \geq 0} (-1)^j C_t^j C_{m-t}^{s-j}$, задаваемые соотношением

$$\sum_{s=0}^{\infty} K_s^m(t) z^s = (1-z)^m (1+z)^{m-t}.$$

Свойства многочленов Кравчука подробно рассмотрены в [5].

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

$$\begin{aligned} & \mathbf{P}\{\text{rank}(B) \leq n-l\} \\ & \leq \frac{1}{l2^m} \sum_{t=0}^m C_m^t \left[\prod_{i=1}^n \left(1 + \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right) - \sum_{i=1}^n \frac{K_{s_i}^m(t)}{C_m^{s_i}} - 1 \right]. \end{aligned} \quad (1)$$

Так как $\sum_{j \geq 0} C_t^j C_{m-t}^{s-j} = C_m^s$, то $\left| \frac{K_s^m(t)}{C_m^s} \right| < 1$. Более того, как будет показано ниже,

$$\left| \frac{K_s^m(t)}{C_m^s} \right| < \min \left\{ 1, \sqrt{\frac{2^m}{C_m^s C_m^t}} \right\}. \quad (2)$$

С помощью этого неравенства удастся получить довольно грубую, но более удобную оценку для функции распределения ранга. Положим

$$Q(s_1, \dots, s_n) = \sum_{i=1}^n \frac{1}{\sqrt{C_m^{s_i}}}. \quad (3)$$

Теорема 2. Пусть выполнены условия теоремы 1 и числа $s_1, \dots, s_n$ таковы, что найдется натуральное число t_0 , для которого

$$\min \{t \in \{1, \dots, m\} : C_m^t \geq 2^m Q^2(s_1, \dots, s_n)\} \leq t_0 \leq \frac{m}{2}. \quad (4)$$

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

$$l \mathbf{P}\{\text{rank}(B) \leq n-l\} \leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e(m-2t_0+1)Q^2(s_1, \dots, s_n), \quad (5)$$

в частности

$$\mathbf{P}\{\text{rank}(B) < n\} \leq 2^{n-m+1} \sum_{t=0}^{t_0} C_m^t + e(m-2t_0+1)Q^2(s_1, \dots, s_n). \quad (6)$$

Приведем простой пример, показывающий содержательность оценок (5) и (6). Пусть $n, m-n \rightarrow \infty$ и для некоторого фиксированного R

$$\left|s_i - \frac{m}{2}\right| \leq R, \quad i = 1, \dots, n.$$

Тогда величины $C_m^{s_1}, \dots, C_m^{s_n}$ имеют (см. [12]) одинаковый порядок роста $m^{-1/2}2^m$ и $Q^2(s_1, \dots, s_n) = O(m^{5/2}2^{-m})$, поэтому при больших m можно положить $t_0 = 3$. Подставляя полученные оценки в (5), получаем, что равномерно по $l \in \{1, \dots, n-1\}$

$$l \mathbf{P}\{\text{rank}(B) \leq n-l\} = O(m^3 2^{n-m} + m^{5/2} 2^{-m}), \quad n, m-n \rightarrow \infty.$$

Замечание 1. Теоремы 1 и 2 продолжают исследования [3, 4, 20] свойств случайных линейных кодов над простыми конечными полями.

3. Доказательство теоремы 1

Пусть $\Delta = n - \text{rank}(B)$ — дефект ранга матрицы B , а ζ — число нулевых линейных комбинаций строк матрицы B :

$$\zeta = \sum_{r=1}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} I\{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\}. \quad (7)$$

Здесь и далее $I\{E\}$ — индикатор события E , а $\oplus$ — операция сложения в поле $GF(2)$.

Так как $\Delta \leq \zeta$, то

$$\mathbf{P}\{\text{rank}(B) \leq n-l\} = \mathbf{P}\{\Delta \geq l\} \leq \mathbf{P}\{\zeta \geq l\}. \quad (8)$$

Случайная величина ζ принимает только неотрицательные целочисленные значения, следовательно,

$$\mathbf{P}\{\zeta \geq l\} \leq \frac{1}{l} \mathbf{E}\zeta. \quad (9)$$

Из (8) и (9) получаем, что

$$\mathbf{P}\{\text{rank}(B) \leq n - l\} \leq \frac{1}{l} \mathbf{E}\zeta, \quad (10)$$

после чего нам остается подходящим образом оценить сверху величину $\mathbf{E}\zeta$.

Следующие рассуждения заимствованы (с небольшими изменениями) из доказательства теоремы 5 в [3].

Пусть $g(s; z_1, \dots, z_m)$ — 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 , тогда

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

Следовательно, для производящей функции $g(s_{i_1}, \dots, s_{i_r}; z_1, \dots, z_r)$ распределения суммы независимых случайных векторов $b_{i_1}, \dots, b_{i_r}$, имеющих равновероятные распределения на множествах векторов весов $s_{i_1}, \dots, s_{i_r}$ соответственно, справедливо равенство

$$\begin{aligned} g(s_{i_1}, \dots, s_{i_r}; z_1, \dots, z_m) &= \mathbf{E}z_1^{x_{i_1,1} + \dots + x_{i_r,1}} \dots z_m^{x_{i_1,m} + \dots + x_{i_r,m}} \\ &= \prod_{h=1}^r g(s_{i_h}; z_1, \dots, z_m) = \prod_{h=1}^r \frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} z_{k_1} \dots z_{k_{s_{i_h}}}. \end{aligned}$$

Воспользуемся леммой 2 из [3], согласно которой *если 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*

$$\mathbf{P}\{\xi_1 = 0, \dots, \xi_r = 0\} = \frac{1}{2^r} \sum_{z_1, \dots, z_r = \pm 1} f(z_1, \dots, z_r).$$

Применяя эту лемму к случайным величинам $\xi_j = x_{i_1,j} + \dots + x_{i_r,j}$, $j = 1, \dots, r$, получаем, что

$$\begin{aligned}
 & \mathbf{P} \{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\} \\
 &= \mathbf{P} \{x_{i_1,j} + \dots + x_{i_r,j} \equiv 0 \pmod{2}, j = 1, \dots, r\} \\
 &= \frac{1}{2^m} \sum_{z_1, \dots, z_m = \pm 1} g(s_{i_1}, \dots, s_{i_r}; z_1, \dots, z_m) = \frac{1}{2^m} \sum_{z_1, \dots, z_m = \pm 1} \prod_{h=1}^r g(s_{i_h}; z_1, \dots, z_m) \\
 &= \frac{1}{2^m} \sum_{z_1, \dots, z_m = \pm 1} \prod_{h=1}^r \frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} z_{k_1} \dots z_{k_{s_{i_h}}} \\
 &= \frac{1}{2^m} \sum_{t=0}^m C_m^t \prod_{h=1}^r \frac{1}{C_m^{s_{i_h}}} \sum_{1 \leq k_1 < \dots < k_{s_{i_h}} \leq m} z_{k_1}^{(t)} \dots z_{k_{s_{i_h}}}^{(t)},
 \end{aligned}$$

где $z_j^{(t)} = -1$ при $1 \leq j \leq t$ и $z_j^{(t)} = 1$ при $t < j \leq m$. Следовательно,

$$\begin{aligned}
 & \mathbf{P} \{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\} \\
 &= \frac{1}{2^m} \sum_{t=0}^m C_m^t \prod_{h=1}^r \frac{1}{C_m^{s_{i_h}}} \sum_{j \geq 0} (-1)^j \cdot (1)^{s_{i_h}-j} C_t^j C_{m-t}^{s_{i_h}-j} \\
 &= \frac{1}{2^m} \sum_{t=0}^m C_m^t \prod_{h=1}^r \frac{K_{s_{i_h}}^m(t)}{C_m^{s_{i_h}}}. \quad (11)
 \end{aligned}$$

Согласно определению (7) случайной величины ζ

$$\begin{aligned}
 \mathbf{E}\zeta &= \sum_{r=1}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} \mathbf{P} \{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\} \\
 &= \sum_{r=2}^n \sum_{1 \leq i_1 < \dots < i_r \leq n} \mathbf{P} \{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\}, \quad (12)
 \end{aligned}$$

поскольку событие $\{b_{i_1} = 0\}$ является невозможным при $r = 1$.

Из (11) и (12) следует, что

$$\begin{aligned}
 \mathbf{E}\zeta &= \sum_{2 \leq r \leq n} \sum_{1 \leq i_1 < \dots < i_r \leq n} \mathbf{P} \{b_{i_1} \oplus \dots \oplus b_{i_r} = 0\} \\
 &= \sum_{2 \leq r \leq n} \sum_{1 \leq i_1 < \dots < i_r \leq n} \frac{1}{2^m} \sum_{t=0}^m C_m^t \prod_{h=1}^r \frac{K_{s_{i_h}}^m(t)}{C_m^{s_{i_h}}}
 \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2^m} \sum_{t=0}^m C_m^t \sum_{2 \leq r \leq n} \sum_{1 \leq i_1 < \dots < i_r \leq n} \prod_{h=1}^r \frac{K_{s_{i_h}}^m(t)}{C_m^{s_{i_h}}} \\
&= \frac{1}{2^m} \sum_{t=0}^m C_m^t \left[\prod_{i=1}^n \left(1 + \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right) - \sum_{i=1}^n \frac{K_{s_i}^m(t)}{C_m^{s_i}} - 1 \right].
\end{aligned}$$

Подставив это выражение в (10), получим (1). Теорема 1 доказана.

4. Доказательство теоремы 2

В [17] доказана оценка

$$(K_s^m(t))^2 < 2^m C_m^s (C_m^t)^{-1}, \quad s, t \in [0, m],$$

из которой следует оценка (2).

Перейдем непосредственно к доказательству теоремы 2. Прежде всего заметим, что в силу неравенства

$$\begin{aligned}
&\left| \prod_{i=1}^n (1 + x_i) - \sum_{i=1}^n x_i - 1 \right| \\
&\leq \prod_{i=1}^n (1 + |x_i|) - \sum_{i=1}^n |x_i| - 1, \quad |x_1|, \dots, |x_n| < 1, \quad (13)
\end{aligned}$$

из неравенства (1) следует оценка

$$\begin{aligned}
&l \mathbf{P}\{\text{rank}(B) \leq n - l\} \\
&\leq \frac{1}{2^m} \sum_{t=0}^m C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right], \quad (14)
\end{aligned}$$

которой будем пользоваться далее.

Сумму в правой части оценки (14) разобьем на слагаемые S_1, S_2, S_3 , где

$$\begin{aligned}
S_1 &= \sum_{t=0}^{t_0(s_1, \dots, s_n)-1} C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right], \\
S_2 &= \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right],
\end{aligned}$$

$$S_3 = \sum_{t=m-t_0(s_1, \dots, s_n)+1}^m C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right].$$

Из (2) и (13) следует оценка для S_1 :

$$\begin{aligned} S_1 &= \sum_{t=0}^{t_0(s_1, \dots, s_n)-1} C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right] \\ &< \sum_{t=0}^{t_0(s_1, \dots, s_n)-1} C_m^t \prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) < 2^n \sum_{t=0}^{t_0(s_1, \dots, s_n)-1} C_m^t. \end{aligned} \quad (15)$$

Рассуждая аналогично, получаем, что

$$S_3 < 2^n \sum_{t=m-t_0(s_1, \dots, s_n)+1}^m C_m^t = 2^n \sum_{t=0}^{t_0(s_1, \dots, s_n)-1} C_m^t. \quad (16)$$

Теперь оценим S_2 . Из (2) следует, что

$$\begin{aligned} S_2 &= \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} C_m^t \left[\prod_{i=1}^n \left(1 + \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| \right) - \sum_{i=1}^n \left| \frac{K_{s_i}^m(t)}{C_m^{s_i}} \right| - 1 \right] \\ &< \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} C_m^t \left[\prod_{i=1}^n \left(1 + \sqrt{\frac{2^m}{C_m^{s_i} C_m^t}} \right) - \sum_{i=1}^n \sqrt{\frac{2^m}{C_m^{s_i} C_m^t}} - 1 \right] \\ &< \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} C_m^t \left[\exp \left\{ \sum_{i=1}^n \sqrt{\frac{2^m}{C_m^{s_i} C_m^t}} \right\} - \sum_{i=1}^n \sqrt{\frac{2^m}{C_m^{s_i} C_m^t}} - 1 \right]. \end{aligned} \quad (17)$$

Из неравенства

$$e^x - 1 - x \leq x^2 e^x, \quad x > 0,$$

оценки (17) и определения (3) следует, что

$$\begin{aligned} S_2 &< \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} \left(\sum_{i=1}^n \sqrt{\frac{2^m}{C_m^{s_i}}} \right)^2 \exp \left\{ \sqrt{\frac{2^m}{C_m^t}} \sum_{i=1}^n \sqrt{\frac{1}{C_m^{s_i}}} \right\} \\ &= 2^m Q^2(s_1, \dots, s_n) \sum_{t=t_0(s_1, \dots, s_n)}^{m-t_0(s_1, \dots, s_n)} \exp \left\{ \sqrt{\frac{2^m}{C_m^t}} Q(s_1, \dots, s_n) \right\} \\ &\leq e 2^m (m - 2t_0(s_1, \dots, s_n) + 1) Q^2(s_1, \dots, s_n). \end{aligned} \quad (18)$$

Из оценок (14), (16) и (18) следует неравенство (5). Теорема 2 доказана.

Авторы признательны А. М. Зубкову и Г. И. Ивченко за полезные замечания.

Список литературы

- [1] Балакин Г. В., “О случайных матрицах”, *Теория вероятн. и ее примен.*, **12:2** (1967), 346–353.
- [2] Балакин Г. В., “Распределение ранга случайных матриц над конечным полем”, *Теория вероятн. и ее примен.*, **13:4** (1968), 631–641.
- [3] Зубков А. М., Круглов В. И., “Моментные характеристики весов векторов в случайных двоичных линейных кодах”, *Математические вопросы криптографии*, **3:4** (2012), 55–70.
- [4] Зубков А. М., Круглов В. И., “Статистические характеристики весовых спектров случайных линейных кодов над $GF(p)$ ”, *Математические вопросы криптографии*, **5:1** (2014), 27–38.
- [5] 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.
- [6] Коблиц Н., *Курс теории чисел и криптографии*, М.: Научное изд-во ТВП, 2001.
- [7] Коваленко И. Н., “О распределении линейного ранга случайной матрицы”, *Теория вероятн. и ее примен.*, **17:2** (1972), 354–359.
- [8] Коваленко И. Н., Левитская А. А., Савчук М. Н., *Избранные задачи вероятностной комбинаторики*, Киев: Наукова думка, 1986.
- [9] Колчин В. Ф., *Случайные графы*, М.: ФИЗМАТЛИТ, 2000.
- [10] Лидл Р., Нидеррайтер Г., *Конечные поля*, т. 2, М.: Мир, 1988.
- [11] Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А., *Теория кодов, исправляющих ошибки*, М.: Связь, 1979.
- [12] Феллер В., *Введение в теорию вероятностей и ее приложения*, т. 1, М.: Мир, 1984.
- [13] Blake I. F., Studholme C., “Properties of random matrices and applications”, Unpublished report, 2006, http://www.cs.toronto.edu/cvs/coding/random_report.pdf.
- [14] Cooper C., Frieze A., Pegden W., “On the rank of a random binary matrix”, 2018, <https://arxiv.org/pdf/1806.04988v2>.
- [15] Darling R., Penrose M., Wade A., Zabel S., “Rank deficiency in sparse random $GF[2]$ matrices”, *Electron. J. Probab.*, **19** (2014).
- [16] Fulman J., Goldstein L., “Stein’s method and the rank distribution of random matrices over finite fields”, *Ann. Probab.*, **43:3** (2015), 1274–1314.
- [17] Krasikov I., “Nonnegative quadratic forms and bounds on orthogonal polynomials”, *J. Approx. Theory*, **111:1** (2001), 31–49.
- [18] 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>.
- [19] Tulino A. M., Verdu S., *Random matrix theory and wireless communications*, Now Publishers, 2004, 182 pp.
- [20] Zubkov A. M., Kруглов V. I., “On quantiles of minimal codeword weights of random linear codes over F_p ”, *Математические вопросы криптографии*, **9:2** (2018), 99–102.