Math-Net.Ru

Общероссийский математический портал

А. А. Ирматов, Ж. Д. Ковиянич, Об асимптотике логарифма числа пороговых функций K -значной логики, *Дискрет. матем.*, 1998, том 10, выпуск 3, 35–56

DOI: <https://doi.org/10.4213/dm433>

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: 18.209.158.208

26 апреля 2023 г., 17:20:53

УДК 519.7

Об асимптотике логарифма числа пороговых функций K -значной логики

© 1998 г. А. А. Ирматов, Ж. Д. Ковиянич

В работе для числа $P(K, n)$ пороговых функций K -значной логики от n переменных получена оценка снизу

$$P(K, n+1) \geq \frac{1}{2} \binom{K^n}{\lfloor n-4-2n/\log_K n \rfloor} P(K, \lfloor 2n/\log_K n + 4 \rfloor).$$

Для вывода этой оценки обобщается на K -значный случай результат Оддызко. Именно, доказано, что при $n \rightarrow \infty$ для любого $p \leq n - (3 + \log_{2Q} 36)n/\log_{2Q} n$ при $K = 2Q$ (соответственно для любого $p \leq n - (3 + \log_{2Q+1} 36)n/\log_{2Q+1} n$ при $K = 2Q + 1$) вероятность того, что линейная оболочка p случайно выбранных векторов $v_1, v_2, \dots, v_p \in (E'_K)^n = \{\pm 1, \pm 3, \dots, \pm(2Q-1)\}^n$ (соответственно $E'_K = \{0, \pm 1, \dots, \pm Q\}^n$) содержит хотя бы один вектор из $(E'_K)^n \setminus \bigcup_{i=1}^p \langle v_i \rangle$, соответственно из $E'_K \setminus \bigcup_{i=1}^p \langle v_i \rangle$, равняется при четном $K = 2Q$ для $Q \neq 1$

$$4 \binom{p}{3} \left(\frac{2}{3} + \frac{1}{12Q^2} \right)^n + O \left(p^3 \left(\frac{2}{3} + \frac{Q-3}{12Q^3} \right)^n \right),$$

а для $Q = 1$

$$4 \binom{p}{3} \left(\frac{3}{4} \right)^n + O \left(p^4 \left(\frac{5}{8} \right)^n \right),$$

и соответственно для нечетного $K = 2Q + 1$ и $Q \neq 1$

$$2 \binom{p}{2} \left(\frac{3}{4} + \frac{1}{4(2Q+1)^2} \right)^n + O \left(p^2 \left(\frac{3}{4} - \frac{7}{4(2Q+1)^2} \right)^n \right),$$

а для $Q = 1$

$$2 \binom{p}{2} \left(\frac{7}{9} \right)^n + O \left(p^3 \left(\frac{17}{27} \right)^n \right).$$

Работа первого автора выполнена при поддержке Миннауки Российской Федерации, проект «Перспективные информационные технологии» №0201.05.028.

1. Введение

Пусть

$$\begin{aligned} E_K &= \{0, \pm 1, \dots, \pm Q\}, & K &= 2Q + 1, \\ E'_K &= \{\pm 1, \pm 3, \dots, \pm(2Q-1)\}, & K &= 2Q. \end{aligned}$$

Функция $f: E_K^n \rightarrow \{-1, 1\}$ (соответственно $f: (E'_K)^n \rightarrow \{-1, 1\}$) называется пороговой, если существуют вещественные числа $a_0, \dots, a_n$ такие, что $f(x_1, \dots, x_n) = 1$ тогда и только тогда, когда $a_1 x_1 + \dots + a_n x_n + a_0 \geq 0$.

Отождествим пороговую функцию с вектором $(a_0, a_1, \dots, a_n)$ в $(n+1)$ -мерном евклидовом пространстве, а набору $(x_1, \dots, x_n)$, на котором задана функция сопоставим $(n+1)$ -мерный вектор $(1, x_1, \dots, x_n)$. Значение функции на наборе определяется знаком скалярного произведения вектор-функции и вектор-набора. Тогда подсчет пороговых функций сводится к подсчету числа $C(H)$ открытых многогранных конусов, на которые $(n+1)$ -мерное пространство разбивается проходящими через начало координат $(2Q+1)^n$ (соответственно $(2Q)^n$) гиперплоскостями с нормальными векторами из множества

$$H = \{(1, b_1, \dots, b_n) \mid b_i \in E_K(E'_K), i = 1, \dots, n\}.$$

Это дает один из способов получения верхних и нижних оценок числа пороговых функций, которое будем обозначать через $P(K, n)$. Верхняя оценка числа $C(A)$ для произвольного множества A нормальных векторов была получена Шлефли в 1850 году (см. [1]) и в нашем случае имеет вид

$$P(K, n) \leq 2 \sum_{i=0}^n \binom{K^n - 1}{i}. \quad (1)$$

В данной работе мы обобщаем полученную в [2] оценку

$$P(2, n) > 2^{n^2(1-7/\ln n)} P(2, [7(n-1) \ln 2 / \ln(n-1)]),$$

с использованием метода, предложенного в этой работе. Попутно мы обобщаем основной результат работы [3], что хотя и продиктовано нашей основной целью, но представляет самостоятельный интерес.

2. K -значное обобщение леммы Литлвуда–Оффорда

Пользуясь хорошо известной леммой Шпернера (см. [4]), Эрдёш [5] доказал следующее утверждение, сформулированное Литлвудом и Оффордом.

Лемма 1. Для любых вещественных чисел c, r, a_i таких, что $r > 0, |a_i| \geq r, i = 1, \dots, n$, число наборов $(\varepsilon_1, \dots, \varepsilon_n) \in \{\pm 1\}^n$, удовлетворяющих условию $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n \in (c - r, c + r)$, не превосходит $\binom{n}{\lfloor n/2 \rfloor}$.

В [3] использован следующий вариант леммы 1.

Следствие 1. Для любого вещественного числа c и любых ненулевых вещественных чисел $a_1, \dots, a_n$ максимальное число векторов $(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}^n$ таких, что $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = c$, не превосходит $\binom{n}{\lfloor n/2 \rfloor}$.

Следующая лемма является обобщением на K -значный случай леммы Литлвуда–Оффорда и необходима нам для оценки соответствующих вероятностей в общем случае.

Лемма 2. Пусть $a_1, \dots, a_n \in \mathbf{R} \setminus \{0\}$ и $c \in \mathbf{R}$. Тогда для любых $K, n \in \mathbf{N}$, $K \geq 2$, число наборов $(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1, \dots, K-1\}^n$, удовлетворяющих условию $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = c$, не превосходит $K^{n+1}/(2\sqrt{n})$.

Доказательство. Доказательство проведем методом математической индукции по K . Для случая $K = 2$, утверждение следует из леммы Литлвуда–Оффорда. Предположим, что для всех чисел $K \leq k$ наше утверждение доказано. Докажем утверждение леммы для $K = k + 1$. Из предположения индукции следует, что существует не более $k^{n+1}/(2\sqrt{n})$ векторов $(\varepsilon_1, \dots, \varepsilon_n) \in \{1, \dots, k\}^n$ таких, что

$$(\varepsilon_1 - 1)a_1 + \dots + (\varepsilon_n - 1)a_n = c - \sum_{i=1}^n a_i,$$

что эквивалентно равенству

$$\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = c.$$

Поэтому максимальное число n -векторов $(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1, \dots, k\}^n$, удовлетворяющих тому же тождеству, не превосходит

$$1 + \sum_{s=1}^n \binom{n}{s} \frac{k^{s+1}}{2\sqrt{s}}.$$

Здесь s указывает на число индексов i , для которых $\varepsilon_i \neq 0$. Нетрудно видеть, что

$$\begin{aligned} 1 + \sum_{s=1}^n \binom{n}{s} \frac{k^{s+1}}{2\sqrt{s}} &= 1 + \sum_{s=1}^n \binom{n}{s} \frac{k^{s+1}}{s+1} \frac{s+1}{2\sqrt{s}} \\ &\leq 1 + \frac{1}{2} \frac{n+1}{\sqrt{n}} \sum_{s=1}^n \binom{n}{s} \frac{k^{s+1}}{s+1} \leq \frac{1}{2} \frac{n+1}{\sqrt{n}} \sum_{s=0}^n \binom{n}{s} \frac{k^{s+1}}{s+1} \\ &= \frac{(k+1)^{n+1} - 1}{2\sqrt{n}} < \frac{(k+1)^{n+1}}{2\sqrt{n}}. \end{aligned}$$

Лемма 3. Пусть $n \in \mathbf{N}$, $c \in \mathbf{R}$, $a_1, \dots, a_n \in \mathbf{R} \setminus \{0\}$. Тогда существует не более K^{n-1} векторов $(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1, \dots, K-1\}^n$, удовлетворяющих равенству $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = c$.

Доказательство. Расслоим решетку $\{0, 1, \dots, K-1\}^n$ на K слоев вида $x_n = i$, $i = 0, \dots, K-1$. Тогда каждая точка $\bar{\varepsilon} = (\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1, \dots, K-1\}^n$ принадлежит одному из слоев решетки. Так как $a_1 \neq 0$, максимальное число $\bar{\varepsilon}$ -точек, принадлежащих пересечению гиперплоскости $a_1 x_1 + \dots + a_n x_n = c$ с любым фиксированным слоем, не превосходит числа проекций этих точек на гиперплоскость $x_1 = 0$, а это не больше, чем K^{n-2} , что и требовалось доказать.

Из лемм 2 и 3 вытекает следующая теорема.

Теорема 1. Для любых $K = 2Q + 1$, $n \in \mathbf{N}$ и $a_1, \dots, a_n \in \mathbf{R} \setminus \{0\}$, $c \in \mathbf{R}$ вероятность $p_n^{[2Q+1]}$, для $K = 2Q$ соответственно $p_n^{[2Q]}$, выбора случайного вектора

$$(\varepsilon_1, \dots, \varepsilon_n) \in \{0, \pm 1, \dots, \pm Q\}^n,$$

соответственно

$$(\varepsilon_1, \dots, \varepsilon_n) \in \{\pm 1, \pm 3, \dots, \pm(2Q-1)\}^n,$$

удовлетворяющего условию $\varepsilon_1 a_1 + \dots + \varepsilon_n a_n = c$, не превосходит

$$\min \left\{ \frac{1}{2Q+1}, \frac{2Q+1}{2\sqrt{n}} \right\},$$

соответственно

$$\min \left\{ \frac{1}{2Q}, \frac{Q}{\sqrt{n}} \right\}.$$

3. K -значное обобщение теоремы Одлызко

Назовем матрицу $M_{m \times n}$ размера $m \times n$ со строками из множества E_K^n вырожденной, если существует линейная комбинация ее строк с ненулевыми коэффициентами, принадлежащая множеству E_K^n . Пусть R_m вероятность того, что случайная матрица $M_{m \times n}$ вырожденная. Аналогичные определения можно дать для матриц со строками из множества $(E'_K)^n$. Для фиксированного p и любого $m \leq p$ обозначим через P_m , соответственно P'_m , вероятность того, что из p случайно выбранных векторов $v_1, \dots, v_p \in E_K^n$, соответственно $v_1, \dots, v_p \in (E'_K)^n$, можно найти m векторов, образующих вырожденную матрицу. Очевидно, что $P_m \leq \binom{p}{m} R_m$ (соответственно $P'_m \leq \binom{p}{m} R'_m$).

В этом параграфе мы найдем асимптотику вероятности P_2 и P'_3 и докажем, что $P_m = o(P_2)$ при $n \rightarrow \infty$ и

$$2 \neq m \leq p \leq n - (3 + \log_{2Q+1} 36) \frac{n}{\log_{2Q+1} n}$$

и $P'_m = o(P_3)$ при $n \rightarrow \infty$ и

$$3 \neq m \leq p \leq n - (3 + \log_{2Q} 36) \frac{n}{\log_{2Q} n}.$$

Лемма 4. Для любого p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$P_2 \leq 2 \binom{p}{2} \left(\frac{3}{4} + \frac{1}{4(2Q+1)^2} \right)^n + O \left(p^2 \left(\frac{3}{4} - \frac{7}{4(2Q+1)^2} \right)^n \right), \quad (2)$$

$$P'_2 \leq 2 \binom{p}{2} \left(\frac{1}{2} \right)^n + O \left(p^2 \left(\frac{2Q^2-2}{(2Q)^2} \right)^n \right). \quad (3)$$

Доказательство. Пусть $M_{2 \times n}$ — вырожденная матрица со строками, принадлежащими множеству E_K^n . Тогда существует двойка (α_1, α_2) , $\alpha_1, \alpha_2 \in \mathbf{R} \setminus \{0\}$, такая, что для каждого столбца $(\varepsilon_1, \varepsilon_2)^T$ матрицы $M_{2 \times n}$ соответствующая ему точка решетки $C = \{0, \pm 1, \dots, \pm Q\}^2$ принадлежит одной из $2Q+1$ -прямых h_l :

$$\alpha_1 x + \alpha_2 y = l, \quad l = 0, \pm 1, \dots, \pm Q.$$

Обозначим через L_i , $i = 0, \pm 1, \dots, \pm Q$, число точек решетки C , принадлежащих прямой h_i . Нетрудно показать, что

$$L = \sum_{i=-Q}^Q L_i$$

Рис. 1.

достигает своего максимума в двух случаях. Один из них показан на рис. 1.

Рисунок для второго случая получается из рисунка для первого случая отражением относительно оси x . Таким образом, максимальное число различных столбцов, которые могут появиться в вырожденной матрице, не превосходит числа

$$L = L_0 + 2 \sum_{i=1}^Q L_i = 3Q^2 + 3Q + 1.$$

Обозначим эти множества вектор-столбцов через E_1 и E_2 соответственно. Они соответствуют наборам $\bar{\alpha}_1 = (1, 1)$ и $\bar{\alpha}_2 = (1, -1)$. Легко обнаружить, что для любого другого набора $\bar{\alpha} = (\alpha_1, \alpha_2)$, $\alpha_i \in R \setminus \{0\}$, порождающего множество вектор-столбцов E , отличное от множеств E_1 и E_2 , мощность множества E не превосходит $L - 2$, то есть любая вырожденная матрица размера $2 \times n$ такая, что $\bar{\alpha}M$ принадлежит E_K^n , имеет не более $L - 2$ различных столбцов, следовательно, при $n \rightarrow \infty$

$$R_2 = 2 \frac{L^n + O((L - 2)^n)}{(2Q + 1)^{2n}}. \quad (4)$$

Теперь утверждение леммы следует из неравенства

$$P_2 \leq \binom{p}{2} R_2.$$

Для четного случая, то есть для множества E'_K , определим числа L'_{2i-1} для $i = \pm 1, \pm 2, \dots, \pm Q$ и L' по аналогии с числами L_i и L в нечетном случае. Тогда число столбцов L' достигает максимума в двух случаях, соответствующих наборам $\bar{\alpha}'_1 = (1/2, 1/2)$ и $\bar{\alpha}'_2 = (1/2, -1/2)$. Соответствующие им множества вектор-столбцов

обозначим через E'_1 и E'_2 . Число L' вычисляется по формуле

$$L' = 2 \sum_{i=1}^Q L'_{2i-1},$$

где $L'_{2i-1} = 2Q - 2i + 1$, $i = 1, 2, \dots, Q$.

Следовательно, $L' = 2Q^2$ и

$$R'_2 = 2 \left(\frac{1}{2^n} + O \left(\frac{1}{2^n} \left(1 - \frac{1}{Q^2} \right)^n \right) \right).$$

Лемма 5. Для любого p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$P_3 \leq 4 \binom{p}{3} \left(\frac{2}{3} + \frac{1}{3(2Q+1)^2} \right)^n + O \left(p^3 \left(\frac{2}{3} + \frac{2Q-5}{3(2Q+1)^3} \right)^n \right), \quad (5)$$

$$P'_3 \leq 4 \binom{p}{3} \left(\frac{2}{3} + \frac{1}{12Q^2} \right)^n + O \left(p^3 \left(\frac{2}{3} + \frac{Q-3}{12Q^3} \right)^n \right). \quad (6)$$

Доказательство. Доказательство утверждения относительно вероятности P'_3 аналогично доказательству утверждения о вероятности P_3 , поэтому мы проведем доказательство для P_3 и дадим только необходимые для четного случая параметры и константы.

Пусть $M_{3 \times n}$ — вырожденная $(\pm 1, \dots, \pm Q)$ -матрица. Тогда существует тройка чисел $(\alpha_1, \alpha_2, \alpha_3)$, $\alpha_i \in \mathbf{R} \setminus \{0\}$, такая, что для каждого столбца $(\varepsilon_1, \varepsilon_2, \varepsilon_3)^T$ матрицы $M_{3 \times n}$ соответствующая ему точка решетки $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ принадлежит одной из $2Q+1$ гиперплоскостей

$$H_l: \alpha_1 x + \alpha_2 y + \alpha_3 z = l, \quad l = 0, \pm 1, \dots, \pm Q.$$

Рассмотрим семейство C_i , состоящее из $2Q+1$ параллельных прямых, являющихся пересечением гиперплоскости H_i с гиперплоскостями π_l в $\mathbf{R}^3$ вида $z = l$, $l = 0, \pm 1, \dots, \pm Q$. Так как $\alpha_3 \neq 0$, любые две прямые из этого семейства при проекции вдоль оси z не проектируются друг на друга. Обозначим через L_i , $i = 0, \pm 1, \dots, \pm Q$, число точек решетки $C = \{0, \pm 1, \dots, \pm Q\}^3$, принадлежащих гиперплоскости H_i . Заметим, что число L_i не превосходит числа точек из подмножества $\{0, \pm 1, \dots, \pm Q\}^2$ гиперплоскости π_0 , лежащих в образе проекции множества C_i вдоль оси z на гиперплоскость π_0 . Для каждого набора $\bar{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$ положим

$$E_{\bar{\alpha}} = \bigcup_{l=-Q}^Q H_l \cap C.$$

Нетрудно показать, что множество $E_{\bar{\alpha}}$ имеет максимальную мощность в четырех случаях, а именно, для наборов

$$\bar{\alpha} \in \{(-1, 1, 1), (1, -1, 1), (-1, -1, 1), (1, 1, 1)\}.$$

Для первых двух наборов проекция множества C_0 вдоль оси z на гиперплоскость π_0 показана на рис. 2.

Рис. 2.

Следовательно, для наборов $\bar{\alpha}$, для которых множество $E_{\bar{\alpha}}$ имеет максимальную мощность,

$$L_i = L_{-i} = ((Q - i + 1) + \dots + 2Q) + (2Q + 1) + (2Q + \dots + (Q + i + 1))$$

для всех i , $1 \leq i \leq Q$. Таким образом, максимальное число различных столбцов, которые могут появиться в вырожденной матрице, не превосходит числа

$$L = L_0 + 2 \sum_{i=1}^Q L_i = \frac{16}{3}Q^3 + 8Q^2 + \frac{14}{3}Q + 1$$

и только для наборов $\bar{\alpha} \in \{(1, -1, 1), (-1, 1, 1), (-1, -1, 1), (1, 1, 1)\}$ существуют вырожденные $M_{3 \times n}$ матрицы с L различными столбцами, удовлетворяющие условию $\bar{\alpha}M \in E_K^n$. Для векторов $\bar{\alpha} = (1, -1, 1)$ и $\bar{\alpha} = (-1, 1, 1)$ векторы-столбцы $M_{3 \times n}$ лежат в экстремальных сечениях C_i , $i = 0, \pm 1, \dots, \pm Q$, проекции которых на плоскость π_0 для $i = 0$ представлены на рис. 2. Для векторов $\bar{\alpha} = (-1, -1, 1)$ и $\bar{\alpha} = (1, 1, 1)$ векторы-столбцы $M_{3 \times n}$ лежат в экстремальных сечениях C_i , $i = 0, \pm 1, \dots, \pm Q$, проекции которых получаются из предыдущих симметричным отражением относительно оси x . Обозначим эти множества вектор-столбцов через E_1, E_2, E_3 и E_4 соответственно. Теперь легко показать, что для любого другого набора $\bar{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$, $\alpha_i \in \mathbf{R} \setminus \{0\}$, $i = 1, 2, 3$, любая вырожденная матрица размера $3 \times n$ такая, что $\bar{\alpha}M$ принадлежит E_K^n , имеет не более $L - 2$ различных столбцов, то есть при $n \rightarrow \infty$

$$R_3 = 4 \frac{L^n + O((L - 2)^n)}{(2Q + 1)^{3n}}. \quad (7)$$

Теперь утверждение леммы следует из неравенства

$$P_3 \leq \binom{p}{3} R_3.$$

Для четного случая, то есть для множества $(E'_K)^n$, максимальное число различных столбцов L' вычисляется по формуле

$$L' = 2 \sum_{i=1}^Q L_{2i-1},$$

где

$$L_{2i-1} = ((Q - i + 1) + \dots + (2Q - 1)) + (2Q + \dots + (Q + i)) = 3Q^2 - i^2 + i,$$

и достигается на множествах вектор-столбцов E'_1, E'_2, E'_3, E'_4 , соответствующих наборам

$$\bar{\alpha} = \{(1, -1, 1), (-1, 1, 1), (-1, -1, 1), (1, 1, 1)\}.$$

Следовательно,

$$L' = \frac{2}{3}(8Q^3 + Q).$$

Через $\tilde{P}'_3$ обозначим вероятность следующего события: среди p случайно выбранных векторов $v_1, \dots, v_p \in (E'_K)^n$ существуют два подмножества множества их индексов

$$I = \{i_1, i_2, i_3\} \subset \{1, \dots, p\}, \quad J = \{j_1, j_2, j_3\} \subset \{1, \dots, p\}$$

такие, что множества векторов

$$V = \{v_{i_1}, v_{i_2}, v_{i_3}\}, \quad W = \{v_{j_1}, v_{j_2}, v_{j_3}\}$$

образуют вырожденные матрицы. Используя формулу включения-исключения, легко получить, что

$$\binom{p}{3} R'_3 - \tilde{P}'_3 \leq P'_3 \leq \binom{p}{3} R'_3. \quad (8)$$

Лемма 6. Для любого p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$\tilde{P}'_3 \leq O\left(p^4 \left(\frac{(2Q-1)L' + 4Q^2}{(2Q)^4}\right)^n\right),$$

где

$$L' = \frac{2}{3}(8Q^3 + Q).$$

Доказательство. Для взаиморасположения множеств индексов I и J существуют три возможности

$$I \cap J = \emptyset, \quad |I \cap J| = 1, \quad |I \cap J| = 2.$$

Через $q_i, i = 0, 1, 2$, обозначим вероятность того, что множества векторов V и W образуют вырожденные матрицы при условии, что $|I \cap J| = i$. Нетрудно заметить, что

$$q_0 = (R'_3)^2. \quad (9)$$

Далее,

$$q_1 = \frac{N_1}{(2Q)^{5n}}, \quad (10)$$

где N_1 — число $(\pm 1, \dots, \pm(2Q-1))$ -матриц M размера $5 \times n$, удовлетворяющих одному из следующих трех условий:

- (1) подматрица $M_{[1,4,5]}$, полученная в результате вычеркивания второй и третьей строк матрицы M размера $5 \times n$, и подматрица $M_{[1,2,3]}$, полученная в результате вычеркивания четвертой и пятой строк, являются вырожденными и в каждой из них не более $L' - 2$ различных столбцов, где L' — число из леммы 5;
- (2) обе подматрицы $M_{[1,4,5]}$ и $M_{[1,2,3]}$ являются вырожденными, но одна из них имеет L' или $L' - 1$ различных столбцов, а вторая имеет не более чем $L' - 2$ различных столбцов;
- (3) обе подматрицы $M_{[1,4,5]}$ и $M_{[1,2,3]}$ являются вырожденными и имеют L' или $L' - 1$ различных столбцов, принадлежащих множеству E'_i , $i = 1, 2, 3, 4$, где множества E'_i определены в доказательстве леммы 5.

Оценим сверху вероятность q_1 . Пусть S_i — множество матриц размера $5 \times n$, удовлетворяющих условию (i), $i = 1, 2, 3$. Тогда $N_1 = |S_1| + |S_2| + |S_3|$ и при $n \rightarrow \infty$

$$|S_1| \leq (2Q)^{2n} \sum_{i=1}^{L'-2} \binom{(2Q)^3}{i} i^n = O((2Q)^{2n} (L' - 2)^n),$$

$$|S_2| \leq 2(2Q)^{2n} \sum_{i=1}^{L'-2} \binom{(2Q)^3}{i} i^n = O((2Q)^{2n} (L' - 2)^n).$$

Нетрудно проверить, что максимальное число векторов множества E'_i , $i = 1, 2, 3, 4$, с одной и той же первой координатой равно $3Q^2$, откуда легко получить, что

$$|S_3| \leq (L')^n (3Q^2)^n.$$

Следовательно, при $n \rightarrow \infty$

$$q_1 \leq O\left(\left(\frac{3Q^2 L'}{(2Q)^5}\right)^n\right). \quad (11)$$

Оценим сверху вероятность q_2 . Заметим, что

$$q_2 = \frac{N_2}{(2Q)^{4n}}, \quad (12)$$

где $N_2 = |s_1| + |s_2| + |s_3|$ и множества s_1, s_2, s_3 являются подмножествами множества $(0, \pm 1, \dots, \pm(2Q-1))$ -матриц M размера $4 \times n$, удовлетворяющих следующим условиям соответственно:

- (1) подматрица $M_{[1,2,3]}$, полученная в результате вычеркивания четвертой строки, и подматрица $M_{[1,2,4]}$, полученная в результате вычеркивания третьей строки, являются вырожденными и в каждой из них не более $L' - 2$ различных столбцов;

- (2) обе подматрицы $M_{[1,2,3]}$ и $M_{[1,2,4]}$ являются вырожденными, но одна из них имеет L или $L' - 1$ различных столбцов, а вторая имеет не более $L' - 2$ различных столбцов,
- (3) обе подматрицы $M_{[1,2,3]}$ и $M_{[1,2,4]}$ являются вырожденными и имеют L' или $L' - 1$ различных столбцов.

Нетрудно видеть, что при $n \rightarrow \infty$

$$|s_1| \leq (2Q)^n \sum_{i=1}^{L'-2} \binom{(2Q)^3}{i} i^n = O((2Q)^n (L' - 2)^n),$$

$$|s_2| \leq O((2Q)^n (L' - 2)^n).$$

Пусть все столбцы матрицы $M_{[1,2,3]}$ принадлежат множеству E'_1 или E'_2 . Обозначим через r число столбцов вида $(l, l)^T$, $l = \pm 1, \dots, \pm(2Q - 1)$, в подматрице $M_{[1,2]}$, соответствующей одинаковым векторам множеств V и W . Если все столбцы матрицы $M_{[1,2,3]}$ принадлежат множествам E'_3 или E'_4 , то вместо столбцов вида $(l, l)^T$ подматрицы $M_{[1,2]}$ будем рассматривать столбцы вида $(l, -l)$, $l = \pm 1, \dots, \pm(2Q - 1)$. Тогда

$$\begin{aligned} |s_3| &\leq 4 \sum_{r=(2Q)^2}^n \binom{n}{r} ((2Q)^{2r} (L' - (2Q)^2)^{n-r} (2Q)^r (2Q - 1)^{n-r}) \\ &\leq 4 \sum_{r=1}^n \binom{n}{r} ((2Q)^{3r} ((L' - (2Q)^2)(2Q - 1))^{n-r}) \\ &= 4((2Q)^3 + (2Q - 1)(L' - (2Q)^2))^n, \end{aligned}$$

откуда получаем, что при $n \rightarrow \infty$

$$q_2 \leq O\left(\left(\frac{(2Q - 1)L' + (2Q)^2}{(2Q)^4}\right)^n\right), \quad (13)$$

Комбинируя неравенства (9), (11), (13), получим, что при $n \rightarrow \infty$

$$\tilde{P}'_3 \leq O\left(p^4 \left(\frac{(2Q - 1)L' + (2Q)^2}{(2Q)^4}\right)^n\right).$$

Аналогично предыдущему случаю через $\tilde{P}_2$ обозначим вероятность события: среди p случайно выбранных векторов $v_1, \dots, v_p \in E_K^n$ существуют два подмножества множества их индексов

$$I = \{i_1, i_2\} \subset \{1, \dots, p\}, \quad J = \{j_1, j_2\} \subset \{1, \dots, p\}$$

такие, что множества векторов

$$V = \{v_{i_1}, v_{i_2}\}, \quad W = \{v_{j_1}, v_{j_2}\}$$

образуют вырожденные матрицы. Используя формулу включения-исключения, получаем, что

$$\binom{p}{2} R_2 - \tilde{P}_2 \leq P_2 \leq \binom{p}{2} R_2. \quad (14)$$

Лемма 7. Для любого p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$\tilde{P}_2 \leq O\left(p^3 \left(\frac{2QL + 2Q + 1}{(2Q + 1)^3}\right)^n\right).$$

Доказательство. Для взаиморасположения множеств индексов I и J теперь существуют две возможности: $I \cap J = \emptyset$ и $|I \cap J| = 1$. Через q_i , $i = 0, 1$, обозначим вероятность того, что множества векторов V и W образуют вырожденные матрицы при условии, что $|I \cap J| = i$. Нетрудно заметить, что

$$q_0 = R_2^2. \quad (15)$$

$$q_1 = \frac{N}{(2Q + 1)^{3n}}, \quad (16)$$

где N — число $(0, \pm 1, \dots, \pm Q)$ -матриц M размера $3 \times n$, удовлетворяющих одному из следующих трех условий:

- (1) подматрица $M_{[1,2]}$, полученная в результате вычеркивания третьей строки матрицы M размера $3 \times n$, и подматрица $M_{[1,3]}$, полученная в результате вычеркивания второй строки, являются вырожденными и в каждой из них не более $L - 2$ различных столбцов, где L — число, определенное в доказательстве леммы 4;
- (2) обе подматрицы $M_{[1,2]}$ и $M_{[1,3]}$ являются вырожденными, но одна из них имеет L или $L - 1$ различных столбцов, а вторая имеет не более чем $L - 2$ различных столбцов;
- (3) обе подматрицы $M_{[1,2]}$ и $M_{[1,3]}$ являются вырожденными и имеют L или $L - 1$ различных столбцов, принадлежащих множеству E_i , $i = 1, 2$, из доказательства леммы 4.

Оценим сверху вероятность q_1 . Пусть S_i — множество матриц размера $3 \times n$, удовлетворяющих условию i), $i = 1, 2, 3$. Тогда $N = |S_1| + |S_2| + |S_3|$ и при $n \rightarrow \infty$

$$|S_1| \leq (2Q + 1)^n \sum_{i=1}^{L-2} \binom{(2Q + 1)^2}{i} i^n = O((2Q + 1)^n (L - 2)^n),$$

$$|S_2| \leq 2(2Q + 1)^n \sum_{i=1}^{L-2} \binom{(2Q + 1)^2}{i} i^n = O((2Q + 1)^n (L - 2)^n).$$

Пусть все столбцы матрицы $M_{[1,2]}$ принадлежат множеству E_1 (или E_2). Обозначим через r число столбцов вида $(0, l)^T$, $l = 0, \pm 1, \dots, \pm Q$, в подматрице $M_{[1,2]}$. Тогда

$$\begin{aligned} |S_3| &\leq 2 \sum_{r=2Q+1}^n \binom{n}{r} (2Q + 1)^r (L - (2Q + 1))^{n-r} (2Q + 1)^r (2Q)^{n-r} \\ &\leq 2 \sum_{r=1}^n \binom{n}{r} (2Q + 1)^{2r} ((L - (2Q + 1))2Q)^{n-r} \\ &= 2((2Q + 1)^2 + 2Q(L - (2Q + 1)))^n = 2(2Q + 1 + 2QL)^n, \end{aligned}$$

откуда получаем, что при $n \rightarrow \infty$

$$q_1 \leq O\left(\left(\frac{2Q+1+2QL}{(2Q+1)^3}\right)^n\right). \quad (17)$$

Комбинируя неравенства (15) и (17), получим, что при $n \rightarrow \infty$

$$\bar{P}_2 \leq O\left(p^3 \frac{(2QL+2Q+1)^n}{(2Q+1)^{3n}}\right).$$

Из лемм 4, 5, 6 и 7 вытекают следующие теоремы.

Теорема 2. Для любых $Q \in \mathbb{N}$, $Q \neq 1$, p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$P_2 = 2 \binom{p}{2} \left(\frac{3}{4} + \frac{1}{4(2Q+1)^2}\right)^n + O\left(p^2 \left(\frac{3}{4} - \frac{7}{4(2Q+1)^2}\right)^n\right),$$

а для $Q = 1$

$$P_2 = 2 \binom{p}{2} \left(\frac{7}{9}\right)^n + O\left(p^3 \left(\frac{17}{27}\right)^n\right).$$

Теорема 3. Для любых $Q \in \mathbb{N}$, $Q \neq 1$, p , $1 \leq p \leq n$, при $n \rightarrow \infty$

$$P'_3 = 4 \binom{p}{3} \left(\frac{2}{3} + \frac{1}{12Q^2}\right)^n + O\left(p^3 \left(\frac{2}{3} + \frac{Q-3}{12Q^3}\right)^n\right),$$

а для $Q = 1$

$$P'_3 = 4 \binom{p}{3} \left(\frac{3}{4}\right)^n + O\left(p^4 \left(\frac{5}{8}\right)^n\right).$$

Среди всех векторов $\bar{a} = (a_1, a_2, \dots, a_m) \in \mathbf{R}^m$, $a_i \neq 0$, $i = 1, \dots, m$, выберем вектор, для которого мощность множества $\{\bar{x} \mid \bar{x} \in (E'_K)^m, \langle \bar{a}, \bar{x} \rangle \in E'_K\}$ достигает максимального значения $L'^{[m]}$. Аналогично определим число $L^{[m]}$.

Лемма 8. При $m > 3$

$$\frac{L'^{[m]}}{(2Q)^m} \leq \frac{1}{2},$$

если m чётно, и

$$\frac{L'^{[m]}}{(2Q)^m} \leq \max \left\{ \frac{1}{2}, \frac{L'^{[3]}}{(2Q)^3} - \frac{1}{2Q+1} \left(1 - \frac{1}{(2Q)^{m-1}}\right) \right\},$$

если m нечётно.

При $m \geq 3$

$$\frac{L'^{[m]}}{(2Q)^m} \leq \frac{L^{[2]}}{(2Q+1)^2} - \frac{1}{(2Q+1)^2} \left(1 - \frac{1}{(2Q+1)^{m-2}}\right).$$

Здесь

$$L'^{[3]} = \frac{2}{3}(8Q^3 + Q), \quad L^{[2]} = 3Q^2 + 3Q + 1.$$

Доказательство. Без ограничения общности мы можем считать, что все коэффициенты вектора $\bar{a}$ положительны. Предположим, что существуют два из них, например, a_1 и a_2 , такие, что $a_1 \neq a_2$. Тогда для каждого фиксированного $(m-2)$ -набора $(x_3, x_4, \dots, x_m) \in (E'_K)^{m-2}$ выполнено неравенство

$$\left| \bigcup_{i \in E'_K} \left\{ (x_1, x_2) \mid a_1 x_1 + a_2 x_2 = - \sum_{i=3}^m a_i x_i + i \right\} \cap (E'_K \times E'_K) \right| \leq 2Q^2.$$

Следовательно,

$$|\{\bar{x} \mid \bar{x} \in (E'_K)^m, \langle \bar{a}, \bar{x} \rangle \in E'_K\}| < 2Q^2(2Q)^{m-2} = Q(2Q)^{m-1}. \quad (18)$$

Рассмотрим случай, когда $a_1 = a_2 = \dots = a_m = 1/c$ для некоторого $c \in \mathbf{R}$.

Пусть m — четное число. Из условия $\langle \bar{a}, \bar{x} \rangle \in E'_K$, $\bar{x} \in (E'_K)^m$, следует, что

$$x_m = - \sum_{i=1}^{m-1} x_i + ci, \quad i = \pm 1, \dots, \pm(2Q-1).$$

Зафиксируем вектор $(x_1, \dots, x_{m-1}) \in (E'_K)^{m-1}$ и введем обозначение

$$s = - \sum_{i=1}^{m-1} x_i.$$

Нам необходимо определить максимальное число различных $x_m \in E'_K$, удовлетворяющих условию $x_m = s + ci$ для некоторого $i \in \{\pm 1, \dots, \pm(2Q-1)\}$. Так как число m четное, число s нечетное и, следовательно, ci должно быть четным. Нетрудно заметить, что максимальным число различных чисел i из множества $\{\pm 1, \dots, \pm(2Q-1)\}$, удовлетворяющих условию $s + ci \in E'_K$ будет при $c = 2$. Так как

$$|\{s + 2i \mid i \in \{\pm 1, \dots, \pm(2Q-1)\}\} \cap E'_K| \leq |E'_K|/2,$$

для каждого четного m и $c \in \mathbf{R}$ верно неравенство

$$|\{\bar{x} \mid \bar{x} \in (E'_K)^m, \langle \bar{1}/c, \bar{x} \rangle \in E'_K\}| < Q(2Q)^{m-1}. \quad (19)$$

Пусть m — нечетное число. Если $c \neq 1$, то не более Q чисел вида $s + ci$, $i \in \{\pm 1, \dots, \pm(2Q-1)\}$, принадлежат множеству E'_K , и, следовательно, в этом случае будет выполнено неравенство (19). Пусть $c = 1$. Зафиксируем вектор $(x_{m-1}, x_m) \in E'_K \times E'_K$. Оценим сверху число векторов $(x_1, \dots, x_{m-2}) \in (E'_K)^{m-2}$, удовлетворяющих хотя бы одному из уравнений

$$x_1 + \dots + x_{m-2} = -(x_{m-1} + x_m) + i, \quad i \in \{\pm 1, \dots, \pm(2Q-1)\}.$$

Если $x_{m-1} = -x_m$, то число таких векторов не больше $L^{[m-2]}$. В случае $x_{m-1} \neq -x_m$ нам необходимо оценить число N_s векторов $(x_1, \dots, x_{m-2}) \in (E'_K)^{m-2}$, удовлетворяющих хотя бы одному уравнению

$$x_1 + \dots + x_{m-2} = s + i, \quad s \neq 0, \quad i \in \{\pm 1, \dots, \pm(2Q-1)\}.$$

Мы утверждаем, что число N_s достигает своего максимума при $s = 0$. Для этого достаточно показать, что число решений M_d^m вида $(x_1, \dots, x_m) \in (E'_K)^m$ уравнения

$x_1 + \dots + x_m = d$ для целочисленных положительных d_1, d_2 , удовлетворяет неравенству $M_{d_1}^m \geq M_{d_2}^m$, если $d_1 < d_2$ и $d_2 - d_1$ — четное число. Если $M_{d_1}^1 > 0$, то для $m \geq 2$ верно неравенство $M_{d_1}^m > M_{d_2}^m$. Доказательство проведем математической индукцией по m . База индукции очевидна. Сопоставим каждому решению $(x_1, \dots, x_m)$ из $(E'_K)^m$ с $x_1 \neq -(2Q-1)$ уравнения $x_1 + \dots + x_m = d_2$ решение $(x_1 - 2, \dots, x_m) \in (E'_K)^m$ уравнения $x_1 + \dots + x_m = d_1$. Пусть $(-(2Q-1), x_2, \dots, x_m) \in (E'_K)^m$ — решение уравнения $x_1 + \dots + x_m = d_2$, то есть $(x_2, \dots, x_m) \in (E'_K)^{m-1}$ удовлетворяет уравнению $x_2 + \dots + x_m = d_2 + (2Q-1)$. Так как множество E'_K симметрично, число решений $M_{d_2+(2Q-1)}^{m-1}$ последнего уравнения по предположению индукции не превосходит числа решений $M_{|d_1-(2Q-1)|}^{m-1}$ уравнения $x_2 + \dots + x_m = d_2 - (2Q-1)$, то есть число решений уравнения $x_1 + \dots + x_m = d_2$ с $x_1 = -(2Q-1)$ не превосходит числа решений уравнения $x_1 + \dots + x_m = d_1$ с $x_1 = 2Q-1$, что нам и требовалось.

Таким образом, при $x_{m-1} \neq x_m$ число векторов $(x_1, \dots, x_{m-2}) \in (E'_K)^{m-2}$, удовлетворяющих хотя бы одному из уравнений

$$x_1 + \dots + x_{m-2} = -(x_{m-1} + x_m) + i, \quad i \in \{\pm 1, \dots, \pm(2Q-1)\}$$

не превосходит $L^{[m-2]} - 1$. Следовательно,

$$\begin{aligned} |\{\bar{x} \mid \bar{x} \in (E'_K)^m, \langle \bar{1}/c, \bar{x} \rangle \in E'_K\}| &\leq 2Q(L^{[m-2]} + ((2Q)^2 - 2Q)(L^{[m-2]} - 1)) \\ &= (2Q)^2 L^{[m-2]} - 2Q(2Q-1). \end{aligned} \quad (20)$$

Теперь первое утверждение леммы следует из (18), (19) и (20).

При доказательстве второго утверждения леммы нет необходимости рассматривать отдельно случаи четного и нечетного m . Здесь ключевое неравенство выглядит так:

$$L^{[m]} \leq L^{[m-1]} + 2Q(L^{[m-1]} - 1) = (2Q+1)L^{[m-1]} - 2Q,$$

то есть

$$\begin{aligned} \frac{L^{[m]}}{(2Q+1)^m} &\leq \frac{L^{[m-1]}}{(2Q+1)^{m-1}} - \frac{2Q}{(2Q+1)^m} \\ &\leq \frac{L^{[2]}}{(2Q+1)^2} - 2Q \left(\frac{1}{(2Q+1)^m} + \frac{1}{(2Q+1)^{m-1}} + \dots + \frac{1}{(2Q+1)^3} \right) \\ &= \frac{L^{[2]}}{(2Q+1)^2} - \frac{1}{(2Q+1)^2} \left(1 - \frac{1}{(2Q+1)^{m-2}} \right). \end{aligned}$$

Лемма 9. Для любых $K = 2Q$, $m, p \in \mathbb{N}$,

$$\frac{729}{16} Q^4 \leq m \leq p \leq n - (3 + \log_{2Q} 36) \frac{n}{\log_{2Q} n},$$

при $n \rightarrow \infty$

$$P'_m = o((2/3)^n).$$

Для любых $K = 2Q+1$, $m, p \in \mathbb{N}$,

$$\frac{729}{256} (2Q+1)^4 \leq m \leq p \leq n - (3 + \log_{2Q+1} 36) \frac{n}{\log_{2Q+1} n},$$

при $n \rightarrow \infty$

$$P_m = o((2/3)^n).$$

Доказательство. Для любого $0 \leq q \leq n - m$

$$R'_m \leq \mathbf{P}(A \mid B_{m,q,n}) + Q_{m,q}, \quad (21)$$

где событие A состоит в том, что случайная матрица $M_{m \times n}$ со строками из множества $(E'_K)^n$ является вырожденной; событие $B_{m,q,n}$ состоит в том, что матрица, составленная из первых $m + q$ столбцов случайной матрицы $M_{m \times n}$ имеет ранг m , и через $Q_{m,q}$ обозначена вероятность того, что матрица $M_{m \times (m+q)}$ размера $m \times (m+q)$ имеет ранг, меньший m .

Оценим сверху первое слагаемое. Пусть $j_1 < j_2 < \dots < j_m \leq m + q$ — линейно независимые столбцы матрицы $M_{m \times n}$. Тогда для любого $(\varepsilon_1, \dots, \varepsilon_m) \in (E'_K)^m$ существует единственный вектор коэффициентов $(\alpha_1, \dots, \alpha_m)$, $\alpha_i \in \mathbf{R}, i = 1, \dots, m$, удовлетворяющий следующему условию: координаты с номерами $j_1, j_2, \dots, j_m$ линейной комбинации векторов-строк матрицы $M_{m \times n}$ с коэффициентами $\alpha_1, \dots, \alpha_m$, равняются $\varepsilon_1, \dots, \varepsilon_m$ соответственно. Следовательно, существует не более $(2Q)^m$ векторов $\bar{\alpha} = (\alpha_1, \dots, \alpha_m)$, $\alpha_i \in \mathbf{R} \setminus \{0\}, i = 1, \dots, m$, таких, что первые $(m + q)$ координат вектора $\bar{\alpha} M_{m \times n}$ принадлежат множеству E'_K . Для фиксированного вектора $\bar{\alpha}$ вероятность того, что j -я координата вектора $\bar{\alpha} M_{m \times n}$ принадлежит множеству E'_K , не превосходит $p_m^{[2Q]}$, следовательно,

$$\begin{aligned} \mathbf{P}(A \mid B_{m,q,n}) &\leq \frac{\binom{m+q}{m} (2Q)^{m(m+q)} (2Q)^m ((2Q)^m p_m^{[2Q]} 2Q)^{n-(m+q)}}{(2Q)^{mn}} \\ &\leq (2Q)^{n-q} \binom{m+q}{m} (p_m^{[2Q]})^{n-m-q} \end{aligned} \quad (22)$$

и

$$Q_{m,q} \leq \sum_{i=1}^{m-1} (m-i) \binom{m}{i} \binom{m+q}{i} Q_{m,q,i}, \quad (23)$$

где $Q_{m,q,i}$ — вероятность того, что случайная $(\pm 1, \dots, \pm(2Q-1))$ -матрица размера $m \times (m+q)$ удовлетворяет следующим трем условиям:

- (1) любые i строк этой матрицы линейно независимы;
- (2) подматрица размера $i \times i$, находящаяся в верхнем левом углу, имеет ранг i ;
- (3) $(i+1)$ -я строка лежит в линейной оболочке первых i строк.

Если матрица $M_{m \times (m+q)}$ удовлетворяет этим условиям, то строки подматрицы размера $(i+1) \times i$, находящейся в верхнем левом углу, определяют единственные ненулевые коэффициенты $\alpha_1, \dots, \alpha_i$ такие, что для первых i столбцов $\tilde{v}_1, \dots, \tilde{v}_{i+1}$ выполнено тождество

$$\alpha_1 \tilde{v}_1 + \dots + \alpha_i \tilde{v}_i = -\tilde{v}_{i+1}.$$

Вероятность того, что это тождество верно для любого из оставшихся $m + q - i$ столбцов согласно теореме 1 не превосходит $(p_i^{[2Q]})^{m+q-i}$. Следовательно, $Q_{m,q,i} \leq (p_i^{[2Q]})^{m+q-i}$. Используя неравенство $P'_m \leq \binom{p}{m} R'_m$, получаем, что

$$P'_m \leq \binom{p}{m} \left((2Q)^{n-q} \binom{m+q}{m} (p_m^{[2Q]})^{n-m-q} + m \sum_{i=1}^{m-1} \binom{m}{i} \binom{m+q}{i} (p_i^{[2Q]})^{m+q-i} \right). \quad (24)$$

Оценим сверху P'_m при

$$\frac{3^6}{2^4} Q^4 \leq m \leq \frac{n}{(2Q)^b},$$

где b — некоторое фиксированное число. Пусть $q = cn$. Константы b и c будут определены позже. Пользуясь теоремой 1, оценим первое слагаемое неравенства (24) (замечая, что $p_m^{[2]} < \sqrt{2/(\pi m)}$ при $Q = 1$):

$$\begin{aligned} \binom{p}{m} (2Q)^{n-q} \binom{m+q}{m} \left(p_m^{[2Q]}\right)^{n-m-q} &\leq (2Q)^{n-q} \binom{n}{m}^2 \left(\frac{Q}{\sqrt{m}}\right)^{n-m-q} \\ &\leq (2Q)^{n-cn} \binom{n}{n/(2Q)^b}^2 \left(\frac{Q}{\sqrt{m}}\right)^{n-n/(2Q)^b-cn} \\ &\leq (2Q)^{n(1-c)} (e(2Q)^b)^{2n/(2Q)^b} (2Q)^{n(1-(2Q)^{-b}-c) \log_{2Q}(Q/\sqrt{3^6 Q^4/2^4})} \\ &\leq (2Q)^{n(1-c+2(b+2)/(2Q)^b+(1-(2Q)^{-b}-c)(3 \log_{2Q}(2/3)-1))}. \end{aligned}$$

Последнее выражение есть $o((2/3)^n)$ при $n \rightarrow \infty$, если выполняется неравенство

$$1 - c + \frac{2(b+2)}{(2Q)^b} + \left(1 - \frac{1}{(2Q)^b} - c\right) \left(3 \log_{2Q} \frac{2}{3} - 1\right) < \log_{2Q} \frac{2}{3}. \quad (25)$$

На втором шаге предыдущего вычисления использовано известное неравенство

$$\binom{n}{r} \leq \left(\frac{en}{r}\right)^r.$$

Далее, при $n \rightarrow \infty$

$$\begin{aligned} m \binom{p}{m} \sum_{i=1}^{m-1} \binom{m}{i} \binom{m+q}{i} \left(p_i^{[2Q]}\right)^{m+q-i} &\leq m \binom{p}{m} \sum_{i=1}^{m-1} 2^m \binom{m+q}{m} \left(\frac{1}{2Q}\right)^{m+q-i} \\ &\leq m(m-1)(2Q)^{n/(2Q)^b} \binom{n}{m}^2 (2Q)^{-(q+1)} \\ &\leq n(n-1)(2Q)^{n/(2Q)^b+2(b+2)n/(2Q)^b-cn} \\ &\leq (2Q)^{n((2b+5)/(2Q)^b-c)} = o((2/3)^n), \end{aligned}$$

если

$$\frac{2b+5}{(2Q)^b} - c < \log_{2Q} \frac{2}{3}. \quad (26)$$

Теперь легко подобрать константы b и c , удовлетворяющие неравенствам (25) и (26) и, следовательно, для любого m ,

$$\frac{3^6}{2^4} Q^4 \leq m \leq \frac{n}{(2Q)^b},$$

выполнено равенство $P'_m = o((2/3)^n)$.

Оценим сверху P'_m для

$$\frac{n}{(2Q)^b} < m \leq p.$$

Заметим, что

$$P'_m \leq \binom{p}{m} R_m^* + Q_{p,q},$$

где R_m^* — вероятность того, что случайная $(\pm 1, \dots, \pm(2Q-1))$ -матрица размера $m \times n$ является вырожденной и ее первые $p+q$ столбцов имеют ранг m . Вышеизложенными рассуждениями можно получить оценки

$$\begin{aligned} \binom{p}{m} R_m^* &\leq \binom{p}{m} (2Q)^n \binom{p+q}{m} \left(p_m^{[2Q]}\right)^{n-p-q} \leq \binom{n}{m}^2 (2Q)^n \left(\frac{Q}{\sqrt{m}}\right)^{n-p-q} \\ &\leq (2Q)^{n(1+2\log_2 Q) + (n-p-q)(1+b/2-\log_2 Q - \log_2 Q \sqrt{n}/n)}, \\ Q_{p,q} &\leq n \sum_{i=1}^{p-1} \binom{p}{i} \binom{p+q}{i} \left(p_i^{[2Q]}\right)^{p+q-i}. \end{aligned}$$

Следовательно, $\binom{p}{m} R_m^*$ есть $o((2/3)^n)$ при $n \rightarrow \infty$, если

$$1 + 2\log_2 Q + \left(1 + \frac{b}{2} - \log_2 Q - \log_2 Q \sqrt{n}\right) \frac{n-p-q}{n} < \log_2 Q \frac{2}{3},$$

или

$$n-p-q > n \frac{2 + \log_2 Q \cdot 36}{\log_2 Q \cdot n + \log_2 Q \cdot 4 - (b+2)}. \quad (27)$$

Выберем q так, чтобы выполнялось равенство

$$n-p-q = \left\lfloor n \frac{2 + \log_2 Q \cdot 36}{\log_2 Q \cdot n + \log_2 Q \cdot 4 - (b+2)} \right\rfloor. \quad (28)$$

Из (27) следует, что p удовлетворяет неравенству

$$p \leq n - n \frac{2 + \log_2 Q \cdot 36}{\log_2 Q \cdot n + \log_2 Q \cdot 4 - (b+2)}. \quad (29)$$

Оценивая сверху число $Q_{p,q}$, находим, что

$$Q_{p,q} \leq \Sigma_1 + \Sigma_2, \quad (30)$$

где

$$\begin{aligned} \Sigma_1 &= n \sum_{i=1}^{[\sqrt{n}]} \binom{p}{i} \binom{p+q}{i} \left(p_i^{[2Q]}\right)^{p+q-i}, \\ \Sigma_2 &= n \sum_{i=[\sqrt{n}]+1}^{p-1} \binom{p}{i} \binom{p+q}{i} \left(p_i^{[2Q]}\right)^{p+q-i}. \end{aligned}$$

Для любого $l \in \mathbb{N}$ существует $M \in \mathbb{N}$ такое, что для всех $n > M$

$$n^{1/2} < \frac{n}{(2Q)^l} < \frac{n}{2}.$$

Используя это неравенство и теорему 1, мы получаем, что при $n \rightarrow \infty$

$$\begin{aligned}\Sigma_1 &\leq n^{3/2} \binom{n}{\lfloor \sqrt{n} \rfloor}^2 (2Q)^{-(p+q-\lfloor \sqrt{n} \rfloor)} \leq n^{3/2} \binom{n}{n(2Q)^{-l}}^2 (2Q)^{-(p+q-\lfloor \sqrt{n} \rfloor)} \\ &\leq n^{3/2} (2Q)^{(2(l+1)(2Q)^{-l} + n^{-1/2} - (p+q)/n)n} = o((2/3)^n),\end{aligned}$$

если

$$\frac{p+q}{n} > 2 \frac{l+1}{(2Q)^l} + n^{-1/2} - \log_{2Q} \frac{2}{3}. \quad (31)$$

Выберем число $l \in \mathbb{N}$ так, чтобы для достаточно больших n выполнялось неравенство

$$\frac{n - \lfloor n(2 + \log_{2Q} 36) / (\log_{2Q} n + \log_{2Q} 4 - (b+2)) \rfloor}{n} > \frac{2(l+1)}{(2Q)^l} + n^{-1/2} - \log_{2Q} \frac{2}{3}.$$

Тогда для выбранного l неравенство (31) будет выполнено.

Оценим сверху второе слагаемое в неравенстве (30). При $n \rightarrow \infty$

$$\Sigma_2 \leq n^2 2^{2n} \left(\frac{Q}{\sqrt{\lfloor \sqrt{n} \rfloor} + 2} \right)^q \leq n^2 (2Q)^{2n \log_{2Q} 2} (2Q)^{q(\log_{2Q} Q - (1/4) \log_{2Q} n)} = o((2/3)^n),$$

если

$$\frac{q}{n} > 4 \frac{\log_{2Q} 6}{\log_{2Q} n - 4 \log_{2Q} Q}.$$

Из равенства (28) следует, что должно выполняться неравенство

$$\frac{n - p - \lfloor n(2 + \log_{2Q} 36) / (\log_{2Q} n + \log_{2Q} 4 - (b+2)) \rfloor}{n} > \frac{4 \log_{2Q} 6}{\log_{2Q} n - 4 \log_{2Q} Q}.$$

Нетрудно проверить, что при

$$p = n - (3 + \log_{2Q} 36) \frac{n}{\log_{2Q} n}$$

последнее неравенство выполняется для достаточно больших n .

Теорема 4. Для любого

$$p \leq n - (3 + \log_{2Q} 36) \frac{n}{\log_{2Q} n},$$

соответственно

$$p \leq n - (3 + \log_{2Q+1} 36) \frac{n}{\log_{2Q+1} n},$$

вероятность того, что линейная оболочка p случайно выбранных векторов $v_1, v_2, \dots, v_p$ из $(E'_K)^n$, соответственно из E_K^n , содержит хотя бы один вектор из

$$(E'_K)^n \setminus \bigcup_{i=1}^p \langle v_i \rangle,$$

соответственно из

$$E_K^n \setminus \bigcup_{i=1}^p \langle v_i \rangle,$$

равняется при $n \rightarrow \infty$

$$P'_3 + o((2/3)^n),$$

соответственно

$$P_2 + o((3/4)^n).$$

Доказательство. Заметим, что для

$$m \leq \frac{3^6}{2^4} Q^4 - 1,$$

соответственно

$$m \leq \frac{3^6}{2^8} (2Q + 1)^4 - 1,$$

при $n \rightarrow \infty$ имеет место соотношение

$$P'_m = O\left(\binom{p}{m} \left(\frac{L'^{[m]}}{(2Q)^m}\right)^n\right),$$

соответственно

$$P_m = O\left(\binom{p}{m} \left(\frac{L^{[m]}}{(2Q + 1)^m}\right)^n\right).$$

Теперь теорема следует из лемм 8 и 9.

4. Нижняя оценка числа $P(K, n)$

Пусть

$$H: a_1 x_1 + \dots + a_n x_n = 0$$

— гиперплоскость в n -мерном евклидовом пространстве, проходящая через начало координат. Гиперплоскость H разбивает дискретный гиперкуб E_K^n на три части

$$A_H = E_K^n \cap H^+, \quad B_H = E_K^n \cap H, \quad C_H = E_K^n \cap H^-,$$

где H^+ и H^- — открытые полупространства в $\mathbf{R}^n$, определенные гиперплоскостью H . Рассмотрим две гиперплоскости

$$H_{-\varepsilon}: a_1 x_1 + \dots + a_n x_n - \varepsilon = 0,$$

$$H_{\varepsilon}: a_1 x_1 + \dots + a_n x_n + \varepsilon = 0.$$

Без ограничения общности можно считать, что $H_{-\varepsilon}^+ \cap H_{\varepsilon}^- \neq \emptyset$. Выберем $\varepsilon > 0$ так, чтобы выполнялось равенство

$$(H_{-\varepsilon}^+ \cap H_{\varepsilon}^-) \cap E_K^n = B_H.$$

Следовательно,

$$A_H = E_K^n \cap H_{\varepsilon}^+, \quad C_H = E_K^n \cap H_{-\varepsilon}^-.$$

С другой стороны, если мы имеем три подмножества A_H, B_H, C_H множества точек гиперкуба E_K^n , полученные, как было указано выше, с помощью двух параллельных гиперплоскостей, то этой тройке мы можем сопоставить разбиение $(n+1)$ -мерного гиперкуба E_K^{n+1} гиперплоскостью

$$\bar{H}: a_1x_1 + \dots + a_nx_n + \frac{\varepsilon}{Q}x_{n+1} = 0$$

в $\mathbf{R}^{n+1}$: на нижнем основании гиперкуба $\{(x_1, \dots, x_{n+1}) \in E_K^{n+1} \mid x_{n+1} = -Q\}$ мы будем иметь разбиение гиперплоскостью $H_{-\varepsilon}$, то есть $(A_H \cup B_H) \cup C_H$, а на верхнем слое гиперкуба, мы будем иметь разбиение гиперплоскостью H_ε , то есть $A_H \cup (B_H \cup C_H)$.

Лемма 10. Пусть H и G — две гиперплоскости в $\mathbf{R}^n$, для которых $B_H \neq B_G$. Тогда гиперплоскости $\bar{H}$ и $\bar{G}$ реализуют разные пороговые функции в $\mathbf{R}^{n+1}$.

Доказательство. Предположим противное. Тогда из равенства на верхнем и нижнем слоях следует, что $A_H \cup (B_H \cup C_H) = A_G \cup (B_G \cup C_G)$ и соответственно $(A_H \cup B_H) \cup C_H = (A_G \cup B_G) \cup C_G$, из чего вытекает, что $C_H = C_G$ и $A_H = A_G$. Следовательно,

$$B_H = E_K^n \setminus (A_H \cup C_H) = E_K^n \setminus (A_G \cup C_G) = B_G.$$

Из леммы следует, что, оценив число различных множеств B_H , мы получим нижнюю оценку для числа пороговых функций.

Теорема 5. Для достаточно большого n

$$P(K, n+1) \geq \frac{1}{2} \binom{K^n}{\lfloor n-4-2n/\log_K n \rfloor} P(K, \lfloor 2n/\log_K n + 4 \rfloor).$$

Доказательство повторяет доказательство основной теоремы работы [2]. При этом основным в доказательстве является то, что в теореме Одлышко соответствующая вероятность стремится к нулю при $n \rightarrow \infty$. Если ограничиться только этим требованием, то границы параметра p теоремы 4 можно поднять.

Обозначим P вероятность того, что линейная оболочка p векторов $v_1, \dots, v_p$, случайно выбранных из E_K^n , содержит хотя бы один вектор из $E_K^n \setminus \bigcup_{i=1}^p \langle v_i \rangle$.

Теорема 6. Для любого $p \leq n - 2n/\log_K n - 4$ имеют место следующие соотношения: при $n \rightarrow \infty$ для четного K

$$P \leq P'_3 + o((2/3)^n) + \frac{1 + \log_K 36}{\log_K n} - \frac{4}{n},$$

и для нечетного K

$$P \leq P_2 + o((3/4)^n) + \frac{1 + \log_K 36}{\log_K n} - \frac{4}{n}$$

Доказательство. Покажем, что для

$$m \in \mathbf{N}, \quad m \leq s = n - (3 + \log_{2Q} 36) \frac{n}{\log_{2Q} n},$$

и

$$p \leq n - \frac{2n}{\log_K n} - 4$$

утверждение леммы 9 остается в силе. Для $3 \neq m \leq n/(2Q)^b$, не изменяя рассуждений леммы 9, мы получим, что $P'_m = o((2/3)^n)$. Для $n/(2Q)^b \leq m \leq s$ справедлива оценка

$$P'_m \leq \binom{p}{m} R_{m,s+q}^* + T_{p,s+q},$$

где $R_{m,s+q}^*$ — вероятность того, что случайная матрица $M_{m \times n}$ вырождена и ее первые $s+q$ столбцов имеют ранг m , а $T_{p,s+q}$ — вероятность того, что в случайной матрице $M_{p \times (s+q)}$ размера $p \times (s+q)$ существуют s линейно зависимых строк. Тогда

$$\binom{p}{m} R_{m,s+q}^* \leq (2Q)^n \binom{p}{m} \binom{s+q}{m} (p_m^{[2Q]})^{n-(s+q)} \leq (2Q)^n \binom{n}{m}^2 (p_m^{[2Q]})^{n-(s+q)}$$

и, следовательно, первое слагаемое есть $o((2/3)^n)$ для p , удовлетворяющих неравенству (29). Далее,

$$T_{p,s+q} \leq \sum_{k=1}^{s-1} (p-k) \binom{p}{k} \binom{s+q}{k} T_{p,s+q,k},$$

где $T_{p,s+q,k}$ — вероятность того, что матрица M размера $p \times (s+q)$ удовлетворяет следующим условиям: любые k строк матрицы линейно независимы; минор размера $k \times k$, находящийся в верхнем левом углу имеет ранг k ; $(k+1)$ -я строка линейно выражается через первые k строк. Тогда

$$T_{p,s+q,k} \leq (p_k^{[2Q]})^{s+q-k},$$

$$T_{p,s+q} \leq p \sum_{k=1}^{s-1} \binom{p}{k} \binom{s+q}{k} (p_k^{[2Q]})^{s+q-k}.$$

Так как $s = n - (3 + \log_{2Q} 36)n / \log_{2Q} n$, по аналогии с оценкой величины $Q_{p,q}$ в доказательстве леммы 9 получаем, что $P'_m = o((2/3)^n)$.

Через $\bar{P}_m$, $m \geq 3$, обозначим вероятность того, что среди p случайно выбранных векторов $v_1, \dots, v_p$ из E_K^n , соответственно из $(E'_K)^n$, существуют m векторов $v_{i_1}, \dots, v_{i_m}$, линейная комбинация с ненулевыми коэффициентами которых принадлежит множеству E_K^n , соответственно $(E'_K)^n$, и данное условие не выполняется для меньшего числа векторов k , $2 \leq k < m$. Заметим, что векторы $v_{i_1}, \dots, v_{i_m}$ линейно независимы и

$$\bar{P}_m \leq K^n \binom{p}{m} \binom{n}{m} (p_m^{[K]})^{n-m}.$$

Пусть $s = n - (3 + \log_K 36)n / \log_K n$. Из теоремы 4 и вышеприведенных рассуждений следует, что для доказательства нашего утверждения нам достаточно найти p такое, что для любого m , $s+1 \leq m \leq p$, выполняется неравенство $\bar{P}_m \leq 1/n$. Положим

$$p = n - 2 \frac{(1+\varepsilon)n}{\log_K n}.$$

Тогда

$$\begin{aligned}
 \bar{P}_m &\leq K^n \binom{p}{m} \binom{n}{m} \left(p_m^{[K]}\right)^{n-m} \leq K^n \binom{n}{(3 + \log_K 36)n / \log_K n}^2 \left(\frac{K}{2\sqrt{m}}\right)^{n-m} \\
 &\leq K^n \left(\frac{e \log_K n}{3 + \log_K 36}\right)^{(2n(3 + \log_K 36) / \log_K n)} K^{(n-m)(1 - (1/2) \log_K (4m))} \\
 &\leq K^{(n+2(3 + \log_K 36)n \log_K (e \log_K n / (3 + \log_K 36)) / \log_K n - (n-p)(\log_K n(1 - 2(1+\varepsilon) / \log_K n) - 2)/2)} \\
 &= K^{n(-\varepsilon + f_1 + f_2 + f_3)} < K^{n(-(\log_K n)/n)} = \frac{1}{n},
 \end{aligned}$$

если при $n \rightarrow \infty$

$$\varepsilon > \frac{\log_K n}{n} + f_1 + f_2 + f_3. \quad (32)$$

Здесь

$$\begin{aligned}
 f_1 &= 2(3 + \log_K 36) \frac{\log_K (e \log_K n / (3 + \log_K 36))}{\log_K n}, \\
 f_2 &= -(1 + \varepsilon) \frac{\log_K (1 - 2(1 + \varepsilon) / \log_K n)}{\log_K n}, \quad f_3 = (1 + \varepsilon) \frac{2}{\log_K n},
 \end{aligned}$$

и $f_1, f_2, f_3 \rightarrow 0$ при $n \rightarrow \infty$. Теперь легко видеть, что при $\varepsilon = 2 \log_K n / n$ неравенство (32) выполнено. Рассуждения для нечетного K дословно повторяют рассуждения для четного K . Теорема доказана.

Список литературы

1. Schläfli L. *Gesammelte Mathematische Abhandlungen*. Birkhäuser, Basel, 1850.
2. Ирматов А. А. О числе пороговых функций. *Дискретная математика* (1993) **5**, №3, 40–43.
3. Odlyzko A. M. On subspaces spanned by random selections of ± 1 vectors. *J. Combin. Theory Ser. A* (1988) **47**, 124–133.
4. Sperner E. Ein Satz über Untermenge einer endliche Menge. *Math. Z.* (1928) **27**, 544–548.
5. Erdős P. On a lemma of Littlewood and Offord. *Bull. Amer. Math. Soc.* (1945) **51**, 898–902.

Статья поступила 22.06.1998.