



Math-Net.Ru

All Russian mathematical portal

V. A. Kopyttsev, V. G. Mikhailov, Poisson-type theorems for the number of special solutions of a random linear inclusion, *Diskr. Mat.*, 2010, Volume 22, Issue 2, 3–21

DOI: 10.4213/dm1091

Use of the all-Russian mathematical portal Math-Net.Ru implies that you have read and agreed to these terms of use

<http://www.mathnet.ru/eng/agreement>

Download details:

IP: 18.97.14.85

March 22, 2025, 05:43:34



## Теоремы пуассоновского типа для числа специальных решений случайного линейного включения

© 2010 г. В. А. Копытцев, В. Г. Михайлов

При заданных множествах  $D$  и  $B$  векторов линейных пространств над конечным полем размерности  $n$  и  $T$  соответственно и случайной матрице  $A$  размера  $T \times n$  над этим полем рассматривается распределение числа векторов, удовлетворяющих системе соотношений  $x \in D$ ,  $Ax \in B$  (числа решений случайного линейного включения  $Ax \in B$ , принадлежащих множеству  $D$ ). Указаны условия, обеспечивающие при  $n, T \rightarrow \infty$  сходимость этого распределения к простому и к сложному распределениям Пуассона. В них предполагается, что распределение матрицы  $A$  сближается с равномерным распределением, а хотя бы одно из множеств  $D$  или  $B$  удовлетворяет условию, которое в работе названо условием асимптотической свободы от линейных комбинаций. Эти результаты обобщают известные предельные теоремы о числе специальных решений систем случайных линейных уравнений. Они, в частности, позволяют описать асимптотическое поведение числа приближенных решений заведомо совместных систем.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (проект 08-01-00078а).

### 1. Введение

Линейным включением (над полем  $K$ ) размерности  $T$  относительно  $n$ -мерного вектора мы называем запись  $Ax \in B$ , где  $A$  — матрица из элементов поля  $K$  размера  $T$  на  $n$ , а  $B$  — некоторое множество  $T$ -мерных векторов над этим полем. Решением линейного включения будет любой вектор  $x$   $n$ -мерного линейного пространства  $V^n$  над полем  $K$ , для которого вектор  $Ax$  принадлежит множеству  $B$ . Полным решением линейного включения является множество всех таких векторов  $x$ .

К линейным включениям приводит, например, задача о числе приближенных решений заведомо совместной системы линейных уравнений  $Ax = Ax^0$ . Под приближенными решениями понимаются такие векторы  $x$ , для которых разности  $x - x^0$  и  $Ax - Ax^0$  малы в том или ином смысле. Например, пусть они имеют относительно небольшое число ненулевых координат (их число у вектора  $y$  далее обозначаем как  $\|y\|$ ). Преобразуем нашу систему заменой  $x - x^0 = y$  в систему однородных уравнений  $Ay = 0$ . Тогда мы придем к задаче о числе тех решений линейного включения  $Ay \in B_r$ , где

$$B_r = \{b: \|b\| \leq r\},$$

которые принадлежат множеству

$$D_r = \{y: 1 \leq \|y\| \leq r\}.$$

Далее решения линейного включения, принадлежащие заданному собственному подмножеству  $D$ , будем называть специальными.

В настоящей работе изучаются свойства распределения числа специальных решений случайного линейного включения над полем  $K = GF(q)$  со случайной матрицей  $A = \|a_{i,j}\|$ , элементы которой независимы в совокупности и распределены с вероятностями

$$\mathbf{P}\{a_{i,j} = k\} = \frac{1 + \Delta_{i,j}(k)}{q}, \quad k \in K, \quad (1)$$

где

$$\sum_{k \in K} \Delta_{i,j}(k) = 0, \quad i = 1, \dots, T, \quad j = 1, \dots, n.$$

Пусть

$$\Delta = \max_{i,j,k} |\Delta_{i,j}(k)| < 1.$$

Рассматривается случай, когда параметры  $n$  и  $T$  согласованно возрастают:  $n, T \rightarrow \infty$ . Нас интересуют условия, которым должны удовлетворять множества  $B$  и  $D$  для того, чтобы распределение числа специальных решений случайного линейного включения сходилось к пуассоновскому или сложному пуассоновскому распределению. Аналогичные вопросы для числа всех решений случайного линейного включения изучались в работах [4, 5].

В работе [4] были получены достаточные условия сходимости распределения числа ненулевых решений случайного линейного включения над полем  $GF(q)$  к сложному пуассоновскому распределению. В ней было использовано следующее условие на правую часть включения.

Пусть  $N(a_1, a_2, a_3, d, B)$  обозначает число решений системы из  $T$  линейных уравнений над полем  $K$ , записанной в виде уравнения

$$a_1 u^1 \oplus a_2 u^2 \oplus a_3 u^3 = d,$$

относительно тройки векторов  $(u^1, u^2, u^3) \in B^3$ , где  $B$  — некоторое заданное подмножество  $V^T$ ,  $a_1, a_2, a_3 \in K \setminus \{0\}$ ,  $d \in V^T$ . Положим

$$\begin{aligned} N(B) &= \max_{a_1, a_2, a_3, d} N(a_1, a_2, a_3, d, B), \\ \rho(B) &= \frac{N(B)}{|B|^2}, \end{aligned} \quad (2)$$

где  $|B|$  обозначает число элементов конечного множества  $B$ . Очевидно, что  $0 \leq \rho(B) \leq 1$ .

Отношение  $\rho(B) = N(B)/|B|^2$  является своего рода мерой отличия множества  $B$  от линейного или аффинного пространства. Для линейных и аффинных подпространств эта мера принимает максимально возможное значение  $\rho(B) = 1$  (см. [5]). Если  $0 < \rho(B) < 1$ , то множество  $B$  можно считать частично линейным. Условие

$$\rho(B) \rightarrow 0 \quad (3)$$

можно трактовать как асимптотическую нелинейность множества  $B = B(T)$  при  $T \rightarrow \infty$ , или, что более точно (см. раздел 5), как его асимптотическую свободу от линейных комбинаций.

**Замечание 1.** Непосредственно из определения величины  $\rho(B)$  вытекают следующие свойства.

- (А) Соотношения  $\rho(B \oplus b^0) \rightarrow 0$  выполнены (или не выполнены) одновременно при всех  $b^0 = b^0(T) \in V^T$ .
- (Б) Из соотношения  $\rho(B) \rightarrow 0$  вытекает соотношение  $\rho(B \cup B') \rightarrow 0$  для любого множества  $B'$ , удовлетворяющего условию  $|B'|/|B| \rightarrow 0$  при  $T \rightarrow \infty$ .

**Теорема 1.** Пусть

$$T \rightarrow \infty, \quad r \geq 1, \quad rT^{-1} \leq \rho \quad (4)$$

при некотором  $0 < \rho < (q-1)/q$ . Тогда для множеств

$$S_r(b^0) = \{b \in V^T : 1 \leq \|b - b^0\| \leq r\}, \quad (5)$$

$$S'_r(b^0) = \{b \in V^T : \|b - b^0\| = r\} \quad (6)$$

при любых  $b^0 = b^0(T) \in V^T$  выполнено соотношение (3).

Обозначим через  $\xi = \xi(D, A, B)$  число тех ненулевых решений включения  $Ax \in B$ , которые принадлежат множеству  $D$ . Другими словами,

$$\xi = \xi(D, A, B) = |\{x \in D, Ax \in B\}|.$$

Цель работы — исследовать предельное поведение этой случайной величины при таком изменении параметров, когда  $|D| \rightarrow \infty$  и

$$\mathbf{E}\xi(D, A, B) = q^{-T} |D \times B| \rightarrow \lambda, \quad 0 < \lambda < \infty. \quad (7)$$

Основные результаты статьи сформулированы в двух следующих разделах. В разделе 2 описано совместное распределение чисел специальных решений  $\xi(D, A, B_k)$  случайных линейных включений  $Ax \in B_k$ ,  $k = 1, \dots, s$ , с общей левой частью и с непересекающимися множествами  $B_1, \dots, B_s$  в правых частях включений в том случае, когда в множестве  $D \times B = D \times \bigcup_{k=1}^s B_k$  нет подобных векторов или их относительно мало. Напомним, что подобными называются векторы, получаемые друг из друга умножением на ненулевой элемент поля. Выведены условия выполнения для величин  $\xi(D, A, B_k)$  многомерной предельной теоремы Пуассона (теорема 2). В разделе 3 рассмотрен случай, когда  $s = 1$ , а подобные векторы в множестве  $B = B_1$  имеются, причем в числе, сравнимом по порядку с  $|D \times B|$ . Тогда предельное распределение величины  $\xi(D, A, B)$  оказывается сложным пуассоновским распределением (теорема 3). Раздел 4 посвящен доказательству теорем 2 и 3. Теорема 1 доказывается в разделе 5.

## 2. Многомерная предельная теорема Пуассона

Зададим множество  $D = D(n) \subset V^n$  и набор попарно не пересекающихся множеств  $B_1 = B_1(T), \dots, B_s = B_s(T) \subset V^T$ . Положим  $B = B_1 \cup \dots \cup B_s$ .

**Теорема 2.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0 \notin D$ , множество  $D \times B$  не содержит подобных векторов и при  $n, T \rightarrow \infty$  выполнены соотношения  $T\Delta \rightarrow 0$ ,  $|D| \rightarrow \infty$ ,

$$q^{-T} |D| |B_k| \rightarrow \lambda_k, \quad 0 \leq \lambda_k < \infty, \quad k = 1, \dots, s, \quad \exists k: \lambda_k > 0, \quad (8)$$

$$\rho(D)\rho(B) \rightarrow 0. \quad (9)$$

Тогда случайные величины  $\xi(D, A, B_k)$  асимптотически независимы, а их распределения сходятся к распределениям Пуассона с параметрами  $\lambda_k$  соответственно.

**Замечание 2.** В теореме 2 и далее считаем, что вырожденное в нуле распределение является распределением Пуассона с параметром  $\lambda = 0$ .

**Замечание 3.** Условие (8) определяет значения параметров предельных распределений случайных величин  $\xi(D, A, B_k)$ , а условие (9) означает, что по крайней мере для одного из множеств  $D$  и  $B$  выполнено соотношение (3).

**Замечание 4.** Условие (9) в теоремах для числа решений случайных линейных включений используется впервые. Если при переходе к пределу  $|B| \leq C < \infty$ , то соотношение  $\rho(B) \rightarrow 0$  не может выполняться. В этом случае условие (9) принимает вид  $\rho(D) \rightarrow 0$ .

**Замечание 5.** Если  $0 \in B$ , то условие отсутствия подобных векторов в множестве  $D \times B$  эквивалентно отсутствию подобных векторов в множестве  $D$ .

**Замечание 6.** Условия отсутствия подобных векторов в множествах  $D$ ,  $B$  и  $D \times B$  выполнены автоматически, если  $K = GF(2)$ .

**Замечание 7.** В случае, когда  $B_1 = \{b^1\}, \dots, B_s = \{b^s\}$ , теорема 2 рассматривает поведение совместного распределения чисел специальных решений у  $s$  случайных систем линейных уравнений  $Ax = b^1, \dots, Ax = b^s$  с одинаковой левой и разными правыми частями. Для этого случая из нее вытекает следующее утверждение.

**Следствие 1.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0 \notin D$ ,  $b^1, \dots, b^s \in V^T \setminus \{0\}$  и среди них нет подобных векторов. Если  $n, T \rightarrow \infty$ , выполнены соотношения  $T\Delta \rightarrow 0$ ,  $\rho(D) \rightarrow 0$ , и

$$q^{-T}|D| \rightarrow \lambda, \quad 0 < \lambda < \infty, \quad (10)$$

то числа тех решений систем  $Ax = b^1, \dots, Ax = b^s$ , которые принадлежат множеству  $D$ , асимптотически независимы, а распределение каждого из них сходится к распределению Пуассона с параметром  $\lambda$ .

**Замечание 8.** Если в множестве  $D$  нет подобных векторов, то утверждение следствия 1 распространяется также на систему  $Ax = 0$ .

**Замечание 9.** Сформулированные выше результаты естественным образом распространяются на случай, когда множество  $D \times B$  (либо множество  $D$  в случае замечания 8) содержит подобные векторы, но их общее число бесконечно мало по сравнению с  $|D \times B|$  при  $n, T \rightarrow \infty$ .

### 3. Теорема о сходимости к сложному пуассоновскому распределению

Опишем теперь асимптотическое поведение распределения числа решений, принадлежащих множеству  $D$ , у случайного линейного включения  $Ax \in B$  в том случае, когда множество  $D \times B$  содержит подобные векторы в числе, сравнимом с  $|D \times B|$ . Разобьем множество  $D \times B$  на классы  $DB_1, \dots, DB_M$  подобных векторов, где  $M$  — общее число таких классов. Положим

$$l_r(D, B) = |\{k \in \{1, \dots, M\} : |DB_k| = r\}|, \quad r = 1, \dots, q-1. \quad (11)$$

**Теорема 3.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0 \notin D$ , а при  $n, T \rightarrow \infty$  выполнены соотношения  $T\Delta \rightarrow 0$ ,  $|D| \rightarrow \infty$ , (9) и условие

$$q^{-T} l_r(D, B) \rightarrow \lambda_r, \quad 0 \leq \lambda_r < \infty, \quad r = 1, \dots, q-1, \quad \exists r: \lambda_r > 0. \quad (12)$$

Тогда распределение случайной величины  $\xi(D, A, B)$  сходится к распределению выражения  $\pi_1 + 2\pi_2 + \dots + (q-1)\pi_{q-1}$ , где  $\pi_1, \dots, \pi_{q-1}$  — независимые в совокупности случайные величины, распределенные по закону Пуассона с параметрами  $\lambda_1, \dots, \lambda_{q-1}$  соответственно.

Рассмотрим частный случай, когда оба множества  $D$  и  $B$  замкнуты относительно умножения векторов на ненулевые элементы поля. Из теоремы 3 вытекает следующее утверждение.

**Следствие 2.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0 \notin D$ , множества  $D$  и  $B$  замкнуты относительно умножения векторов на ненулевые элементы поля  $K$ ,  $n, T \rightarrow \infty$ ,  $T\Delta \rightarrow 0$ ,  $|D| \rightarrow \infty$ , и выполнены условия (9) и (7). Тогда распределение случайной величины  $\xi(D, A, B)/(q-1)$  сходится к распределению Пуассона с параметром  $\lambda/(q-1)$ .

**Замечание 10.** В случае, когда

$$D = D_r = \{x \in V^n: 1 \leq \|x\| \leq r\},$$

$$B = B_r = \{b \in V^T: \|b\| \leq r\},$$

следствие 2 описывает предельное поведение числа приближенных решений заведомо совместной системы линейных уравнений  $Ax = Ax^0$  (см. раздел 1). В этом случае с учетом теоремы 1 и замечания 1 получаем следующие утверждения.

**Следствие 3.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $n, T \rightarrow \infty$ ,  $T\Delta \rightarrow 0$ , параметры  $r_1, r_2 \geq 1$  меняются так, что

$$q^{-T} \sum_{i=1}^{r_1} \binom{n}{i} (q-1)^i \sum_{j=1}^{r_2} \binom{T}{j} (q-1)^j \rightarrow \lambda, \quad 0 < \lambda < \infty,$$

и при некотором  $\rho$ ,  $0 < \rho < (q-1)/q$ , выполнено хотя бы одно из условий  $r_1 n^{-1} \leq \rho$ ,  $r_2 T^{-1} \leq \rho$ . Тогда распределение случайной величины  $\xi_{r_1, r_2}(x^0)/(q-1)$ , где  $\xi_{r_1, r_2}(x^0)$  — число тех  $x \in V^n$ , для которых  $1 \leq \|x - x^0\| \leq r_1$  и  $\|Ax - Ax^0\| \leq r_2$ , при любом изменении  $x^0$  сходится к распределению Пуассона с параметром  $\lambda/(q-1)$ .

**Следствие 4.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  определяется соотношениями (1),  $n, T \rightarrow \infty$ ,  $T\Delta \rightarrow 0$ , параметр  $r \geq 1$  меняется так, что

$$q^{-T} \sum_{i=1}^r \binom{n}{i} (q-1)^i \rightarrow \lambda, \quad 0 < \lambda < \infty,$$

и при некотором  $\rho$ ,  $0 < \rho < (q-1)/q$ , выполнено условие  $rn^{-1} \leq \rho$ . Тогда распределение случайной величины  $\xi_r(x^0)/(q-1)$ , где  $\xi_r(x^0)$  — число тех решений системы уравнений  $Ax = Ax^0$ , для которых  $1 \leq \|x - x^0\| \leq r$ , при любом изменении вектора  $x^0$  сходится к распределению Пуассона с параметром  $\lambda/(q-1)$ .

**Замечание 11.** Следствия 3 и 4 существенно дополняют результаты работ [1] и [2], распространяя некоторые из них на случай множеств общего вида.

Значительный интерес теорема 3 представляет в случае, когда  $B = \{0^T\}$ . Тогда речь идет о числе специальных решений системы случайных однородных уравнений  $Ax = 0^T$ . Положим  $l_r(D) = l_r(D, \{0^T\})$ .

**Следствие 5.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0^n \notin D$ , а при  $n, T \rightarrow \infty$  выполнены соотношения  $T\Delta \rightarrow 0$ ,  $|D| \rightarrow \infty$ ,  $\rho(D) \rightarrow 0$  и условие

$$q^{-T}l_r(D) \rightarrow \lambda_r, \quad 0 \leq \lambda_r < \infty, \quad r = 1, \dots, q-1, \quad \exists r: \lambda_r > 0. \quad (13)$$

Тогда распределение случайной величины  $\xi(D, A, \{0^T\})$  сходится к распределению выражения  $\pi_1 + 2\pi_2 + \dots + (q-1)\pi_{q-1}$ , где  $\pi_1, \dots, \pi_{q-1}$  — независимые в совокупности случайные величины, распределенные по закону Пуассона с параметрами  $\lambda_1, \dots, \lambda_{q-1}$  соответственно.

**Замечание 12.** Предельная теорема для числа специальных решений системы случайных однородных уравнений  $Ax = 0$  при более жестких предположениях относительно свойств распределения элементов матрицы  $A$  была доказана в [5]. Там предполагалось, что  $\Delta = 0$ .

## 4. Доказательство теорем 2 и 3

Введем характеристику, которой мы будем описывать асимптотические свойства множества  $D \subseteq V^n$ . Положим

$$\bar{D}_{k,j} = \{(x^1, \dots, x^k) \in D^k: x^\alpha \neq cx^\beta, c \in K, \alpha \neq \beta, \text{rank}(x^1, \dots, x^k) = j\}.$$

Пусть  $I\{E\}$  обозначает индикатор случайного события  $E$ . Рассмотрим систему случайных индикаторов  $\{I\{Ax = b\}: (x, b) \in J\}$ , где  $J \subseteq D \times B$ . Пусть задан набор  $R_1, \dots, R_s$  непересекающихся подмножеств множества  $J$ . Пусть

$$\xi_u = \sum_{(x,b) \in R_u} I\{Ax = b\}, \quad u = 1, \dots, s.$$

**Теорема 4.** Пусть  $K = GF(q)$ , распределение элементов матрицы  $A$  описывается формулой (1),  $0^n \notin D$ , множество  $J$  не содержит подобных векторов и при  $n, T \rightarrow \infty$  выполнены соотношения  $T\Delta \rightarrow 0$ ,  $|D| \rightarrow \infty$ ,

$$q^{-T}|D||B| = O(1), \quad (14)$$

$$q^{-T}|R_k| \rightarrow \lambda'_k, \quad 0 \leq \lambda'_k < \infty, \quad k = 1, \dots, s, \quad (15)$$

и при всех  $k > j \geq 2$

$$\frac{|\bar{D}_{k,j}|}{|D|^j} \rho(B) \rightarrow 0. \quad (16)$$

Тогда случайные величины  $\xi_1, \dots, \xi_s$  асимптотически независимы, а их распределения сходятся к распределениям Пуассона с параметрами  $\lambda_1, \dots, \lambda_s$  соответственно.

Для доказательства теоремы 4 мы воспользуемся многомерной версией известной теоремы Б. А. Севастьянова об условиях справедливости предельной теоремы Пуассона для сумм зависимых индикаторов (см. [3]). Ее условия используют понятие исключительных множеств, к заданию которых мы и приступаем. Пусть (используем обозначение  $v^i = (x^i, b^i)$ )

$$\begin{aligned} J_k &= \{(v^1, \dots, v^k) \in J^k: v^\alpha \neq v^\beta \ (\alpha \neq \beta)\}, \\ D_{k,j} &= \{(x^1, \dots, x^k) \in D^k: \text{rank}(x^1, \dots, x^k) = j\}, \\ D_k &= \bigcup_{j=1}^{k-1} D_{k,j}. \end{aligned}$$

Нетрудно убедиться, что

$$|D_{k,j}| \leq \binom{k}{j} q^{j(k-j)} |D|^j. \quad (17)$$

Исключительные множества  $I_k \subset J_k$  определим равенством

$$I_k = \{((x^1, b^1), \dots, (x^k, b^k)) \in J_k: (x^1, \dots, x^k) \in D_k\}.$$

Утверждение теоремы 4 будет доказано, если убедиться, что выполнены условия

$$\sum_{(x,b) \in R_u} \mathbf{P}\{Ax = b\} \rightarrow \lambda'_u, \quad u = 1, \dots, s, \quad (18)$$

$$\max_{(x,b) \in J} \mathbf{P}\{Ax = b\} \rightarrow 0 \quad (19)$$

и при всех  $k = 2, 3, \dots$  (используем обозначение  $v^i = (x^i, b^i)$ )

$$\max_{(v^1, \dots, v^k) \in J_k \setminus I_k} \left| \frac{\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\}}{\mathbf{P}\{Ax^1 = b^1\} \dots \mathbf{P}\{Ax^k = b^k\}} - 1 \right| \rightarrow 0, \quad (20)$$

$$\sum_{(v^1, \dots, v^k) \in I_k} \prod_{j=1}^k \mathbf{P}\{Ax^j = b^j\} \rightarrow 0, \quad (21)$$

$$\sum_{(v^1, \dots, v^k) \in I_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} \rightarrow 0. \quad (22)$$

Приступим к проверке этих условий. Нам понадобится следующая лемма.

**Лемма 1.** Пусть  $x^1, \dots, x^k \in D$  и  $b^1, \dots, b^k \in V^T$ . Тогда при всех  $k = 1, 2, \dots$

$$\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} \leq \left( \frac{1 + \Delta}{q} \right)^{lT}, \quad (23)$$

если  $\text{rank}(x^1, \dots, x^k) = l \leq k - 1$ , и

$$\left( \frac{1 - \Delta}{q} \right)^{kT} \leq \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} \leq \left( \frac{1 + \Delta}{q} \right)^{kT}, \quad (24)$$

если  $\text{rank}(x^1, \dots, x^k) = k$ .



Доказательство леммы 1 аналогично доказательству леммы 3 в [2]. Поэтому мы его не приводим.

Из неравенств (24), условий  $T\Delta \rightarrow 0$  и (10) следуют соотношения (18) и (19).

Проверим выполнение условия (20). Согласно определениям, множество  $J_k \setminus I_k$  образуют все наборы  $((x^1, b^1), \dots, (x^k, b^k))$ , в которых  $(x^1, \dots, x^k) \in D_{k,k}$ . Из неравенств (24) вытекает, что для них

$$\left(\frac{1-\Delta}{1+\Delta}\right)^{kT} \leq \frac{\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\}}{\mathbf{P}\{Ax^1 = b^1\} \dots \mathbf{P}\{Ax^k = b^k\}} \leq \left(\frac{1+\Delta}{1-\Delta}\right)^{kT}.$$

Поэтому из условия  $T\Delta \rightarrow 0$  следует (20).

Проверим соотношение (21) при  $k \geq 2$ . Используя условия (24) (где  $k = 1$ ) и (17), получаем, что

$$\begin{aligned} \sum_{(v^1, \dots, v^k) \in I_k} \prod_{j=1}^k \mathbf{P}\{Ax^j = b^j\} &\leq \sum_{(x^1, \dots, x^k) \in D_k} \sum_{b^1 \in B} \dots \sum_{b^k \in B} \prod_{j=1}^k \mathbf{P}\{Ax^j = b^j\} \\ &= \sum_{(x^1, \dots, x^k) \in D_k} \prod_{i=1}^k \mathbf{P}\{Ax^i \in B\} \\ &= \sum_{j=1}^{k-1} \sum_{(x^1, \dots, x^k) \in D_{k,j}} \prod_{i=1}^k \mathbf{P}\{Ax^i \in B\} \\ &\leq \sum_{j=1}^{k-1} \sum_{(x^1, \dots, x^k) \in D_{k,j}} \left(\frac{1+\Delta}{q}\right)^{kT} |B|^k \\ &= \sum_{j=1}^{k-1} |D_{k,j}| \left(\frac{1+\Delta}{q}\right)^{kT} |B|^k \\ &\leq \left(\frac{|D||B|}{q^T}\right)^k (1+\Delta)^{kT} \frac{1}{|D|^k} \sum_{j=1}^{k-1} \binom{k}{j} q^{j(k-j)} |D|^j. \end{aligned} \quad (25)$$

Из условий (14),  $T\Delta \rightarrow 0$  и  $|\Delta| \rightarrow \infty$  следует, что выражение в правой части (25) стремится к нулю при всех  $k \geq 2$ . Соотношение (21) доказано.

Наконец, проверим соотношение (22). Пусть опять  $k \geq 2$ . Из определений следует равенство

$$\sum_{(v^1, \dots, v^k) \in I_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = \sum_{(v^1, \dots, v^k) \in I_k, (x^1, \dots, x^k) \in D_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\}. \quad (26)$$

Заметим, что  $\bar{D}_{k,1} = \emptyset$ ,  $k = 2, 3, \dots$ , и положим

$$\bar{D}_k = \bigcup_{j=2}^{k-1} \bar{D}_{k,j}.$$

**Лемма 2.** Пусть  $D \times B$  не содержит подобных векторов,  $(x^1, \dots, x^k) \in D_k \setminus \bar{D}_k$ ,  $((x^1, b^1), \dots, (x^k, b^k)) \in J_k$ . Тогда

$$\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = 0.$$

*Доказательство.* Предположим противное, а именно, предположим, что для некоторого набора векторов  $(x^1, \dots, x^k) \in D_k \setminus \bar{D}_k$  выполнено неравенство

$$\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} > 0.$$

Это означает, что для некоторой реализации  $A'$  случайной матрицы  $A$  выполнен набор из  $k$  равенств  $A'x^1 = b^1, \dots, A'x^k = b^k$ . Согласно определениям, в нашем наборе  $(x^1, \dots, x^k) \in D_k \setminus \bar{D}_k$  найдутся такие векторы  $x^i \in D$ ,  $x^j \in D$ ,  $x^i \neq x^j$ , и найдется такое число  $\alpha \in K \setminus \{0\}$ , что  $x^j = \alpha x^i$ .

Пусть  $\alpha = 1$ . Тогда из равенства  $x^j = x^i$  следует, что и  $b^j = b^i$ . Последнее противоречит условию  $((x^1, b^1), \dots, (x^k, b^k)) \in J_k$ . Значит, наше предположение ошибочно.

Пусть  $q \geq 3$  и  $\alpha \neq 1$ . Тогда  $(x^i, b^i) \in D \times B$ ,  $(x^j, b^j) = \alpha(x^i, b^i) \in D \times B$ . Это противоречит условию, что множество  $D \times B$  не содержит подобных векторов. Таким образом, и в этом случае наше предположение ошибочно. Значит,  $\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = 0$ . Лемма доказана.

Из (26) и леммы 2 следует, что

$$\sum_{(v^1, \dots, v^k) \in I_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = \sum_{(v^1, \dots, v^k) \in I_k, (x^1, \dots, x^k) \in \bar{D}_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\}. \quad (27)$$

Теперь рассмотрим произвольный набор  $x^1, \dots, x^r$  векторов пространства  $V^n$ . Ему соответствует система  $L_x(x^1, \dots, x^r)$  однородных линейных уравнений вида

$$\alpha_1 x^1 \oplus \dots \oplus \alpha_r x^r = 0,$$

возможно пустая, состоящая из всех линейных соотношений, которым удовлетворяет набор  $x^1, \dots, x^r$ . Системе  $L_x(x^1, \dots, x^r)$  сопоставим идентичную по составу систему  $L_b(x^1, \dots, x^r)$  из линейных уравнений относительно  $b^1, \dots, b^r \in B$ . Обозначим через  $B(x^1, \dots, x^r)$  множество решений  $(b^1, \dots, b^r)$ ,  $b^1, \dots, b^r \in B$ , системы  $L_b(x^1, \dots, x^r)$ .

**Лемма 3.** Пусть  $(b^1, \dots, b^r) \notin B(x^1, \dots, x^r)$ ,  $(x^1, \dots, x^r) \in \bar{D}_k$ . Тогда

$$\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = 0.$$

*Доказательство.* Доказательство леммы 3 проведем аналогично доказательству леммы 2. Предположим противное, именно, что для некоторых наборов векторов  $(x^1, \dots, x^r) \in \bar{D}_k$  и  $(b^1, \dots, b^r) \notin B(x^1, \dots, x^r)$  выполнено неравенство

$$\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} > 0.$$

Тогда найдется такой набор элементов поля  $(\alpha_1, \dots, \alpha_k) \neq (0, \dots, 0)$ , что

$$\alpha_1 x^1 \oplus \dots \oplus \alpha_k x^k = 0, \quad \alpha_1 b^1 \oplus \dots \oplus \alpha_k b^k \neq 0, \quad (28)$$

и, кроме того, для некоторой реализации  $A'$  случайной матрицы  $A$  будет выполнен набор равенств

$$A'x^1 = b^1, \quad \dots, \quad A'x^k = b^k. \quad (29)$$

Очевидно, что условия (28) и (29) не могут выполняться одновременно. Следовательно,  $\mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} = 0$ . Лемма 3 доказана.

Из леммы 3 следует, что

$$\begin{aligned} & \sum_{\substack{(v^1, \dots, v^k) \in I_k \\ (x^1, \dots, x^k) \in \bar{D}_k}} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} \\ &= \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \bar{D}_{k,j}} \sum_{(b^1, \dots, b^r) \in B(x^1, \dots, x^r)} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\}. \quad (30) \end{aligned}$$

Теперь нам понадобится одно вспомогательное утверждение, связанное с характеристикой  $\rho(B)$  множества  $B$ .

**Лемма 4.** Пусть  $2 \leq j \leq k-1$  и  $(x^1, \dots, x^k) \in \bar{D}_k$ . Тогда

$$|B(x^1, \dots, x^r)| \leq \rho(B)|B|^j.$$

*Доказательство.* Так как  $\text{rank}(x^1, \dots, x^r) \leq k-1$ , система  $L_b(x^1, \dots, x^r)$  непуста. Перенумеруем векторы  $x^1, \dots, x^r$  так, чтобы первые  $j$  из них составляли базис. Преобразованная система  $L_b(x^1, \dots, x^r)$  будет содержать уравнение вида  $b^{j+1} = l_{j+1}(b^1, \dots, b^j)$ , где  $l_{j+1}$  — однородная линейная функция своих аргументов. При этом значения векторов  $b^{j+1}, \dots, b^r$  определяются однозначно векторами  $b^1, \dots, b^j$ . Поэтому величина  $|B(x^1, \dots, x^r)|$  не превосходит числа решений уравнения  $b^{j+1} = l_{j+1}(b^1, \dots, b^j)$  относительно  $b^1, \dots, b^{j+1}$ . Так как  $(x^1, \dots, x^k) \in \bar{D}_k$ , в системе  $L_b(x^1, \dots, x^r)$  нет одночленных и двучленных уравнений. Значит, уравнение  $b^{j+1} = l_{j+1}(b^1, \dots, b^j)$  содержит, по крайней мере, три существенные переменные. Не нарушая общности, можно считать, что оно имеет вид

$$b^{j+1} = \alpha_1 b^1 \oplus \alpha_2 b^2 \oplus l'_{j+1}(b^3, \dots, b^j), \quad (31)$$

где  $l'_{j+1}$  — некоторая линейная функция своих аргументов, возможно, тождественно равная нулю. Число решений уравнения (31) не превосходит суммы чисел решений этого уравнения относительно неизвестных  $b^1, b^2, b^{j+1}$  при переборе всех значений векторов  $b^3, \dots, b^j \in B$ . Следовательно, это число (и тем более, число  $|B(x^1, \dots, x^r)|$ ) не превосходит

$$N(B)|B|^{j-2} = \rho(B)|B|^j$$

(величина  $N(B)$  определена во введении). Лемма 4 доказана.

Применим лемму 4 и оценку (23) к выражению в правой части цепочки неравенств

(30), а результат подставим в (27). Получим цепочку неравенств

$$\begin{aligned}
 \sum_{(v^1, \dots, v^k) \in I_k} \mathbf{P}\{Ax^1 = b^1, \dots, Ax^k = b^k\} &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \bar{D}_{k,j}} \sum_{(b^1, \dots, b^r) \in B(x^1, \dots, x^r)} \left(\frac{1+\Delta}{q}\right)^{jT} \\
 &\leq \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \bar{D}_{k,j}} |B(x^1, \dots, x^r)| \left(\frac{1+\Delta}{q}\right)^{jT} \\
 &\leq \rho(B) \sum_{j=2}^{k-1} \sum_{(x^1, \dots, x^k) \in \bar{D}_{k,j}} |B|^j \left(\frac{1+\Delta}{q}\right)^{jT} \\
 &\leq \rho(B) \sum_{j=2}^{k-1} |\bar{D}_{k,j}| |B|^j \left(\frac{1+\Delta}{q}\right)^{jT} \\
 &\leq \rho(B) \sum_{j=2}^{k-1} \frac{|\bar{D}_{k,j}|}{|D|^j} \sum_{j=2}^{k-1} \left(\frac{(1+\Delta)^T |D| |B|}{q}\right)^j. \quad (32)
 \end{aligned}$$

В силу условий (15), (16) и  $T\Delta \rightarrow 0$ , выражение в правой части (32) стремится к нулю. Значит, условие (22) тоже выполнено, и мы можем воспользоваться многомерной версией теоремы Б. А. Севастьянова. Теорема 4 доказана.

**Лемма 5.** Пусть  $2 \leq j \leq k-1$ ,  $n \rightarrow \infty$ , а множество  $D = D(n) \subset V^n$  меняется так, что  $\rho(D) \rightarrow 0$ . Тогда

$$\frac{|\bar{D}_{k,j}|}{|D|^j} \rightarrow 0.$$

Из леммы 5 вытекает следующее утверждение.

**Следствие 6.** Пусть  $n \rightarrow \infty$ , множества  $D = D(n) \subset V^n$  и  $B = B(T) \subset V^T$  меняются так, что  $\rho(D)\rho(B) \rightarrow 0$ . Тогда при всех  $k > j \geq 2$  выполнено соотношение (16).

*Доказательство леммы 5.* Нетрудно убедиться, что  $\bar{D}_{k,1} = \emptyset$ ,  $k = 2, 3, \dots$ , а в других случаях

$$\bar{D}_{k,j} = \bigcup_{L_{k,j}} D(L_{k,j}), \quad (33)$$

где  $D(L_{k,j})$  — множество наборов  $(x^1, \dots, x^k) \in D^k$ , удовлетворяющих совокупности  $L_{k,j}$  из  $k-j$  линейных соотношений с не менее чем тремя ненулевыми коэффициентами в каждом (один из них можно положить равным единице), а объединение проводится по всем таким наборам. Их общее число не превосходит  $\left(\sum_{l=3}^k (q-1)^{l-1} \binom{k}{l}\right)^{k-j} < q^{k(k-j)}$ . Поэтому

$$|\bar{D}_{k,j}| < q^{k(k-j)} \max_{L_{k,j}} D(L_{k,j}). \quad (34)$$

Воспользуемся тем, что множество  $D(L_{k,j})$  определено по набору линейных соотношений  $L_{k,j}$  точно так же, как множество  $B(x^1, \dots, x^r)$  выше было определено системой  $L_b(x^1, \dots, x^r)$ . Поэтому их свойства во многом совпадают. В частности, наряду с леммой 4 справедливо (и доказывается теми же рассуждениями) следующее утверждение.

**Лемма 6.** Пусть  $2 \leq j \leq k - 1$ . Тогда

$$|D(L_{k,j})| \leq \rho(D)|D|^j. \quad (35)$$

Используя (34) и (35), получаем, что

$$|\bar{D}_{k,j}| \leq q^{k(k-j)} \rho(D)|D|^j.$$

Значит, из соотношения  $\rho(D) \rightarrow 0$  следует, что  $|\bar{D}_{k,j}|/|D|^j \rightarrow 0$ . Лемма 5 доказана.

*Доказательство теоремы 2.* Заметим, что условия теоремы 4 (с точностью до замены условия (9) условием (16)) повторяют условия теоремы 2 применительно к подмножествам  $R_1, \dots, R_s$  множества  $J \subseteq D \times B$ . Возьмем  $J = D \times B$ ,  $R_j = D \times B_j$ ,  $j = 1, \dots, s$ ,  $B = B_1 \cup \dots \cup B_s$ . Тогда  $\lambda'_j = \lambda_j$ ,  $j = 1, \dots, s$ . Используя теорему 4 и следствие 6, получаем утверждение теоремы 2.

*Доказательство теоремы 3.* Напомним, что согласно (11)

$$l_r(D, B) = |\{k \in \{1, \dots, M\} : |DB_k| = r\}|, \quad r = 1, \dots, q - 1.$$

где  $DB_1, \dots, DB_M$  — разбиение множества  $D \times B$  на классы подобных векторов и  $M$  — общее число таких классов. Выберем из каждого множества  $DB_k$  по одному произвольному вектору  $db_k \in DB_k$  и положим  $J = \{db_1, db_2, \dots, db_M\} \subseteq D \times B$ . Построим разбиение этого множества на непересекающиеся множества  $R_1, \dots, R_{q-1}$  по правилу

$$R_k = |\{db_k : k \in \{1, \dots, M\}, |DB_k| = r\}|, \quad r = 1, \dots, q - 1, \quad (36)$$

и введем случайные величины

$$\xi_r = \sum_{(x,b) \in R_k} I\{Ax = b\}, \quad r = 1, \dots, q - 1, \quad (37)$$

с множествами  $R_1, \dots, R_{q-1}$  из (36). Тогда

$$\xi(D, A, B) = \xi_1 + 2\xi_2 + \dots + (q - 1)\xi_{q-1}. \quad (38)$$

Используя предположения теоремы 3 и следствие 6, нетрудно убедиться, что для случайных величин (37) выполнены условия теоремы 4, причем  $\lambda'_j = \lambda_j$ ,  $j = 1, \dots, q - 1$ . Поэтому, согласно теореме 4, распределение вектора  $(\xi_1, \dots, \xi_{q-1})$  сходится к распределению вектора  $(\pi_1, \dots, \pi_{q-1})$ , компоненты которого определены в формулировке теоремы 3. Осталось воспользоваться равенством (38). Теорема 3 доказана.

## 5. Доказательство теоремы 1

Размерность пространства в этом разделе обозначим символом  $T$ . Во всех предельных переходах считается, что  $T \rightarrow \infty$ . Будем также использовать обозначения

$$S_r(d) = \{x = (x^1, \dots, x^T) \in V^T : 1 \leq \|x - d\| \leq r\},$$

$$S'_r(d) = \{x = (x^1, \dots, x^T) \in V^T : \|x - d\| = r\}.$$

Пусть  $B$  — заданное подмножество  $V^T$ ,  $a_1, a_2, a_3 \in K \setminus \{0\}$ ,  $d \in V^T$  и  $N(a_1, a_2, a_3, d, B)$  — число решений уравнения

$$a_1 u^1 \oplus \dots \oplus a_3 u^3 = d \quad (39)$$

относительно тройки  $(u^1, u^2, u^3) \in B^3$ . Пусть  $T \rightarrow \infty$ . Нас интересуют условия на характер изменения множества  $B$ , при которых для величины

$$\rho(B) = \frac{N(B)}{|B|^2},$$

где

$$N(B) = \max_{a_1, a_2, a_3, d} N(a_1, a_2, a_3, d, B),$$

выполнено соотношение  $\rho(B) \rightarrow 0$ .

Пусть случайные векторы  $\xi^1, \xi^2$  выбраны случайно и независимо из множества  $B$  в соответствии с равномерным распределением на нем. Тогда

$$N(a_1, a_2, a_3, d, B) = |B|^2 \mathbf{P}\{a_1 \xi^1 \oplus a_2 \xi^2 \in a_3 B \oplus d\},$$

а условие  $\rho(B) \rightarrow 0$  эквивалентно соотношению

$$\max_{a_1, a_2, a_3, d} \mathbf{P}\{a_1 \xi^1 \oplus a_2 \xi^2 \in a_3 B \oplus d\} \rightarrow 0. \quad (40)$$

Когда множество  $B$  замкнуто относительно умножения на ненулевые элементы поля, это соотношение можно упростить, взяв в качестве множителей  $a_1, a_2, a_3$  единицы. В частности, когда  $B = S_r(0)$ , условие (3) принимает вид

$$\max_d \mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d)\} \rightarrow 0. \quad (41)$$

Аналогичный вид это условие принимает в случае, когда  $B = S'_r(0)$ .

Для доказательства теоремы 1 потребуется информация об асимптотических свойствах суммы случайных векторов  $\xi^1$  и  $\xi^2$ , которую мы получим из следующей леммы.

**Лемма 7.** Пусть множество  $B \in \{S_r(0), S'_r(0)\}$ , случайные векторы  $\xi^1, \xi^2, \dots, \xi^s$ ,  $s \geq 2$ , выбраны случайно и независимо в соответствии с равномерным распределением на множестве  $B$  и для параметров  $T, r$  выполнены условия

$$T \rightarrow \infty, \quad r \rightarrow \infty, \quad rT^{-1} \leq \rho < (q-1)/q. \quad (42)$$

Тогда при любом  $\varepsilon > 0$

$$\mathbf{E}\|\xi^1 \oplus \dots \oplus \xi^s\| = r \sum_{k=0}^{s-1} \left(1 - \frac{r}{T} \frac{q}{q-1}\right)^k (1 + O(r^{\varepsilon-1})), \quad (43)$$

$$\mathbf{D}\|\xi^1 \oplus \dots \oplus \xi^s\| = O(r^{1+\varepsilon}). \quad (44)$$

В случае  $S'_r(0)$  множитель  $1 + O(r^{\varepsilon-1})$  в соотношении (43) равен единице, а равенство (44) принимает вид

$$\mathbf{D}\|\xi^1 \oplus \dots \oplus \xi^s\| = O(r).$$

*Доказательство.* Пусть  $B = S_r(0)$ . Положим

$$\eta_i(s) = I\{(\xi^1 \oplus \dots \oplus \xi^s)_i \neq 0\}, \quad i = 1, \dots, T,$$

где  $(x)_i$  —  $i$ -я координата вектора  $x$ . Тогда

$$\mathbf{E}\|\xi^1 \oplus \dots \oplus \xi^s\| = \sum_{i=1}^T \mathbf{P}\{\eta_i(s) = 1\}. \quad (45)$$

Найдем величины  $\mathbf{P}\{\eta_i(s) = 1\}$ . Введем обозначения

$$p_i(\alpha | \beta) = \mathbf{P}\{\eta_i(s+1) = \alpha \mid \eta_i(s) = \beta\}, \quad \alpha, \beta \in \{0, 1\}. \quad (46)$$

Тогда при всех  $s = 1, 2, \dots$

$$\begin{aligned} \mathbf{P}\{\eta_i(s+1) = 1\} &= \mathbf{P}\{\eta_i(s) = 1\}p_i(1 | 1) + \mathbf{P}\{\eta_i(s) = 0\}p_i(1 | 0) \\ &= \mathbf{P}\{\eta_i(s) = 1\}(p_i(1 | 1) - p_i(1 | 0)) + p_i(1 | 0). \end{aligned} \quad (47)$$

Используя рекуррентное соотношение (47), получаем для производящей функции

$$\varphi(z) = \sum_{s=1}^{\infty} \mathbf{P}\{\eta_i(s) = 1\}z^s$$

равенство

$$\varphi(z)(1 - z(p_i(1 | 1) - p_i(1 | 0))) = p_i(1 | 0) \sum_{s=1}^{\infty} z^s + z(\mathbf{P}\{\eta_i(1) = 1\} - p_i(1 | 0)).$$

Согласно определениям,

$$\mathbf{P}\{\eta_i(1) = 1\} = p_i(1 | 0).$$

Поэтому

$$\varphi(z) = p_i(1 | 0) \sum_{s=1}^{\infty} z^s \sum_{s=0}^{\infty} (p_i(1 | 1) - p_i(1 | 0))^s z^s.$$

Разлагая это выражение в степенной ряд, получаем, что

$$\mathbf{P}\{\eta_i(s) = 1\} = p_i(1 | 0) \sum_{k=0}^{s-1} (p_i(1 | 1) - p_i(1 | 0))^k. \quad (48)$$

Осталось найти величины  $p_i(1 | \alpha)$ ,  $\alpha \in \{0, 1\}$ . Согласно (46),

$$\begin{aligned} p_i(1 | 1) &= \mathbf{P}\{\xi_i^{s+1} = 0\} + \mathbf{P}\{\xi_i^{s+1} \neq 0, \xi_i^{s+1} \neq -(\xi_i^1 + \dots + \xi_i^s)\}, \\ p_i(1 | 0) &= \mathbf{P}\{\xi_i^{s+1} \neq 0\}. \end{aligned} \quad (49)$$

Раскрывая слагаемые в правых частях равенств (49), получаем равенства

$$\begin{aligned} p_i(1 | 1) &= \frac{1}{|S_r(0)|} \sum_{w=1}^r \binom{T}{w} (q-1)^w \left(1 - (q-1)^{-1} \frac{w}{T}\right), \\ p_i(1 | 0) &= \frac{1}{|S_r(0)|} \sum_{w=1}^r \binom{T}{w} (q-1)^w \frac{w}{T} = \mathbf{P}\{\eta_i(1) = 1\}. \end{aligned} \quad (50)$$

Значит,

$$p_i(1 | 1) - p_i(1 | 0) = \frac{1}{|S_r(0)|} \sum_{w=1}^r \binom{T}{w} (q-1)^w \left(1 - \frac{q}{q-1} \frac{w}{T}\right), \quad (51)$$

где

$$|S_r(0)| = \sum_{w=1}^r \binom{T}{w} (q-1)^w.$$

Из (45), (48) и (51) следует, что

$$\begin{aligned} \mathbf{E}\|\xi^1 \oplus \dots \oplus \xi^s\| &= \frac{1}{\sum_{w=1}^r \binom{T}{w} (q-1)^w} \sum_{w=1}^r \binom{T}{w} (q-1)^w w \\ &\times \sum_{k=0}^{s-1} \left( \frac{1}{\sum_{w=1}^r \binom{T}{w} (q-1)^w} \sum_{w=1}^r \binom{T}{w} (q-1)^w \left(1 - \frac{q}{q-1} \frac{w}{T}\right) \right)^k. \end{aligned} \quad (52)$$

Стандартными рассуждениями нетрудно показать, что при условии (42) и любых  $m, \varepsilon > 0$

$$\frac{1}{\sum_{w=1}^r \binom{T}{w} (q-1)^w} \sum_{w=1}^r \binom{T}{w} (q-1)^w w^m = r^m (1 + O(r^{\varepsilon-1})). \quad (53)$$

Поэтому из (50) следует, что

$$\begin{aligned} p_i(1 | 1) &= \left(1 - \frac{r}{T(q-1)}\right) (1 + O(r^{\varepsilon-1})), \\ p_i(1 | 0) &= \frac{r}{T} (1 + O(r^{\varepsilon-1})), \end{aligned} \quad (54)$$

а из (52) следует (43).

Оценим дисперсию  $\mathbf{D}\|\xi^1 \oplus \dots \oplus \xi^s\|$ . Введем обозначения

$$\begin{aligned} P_i^{(\alpha)}(s) &= \mathbf{P}\{\eta_i(s) = \alpha\}, \\ P_{i,j}^{(\alpha,\beta)}(s) &= \mathbf{P}\{\eta_i(s) = \alpha, \eta_j(s) = \beta\} \end{aligned}$$

и запишем равенство

$$\begin{aligned} \mathbf{D}\|\xi^1 \oplus \dots \oplus \xi^s\| &= \mathbf{D}(\eta_1(s) + \dots + \eta_T(s)) \\ &= \sum_{i=1}^T P_i^{(1)}(s)(1 - P_i^{(1)}(s)) + 2 \sum_{1 \leq i < j \leq T} (P_{i,j}^{(1,1)}(s) - P_i^{(1)}(s)P_j^{(1)}(s)). \end{aligned} \quad (55)$$

Задача сводится к вычислению величин  $P_{i,j}^{(1,1)}(s)$ . Для этого используем соотношения

$$P_{i,j}^{(1,1)}(s+1) = \sum_{\alpha, \beta \in \{0,1\}} P_{i,j}^{(\alpha,\beta)}(s) p_{i,j}(1,1 | \alpha, \beta), \quad s = 1, 2, \dots, \quad (56)$$

$$p_{i,j}(1,1 | \alpha, \beta) = \mathbf{P}\{\eta_i(s+1) = 1, \eta_j(s+1) = 1 | \eta_i(s) = \alpha, \eta_j(s) = \beta\}.$$



Вычислим сначала величины  $P_{i,j}^{(\alpha,\beta)}(1)$  и  $p_{i,j}(1, 1 | \alpha, \beta)$ . Справедливо равенство

$$P_{i,j}^{(\alpha,\beta)}(1) = \alpha\beta\mathbf{P}\{\xi_i^1 \neq 0, \xi_j^1 \neq 0\} + (1-\alpha)\beta\mathbf{P}\{\xi_i^1 = 0, \xi_j^1 \neq 0\} \\ + \alpha(1-\beta)\mathbf{P}\{\xi_i^1 \neq 0, \xi_j^1 = 0\} + (1-\alpha)(1-\beta)\mathbf{P}\{\xi_i^1 = 0, \xi_j^1 = 0\}.$$

Следовательно,

$$P_{i,j}^{(\alpha,\beta)}(1)|S_r(0)| = \alpha\beta \sum_{w=2}^r \binom{T-2}{w-2} (q-1)^w + (\alpha + \beta - 2\alpha\beta) \sum_{w=1}^r \binom{T-2}{w-1} (q-1)^w \\ + (1-\alpha)(1-\beta) \sum_{w=1}^r \binom{T-2}{w} (q-1)^w \\ = \alpha\beta \sum_{w=2}^r \binom{T}{w} (q-1)^w \frac{w(w-1)}{T(T-1)} \\ + (\alpha + \beta - 2\alpha\beta) \sum_{w=1}^r \binom{T}{w} (q-1)^w \frac{w(T-w)}{T(T-1)} \\ + (1-\alpha)(1-\beta) \sum_{w=1}^r \binom{T}{w} (q-1)^w \frac{(T-w)(T-w-1)}{T(T-1)}.$$

Отсюда и из (53) получаем, что

$$\frac{P_{i,j}^{(\alpha,\beta)}(1)}{1 + O(r^{\varepsilon-1})} = \alpha\beta \left(\frac{r}{T}\right)^2 + (\alpha + \beta - 2\alpha\beta) \frac{r}{T} \left(1 - \frac{r}{T}\right) \\ + (1-\alpha)(1-\beta) \left(1 - \frac{r}{T}\right)^2, \\ \frac{P_i^{(\alpha)}(1)}{1 + O(r^{\varepsilon-1})} = \alpha \frac{r}{T} + (1-\alpha) \left(1 - \frac{r}{T}\right). \quad (57)$$

Поэтому

$$P_{i,j}^{(\alpha,\beta)}(1) = P_i^{(\alpha)}(1)P_j^{(\beta)}(1) (1 + O(r^{\varepsilon-1})). \quad (58)$$

Аналогично доказывается, что при  $\alpha, \beta \in \{0, 1\}$

$$p_{i,j}(1, 1 | \alpha, \beta) = p_i(1 | \alpha)p_j(1 | \beta)(1 + O(r^{\varepsilon-1})). \quad (59)$$

Действительно (здесь мы опускаем промежуточные выкладки),

$$p_{i,j}(1, 1 | \alpha, \beta)|S_r(0)| \\ = \alpha\beta \sum_{w=1}^r \left( \binom{T-2}{w} (q-1)^w + 2 \binom{T-2}{w-1} (q-2)(q-1)^{w-1} + \binom{T-2}{w-2} (q-2)^2 (q-1)^{w-2} \right) \\ + (\alpha + \beta - 2\alpha\beta) \sum_{w=1}^r \left( \binom{T-2}{w-1} (q-1)^w + \binom{T-2}{w-2} (q-2)(q-1)^{w-1} \right) \\ + (1-\alpha)(1-\beta) \sum_{w=1}^r \binom{T-2}{w-2} (q-1)^w, \quad (60)$$

где полагаем  $\binom{n}{v} = 0$  при  $v < 0$ . Воспользуемся теперь (53) и получим равенство

$$\frac{p_{i,j}(1, 1 | \alpha, \beta)}{1 + O(r^{\varepsilon-1})} = \alpha\beta \left(1 - \frac{r}{(q-1)T}\right)^2 + (\alpha + \beta - 2\alpha\beta) \frac{r}{T} \left(1 - \frac{r}{(q-1)T}\right) + (1-\alpha)(1-\beta) \left(\frac{r}{T}\right)^2. \quad (61)$$

Из (61) и (54) получаем (59). Теперь, используя рекуррентную формулу (56) и соотношения (58), (59), индукцией по значениям  $s$  выводим оценки

$$P_{i,j}^{(1,1)}(s) = P_i^{(1)}(s)P_j^{(1)}(s)(1 + O(r^{\varepsilon-1})), \quad s = 1, 2, \dots, \quad (62)$$

равномерные по  $1 \leq i < j \leq T$ . Из (55) и (62) с учетом соотношений

$$\sum_{i=1}^T P_i^{(1)}(s) = \mathbf{E}\|\xi^1 \oplus \dots \oplus \xi^s\| = O(r)$$

получаем оценку (44).

Если  $B = S_r'(0)$ , то доказательство соотношений (43) и (44) повторяет (с очевидными упрощениями) доказательство для случая, когда  $B = S_r(0)$ . При этом множитель  $1 + O(r^{\varepsilon-1})$  в (43) заменяется единицей, а для дисперсии вместо (44) получается оценка

$$\mathbf{D}\|\xi^1 \oplus \dots \oplus \xi^s\| = O(r).$$

Лемма 7 доказана.

*Доказательство теоремы 1.* Проверим свойство (3) для множества  $B = S_r(0)$ . Пусть  $\xi^1$  и  $\xi^2$  — независимые случайные векторы, распределенные на множестве  $S_r(0)$  равномерно. Так как их распределения инвариантны относительно перестановки и умножения координат на ненулевые элементы поля, то этими же свойствами обладает и их сумма  $\xi^1 \oplus \xi^2$ . Поэтому при  $\|x\| = k$ ,  $k = 0, 1, \dots$ ,

$$\mathbf{P}\{\xi^1 \oplus \xi^2 = x\} = \frac{1}{(q-1)^k \binom{T}{k}} \mathbf{P}\{\|\xi^1 \oplus \xi^2\| = k\}. \quad (63)$$

Сначала проверим выполнение условия (41) при условии (42), то есть  $T, r \rightarrow \infty$ ,  $rT^{-1} \leq \rho < (q-1)/q$ , а затем рассмотрим случай, когда  $T \rightarrow \infty$ ,  $1 \leq r = O(1)$ . Согласно лемме 7, при любом  $\varepsilon > 0$

$$\begin{aligned} \mathbf{E}\|\xi^1 \oplus \xi^2\| &= r_2(1 + O(r^{\varepsilon-1})), \\ \mathbf{D}\|\xi^1 \oplus \xi^2\| &= O(r^{1+\varepsilon}), \end{aligned} \quad (64)$$

где

$$r_2 = r + r \left(1 - \frac{r}{T} \frac{q}{q-1}\right). \quad (65)$$

Исходя из (65) и неравенств  $rT^{-1} \leq \rho < (q-1)/q$ , выберем такое  $0 < \varepsilon < 1$ , что

$$r(1 + \varepsilon) < r_2(1 - \varepsilon), \quad r_2(1 + \varepsilon) < T(q-1)/q. \quad (66)$$

Используя (63), получаем, что

$$\begin{aligned}
\mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d)\} &= \mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d), \|\xi^1 \oplus \xi^2\| \leq r_2(1-\varepsilon)\} \\
&\quad + \mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d), \|\xi^1 \oplus \xi^2\| \geq r_2(1+\varepsilon)\} \\
&\quad + \mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d), r_2(1-\varepsilon) < \|\xi^1 \oplus \xi^2\| < r_2(1+\varepsilon)\} \\
&\leq \mathbf{P}\{\|\xi^1 \oplus \xi^2\| \leq r_2(1-\varepsilon)\} + \mathbf{P}\{\|\xi^1 \oplus \xi^2\| \\
&\leq r_2(1+\varepsilon)\} + \sum_{r_2(1-\varepsilon) < k < r_2(1+\varepsilon)} \frac{|S_r(d)|}{(q-1)^k \binom{T}{k}} \mathbf{P}\{\|\xi^1 \oplus \xi^2\| = k\}. \quad (67)
\end{aligned}$$

Из соотношений (64) и неравенства Чебышёва следует, что первое и второе слагаемые в правой части неравенства (67) стремятся к нулю. В силу правого неравенства (66), в интервале  $r_2(1-\varepsilon) < k < r_2(1+\varepsilon)$  величина  $(q-1)^k \binom{T}{k}$  возрастает вместе с  $k$  (эта величина имеет точку максимума  $k^*$ ,  $k^*/T \rightarrow (q-1)/q$  при  $T \rightarrow \infty$ ). Кроме того,

$$|S_r(d)| < r(q-1)^r \binom{T}{r}.$$

Поэтому

$$\begin{aligned}
\sum_{r_2(1-\varepsilon) < k < r_2(1+\varepsilon)} \frac{|S_r(d)|}{(q-1)^k \binom{T}{k}} \mathbf{P}\{\|\xi^1 \oplus \xi^2\| = k\} &\leq \frac{|S_r(d)|}{(q-1)^{\lfloor r_2(1-\varepsilon) \rfloor} \binom{T}{\lfloor r_2(1-\varepsilon) \rfloor}} \\
&\leq \frac{r(q-1)^r \binom{T}{r}}{(q-1)^{\lfloor r_2(1-\varepsilon) \rfloor} \binom{T}{\lfloor r_2(1-\varepsilon) \rfloor}}, \quad (68)
\end{aligned}$$

где  $\lfloor a \rfloor$  — целая часть числа  $a$ . В силу левого неравенства в (66), последняя дробь в (68) стремится к нулю.

Таким образом,

$$\mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d)\} \rightarrow 0$$

при  $T \rightarrow \infty$ ,  $r \rightarrow \infty$ ,  $rT^{-1} \leq \rho < (q-1)/q$  равномерно по  $d \in V^T$ . Осталось отметить, что при  $T \rightarrow \infty$ ,  $1 \leq r = O(1)$ , выполнено соотношение

$$\mathbf{P}\{\|\xi^1 \oplus \xi^2\| = 2r\} \rightarrow 1,$$

поэтому

$$\mathbf{P}\{\xi^1 \oplus \xi^2 \in S_r(d)\} \leq \mathbf{P}\{\|\xi^1 \oplus \xi^2\| \neq 2r\} + \mathbf{P}\{\|\xi^1 \oplus \xi^2\| = 2r\} \frac{|S_r(d)|}{(q-1)^{2r} \binom{T}{2r}} \rightarrow 0.$$

Значит, в условиях теоремы 1 свойства (41) и  $\rho(S_r(0)) \rightarrow 0$  выполнены. Тогда (см. замечание 1) и  $\rho(S_r(b^0)) \rightarrow 0$ .

Доказательство теоремы в случае, когда  $B = S'_r(b^0)$  повторяет предшествующие рассуждения с заменой во всех выкладках множества  $S_r(d)$  множеством  $S'_r(d)$  и заменой в правой части последнего неравенства (68) множителя  $r$  единицей. Теорема 1 доказана.

Авторы благодарны А. М. Зубкову и Б. А. Севастьянову за полезные замечания.

## Список литературы

1. Копытцев В. А., О числе решений систем линейных булевых уравнений в множестве векторов, обладающих заданным числом единиц. *Дискретная математика* (2002) **14**, №4, 87–109.
2. Копытцев В. А., О числе решений системы случайных линейных уравнений. *Дискретная математика* (2006) **18**, №1, 40–62.
3. Михайлов В. Г., О предельной теореме Б. А. Севастьянова для сумм зависимых случайных индикаторов. *Обозрение прикладной и промышленной математики* (2003) **10**, №3, 571–578.
4. Михайлов В. Г., Предельные теоремы для числа точек случайного линейного подпространства, попавших в заданное множество. *Дискретная математика* (2003) **15**, №2, 128–137.
5. Михайлов В. Г., Предельные теоремы для числа решений системы случайных линейных уравнений, попавших в заданное множество. *Дискретная математика* (2007) **19**, №1, 17–26.

Статья поступила 11.03.2010.